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

Mike Delaguardia
Matthew Hyatt
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

Christopher Altman
Marco Genovese
Google Cloud
Mill Valley, CA

Nalini Kannan
John Dombroski
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

Joey Cruz
Carmichael Patton
Microsoft
Redmond, WA

Vinu Panicker
Okta
San Francisco, CA

Seetal Patel
Norman Wong
Palo Alto Networks
Santa Clara, CA

Shawn Higgins
Rob Woodworth
PC Matic
Myrtle Beach, SC

Mitchell Lewars
Bryan Rosensteel
Ping Identity
Denver, CO

Don Coltrain
Wade Ellery
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

Peter Bjork
Genc Domi
VMware
Palo Alto, CA

Joe Brown
Jim Kovach
Zimperium
Dallas, TX

Syed Ali
Bob Smith
Zscaler
San Jose, CA

August 2023

THIRD 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, 270 pages, August 2023, 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 22, 2023 to October 9, 2023

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

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

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
Madhu Balaji	Amazon Web Services
Harrison Holstein	Amazon Web Services
Quint Van Deman	Amazon Web Services
Jason Garbis	Appgate
Adam Rose	Appgate
Jonathan Roy	Appgate
Eric Michael	Broadcom Software
Ken Andrews	Cisco
Robert Bui	Cisco
Brian Butler	Cisco
Leo Lebel	Cisco
Randy Martin	Cisco

Name	Organization
Tom Oast	Cisco
Aaron Rodriguez	Cisco
Peter Romness	Cisco
Steve Vetter	Cisco
Micah Wilson	Cisco
Daniel Cayer	F5
David Clark	F5
Jay Kelley	F5
Tim Jones	Forescout
Yejin Jang	Forescout
Tim Knudson	Google Cloud
Nilesh Atal	IBM
Andrew Campagna	IBM
Adam Frank	IBM
Himanshu Gupta	IBM
Lakshmeesh Hegde	IBM
Sharath Math	IBM
Naveen Murthy	IBM

Name	Organization
Priti Patil	IBM
Nikhil Shah	IBM
Deepa Shetty	IBM
Harmeet Singh	IBM
Harishkumar Somashekaraiah	IBM
Mike Spisak	IBM
Krishna Yellepeddy	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
Tarek Dawoud	Microsoft
Janet Jones	Microsoft
Hemma Prafullchandra	Microsoft

Name	Organization
Enrique Saggese	Microsoft
Brandon Stephenson	Microsoft
Clay Taylor	Microsoft
Sarah Young	Microsoft
Spike Dog	MITRE
Sallie Edwards	MITRE
Ayayidjin Gabiam	MITRE
Jolene Loveless	MITRE
Karri Meldorf	MITRE
Kenneth Sandlin	MITRE
Lauren Swan	MITRE
Jessica Walton	MITRE
Mike Bartock	NIST
Gema Howell	NIST
Douglas Montgomery	NIST
Kevin Stine	NIST
Sean Frazier	Okta
Kelsey Nelson	Okta

Name	Organization
Ali Haider	Palo Alto Networks
Sean Morgan	Palo Alto Networks
Imran Bashir	Palo Alto Networks
Zack Austin	PC Matic
Andy Tuch	PC Matic
Ivan Anderson	Ping Identity
Aubrey Turner	Ping Identity
Bill Baz	Radiant Logic
Rusty Deaton	Radiant Logic
Deborah McGinn	Radiant Logic
John Petrutiu	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

Name	Organization
Keith Luck	VMware
Paul Mancuso	VMware
Dennis Moreau	VMware*
Wayne Pauley	VMware
Jacob Rapp	VMware*
Jeffrey Adorno	Zscaler
Jeremy James	Zscaler
Lisa Lorenzin	Zscaler*
Matt Moulton	Zscaler
Patrick Perry	Zscaler

** Former employee; all work for this publication was done while at that organization*

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
AWS
Broadcom Software
Cisco
DigiCert
F5
Forescout
Google Cloud
IBM
Ivanti
Lookout
Mandiant
Microsoft
Okta
Palo Alto Networks
PC Matic
Ping Identity
Radiant Logic
SailPoint
Tenable
Trellix
VMware
Zimperium
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

List of Tables

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. Please note the demonsration results are based on the results at the time of demonstration and represent a snapshot in time.

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 third preliminary draft, we will publish at least one additional draft for public comment before it is finalized.

This guide contains five 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 in a controlled laboratory setting with each of the example implementations **(you are here)**
- NIST SP 1800-35E: *Risk and Compliance Management* – risk analysis and mapping of ZTA security characteristics to cybersecurity standards and recommended practices

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.

Also, Section 3 of *Risk and Compliance Management*, *NIST SP 1800-35E,* will be of particular interest. Section 3, ZTA Reference Architecture Security Mappings, maps logical components of the general ZTA reference design to security characteristics listed in various cybersecurity guidelines and recommended practices documents, including *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework), *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53), and *Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028*.

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 third preliminary draft guide. As the project progresses, the third 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 Lab Demonstration

This section is intended to assist the lab 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 noncompliant 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 lab demonstration playbook is not exhaustive for all enterprise operations, and it does not capture all possible demonstration cases.

Several demonstration scenarios listed here are presented as a maximal approach to zero trust. This includes assumptions about user intent that may not always be determined in an actual operational setting. For example, subjects may be classified as compromised in some way so that all access requests are part of an intentional attack and not mistaken queries from valid (uncompromised) subjects. As such, some demonstrations may seem extreme for most enterprise operations. This is only to demonstrate the most extreme cases, as a less severe response such as logging and/or sending an alert to a human administrator is also possible.

This collection of demonstration scenarios 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.

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]. Here, a *network identity* is used here simply as an identity that allows the subject to identify itself to all (network) connected enterprise resources. The following definitions are used for network IDs:

- **Enterprise-ID:** An ID issued and maintained by the enterprise. It is stored in one (or more) identity stores maintained by the enterprise.
- **Federated-ID:** An 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:** An 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 ID unknown to the enterprise that the enterprise would be unable to authenticate. This is also referred to as a “guest” to the enterprise. No-ID will also be used to indicate an anonymous subject that does not present any ID.

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. An EP could be physical (e.g., a laptop) or virtual (e.g., virtual machine or container). Each EP should be able to be uniquely identified by the enterprise.
- **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. Like EP above, each RSS should be uniquely identified by the enterprise.
- **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 is not managed. A BYOD is usually acting as the requesting subject or as the target of a management utility. A BYOD device may be uniquely identified by the enterprise.

- **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. Guest devices are not assumed to be uniquely identified by the enterprise.

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. An endpoint is considered to be in compliance if both of the above are true.
- **(EIG) Resource Compliance:** Policy that requires the enterprise-managed resource to be identified and to conform to the enterprise security policy for the resource. A resource is considered to be in compliance if both of the above are true.

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 for the enterprise. This result is only applicable to select on-premises (or branch) demonstrations. This does not grant the endpoint any privileges beyond the ability to send traffic on the network.
- **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. This does not grant the endpoint any privileges beyond the ability to send traffic on the network. Traffic bound for external Internet connected resources may be further screened or monitored.
- **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. This does not grant the endpoint any privileges beyond the ability to send traffic on the network that may be restricted to only provide reachability to a select set of services.
- **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. This means the endpoint cannot send queries to any resource.
- **Access (to Resource) Successful:** Access to the resources that are specified in the profile is achieved. The subject initiates a session with the authorized privileges.

- **Access (to Resource) Limited:** Access to a subset, but not all, of the resources that are specified in the profile is achieved. The subject initiates a session with a restricted subset of the authorized privileges.
- **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. This is similar to Limited Access to Network (above), but may allow the endpoint to access a set of resources beyond enterprise endpoint management/update services.
- **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 and verified
A-	Authentication not successful	One or more credentials were not verified such as password failure, multifactor authentication (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	One or more credentials were not verified such as password failure, MFA failure, account does not exist, account blocked, suspicious activity
A	Actively authenticated	Previously authenticated and 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. The Downgrade Trigger Examples are situations where the access would be restricted from the original Access Profile to remove some of the capabilities. For example, moving UP-E1 from P_FULL to a temporary P_LIMITED for the scenario.

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.

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

This setup enabled the following dual-purpose MSV deployment:

1. **A typical MSV deployment, in which each enterprise deploys MSV as an application within its own enterprise and uses it for self-auditing and testing.** Each enterprise deploys a director and multiple actors that function as applications within the enterprise, enabling the enterprise to monitor and test its own enterprise security capabilities, verifying the protections it receives from the ZTA and its ability to operate as expected. In this capacity, MSV is treated just like any other application deployed within that enterprise. The components may be protected by PEPs according to enterprise policies, and directors and actors exchange traffic over the same data communications paths as other enterprise applications. Firewalls and policies within the ZTA must be configured to permit the communications that the MSV components send and receive, including traffic that is sent between actors and the director to control the actions that are performed to test various security controls.

2. **The NCCoE project team, as testers, use MSV to monitor and audit enterprise and 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 operating system [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. The enterprise endpoint management system should be able to differentiate between enterprise-owned and non-owned endpoints and place devices on the correct network segment.

Table 2-6 Scenario A-1 Demonstrations

Demo ID		Subj Type	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	Desired Outcome
A-1.1	a	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		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
A-1.2	a	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
	m	Guest Dev.	---	---	---		Access to Public Network
A-1.3	a	EP	Y	A+	Y		Access to Network

Demo ID		Subj Type	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	Desired Outcome
	b	EP	Y	A+	N	Remote	Max. Limited Access to Network
	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 Network
	f	BYOD	Y	A-	---		No Access to Network
A-1.4	a	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 Network
	g	EP	Y	A-	---		No Access to Network

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		Subj Type	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	Desired Outcome
A-2.1	a	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

Demo ID		Subj Type	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	Desired Outcome
	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
	g	BYOD	Y	RA+	Y		Keep Access to Network
	h	BYOD	Y	RA+	N		Max. Limited Access to Network
	i	BYOD	Y	RA-	---		Terminate Access to Network
A-2.2	a	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 Network
	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 Network
	i	BYOD	Y	RA-	---		Terminate Access to Network
A-2.3	a	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
A-2.4	a	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

Demo ID		Subj Type	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	Desired Outcome
	e	EP	Y	RA+	N		Max. Limited Access to Network
	f	EP	Y	RA-	---		Terminate Access to Network

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.

Purpose and Outcome: This scenario demonstrates the discovery and recording of metadata of traffic flows between resources and user access requests/actions. The actual inspection of traffic (e.g., inspection of data) is not necessary.

Table 2-8 Scenario A-3 Demonstrations

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

2.5 Use Case B: Enterprise-ID Access

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

Each activity demonstrates the capability of authentication from within a given setting. The access is authenticated with an “enterprise-ID” using an enterprise-owned endpoint (EP) as well as a privately owned endpoint (BYOD). Each scenario provides a set of pre-conditions as well as multiple demonstrations. Each scenario could be repeated using different transport protocols (TCP- and UDP-based protocols).

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

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

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

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

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

Table 2-9 Scenario B-1 Demonstrations

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
B-1.1	a	E1	On-Prem → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	E1		A-	A	---	---	Y	---	Access Not Successful
	d	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	E2		A-	A	---	---	Y	---	Access Not Successful
	g	E3		A-	A	---	---	Y	---	Access Not Successful
	h	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	E1		RA+	A	A	RSS1	N	Y	Access Not Successful

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

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

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

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
	k	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	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. This is to simulate an enterprise that may have policies around accessing public Internet resources using enterprise-owned devices.

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

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

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

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

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

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

Table 2-11 Scenario B-3 Demonstrations

Demo ID		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	E6	On-Prem On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	E6		A-	---	N	Access Not Successful	---
	c	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	E6		A	A-	N	Keep Access	Access Not Successful
	e	E6		---	A+	N	---	Access Successful
	f	E6		---	A-	N	---	Access Not Successful
	g	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	E6		A-	A	N	Access Not Successful	Keep Access
	i	E7		A+	---	Y	Access Successful	---
	j	E7		A	A-	Y	Keep Access	Access Not Successful
	k	E7		---	A-	Y	---	Access Not Successful
	l	E7		RA+	---	Y	Access Successful	---
	m	E7		---	RA-	Y	---	Access Not Successful
	n	E7		---	A	Y	---	All Sessions Terminated

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	o	E7		A	---	Y	All Sessions Terminated	---
B-3.2	a	E6	On-Prem Branch → On-Prem	A+	---	N	Access Successful	---
	b	E6		A-	---	N	Access Not Successful	---
	c	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	E6		A	A-	N	Keep Access	Access Not Successful
	e	E6		---	A+	N	---	Access Successful
	f	E6		---	A-	N	---	Access Not Successful
	g	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	E6		A-	A	N	Access Not Successful	Keep Access
	i	E7		A+	---	Y	Access Successful	---
	j	E7		A	A-	Y	Keep Access	Access Not Successful
	k	E7		---	A-	Y	---	Access Not Successful
	l	E7		RA+	---	Y	Access Successful	---
	m	E7		---	RA-	Y	---	Access Not Successful
	n	E7		---	A	Y	---	Change to Access Limited
	o	E7		A	---	Y	Change to Access Limited	---
B-3.3	a	E6	Branch On-Prem →	A+	---	N	Access Successful	---
	b	E6		A-	---	N	Access Not Successful	---

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	c	E6	On-Prem	A	A+	N	Change to Access Limited	Access Not Successful
	d	E6		A	A-	N	Keep Access	Access Not Successful
	e	E6		---	A+	N	---	Access Successful
	f	E6		---	A-	N	---	Access Not Successful
	g	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	E6		A-	A	N	Access Not Successful	Keep Access
	i	E7		A+	---	Y	Access Successful	---
	j	E7		A	A-	Y	Keep Access	Access Not Successful
	k	E7		---	A-	Y	---	Access Not Successful
	l	E7		RA+	---	Y	Access Successful	---
	m	E7		---	RA-	Y	---	Access Not Successful
	n	E7		---	A	Y	---	Change to Access Limited
	o	E7		A	---	Y	Change to Access Limited	---
B-3.4	a	E6	Remote On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	E6		A-	---	N	Access Not Successful	---
	c	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	E6		A	A-	N	Keep Access	Access Not Successful
	e	E6		---	A+	N	---	Access Successful

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	f	E6		---	A-	N	---	Access Not Successful
	g	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	E6		A-	A	N	Access Not Successful	Keep Access
	i	E7		A+	---	Y	Access Successful	---
	j	E7		A	A-	Y	Keep Access	Access Not Successful
	k	E7		---	A-	Y	---	Access Not Successful
	l	E7		RA+	---	Y	Access Successful	---
	m	E7		---	RA-	Y	---	Access Not Successful
	n	E7		---	A	Y	---	Change to Access Limited
	o	E7		A	---	Y	Change to Access Limited	---
B-3.5	a	E6	On-Prem Remote → On-Prem	A+	---	N	Access Successful	---
	b	E6		A-	---	N	Access Not Successful	---
	c	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	E6		A	A-	N	Keep Access	Access Not Successful
	e	E6		---	A+	N	---	Access Successful
	f	E6		---	A-	N	---	Access Not Successful
	g	E6		A+	A	N	Access Not Successful	Change to Access Limited

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	h	E6		A-	A	N	Access Not Successful	Keep Access
	i	E7		A+	---	Y	Access Successful	---
	j	E7		A	A-	Y	Keep Access	Access Not Successful
	k	E7		---	A-	Y	---	Access Not Successful
	l	E7		RA+	---	Y	Access Successful	---
	m	E7		---	RA-	Y	---	Access Not Successful
	n	E7		---	A	Y	---	Change to Access Limited
	o	E7		A	---	Y	Change to Access Limited	---

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

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

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

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

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

658 **Table 2-12 Scenario B-4 Demonstrations**

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
B-4.1	a	E1	On-Prem → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	E1		A-	A	---	---	Y	---	Access Not Successful
	d	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	E2		A-	A	---	---	Y	---	Access Not Successful
	g	E3		A-	A	---	---	Y	---	Access Not Successful
	h	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-4.2	a	E1	Branch → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	E1		A-	A	---	---	Y	---	Access Not Successful
	d	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	E2		A-	A	---	---	Y	---	Access Not Successful
	g	E3		A-	A	---	---	Y	---	Access Not Successful
	h	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	E1		RA-	A	---	---	Y	---	Access Not Successful

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
	j	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-4.3	a	E1	Remote → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	E1		A-	A	---	---	Y	---	Access Not Successful
	d	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	E2		A-	A	---	---	Y	---	Access Not Successful
	g	E3		A-	A	---	---	Y	---	Access Not Successful
	h	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-4.4	a	E1	On-Prem → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	E1		A-	A	---	---	Y	---	Access Not Successful
	d	E2		A+	A	A	RSS1	Y	Y	Access Not Successful

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

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

2.5.5 Scenario B-5: Full/limited internet access based on ID attributes

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		UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
				User	EP		EP	Out of Hours	
B-5.1	a	E4	On-Prem → Internet	A+	A	URL1	Y	N	Access Successful
	b	E4		A+	A	URL2	Y	N	Access Successful
	c	E4		A+	A	URL1	Y	Y	Access Successful
	d	E4		A+	A	URL1	Y	Y	Access Successful
	e	E4		A-	A	---	Y	---	Access Not Successful
	f	E5		A+	A	URL1	Y	N	Access Not Successful
	g	E5		A+	A	URL2	Y	N	Access Successful
	h	E5		A+	A	URL1	Y	Y	Access Not Successful
	i	E5		A+	A	URL1	Y	Y	Access Not Successful
	j	E5		A-	A	---	Y	---	Access Not Successful
	k	E4		RA+	A	URL1	Y	---	Access Successful
	l	E4		RA-	A	---	Y	---	Access Not Successful
	m	E4		A+	A	URL1	N	---	Access Not Successful
	n	E4		A+	A	URL2	N	---	Access Successful
	o	E5		A+	A	URL1	N	N	Access Not Successful
	p	E5		A+	A	URL2	N	N	Access Not Successful
B-5.2	a	E4	Branch → Internet	A+	A	URL1	Y	N	Access Successful
	b	E4		A+	A	URL2	Y	N	Access Successful
	c	E4		A+	A	URL1	Y	Y	Access Successful
	d	E4		A+	A	URL1	Y	Y	Access Successful
	e	E4		A-	A	---	Y	---	Access Not Successful
	f	E5		A+	A	URL1	Y	N	Access Not Successful
	g	E5		A+	A	URL2	Y	N	Access Successful
	h	E5		A+	A	URL1	Y	Y	Access Not Successful

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

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

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

Table 2-14 Scenario B-6 Demonstrations

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

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	j			A	A-	Y	Keep Access	Access Not Successful
	k			---	A-	Y	---	Access Not Successful
	l	E6		RA+	---	Y	Access Successful	---
	m	E6		---	RA-	Y	---	Access Not Successful
	n	E6		---	A	Y	---	All Sessions Terminated
	o	E6		A	---	Y	All Sessions Terminated	---
B-6.2	a	E6	On-Prem Branch → On-Prem	A+	---	N	Access Successful	---
	b	E6		A-	---	N	Access Not Successful	---
	c	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	E6		A	A-	N	Keep Access	Access Not Successful
	e	E6		---	A+	N	---	Access Successful
	f	E6		---	A-	N	---	Access Not Successful
	g	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	E6		A-	A	N	Access Not Successful	Keep Access
	i	E7		A+	---	Y	Access Successful	---
	j	E7		A	A-	Y	Keep Access	Access Not Successful
	k	E7		---	A-	Y	---	Access Not Successful
	l	E7		RA+	---	Y	Access Successful	---

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	m	E7		---	RA-	Y	---	Access Not Successful
	n	E7		---	A	Y	---	Change to Access Limited
	o	E7		A	---	Y	Change to Access Limited	---
B-6.3	a	E6	Branch On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	E6		A-	---	N	Access Not Successful	---
	c	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	E6		A	A-	N	Keep Access	Access Not Successful
	e	E6		---	A+	N	---	Access Successful
	f	E6		---	A-	N	---	Access Not Successful
	g	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	E6		A-	A	N	Access Not Successful	Keep Access
	i	E7		A+	---	Y	Access Successful	---
	j	E7		A	A-	Y	Keep Access	Access Not Successful
	k	E7		---	A-	Y	---	Access Not Successful
	l	E7		RA+	---	Y	Access Successful	---
	m	E7		---	RA-	Y	---	Access Not Successful
	n	E7		---	A	Y	---	Change to Access Limited

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	o	E7		A	---	Y	Change to Access Limited	---
B-6.4	a	E6	Remote On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	E6		A-	---	N	Access Not Successful	---
	c	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	E6		A	A-	N	Keep Access	Access Not Successful
	e	E6		---	A+	N	---	Access Successful
	f	E6		---	A-	N	---	Access Not Successful
	g	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	E6		A-	A	N	Access Not Successful	Keep Access
	i	E7		A+	---	Y	Access Successful	---
	j	E7		A	A-	Y	Keep Access	Access Not Successful
	k	E7		---	A-	Y	---	Access Not Successful
	l	E7		RA+	---	Y	Access Successful	---
	m	E7		---	RA-	Y	---	Access Not Successful
	n	E7		---	A	Y	---	Change to Access Limited
	o	E7		A	---	Y	Change to Access Limited	---
B-6.5	a	E6	On-Prem Remote →	A+	---	N	Access Successful	---
	b	E6		A-	---	N	Access Not Successful	---

Demo ID	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
			Real Req	Hostile Req			
c	E6	On-Prem	A	A+	N	Change to Access Limited	Access Not Successful
d	E6		A	A-	N	Keep Access	Access Not Successful
e	E6		---	A+	N	---	Access Successful
f	E6		---	A-	N	---	Access Not Successful
g	E6		A+	A	N	Access Not Successful	Change to Access Limited
h	E6		A-	A	N	Access Not Successful	Keep Access
i	E7		A+	---	Y	Access Successful	---
j	E7		A	A-	Y	Keep Access	Access Not Successful
k	E7		---	A-	Y	---	Access Not Successful
l	E7		RA+	---	Y	Access Successful	---
m	E7		---	RA-	Y	---	Access Not Successful
n	E7		---	A	Y	---	Change to Access Limited
o	E7		A	---	Y	Change to Access Limited	---

2.5.7 Scenario B-7: Just-in-Time Access Privileges

In this demonstration, an enterprise provisions access privileges to a resource based on a single business process flow. Temporary privileges are granted to perform a portion of a business process, then revoked when the process is complete.

Pre-Condition: There are no active sessions from a subject to the resource. Both the subject endpoint and resource are in compliance with enterprise security posture or expected to be in compliance after the session is completed.

Demonstration: A subject is granted privileges to access a resource. The subject then establishes a session with an endpoint to perform some administrative task, then closes the connection. Privilege to access that resource is then removed.

Purpose and Outcome: The enterprise can provide just-in-time (JIT) access privileges to resources.

Table 2-15 Scenario B-7 Demonstrations

Demo ID		Subject Location	Resource Location	Priv. Provisioned	Desired Outcome
B-7.1	a	On-Prem	On-Prem	No	Access Not Successful
	b	On-Prem	On-Prem	Yes	Access Successful
	c	On-Prem	Branch	No	Access Not Successful
	d	On-Prem	Branch	Yes	Access Successful
	e	On-Prem	Remote	No	Access Not Successful
	f	On-Prem	Remote	Yes	Access Successful
	g	On-Prem	IaaS	No	Access Not Successful
	h	On-Prem	IaaS	Yes	Access Successful
	i	On-Prem	PaaS	No	Access Not Successful
	j	On-Prem	PaaS	Yes	Access Successful
	k	On-Prem	SaaS	No	Access Not Successful
	l	On-Prem	SaaS	Yes	Access Successful
	m	Branch	On-Prem	No	Access Not Successful
	n	Branch	On-Prem	Yes	Access Successful
	o	Branch	Branch	No	Access Not Successful
	p	Branch	Branch	Yes	Access Successful
	q	Branch	Remote	No	Access Not Successful
	r	Branch	Remote	Yes	Access Successful
	s	Branch	IaaS	No	Access Not Successful
	t	Branch	IaaS	Yes	Access Successful
	u	Branch	PaaS	No	Access Not Successful
	v	Branch	PaaS	Yes	Access Successful
	w	Branch	SaaS	No	Access Not Successful
	x	Branch	SaaS	Yes	Access Successful

Demo ID		Subject Location	Resource Location	Priv. Provisioned	Desired Outcome
	y	Remote	On-Prem	No	Access Not Successful
	z	Remote	On-Prem	Yes	Access Successful
	aa	Remote	Branch	No	Access Not Successful
	ab	Remote	Branch	Yes	Access Successful
	ac	Remote	Remote	No	Access Not Successful
	ad	Remote	Remote	Yes	Access Successful
	ae	Remote	IaaS	No	Access Not Successful
	af	Remote	IaaS	Yes	Access Successful
	ag	Remote	PaaS	No	Access Not Successful
	ah	Remote	PaaS	Yes	Access Successful
	ai	Remote	SaaS	No	Access Not Successful
	aj	Remote	SaaS	Yes	Access Successful

2.5.8 Scenario B-8: Enterprise-ID Step-Up Authentication

In this demonstration, the subject has an open session to the resource, but requests to perform an action that requires additional authentication checks. If successful, the subject session proceeds as normal; if failed, the session is terminated.

Pre-Condition: The subject has a current session with the resource and has successfully authenticated for the current action. The subject is authorized to perform higher security action. Both the subject endpoint and resource are in compliance with the enterprise security posture.

Demonstration: The subject has an open session to the resource and desires to perform a different action that is considered more sensitive. The system prompts the subject to re-authenticate or perform a higher level of authentication (e.g., additional factor of MFA or similar).

Purpose and Outcome: The system can request additional authentication mechanisms to match with an increased sensitive action during an active session.

Table 2-16 Scenario B-8 Demonstrations

Demo ID		Subj Type	Subject Location	Auth Success	RSS Loc	Desired Outcome
B-8.1	a	EP	On-Prem	Yes		Session Continues

Demo ID		Subj Type	Subject Location	Auth Success	RSS Loc	Desired Outcome
	b	BYOD	On-Prem	Yes	On-Prem	Session Continues
	c	Guest	On-Prem	Yes		Session Continues
	d	EP	On-Prem	No		Session Terminated
	e	BYOD	On-Prem	No		Session Terminated
	f	Guest	On-Prem	No		Session Terminated
	g	EP	Branch	Yes		Session Continues
	h	BYOD	Branch	Yes		Session Continues
	i	Guest	Branch	Yes		Session Continues
	j	EP	Branch	No		Session Terminated
	k	BYOD	Branch	No		Session Terminated
	l	Guest	Branch	No		Session Terminated
	m	EP	Remote	Yes		Session Continues
	n	BYOD	Remote	Yes		Session Continues
	o	Guest	Remote	Yes		Session Continues
	p	EP	Remote	No		Session Terminated
	q	BYOD	Remote	No		Session Terminated
	r	Guest	Remote	No		Session Terminated
B-8.2	a	EP	On-Prem	Yes	Branch	Session Continues
	b	BYOD	On-Prem	Yes		Session Continues
	c	Guest	On-Prem	Yes		Session Continues
	d	EP	On-Prem	No		Session Terminated
	e	BYOD	On-Prem	No		Session Terminated
	f	Guest	On-Prem	No		Session Terminated
	g	EP	Branch	Yes		Session Continues
	h	BYOD	Branch	Yes		Session Continues
	i	Guest	Branch	Yes		Session Continues
	j	EP	Branch	No		Session Terminated
	k	BYOD	Branch	No		Session Terminated
	l	Guest	Branch	No		Session Terminated

Demo ID		Subj Type	Subject Location	Auth Success	RSS Loc	Desired Outcome
	m	EP	Remote	Yes		Session Continues
	n	BYOD	Remote	Yes		Session Continues
	o	Guest	Remote	Yes		Session Continues
	p	EP	Remote	No		Session Terminated
	q	BYOD	Remote	No		Session Terminated
	r	Guest	Remote	No		Session Terminated
B-8.3	a	EP	On-Prem	Yes	IaaS	Session Continues
	b	BYOD	On-Prem	Yes		Session Continues
	c	Guest	On-Prem	Yes		Session Continues
	d	EP	On-Prem	No		Session Terminated
	e	BYOD	On-Prem	No		Session Terminated
	f	Guest	On-Prem	No		Session Terminated
	g	EP	Branch	Yes		Session Continues
	h	BYOD	Branch	Yes		Session Continues
	i	Guest	Branch	Yes		Session Continues
	j	EP	Branch	No		Session Terminated
	k	BYOD	Branch	No		Session Terminated
	l	Guest	Branch	No		Session Terminated
	m	EP	Remote	Yes		Session Continues
	n	BYOD	Remote	Yes		Session Continues
	o	Guest	Remote	Yes		Session Continues
	p	EP	Remote	No		Session Terminated
	q	BYOD	Remote	No		Session Terminated
	r	Guest	Remote	No		Session Terminated
B-8.4	a	EP	On-Prem	Yes	PaaS	Session Continues
	b	BYOD	On-Prem	Yes		Session Continues
	c	Guest	On-Prem	Yes		Session Continues
	d	EP	On-Prem	No		Session Terminated
	e	BYOD	On-Prem	No		Session Terminated

Demo ID		Subj Type	Subject Location	Auth Success	RSS Loc	Desired Outcome
	f	Guest	On-Prem	No		Session Terminated
	g	EP	Branch	Yes		Session Continues
	h	BYOD	Branch	Yes		Session Continues
	i	Guest	Branch	Yes		Session Continues
	j	EP	Branch	No		Session Terminated
	k	BYOD	Branch	No		Session Terminated
	l	Guest	Branch	No		Session Terminated
	m	EP	Remote	Yes		Session Continues
	n	BYOD	Remote	Yes		Session Continues
	o	Guest	Remote	Yes		Session Continues
	p	EP	Remote	No		Session Terminated
	q	BYOD	Remote	No		Session Terminated
	r	Guest	Remote	No		Session Terminated
B-8.5	a	EP	On-Prem	Yes	SaaS	Session Continues
	b	BYOD	On-Prem	Yes		Session Continues
	c	Guest	On-Prem	Yes		Session Continues
	d	EP	On-Prem	No		Session Terminated
	e	BYOD	On-Prem	No		Session Terminated
	f	Guest	On-Prem	No		Session Terminated
	g	EP	Branch	Yes		Session Continues
	h	BYOD	Branch	Yes		Session Continues
	i	Guest	Branch	Yes		Session Continues
	j	EP	Branch	No		Session Terminated
	k	BYOD	Branch	No		Session Terminated
	l	Guest	Branch	No		Session Terminated
	m	EP	Remote	Yes		Session Continues
	n	BYOD	Remote	Yes		Session Continues
	o	Guest	Remote	Yes		Session Continues
	p	EP	Remote	No		Session Terminated

Demo ID		Subj Type	Subject Location	Auth Success	RSS Loc	Desired Outcome
	q	BYOD	Remote	No		Session Terminated
	r	Guest	Remote	No		Session Terminated

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 2-17 Scenario C-1 Demonstrations

Demo ID		Req EP Compl	Req Loc	RSS EP Compl	RSS Loc	Desired Outcome
C-1.1	a	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	Branch	Y	On-Prem	Access Successful
	b	N		Y		Access Not Successful
C-1.3	A	Y	Remote	Y	On-Prem	Access Successful
	b	N		Y		Access Not Successful

Demo ID		Req EP Compl	Req Loc	RSS EP Compl	RSS Loc	Desired Outcome
C-1.4	a	Y	On-Prem	Y	Cloud	Access Successful
	b	N		Y		Access Not Successful
	c	Y		N		Access Limited
	d	N		N		Access Not Successful
C-1.5	a	Y	Branch	Y	Cloud	Access Successful
	b	N		Y		Access Not Successful
C-1.6	a	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 2-18 Scenario C-2 Demonstrations

Demo ID		Req EP Compl	Req Loc	RSS EP Compl	RSS Loc	Desired Outcome
C-2.1	a	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

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

Table 2-19 Scenario C-3 Demonstrations

Demo ID		Req EP Compl	Req Loc	RSS Access Policy	RSS Loc	Desired Outcome
C-3.1	a	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	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	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

2.6.4 Scenario C-4: No internet access using enterprised owned endpoint

This scenario deals with a request using a successfully authenticated Federated-ID accessing a non-enterprise-controlled resource in the public internet using a enterprise-owned endpoint device with internet access disabled. In this scenario, the Enterprise-ID may be allowed to access certain public internet resources but there is a separate policy for the endpoint which is not allowed any public internet access. The endpoint policy overrides the user identity policy and no requests for internet based resources are allowed.

Pre-Condition: The requestor is identified and authenticated. Per configuration, the requestor ID is authorized with limited access to the public Internet but not when coming from a particular enterprise owned endpoint that is not allowed to access the public internet.

Demonstration: The requestor using a Federated-ID will attempt to access two resources both located in the public Internet. The resources are not controlled by the enterprise. When using an endpoint that is denied all internet access, the endpoint policy overrides the identity policy and all internet access requests are denied.

Purpose and Outcome: This demonstration focuses on the endpoint access policies of non-enterprise-controlled resources on the internet by an endpoint that is not permitted internet access.

Table 2-20 Scenario C-4 Demonstrations

Demo ID		Req EP Compl	Req Loc	RSS Access Policy	RSS Loc	Desired Outcome
C-4.1	a	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	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	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

2.6.5 Scenario C-5: Internet access using BYOD

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

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

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

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

Table 2-21 Scenario C-5 Demonstrations

Demo ID		Req EP Compl	Req Loc	RSS Access Policy	RSS Loc	Desired Outcome
C-5.1	a	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	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	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.						

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.

Table 2-22 Scenario D-1 Demonstrations

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

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

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
	o	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	E2		A+	A	A	RSS2	Y	N	Access Not Successful
D-1.4	a	O1	On-Prem → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	O1		A-	A	---	---	Y	---	Access Not Successful
	d	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	E2		A-	A	---	---	Y	---	Access Not Successful
	g	E3		A-	A	---	---	Y	---	Access Not Successful
	h	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	E2		A+	A	A	RSS2	Y	N	Access Not Successful
D-1.5	a	O1	Branch → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	O1		A-	A	---	---	Y	---	Access Not Successful
	d	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	O2		A-	A	---	---	Y	---	Access Not Successful
	g	O3		A-	A	---	---	Y	---	Access Not Successful
	h	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	O1		RA-	A	---	---	Y	---	Access Not Successful

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
	j	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	O2		A+	A	A	RSS2	Y	N	Access Not Successful
D-1.6	a	O1	Remote → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	O1		A-	A	---	---	Y	---	Access Not Successful
	d	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	O2		A-	A	---	---	Y	---	Access Not Successful
	g	O3		A-	A	---	---	Y	---	Access Not Successful
	h	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	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. This is to simulate an enterprise that may have policies on public Internet access using enterprise-owned endpoints for Other-IDs.

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 2-23 Scenario D-2 Demonstrations

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

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

Demo ID		UP	Location Req. → RSS	Auth Stat		Access	Compl		Desired Outcome
				User	EP		EP	Out of Hours	
	k	O4		RA+	A	URL1	Y	---	Access Successful
	l	O4		RA-	A	---	Y	---	Access Not Successful
	m	O4		A+	A	URL1	N	---	Access Not Successful
	n	O4		A+	A	URL2	N	---	Access Successful
	o	O5		A+	A	URL1	N	N	Access Not Successful
	p	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 being reported stolen, and that request can succeed. The "Hostile Request" is performed using a stolen Enterprise-ID. All authentication methods are compromised. Re-authentication always follows a previously successful authentication.

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

Table 2-24 Scenario D-3 Demonstrations

Demo ID		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	O6	On-Prem On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	O6		A-	---	N	Access Not Successful	---
	c	O6		A	A+	N	Change to Access Limited	Access Not Successful

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	d	O6		A	A-	N	Keep Access	Access Not Successful
	e	O6		---	A+	N	---	Access Successful
	f	O6		---	A-	N	---	Access Not Successful
	g	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	O6		A-	A	N	Access Not Successful	Keep Access
	i	O7		A+	---	Y	Access Successful	---
	j	O7		A	A-	Y	Keep Access	Access Not Successful
	k	O7		---	A-	Y	---	Access Not Successful
	l	O7		RA+	---	Y	Access Successful	---
	m	O7		---	RA-	Y	---	Access Not Successful
	n	O7		---	A	Y	---	All Sessions Terminated
	o	O7		A	---	Y	All Sessions Terminated	---
D-3.2	a	O6	On-Prem Branch → On-Prem	A+	---	N	Access Successful	---
	b	O6		A-	---	N	Access Not Successful	---
	c	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	O6		A	A-	N	Keep Access	Access Not Successful
	e	O6		---	A+	N	---	Access Successful
	f	O6		---	A-	N	---	Access Not Successful

Demo ID		UP	Location	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
			Real Hostile > RSS	Real Req	Hostile Req			
	g	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	O6		A-	A	N	Access Not Successful	Keep Access
	i	O7		A+	---	Y	Access Successful	---
	j	O7		A	A-	Y	Keep Access	Access Not Successful
	k	O7		---	A-	Y	---	Access Not Successful
	l	O7		RA+	---	Y	Access Successful	---
	m	O7		---	RA-	Y	---	Access Not Successful
	n	O7		---	A	Y	---	Change to Access Limited
	o	O7		A	---	Y	Change to Access Limited	---
D-3.3	a	O6	Branch On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	O6		A-	---	N	Access Not Successful	---
	c	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	O6		A	A-	N	Keep Access	Access Not Successful
	e	O6		---	A+	N	---	Access Successful
	f	O6		---	A-	N	---	Access Not Successful
	g	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	O6		A-	A	N	Access Not Successful	Keep Access

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	i	O7		A+	---	Y	Access Successful	---
	j	O7		A	A-	Y	Keep Access	Access Not Successful
	k	O7		---	A-	Y	---	Access Not Successful
	l	O7		RA+	---	Y	Access Successful	---
	m	O7		---	RA-	Y	---	Access Not Successful
	n	O7		---	A	Y	---	Change to Access Limited
	o	O7		A	---	Y	Change to Access Limited	---
D-3.4	a	O6	Remote On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	O6		A-	---	N	Access Not Successful	---
	c	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	O6		A	A-	N	Keep Access	Access Not Successful
	e	O6		---	A+	N	---	Access Successful
	f	O6		---	A-	N	---	Access Not Successful
	g	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	O6		A-	A	N	Access Not Successful	Keep Access
	i	O7		A+	---	Y	Access Successful	---
	j	O7		A	A-	Y	Keep Access	Access Not Successful
	k	O7		---	A-	Y	---	Access Not Successful

Demo ID		UP	Location	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
			Real Hostile > RSS	Real Req	Hostile Req			
	l	O7		RA+	---	Y	Access Successful	---
	m	O7		---	RA-	Y	---	Access Not Successful
	n	O7		---	A	Y	---	Change to Access Limited
	o	O7		A	---	Y	Change to Access Limited	---
D-3.5	a	O6	On-Prem Remote → On-Prem	A+	---	N	Access Successful	---
	b	O6		A-	---	N	Access Not Successful	---
	c	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	O6		A	A-	N	Keep Access	Access Not Successful
	e	O6		---	A+	N	---	Access Successful
	f	O6		---	A-	N	---	Access Not Successful
	g	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	O6		A-	A	N	Access Not Successful	Keep Access
	i	O7		A+	---	Y	Access Successful	---
	j	O7		A	A-	Y	Keep Access	Access Not Successful
	k	O7		---	A-	Y	---	Access Not Successful
	l	O7		RA+	---	Y	Access Successful	---
	m	O7		---	RA-	Y	---	Access Not Successful
	n	O7		---	A	Y	---	Change to Access Limited

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	o	O7		A	---	Y	Change to Access Limited	---

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

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

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

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

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

Table 2-25 Scenario D-4 Demonstrations

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
D-4.1	a	O1	On-Prem → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	O1		A-	A	---	---	Y	---	Access Not Successful
	d	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	E2		A-	A	---	---	Y	---	Access Not Successful
	g	E3		A-	A	---	---	Y	---	Access Not Successful
	h	O1		RA+	A	A	RSS1	Y	Y	Access Successful

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
	i	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	E2		A+	A	A	RSS2	Y	N	Access Not Successful
D-4.2	a	O1	Branch → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	O1		A-	A	---	---	Y	---	Access Not Successful
	d	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	O2		A-	A	---	---	Y	---	Access Not Successful
	g	E3		A-	A	---	---	Y	---	Access Not Successful
	h	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	O2		A+	A	A	RSS2	Y	N	Access Not Successful
D-4.3	a	O1	Remote →	A+	A	A	RSS1	Y	Y	Access Successful
	b	O1		A+	A	A	RSS2	Y	Y	Access Successful

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
	c	O1	On-Prem	A-	A	---	---	Y	---	Access Not Successful
	d	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	O2		A-	A	---	---	Y	---	Access Not Successful
	g	E3		A-	A	---	---	Y	---	Access Not Successful
	h	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	O2		A+	A	A	RSS2	Y	N	Access Not Successful
D-4.4	a	O1	On-Prem → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	O1		A-	A	---	---	Y	---	Access Not Successful
	d	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	O2		A-	A	---	---	Y	---	Access Not Successful
	g	O3		A-	A	---	---	Y	---	Access Not Successful
	h	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	O1		RA+	A	A	RSS2	N	Y	Access Limited

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
	l	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	O2		A+	A	A	RSS2	Y	N	Access Not Successful
D-4.5	a	O1	Branch → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	O1		A-	A	---	---	Y	---	Access Not Successful
	d	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	O2		A-	A	---	---	Y	---	Access Not Successful
	g	O2		A-	A	---	---	Y	---	Access Not Successful
	h	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	O2		A+	A	A	RSS2	Y	N	Access Not Successful
D-4.6	a	O1	Remote → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	O1		A-	A	---	---	Y	---	Access Not Successful
	d	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	O2		A-	A	---	---	Y	---	Access Not Successful

Demo ID		UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
				User	EP	RSS		EP	RSS	
	g	O3		A-	A	---	---	Y	---	Access Not Successful
	h	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	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.

852 **Table 2-26 Scenario D-5 Demonstrations**

Demo ID		UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
				User	EP		EP	Out of Hours	
D-5.1	a	O4	On-Prem → Internet	A+	A	URL1	Y	N	Access Successful
	b	O4		A+	A	URL2	Y	N	Access Successful
	c	O4		A+	A	URL1	Y	Y	Access Successful
	d	O4		A+	A	URL1	Y	Y	Access Successful
	e	O4		A-	A	---	Y	---	Access Not Successful
	f	O5		A+	A	URL1	Y	N	Access Not Successful
	g	O5		A+	A	URL2	Y	N	Access Successful
	h	O5		A+	A	URL1	Y	Y	Access Not Successful
	i	O5		A+	A	URL1	Y	Y	Access Not Successful
	j	O5		A-	A	---	Y	---	Access Not Successful
	k	O4		RA+	A	URL1	Y	---	Access Successful
	l	O4		RA-	A	---	Y	---	Access Not Successful
	m	O4		A+	A	URL1	N	---	Access Not Successful
	n	O4		A+	A	URL2	N	---	Access Successful
	o	O5		A+	A	URL1	N	N	Access Not Successful
	p	O5		A+	A	URL2	N	N	Access Not Successful
D-5.2	a	O4	Branch → Internet	A+	A	URL1	Y	N	Access Successful
	b	O4		A+	A	URL2	Y	N	Access Successful
	c	O4		A+	A	URL1	Y	Y	Access Successful
	d	O4		A+	A	URL1	Y	Y	Access Successful
	e	O4		A-	A	---	Y	---	Access Not Successful
	f	O5		A+	A	URL1	Y	N	Access Not Successful
	g	O5		A+	A	URL2	Y	N	Access Successful
	h	O5		A+	A	URL1	Y	Y	Access Not Successful
	i	O5		A+	A	URL1	Y	Y	Access Not Successful
	j	O5		A-	A	---	Y	---	Access Not Successful

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

Demonstration: One request is performed and is successful, in parallel using the same user identity from two separate devices to one resource. One of the requestors is an attacker using a stolen enterprise-ID who will attempt to access an Enterprise Resource using a BYOD endpoint.

The "Real Req" always uses the latest credentials which are modified/replaced after being reported stolen. Re-authentication always follows a previously successful authentication. The "Hostile Request" is performed using a stolen enterprise-ID. All authentication methods are compromised in that the attacker can successfully respond to challenges. Hostile request re-authentication always follows a previously successful authentication.

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

Table 2-27 Scenario D-6 Demonstrations

Demo ID		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	O6	On-Prem On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	O6		A-	---	N	Access Not Successful	---
	c	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	O6		A	A-	N	Keep Access	Access Not Successful
	e	O6		---	A+	N	---	Access Successful
	f	O6		---	A-	N	---	Access Not Successful
	g	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	O6		A-	A	N	Access Not Successful	Keep Access

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	i	O7		A+	---	Y	Access Successful	---
	j	O7		A	A-	Y	Keep Access	Access Not Successful
	k	O7		---	A-	Y	---	Access Not Successful
	l	O7		RA+	---	Y	Access Successful	---
	m	O7		---	RA-	Y	---	Access Not Successful
	n	O7		---	A	Y	---	All Sessions Terminated
	o	O7		A	---	Y	All Sessions Terminated	---
D-6.2	a	O6	On-Prem Branch → On-Prem	A+	---	N	Access Successful	---
	b	O6		A-	---	N	Access Not Successful	---
	c	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	O6		A	A-	N	Keep Access	Access Not Successful
	e	O6		---	A+	N	---	Access Successful
	f	O6		---	A-	N	---	Access Not Successful
	g	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	O6		A-	A	N	Access Not Successful	Keep Access
	i	O7		A+	---	Y	Access Successful	---
	j	O7		A	A-	Y	Keep Access	Access Not Successful

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	k	O7		---	A-	Y	---	Access Not Successful
	l	O7		RA+	---	Y	Access Successful	---
	m	O7		---	RA-	Y	---	Access Not Successful
	n	O7		---	A	Y	---	Change to Access Limited
	o	O7		A	---	Y	Change to Access Limited	---
D-6.3	a	O6	Branch On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	O6		A-	---	N	Access Not Successful	---
	c	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	O6		A	A-	N	Keep Access	Access Not Successful
	e	O6		---	A+	N	---	Access Successful
	f	O6		---	A-	N	---	Access Not Successful
	g	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	O6		A-	A	N	Access Not Successful	Keep Access
	i	O7		A+	---	Y	Access Successful	---
	j	O7		A	A-	Y	Keep Access	Access Not Successful
	k	O7		---	A-	Y	---	Access Not Successful
	l	O7		RA+	---	Y	Access Successful	---
	m	O7		---	RA-	Y	---	Access Not Successful

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	n	O7		---	A	Y	---	Change to Access Limited
	o	O7		A	---	Y	Change to Access Limited	---
D-6.4	a	O6	Remote On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	O6		A-	---	N	Access Not Successful	---
	c	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	O6		A	A-	N	Keep Access	Access Not Successful
	e	O6		---	A+	N	---	Access Successful
	f	O6		---	A-	N	---	Access Not Successful
	g	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	O6		A-	A	N	Access Not Successful	Keep Access
	i	O7		A+	---	Y	Access Successful	---
	j	O7		A	A-	Y	Keep Access	Access Not Successful
	k	O7		---	A-	Y	---	Access Not Successful
	l	O7		RA+	---	Y	Access Successful	---
	m	O7		---	RA-	Y	---	Access Not Successful
	n	O7		---	A	Y	---	Change to Access Limited
	o	O7		A	---	Y	Change to Access Limited	---
D-6.5	a	O6	On-Prem	A+	---	N	Access Successful	---

Demo ID		UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
	b	O6	Remote → On-Prem	A-	---	N	Access Not Successful	---
	c	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	O6		A	A-	N	Keep Access	Access Not Successful
	e	O6		---	A+	N	---	Access Successful
	f	O6		---	A-	N	---	Access Not Successful
	g	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	O6		A-	A	N	Access Not Successful	Keep Access
	i	O7		A+	---	Y	Access Successful	---
	j	O7		A	A-	Y	Keep Access	Access Not Successful
	k	O7		---	A-	Y	---	Access Not Successful
	l	O7		RA+	---	Y	Access Successful	---
	m	O7		---	RA-	Y	---	Access Not Successful
	n	O7		---	A	Y	---	Change to Access Limited
	o	O7		A	---	Y	Change to Access Limited	---

869 2.7.7 Scenario D-7: Just-in-Time Access Privileges

In this demonstration, an enterprise provisions access privileges to a resource based on a single business process flow. Temporary privileges are granted to perform a portion of a business process, then revoked when the process is complete.

Pre-Condition: There is no active sessions from a subject to the resource. Both the subject endpoint and resource are in compliance with enterprise security posture or expected to be in compliance after the session is completed.

Demonstration: A subject is granted privileges to access a resource. The subject then establishes a session with an endpoint to perform some administrative task, then closes the connection. Privilege to access that resource is then removed.

Purpose and Outcome: The enterprise can provide JIT access privileges to resources.

Table 2-28 Scenario D-7 Demonstrations

Demo ID		Subject Location	Resource Location	Priv. Provisioned	Desired Outcome
D-7.1	a	On-Prem	On-Prem	No	Access Not Successful
	b	On-Prem	On-Prem	Yes	Access Successful
	c	On-Prem	Branch	No	Access Not Successful
	d	On-Prem	Branch	Yes	Access Successful
	e	On-Prem	Remote	No	Access Not Successful
	f	On-Prem	Remote	Yes	Access Successful
	g	On-Prem	IaaS	No	Access Not Successful
	h	On-Prem	IaaS	Yes	Access Successful
	i	On-Prem	PaaS	No	Access Not Successful
	j	On-Prem	PaaS	Yes	Access Successful
	k	On-Prem	SaaS	No	Access Not Successful
	l	On-Prem	SaaS	Yes	Access Successful
	m	Branch	On-Prem	No	Access Not Successful
	n	Branch	On-Prem	Yes	Access Successful
	o	Branch	Branch	No	Access Not Successful
	p	Branch	Branch	Yes	Access Successful
	q	Branch	Remote	No	Access Not Successful
	r	Branch	Remote	Yes	Access Successful
	s	Branch	IaaS	No	Access Not Successful
	t	Branch	IaaS	Yes	Access Successful
	u	Branch	PaaS	No	Access Not Successful
	v	Branch	PaaS	Yes	Access Successful

Demo ID		Subject Location	Resource Location	Priv. Provisioned	Desired Outcome
	w	Branch	SaaS	No	Access Not Successful
	x	Branch	SaaS	Yes	Access Successful
	y	Remote	On-Prem	No	Access Not Successful
	z	Remote	On-Prem	Yes	Access Successful
	aa	Remote	Branch	No	Access Not Successful
	ab	Remote	Branch	Yes	Access Successful
	ac	Remote	Remote	No	Access Not Successful
	ad	Remote	Remote	Yes	Access Successful
	ae	Remote	IaaS	No	Access Not Successful
	af	Remote	IaaS	Yes	Access Successful
	ag	Remote	PaaS	No	Access Not Successful
	ah	Remote	PaaS	Yes	Access Successful
	ai	Remote	SaaS	No	Access Not Successful
	aj	Remote	SaaS	Yes	Access Successful

2.7.8 Scenario D-8: Other-ID Step-Up Authentication

In this demonstration, the subject has an open session to the resource, but requests to perform an action that requires additional authentication checks. If successful, the subject session proceeds as normal, if failed, the session is terminated.

Pre-Condition: The subject has a current session with the resource and has successfully authenticated for the current action. The subject is authorized to perform higher security action. Both the subject endpoint and resource are in compliance with enterprise security posture.

Demonstration: The subject has an open session to the resource and desires to perform a different action that is considered more sensitive. The system prompts the subject to re-authenticate or perform a higher level of authentication (e.g., additional factor of MFA or similar).

Purpose and Outcome: The system can request additional authentication mechanisms to match with an increased sensitive action during an active session.

Table 2-29 Scenario D-8 Demonstrations

Demo ID		Subj Type	Subject Location	Auth Success	RSS Loc	Desired Outcome
D-8.1	a	EP	On-prem	Yes	On-Prem	Session Continues
	b	BYOD	On-prem	Yes		Session Continues
	c	Guest	On-Prem	Yes		Session Continues
	d	EP	On-prem	No		Session Terminated
	e	BYOD	On-prem	No		Session Terminated
	f	Guest	On-Prem	No		Session Terminated
	g	EP	Branch	Yes		Session Continues
	h	BYOD	Branch	Yes		Session Continues
	i	Guest	Branch	Yes		Session Continues
	j	EP	Branch	No		Session Terminated
	k	BYOD	Branch	No		Session Terminated
	l	Guest	Branch	No		Session Terminated
	m	EP	Remote	Yes		Session Continues
	n	BYOD	Remote	Yes		Session Continues
	o	Guest	Remote	Yes		Session Continues
	p	EP	Remote	No		Session Terminated
	q	BYOD	Remote	No		Session Terminated
	r	Guest	Remote	No		Session Terminated
D-8.2	a	EP	On-prem	Yes	Branch	Session Continues
	b	BYOD	On-prem	Yes		Session Continues
	c	Guest	On-Prem	Yes		Session Continues
	d	EP	On-prem	No		Session Terminated
	e	BYOD	On-prem	No		Session Terminated
	f	Guest	On-Prem	No		Session Terminated
	g	EP	Branch	Yes		Session Continues
	h	BYOD	Branch	Yes		Session Continues
	i	Guest	Branch	Yes		Session Continues
	j	EP	Branch	No		Session Terminated

Demo ID		Subj Type	Subject Location	Auth Success	RSS Loc	Desired Outcome
	k	BYOD	Branch	No		Session Terminated
	l	Guest	Branch	No		Session Terminated
	m	EP	Remote	Yes		Session Continues
	n	BYOD	Remote	Yes		Session Continues
	o	Guest	Remote	Yes		Session Continues
	p	EP	Remote	No		Session Terminated
	q	BYOD	Remote	No		Session Terminated
	r	Guest	Remote	No		Session Terminated
D-8.3	a	EP	On-prem	Yes	IaaS	Session Continues
	b	BYOD	On-prem	Yes		Session Continues
	c	Guest	On-Prem	Yes		Session Continues
	d	EP	On-prem	No		Session Terminated
	e	BYOD	On-prem	No		Session Terminated
	f	Guest	On-Prem	No		Session Terminated
	g	EP	Branch	Yes		Session Continues
	h	BYOD	Branch	Yes		Session Continues
	i	Guest	Branch	Yes		Session Continues
	j	EP	Branch	No		Session Terminated
	k	BYOD	Branch	No		Session Terminated
	l	Guest	Branch	No		Session Terminated
	m	EP	Remote	Yes		Session Continues
	n	BYOD	Remote	Yes		Session Continues
	o	Guest	Remote	Yes		Session Continues
	p	EP	Remote	No		Session Terminated
	q	BYOD	Remote	No		Session Terminated
	r	Guest	Remote	No		Session Terminated
D-8.4	a	EP	On-prem	Yes	PaaS	Session Continues
	b	BYOD	On-prem	Yes		Session Continues
	c	Guest	On-Prem	Yes		Session Continues

Demo ID		Subj Type	Subject Location	Auth Success	RSS Loc	Desired Outcome
	d	EP	On-prem	No		Session Terminated
	e	BYOD	On-prem	No		Session Terminated
	f	Guest	On-Prem	No		Session Terminated
	g	EP	Branch	Yes		Session Continues
	h	BYOD	Branch	Yes		Session Continues
	i	Guest	Branch	Yes		Session Continues
	j	EP	Branch	No		Session Terminated
	k	BYOD	Branch	No		Session Terminated
	l	Guest	Branch	No		Session Terminated
	m	EP	Remote	Yes		Session Continues
	n	BYOD	Remote	Yes		Session Continues
	o	Guest	Remote	Yes		Session Continues
	p	EP	Remote	No		Session Terminated
	q	BYOD	Remote	No		Session Terminated
	r	Guest	Remote	No		Session Terminated
D-8.5	a	EP	On-prem	Yes	SaaS	Session Continues
	b	BYOD	On-prem	Yes		Session Continues
	c	Guest	On-Prem	Yes		Session Continues
	d	EP	On-prem	No		Session Terminated
	e	BYOD	On-prem	No		Session Terminated
	f	Guest	On-Prem	No		Session Terminated
	g	EP	Branch	Yes		Session Continues
	h	BYOD	Branch	Yes		Session Continues
	i	Guest	Branch	Yes		Session Continues
	j	EP	Branch	No		Session Terminated
	k	BYOD	Branch	No		Session Terminated
	l	Guest	Branch	No		Session Terminated
	m	EP	Remote	Yes		Session Continues
	n	BYOD	Remote	Yes		Session Continues

Demo ID		Subj Type	Subject Location	Auth Success	RSS Loc	Desired Outcome
	o	Guest	Remote	Yes		Session Continues
	p	EP	Remote	No		Session Terminated
	q	BYOD	Remote	No		Session Terminated
	r	Guest	Remote	No		Session Terminated

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 observable compliance state or sent traffic 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 2-30 Scenario E-1 Demonstrations

Demo ID		Location of Subject	Access	Desired Outcome
E-1.1	a	On-Prem	Public resource	Access Successful
	b		Public internet	Access Successful
E-1.2	a	Branch	Public resource	Access Successful
	b		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, reducing the confidence level to a point where the enterprise policy states that the active session should be terminated. 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 2-31 Scenario F-1 Demonstrations

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

Demo ID		Re-auth	Req Loc	RSS Loc	Desired Outcome
F-1.6	a	Passes	Remote	Cloud	Session stays active
	b	Fails			Session will be terminated

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

This scenario is based on a successful request with an established session to an enterprise resource using an enterprise-owned endpoint. The reauthentication of the requesting endpoint will fail, reducing the confidence level. The given enterprise has a policy that would trigger termination of an active session. 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 2-32 Scenario F-2 Demonstrations

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

Demo ID		Re-auth	Req. Loc	RSS Loc	Desired Outcome
F-2.5	a	Passes	Branch	Cloud	Session stays active
	b	Fails			Session will be terminated
F-2.6	a	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, reducing the confidence level. The level is now below the acceptable level for the resource according to enterprise policy. 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 2-33 Scenario F-3 Demonstrations

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

Demo ID		Re-auth	Req. Loc	RSS Loc	Desired Outcome
	b	Fails			Session will be terminated
F-3.5	a	Passes	Branch	Cloud	Session stays active
	b	Fails			Session will be terminated
F-3.6	a	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, reducing the confidence level. The enterprise has a policy that indicates that the endpoint can no longer be used to access the given resource. 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 2-34 Scenario F-4 Demonstrations

Demo ID		Req EP Compl	Req Loc	RSS Loc	Desired Outcome
F-4.1	a	Y	On-Prem	On-Prem	Session stays active
	b	N			Session will be terminated
F-4.2	a	Y	Branch	On-Prem	Session stays active
	b	N			Session will be terminated

Demo ID		Req EP Compl	Req Loc	RSS Loc	Desired Outcome
F-4.3	a	Y	Remote	On-Prem	Session stays active
	b	N			Session will be terminated
F-4.4	a	Y	On-Prem	Cloud	Session stays active
	b	N			Session will be terminated
F-4.5	a	Y	Branch	Cloud	Session stays active
	b	N			Session will be terminated
F-4.6	a	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 establish a session to an enterprise resource.

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

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

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

Table 2-35 Scenario F-5 Demonstrations

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

Demo ID		Req EP Compl	Req Loc	RSS Loc	Desired Outcome
F-5.2	a	N	Branch	On-Prem	Access Not Successful
	b	Y			Access Successful
F-5.3	a	N	Remote	On-Prem	Access Not Successful
	b	Y			Access Successful
F-5.4	a	N	On-Prem	Cloud	Access Not Successful
	b	Y			Access Successful
F-5.5	a	N	Branch	Cloud	Access Not Successful
	b	Y			Access Successful
F-5.6	a	N	Remote	Cloud	Access Not Successful
	b	Y			Access Successful

2.9.6 Scenario F-6: Enterprise-ID Violating Data Use Policy

This scenario demonstrates the enterprise's ability to detect and respond to a violation of the enterprise data use policy. In this scenario, an enterprise-ID attempts to transfer a large amount of data from the resource, triggering a data use policy violation. Example: The ID is only allowed to access 1 file/day but attempts to access 2 files/day (note that the time interval here is arbitrary and can be set to whatever makes operation easiest). The enterprise then closes the session between the subject and the resource and may take additional action based on the build (quarantine, log out, etc.). In this scenario, the subject is playing the role of an insider threat and is intentionally trying to perform actions that violate the enterprise data use policy.

Pre-Condition: Valid Enterprise-ID has successfully authenticated to resource and authorized to use resource within data use policy. Endpoint used is compliant with the enterprise security policy (either enterprise-owned or BYOD).

Demonstration: A valid Enterprise-ID attempts to access more data than allowed during an authenticated/authorized session. The system detects and responds by terminating the session.

Purpose and Outcome: Demonstrating the system responding to violation of the enterprise data security policy by terminating access to the resource.

Table 2-36 Scenario F-6 Demonstrations

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
F-6.1	a	Ent-Owned	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	Ent-Owned	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	Ent-Owned	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	Ent-Owned	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	Ent-Owned	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	Ent-Owned	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	Ent-Owned	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	Ent-Owned	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	Ent-Owned	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	Ent-Owned	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	Ent-Owned	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	Ent-Owned	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
F-6.2	a	BYOD	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	BYOD	Branch	On-prem	Access stopped (no longer able to connect to resource).

Demo ID	Subj Type	Subject Location	RSS Location	Desired Outcome
c	BYOD	Remote	On-prem	Access stopped (no longer able to connect to resource).
d	BYOD	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
e	BYOD	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
f	BYOD	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
g	BYOD	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
h	BYOD	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
i	BYOD	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
j	BYOD	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
k	BYOD	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
l	BYOD	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).

2.9.7 Scenario F-7: Other-ID Violating Data Use Policy

This scenario demonstrates the enterprise's ability to detect and respond to a violation of the enterprise data use policy. In this scenario, an other-ID attempts to transfer a large amount of data from the resource, triggering a data use policy violation. Example: The ID is only allowed to access one file/day but attempts to access two files/day. The enterprise then closes the session between the subject and the resource and may take additional action based on the build (quarantine, log out, etc.). In this scenario, the subject is playing the role of an insider threat and is intentionally trying to perform actions that violate the enterprise data use policy.

Pre-Condition: Valid Other-ID has successfully authenticated to resource and authorized to use resource within data use policy. Endpoint used is compliant with the enterprise security policy (either enterprise-owned or BYOD).

Demonstration: The enterprise can detect and respond when an Other-ID attempts to violate data use policy.

Purpose and Outcome: The enterprise can enforce data use policies on Other-IDs and can terminate access when a violation is detected.

Table 2-37 Scenario F-7 Demonstrations

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
F-7.1	a	Ent-Owned	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	Ent-Owned	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	Ent-Owned	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	Ent-Owned	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	Ent-Owned	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	Ent-Owned	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	Ent-Owned	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	Ent-Owned	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	Ent-Owned	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	Ent-Owned	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	Ent-Owned	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	Ent-Owned	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
F-7.2	a	BYOD	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	BYOD	Branch	On-prem	Access stopped (no longer able to connect to resource).

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	c	BYOD	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	BYOD	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	BYOD	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	BYOD	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	BYOD	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	BYOD	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	BYOD	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	BYOD	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	BYOD	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	BYOD	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).

2.9.8 Scenario F-8: Enterprise-ID Violating Internet Use Policy

This scenario demonstrates the enterprise’s ability to detect and respond to a violation of the enterprise Internet use policy. In this scenario, an enterprise-ID has an open session for a resource, but the endpoint sends an HTTP GET to a known bad URL, triggering policy violation. The enterprise then closes the session between the subject and the resource and may take additional action based on the build (quarantine, log out, etc.). In this scenario, the subject could be playing the role of an insider threat or the endpoint has been compromised, resulting in observed queries that appear to violate the enterprise Internet use policy.

Pre-Condition: Valid Enterprise-ID has successfully authenticated to resource and authorized to use resource. The endpoint used by the subject is compliant to the enterprise security policy (either enterprise-owned, BYOD or Guest). The enterprise can monitor outbound queries.

Demonstration: A valid Enterprise-ID has an open session and then attempts to open a session to a known bad URL. The system detects and responds by terminating the open session.

Purpose and Outcome: The enterprise can detect and respond when Enterprise-ID is using a potentially subverted endpoint and/or detects a violation of Internet use policies.

Table 2-38 Scenario F-8 Demonstrations

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
F-8.1	a	Ent-Owned	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	Ent-Owned	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	Ent-Owned	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	Ent-Owned	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	Ent-Owned	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	Ent-Owned	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	Ent-Owned	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	Ent-Owned	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	Ent-Owned	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	Ent-Owned	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	Ent-Owned	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	Ent-Owned	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
F-8.2	a	BYOD	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	BYOD	Branch	On-prem	Access stopped (no longer able to connect to resource).

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	c	BYOD	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	BYOD	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	BYOD	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	BYOD	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	BYOD	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	BYOD	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	BYOD	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	BYOD	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	BYOD	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	BYOD	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
F-8.3	a	Guest	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	B	Guest	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	Guest	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	Guest	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	Guest	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	Guest	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	Guest	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	h	Guest	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	Guest	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	Guest	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	Guest	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	Guest	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).

2.9.9 Scenario F-9: Other-ID Violating Internet Use Policy

This scenario demonstrates the enterprise's ability to detect and respond to a violation of the enterprise Internet use policy. In this scenario, an other-ID has an open session for a resource, but the endpoint sends an HTTP GET to a known bad URL, triggering policy violation. The enterprise then closes the session between the subject and the resource and may take additional action based on the build (quarantine, log out, etc.). In this scenario, the subject could be playing the role of an insider threat or the endpoint has been compromised, resulting in observed queries that appear to violate the enterprise Internet use policy.

Pre-Condition: Valid other-ID has successfully authenticated to resource and authorized to use resource. The endpoint used by the subject is compliant to the enterprise security policy (either enterprise-owned, BYOD or Guest). The enterprise can monitor outbound queries.

Demonstration: A valid other-ID is has an open session and then attempts to open a session to a known bad URL. The system detects and responds by terminating the open session.

Purpose and Outcome: The enterprise can detect and respond when other-ID is using a potentially subverted endpoint and/or detects a violation of Internet use policies.

Table 2-39 Scenario F-9 Demonstrations

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
F-9.1	a	Ent-Owned	On-prem	On-prem	Access stopped (no longer able to connect to resource).

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	b	Ent-Owned	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	Ent-Owned	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	Ent-Owned	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	Ent-Owned	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	Ent-Owned	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	Ent-Owned	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	Ent-Owned	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	Ent-Owned	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	Ent-Owned	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	Ent-Owned	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	Ent-Owned	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
F-8.2	a	BYOD	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	BYOD	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	BYOD	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	BYOD	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	BYOD	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	BYOD	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	g	BYOD	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	BYOD	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	BYOD	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	BYOD	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	BYOD	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	BYOD	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
F-9.3	a	Guest	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	Guest	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	Guest	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	Guest	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	Guest	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	Guest	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	Guest	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	Guest	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	Guest	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	Guest	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	Guest	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	l	Guest	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).

2.9.10 Scenario F-10: Enterprise-ID Attempting Unauthorized Access Detection and Response, Access Queries

This scenario demonstrates the enterprise's ability to detect and respond to violations of the enterprise authorization policy. In this scenario, an enterprise-ID attempts to access an unauthorized resource (and is prevented). Access privileges to previously authorized resources are then revoked and the Enterprise-ID is prevented from accessing previously authorized resources. The enterprise may take additional action based on the build (quarantine, log out, etc.). The subject is playing the role of an insider threat and is intentionally trying to access unauthorized resources.

Pre-Condition: The endpoint used by the subject is compliant to the enterprise security policy (either enterprise-owned, BYOD or Guest). The Enterprise-ID makes an unauthorized request that is flagged.

Demonstration: The enterprise can detect and respond when a possibly subverted or insider threat enterprise-ID is attempts to access unauthorized resources.

Purpose and Outcome: Previously authorized access privileges being revoked and follow-up access requests for authorized resources is denied.

Table 2-40 Scenario F-10 Demonstrations

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
F-10.1	a	Ent-Owned	On-prem	On-prem	On-prem	Access not successful.
	b	Ent-Owned	On-prem	Cloud (IaaS)	On-prem	Access not successful.
	c	Ent-Owned	On-prem	Cloud (PaaS)	On-prem	Access not successful.
	d	Ent-Owned	On-prem	Cloud (SaaS)	On-prem	Access not successful.
	e	Ent-Owned	Branch	On-prem	On-prem	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	f	Ent-Owned	Branch	Cloud (IaaS)	On-prem	Access not successful.
	g	Ent-Owned	Branch	Cloud (PaaS)	On-prem	Access not successful.
	h	Ent-Owned	Branch	Cloud (SaaS)	On-prem	Access not successful.
	i	Ent-Owned	Remote	On-prem	On-prem	Access not successful.
	j	Ent-Owned	Remote	Cloud (IaaS)	On-prem	Access not successful.
	k	Ent-Owned	Remote	Cloud (PaaS)	On-prem	Access not successful.
	l	Ent-Owned	Remote	Cloud (SaaS)	On-prem	Access not successful.
	m	Ent-Owned	On-prem	On-prem	Cloud (IaaS)	Access not successful.
	n	Ent-owned	On-prem	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	o	Ent-owned	On-prem	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	p	End-owned	On-prem	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	q	Ent-Owned	Branch	On-prem	Cloud (IaaS)	Access not successful.
	r	Ent-owned	Branch	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	s	Ent-owned	Branch	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	t	End-owned	Branch	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	u	Ent-Owned	Remote	On-prem	Cloud (IaaS)	Access not successful.
	v	Ent-owned	Remote	Cloud (IaaS)	Cloud (IaaS)	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	w	Ent-owned	Remote	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	x	End-owned	Remote	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	y	Ent-Owned	On-prem	On-prem	Cloud (PaaS)	Access not successful.
	z	Ent-owned	On-prem	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	aa	Ent-owned	On-prem	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	ab	End-owned	On-prem	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ac	Ent-Owned	Branch	On-prem	Cloud (PaaS)	Access not successful.
	ad	Ent-owned	Branch	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ae	Ent-owned	Branch	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	af	End-owned	Branch	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ag	Ent-Owned	Remote	On-prem	Cloud (PaaS)	Access not successful.
	ah	Ent-owned	Remote	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	Ai	Ent-owned	Remote	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	aj	End-owned	Remote	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ak	Ent-Owned	On-prem	On-prem	Cloud (SaaS)	Access not successful.
	Al	Ent-owned	On-prem	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	am	Ent-owned	On-prem	Cloud (PaaS)	Cloud (SaaS)	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	an	End-owned	On-prem	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	ao	Ent-Owned	Branch	On-prem	Cloud (SaaS)	Access not successful.
	ap	Ent-owned	Branch	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	aq	Ent-owned	Branch	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	ar	End-owned	Branch	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	as	Ent-Owned	Remote	On-prem	Cloud (SaaS)	Access not successful.
	at	Ent-owned	Remote	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	au	Ent-owned	Remote	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	av	End-owned	Remote	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
F-10.2	a	BYOD	On-prem	On-prem	On-prem	Access not successful.
	B	BYOD	On-prem	Cloud (IaaS)	On-prem	Access not successful.
	c	BYOD	On-prem	Cloud (PaaS)	On-prem	Access not successful.
	d	BYOD	On-prem	Cloud (SaaS)	On-prem	Access not successful.
	e	BYOD	Branch	On-prem	On-prem	Access not successful.
	f	BYOD	Branch	Cloud (IaaS)	On-prem	Access not successful.
	g	BYOD	Branch	Cloud (PaaS)	On-prem	Access not successful.
	h	BYOD	Branch	Cloud (SaaS)	On-prem	Access not successful.
	i	BYOD	Remote	On-prem	On-prem	Access not successful.
	j	BYOD	Remote	Cloud (IaaS)	On-prem	Access not successful.
	k	BYOD	Remote	Cloud (PaaS)	On-prem	Access not successful.
	l	BYOD	Remote	Cloud (SaaS)	On-prem	Access not successful.
	m	BYOD	On-prem	On-prem	Cloud (IaaS)	Access not successful.
	n	BYOD	On-prem	Cloud (IaaS)	Cloud (IaaS)	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	o	BYOD	On-prem	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	p	BYOD	On-prem	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	q	BYOD	Branch	On-prem	Cloud (IaaS)	Access not successful.
	r	BYOD	Branch	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	s	BYOD	Branch	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	t	BYOD	Branch	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	u	BYOD	Remote	On-prem	Cloud (IaaS)	Access not successful.
	v	BYOD	Remote	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	w	BYOD	Remote	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	x	BYOD	Remote	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	y	BYOD	On-prem	On-prem	Cloud (PaaS)	Access not successful.
	z	BYOD	On-prem	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	aa	BYOD	On-prem	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	ab	BYOD	On-prem	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ac	BYOD	Branch	On-prem	Cloud (PaaS)	Access not successful.
	ad	BYOD	Branch	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ae	BYOD	Branch	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	af	BYOD	Branch	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ag	BYOD	Remote	On-prem	Cloud (PaaS)	Access not successful.
	ah	BYOD	Remote	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ai	BYOD	Remote	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	aj	BYOD	Remote	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ak	BYOD	On-prem	On-prem	Cloud (SaaS)	Access not successful.
	al	BYOD	On-prem	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	am	BYOD	On-prem	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	an	BYOD	On-prem	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	ao	BYOD	Branch	On-prem	Cloud (SaaS)	Access not successful.
	ap	BYOD	Branch	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	aq	BYOD	Branch	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	ar	BYOD	Branch	Cloud (SaaS)	Cloud (SaaS)	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	as	BYOD	Remote	On-prem	Cloud (SaaS)	Access not successful.
	at	BYOD	Remote	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	au	BYOD	Remote	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	av	BYOD	Remote	Cloud (SaaS)	Cloud (SaaS)	Access not successful
F-10.3	a	Guest	On-prem	On-prem	On-prem	Access not successful.
	b	Guest	On-prem	Cloud (IaaS)	On-prem	Access not successful.
	c	Guest	On-prem	Cloud (PaaS)	On-prem	Access not successful.
	d	Guest	On-prem	Cloud (SaaS)	On-prem	Access not successful.
	e	Guest	Branch	On-prem	On-prem	Access not successful.
	f	Guest	Branch	Cloud (IaaS)	On-prem	Access not successful.
	g	Guest	Branch	Cloud (PaaS)	On-prem	Access not successful.
	h	Guest	Branch	Cloud (SaaS)	On-prem	Access not successful.
	i	Guest	Remote	On-prem	On-prem	Access not successful.
	j	Guest	Remote	Cloud (IaaS)	On-prem	Access not successful.
	k	Guest	Remote	Cloud (PaaS)	On-prem	Access not successful.
	l	Guest	Remote	Cloud (SaaS)	On-prem	Access not successful.
	m	Guest	On-prem	On-prem	Cloud (IaaS)	Access not successful.
	n	Guest	On-prem	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	o	Guest	On-prem	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	p	Guest	On-prem	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	q	Guest	Branch	On-prem	Cloud (IaaS)	Access not successful.
	r	Guest	Branch	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	s	Guest	Branch	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	t	Guest	Branch	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	u	Guest	Remote	On-prem	Cloud (IaaS)	Access not successful.
	v	Guest	Remote	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	w	Guest	Remote	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	x	Guest	Remote	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	y	Guest	On-prem	On-prem	Cloud (PaaS)	Access not successful.
	z	Guest	On-prem	Cloud (IaaS)	Cloud (PaaS)	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	aa	Guest	On-prem	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	ab	Guest	On-prem	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ac	Guest	Branch	On-prem	Cloud (PaaS)	Access not successful.
	ad	Guest	Branch	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ae	Guest	Branch	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	af	Guest	Branch	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ag	Guest	Remote	On-prem	Cloud (PaaS)	Access not successful.
	ah	Guest	Remote	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ai	Guest	Remote	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	aj	Guest	Remote	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ak	Guest	On-prem	On-prem	Cloud (SaaS)	Access not successful.
	al	Guest	On-prem	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	am	Guest	On-prem	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	an	Guest	On-prem	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	ao	Guest	Branch	On-prem	Cloud (SaaS)	Access not successful.
	ap	Guest	Branch	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	aq	Guest	Branch	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	ar	Guest	Branch	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	as	Guest	Remote	On-prem	Cloud (SaaS)	Access not successful.
	at	Guest	Remote	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	au	Guest	Remote	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	av	Guest	Remote	Cloud (SaaS)	Cloud (SaaS)	Access not successful.

2.9.11 Scenario F-11: Enterprise-ID Attempting Unauthorized Access Detection and Response, Ongoing Sessions

This scenario demonstrates the enterprise's ability to detect and respond to violations of the enterprise authorization policy. In this scenario, an enterprise-ID has an open session for a resource, but the endpoint sends an HTTP GET to a known bad URL, triggering policy violation. The enterprise then closes the session between the subject and the resource and may take additional action based on the build (quarantine, log out, etc.). The subject is playing the role of an insider threat and is intentionally trying to access unauthorized resources.

Pre-Condition: Valid enterprise-ID has successfully authenticated to resource and authorized to use resource. The endpoint used by the subject is compliant to the enterprise security policy (either enterprise-owned, BYOD or Guest). The Enterprise-ID makes an authorized request that is flagged that results in current sessions being terminated.

Demonstration: The enterprise can detect and respond when a possibly subverted or insider threat enterprise-ID attempts to access unauthorized resources.

Purpose and Outcome: Previously authorized access privileges being revoked and follow-up access requests for authorized resources is denied.

Table 2-41 Scenario F-11 Demonstrations

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
F-11.1	a	Ent-Owned	On-prem	On-prem	On-prem	Active session terminated.
	b	Ent-Owned	On-prem	Cloud (IaaS)	On-prem	Active session terminated.
	c	Ent-Owned	On-prem	Cloud (PaaS)	On-prem	Active session terminated.
	d	Ent-Owned	On-prem	Cloud (SaaS)	On-prem	Active session terminated.
	e	Ent-Owned	Branch	On-prem	On-prem	Active session terminated.
	f	Ent-Owned	Branch	Cloud (IaaS)	On-prem	Active session terminated.
	g	Ent-Owned	Branch	Cloud (PaaS)	On-prem	Active session terminated.
	h	Ent-Owned	Branch	Cloud (SaaS)	On-prem	Active session terminated.
	i	Ent-Owned	Remote	On-prem	On-prem	Active session terminated.
	j	Ent-Owned	Remote	Cloud (IaaS)	On-prem	Active session terminated.
	k	Ent-Owned	Remote	Cloud (PaaS)	On-prem	Active session terminated.
	l	Ent-Owned	Remote	Cloud (SaaS)	On-prem	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	m	Ent-Owned	On-prem	On-prem	Cloud (IaaS)	Active session terminated.
	n	Ent-owned	On-prem	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	o	Ent-owned	On-prem	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	p	End-owned	On-prem	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	q	Ent-Owned	Branch	On-prem	Cloud (IaaS)	Active session terminated.
	r	Ent-owned	Branch	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	s	Ent-owned	Branch	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	t	End-owned	Branch	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	u	Ent-Owned	Remote	On-prem	Cloud (IaaS)	Active session terminated.
	v	Ent-owned	Remote	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	w	Ent-owned	Remote	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	x	End-owned	Remote	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	y	Ent-Owned	On-prem	On-prem	Cloud (PaaS)	Active session terminated.
	z	Ent-owned	On-prem	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	aa	Ent-owned	On-prem	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	ab	End-owned	On-prem	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ac	Ent-Owned	Branch	On-prem	Cloud (PaaS)	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	ad	Ent-owned	Branch	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	ae	Ent-owned	Branch	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	af	End-owned	Branch	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ag	Ent-Owned	Remote	On-prem	Cloud (PaaS)	Active session terminated.
	ah	Ent-owned	Remote	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	ai	Ent-owned	Remote	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	aj	End-owned	Remote	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ak	Ent-Owned	On-prem	On-prem	Cloud (SaaS)	Active session terminated.
	al	Ent-owned	On-prem	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	am	Ent-owned	On-prem	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	an	End-owned	On-prem	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	ao	Ent-Owned	Branch	On-prem	Cloud (SaaS)	Active session terminated.
	ap	Ent-owned	Branch	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	aq	Ent-owned	Branch	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	ar	End-owned	Branch	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	as	Ent-Owned	Remote	On-prem	Cloud (SaaS)	Active session terminated.
	at	Ent-owned	Remote	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	au	Ent-owned	Remote	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	av	End-owned	Remote	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
F-11.2	a	BYOD	On-prem	On-prem	On-prem	Active session terminated.
	b	BYOD	On-prem	Cloud (IaaS)	On-prem	Active session terminated.
	c	BYOD	On-prem	Cloud (PaaS)	On-prem	Active session terminated.
	d	BYOD	On-prem	Cloud (SaaS)	On-prem	Active session terminated.
	e	BYOD	Branch	On-prem	On-prem	Active session terminated.
	f	BYOD	Branch	Cloud (IaaS)	On-prem	Active session terminated.
	g	BYOD	Branch	Cloud (PaaS)	On-prem	Active session terminated.
	h	BYOD	Branch	Cloud (SaaS)	On-prem	Active session terminated.
	i	BYOD	Remote	On-prem	On-prem	Active session terminated.
	j	BYOD	Remote	Cloud (IaaS)	On-prem	Active session terminated.
	k	BYOD	Remote	Cloud (PaaS)	On-prem	Active session terminated.
	l	BYOD	Remote	Cloud (SaaS)	On-prem	Active session terminated.
	m	BYOD	On-prem	On-prem	Cloud (IaaS)	Active session terminated.
	n	BYOD	On-prem	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	o	BYOD	On-prem	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	p	BYOD	On-prem	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	q	BYOD	Branch	On-prem	Cloud (IaaS)	Active session terminated.
	r	BYOD	Branch	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	s	BYOD	Branch	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	t	BYOD	Branch	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	u	BYOD	Remote	On-prem	Cloud (IaaS)	Active session terminated.
	v	BYOD	Remote	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	w	BYOD	Remote	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	x	BYOD	Remote	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	y	BYOD	On-prem	On-prem	Cloud (PaaS)	Active session terminated.
	z	BYOD	On-prem	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	aa	BYOD	On-prem	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	ab	BYOD	On-prem	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ac	BYOD	Branch	On-prem	Cloud (PaaS)	Active session terminated.
	ad	BYOD	Branch	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	ae	BYOD	Branch	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	af	BYOD	Branch	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ag	BYOD	Remote	On-prem	Cloud (PaaS)	Active session terminated.
	ah	BYOD	Remote	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	ai	BYOD	Remote	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	aj	BYOD	Remote	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ak	BYOD	On-prem	On-prem	Cloud (SaaS)	Active session terminated.
	al	BYOD	On-prem	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	am	BYOD	On-prem	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	an	BYOD	On-prem	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	ao	BYOD	Branch	On-prem	Cloud (SaaS)	Active session terminated.
	ap	BYOD	Branch	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	aq	BYOD	Branch	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	ar	BYOD	Branch	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	as	BYOD	Remote	On-prem	Cloud (SaaS)	Active session terminated.
	at	BYOD	Remote	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	au	BYOD	Remote	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	av	BYOD	Remote	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
F-11.3	a	Guest	On-prem	On-prem	On-prem	Active session terminated.
	b	Guest	On-prem	Cloud (IaaS)	On-prem	Active session terminated.
	c	Guest	On-prem	Cloud (PaaS)	On-prem	Active session terminated.
	d	Guest	On-prem	Cloud (SaaS)	On-prem	Active session terminated.
	e	Guest	Branch	On-prem	On-prem	Active session terminated.
	f	Guest	Branch	Cloud (IaaS)	On-prem	Active session terminated.
	g	Guest	Branch	Cloud (PaaS)	On-prem	Active session terminated.
	h	Guest	Branch	Cloud (SaaS)	On-prem	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	i	Guest	Remote	On-prem	On-prem	Active session terminated.
	j	Guest	Remote	Cloud (IaaS)	On-prem	Active session terminated.
	k	Guest	Remote	Cloud (PaaS)	On-prem	Active session terminated.
	l	Guest	Remote	Cloud (SaaS)	On-prem	Active session terminated.
	m	Guest	On-prem	On-prem	Cloud (IaaS)	Active session terminated.
	n	Guest	On-prem	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	o	Guest	On-prem	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	p	Guest	On-prem	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	q	Guest	Branch	On-prem	Cloud (IaaS)	Active session terminated.
	r	Guest	Branch	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	s	Guest	Branch	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	t	Guest	Branch	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	u	Guest	Remote	On-prem	Cloud (IaaS)	Active session terminated.
	v	Guest	Remote	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	w	Guest	Remote	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	x	Guest	Remote	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	y	Guest	On-prem	On-prem	Cloud (PaaS)	Active session terminated.
	z	Guest	On-prem	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	aa	Guest	On-prem	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	ab	Guest	On-prem	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ac	Guest	Branch	On-prem	Cloud (PaaS)	Active session terminated.
	ad	Guest	Branch	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	ae	Guest	Branch	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	af	Guest	Branch	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ag	Guest	Remote	On-prem	Cloud (PaaS)	Active session terminated.
	ah	Guest	Remote	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	ai	Guest	Remote	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	aj	Guest	Remote	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ak	Guest	On-prem	On-prem	Cloud (SaaS)	Active session terminated.
	al	Guest	On-prem	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	am	Guest	On-prem	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	an	Guest	On-prem	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	ao	Guest	Branch	On-prem	Cloud (SaaS)	Active session terminated.
	ap	Guest	Branch	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	aq	Guest	Branch	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	ar	Guest	Branch	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	as	Guest	Remote	On-prem	Cloud (SaaS)	Active session terminated.
	at	Guest	Remote	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	au	Guest	Remote	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	av	Guest	Remote	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.

2.9.12 Scenario F-12: Other-ID Attempting Unauthorized Access Detection and Response, Access Queries

This scenario demonstrates the enterprise's ability to detect and respond to violations of the enterprise authorization policy. In this scenario, an Other-ID attempts to access an unauthorized resource (and is prevented). Access privileges to previously authorized resources are then revoked and the Other-ID is prevented from accessing previously authorized resources. The enterprise may take additional action based on the build (quarantine, log out, etc.). The subject is playing the role of an insider threat and is intentionally trying to access unauthorized resources.

Pre-Condition: The endpoint used by the subject is compliant to the enterprise security policy (either enterprise-owned, BYOD or Guest). The Other-ID makes an unauthorized request that is flagged.

Demonstration: The enterprise can detect and respond when a possibly subverted or insider threat Other-ID attempts to access unauthorized resources.

Purpose and Outcome: Previously authorized access privileges being revoked and follow-up access requests for authorized resources are denied.

Table 2-42 Scenario F-12 Demonstrations

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
F-12.1	a	Ent-Owned	On-prem	On-prem	On-prem	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	b	Ent-Owned	On-prem	Cloud (IaaS)	On-prem	Access not successful.
	c	Ent-Owned	On-prem	Cloud (PaaS)	On-prem	Access not successful.
	d	Ent-Owned	On-prem	Cloud (SaaS)	On-prem	Access not successful.
	e	Ent-Owned	Branch	On-prem	On-prem	Access not successful.
	f	Ent-Owned	Branch	Cloud (IaaS)	On-prem	Access not successful.
	g	Ent-Owned	Branch	Cloud (PaaS)	On-prem	Access not successful.
	h	Ent-Owned	Branch	Cloud (SaaS)	On-prem	Access not successful.
	i	Ent-Owned	Remote	On-prem	On-prem	Access not successful.
	j	Ent-Owned	Remote	Cloud (IaaS)	On-prem	Access not successful.
	k	Ent-Owned	Remote	Cloud (PaaS)	On-prem	Access not successful.
	l	Ent-Owned	Remote	Cloud (SaaS)	On-prem	Access not successful.
	m	Ent-Owned	On-prem	On-prem	Cloud (IaaS)	Access not successful.
	n	Ent-owned	On-prem	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	o	Ent-owned	On-prem	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	p	End-owned	On-prem	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	q	Ent-Owned	Branch	On-prem	Cloud (IaaS)	Access not successful.
	r	Ent-owned	Branch	Cloud (IaaS)	Cloud (IaaS)	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	s	Ent-owned	Branch	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	t	End-owned	Branch	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	u	Ent-Owned	Remote	On-prem	Cloud (IaaS)	Access not successful.
	v	Ent-owned	Remote	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	w	Ent-owned	Remote	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	x	End-owned	Remote	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	y	Ent-Owned	On-prem	On-prem	Cloud (PaaS)	Access not successful.
	z	Ent-owned	On-prem	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	aa	Ent-owned	On-prem	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	ab	End-owned	On-prem	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ac	Ent-Owned	Branch	On-prem	Cloud (PaaS)	Access not successful.
	ad	Ent-owned	Branch	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ae	Ent-owned	Branch	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	af	End-owned	Branch	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ag	Ent-Owned	Remote	On-prem	Cloud (PaaS)	Access not successful.
	ah	Ent-owned	Remote	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ai	Ent-owned	Remote	Cloud (PaaS)	Cloud (PaaS)	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	aj	End-owned	Remote	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ak	Ent-Owned	On-prem	On-prem	Cloud (SaaS)	Access not successful.
	al	Ent-owned	On-prem	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	am	Ent-owned	On-prem	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	an	End-owned	On-prem	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	ao	Ent-Owned	Branch	On-prem	Cloud (SaaS)	Access not successful.
	ap	Ent-owned	Branch	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	aq	Ent-owned	Branch	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	ar	End-owned	Branch	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	as	Ent-Owned	Remote	On-prem	Cloud (SaaS)	Access not successful.
	at	Ent-owned	Remote	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	au	Ent-owned	Remote	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	av	End-owned	Remote	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
F-12.2	a	BYOD	On-prem	On-prem	On-prem	Access not successful.
	b	BYOD	On-prem	Cloud (IaaS)	On-prem	Access not successful.
	c	BYOD	On-prem	Cloud (PaaS)	On-prem	Access not successful.
	d	BYOD	On-prem	Cloud (SaaS)	On-prem	Access not successful.
	e	BYOD	Branch	On-prem	On-prem	Access not successful.
	f	BYOD	Branch	Cloud (IaaS)	On-prem	Access not successful.
	g	BYOD	Branch	Cloud (PaaS)	On-prem	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	h	BYOD	Branch	Cloud (SaaS)	On-prem	Access not successful.
	i	BYOD	Remote	On-prem	On-prem	Access not successful.
	j	BYOD	Remote	Cloud (IaaS)	On-prem	Access not successful.
	k	BYOD	Remote	Cloud (PaaS)	On-prem	Access not successful.
	l	BYOD	Remote	Cloud (SaaS)	On-prem	Access not successful.
	m	BYOD	On-prem	On-prem	Cloud (IaaS)	Access not successful.
	n	BYOD	On-prem	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	o	BYOD	On-prem	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	p	BYOD	On-prem	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	q	BYOD	Branch	On-prem	Cloud (IaaS)	Access not successful.
	r	BYOD	Branch	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	s	BYOD	Branch	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	t	BYOD	Branch	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	u	BYOD	Remote	On-prem	Cloud (IaaS)	Access not successful.
	v	BYOD	Remote	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	w	BYOD	Remote	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	x	BYOD	Remote	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	y	BYOD	On-prem	On-prem	Cloud (PaaS)	Access not successful.
	z	BYOD	On-prem	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	aa	BYOD	On-prem	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	ab	BYOD	On-prem	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ac	BYOD	Branch	On-prem	Cloud (PaaS)	Access not successful.
	ad	BYOD	Branch	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ae	BYOD	Branch	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	af	BYOD	Branch	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ag	BYOD	Remote	On-prem	Cloud (PaaS)	Access not successful.
	ah	BYOD	Remote	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ai	BYOD	Remote	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	aj	BYOD	Remote	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ak	BYOD	On-prem	On-prem	Cloud (SaaS)	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	al	BYOD	On-prem	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	am	BYOD	On-prem	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	an	BYOD	On-prem	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	ao	BYOD	Branch	On-prem	Cloud (SaaS)	Access not successful.
	ap	BYOD	Branch	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	aq	BYOD	Branch	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	ar	BYOD	Branch	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	as	BYOD	Remote	On-prem	Cloud (SaaS)	Access not successful.
	at	BYOD	Remote	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	au	BYOD	Remote	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	av	BYOD	Remote	Cloud (SaaS)	Cloud (SaaS)	Access not successful
F-12.3	a	Guest	On-prem	On-prem	On-prem	Access not successful.
	b	Guest	On-prem	Cloud (IaaS)	On-prem	Access not successful.
	c	Guest	On-prem	Cloud (PaaS)	On-prem	Access not successful.
	d	Guest	On-prem	Cloud (SaaS)	On-prem	Access not successful.
	e	Guest	Branch	On-prem	On-prem	Access not successful.
	f	Guest	Branch	Cloud (IaaS)	On-prem	Access not successful.
	g	Guest	Branch	Cloud (PaaS)	On-prem	Access not successful.
	h	Guest	Branch	Cloud (SaaS)	On-prem	Access not successful.
	i	Guest	Remote	On-prem	On-prem	Access not successful.
	j	Guest	Remote	Cloud (IaaS)	On-prem	Access not successful.
	k	Guest	Remote	Cloud (PaaS)	On-prem	Access not successful.
	l	Guest	Remote	Cloud (SaaS)	On-prem	Access not successful.
	m	Guest	On-prem	On-prem	Cloud (IaaS)	Access not successful.
	n	Guest	On-prem	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	o	Guest	On-prem	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	p	Guest	On-prem	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	q	Guest	Branch	On-prem	Cloud (IaaS)	Access not successful.
	r	Guest	Branch	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	s	Guest	Branch	Cloud (PaaS)	Cloud (IaaS)	Access not successful.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	t	Guest	Branch	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	u	Guest	Remote	On-prem	Cloud (IaaS)	Access not successful.
	v	Guest	Remote	Cloud (IaaS)	Cloud (IaaS)	Access not successful.
	w	Guest	Remote	Cloud (PaaS)	Cloud (IaaS)	Access not successful.
	x	Guest	Remote	Cloud (SaaS)	Cloud (IaaS)	Access not successful.
	y	Guest	On-prem	On-prem	Cloud (PaaS)	Access not successful.
	z	Guest	On-prem	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	aa	Guest	On-prem	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	ab	Guest	On-prem	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ac	Guest	Branch	On-prem	Cloud (PaaS)	Access not successful.
	ad	Guest	Branch	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ae	Guest	Branch	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	af	Guest	Branch	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ag	Guest	Remote	On-prem	Cloud (PaaS)	Access not successful.
	ah	Guest	Remote	Cloud (IaaS)	Cloud (PaaS)	Access not successful.
	ai	Guest	Remote	Cloud (PaaS)	Cloud (PaaS)	Access not successful.
	aj	Guest	Remote	Cloud (SaaS)	Cloud (PaaS)	Access not successful.
	ak	Guest	On-prem	On-prem	Cloud (SaaS)	Access not successful.
	al	Guest	On-prem	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	am	Guest	On-prem	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	an	Guest	On-prem	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	ao	Guest	Branch	On-prem	Cloud (SaaS)	Access not successful.
	ap	Guest	Branch	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	aq	Guest	Branch	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	ar	Guest	Branch	Cloud (SaaS)	Cloud (SaaS)	Access not successful.
	as	Guest	Remote	On-prem	Cloud (SaaS)	Access not successful.
	at	Guest	Remote	Cloud (IaaS)	Cloud (SaaS)	Access not successful.
	au	Guest	Remote	Cloud (PaaS)	Cloud (SaaS)	Access not successful.
	av	Guest	Remote	Cloud (SaaS)	Cloud (SaaS)	Access not successful.

2.9.13 Scenario F-13: Other-ID Attempting Unauthorized Access Detection and Response, Ongoing Sessions

This scenario demonstrates the enterprise's ability to detect and respond to violations of the enterprise authorization policy. In this scenario, an other-ID has an open session for a resource, but the endpoint sends an HTTP GET to a known bad URL, triggering a policy violation. The enterprise then closes the session between the subject and the resource and may take additional action based on the build (quarantine, log out, etc.). The subject is playing the role of an insider threat and is intentionally trying to access unauthorized resources.

Pre-Condition: Valid other-ID has successfully authenticated to resource and is authorized to use resource. The endpoint used by the subject is compliant to the enterprise security policy (either enterprise-owned, BYOD or Guest). The Other-ID makes an authorized request that is flagged as a violation and results in current sessions being terminated.

Demonstration: A valid other-ID has an authenticated and authorized session to a resource. The other-ID attempts to perform an unauthorized action or access request. The system responds by terminating active session(s).

Purpose and Outcome: The enterprise can detect and respond when a possibly subverted or insider threat other-ID attempts to access unauthorized resources.

Table 2-43 Scenario F-13 Demonstrations

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
F-13.1	a	Ent-Owned	On-prem	On-prem	On-prem	Active session terminated.
	b	Ent-Owned	On-prem	Cloud (IaaS)	On-prem	Active session terminated.
	c	Ent-Owned	On-prem	Cloud (PaaS)	On-prem	Active session terminated.
	d	Ent-Owned	On-prem	Cloud (SaaS)	On-prem	Active session terminated.
	e	Ent-Owned	Branch	On-prem	On-prem	Active session terminated.
	f	Ent-Owned	Branch	Cloud (IaaS)	On-prem	Active session terminated.
	g	Ent-Owned	Branch	Cloud (PaaS)	On-prem	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	h	Ent-Owned	Branch	Cloud (SaaS)	On-prem	Active session terminated.
	i	Ent-Owned	Remote	On-prem	On-prem	Active session terminated.
	j	Ent-Owned	Remote	Cloud (IaaS)	On-prem	Active session terminated.
	k	Ent-Owned	Remote	Cloud (PaaS)	On-prem	Active session terminated.
	l	Ent-Owned	Remote	Cloud (SaaS)	On-prem	Active session terminated.
	m	Ent-Owned	On-prem	On-prem	Cloud (IaaS)	Active session terminated.
	n	Ent-owned	On-prem	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	o	Ent-owned	On-prem	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	p	End-owned	On-prem	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	q	Ent-Owned	Branch	On-prem	Cloud (IaaS)	Active session terminated.
	r	Ent-owned	Branch	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	s	Ent-owned	Branch	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	t	End-owned	Branch	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	u	Ent-Owned	Remote	On-prem	Cloud (IaaS)	Active session terminated.
	v	Ent-owned	Remote	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	w	Ent-owned	Remote	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	x	End-owned	Remote	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.

Demo ID	Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
y	Ent-Owned	On-prem	On-prem	Cloud (PaaS)	Active session terminated.
z	Ent-owned	On-prem	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
aa	Ent-owned	On-prem	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
ab	End-owned	On-prem	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
ac	Ent-Owned	Branch	On-prem	Cloud (PaaS)	Active session terminated.
ad	Ent-owned	Branch	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
ae	Ent-owned	Branch	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
af	End-owned	Branch	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
ag	Ent-Owned	Remote	On-prem	Cloud (PaaS)	Active session terminated.
ah	Ent-owned	Remote	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
ai	Ent-owned	Remote	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
aj	End-owned	Remote	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
ak	Ent-Owned	On-prem	On-prem	Cloud (SaaS)	Active session terminated.
al	Ent-owned	On-prem	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
am	Ent-owned	On-prem	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
an	End-owned	On-prem	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
ao	Ent-Owned	Branch	On-prem	Cloud (SaaS)	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	ap	Ent-owned	Branch	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	aq	Ent-owned	Branch	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	ar	End-owned	Branch	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	as	Ent-Owned	Remote	On-prem	Cloud (SaaS)	Active session terminated.
	at	Ent-owned	Remote	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	au	Ent-owned	Remote	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	av	End-owned	Remote	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
F-13.2	a	BYOD	On-prem	On-prem	On-prem	Active session terminated.
	b	BYOD	On-prem	Cloud (IaaS)	On-prem	Active session terminated.
	c	BYOD	On-prem	Cloud (PaaS)	On-prem	Active session terminated.
	d	BYOD	On-prem	Cloud (SaaS)	On-prem	Active session terminated.
	e	BYOD	Branch	On-prem	On-prem	Active session terminated.
	f	BYOD	Branch	Cloud (IaaS)	On-prem	Active session terminated.
	g	BYOD	Branch	Cloud (PaaS)	On-prem	Active session terminated.
	h	BYOD	Branch	Cloud (SaaS)	On-prem	Active session terminated.
	i	BYOD	Remote	On-prem	On-prem	Active session terminated.
	j	BYOD	Remote	Cloud (IaaS)	On-prem	Active session terminated.
	k	BYOD	Remote	Cloud (PaaS)	On-prem	Active session terminated.
	l	BYOD	Remote	Cloud (SaaS)	On-prem	Active session terminated.
	m	BYOD	On-prem	On-prem	Cloud (IaaS)	Active session terminated.
	n	BYOD	On-prem	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	o	BYOD	On-prem	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	p	BYOD	On-prem	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	q	BYOD	Branch	On-prem	Cloud (IaaS)	Active session terminated.
	r	BYOD	Branch	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	s	BYOD	Branch	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	t	BYOD	Branch	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	u	BYOD	Remote	On-prem	Cloud (IaaS)	Active session terminated.
	v	BYOD	Remote	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	w	BYOD	Remote	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	x	BYOD	Remote	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	y	BYOD	On-prem	On-prem	Cloud (PaaS)	Active session terminated.
	z	BYOD	On-prem	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	aa	BYOD	On-prem	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	ab	BYOD	On-prem	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ac	BYOD	Branch	On-prem	Cloud (PaaS)	Active session terminated.
	ad	BYOD	Branch	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	ae	BYOD	Branch	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	af	BYOD	Branch	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ag	BYOD	Remote	On-prem	Cloud (PaaS)	Active session terminated.
	ah	BYOD	Remote	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	ai	BYOD	Remote	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	aj	BYOD	Remote	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ak	BYOD	On-prem	On-prem	Cloud (SaaS)	Active session terminated.
	al	BYOD	On-prem	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	am	BYOD	On-prem	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	an	BYOD	On-prem	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	ao	BYOD	Branch	On-prem	Cloud (SaaS)	Active session terminated.
	ap	BYOD	Branch	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	aq	BYOD	Branch	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	ar	BYOD	Branch	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	as	BYOD	Remote	On-prem	Cloud (SaaS)	Active session terminated.
	at	BYOD	Remote	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	au	BYOD	Remote	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	av	BYOD	Remote	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
F-13.3	a	Guest	On-prem	On-prem	On-prem	Active session terminated.
	b	Guest	On-prem	Cloud (IaaS)	On-prem	Active session terminated.
	c	Guest	On-prem	Cloud (PaaS)	On-prem	Active session terminated.
	d	Guest	On-prem	Cloud (SaaS)	On-prem	Active session terminated.
	e	Guest	Branch	On-prem	On-prem	Active session terminated.
	f	Guest	Branch	Cloud (IaaS)	On-prem	Active session terminated.
	g	Guest	Branch	Cloud (PaaS)	On-prem	Active session terminated.
	h	Guest	Branch	Cloud (SaaS)	On-prem	Active session terminated.
	i	Guest	Remote	On-prem	On-prem	Active session terminated.
	j	Guest	Remote	Cloud (IaaS)	On-prem	Active session terminated.
	k	Guest	Remote	Cloud (PaaS)	On-prem	Active session terminated.
	l	Guest	Remote	Cloud (SaaS)	On-prem	Active session terminated.
	m	Guest	On-prem	On-prem	Cloud (IaaS)	Active session terminated.
	n	Guest	On-prem	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	o	Guest	On-prem	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	p	Guest	On-prem	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	q	Guest	Branch	On-prem	Cloud (IaaS)	Active session terminated.
	r	Guest	Branch	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	s	Guest	Branch	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	t	Guest	Branch	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	u	Guest	Remote	On-prem	Cloud (IaaS)	Active session terminated.
	v	Guest	Remote	Cloud (IaaS)	Cloud (IaaS)	Active session terminated.
	w	Guest	Remote	Cloud (PaaS)	Cloud (IaaS)	Active session terminated.
	x	Guest	Remote	Cloud (SaaS)	Cloud (IaaS)	Active session terminated.
	y	Guest	On-prem	On-prem	Cloud (PaaS)	Active session terminated.
	z	Guest	On-prem	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	aa	Guest	On-prem	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	ab	Guest	On-prem	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ac	Guest	Branch	On-prem	Cloud (PaaS)	Active session terminated.
	ad	Guest	Branch	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.

Demo ID		Subj Type	Subject Location	Unauthorized RSS Location	Authorized RSS Location	Desired Outcome
	ae	Guest	Branch	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	af	Guest	Branch	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ag	Guest	Remote	On-prem	Cloud (PaaS)	Active session terminated.
	ah	Guest	Remote	Cloud (IaaS)	Cloud (PaaS)	Active session terminated.
	ai	Guest	Remote	Cloud (PaaS)	Cloud (PaaS)	Active session terminated.
	aj	Guest	Remote	Cloud (SaaS)	Cloud (PaaS)	Active session terminated.
	ak	Guest	On-prem	On-prem	Cloud (SaaS)	Active session terminated.
	al	Guest	On-prem	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	am	Guest	On-prem	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	an	Guest	On-prem	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	ao	Guest	Branch	On-prem	Cloud (SaaS)	Active session terminated.
	ap	Guest	Branch	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	aq	Guest	Branch	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	ar	Guest	Branch	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.
	as	Guest	Remote	On-prem	Cloud (SaaS)	Active session terminated.
	at	Guest	Remote	Cloud (IaaS)	Cloud (SaaS)	Active session terminated.
	au	Guest	Remote	Cloud (PaaS)	Cloud (SaaS)	Active session terminated.
	av	Guest	Remote	Cloud (SaaS)	Cloud (SaaS)	Active session terminated.

2.9.14 Scenario F-14: Enterprise-ID Denied Access Due to Suspicious Endpoint

This scenario demonstrates the enterprise's ability to detect and respond to prevent access by an Enterprise-ID using a suspected compromised endpoint. In this scenario, an enterprise-ID sends an access request, but the subject endpoint has been flagged for suspicious traffic (e.g., doing nmap scans). The enterprise then flags the endpoint and prevents any access by the Enterprise-ID. The ID is not specifically being used in this scenario, and the subverted endpoint may not be performing actions that require authentication by the Enterprise-ID (e.g., access request to another resource).

Pre-Condition: Valid Enterprise-ID is authorized to use resource. The endpoint used by the subject has performed suspicious activity. The enterprise can monitor network traffic.

Demonstration: A valid enterprise-ID is using a possibly subverted endpoint. The enterprise-ID attempts to access an authorized resource, but the system determines the endpoint is untrusted and denies the access request.

Purpose and Outcome: The enterprise can detect and respond when Enterprise-ID is using a potentially subverted endpoint and prevents resource access.

Table 2-44 Scenario F-14 Demonstrations

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
F-14.1	a	Ent-Owned	On-prem	On-prem	Access not successful
	b	Ent-Owned	Branch	On-prem	Access not successful
	c	Ent-Owned	Remote	On-prem	Access not successful
	d	Ent-Owned	On-prem	Cloud (IaaS)	Access not successful
	e	Ent-Owned	Branch	Cloud (IaaS)	Access not successful
	f	Ent-Owned	Remote	Cloud (IaaS)	Access not successful
	g	Ent-Owned	On-prem	Cloud (PaaS)	Access not successful
	h	Ent-Owned	Branch	Cloud (PaaS)	Access not successful
	i	Ent-Owned	Remote	Cloud (PaaS)	Access not successful
	j	Ent-Owned	On-prem	Cloud (SaaS)	Access not successful
	k	Ent-Owned	Branch	Cloud (SaaS)	Access not successful
	l	Ent-Owned	Remote	Cloud (SaaS)	Access not successful
F-14.2	a	BYOD	On-prem	On-prem	Access not successful
	b	BYOD	Branch	On-prem	Access not successful
	c	BYOD	Remote	On-prem	Access not successful
	d	BYOD	On-prem	Cloud (IaaS)	Access not successful
	e	BYOD	Branch	Cloud (IaaS)	Access not successful
	f	BYOD	Remote	Cloud (IaaS)	Access not successful
	g	BYOD	On-prem	Cloud (PaaS)	Access not successful
	h	BYOD	Branch	Cloud (PaaS)	Access not successful
	i	BYOD	Remote	Cloud (PaaS)	Access not successful
	j	BYOD	On-prem	Cloud (SaaS)	Access not successful
	k	BYOD	Branch	Cloud (SaaS)	Access not successful
	l	BYOD	Remote	Cloud (SaaS)	Access not successful

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
F-14.3	a	Guest	On-prem	On-prem	Access not successful
	b	Guest	Branch	On-prem	Access not successful
	c	Guest	Remote	On-prem	Access not successful
	d	Guest	On-prem	Cloud (IaaS)	Access not successful
	e	Guest	Branch	Cloud (IaaS)	Access not successful
	f	Guest	Remote	Cloud (IaaS)	Access not successful
	g	Guest	On-prem	Cloud (PaaS)	Access not successful
	h	Guest	Branch	Cloud (PaaS)	Access not successful
	i	Guest	Remote	Cloud (PaaS)	Access not successful
	j	Guest	On-prem	Cloud (SaaS)	Access not successful
	k	Guest	Branch	Cloud (SaaS)	Access not successful
	l	Guest	Remote	Cloud (SaaS)	Access not successful

2.9.15 Scenario F-15: Other-ID Denied Access due to Suspicious Endpoint

This scenario demonstrates the enterprise's ability to detect and respond to prevent access by an Other-ID using a suspected compromised endpoint. In this scenario, an Other-ID sends an access request, but the subject endpoint has been flagged for suspicious traffic (e.g., doing nmap scans). The enterprise then flags the endpoint and prevents any access by the Other-ID. The ID may not play a role in this scenario, the subverted endpoint may not be performing actions that require authentication by the Other-ID (e.g., service call from endpoint service, nmap scan, etc.).

Pre-Condition: Valid Other-ID is authorized to use resource. The endpoint used by the subject has performed suspicious activity. The enterprise can monitor network traffic.

Demonstration: A valid other-ID is using a possibly subverted endpoint. The other-ID attempts to access an authorized resource, but the system determines the endpoint is untrusted and denies the access request.

Purpose and Outcome: The enterprise can detect and respond when Other-ID is using a potentially subverted endpoint and prevents resource access.

Table 2-45 Scenario F-15 Demonstrations

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	a	Ent-Owned	On-prem	On-prem	Access not successful

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
F-15.1	b	Ent-Owned	Branch	On-prem	Access not successful
	c	Ent-Owned	Remote	On-prem	Access not successful
	d	Ent-Owned	On-prem	Cloud (IaaS)	Access not successful
	e	Ent-Owned	Branch	Cloud (IaaS)	Access not successful
	f	Ent-Owned	Remote	Cloud (IaaS)	Access not successful
	g	Ent-Owned	On-prem	Cloud (PaaS)	Access not successful
	h	Ent-Owned	Branch	Cloud (PaaS)	Access not successful
	i	Ent-Owned	Remote	Cloud (PaaS)	Access not successful
	j	Ent-Owned	On-prem	Cloud (SaaS)	Access not successful
	k	Ent-Owned	Branch	Cloud (SaaS)	Access not successful
	l	Ent-Owned	Remote	Cloud (SaaS)	Access not successful
F-15.2	a	BYOD	On-prem	On-prem	Access not successful
	b	BYOD	Branch	On-prem	Access not successful
	c	BYOD	Remote	On-prem	Access not successful
	d	BYOD	On-prem	Cloud (IaaS)	Access not successful
	e	BYOD	Branch	Cloud (IaaS)	Access not successful
	f	BYOD	Remote	Cloud (IaaS)	Access not successful
	g	BYOD	On-prem	Cloud (PaaS)	Access not successful
	h	BYOD	Branch	Cloud (PaaS)	Access not successful
	i	BYOD	Remote	Cloud (PaaS)	Access not successful
	j	BYOD	On-prem	Cloud (SaaS)	Access not successful
	k	BYOD	Branch	Cloud (SaaS)	Access not successful
	l	BYOD	Remote	Cloud (SaaS)	Access not successful
F-15.3	a	Guest	On-prem	On-prem	Access not successful
	b	Guest	Branch	On-prem	Access not successful
	c	Guest	Remote	On-prem	Access not successful
	d	Guest	On-prem	Cloud (IaaS)	Access not successful
	e	Guest	Branch	Cloud (IaaS)	Access not successful
	f	Guest	Remote	Cloud (IaaS)	Access not successful
	g	Guest	On-prem	Cloud (PaaS)	Access not successful
	h	Guest	Branch	Cloud (PaaS)	Access not successful

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	i	Guest	Remote	Cloud (PaaS)	Access not successful
	j	Guest	On-prem	Cloud (SaaS)	Access not successful
	k	Guest	Branch	Cloud (SaaS)	Access not successful
	l	Guest	Remote	Cloud (SaaS)	Access not successful

2.9.16 Scenario F-16: Enterprise-ID Access Terminated Due to Suspicious Endpoint

This scenario demonstrates the enterprise's ability to detect and respond to a suspicious endpoint that is in use. In this scenario, an enterprise-ID has an open session for a resource, but the endpoint is performing suspicious activity (e.g., an nmap scan). The enterprise then closes the session between the subject and the resource and may take additional action based on the build (quarantine, log out, etc.). The ID is not specifically being tested in this scenario, and the subverted endpoint may not be performing actions that require authentication by the Enterprise-ID.

Pre-Condition: Valid Enterprise-ID has successfully authenticated to resource and is authorized to use resource. The enterprise can monitor outbound queries.

Demonstration: A valid enterprise-ID has an authenticated and authorized session open to a resource. The system detects suspicious activity from the subject endpoint and terminates active session(s).

Purpose and Outcome: The enterprise can detect and respond when Enterprise-ID is using a potentially subverted endpoint.

Table 2-46 Scenario F-16 Demonstrations

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
F-16.1	a	Ent-Owned	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	Ent-Owned	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	Ent-Owned	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	Ent-Owned	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	Ent-Owned	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	f	Ent-Owned	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	Ent-Owned	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	Ent-Owned	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	Ent-Owned	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	Ent-Owned	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	Ent-Owned	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	Ent-Owned	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
F-16.2	a	BYOD	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	BYOD	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	BYOD	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	BYOD	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	BYOD	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	BYOD	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	BYOD	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	BYOD	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	BYOD	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	BYOD	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	k	BYOD	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	BYOD	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
F-16.3	a	Guest	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	Guest	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	Guest	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	Guest	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	Guest	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	Guest	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	Guest	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	Guest	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	Guest	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	Guest	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	Guest	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	Guest	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).

2.9.17 Scenario F-17: Other-ID Access Terminated Due to Suspicious Endpoint

This scenario demonstrates the enterprise's ability to detect and respond to suspicious endpoint that is in use. In this scenario, an Other-ID has an open session for a resource, but the endpoint is performing suspicious activity (e.g., an nmap scan). The enterprise then closes the session between the subject and the resource and may take additional action based on the build (quarantine, log out, etc.). The ID may not play a role in this scenario, and the subverted endpoint may not be performing actions that require authentication by the Other-ID.

Pre-Condition: Valid Other-ID has successfully authenticated to resource and is authorized to use resource. The enterprise can monitor outbound queries.

Demonstration: A valid enterprise-ID has an authenticated and authorized session open to a resource. The system detects suspicious activity from the subject endpoint and terminates active session(s).

Purpose and Outcome: The enterprise can detect and respond when Other-ID is using a potentially subverted endpoint.

Table 2-47 Scenario F-17 Demonstrations

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
F-17.1	a	Ent-Owned	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	Ent-Owned	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	Ent-Owned	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	Ent-Owned	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	Ent-Owned	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	Ent-Owned	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	Ent-Owned	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	Ent-Owned	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	Ent-Owned	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	Ent-Owned	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	Ent-Owned	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	l	Ent-Owned	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
F-17.2	a	BYOD	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	BYOD	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	BYOD	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	BYOD	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	e	BYOD	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	f	BYOD	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	BYOD	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	BYOD	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	i	BYOD	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	j	BYOD	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	BYOD	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	l	BYOD	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
F-17.3	a	Guest	On-prem	On-prem	Access stopped (no longer able to connect to resource).
	b	Guest	Branch	On-prem	Access stopped (no longer able to connect to resource).
	c	Guest	Remote	On-prem	Access stopped (no longer able to connect to resource).
	d	Guest	On-prem	Cloud (IaaS)	Access stopped (no longer able to connect to resource).

Demo ID		Subj Type	Subject Location	RSS Location	Desired Outcome
	e	Guest	Branch	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	F	Guest	Remote	Cloud (IaaS)	Access stopped (no longer able to connect to resource).
	g	Guest	On-prem	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	h	Guest	Branch	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	I	Guest	Remote	Cloud (PaaS)	Access stopped (no longer able to connect to resource).
	J	Guest	On-prem	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	k	Guest	Branch	Cloud (SaaS)	Access stopped (no longer able to connect to resource).
	L	Guest	Remote	Cloud (SaaS)	Access stopped (no longer able to connect to resource).

2.10 Use Case G: Service-Service Interactions

This use case covers non-person entities and API calls between services. This covers automated processes as well. It is assumed MFA is not possible as there is no human subject involved in the session establishment. The enterprise should be able to uniquely identify (and authenticate) both the subject and resource in each test scenario. The method of this could vary and is not dictated in these scnearios. Endpoints where the service is running could be physical or virtual and include services running in containers.

2.10.1 Scenario G-1: Service Calls Between Resources

This scenario demonstrates service-to-service communication between resources located on enterprise-operated infrastructure (on-prem or branch). Both resources (subject and requested resource) are considered authenticated and in compliance. The subject can be authorized or unauthorized to perform the action, as indicated in the table.

Pre-Condition: Two subjects, one authorized to perform the action and the other not authorized. All actors are in compliance with the enterprise security posture and authenticated to all relevant enterprise systems. All communications (successful and failed) are logged.

Demonstration: The subject system performs an action that involves an API call, or other service-to-service communication to another resource. All communication is logged.

Purpose and Outcome: This scenario demonstrates how the enterprise architecture prevents unauthorized communication between services and records all communication attempts (successful and prevented).

Table 2-48 Scenario G-1 Demonstrations

Demo ID		Subj. Location	Authorized	RSS Loc	Desired Outcome
G-1.1	a	On-prem	Yes	On-Prem	Access successful
	b	On-prem	No		Access not successful
	c	Branch	Yes		Access successful
	d	Branch	No		Access not successful
	e	Remote (IaaS)	Yes		Access successful
	f	Remote (IaaS)	No		Access not successful
	g	Remote (PaaS)	Yes		Access successful
	h	Remote (PaaS)	No		Access not successful
	i	Remote (SaaS)	Yes		Access successful
	j	Remote (SaaS)	No		Access not successful
G-1.2	a	On-prem	Yes	Branch	Access successful
	b	On-Prem	No		Access not successful
	c	Branch	Yes		Access successful
	d	Branch	No		Access not successful
	e	Remote (IaaS)	Yes		Access successful
	f	Remote (IaaS)	No		Access not successful
	g	Remote (PaaS)	Yes		Access successful
	h	Remote (Paas)	No		Access not successful
	i	Remote (SaaS)	Yes		Access successful
	j	Remote (Saas)	No		Access not successful

2.10.2 Scenario G-2: Service Calls to Cloud-Based Resources

This scenario demonstrates service-to-service communication between resources located on enterprise-operated infrastructure (on-prem or branch) and cloud-based assets. Both resources (subject and requested resource) are considered authenticated and in compliance. The subject can be authorized or unauthorized to perform the action, as indicated in the table. The requested resource is IaaS, PaaS, or SaaS.

Pre-Condition: Two subjects, one authorized to perform the action and the other not authorized. All actors are in compliance and authenticated to all relevant enterprise systems. All communications (successful and failed) are logged.

Demonstration: The subject system performs an action that involves an API call or some other service-to-service communication to a resource. All communication is logged.

Purpose and Outcome: This scenario demonstrates how the enterprise architecture prevents unauthorized communication between services and records all communication attempts (successful and prevented).

Table 2-49 Scenario G-2 Demonstrations

Demo ID		Subj. Location	Authorized	RSS Type	Desired Outcome
G-2.1	a	On-prem	Yes	IaaS	Access successful
	b	On-prem	No		Access not successful
	c	Branch	Yes		Access successful
	d	Branch	No		Access not successful
	e	Remote	Yes		Access successful
	f	Remote	No		Access not successful
G-2.2	a	On-prem	Yes	PaaS	Access successful
	b	On-prem	No		Access not successful
	c	Branch	Yes		Access successful
	d	Branch	No		Access not successful
	e	Remote	Yes		Access successful
	f	Remote	No		Access not successful
G-2.3	a	On-prem	Yes	SaaS	Access successful
	b	On-Prem	No		Access not successful
	c	Branch	Yes		Access successful
	d	Branch	No		Access not successful
	e	Remote	Yes		Access successful
	f	Remote	No		Access not successful

2.10.3 Scenario G-3: Service Calls between Cloud-Based Resources

This scenario demonstrates service-to-service communication between resources located on separate cloud-based resources. Both resources (subject and requested resource) are considered authenticated and in compliance. The subject can be authorized or unauthorized to perform the action, as indicated in the table. The resources are IaaS, PaaS, or SaaS.

Pre-Condition: Two subjects, one authorized to perform the action and the other not authorized. All actors are in compliance and authenticated to all relevant enterprise systems. All communications (successful and failed) are logged.

Demonstration: The subject system performs an action that involves an API call or some other service-to-service communication to a resource. All communication is logged.

Purpose and Outcome: This scenario demonstrates how the enterprise architecture prevents unauthorized communication between services and records all communication attempts (successful and prevented).

Table 2-50 Scenario G-3 Demonstrations

Demo ID		Subj. Type	Authorized	RSS Type	Desired Outcome
G-3.1	a	IaaS	Yes	IaaS	Access successful
	b	IaaS	No		Access not successful
	c	PaaS	Yes		Access successful
	d	PaaS	No		Access not successful
	e	SaaS	Yes		Access successful
	f	SaaS	No		Access not successful
G-3.2	a	IaaS	Yes	PaaS	Access successful
	b	IaaS	No		Access not successful
	c	PaaS	Yes		Access successful
	d	PaaS	No		Access not successful
	e	SaaS	Yes		Access successful
	f	SaaS	No		Access not successful
G-3.3	a	IaaS	Yes	SaaS	Access successful
	b	IaaS	No		Access not successful
	c	PaaS	Yes		Access successful
	d	PaaS	No		Access not successful

Demo ID		Subj. Type	Authorized	RSS Type	Desired Outcome
	e	SaaS	Yes		Access successful
	f	SaaS	No		Access not successful

2.10.4 Scenario G-4: Service Calls between Containers

This scenario demonstrates service-to-service communication between resources located on separate containers, both in the same runtime or part of a larger Kubernetes pod(s) deployment. Both resources (subject and requested resource) are considered authenticated and in compliance. The subject can be authorized or unauthorized to perform the action, as indicated in the table. The subject is either another container in a single container runtime (e.g., Docker), in the same Kubernetes pod, or in a different Kubernetes pod from the requested resource.

Pre-Condition: Two subjects, one authorized to perform the action and the other unauthorized. All actors are in compliance and authenticated to all relevant enterprise systems. All communications (successful and failed) are logged.

Demonstration: The subject system performs an action that involves an API call or some other service-to-service communication to a resource. The enterprise can prevent unauthorized service-to-server communication. All communication is logged regardless of the outcome.

Purpose and Outcome: This scenario demonstrates how the enterprise architecture prevents unauthorized communication between services and records all communication attempts (successful and prevented).

Table 2-51 Scenario G-4 Demonstrations

Demo ID		Subj. Location	Authorized	Desired Outcome
G-4.1	a	Bare runtime	Yes	Access successful
	b	Bare runtime	No	Access not successful
	c	Separate pod	Yes	Access successful
	d	Separate pod	No	Access not successful
	e	Same pod	Yes	Access successful
	f	Same pod	No	Access successful

2.10.5 Scenario G-5: Service to Endpoint

In this demonstration, an enterprise service reaches out to an enterprise managed endpoint to perform some action (e.g., maintenance, reconfiguration, etc.). User IDs are not directly involved in this scenario.

Pre-Condition: There is no active session from a subject to an enterprise resource. Both the subject endpoint and resource may be in compliance with enterprise security posture or expected to be in compliance after the session is completed. Service is located on-premises or as PaaS/SaaS (IaaS does not make sense as it is a service that is running in the cloud).

Demonstration: An enterprise service establishes a session with an endpoint to perform some administrative task, then closes the connection.

Purpose and Outcome: The enterprise can push administrative actions to enterprise endpoints in a secure manner.

Table 2-52 Scenario G-5 Demonstrations

Demo ID		Service Location	Endpoint Location	Endpoint Type	Desired Outcome
G-5.1	a	On-Prem	On-prem	Ent-Owned	Access Successful
	b	On-Prem	Branch	Ent-Owned	Access Successful
	c	On-Prem	Remote	Ent-Owned	Access Successful
	d	On-Prem	On-prem	BYOD	Access Successful
	e	On-Prem	Branch	BYOD	Access Successful
	f	On-Prem	Remote	BYOD	Access Successful
	g	PaaS	On-prem	Ent-Owned	Access Successful
	h	PaaS	Branch	Ent-Owned	Access Successful
	i	PaaS	Remote	End-Owned	Access Successful
	j	PaaS	On-prem	BYOD	Access Successful
	k	PaaS	Branch	BYOD	Access Successful
	l	PaaS	Remote	BYOD	Access Successful
	m	SaaS	On-prem	Ent-Owned	Access Successful
	n	SaaS	Branch	Ent-Owned	Access Successful
	o	SaaS	Remote	End-Owned	Access Successful
	p	SaaS	On-prem	BYOD	Access Successful
	q	SaaS	Branch	BYOD	Access Successful
	r	SaaS	Remote	BYOD	Access Successful

3 Functional Demonstration Result Summaries

This section provides a summary of the demonstration results for each of the builds that was implemented as part of this project. The summary results are organized according to the build phases that were defined in *NIST SP 1800-35B: Approach, Architecture, and Security Characteristics*. Detailed results for each of the builds are provided in Appendices C, D, and E. For each build, summary results for use cases A-G are provided.

3.1 EIG Crawl Phase Summary Demonstration Results

This section lists the summary demonstration results for each of the builds that was implemented as part of the EIG crawl phase: E1B1, E2B1, and E3B1. Cloud-based scenarios, and more sophisticated scenarios such as Stolen Credential, Just-in-Time Access Privileges, Enterprise-ID Step-Up Authentication, Federated-ID Access, Confidence Level, and Service-Service Interactions scenarios were decided to be out of scope for the EIG crawl phase. Only E1B1 has a branch office; E2B1 and E3B1 do not.

3.1.1 Enterprise 1 Build 1 (E1B1) Summary Demonstration Results

This build does not have IaaS, PaaS, or SaaS resources. Its summary results are as follows:

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

Description: This use case demonstrates the ability of the enterprise to discover network assets, authenticate devices, and demonstrate network connectivity.

- Discovery and authentication of endpoint assets – Not demonstrated due to lack of capability. There is no network-level enforcement present in this build.
- Reauthentication of identified assets – Not demonstrated due to lack of capability.
- Discovery of transaction flows – Demonstrated visibility of authentication and resource access attempts via Okta logs.

Use Case B: Enterprise-ID Access, Use Case D: Other-ID Access

Description: This use case demonstrates user access to enterprise resources based on successfully achieving user and device security preconditions.

- For this build, we successfully demonstrated access using mobile device iOS and Android endpoints.
- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to enterprise resources (on-prem) in accordance with policy via Okta Identity Cloud.

    - The policy engine can differentiate between employees and contractors and provide different access permissions to each user type.

- Internet access enforcement for Enterprise and Contractor Users on an enterprise endpoint or BYOD – Out of scope for EIG crawl phase.
- Stolen credential using an enterprise endpoint or BYOD – Out of scope for EIG crawl phase.
- Just-in-Time Access Privileges – Out of scope for EIG crawl phase.
- Enterprise-ID Step-Up Authentication – Out of scope for EIG crawl phase.
- This build did not have the capability to verify resource compliance with policy.

Use Case C: Federated-ID Access – Out of scope for EIG crawl phase.

Use Case D: Other-ID Access – Results are the same as for use case B. Users with Other-ID Access (e.g., a contractor) have authorized access to resources based on need, so results for these users are no different than the results for users with Enterprise-ID Access.

Use Case E: Guest: No-ID Access – Out of scope for EIG crawl phase.

Use Case F: Confidence Level – Out of scope for EIG crawl phase.

Use Case G: Service-Service Interactions – Out of scope for EIG crawl phase.

3.1.2 Enterprise 2 Build 1 (E2B1) Summary Demonstration Results

This build does not have IaaS, PaaS, or SaaS resources. Its summary results are as follows:

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

Description: This use case demonstrates the ability of the enterprise to discover network assets, authenticate devices, and demonstrate network connectivity

- Discovery and authentication of endpoint assets – Not demonstrated due to lack of capability. There is no network-level enforcement present in this build.
- Reauthentication of identified assets – Not demonstrated due to lack of capability.
- Discovery of transaction flows – Demonstrated visibility of authentication and resource access attempts via Ping Federate and Cisco Duo.

Use Case B: Enterprise-ID Access, Use Case D: Other-ID Access

Description: This use case demonstrates user access to enterprise resources based on successfully achieving user and device security preconditions.

- For this build, we successfully demonstrated access using Windows, macOS, and mobile device iOS and Android endpoints.

- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to enterprise resources (on-prem) in accordance with policy via Ping Federate.
    - The policy engine can differentiate between employees and contractors and provide different access permissions to each user type.
- Internet access enforcement for Enterprise and Contractor users on an enterprise endpoint or BYOD – Out of scope for EIG crawl phase.
- Stolen credential using an enterprise endpoint or BYOD – Out of scope for EIG crawl phase.
- Just-in-Time Access Privileges – Out of scope for EIG crawl phase.
- Enterprise-ID Step-Up Authentication – Out of scope for EIG crawl phase.
- This build did not have the capability to verify resource compliance with policy.

Use Case C: Federated-ID Access – Out of scope for EIG crawl phase.

Use Case D: Other-ID Access – Results are the same as for use case B. Users with Other-ID Access (e.g., a contractor) have authorized access to resources based on need, so results for these users are no different than the results for users with Enterprise-ID Access.

Use Case E: Guest: No-ID Access – Out of scope for EIG crawl phase.

Use Case F: Confidence Level – Out of scope for EIG crawl phase.

Use Case G: Service-Service Interactions – Out of scope for EIG crawl phase.

3.1.3 Enterprise 3 Build 1 (E3B1) Summary Demonstration Results

This build does not have IaaS or PaaS resources. Its summary results are as follows:

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

Description: This use case demonstrates the ability of the enterprise to discover network assets, authenticate devices, and demonstrate network connectivity.

- Discovery and authentication of endpoint assets – Not demonstrated due to lack of capability. There is no network-level enforcement present in this build.
- Reauthentication of identified assets – Not demonstrated due to lack of capability.
- Discovery of transaction flows – Demonstrated visibility of authentication and resource access attempts using Azure AD. Also, Azure AD audit logs that show activities were captured.

Use Case B: Enterprise-ID Access, Use Case D: Other-ID Access

Description: This use case demonstrates user access to enterprise resources based on successfully achieving user and device security preconditions.

- For this build, we successfully demonstrated access using Windows, macOS, and mobile device iOS and Android endpoints.
- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to enterprise resources (on-prem) in accordance with policy via Azure AD Conditional Access.
    - The policy engine can differentiate between employees and contractors and provide different access permissions to each user type.
- Internet access enforcement for Enterprise and Contractor Users on an enterprise endpoint or BYOD – Out of scope for EIG crawl phase.
- Stolen credential using an enterprise endpoint or BYOD – Out of scope for EIG crawl phase.
- Just-in-Time Access Privileges – Out of scope for EIG crawl phase.
- Enterprise-ID Step-Up Authentication – Out of scope for EIG crawl phase.
- This build did not have the capability to verify resource compliance with policy.

Use Case C: Federated-ID Access – Out of scope for EIG crawl phase.

Use Case D: Other-ID Access – Results are the same as for use case B. Users with Other-ID Access (e.g., a contractor) have authorized access to resources based on need, so results for these users are no different than the results for users with Enterprise-ID Access.

Use Case E: Guest: No-ID Access – Out of scope for EIG crawl phase.

Use Case F: Confidence Level – Out of scope for EIG crawl phase.

Use Case G: Service-Service Interactions – Out of scope for EIG crawl phase.

3.2 EIG Run Phase Summary Demonstration Results

This section lists the summary demonstration results for each of the builds that was implemented as part of the EIG run phase: E1B2, E3B2, and E4B3. Only E1B2 has a branch office; E3B2 and E4B3 do not. More sophisticated scenarios such as Just-in-Time Access Privileges, Enterprise-ID Step-Up Authentication, Federated-ID Access, Confidence Level, and Service-Service Interactions scenarios were decided to be out of scope for the EIG run phase for E1B2 and E3B2.

3.2.1 Enterprise 1 Build 2 (E1B2) Summary Demonstration Results

This build does not have SaaS resources. Its summary results are as follows:

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

Description: This use case demonstrates the ability of the enterprise to discover network assets, authenticate devices, and demonstrate network connectivity.

- Discovery and authentication of endpoint assets – Not demonstrated due to lack of capability. There is no network-level enforcement present in this build.
- Reauthentication of identified assets – Not demonstrated due to lack of capability.
- Discovery of transaction flows – Demonstrated visibility of authentication and resource access attempts via Okta logs and Zscaler Private Access (ZPA).

Use Case B: Enterprise-ID Access, Use Case D: Other-ID Access

Description: This use case demonstrates user access to enterprise resources based on successfully achieving user and device security preconditions.

- For this build, we successfully demonstrated access using Windows, macOS, Linux, and mobile device iOS and Android endpoints.
- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to enterprise resources (on-prem and cloud) in accordance with policy via ZPA.
    - The policy engine can differentiate between employees and contractors and provide different access permissions to each user type.
- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to internet resources accordance with policy via ZIA.
- Stolen credential using an enterprise endpoint or BYOD – Zscaler does not detect a hostile request if all credentials are correct.
- Just-in-Time Access Privileges – Out of scope for EIG run phase.
- Enterprise-ID Step-Up Authentication – Out of scope for EIG run phase.
- This build did not have the capability to verify resource compliance with policy.

Use Case C: Federated-ID Access – Out of scope for EIG run phase.

Use Case D: Other-ID Access – Results are the same as for use case B. Users with Other-ID Access (e.g., a contractor) have authorized access to resources based on need, so results for these users are no different than the results for users with Enterprise-ID Access.

Use Case E: Guest: No-ID Access – Guest requests public internet access. Zscaler Internet Access (ZIA) is configured to allow access to the internet if the device is unmanaged (i.e., No-ID).

Use Case F: Confidence Level – Out of scope for EIG run phase. This use case was demonstrated in a later iteration of this build, E1B3.

Use Case G: Service-Service Interactions – Out of scope for EIG run phase.

3.2.2 Enterprise 3 Build 2 (E3B2) Summary Demonstration Results

This build's summary results are as follows:

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

Description: This use case demonstrates the ability of the enterprise to discover network assets, authenticate devices, and demonstrate network connectivity

- Discovery and authentication of endpoint assets was successfully demonstrated. Resources and endpoints were granted access to the network and if applicable, limited to a specific subnet or resource set based on Forescout policy. These policies were enforced by a Palo Alto Next-Generation Firewall (NGFW) and Cisco switch. Due to the location of these policy enforcement points (PEPs), unauthenticated endpoints were restricted to the local subnet in accordance with Forescout policy.
    - Network assets were discovered by Forescout via both passive and active detection.
- Reauthentication of identified assets was also successfully demonstrated using Forescout and Microsoft Intune.
- Discovery of transaction flows – Demonstrated visibility of authentication and resource access attempts.
    - Azure AD captures sign-in logs to SaaS applications, PaaS, IaaS resources, and on-prem applications.
    - Azure AD audit logs are captured that show activity including changes to cloud resources in the Azure tenant.
    - Forescout captures sign-in and audit logs and network traffic for on-premises components.

Use Case B: Enterprise-ID Access, Use Case D: Other-ID Access

Description: This use case demonstrates user access to enterprise resources based on successfully achieving user and device security preconditions.

- For this build, we successfully demonstrated access using Windows, macOS, and mobile device iOS and Android endpoints.
- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to enterprise resources (on-prem and cloud) in accordance with policy via Azure AD Conditional Access.
    - The policy engine can differentiate between employees and contractors and provide different access permissions to each user type.

- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to internet resources in accordance with policy via Defender for Cloud Apps and Defender for Endpoint.
    - Policies within Defender for Cloud Apps were set up to allow, block, or limit access to resources.
    - The build demonstrated that documents with sensitive data such as credit cards could be viewed but not downloaded.
- Stolen credential using an enterprise endpoint or BYOD – Azure AD does not detect a hostile request if all credentials are correct.
- Just-in-Time Access Privileges – Out of scope for EIG run phase.
- Enterprise-ID Step-Up Authentication – Out of scope for EIG run phase.
- This build did not have the capability to verify chosen resource (e.g., GitLab) compliance with policy.

Use Case C: Federated-ID Access – Out of scope for EIG run phase.

Use Case D: Other-ID Access – Results are the same as for use case B. Users with Other-ID Access (e.g., a contractor) have authorized access to resources based on need, so results for these users are no different than the results for users with Enterprise-ID Access.

Use Case E: Guest: No-ID Access

Description: This use case demonstrates the ability of the enterprise to allow unmanaged guest devices to have access to public Internet resources.

- Forescout was able to provide Internet access to unauthenticated guest devices connecting to a segmented portion of the enterprise network.

Use Case F: Confidence Level – Out of scope for EIG run phase. This use case was demonstrated in a later iteration of this build, E3B3.

Use Case G: Service-Service Interactions – Out of scope for EIG run phase. This use case was demonstrated in a later iteration of this build, E3B3.

3.2.3 Enterprise 4 Build 3 (E4B3) Summary Demonstration Results

This build does not have SaaS or PaaS resources. Its summary results are as follows:

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

Description: This use case demonstrates the ability of the enterprise to discover network assets, authenticate devices, and demonstrate network connectivity.

- Discovery and authentication of managed endpoint assets were successfully demonstrated, based on IBM Security MaaS360 policy configuration.
    - This build also demonstrated the capability to limit or reduce user access levels in certain scenarios.
    - Resource authentication and limited access to the network were not demonstrated because IBM considers them out of scope for their products. Other technologies should be used to perform these functions.
- Reauthentication of identified assets was also successfully demonstrated using IBM Security MaaS360.
- Discovery of transaction flows – Demonstrated visibility of authentication and resource access attempts.
    - IBM Verify captures sign-in logs to cloud resources and on-prem applications.
    - IBM QRadar receives and parses sign-in logs for visibility.
    - IBM considers API call visibility out of scope for their products. Other technologies should be used to perform this function.

Use Case B: Enterprise-ID Access, Use Case D: Other-ID Access

Description: This use case demonstrates user access to enterprise resources based on successfully achieving user and device security preconditions.

- For this build, we successfully demonstrated access using Windows and mobile device iOS and Android endpoints.
- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to enterprise resources (on-prem and cloud) in accordance with policy via IBM Verify.
    - The policy engine can differentiate between employees and contractors and provide different access permissions to each user type.
    - We were unable to invalidate MaaS360 certificates to complete some scenarios, including scenarios that require the endpoint to fail authentication.
- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to internet resources (on-prem and cloud) in accordance with policy via the IBM Secure Browser.
    - Policies within IBM MaaS360 were set up to allow, block, or limit access to resources.
    - MaaS360 disables resources like the Secure Browser outside of policy hours, and some scenarios related to this were not completed.
    - The IBM Secure Browser is only available on mobile devices.

- Stolen credential scenarios using an enterprise endpoint or BYOD were completed successfully.
    - We were unable to invalidate MaaS360 certificates or duplicate MaaS360 certificates to another mobile device to complete some scenarios, including stolen credential scenarios and scenarios that require the endpoint to fail authentication. IBM Security MaaS360 does not detect a hostile request if all credentials are correct.
- Just-in-Time (JIT) Access Privileges – Users are allowed to request and elevate privileges required to perform a given task for a limited period.
    - Administrators can manually add/revoke these JIT access privileges for users.
    - JIT access privileges with automation were not tested and require integration with other zero trust tools that have the capabilities to manage access for users.
- Enterprise-ID Step-Up Authentication – The build did not include the capability to prompt for re-authentication in the middle of an active session with the chosen resources (e.g., GitLab).
- This build did not have the capability to verify resource compliance with policy.

Use Case C: Federated-ID Access – Out of scope for EIG run phase.

Use Case D: Other-ID Access – Results are the same as for use case B. Users with Other-ID Access (e.g., a contractor) have authorized access to resources based on need, so results for these users are no different than the results for users with Enterprise-ID Access.

Use Case E: Guest: No-ID Access – IBM considers Guest (No-ID) access out of scope for their products. Other technologies should be used to perform this function.

Use Case F: Confidence Level

Description: This use case demonstrates the ability of the enterprise to allow, prevent, or terminate sessions to resources based on the continuous evaluation of user and device risk.

- Users that fail re-authentication lose access to resources. With successful re-authentication, access is maintained.
    - Users that are not able to reauthenticate successfully to IBM Verify immediately lose access to resources.
- Requesting endpoint reauthentication failure during active session use case was not demonstrated.
    - Due to security of MaaS360 certificate storage, we were unable to invalidate the endpoint’s credentials to produce an unsuccessful endpoint authentication.
- Resource authentication is out of scope for IBM; other technologies should be used.
- Compliant devices maintain or regain access to resources. Noncompliant devices or users with noncompliant devices lose access to resources.

    - MaaS360 determines the compliance state of devices that it manages.
    - Devices lose access to resources and internet sites defined in policy once QRadar and CloudPak 4 Security are made aware of their noncompliant status.
    - Devices that return to a compliant state have their access restored.
- User sessions violating data use policies are blocked or terminated.
    - IBM Guardium Data Security was configured to alert QRadar of access to sensitive database tables and successfully terminated active sessions to a monitored database.
    - QRadar and CloudPak 4 Security were configured to remove previously authorized user access to authorized resources after receiving alerts from IBM Guardium Data Security.
- User access for accounts violating internet use policy was terminated and blocked.
    - On accessing a known bad URL with MaaS360 Secure Browser on a mobile device, access to GitLab was revoked via CloudPak for Security, and IBM Verify disabled the user's account.
- User sessions and devices attempting to access unauthorized resources or bad URLs were blocked or terminated.
    - IBM Verify was configured to alert QRadar of unauthorized access requests.
    - QRadar and CloudPak 4 Security were configured to remove previously authorized user access to authorized resources after receiving alerts from IBM Verify.
    - User's follow-up access requests for authorized resources were denied.
- ID denied/terminated access due to suspicious endpoint use case was not demonstrated.
    - IBM considers suspicious activity/network monitoring out of scope for their product. Other technologies should be used for this use case.

Use Case G: Service-Service Interactions – Out of scope for EIG run phase. IBM considers service-to-service use cases out of scope for their product. Other technologies should be used for this use case.

3.3 SDP and Microsegmentation Phase Summary Demonstration Results

This section lists the summary demonstration results for each of the builds that was implemented as part of the Software-Defined Perimeter (SDP) and Microsegmentation phase: E1B3, E2B3, E3B3, and E1B4. Only E1B3 and E1B4 have branch offices; E2B3 and E3B3 do not.

3.3.1 Enterprise 1 Build 3 (E1B3) Summary Demonstration Results

E1B3 is very similar to E1B2. They use the same products and technologies and have the same architecture, but are configured differently with respect to timouts and policies. Consequently, the results of use Cases A, B (1-6), C, D (1-6), and E were the same for build E1B3 as they were for E1B2. Summary results for other use cases demonstrated with E1B3 are as follows:

Use Case B: Enterprise-ID Access, Use Case D: Other-ID Access

Description: This use case demonstrates user access to enterprise resources based on successfully achieving user and device security preconditions.

- Just-in-Time Access Privileges – Users are allowed to request and elevate privileges required to perform a given task for a limited period.
    - A manual process was used to demonstrate providing users with additional privileges to resources.
    - Integration with other products can be used to automate just-in-time privileges. However, those products were not part of this build.
- Enterprise-ID Step-Up Authentication – Both Enterprise and Contractor Users are prompted for additional factor authentication when attempting to access sensitive resources.
    - Step-up authentication is available through an enhancement request to upgrade ZPA. However, this enhancement was not available during the time of this build.

Use Case F: Confidence Level

Description: This use case demonstrates the ability of the enterprise to allow, prevent, or terminate sessions to resources based on the continuous evaluation of user and device risk.

- Users successfully authenticate and reauthenticate to Zscaler. Once authenticated, access to resources is available based on policies.
    - Once the authentication time period expires, user cannot access resources. If reauthentication fails, the user loses access to resources.
- Resource authentication is out of scope for Zscaler; other technologies should be used to perform this function.
- Compliant devices maintain or regain access to resources. Noncompliant devices or users with noncompliant devices lose access to resources.
    - Zscaler checks endpoint compliance prior to allowing access. Endpoint compliance is checked periodically.
- This build was not used to demonstrate that user sessions violating data use policies are blocked or terminated because the tool that can provide this capability, Cloud Browser Isolation (CBI), was not available during the time of this build.
- User sessions and devices attempting to access malicious sites were blocked.

    - Internet use policy: ZIA policies denied access to malicious internet resources and ZIA displayed the access denied message on the browser.

- User sessions and devices attempting to access unauthorized resources were blocked.
    - Policies configured in ZPA and ZIA dictated what resources a user could access. User access to resources were evaluated on an individual basis based on ZIA and ZPA policies.
- This build was not used to demonstrate that an ID is denied/terminated access due to suspicious endpoint because the tool that can provide this capability, Zscaler Deception, was not available during the time of this build.

Use Case G: Service-to-Service Interactions

Description: This use case covers API calls between services and the ability of the policy engine to allow or deny calls to services based on properly assigned authorizations.

- Service-to-Service use cases were not demonstrated because the tool that can provide this capability, Zscaler for Workloads, was not available during the time of this build.

3.3.2 Enterprise 2 Build 3 (E2B3) Summary Demonstration Results

This build does not have IaaS, SaaS, or PaaS resources. Its summary results are as follows:

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

Description: This use case demonstrates the ability of the enterprise to discover network assets, authenticate devices, and demonstrate network connectivity.

- Discovery and authentication of endpoint assets were successfully demonstrated.
    - Resources and endpoints were discovered, authenticated, granted access to the network and, if applicable, limited to a specific subnet or resource set based on Cisco Identity Services Engine (ISE) policy. These policies were enforced by a Palo Alto NGFW, Cisco Switch, or Cisco Access Point.
    - Cisco Secure Workload (CSW) enforces resource access policies. CSW does not verify resource compliance.
- Reauthentication of identified assets was also successfully demonstrated using Cisco ISE policy configuration.
- Discovery of transaction flows – Demonstrated visibility of authentication and resource access attempts.
    - Cisco ISE captured sign-in logs to on-prem applications.
    - Logs for resources are provided by CSW.

    - IBM QRadar received logs from ISE as well as other components in the build.

Use Case B: Enterprise-ID Access, Use Case D: Other-ID Access

Description: This use case demonstrates user access to enterprise resources based on successfully achieving user and device security preconditions.

- For this build, we successfully demonstrated access using Windows, macOS, Linux, and mobile device iOS and Android endpoints.
- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to enterprise resources (on-prem) in accordance with policy via Cisco ISE and Ping Federate.
    - The policy engines can differentiate between employees and contractors and provide different access permissions to each user type.
    - Although Cisco ISE can be leveraged to deny-list URLs, Cisco recommends using a web filtering tool to control access to internet resources.
- Stolen credential using an enterprise endpoint or BYOD – Cisco ISE does not detect a hostile request if all credentials are correct.
- Just-in-Time Access Privileges – Users are allowed to request and elevate privileges required to perform a given task for a limited period.
    - Policies are updated within ISE to allow specific access.
- Enterprise-ID Step-Up Authentication – Both Enterprise and Contractor Users are prompted for additional factor authentication when attempting to access sensitive resources.
    - Cisco ISE does not provide an authentication mechanism to authenticate to the resource. However, a policy must be updated to allow the user and endpoint to reach the resource via the specific protocol that the resource is using. Therefore, we updated an ISE policy to allow that specific protocol for the user. The user then got reauthenticated and was allowed access.
- This build did not have the capability to verify resource compliance with policy. CSW information is not relayed to Cisco ISE.

Use case C: Federated-ID Access – Out of scope for this phase.

Use Case D: Other-ID Access – Results are the same as for use case B. Users with Other-ID Access (e.g., a contractor) have authorized access to resources based on need, so results for these users are no different than the results for users with Enterprise-ID Access.

Use Case E: Guest: No-ID Access – Access to the internet is allowed for all guest users.

Use Case F: Confidence Level

Description: This use case demonstrates the ability of the enterprise to allow, prevent, or terminate sessions to resources based on the continuous evaluation of user and device risk.

- Users or devices that fail reauthentication lose access to resources. With successful reauthentication, access is maintained.
  - Devices that are not able to reauthenticate successfully to Cisco ISE will immediately lose access to resources.
  - Initial authentication with Cisco ISE provides user with access to resources per ISE policy. Periodic reauthentication is required, which verifies compliance as well.
- Resource authentication was not demonstrated. Currently, CSW does not provide information to Cisco ISE.
- Compliant devices maintain or regain access to resources. Noncompliant devices or users with noncompliant devices lose access to resources.
  - Upon login to endpoint device, compliance information is sent to the Cisco ISE and validated before the endpoint gains access to the network. Device compliance is checked periodically.
  - Devices lose access to resources once the Cisco ISE is made aware of a noncompliant state.
- Cisco Secure Network Analytics (SNA) was leveraged to create policies to monitor violations of data use. Cisco Secure Endpoint also informed ISE of threats to the endpoints.
  - Information from SNA was relayed to Cisco ISE to revoke user access.
- Cisco SNA has native policies to detect malicious traffic such as command and control, Tor, bogon sites, etc. Specific URLs can be blocked, but Cisco recommends using a web filtering tool instead of SNA or ISE.
  - User sessions and devices attempting to access unauthorized resources were blocked by Cisco ISE once the access attempt information was detected by SNA and relayed to ISE.
- Enterprise can deny access to resources when users are attempting access from suspicious endpoints.
  - SNA policies were able to detect suspicious activities by endpoints. That information was passed to Cisco ISE, which quarantined the endpoint.

Use Case G: Service-to-Service Interactions

Description: This use case covers API calls between services and the ability of the policy engine to allow or deny calls to services based on properly assigned authorizations.

- Cisco CSW agents were deployed on resources and policies were applied to the resource to allow or deny API calls. A resource without the right authorizations to communicate with another resource was denied.

- CSW continuously monitors the communications in and out of a subject and develops policies based on that information.
- Service-to-endpoint communications were demonstrated by using the CSW agents on resources.
- Communication was successful by applying policy to allow access from the service to the endpoint.

3.3.3 Enterprise 3 Build 3 (E3B3) Summary Demonstration Results

A summary of this build's results are as follows:

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

Description: This use case demonstrates the ability of the enterprise to discover network assets, authenticate devices, and demonstrate network connectivity.

- Discovery and authentication of endpoint assets were successfully demonstrated. Resources and endpoints were granted access to the network and if applicable, limited to a specific subnet or resource set based on Forescout policy. These policies were enforced by a Palo Alto NGFW and Cisco Switch. Due to the location of these PEPs, unauthenticated endpoints were restricted to the local subnet in accordance with Forescout policy.
    - Network assets were discovered by Forescout via both passive and active detection.
- Reauthentication of identified assets was also successfully demonstrated using Forescout and Microsoft Intune.
- Discovery of transaction flows – Demonstrated visibility of authentication and resource access attempts.
    - Azure AD captures sign-in logs to SaaS applications, PaaS, IaaS resources, and on-prem applications.
    - Azure AD audit logs are captured that show activity including changes to cloud resources in the Azure tenant.
    - Forescout captures sign-in and audit logs and network traffic for on-premises components.

Use Case B: Enterprise-ID Access, Use Case D: Other-ID Access

Description: This use case demonstrates user access to enterprise resources based on successfully achieving user and device security preconditions.

- For this build, we successfully demonstrated access using Windows, macOS, and mobile device iOS and Android endpoints.
- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to enterprise resources (on-prem and cloud) in accordance with policy via Azure AD Conditional Access.

    - The policy engine can differentiate between employees and contractors and provide different access permissions to each user type.
  - Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, are allowed or denied access to internet resources (on-prem and cloud) in accordance with policy via Defender for Cloud Apps and Defender for Endpoint.
    - Policies within Defender for Cloud Apps were set up to allow, block, or limit access to resources.
    - The build demonstrated that documents with sensitive data such as credit cards could be viewed but not downloaded.
  - Stolen credential using an enterprise endpoint or BYOD – Azure AD does not detect a hostile request if all credentials are correct.
  - Just-in-Time (JIT) Access Privileges – Users are allowed to request and elevate privileges required to perform a given task for a limited period.
    - JIT for VM Access
      - Azure has a just-in-time feature capability for VM access that enables a user to access an Azure VM with SSH or RDP for a limited time when requested.
      - Defender for Cloud checks that the user has the appropriate Azure role, then inserts allow rules from a specific user’s IP address into the network security groups and Azure Firewall.
      - This only occurs at the time that the user requests access to the VMs.
    - JIT with Privileged Identity Management (PIM)
      - PIM is used to provide an additional layer of authentication and authorization before requesting users are granted access to privileged Azure AD roles for a limited time.
      - Once granted, a user gains elevated Azure AD administration privileges for a limited time.
      - For this build, PIM only works within the Azure environment and does not extend to the on-prem infrastructure.
  - Enterprise-ID Step-Up Authentication – Both Enterprise and Contractor Users are prompted for additional factor authentication when attempting to access sensitive resources.
    - Azure AD Conditional Access provides additional authentication when a user attempts to access a portion of a site or a document with a sensitive label.
    - An example of a sensitive site is a SharePoint site with a sensitive label.
    - Conditional Access would prompt the user for additional authentication prior to allowing access.

- This build did not have the capability to verify chosen resource (e.g., GitLab) compliance with policy.

Use Case C: Federated-ID Access – Out of scope for this phase.

Use Case D: Other-ID Access – Results are the same as for use case B. Users with Other-ID Access (e.g., a contractor) have authorized access to resources based on need, so results for these users are no different than the results for users with Enterprise-ID Access.

Use Case E: Guest: No-ID Access

Description: This use case demonstrates the ability of the enterprise to allow unmanaged guest devices to have access to public Internet resources.

- Forescout was able to provide Internet access to unauthenticated guest devices connecting to a segmented portion of the enterprise network.

Use Case F: Confidence Level

Description: This use case demonstrates the ability of the enterprise to allow, prevent, or terminate sessions to resources based on the continuous evaluation of user and device risk.

- Users or devices that fail reauthentication lose access to resources. With successful re-authentication, access is maintained.
    - Devices that are not able to reauthenticate successfully to Microsoft Intune Mobile Device Management (MDM) will be offboarded and immediately lose access to resources. Periodic reauthentication is required.
    - Azure AD Conditional Access was configured to only allow connections from Intune compliant devices.
- Resource authentication was not demonstrated. It could not be performed by the products in this build.
- Compliant devices maintain or regain access to resources. Noncompliant devices or users with noncompliant devices lose access to resources.
    - Microsoft Intune determines, and then reports to Azure AD, the compliance state of devices that it manages. Endpoint compliance must be validated prior to allowing access. Endpoint compliance is checked periodically.
    - Devices lose access to resources once Azure AD is made aware of a noncompliant state.
- The ability to monitor and detect violations of data use policies was not demonstrated due to time limitations.
- User sessions and devices attempting to access unauthorized resources and malicious sites were blocked or the sessions were terminated.

    - Defender for Cloud Apps was configured to label sites as trusted or untrusted.
    - If a site was untrusted, Defender for Endpoint enforced Defender for Cloud Apps Policy and prevented the user from visiting the site by blocking it.
    - Additionally, Azure AD Conditional Access was configured to block users from accessing resources without proper authorization.
    - Microsoft Sentinel was successfully configured to send API requests to Azure AD to terminate active sessions and disable user accounts when alerts indicating malicious events (e.g., attempts to access known bad internet sites) were received. Session termination was successfully tested for Office SaaS apps.
    - The build did not have the capability to terminate sessions for the chosen on-premises/IaaS resource (e.g., GitLab).
- Enterprise can detect malicious behavior on enterprise endpoints and BYOD but not on unmanaged endpoints.
    - Defender for Endpoint was configured as the Endpoint Detection and Response solution to detect and block threats and inform Azure AD via Intune.
    - Defender for Endpoint has built-in sensors in the Windows platform and utilizes Windows Defender Firewall and Windows Anti-Virus to detect threats.
- Enterprise can deny access to resources when users are accessing from suspicious endpoints.
    - Once onboarded, devices with Defender for Endpoint detected threats that included malicious script execution, network reconnaissance, and Active Directory reconnaissance.
    - Defender for Endpoint categorized the threats, forwarded the alerts to Microsoft 365 Defender, and forwarded the risk information to Intune.
    - Depending on the risk threshold set, Microsoft Intune changed the endpoint status to noncompliant.
    - Azure AD received the noncompliant status information and blocked the devices from accessing resources.

Use Case G: Service-Service Interactions

Description: This use case covers API calls between services and the ability of the policy engine to allow or deny calls to services based on properly assigned authorizations.

- Client apps were able to utilize either Azure roles or Azure AD authorizations to make successful API calls to Azure IaaS, PaaS, and Microsoft SaaS apps. Client apps without the right authorizations were denied.

    - Client applications made API calls to manage an Azure VM, retrieve data managed by Azure AD, and retrieve data from Office365 mail and Microsoft Sentinel.
    - Client apps without the right API permissions were denied.
- Client apps hosted in Azure IaaS or Azure PaaS were able to make successful API calls to Azure IaaS, Azure PaaS, and Microsoft SaaS apps. Apps without the right authorizations were denied.
    - A client application hosted/stored in an Azure VM or an Azure function was used to make successful API calls to manage an Azure VM, retrieve Azure AD-managed data, and retrieve data from Microsoft Sentinel and Office365 mail.
- Client applications were not able to make API calls to the chosen on-prem/IaaS application (e.g., GitLab) because the API authorization was issued by an external authorization provider.
- For Service to Endpoint use cases:
    - Intune was used to instruct the endpoint to take certain actions, such as to update itself and restart.

3.3.4 Enterprise 1 Build 4 (E1B4) Summary Demonstration Results

This build does not have SaaS resources. Its summary results are as follows:

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

Description: This use case demonstrates the ability of the enterprise to discover network assets, authenticate devices, and demonstrate network connectivity.

- Discovery and authentication of endpoint assets
    - Appgate does not discover network assets. Endpoints must have an Appgate agent on them in order to communicate with the Appgate controller and be authenticated by it.
- Reauthentication of identified assets – Appgate requires reauthentication after a certain period of time.
    - User must reauthenticate once the authentication period is over. If reauthentication fails, the user does not have access to any resources.
- Discovery of transaction flows – Demonstrated visibility of authentication and resource access attempts.
    - Appgate captures sign-in and traffic flow logs to on-prem and IaaS resources.
    - Appgate logs are sent to IBM QRadar.

Use Case B: Enterprise-ID Access, Use Case D: Other-ID Access

Description: This use case demonstrates user access to enterprise resources based on successfully achieving user and device security preconditions.

- For this build, we successfully demonstrated access using Windows, macOS, Linux, and mobile device iOS and Android endpoints.
- Both Enterprise and Contractor Users on an enterprise endpoint or BYOD, on-prem or remote, were allowed or denied access to enterprise resources (on-prem and cloud) in accordance with policies enforced by the Appgate Gateway. Policies were configured with the Appgate controller.
    - The policy engine can differentiate between employees and contractors and provide different access permissions to each user type.
    - Appgate gateways were deployed on-prem and in the AWS IaaS cloud to protect resources.
    - Compliance of both the endpoint and resource were checked prior to allowing a user to access that resource.
- Appgate does not manage access to internet resources and suggests leveraging a web filtering tool to manage internet access.
- Stolen credential using an enterprise endpoint or BYOD – Appgate does not detect a hostile request if all credentials are correct.
    - Appgate can limit the location (by city, state, or country) and number of simultaneous logins by a user to prevent stolen credentials.
- Just-in-Time Access Privileges – Users are allowed to request and elevate privileges required to perform a given task for a limited period.
    - A manual process was used to demonstrate providing users with additional privileges to resources.
    - Integration with other products can be used to automate just-in-time privileges. However, those products were not part of this build.
- Enterprise-ID Step-Up Authentication – Both Enterprise and Contractor Users were prompted for additional factor authentication when attempting to access sensitive resources.
    - A policy was created within the Appgate Controller to require additional authentication to specific resources that are considered sensitive and need additional protection.

Use Case C: Federated-ID Access – Out of scope for this phase.

Use Case D: Other-ID Access – Results are the same as for use case B. Users with Other-ID Access (e.g., a contractor) have authorized access to resources based on need, so results for these users are no different than the results for users with Enterprise-ID Access.

Use Case E: Guest: No-ID Access – Appgate SDP considers this out of scope for their products. Other technologies should be used to perform guest access enforcement.

Use Case F: Confidence Level

Description: This use case demonstrates the ability of the enterprise to allow, prevent, or terminate sessions to resources based on the continuous evaluation of user and device risk.

- Users or devices that fail reauthentication lose access to resources. With successful reauthentication, access is maintained.
    - Devices that are not able to reauthenticate successfully to the Appgate controller will immediately lose access to resources.
    - Initial authentication with Appgate controller provides user with access to resources assigned to that user. Periodic reauthentication is required, which verifies compliance as well.
- Resource reauthentication failed during an active session.
    - Once Appgate's headless client is authenticated, it periodically reauthenticates automatically using PKI or stored credentials. Compliance checks are also performed periodically per policy. If compliance fails on the resource, a user will lose access within five minutes to the resource. If compliance fails on the endpoint, the user will lose access to all resources.
    - Compliant devices maintain or regain access to resources. Noncompliant devices or users with noncompliant devices lose access to resources.
    - Upon login to the Appgate client, compliance information is sent to the Appgate controller and validated before the user can access any resources. Device compliance is checked every five minutes.
    - Devices lose access to resources once the Appgate controller is made aware of a noncompliant state.
- The ability to monitor and detect violations of data use policies was not demonstrated. Appgate does not have capabilities to manage data use policies.
- User sessions and devices attempting to access unauthorized resources are blocked.
    - Appgate policies dictate if a user has access to a resource or not. If there is no policy to allow a user to access a resource and the user requests to reach that resource, the request will not be able to leave the end device or it will be denied by the Appgate gateway. Appgate will not terminate an active session but it will block access to the unauthorized resource.
    - Appgate does not control access to internet websites and recommends leveraging a web filtering tool to perform this function.
- Enterprise can deny access to resources when users are accessing from suspicious endpoints.
    - Appgate does not allow any traffic past the Appgate gateway if there is no policy to allow that specific access from the user. Logs of these attempts are provided to the SIEM. Note:

    - The SIEM can trigger a security event, which Appgate can consume to further restrict that user's access by deeming the user riskier.

Use Case G: Service-Service Interactions

Description: This use case covers API calls between services and the ability of the policy engine to allow or deny calls to services based on properly assigned authorizations.

- Appgate headless clients are deployed on resources to make successful API calls to other resources (e.g., GitLab). A resource without the correct authorizations to communicate with another resource was denied.
    - Headless clients were deployed to on-prem and AWS resources to validate successful service-to-service communications.
    - Use cases for on-prem and AWS IaaS and PaaS were successfully performed.
    - A SaaS solution was not available for this build.
- Service-to-service communication between resources located on separate containers was successfully performed.
    - A Kubernetes cluster was deployed with Appgate sidecar, which enforced policies applied at the namespace level.
- Service-to-endpoint communications were demonstrated using headless clients installed on resources.
    - Communication was successful by applying policy to allow access from service to the endpoint.

Appendix A List of Acronyms

AD	Active Directory
API	Application Programming Interface
BYOD	Bring Your Own Device
CASB	Cloud Access Security Broker
CBI	Cloud Browser Isolation
CRADA	Cooperative Research and Development Agreement
CSW	Cisco Secure Workload
DNS	Domain Name System
E1B1	Enterprise 1 Build 1
E1B2	Enterprise 1 Build 2
E1B3	Enterprise 1 Build 3
E1B4	Enterprise 1 Build 4
E2B1	Enterprise 2 Build 1
E2B3	Enterprise 2 Build 3
E3B1	Enterprise 3 Build 1
E3B2	Enterprise 3 Build 2
E3B3	Enterprise 3 Build 3
E4B3	Enterprise 4 Build 3
EIG	Enhanced Identity Governance
EP	Enterprise Endpoint
EPP	Endpoint Protection Platform
IaaS	Infrastructure as a Service
ICAM	Identity, Credential, and Access Management
IP	Internet Protocol
ISE	(Cisco) Identity Services Engine

IT	Information Technology
ITL	Information Technology Laboratory
JIT	Just-in-Time
MDM	Mobile Device Management
MFA	Multifactor Authentication
MSV	Mandiant Security Validation
NCCoE	National Cybersecurity Center of Excellence
NGFW	Next-Generation Firewall
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
OS	Operating System
PaaS	Platform as a Service
PEP	Policy Enforcement Point
PIM	Privileged Identity Management
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RDP	Remote Desktop Protocol
RSS	Enterprise Resource
SaaS	Software as a Service
SDP	Software-Defined Perimeter
SIEM	Security Information and Event Management
SNA	(Cisco) Secure Network Analytics
SP	Special Publication
SWG	Secure Web Gateway
UEM	Unified Endpoint Management
UP	User Profile

URL	Uniform Resource Locator
VM	Virtual Machine
VPN	Virtual Private Network
ZCC	Zscaler Client Connector
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access
ZTA	Zero Trust Architecture

Appendix B References

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, *Zero Trust Architecture,* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Gaithersburg, Md., August 2020, 50 pp. Available: https://doi.org/10.6028/NIST.SP.800-207.

[2] P. Grassi, M. Garcia, and J. Fenton, *Digital Identity Guidelines,* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, Gaithersburg, Md., June 2017, 75 pp. Available: https://doi.org/10.6028/NIST.SP.800-63-3.

[3] "National Cybersecurity Center of Excellence (NCCoE) Zero Trust Cybersecurity: Implementing a Zero Trust Architecture," Federal Register Vol. 85, No. 204, October 21, 2020, pp. 66936-66939. Available: https://www.federalregister.gov/documents/2020/10/21/2020-23292/national-cybersecurity-center-of-excellence-nccoe-zero-trust-cybersecurity-implementing-a-zero-trust.

Appendix C EIG Crawl Phase Demonstration Results

This appendix lists the full demonstration results for each of the builds that was implemented as part of the EIG crawl phase: E1B1, E2B1, and E3B1.

C.1 Enterprise 1 Build 1 (E1B1) Detailed Demonstration Results

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

Table C-1 Detailed 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.

Demo ID	Expected Outcome	Observed Outcome	Comments
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.
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 RSS2 is based on endpoint compliance. However, we cannot validate compliance of RSS2.
B-1.1.c, B-1.2.c, B-1.3.c, B-4.1.c, B-4.2.c, B-4.3.c, D-1.1.c, D-1.2.c, D-	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

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

Demo ID	Expected Outcome	Observed Outcome	Comments
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 noncompliant.
B-1.1.n-p, B-1.2.n-p, B-1.3.n-p, B-4.1.n-p, B-4.2.n-p, B-4.3.n-p, D-1.1.n-p, D-1.2.n-p, D-1.3.n-p, D-4.1.n-p, D-4.2.n-p, D-4.3.n-p	N/A	N/A	Demonstration cannot be run. Unable to perform compliance checks on RSS.
B-1.2.a-p			The results are the same as B-1.1 since network policies allow access from branch to Ent1. See results from B-1.1.
B-1.3.a-p			The results are the same as B-1.1 given that network policies allow the user/device to access the enterprise remotely using a VPN connection. See results from B-1.1.
B-1.4.a-p, B-1.5.a-p, B-1.6.a-p, B-4.4.a-p, B-4.5.a-q, and B-4.6.a-p	N/A	N/A	Cloud-based resources are out of scope until run phase.
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.

Demo ID	Expected Outcome	Observed Outcome	Comments
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 Unified Endpoint Management (UEM) agent and Okta Verify App. See results from B-1.1 for B-4.1, B-4.2, and B-4.3.
All C Use Cases	N/A	N/A	Demonstrations cannot be performed. Currently, no federation configuration has been set up between Ent1, Ent2, and Ent3.
All D Use Cases			As documented in the rows above, the results of all D use case demonstrations are the same as the results of the B use cases. Note that the user is a contractor and will have access to resources based on need. The Ivanti Neurons for UEM agent and Okta Verify App will have to be installed on the contractor's device, whether it's provided by the enterprise or BYOD.
All E Use Cases	N/A	N/A	Guest (No-ID) access is considered out of scope for the EIG crawl phase.
All F Use Cases	N/A	N/A	Confidence level use cases are considered out of scope for the EIG crawl phase.

C.2 Enterprise 2 Build 1 (E2B1) Detailed Demonstration Results

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

1971 **Table C-2 Detailed Demonstration Results for E2B1 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, A-1.3.a-f	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build.
A-1.4.a-g	N/A	N/A	Cloud-based resources are out of scope until the run phase.
A-2.1.a-i	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build. There is no tool that can reauthenticate any entity (RSS, EP, BYOD, or guest device) and terminate its network access based on authentication status.
A-2.2.a-I, A-2.3.a-f	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build based on reauthentication status.
A-2.4.a-f	N/A	N/A	Cloud-based resources are out of scope until the run phase.
A-3.1.a, A-3.3.a, A-3.5.a	User request and action is recorded	User login to an application is logged	Success: Both Ping Federate and Duo record the authentication logs. Administrators can 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: Ping Federate and Duo logs have relevant information about the authentication between the user and resource.
A-3.2.a-b, A-3.4.a-b, A-3.6.a	N/A	N/A	Cloud-based resources are out of scope until the run phase.
B-1.1.a, B-1.2.a, B-1.3.a, B-4.1.a, B-	Access Successful	Access Successful	Partial success: User access to resource RSS1 is based on endpoint compliance. Users must have

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

Demo ID	Expected Outcome	Observed Outcome	Comments
1.3.g, D-4.1.g, D-4.2.g, D-4.3.g			the user forgets the login password on the mobile device.
B-1.1.h, B-1.2.h, B-1.3.h, B-4.1.h, B-4.2.h, B-4.3.h, D-1.1.h, D-1.2.h, D-1.3.h, D-4.1.h, D-4.2.h, D-4.3.h	Access Successful	Access Successful	Success: GitLab session timeout is set to one minute for demonstration purposes. After session timed out, user was reauthenticated.
B-1.1.i, B-1.2.i, B-1.3.i, B-4.1.i, B-4.2.i, B-4.3.i, D-1.1.i, D-1.2.i, D-1.3.i, D-4.1.i, D-4.2.i, D-4.3.i	Access Not Successful	Access Not Successful	Success: Only way to do this is to put in a wrong password for failure.
B-1.1.j, B-1.2.j, B-1.3.j, B-4.1.j, B-4.2.j, B-4.3.j, D-1.1.j, D-1.2.j, D-1.3.j, D-4.1.j, D-4.2.j, D-4.3.j	Access Not Successful	Access Not Successful	Success: On Duo, implemented a block on devices that do not have firewall enabled. After GitLab timed out, we turned off the firewall on the device and reauthentication was unsuccessful.
B-1.1.k, B-1.2.k, B-1.3.k, B-4.1.k, B-4.2.k, B-4.3.k, D-1.1.k, D-1.2.k, D-1.3.k, D-4.1.k, D-4.2.k, D-4.3.k	Access Limited	N/A	Partial success: Access to RSS2 is blocked if EP is not compliant. Currently cannot perform limited access.
B-1.1.l-m, B-1.2.l-m, B-1.3.l-m, B-4.1.l-m, B-4.2.l-m, B-4.3.l-m, D-1.1.l-m, D-1.2.l-m, D-1.3.l-m, D-4.1.l-m, D-4.2.l-m, D-4.3.l-m	Access Denied	Access Denied	Success: User was denied access because the endpoint was noncompliant.
B-1.1.n-p, B-1.2.n-p, B-1.3.n-p, B-4.1.n-p, B-4.2.n-p, B-4.3.n-p, D-1.1.n-p, D-1.2.n-p, D-1.3.n-p, D-4.1.n-p, D-4.2.n-p, D-4.3.n-p	N/A	N/A	Demonstration cannot be run. Unable to perform compliance checks on RSS.
B-1.2.a-p			The results are the same as B-1.1 since network policies allow access from a branch office to Ent2.

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

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

C.3 Enterprise 3 Build 1 (E3B1) Detailed Demonstration Results

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

Table C-3 Detailed 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	Access Successful	Partial Success: Authenticated user access to RSS2 successful. Can only partially demonstrate because cannot validate compliance on RSS2.
B-1.1.c	Access Not Successful	Access Not Successful	Partial Success: User authentication failure prevents access. Cannot validate compliance on RSS1. Partial demonstration completed with user not able to authenticate.
B-1.1.d	Access Not Successful	Access Not Successful	Partial Success: Based on configuration in Ent 3, the E2 is not authorized to access RSS1 based on enterprise governance policy. Also, RSS compliance cannot be demonstrated in this phase. In this case, user is not granted access to RSS1.
B-1.1.e	Access Successful	Access Successful	Partial Success: Authenticated user access to RSS2 successful. Can partially demonstrate. Cannot validate compliance on RSS2.
B-1.1.f	Access Not Successful	Access Not Successful	Success: User authentication failure prevents access.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1.g	Access Not Successful	Access Not Successful	Success: User authentication failure prevents access.
B-1.1.h	Access Successful	Access Successful	Partial Success: GitLab session timeout is set to one minute for demonstration purposes. After session timed out, user was re-authenticated. Can only partially demonstrate because cannot validate RSS1 compliance.
B-1.1.i	Access Not Successful	Access Not Successful	Success: Unauthenticated users were prevented from accessing resources.
B-1.1.j	Access Not Successful	Access Not Successful	Partial Success: Authenticated user access to RSS1 successful. Can partially demonstrate. Cannot validate compliance on RSS1. After GitLab timed out, reauthentication 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 noncompliance.
B-1.1.l-p	N/A	N/A	Cannot demonstrate. Unable to perform compliance checks on RSS.
B-1.2.a-p	N/A	N/A	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	N/A	N/A	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.

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

Appendix D EIG Run Phase Demonstration Results

This appendix lists the full demonstration results for each of the builds that was implemented as part of the EIG run phase: E1B2, E3B2, and E4B3.

D.1 Enterprise 1 Build 2 (E1B2) Detailed Demonstration Results

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

Table D-1 Detailed Demonstration Results for E1B2 EIG Crawl Phase

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.a-m	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build. Zscaler uses the client connector to allow a user on a device to access specific resources only, whether on-prem or remote. Users cannot readily access resources in the enterprise (or network) if they do not have permissions to access them. Resources are not authenticated or checked for compliance in this phase.
A-1.2.a-m, A-1.3.a-f, A-1.4.a-g	N/A	N/A	Same as in A-1. Demonstration cannot be completed. There is no network-level enforcement present in this build.
A-2.1.a-I, A-2.2.a-I, A-2.3.a-f, A-2.4.a-f	N/A	N/A	Same as in A-1. Demonstration cannot be completed. There is no network-level enforcement present in this build.
A-3.1.a, A-3.3.a, A-3.5.a	User request and action is recorded	User login to an 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. Zscaler Private Access (ZPA) records relevant information about the connection between the endpoint and resource.
A-3.1.b, A-3.3.b	API call is recorded	Logs contain	Success: Okta records the authentication logs. Administrators can log in to Okta and view logs of

Demo ID	Expected Outcome	Observed Outcome	Comments
		relevant API information	when a user logged onto an application and whether the authentication was successful or not. Zscaler ZPA records relevant information about the connection between the endpoint and resource.
A-3.2.a, A-3.4.a, A-3.6.a	User request and action is recorded	User login to an 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. Zscaler ZPA records relevant information about the connection between the endpoint and resource.
A-3.2.b, A-3.4.b, A-3.6.a	API call is recorded	Logs contain relevant API information	Success: Okta records the authentication logs. Administrators can log in to Okta and view logs of when a user logged onto an application and whether the authentication was successful or not. Zscaler ZPA records relevant information about the connection between the endpoint and resource.
B-1.1.a, B-1.2.a, B-1.3.a, B-4.1.a, B-4.2.a, B-4.3.a, D-1.1.a, D-1.2.a, D-1.3.a, D-4.1.a, D-4.2.a, D-4.3.a	Access Successful	Access Successful	Partial success: User is authenticated via Okta when accessing the resource. User logs into Zscaler client connector as part of login process to the endpoint and policies are applied to the user/endpoint (including laptops, workstations, and mobile devices). User successfully connects to RSS1. However, we cannot validate compliance of RSS1.
B-1.1.b, B-1.2.b, B-1.3.b, B-4.1.b, B-4.2.b, B-4.3.b, D-1.1.b, D-1.2.b, D-1.3.b, D-4.1.b, D-4.2.b, D-4.3.b	Access Successful	Access Successful	Partial success: User is authenticated via Okta when accessing the resource. User logs into Zscaler client connector as part of login process to the endpoint and policies are applied to the user/endpoint (including laptops, workstations, and mobile devices). User successfully connects to RSS1. However, we cannot validate compliance of RSS1.
B-1.1.c, B-1.2.c, B-1.3.c, B-4.1.c, B-4.2.c, B-4.3.c, D-1.1.c, D-1.2.c, D-1.3.c, D-4.1.c, D-4.2.c, D-4.3.c	Access Not Successful	Access Not Successful	Success: Demonstration completed with user not able to log in to resource.

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

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1.j, B-1.2.j, B-1.3.j, B-4.1.j, B-4.2.j, B-4.3.j, D-1.1.j, D-1.2.j, D-1.3.j, D-4.1.j, D-4.2.j, D-4.3.j	Access Not Successful	Access Not Successful	Success: Device posture failure detected by ZPA, so access was denied.
B-1.1.k, B-1.2.k, B-1.3.k, B-4.1.k, B-4.2.k, B-4.3.k, D-1.1.k, D-1.2.k, D-1.3.k, D-4.1.k, D-4.2.k, D-4.3.k	Access Limited	N/A	Partial success: Access to RSS2 is blocked. Currently cannot perform limited access.
B-1.1.l-m, B-1.2.l-m, B-1.3.l-m, B-4.1.l-m, B-4.2.l-m, B-4.3.l-m, D-1.1.l-m, D-1.2.l-m, D-1.3.l-m, D-4.1.l-m, D-4.2.l-m, D-4.3.l-m	Access Denied	Access Denied	Success: User was denied access because the endpoint was noncompliant. Device posture failure detected by ZPA.
B-1.1.n-p, B-1.2.n-p, B-1.3.n-p, B-4.1.n-p, B-4.2.n-p, B-4.3.n-p, D-1.1.n-p, D-1.2.n-p, D-1.3.n-p, D-4.1.n-p, D-4.2.n-p, D-4.3.n-p	N/A	N/A	Demonstration cannot be run. Unable to perform compliance checks on RSS.
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 ZPA policies allow the user/device to access the enterprise remotely the same way that user/device would access a resource within the enterprise. See results from B-1.1.
B-1.4.a-p, B-1.5.a-p, B-1.6.a-p, B-4.4.a-p, B-4.5.a-q, and B-4.6.a-p			Access to cloud-based resources (RSS1 and RSS2) are the same as on-prem. See results from B-1.1.
B-2.1.a-d, B-2.2.a-d, B-2.3.a-d, B-5	Access Successful	Access Successful	Success: Employee is granted access to URL1 and URL2 regardless of hourly access time because

Demo ID	Expected Outcome	Observed Outcome	Comments
			employees have full access to both URLs at all times per ZScaler policy.
B-2.1.e, B-2.2.e, B-2.3.e	Access Not Successful	Access Not Successful	Success: The only way the user is not authenticated is if the user inputs the incorrect password or does not have a second factor during Zscaler Client Connector (ZCC) login. With incorrect 1st or 2nd factor, ZCC will fail to connect with ZIA and will not be able to access the internet.
B-2.1.f, B-2.2.f, B-2.3.f	Access Not Successful	Access Not Successful	Success: Contractor is blocked from URL1 as expected per Zscaler policy.
B-2.1.g, B-2.2.g, B-2.3.g	Access Successful	Access Successful	Success: Contractor is granted access to URL2 as expected per Zscaler policy.
B-2.1.h-I, B-2.2.h-I, B-2.3.h-i	Access Not Successful	Access Not Successful	Success: Contractor is blocked from accessing URL1 due to failed authentication.
B-2.1.j, B-2.2.j, B-2.3.j	Access Not Successful	Access Successful	The only way the user is not authenticated is if the user inputs the incorrect password or does not have a second factor during ZCC login. Access is successful because internet access is required for ZIA to function. If not authenticated to ZIA, internet access is unrestricted unless blocked by company firewall.
B-2.1.k, B-2.2.k, B-2.3.k	Access Successful	Access Successful	Success: Employee is granted access after successful reauthentication per Zscaler policy as expected.
B-2.1.l, B-2.2.l, B-2.3.l	Access Not Successful	Access Not Successful	Success: Employee cannot access URL1 or URL2 after reauthentication to Zscaler fails as expected.
B-2.1.m-p, B-2.2.m-p, B-2.3.m-p	N/A	N/A	Demonstration cannot be completed. ZIA does not perform device posture/compliance checks on endpoints without integration of a third-party EPP product.
B-3.1.a, B-3.4.a, B-3.5.a	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.
B-3.1.b, B-3.4.b, B-3.5.b	Real Req Fail	Real Req Fail	Success: Incorrect credentials were entered, and the Real Request failed as expected.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-3.1.c, B-3.4.c, B-3.5.c	Limit Access for Real Request, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.d, B-3.4.d, B-3.5.d	Real Request Keep Access, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.e, B-3.4.e, B-3.5.e	Hostile Request Successful	Hostile Request Successful	Success: Hostile Request successfully authenticated.
B-3.1.f, B-3.4.f, B-3.5.f	Hostile Request Unsuccessful	Hostile Request Unsuccessful	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.g, B-3.4.g, B-3.5.g	Real Request Fail, Hostile Request Access Limited	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.h, B-3.4.h, B-3.5.h	Real Request Fail, Hostile Request remains authenticated	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.

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

Demo ID	Expected Outcome	Observed Outcome	Comments
			contractor and will have access to resources based on need. The Ivanti Neurons for UEM agent and Okta Verify App will have to be installed on the contractor's device, whether it's provided by the enterprise or BYOD.
E-1.1.a, E-1.2.a	Success	Success	Success: User/device is recognized by Zscaler Internet Access (ZIA) as unmanaged and given access to the internet. Per ZIA enterprise policies, resources on the internet that are deemed safe for access are reachable by the user with No-ID, which includes a public resource from Enterprise 1.
E-1.1.b, E-1.2.b	Success	Success	Success: User/device is recognized by ZIA as unmanaged and given access to the internet. Per ZIA enterprise policies, resources on the internet that are deemed safe for access are reachable by the user with No-ID.
All F Use Cases	N/A	N/A	Test cannot be completed without third-party integration with an endpoint protection platform (EPP).

D.2 Enterprise 3 Build 2 (E3B2) Detailed Demonstration Results

Table D-2 lists the full demonstration results for all EIG run phase demonstrations run in Enterprise 3 Build 2 (E3B2). In all demonstrations that we attempted to conduct, the ZTA functionality included in the build performed as expected. The technology deployed in E3B2 was able to determine endpoint compliance for Windows, macOS, and mobile devices and prevent noncompliant endpoints from accessing private resources.

Table D-2 Detailed Demonstration Results for E3B2 EIG Run Phase

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.a-d	Access to Network	Access to Network	Success: Resource has access to network in accordance with Forescout policy.
A-1.1.b, A-1.1.c, A-1.1.g	No Access to Network	No Access to Network	Partial success: In the current configuration, the endpoint has access limited to the local subnet in accordance with Forescout policy.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.d	No Access to Network	N/A	Demonstration cannot be completed. By Scenario A-1 definition, a resource has already undergone onboarding.
A-1.1.e	Access to Network	Access to Network	Success: Endpoint has access to network in accordance with Forescout policy.
A-1.1.f	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-1.1.h	Access to Public Network	N/A	Demonstration cannot be completed. By Scenario A-1 definition, an endpoint has already undergone onboarding.
A-1.1.i	Access to Network	Access to Network	Success: BYOD has access to network in accordance with Forescout policy.
A-1.1.j	Limited Access to Network	Limited Access to Network	Success: Endpoint has access limited to the local subnet in accordance with Forescout policy.
A-1.1.k	No Access to Network	No Access to Network	Partial success: In the current configuration, the endpoint has access limited to the local subnet in accordance with Forescout policy.
A-1.1.l	Access to Public Network	N/A	Demonstration cannot be completed. By Scenario A-1 definition, the BYOD has already undergone onboarding.
A-1.1.m	Access to Public Network	Access to Public Network	Success: BYOD has access to network in accordance with Forescout policy.
A-1.2.a-m	Access to Network	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
A-1.3.a	Access to Network	Access to Network	Success: Endpoint has access to network in accordance with Forescout policy.
A-1.3.b	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.3.c	No Access to Network	No Access to Network	Success: Endpoint is denied access to the network after failing to authenticate to the GlobalProtect VPN.
A-1.3.d	Access to Network	Access to Network	Success: BYOD has access to network in accordance with Forescout policy.
A-1.3.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-1.3.f	No Access to Network	No Access to Network	Success: BYOD is denied access to the network after failing to authenticate to the GlobalProtect VPN.
A-1.4.a-g	N/A	N/A	Partial Success: Using Azure roles, a user could be allowed, denied, or provided with limited access to cloud resources. With Azure AD Conditional Access and Microsoft Intune, a device can be given access to a cloud application.
A-2.1.a	Keep Access to Network	Keep Access to Network	Success: Resource has access to network in accordance with Forescout policy.
A-2.1.b	Terminate Access to Network	Limit Access to Network	Partial Success: Resource has access limited to the local subnet in accordance with Forescout policy.
A-2.1.c	Terminate Access to Network	Limit Access to Network	Partial Success: Resource has access limited to the local subnet in accordance with Forescout policy.
A-2.1.d	Keep Access to Network	Keep Access to Network	Success: Endpoint has access to network in accordance with Forescout policy.
A-2.1.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-2.1.f	Terminate Access to Network	Limit Access to Network	Partial Success: Resource has access limited to the local subnet in accordance with Forescout policy.
A-2.1.g	Keep Access to Network	Keep Access to Network	Success: BYOD has access to network in accordance with Forescout policy.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-2.1.h	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-2.1.i	Terminate Access to Network	Limit Access to Network	Partial success: BYOD has access limited to the local subnet in accordance with Forescout policy.
A-2.2.a-i	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
A-2.3.a	Keep Access to Network	Keep Access to Network	Success: Endpoint has access to network in accordance with Forescout policy.
A-2.3.b	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-2.3.c	Terminate Access to Network	Terminate Access to Network	Success: Endpoint has access terminated after failing to reauthenticate to the GlobalProtect VPN.
A-2.3.d	Keep Access to Network	Keep Access to Network	Success: BYOD has access to network in accordance with Forescout policy.
A-2.3.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: BYOD has access limited in accordance with Forescout policy.
A-2.3.f	Terminate Access to Network	Terminate Access to Network	Success: BYOD has access terminated after failing to reauthenticate to the GlobalProtect VPN.
A-2.4.a,d	Keep Access to Network	Keep Access to Network	Success: Azure is able to allow access to cloud endpoints and resources.
A-2.4.b,c,f	Terminate Access to Network	Terminate Access to Network	Success: Azure is able to limit access to cloud endpoints and resources.
A-2.4.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: Azure is able to limit access to cloud endpoints and resources.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-3.1.a	User request and action is recorded	User request is recorded	Partial Success: User activity and transaction flow is logged using Forescout. Individual user actions are not visible within this build.
A-3.2.a	User request and action is recorded	User request is recorded	Partial Success: User activity and transaction flow is logged using Forescout and Azure AD. Individual user actions are not visible within this build.
A-3.3.a, A-3.4.a,	User request and action is recorded	N/A	Branch testing is not available for this build.
A-3.5.a, A-3.6.a	User request and action is recorded	User request is recorded	Partial Success: User activity and transaction flow is logged. Individual user actions are not visible.
A-3.1.b, A-3.2.b, A-3.3.b, A-3.4.b	API call is recorded	Activity and transaction flow is recorded	Partial Success: Service activity and transaction flow is logged by Forescout. Individual API calls are not visible.
B-1.1.a	Access Successful	Access Successful	Success: Users access RSS1 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.1.b	Access Successful	Access Successful	Success: Users access RSS2 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.1.c	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.1.d	Access Not Successful	Access Not Successful	Success: E2 is not authorized to access RSS1 in accordance with Azure AD policy.
B-1.1.e	Access Successful	Access Successful	Success: Users access RSS2 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.1.f, B-1.1.g,	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.1.h	Access Successful	Access Successful	Success: Session timeout is set to one minute for demonstration purposes. After session timed out, user was reauthenticated to Azure AD.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1.i	Access Not Successful	Access Not Successful	Success: Users were prevented from accessing resources after reauthentication failure to Azure AD.
B-1.1.j	Access Not Successful	Access Not Successful	Success: Initial user authentication to Azure AD was successful and user was granted access to RSS1. After E1 became noncompliant, user access to RSS1 was blocked in accordance with Forescout policy, and the user was unable to reauthenticate to Azure AD.
B-1.1.k	Access Limited	Access Not Successful	Partial success: Initial user authentication to Azure AD was successful and user was granted access to RSS2. In this case, changing the user's access level on RSS2 would require application-level control that is not available at this time. After E1 became noncompliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to reauthenticate to Azure AD.
B-1.1.l	Access Not Successful	Access Not Successful	Success: After E1 became noncompliant, user access to RSS1 was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.1.m	Access Limited	Access Not Successful	Partial success: In this case, changing the user's access level on RSS2 would require application-level control that is not available at this time. After E1 became noncompliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.1.n-p	Access Not Successful	Access Not Successful	Success: After the RSS became noncompliant, user access to the RSS was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.2.a-p	N/A	N/A	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.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.4.a	Access Successful	Access Successful	Success: Users access RSS1 based on the EP compliance with Forescout and Azure AD policy.
B-1.4.b	Access Successful	Access Successful	Success: Users access RSS2 based on the EP compliance with Forescout and Azure AD policy.
B-1.4.c	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.4.d	Access Not Successful	Access Not Successful	Success: E2 is not authorized to access RSS1 in accordance with Azure AD policy.
B-1.4.e	Access Successful	Access Successful	Success: Users access RSS2 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.4.f, B-1.4.g	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.4.h	Access Successful	Access Successful	Success: Session timeout is set to one minute for demonstration purposes. After session timed out, user was reauthenticated to Azure AD.
B-1.4.i	Access Not Successful	Access Not Successful	Success: Users were prevented from accessing resources after reauthentication failure to Azure AD.
B-1.4.j	Access Not Successful	Access Not Successful	Success: Initial user authentication to Azure AD was successful and user was granted access to RSS1. After E1 became noncompliant, user access to RSS1 was blocked in accordance with Forescout policy, and the user was unable to reauthenticate to Azure AD.
B-1.4.k	Access Limited	Access Not Successful	Partial success: Initial user authentication to Azure AD was successful and user was granted access to RSS2. In this case, changing the user's access level on RSS2 would require application-level control that is not available at this time. After E1 became noncompliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to reauthenticate to Azure AD.
B-1.4.l	Access Not Successful	Access Not Successful	Success: After E1 became noncompliant, user access to RSS1 was blocked in accordance with

Demo ID	Expected Outcome	Observed Outcome	Comments
			Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.4.m	Access Limited	Access Not Successful	Partial success: In this case, changing the user's access level on RSS2 would require application-level control that is not available at this time. After E1 became noncompliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.4.n-p	N/A	N/A	Demonstration cannot be performed as verification of cloud resource compliance is not available at this time.
B-1.5.a-p	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
B-1.6.a-p			In the current implementation, remote users are connected to a VPN that routes network traffic through the on-prem environment. All test results are similar to B-1.4.a-p.
B-2.1.a-d, g, n	Access Successful	Access Successful	Success: Access allowed in accordance with Forescout policy.
B2.1.e, f, l, m, o, p	Access Not Successful	Access Not Successful	Success: Access denied in accordance with Forescout policy.
B-2.2	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
B-2.3			In the current implementation, remote users are connected to a VPN that routes network traffic through the on-prem environment. All test results are similar to B-2.1.a-p.
B-3.1.a, B-3.4.a, B-3.5.a	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.
B-3.1.b, B-3.4.b, B-3.5.b	Real Req Fail	Real Req Fail	Success: Incorrect credentials were entered, and the Real Request failed as expected.
B-3.1.c, B-3.4.c, B-3.5.c	Limit Access for Real Request, Deny Access to	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.

Demo ID	Expected Outcome	Observed Outcome	Comments
	Hostile Request		
B-3.1.d, B-3.4.d, B-3.5.d	Real Request Keep Access, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.e, B-3.4.e, B-3.5.e	Hostile Request Successful	Hostile Request Successful	Success: Hostile Request successfully authenticated.
B-3.1.f, B-3.4.f, B-3.5.f	Hostile Request Unsuccessful	Hostile Request Unsuccessful	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.g, B-3.4.g, B-3.5.g	Real Request Fail, Hostile Request Access Limited	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.h, B-3.4.h, B-3.5.h	Real Request Fail, Hostile Request remains authenticated	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.i, B-3.4.i, B-3.5.i	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.
B-3.1.j, B-3.4.j, B-3.5.j	Real Request remains authenticated, Hostile Request Fail	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.k, B-3.4.k, B-3.5.k	Hostile Request Fail	Hostile Request Fail	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.l, B-3.4.l, B-3.5.l	Real Request Access Successful	Real Request Access Successful	Success: Real Request successfully reauthenticated.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-3.1.m, B-3.4.m, B-3.5.m	Hostile Request Access Denied	Hostile Request Access Denied	Success: Hostile Request reauthentication fails.
B-3.1.n, B-3.4.n, B-3.5.n	Hostile Request Session Terminated	Hostile Request Session Terminated	Success: Azure AD sessions terminated.
B-3.1.o, B-3.4.o, B-3.5.o	Real Request Session Terminated	Real Request Session Terminated	Success: Azure AD sessions terminated.
B-3.2, B-3.3	N/A	N/A	Branch office is not included in Build 3.
B-4			All demonstrations here are the same as B-1 since the device is both authenticated and compliant.
B-5			All demonstrations here are the same as B-2 since the device is both authenticated and compliant.
B-6			All demonstrations here are the same as B-3 since the device is both authenticated and compliant.
All C Use Cases	N/A	N/A	Demonstrations cannot be performed. Currently, no federation configuration has been set up between Ent1, Ent2, and Ent3.
All D Use Cases			All demonstrations here are the same as B since the device is both authenticated and compliant. Note that the user is a contractor.
E-1.1.a, b	Access Successful	Access Successful	Success: Guests can access public resources and internet in accordance with policy using Forescout.
E-1.2.a, b	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
All F Use Cases	N/A	N/A	Confidence level use cases are considered out of scope for the EIG run phase.

D.3 Enterprise 4 Build 3 (E4B3) Detailed Demonstration Results

Table D-3 lists the full demonstration results for EIG run phase demonstrations in Enterprise 4 Build 3 (E4B3). In all demonstrations that we attempted to conduct, the ZTA functionality included in the build performed as expected. The technology deployed in E4B3 was able to determine endpoint compliance for Windows and mobile devices and prevent noncompliant endpoints from accessing private resources.

Table D-3 Detailed Demonstration Results for E4B3 SDP and Microsegmentation Phase

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.a-d, A-1.1.f, A-1.1.j	N/A	N/A	IBM considers RSS management and granting the endpoint limited access to the network out of scope for their products. Other technologies should be used to perform this function.
A-1.1.e, A-1.1.i	Access to Network	Access to Network	Success: MaaS360 configuration allowed iOS and Android devices to successfully authenticate to the Enterprise 4 wireless network.
A-1.1.g, A-1.1.k	No Access to Network	No Access to Network	Success: iOS and Android devices were denied access after failing network authentication.
A-1.1.h, A-1.1.l, A-1.1.m	Access to Public Network	Access to Public Network	Success: The devices are able to access the Public Network.
A-1.2.a-m, A-1.3.a-f, A-1.4.a-g	N/A	N/A	Not demonstrated in this build due to no branch in Ent 4.
A-1.3.a, A-1.3.d	Access to Network	Access to Network	Success: MaaS360 configuration allowed iOS and Android devices to successfully authenticate to the Enterprise 4 wireless network.
A-1.3.c, A-1.3.f	No Access to Network	No Access to Network	Success: iOS and Android devices were denied access after failing network authentication.
A-1.3.b, A-1.3.e	N/A	N/A	IBM considers limited network access out of scope for their products. Other technologies should be used to perform this function.
A-2			A-2 results match results from A-1.
A-3.1.a, A-3.3.a, A-3.5.a	User request and action	User login to an	Success: IBM Security Verify and QRadar record user application requests.

Demo ID	Expected Outcome	Observed Outcome	Comments
	is recorded	application is logged	
A-3.2.a, A-3.4.a, A-3.6.a	User request and action is recorded	User login to an application is logged	Success: IBM Security Verify and QRadar record user application logins.
A-3.1.b, A-3.3.b, A-3.2.b, A-3.4.b, A-3.6.a	N/A	N/A	IBM considers API call visibility out of scope for their products. Other technologies should be used to perform this function.
B-1.1.a, B-1.3.a, B-1.4.a, B-4.1.a, B-4.2.a, B-4.3.a, D-1.1.a, D-1.2.a, D-1.3.a, D-4.1.a, D-4.2.a, D-4.3.a	Access Successful	Access Successful	Partial Success: User is successfully authenticated and granted access to the resource. However, RSS compliance was not obtained.
B-1.1.b, B-1.3.b, B-1.4.b, B-4.1.b, B-4.2.b, B-4.3.b, D-1.1.b, D-1.2.b, D-1.3.b, D-4.1.b, D-4.2.b, D-4.3.b	Access Successful	Access Successful	Partial Success: User is successfully authenticated and granted access to the resource. However, RSS compliance was not obtained.
B-1.1.c, B-1.3.c, B-1.4.c, B-4.1.c, B-4.2.c, B-4.3.c, D-1.1.c, D-1.2.c, D-1.3.c, D-4.1.c, D-4.2.c, D-4.3.c	Access Not Successful	Access Not Successful	Success: Demonstration completed with user not able to log in to resource.
B-1.1.d, B-1.3.d, B-1.4.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	Success: User was denied access due to policy constraints.
B-1.1.e, B-1.3.e, B-1.4.e, B-4.1.e, B-4.2.e, B-4.3.e, D-1.1.e, D-1.2.e, D-	Access Successful	Access Successful	Partial Success: User is successfully authenticated and granted access to the resource. However, RSS compliance was not obtained.

Demo ID	Expected Outcome	Observed Outcome	Comments
1.3.e, D-4.1.e, D-4.2.e, D-4.3.e			
B-1.1.f, B-1.3.f, B-1.4.f, B-4.1.f, B-4.2.f, B-4.3.f, D-1.1.f, D-1.2.f, D-1.3.f, D-4.1.f, D-4.2.f, D-4.3.f	Access Not Successful	Access Not Successful	Success: Without user authentication for the resource the access attempt did not succeed.
B-1.1.g, B-1.3.g, B-1.4.g, B-4.1.g, B-4.2.g, B-4.3.g, D-1.1.g, D-1.2.g, D-1.3.g, D-4.1.g, D-4.2.g, D-4.3.g	Access Not Successful	Access Not Successful	Success: Without user authentication for the resource, the access attempt did not succeed.
B-1.1.h, B-1.3.h, B-1.4.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	Partial Success: GitLab session timeout is set to one minute for demonstration purposes. After session timed out, user was reauthenticated. However, RSS compliance was not obtained.
B-1.1.i, B-1.3.i, B-1.4.i, B-4.1.i, B-4.2.i, B-4.3.i, D-1.1.i, D-1.2.i, D-1.3.i, D-4.1.i, D-4.2.i, D-4.3.i	Access Not Successful	Access Not Successful	Success: After session timeout, user tried to login with incorrect credentials and access was denied.
B-1.1.j, B-1.3.j, B-1.4.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: User was denied access due to endpoint noncompliance.
B-1.1.k, B-1.3.k, B-1.4.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	Access Limited	Partial Success: User access was downgraded due to having a noncompliant endpoint. However, RSS compliance was not obtained.
B-1.1.l-m, B-1.3.l-m, B-1.4.l-m, B-4.1.l-m, B-4.2.l-m, B-4.3.l-m,	Access Denied	Access Denied	Partial Success: User access was downgraded due to having a noncompliant endpoint. However, RSS compliance was not obtained.

Demo ID	Expected Outcome	Observed Outcome	Comments
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			
B-1.1.n-p, B-1.3.n-p, B-1.4.n-p, B-4.1.n-p, B-4.2.n-p, B-4.3.n-p, D-1.1.n-p, D-1.2.n-p, D-1.3.n-p, D-4.1.n-p, D-4.2.n-p, D-4.3.n-p	N/A	N/A	Not demonstrated in this build due to lack of resource compliance verification.
B-1.2.a-p	N/A	N/A	Branch not available in Enterprise 4
B-2.1.a-d, B-2.3.a-d	Access Successful	Access Successful	Success: When using the secure browser on iOS and Android, user was allowed access per policy.
B-2.1.e, B-2.3.e, B-5.1.e, B-5.3.e	Access Not Successful	Access Not Successful	Success: When using the secure browser on iOS and Android, user was allowed access per policy.
B-2.1.f, B-2.3.f, B-5.1.f, B-5.3.f	Access Not Successful	Access Not Successful	Success: When using the secure browser on iOS and Android, user was denied access per policy.
B-2.1.g, B-2.3.g, B-5.1.g, B-5.3.g	N/A	N/A	Not demonstrated in this build due to MaaS360 limitation, as all MaaS360 resources like the secure browser are unavailable outside of the policy hours.
B-2.1.h-i, B-2.3.h-i, B-5.1.h-i, B-5.3.h-i	Access Not Successful	Access Not Successful	Success: User was denied access due to policy constraints.
B-2.1.j-p, B-2.2.j-p, B-2.3.j-p, B-5.1.j-p, B-5.2.j-p, B-5.3.j-p	N/A	N/A	Not demonstrated in this build. Due to security of MaaS360 certificate storage, we were unable to invalidate the credentials and produce a unsuccessful authentication. Resource compliance is not available in Ent4.
B-3.1.a, B-3.4.a, B-3.5.a, B-6.1.a, B-6.4.a, B-6.5.a	Real Req Success	Real Req Success	Success: User is able to successfully authenticate and access the RSS.
B-3.1.b, B-3.4.b, B-3.5.b, B-6.1.b, B-6.4.b, B-6.5.b	Real Req Fail	Real Req Fail	Success: User is unable to successfully authenticate and access the RSS.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-3.1.c, B-3.4.c, B-3.5.c, B-6.1.c, B-6.4.c, B-6.5.c	Limit Access for Real Request, Deny Access to Hostile Request	N/A	Due to security of MaaS360 certificate storage, we were unable to copy the credentials and produce a Hostile authentication. A stolen username/password is insufficient to successfully authenticate.
B-3.1.d, B-3.4.d, B-3.5.d, B-6.1.d, B-6.4.d, B-6.5.d	Real Request Keep Access, Deny Access to Hostile Request	N/A	Due to security of MaaS360 certificate storage, we were unable to copy the credentials and produce a successful Hostile authentication. A stolen username/password is insufficient to successfully authenticate.
B-3.1.e, B-3.4.e, B-3.5.e, B-6.1.e, B-6.4.e, B-6.5.e	Hostile Request Successful	N/A	Due to security of MaaS360 certificate storage, we were unable to copy the credentials and produce a successful Hostile authentication. A stolen username/password is insufficient to successfully authenticate.
B-3.1.f, B-3.4.f, B-3.5.f, B-6.1.f, B-6.4.f, B-6.5.f	Hostile Request Unsuccessful	Hostile Request Unsuccessful	Success: Hostile user fails to properly authenticate and is unable to access the RSS.
B-3.1.g, B-3.4.g, B-3.5.g, B-6.1.g, B-6.4.g, B-6.5.g	Real Request Fail, Hostile Request Access Limited	N/A	Due to security of MaaS360 certificate storage, we were unable to copy the credentials and produce a successful Hostile authentication. A stolen username/password is insufficient to successfully authenticate.
B-3.1.h, B-3.4.h, B-3.5.h, B-6.1.h, B-6.4.h, B-6.5.h	Real Request Fail, Hostile Request remains	N/A	Due to security of MaaS360 certificate storage, we were unable to copy the credentials and produce a successful Hostile authentication. A stolen username/password is insufficient to successfully authenticate.

Demo ID	Expected Outcome	Observed Outcome	Comments
	authenticated		
B-3.1.i, B-3.4.i, B-3.5.i, B-6.1.i, B-6.4.i, B-6.5.i	Real Req Success	Real Req Success	Success: User is able to successfully authenticate after new credentials are provisioned.
B-3.1.j, B-3.4.j, B-3.5.j, B-6.1.j, B-6.4.j, B-6.5.j	Real Request remains authenticated, Hostile Request Fail	N/A	Due to security of MaaS360 certificate storage, we were unable to copy the credentials and produce a Hostile authentication. A stolen username/password is insufficient to successfully authenticate.
B-3.1.k, B-3.4.k, B-3.5.k, B-6.1.k, B-6.4.k, B-6.5.k	Hostile Request Fail	Hostile Request Fail	Success: Stolen credentials are wiped from device using stolen credentials due to administrative action.
B-3.1.l, B-3.4.l, B-3.5.l, B-6.1.l, B-6.4.l, B-6.5.l	Real Request Access Successful	Real Requet Access Successful	Success: User is able to successfully reauthenticate after new credentials are provisioned.
B-3.1.m, B-3.4.m, B-3.5.m, B-6.1.m, B-6.4.m, B-6.5.m	Hostile Request Access Denied	Hostile Request Access Denied	Success: Hostile User is unable to successfully reauthenticate after stolen credentials are wiped and new credentials are provisioned to the user.
B-3.1.n, B-3.4.n, B-3.5.n, B-6.1.n, B-6.4.n, B-6.5.n	All sessions terminated	All sessions terminated	Success: All user sessions for GitLab RSS were terminated.
B-3.1.o, B-3.4.o, B-3.5.o, B-6.1.o, B-6.4.o, B-6.5.o	All sessions terminated	All sessions terminated	Success: All user sessions for GitLab RSS were terminated.
B-7	Success	Partial Success	Partial Success: Just-in-time privileges can be manually completed to allow a user to access a resource. However, just-in-time access privileges with automation are not tested and require

Demo ID	Expected Outcome	Observed Outcome	Comments
			integration with other zero trust tools which have the capabilities to manage access for users.
B-8	N/A	N/A	Not demonstrated in this build, as the ability to prompt for reauthentication in the middle of an active session is not included in Ent 4.
All C Use Cases	N/A	N/A	Use Case C is out of scope for this phase.
All E Use Cases	N/A	N/A	IBM considers this out of scope for their products. Other technologies should be used to perform this function.
F-1.1.a, F-1.3.a, F-1.4.a, F-1.6.a	Access Remains	Access Remains	Success: User successfully reauthenticates a locked RDP session and retains access to RSS.
F-1.1.b, F-1.3.b, F-1.4.b, F-1.6.n	Access Denied	Access Denied	Success: User unsuccessfully reauthenticates a locked RDP session and access is denied to RSS.
F1.2.a-b, F-1.5.a-b	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
F-2	N/A	N/A	Not demonstrated in this build. Due to security of MaaS360 certificate storage, we were unable to invalidate the credentials and produce an unsuccessful endpoint authentication.
F-3	N/A	N/A	IBM considers resource authentication out of scope for their product. Other technologies should be used for this use case.
F-4.1.a, F-4.3.a, F-4.4.a, F-4.6.a	Endpoint compliant, access to resource remains	Endpoint compliant, access to resource remains	Success: Access to the RSS remains as long as the endpoint maintains compliance.
F-4.1.b, F-4.3.b, F-4.4.b, F-4.6.b	Endpoint drops out of compliance, access revoked	Endpoint drops out of compliance, access revoked	Success: When the endpoint drops out of compliance, access to the RSS is revoked. Future access is prevented by Verify.
F-4.2.a-b, F-4.5.a-b	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-5.1.a, F-5.3.a, F-5.4.a, F-5.6.a	Endpoint not compliant, No access to resource	Endpoint not compliant, No access to resource	Success: Access to the GitLab resource fails if the device is not in compliance.
F-5.1b, F-5.3.b, F-5.4.b, F-5.6.b	Endpoint compliant, Access granted to resource	Endpoint compliant, Access granted to resource	Success: Once the endpoint is brought back into compliance, access to the GitLab RSS is granted.
F-5.2a-b, F-5.5.a-b	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
F-6.1.a, F-6.1.d, F-6.1.f, F-6.2.a, F-6.2.d, F-6.2.f	Access revoked from resource, account disabled	Access revoked from resource, account disabled	Success: Access to SQL database RSS is revoked when sensitive data is accessed and events are logged in QRadar. Offenses are created in QRadar and remediation is completed with CloudPak 4 Security to disable the offending account in Verify.
F-6.1.b-c, F-6.1.e, F6.1.g-l, F-6.2.b-c, F-6.2.e, F-6.2.g-l	N/A	N/A	PaaS and SaaS services were not available for this build.
F-7	Access revoked from resource	Violation logged, Access not revoked	All demonstrations here are the same as F-6.
F-8.1.a, F-8.1.c-d, F-8.1.f, F-8.2.a, F-8.2.c-d, F-8.2.f,	Access to resource revoked	Access to resource revoked	Success: On accessing a known bad URL with the MaaS360 Secure Browser on a mobile device, access to a GitLab resource is revoked via CloudPak for Security and Verify disabled the user's account.
F-8.1.b, F-8.1.e, F-8.1.h, F-8.1.k, F-8.2.b, F-8.2.e, F-8.2.h, F-8.2.k	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
F-8.1.g, F-8.1.i-j, F-8.1.l, F-8.2.g, F-8.2.i-j, F-8.2.l	N/A	N/A	PaaS and SaaS services were not available for this build.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-8.3.a-l	N/A	N/A	IBM considers guest network access out of scope for their product. Other technologies should be used for this use case.
F-9 (all use cases)			All demonstrations here are the same as F-8 since the device is both authenticated and compliant.
F-10.1.a-b, F-10.1.i-j, F-10.1.m-n, F-10.1.u-v, F-10.2.a-b, F-10.2.i-j, F-10.2.m-n, F-10.2.u-v	Access not successful, access revoked to current resource, access revoked to all future resources	Access not successful, access revoked to current resource, access revoked to all future resources	Success: If the user attempts to access an unauthorized resource, their access to their current GitLab active session is revoked and their account is disabled in Verify.
F-10.1.c-h, F-10.1.k-l, F-10.1.o-t, F-10.1.w-av, F-10.2.c-h, F-10.2.k-l, F-10.2.o-t, F-10.2.w-av	N/A	N/A	Branch, PaaS, and SaaS services were not available for this build
F-10.3.a-av	N/A	N/A	IBM considers guest network access out of scope for their product. Other technologies should be used for this use case.
F-11.1.a-b, F-11.1.i-j, F-11.1.m-n, F-11.1.u-v, F-11.2.a-b, F-11.2.i-j, F-11.2.m-n, F-11.2.u-v	Bad URL detected, active session revoked, User account disabled in Verify	Bad URL detected, active session revoked, User account disabled in Verify	Success: Once the bad URL was detected, the user session from GitLab was revoked and the user’s account was disabled in Verify. NOTE: This scenario was only tested with mobile devices running IBM MaaS360 Secure Browser to detect the bad URL.
F-11.1.c-h, F-11.1.k-l, F-11.1-t, F-11.1.w-av, F-11.2.c-h, F-	N/A	N/A	Branch, PaaS, and SaaS services were not configured for this build

Demo ID	Expected Outcome	Observed Outcome	Comments
11.2.k-l, F-11.2.o-t, F-11.2.w-av			
F-11.3.a-av	N/A	N/A	IBM considers guest network access out of scope for their product. Other technologies should be used for this use case.
F-12 (all use cases)			All demonstrations here are the same as F-10 since the device is both authenticated and compliant.
F-13 (all use cases)			All demonstrations here are the same as F-11 since the device is both authenticated and compliant.
F-14, F-15, F-16, F-17			IBM considers suspicious activity/network monitoring out of scope for their product. Other technologies should be used for these scenarios.
All G Use Cases	N/A	N/A	IBM considers service-to-service use cases out of scope for their product. Other technologies should be used for this use case.

Appendix E SDP and Microsegmentation Phase Demonstration Results

This appendix lists the full demonstration results for each of the builds that was implemented as part of the SDP and Microsegmentation phase: E1B3, E2B3, E3B3, and E1B4.

E.1 Enterprise 1 Build 3 (E1B3) Detailed Demonstration Results

Table E-1 lists the full demonstration results for SDP phase demonstrations run in Enterprise 1 Build 3 (E1B3). In all demonstrations that we attempted to conduct, the ZTA functionality included in the build performed as expected. The technology deployed in E1B3 was able to determine endpoint compliance for Windows, Linux, macOS, and mobile devices and prevent noncompliant endpoints from accessing private resources.

Table E-1 Detailed Demonstration Results for E1B3 SDP and Microsegmentation Phase

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.a-m	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build. Zscaler uses the client connector to allow a user on a device to access specific resources only, whether on-prem or remote. Users cannot readily access resources in the enterprise (or network) if they do not have permissions to access them. Resources are not authenticated or checked for compliance in this phase.
A-1.2.a-m, A-1.3.a-f, A-1.4.a-g	N/A	N/A	Same as in A-1. Demonstration cannot be completed. There is no network-level enforcement present in this build.
A-2.1.a-l, A-2.2.a-l, A-2.3.a-f, A-2.4.a-f	N/A	N/A	Same as in A-1. Demonstration cannot be completed. There is no network-level enforcement present in this build.
A-3.1.a, A-3.3.a, A-3.5.a	User request and action is recorded	User login to an 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. Zscaler Private Access (ZPA) records relevant information about the connection between the endpoint and resource.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-3.1.b, A-3.3.b	API call is recorded	Logs contain relevant API information	Success: Okta records the authentication logs. Administrators can log in to Okta and view logs of when a user logged onto an application and whether the authentication was successful or not. Zscaler ZPA records relevant information about the connection between the endpoint and resource.
A-3.2.a, A-3.4.a, A-3.6.a	User request and action is recorded	User login to an 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. Zscaler ZPA records relevant information about the connection between the endpoint and resource.
A-3.2.b, A-3.4.b, A-3.6.a	API call is recorded	Logs contain relevant API information	Success: Okta records the authentication logs. Administrators can log in to Okta and view logs of when a user logged onto an application and whether the authentication was successful or not. Zscaler ZPA records relevant information about the connection between the endpoint and resource.
B-1.1.a, B-1.2.a, B-1.3.a, B-4.1.a, B-4.2.a, B-4.3.a, D-1.1.a, D-1.2.a, D-1.3.a, D-4.1.a, D-4.2.a, D-4.3.a	Access Successful	Access Successful	Partial success: User is authenticated via Okta when accessing the resource. User logs into Zscaler client connector as part of login process to the endpoint and policies are applied to the user/endpoint (including laptops, workstations, and mobile devices). User successfully connects to RSS1. However, we cannot validate compliance of RSS1.
B-1.1.b, B-1.2.b, B-1.3.b, B-4.1.b, B-4.2.b, B-4.3.b, D-1.1.b, D-1.2.b, D-1.3.b, D-4.1.b, D-4.2.b, D-4.3.b	Access Successful	Access Successful	Partial success: User is authenticated via Okta when accessing the resource. User logs into Zscaler client connector as part of login process to the endpoint and policies are applied to the user/endpoint (including laptops, workstations, and mobile devices). User successfully connects to RSS1. However, we cannot validate compliance of RSS1.
B-1.1.c, B-1.2.c, B-1.3.c, B-4.1.c, B-4.2.c, B-4.3.c, D-1.1.c, D-1.2.c, D-1.3.c, D-4.1.c, D-4.2.c, D-4.3.c	Access Not Successful	Access Not Successful	Success: Demonstration completed with user not able to log in to resource.

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

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1.j, B-1.2.j, B-1.3.j, B-4.1.j, B-4.2.j, B-4.3.j, D-1.1.j, D-1.2.j, D-1.3.j, D-4.1.j, D-4.2.j, D-4.3.j	Access Not Successful	Access Not Successful	Success: Device posture failure detected by ZPA, so access was denied.
B-1.1.k, B-1.2.k, B-1.3.k, B-4.1.k, B-4.2.k, B-4.3.k, D-1.1.k, D-1.2.k, D-1.3.k, D-4.1.k, D-4.2.k, D-4.3.k	Access Limited	N/A	Partial success: Access to RSS2 is blocked. Currently cannot perform limited access.
B-1.1.l-m, B-1.2.l-m, B-1.3.l-m, B-4.1.l-m, B-4.2.l-m, B-4.3.l-m, D-1.1.l-m, D-1.2.l-m, D-1.3.l-m, D-4.1.l-m, D-4.2.l-m, D-4.3.l-m	Access Denied	Access Denied	Success: User was denied access because the endpoint was noncompliant. Device posture failure detected by ZPA.
B-1.1.n-p, B-1.2.n-p, B-1.3.n-p, B-4.1.n-p, B-4.2.n-p, B-4.3.n-p, D-1.1.n-p, D-1.2.n-p, D-1.3.n-p, D-4.1.n-p, D-4.2.n-p, D-4.3.n-p	N/A	N/A	Demonstration cannot be run. Unable to perform compliance checks on RSS.
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 ZPA policies allow the user/device to access the enterprise remotely the same way that user/device would access a resource within the enterprise. See results from B-1.1.
B-1.4.a-p, B-1.5.a-p, B-1.6.a-p, B-4.4.a-p, B-4.5.a-q, and B-4.6.a-p			Results of access to cloud-based resources (RSS1 and RSS2) are the same as on-prem. See results from B-1.1.
B-2.1.a-d, B-2.2.a-d, B-2.3.a-d	Access Successful	Access Successful	Success: Employee is granted access to URL1 and URL2 regardless of hourly access time because

Demo ID	Expected Outcome	Observed Outcome	Comments
			employees have full access to both URLs at all times per ZScaler policy.
B-2.1.e, B-2.2.e, B-2.3.e	Access Not Successful	Access Not Successful	Success: The only way the user is not authenticated is if the user inputs the incorrect password or does not have a second factor during Zscaler Client Connector (ZCC) login. With incorrect 1st or 2nd factor, ZCC will fail to connect with ZIA and will not be able to access the internet.
B-2.1f, B-2.2f, B-2.3f	Access Not Successful	Access Not Successful	Success: Contractor is blocked from URL1 as expected per Zscaler policy.
B-2.1g, B-2.2g, B-2.3g	Access Successful	Access Successful	Success: Contractor is granted access to URL2 as expected per Zscaler policy.
B-2.1.h-I, B-2.2.h-I, B-2.3.h-i	Access Not Successful	Access Not Successful	Success: Contractor is blocked from accessing URL1 due to failed authentication.
B-2.1.j, B-2.2.j, B-2.3.j	Access Not Successful	Access Successful	The only way the user is not authenticated is if the user inputs the incorrect password or does not have a second factor during ZCC login. Access is successful because internet access is required for ZIA to function. If not authenticated to ZIA, internet access is unrestricted unless blocked by company firewall.
B-2.1.k, B-2.2.k, B-2.3.k	Access Successful	Access Successful	Success: Employee is granted access after successful reauthentication per Zscaler policy as expected.
B-2.1.l, B-2.2.l, B-2.3.l	Access Not Successful	Access Not Successful	Success: Employee cannot access URL1 or URL2 after reauthentication to Zscaler fails as expected.
B-2.1.m-p, B-2.2.m-p, B-2.3.m-p	N/A	N/A	Demonstration cannot be completed. ZIA does not perform device posture/compliance checks on endpoints without integration of a third-party EPP product, which we currently don’t have in the build.
B-3.1.a, B-3.4.a, B-3.5.a	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.
B-3.1.b, B-3.4.b, B-3.5.b	Real Req Fail	Real Req Fail	Success: Incorrect credentials were entered, and the Real Request failed as expected.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-3.1.c, B-3.4.c, B-3.5.c	Limit Access for Real Request, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.d, B-3.4.d, B-3.5.d	Real Request Keep Access, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.e, B-3.4.e, B-3.5.e	Hostile Request Successful	Hostile Request Successful	Success: Hostile Request successfully authenticated.
B-3.1.f, B-3.4.f, B-3.5.f	Hostile Request Unsuccessful	Hostile Request Unsuccessful	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.g, B-3.4.g, B-3.5.g	Real Request Fail, Hostile Request Access Limited	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.h, B-3.4.h, B-3.5.h	Real Request Fail, Hostile Request remains authenticated	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-3.1.i, B-3.4.i, B-3.5.i	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.
B-3.1.j, B-3.4.j, B-3.5.j	Real Request remains authenticated, Hostile Request Fail	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.k, B-3.4.k, B-3.5.k	Hostile Request Fail	Hostile Request Fail	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.l, B-3.4.l, B-3.5.l	Real Request Access Successful	Real Requet Access Successful	Success: Real Request successfully reauthenticated.
B-3.1.m, B-3.4.m, B-3.5.m	Hostile Request Access Denied	Hostile Request Access Denied	Success: Hostile Request reauthentication failed.
B-3.1.n, B-3.4.n, B-3.5.n	N/A	N/A	Demonstration could not be completed due to build not supporting session termination at this level.
B-3.1.o, B-3.4.o, B-3.5.o	N/A	N/A	Demonstration could not be completed due to build not supporting session termination at this level.
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 the ZCC client. See results from B-1.1 for B-4.1, B-4.2, and B-4.3.
B-5			As documented in the rows above, the results of all B-5 use case demonstrations are the same as the results of the B-2 use cases because the device is both authenticated and compliant. In this case, a BYOD device will have to install ZCC client. See results from B-1.1 for B-5.1, B-5.2, and B-5.3.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-6			As documented in the rows above, the results of all B-6 use case demonstrations are the same as the results of the B-3 use cases because the device functions the same. In this case, a BYOD device will have to install ZCC client. See results from B-3.
B-7	Success	Partial Success	Partial Success: Just-in-time privileges can be manually completed to allow a user to access a resource. However, just-in-time access privileges with automation are not tested and require integration with other zero trust tools which have the capabilities to manage access for users.
B-8	N/A	N/A	Step-up authentication is available through an enhancement request to upgrade ZPA. However, this enhancement was not available during the time of this build. Tests cannot be completed.
All C Use Cases	N/A	N/A	Federation will be performed during the next phase by Okta. Once Okta can verify users from Enterprise 2, for example, this will be tested. Users from Enterprise 2 will perform the exact same process of installing ZCC to get access to on-prem resources via ZPA or leverage ZIA to access the internet.
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 ZCC client will have to be installed on the contractor's device, whether it's provided by the enterprise or BYOD.
E-1.1.a, E-1.2.a	Success	Success	Success: User/device is recognized by Zscaler Internet Access (ZIA) as unmanaged and given access to the internet. Per ZIA enterprise policies, resources on the internet that are deemed safe for access are reachable by the user with No-ID, which includes a public resource from Enterprise 1.
E-1.1.b, E-1.2.b	Success	Success	Success: User/device is recognized by ZIA as unmanaged and given access to the internet. Per ZIA enterprise policies, resources on the internet that

Demo ID	Expected Outcome	Observed Outcome	Comments
			are deemed safe for access are reachable by the user with No-ID.
F-1.1.a, F-1.2.a, F-1.3.a, F-1.4.a, F-1.5.a, F-1.6.a	Success	Success	Success: Zscaler timeout set to 10 minutes for testing purposes. Once timed out, user has to reauthenticate to Zscaler again before being able to access any resources. For these test cases, successful authentication allows the user to get access to the resource again.
F-1.1.b, F-1.2.b, F-1.3.b, F-1.4.b, F-1.5.b, F-1.6.b	Success	Success	Success: Zscaler timeout set to 10 minutes for testing purposes. Once timed out, user has to reauthenticate to Zscaler again before being able to access any resources. For these test cases, unsuccessful authentication means that the user does not have access to the resource again. In these use cases, access to GitLab is denied as the web browser will show that connection is unsuccessful.
F-2	N/A	N/A	Authentication and authorization to a resource by Zscaler is based on the policies that are applied to the user and the device that the user logged onto via VCC. ZPA does not check for device authentication. This use case cannot be tested.
F-3	N/A	N/A	For this build, Zscaler considers resource authentication out of scope for their products.
F-4	N/A	N/A	Authentication and authorization to a resource by Zscaler is based on the policies that are applied to the user and the device that the user logged onto via ZCC. The device posture is checked when user tries to access the resource. There is a timeout period that is set in which the user will have to reauthenticate again. At that point, the device posture is checked again. Based on the functions of ZPA, this use case cannot be tested.
F-5.1-6	Success	Success	Success: In this build, device posture is checked when a user attempts to access a resource. If posture check fails, user is denied access. User remediates the issue and tries to access the resource again. Posture check is successful, and user is allowed access to resource.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-6	N/A	N/A	Cloud Browser Isolation (CBI) can provide this capability. However, this product was not available during the time of this build. Tests cannot be completed.
F-7	N/A	N/A	CBI can provide this capability. However, this product was not available during the time of this build. Tests cannot be completed.
F-8	N/A	N/A	While connected to a resource, the Enterprise-ID tries to connect to a known bad URL. Zscaler denies the connection and displays the denied message on the browser. No other action is taken. There is no mechanism to disconnect the active connection to the resource. ZPA controls access to enterprise resources and ZIA controls access to the internet.
F-9	N/A	N/A	While connected to a resource, the Enterprise-ID tries to connect to a known bad URL. Zscaler denies the connection and displays the denied message on the browser. No other action is taken. There is no mechanism to disconnect the active connection to the resource. ZPA controls access to enterprise resources and ZIA controls access to the internet. Test cannot be completed.
F-10	N/A	N/A	Zscaler does not revoke access based on attempts. Policies allow or deny the Enterprise-ID access. Revoking access would be applied to the policy. Test cannot be completed.
F-11	N/A	N/A	While connected to a resource, the Enterprise-ID tries to connect to a known bad URL. Zscaler denies the HTTP connection. No other action is taken. There is no mechanism to disconnect the active connection to the resource. ZPA controls access to enterprise resources and ZIA controls access to the internet. Test cannot be completed.
F-12	N/A	N/A	While connected to a resource, the Enterprise-ID tries to connect to a known bad URL. Zscaler denies the HTTP connection. No other action is taken. There is no mechanism to disconnect the active connection to the resource. ZPA controls access to

Demo ID	Expected Outcome	Observed Outcome	Comments
			enterprise resources and ZIA controls access to the internet. Test cannot be completed.
F-13	N/A	N/A	While connected to a resource, the Enterprise-ID tries to connect to a known bad URL. Zscaler denies the HTTP connection. No other action is taken. There is no mechanism to disconnect the active connection to the resource. ZPA controls access to enterprise resources and ZIA controls access to the internet. Test cannot be completed.
F-14, F-15, F-16, F-17	N/A	N/A	Zscaler "Deception" is a tool that can provide capabilities to successfully test this. However, this product was not available during the time of this build. Tests cannot be completed.
G-1, G-2, G-3, G-4, G-5	N/A	N/A	Zscaler for Workloads is a tool that can provide capabilities to successfully test this. However, this product was not available during the time of this build. Tests cannot be completed.

E.2 Enterprise 2 Build 3 (E2B3) Detailed Demonstration Results

Table E-2 lists the full demonstration results for Microsegmentation (network) phase demonstrations run in Enterprise 2 Build 3 (E2B3). In all demonstrations that we attempted to conduct, the ZTA functionality included in the build performed as expected. The technology deployed in E2B3 was able to determine endpoint compliance for Windows, Linux, macOS, and mobile devices and prevent noncompliant endpoints from accessing private resources.

Table E-2 Detailed Demonstration Results for E2B3 SDP and Microsegmentation Phase

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.a	Success	Partial Success	Partial Success: Using Cisco Secure Workload, an agent is installed on the resource. Policies are applied to the resource to allow or deny traffic to and from this resource. CSW does not verify resource compliance.
A-1.1.b	N/A	N/A	CSW does not perform compliance verifications.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.c	N/A	N/A	Once onboarded, CSW manages the resource using the client. The onboarding process can be considered the authentication mechanism. Otherwise, there is not additional authentication needed.
A-1.1.d	Success	Success	Success: Without onboarding, resource will not receive an IP address. Therefore, it will not have access to the network.
A-1.1.e, I, A-1.3.a, d	Success	Success	Success: EP has access to network and all resources once onboarded, authenticated, and in compliance.
A-1.1.f, j, A-1.3.b, e	Success	Success	Success: EP has access to a specific network so that it has the ability to remediate issues in order to become compliant.
A-1.1.g, k, A-1.3.c, f	Success	Success	Success: Cisco ISE validates credentials prior to allowing the device onto the network. If authentication fails, the endpoint will not have access to the network.
A-1.1.h, l	Success	Success	Success: If not onboarded, the endpoint will have access to a network that allows it to have internet access.
A-1.1.i	Success	Success	Success: EP has access to network and all resources once onboarded, authenticated, and in compliance.
A-1.1.m	Success	Success	Success: All guests will have access to internet only.
A-1.2	N/A	N/A	Enterprise 2 does not have a branch office. However, if resources and endpoints are deployed at a branch office, configuration would be similar to that of the on-prem setup.
A-1.4	N/A	N/A	Currently, Enterprise 2 does not have a cloud component. These use cases cannot be performed.
A-2	Success	Success	Success: All A-2 scenario results are the same as A-1 scenario results. Per policy, Cisco ISE will perform re-authentication periodically.
A-3.1.a, A-3.5.a	User request and action	User login to an application is logged	Success: Cisco ISE logs user login information. This information is also sent to a SIEM.

Demo ID	Expected Outcome	Observed Outcome	Comments
	is recorded		
A-3.1.b	API call is recorded	Logs contain relevant API information	Success: CSW logs all communications from resources.
A-3.3	N/A	N/A	Enterprise 2 does not have a branch location. However, logs would be recorded since the same zero trust would be used to manage the user and resource at the branch office.
A-3.2, A-3.4, A-3.6	N/A	N/A	Enterprise 2 currently does not have cloud components. These use cases are out of scope.
B-1.1.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-4.3.a	Access Successful	Access Successful	Partial Success: User and endpoint are authenticated and compliant. Access to RSS1 was successful. Note: RSS1 authentication and compliance are independent of the endpoint. In our current build, CSW does not relay this information to ISE.
B-1.1.b, B-4.1.b, B-4.2.b, B-4.3.b, D-1.1.b, D-4.1.b, D-4.3.b	Access Successful	Access Successful	Partial Success: User and endpoint are authenticated and compliant. Access to RSS2 was successful. Note: RSS1 authentication and compliance are independent of the endpoint. In our current build, CSW does not relay this information to ISE.
B-1.1.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-4.3.c	Access Not Successful	Access Not Successful	Success: When user logs onto device, incorrect login denies user from accessing the device and network access is denied.
B-1.1.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-4.3.d	Access Not Successful	Access Not Successful	Success: User 2 does not have access to RSS1 based on policy. Therefore, access is denied.
B-1.1.e, B-4.1.e, B-4.2.e, B-4.3.e, D-1.1.e, D-1.2.e, D-	Access Successful	Access Successful	Partial Success: User and endpoint are authenticated and compliant. Access to RSS2 was successful.

Demo ID	Expected Outcome	Observed Outcome	Comments
1.3.e, D-4.1.e, D-4.3.e			Note: RSS2 authentication and compliance are independent of the endpoint. In our current build, CSW does not relay this information to ISE.
B-1.1.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-4.3.f	Access Not Successful	Access Not Successful	Success: When user logs onto device, incorrect login denies user from accessing the device and network access is denied.
B-1.1.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-4.3.g	Access Not Successful	Access Not Successful	Success: When user logs onto device, incorrect login denies user from accessing the device and network access is denied.
B-1.1.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-4.3.h	Access Successful	Access Successful	Success: Initial authentication allow user access. Reauthentication is set to 1800 seconds by ISE, and ISE will check that the device has not changed state. No user interaction is needed. Authentication will fail if device becomes noncompliant or if AD or ISE is unavailable.
B-1.1.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-4.3.i	Access Not Successful	Access Not Successful	Success: Authentication will fail if device becomes noncompliant or if AD or ISE is unavailable.
B-1.1.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-4.3.j	Access Not Successful	Access Not Successful	Success: Device posture failure detected, so access was denied.
B-1.1.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-4.3.k	Access Limited	Access Not Successful	Partial success: Access to RSS2 is blocked. Currently cannot perform limited access.
B-1.1.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-4.3.l-m	Access Denied	Access Denied	Success: User was denied access because the endpoint was noncompliant. Device posture failure detected.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1.n-p, B-1.2.n-p, B-1.3.n-p, B-4.1.n-p, B-4.2.n-p, B-4.3.n-p, D-1.1.n-p, D-1.2.n-p, D-4.1.n-p,	N/A	N/A	CSW's policies will allow or deny based on the resources posture. If resource is not compliant, the firewall on the resource will deny traffic to and from the resource. CSW does not provide input to ISE at this time. Will demonstrate during the next phase.
B-1.2.a-p, B-4.2, D-1.2.a-p, D-4.2	N/A	N/A	Enterprise 2 does not have a branch office. Therefore, these use cases were not performed. However, the results would be the same as B-1.1 since network policies allow access from branch to Ent2. See results from B-1.1.
B-1.3.a-p, B-4.3a-p, D-1.3.a-p, D-4.3a-p	N/A	N/A	These use cases will be performed in the future.
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	Currently, we do not have a cloud component for Enterprise 2 Build 3. Tests were not completed.
B-2, B-5, D-2, D-5	Access Successful	N/A	While each individual URL can be inputted into ISE to manage a user's access, Cisco does not recommend this solution. A solution specifically built for web filtering is recommended for this.
B-3.1, B-6.1, D-3.1, D-6.1	Real Req Success	N/A	The current Cisco solution authenticates both the user and device for access to the resource. Ping Identity authorizes the user to login into the resource. Credentials must be reported stolen in order for ISE or Ping Identity to make updates. Note: ISE has a feature that automates the process of revoking user access on a credential that is reported stolen. Once reported, new credentials are issued and the real user must log in again.
B-3.2, B-3.3, B-3.4, B-3.5, B-6.2, B-5.3, B-6.4, B-6.5, D-3.2, D-3.3, D-3.4, D-3.5, D-6.2, D-5.3, D-6.4, D-6.5	Real Req Fail	N/A	Enterprise 2 does not have a branch office. However, if a branch office is available, the outcome would be the same as B-3.1. For remote/on-prem or on-prem/remote use cases, the results would be the same as B-3.1.
B-7.1.a, y	Access not successful	Access not success	Success: Since user was not provisioned to have access to this resource, access was not successful.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-7.1.b, z	Access successful	Access successful	Success: Once a policy was provisioned for the user, access was successful.
B-7.1.c-x, aa-aj	N/A	N/A	Enterprise 2 currently does not have a branch office or cloud resources. Use cases involving these locations were not performed.
B-8.1.a-c, m-o	Access successful	N/A	Partial success: Cisco ISE does not provide an authentication mechanism to authenticate to the resource. However, a policy must be updated to allow the user and endpoint to reach the resource via the specific protocol that the resource is using. Therefore, ISE updated a policy and reauthenticated the endpoint to allow access.
B-8.1.d-f, p-r	Access not successful	N/A	While each individual URL can be input into ISE to manage a user's access, Cisco does not recommend this solution. A solution specifically built for web filtering is recommended for this.
B-8.1.g-l, B-8.2, B-8.3, B-8.4, B-8.5	N/A	N/A	Enterprise 2 currently does not have a branch office or cloud resources. Use cases involving these locations were not performed.
All C Use Cases	N/A	N/A	Federation will be performed in the future.
E	Success	Success	Access to internet is allowed though the guest network.
F-1.1.a, F-1.3.a	Success	Success	Success: Session will stay alive after a successful reauthentication.
F-1.1.b, F-1.3.b	Success	Success	Success: Session will be terminated upon unsuccessful reauthentication. ISE will revoke all access to resources upon unsuccessful authentication.
F-1.2, F-2.2, F-4.2, F-5.2	N/A	N/A	Enterprise 2 does not have a branch location. However, policies can be applied the same way to users if they are on-premises.
F-1.4, F-1.5, F-1.6, F-2.4, F-2.5, F-2.6, F-4.4, F-4.5, F-4.6, F-5.4, F-5.5, F-5.6	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-2.1.a, F-2.3.a	Success	Success	Success: Session will stay alive after a successful reauthentication.
F-2.1.b, F-2.3.b	Success	Success	Success: Session will be terminated upon unsuccessful reauthentication. ISE will revoke all access to resources upon unsuccessful authentication.
F-3	N/A	N/A	CSW does not provide information to Cisco ISE at this time. This use case cannot be performed.
F-4.1.a, F-4.3.a	Success	Success	Success: When Cisco ISE detects that compliance is succcessful, ISE does not revoke access.
F-4.1.b, F-4.3.b	Access Stopped	Access Stopped	Success: When Cisco ISE detects that compliance fails, access is revoked.
F-5-1.a, F-5-3.a	Access Denied	Access Denied	If compliance is not met, user will continue to not have access to resources.
F-5-1.b, F-5-3.b	Access Successful	Access Successful	Once compliance is met and reauthentication succeeds, ISE will allow user to access resources again.
F-6.1.a, F-6.1.c, F-6.2.a, F-6.2.c, F-7.1.a, F-7.1.c, F-7.2.a, F-7.2.c	Access Stopped	Access Stopped	Success: Leveraging Cisco SNA to identify the violation of data use, SNA informs ISE of the violation. ISE then removes the user's access.
F-6.1.b, F-6.2.b, F-7.1.b, F-7.2.b	N/A	N/A	Enterprise 2 does not have a branch location. However, policies can be applied the same way to users if they are on-premises.
F-6.1.d-k, F-6.2.d-k, F-7.1.d-k, F-7.2.d-k	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
F-8, F-9	N/A	N/A	The current solutions deployed in Enterprise cannot perform this based on URLs. However, SNA has the capability to act based on specific events such Command and Control, bot-infected hosts, brute force login, and connections to Tor or Bogon addresses, amongst other malicious connections. Once SNA detects these malicious interactions, it informs Cisco ISE. Cisco Secure Endpoint also detects threats and informs ISE. ISE will then deny user any access based on policy.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-10.1.a, F-10.1.i, F-10.2.a, F-10.2.i, F-10.3.a, F-10.3.i, F-12.1.a, F-12.1.i, F-12.2.a, F-12.2.i, F-12.3.a, F-12.3.i	Access not successful	Access not successful	Success: Leveraging policies deployed in SNA and ISE, a user attempting to access a resource that they are not authorized to access will be denied.
F-10.1.b, c, d, f, g, h, j-av, F-10.2.b, c, d, f, g, h, j-av, F-10.3.b, c, d, f, g, h, j-av, F-12.1.b, c, d, f, g, h, j-av, F-12.2.b, c, d, f, g, h, j-av, F-12.3.b, c, d, f, g, h, j-av	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
F-10.1.e, F-10.2.e, F-10.3.e, F-12.1.e, F-12.2.e, F-12.3.e	N/A	N/A	Enterprise 2 does not have a branch location. However, policies can be applied the same way to users if they are on-premises.
F-11, F-13	N/A	N/A	The current solutions deployed in Enterprise 2 cannot perform this based on URLs. However, SNA has the capability to act based on specific events such Command and Control, bot infected hosts, brute force login, and connections to Tor or bogon addresses, amongst other malicious connections. ISE can have a session changed based on information from another tool that can manage URL access.
F-14.1.a, F-14.1.c, F-15.1.a, F-15.1.c, F-16.1.a, F-16.1.c, F-17.1.a, F-17.1.c	Access not successful	Access not successful	SNA can detect if a user is performing suspicious activity based on various types of policies. Some of these may fall into compliance. If that’s the case, ISE will quarantine the device until it is remediated. Once SNA sees these malicious interactions, it informs Cisco ISE. Also, Cisco Secure Endpoint detects threats and passes this to ISE. ISE will then deny user any access based on policy.
F-14.1.d-l, F-15.1.d-l, F-16.1.d-l, F-17.1.d-l	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-1.1.a	Access successful	Access successful	Success: CSW policy allows subject to communicate with the resource. Note: CSW continuously monitors

Demo ID	Expected Outcome	Observed Outcome	Comments
			the communications in and out of a subject and develops policies based on that information. The policies are then deployed and enforced on the subject.
G-1.1.b	Access not successful	Access not successful	Success: Based on CSW policy, subject was denied from communicating with the resource by the resource’s local firewall.
G-1.1.c-d	N/A	N/A	Enterprise 2 does not have a branch location. Tests are not performed. However, CSW would deploy policies the same way as on-prem resources to protect resources at a branch location.
G-1.1.e	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-1.1.f	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-1.1.g	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-1.1.h	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-1.1.i	Access successful	Access Successful	Success: CSW allows the communication between a SaaS and on-prem resource based on policies that are created to allow legitimate communications between them.
G-1.1.j	N/A	N/A	Unable to perform this as we are unable modify a SaaS subject.
G-1.2.a-i	N/A	N/A	Enterprise 2 does not have a branch location. Tests are not performed. However, CSW would deploy policies the same way as on-prem resources to protect resources at a branch location. An agent would be installed on these resources.
G-2.1.a	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-2.1.b	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-2.1.c-d	N/A	N/A	Enterprise 2 does not have a branch location. Tests are not performed. However, CSW would deploy

Demo ID	Expected Outcome	Observed Outcome	Comments
			policies the same way as on-prem resources to protect resources at a branch location.
G-2.1.e	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-2.1.f	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-2.2.a	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-2.2.b	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-2.2.c-d	N/A	N/A	Enterprise 2 does not have a branch location. Tests are not performed. However, CSW would deploy policies the same way as on-prem resources to protect resources at a branch location. An agent would be installed on these resources.
G-2.2.e	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-2.2.f	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-2.3.a	Success	Success	Success: CSW allows the communication between an on-prem resource and SaaS based on policies that are created to allow legitimate communications between them from the on-prem resource.
G-2.3.b	Access not successful	Access not successful	Success: CSW only allows the communication between an on-prem resource and SaaS based on policies that are created to allow legitimate communications between them from the on-prem resource. If there is no policy to allow the communication, there is an implicit deny for this use case.
G-2.3.c-d	N/A	N/A	Enterprise 2 does not have a branch location. Tests are not performed. However, CSW would deploy policies the same way as on-prem resources to protect resources at a branch location.
G-2.3.e	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.

Demo ID	Expected Outcome	Observed Outcome	Comments
G-2.3.f	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-3.1.a, c, e	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-3.1.b, d, f	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-3.2.a, c, e	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-3.2.b, d, f	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-3.3.a, c, e	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-3.3.b, d, f	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-4	N/A	N/A	Enterprise does not currently have a cloud component. Use cases cannot be performed.
G-5.1	Access Successful	Access Successful	Policies are applied to the resource for both inbound and outbound communication. In this case, secure communications are between the application and the endpoint. CSW can allow or deny communication with the endpoint by enforcing policies on the resource itself. CSW does not push policies or perform administrative actions to the endpoint.

E.3 Enterprise 3 Build 3 (E3B3) Detailed Demonstration Results

Table E-3 lists the full demonstration results for all SDP and Microsegmentation phase demonstrations run in Enterprise 3 Build 3 (E3B3). In all demonstrations that we attempted to conduct, the ZTA functionality included in the build performed as expected. The technology deployed in E3B3 was able to determine endpoint compliance for Windows, macOS, and mobile devices and prevent noncompliant endpoints from accessing private resources.

2026 Table E-3 Detailed Demonstration Results for E3B3 SDP and Microsegmentation Phase

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

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.2.a-m	Access to Network	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
A-1.3.a	Access to Network	Access to Network	Success: Endpoint has access to network in accordance with Forescout policy.
A-1.3.b	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-1.3.c	No Access to Network	No Access to Network	Success: Endpoint is denied access to the network after failing to authenticate to the GlobalProtect VPN.
A-1.3.d	Access to Network	Access to Network	Success: BYOD has access to network in accordance with Forescout policy.
A-1.3.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-1.3.f	No Access to Network	No Access to Network	Success: BYOD is denied access to the network after failing to authenticate to the GlobalProtect VPN.
A-1.4.a-g	N/A	N/A	Partial Success: Using Azure roles, a user could be allowed, denied, or provided with limited access to cloud resources. With Azure AD Conditional Access and Microsoft Intune, a device can be given access to a cloud application.
A-2.1.a	Keep Access to Network	Keep Access to Network	Success: Resource has access to network in accordance with Forescout policy.
A-2.1.b	Terminate Access to Network	Limit Access to Network	Partial Success: Resource has access limited to the local subnet in accordance with Forescout policy.

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

Demo ID	Expected Outcome	Observed Outcome	Comments
A-2.3.d	Keep Access to Network	Keep Access to Network	Success: BYOD has access to network in accordance with Forescout policy.
A-2.3.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: BYOD has access limited in accordance with Forescout policy.
A-2.3.f	Terminate Access to Network	Terminate Access to Network	Success: BYOD has access terminated after failing to reauthenticate to the GlobalProtect VPN.
A-2.4.a,d	Keep Access to Network	Keep Access to Network	Success: Azure is able to allow access to cloud endpoints and resources.
A-2.4.b,c,f	Terminate Access to Network	Terminate Access to Network	Success: Azure is able to limit access to cloud endpoints and resources.
A-2.4.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: Azure is able to limit access to cloud endpoints and resources.
A-3.1.a	User request and action is recorded	User request is recorded	Partial Success: User activity and transaction flow is logged using Forescout. Individual user actions are not visible within this build.
A-3.2.a	User request and action is recorded	User request is recorded	Partial Success: User activity and transaction flow is logged using Forescout and Azure AD. Individual user actions are not visible within this build.
A-3.3.a, A-3.4.a	User request and action is recorded	N/A	Branch testing is not available for this build.
A-3.5.a, A-3.6.a	User request and action is recorded	User request is recorded	Partial Success: User activity and transaction flow is logged. Individual user actions are not visible.
A-3.1.b, A-3.2.b, A-3.3.b, A-3.4.b	API call is recorded	Activity and transaction	Partial Success: Service activity and transaction flow is logged by

Demo ID	Expected Outcome	Observed Outcome	Comments
		flow is recorded	Forescout. Individual API calls are not visible.
B-1.1.a	Access Successful	Access Successful	Success: Users access RSS1 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.1.b	Access Successful	Access Successful	Success: Users access RSS2 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.1.c	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.1.d	Access Not Successful	Access Not Successful	Success: E2 is not authorized to access RSS1 in accordance with Azure AD policy.
B-1.1.e	Access Successful	Access Successful	Success: Users access RSS2 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.1.f, B-1.1.g	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.1.h	Access Successful	Access Successful	Success: Session timeout is set to one minute for demonstration purposes. After session timed out, user was reauthenticated to Azure AD.
B-1.1.i	Access Not Successful	Access Not Successful	Success: Users were prevented from accessing resources after reauthentication failure to Azure AD.
B-1.1.j	Access Not Successful	Access Not Successful	Success: Initial user authentication to Azure AD was successful and user was granted access to RSS1. After E1 became noncompliant, user access to RSS1 was blocked in accordance with Forescout policy, and the user was unable to re-authenticate to Azure AD.
B-1.1.k	Access Limited	Access Not Successful	Partial success: Initial user authentication to Azure AD was successful and user was granted access to RSS2. In this case, changing the user's access level on RSS2 would

Demo ID	Expected Outcome	Observed Outcome	Comments
			require application-level control that is not available at this time. After E1 became noncompliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to reauthenticate to Azure AD.
B-1.1.l	Access Not Successful	Access Not Successful	Success: After E1 became noncompliant, user access to RSS1 was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.1.m	Access Limited	Access Not Successful	Partial success: In this case, changing the user's access level on RSS2 would require application-level control that is not available at this time. After E1 became noncompliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.1.n-p	Access Not Successful	Access Not Successful	Success: After the RSS became noncompliant, user access to the RSS was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.2.a-p	N/A	N/A	Cannot test because there is no branch office in Ent. 3.
B-1.3.a-p			The results are the same as B-1.1, given that network policies allow the user/device to access the enterprise remotely using a VPN connection. See results from B-1.1.
B-1.4.a	Access Successful	Access Successful	Success: Users access RSS1 based on the EP compliance with Forescout and Azure AD policy.
B-1.4.b	Access Successful	Access Successful	Success: Users access RSS2 based on the EP compliance with Forescout and Azure AD policy.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.4.c	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.4.d	Access Not Successful	Access Not Successful	Success: E2 is not authorized to access RSS1 in accordance with Azure AD policy.
B-1.4.e	Access Successful	Access Successful	Success: Users access RSS2 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.4.f, B-1.4.g	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.4.h	Access Successful	Access Successful	Success: Session timeout is set to one minute for demonstration purposes. After session timed out, user was reauthenticated to Azure AD.
B-1.4.i	Access Not Successful	Access Not Successful	Success: Users were prevented from accessing resources after reauthentication failure to Azure AD.
B-1.4.j	Access Not Successful	Access Not Successful	Success: Initial user authentication to Azure AD was successful and user was granted access to RSS1. After E1 became noncompliant, user access to RSS1 was blocked in accordance with Forescout policy, and the user was unable to reauthenticate to Azure AD.
B-1.4.k	Access Limited	Access Not Successful	Partial success: Initial user authentication to Azure AD was successful and user was granted access to RSS2. In this case, changing the user’s access level on RSS2 would require application-level control that is not available at this time. After E1 became noncompliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to reauthenticate to Azure AD.
B-1.4.l	Access Not Successful	Access Not Successful	Success: After E1 became noncompliant, user access to RSS1 was

Demo ID	Expected Outcome	Observed Outcome	Comments
			blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.4.m	Access Limited	Access Not Successful	Partial success: In this case, changing the user's access level on RSS2 would require application-level control that is not available at this time. After E1 became noncompliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.4.n-p	N/A	N/A	Demonstration cannot be performed as verification of cloud resource compliance is not available at this time.
B-1.5.a-p	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
B-1.6.a-p			In the current implementation, remote users are connected to a VPN that routes network traffic through the on-prem environment. All test results are similar to B-1.4.a-p.
B-2.1.a-d,g,n	Access Successful	Access Successful	Success: Access allowed in accordance with Forescout policy.
B-2.1.e, f, l, m, o, p	Access Not Successful	Access Not Successful	Success: Access denied in accordance with Forescout policy.
B-2.2	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
B-2.3			In the current implementation, remote users are connected to a VPN that routes network traffic through the on-prem environment. All test results are similar to B-2.1.a-p.
B-3.1.a, B-3.4.a, B-3.5.a	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-3.1.b, B-3.4.b, B-3.5.b	Real Req Fail	Real Req Fail	Success: Incorrect credentials were entered, and the Real Request failed as expected.
B-3.1.c, B-3.4.c, B-3.5.c	Limit Access for Real Request, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.d, B-3.4.d, B-3.5.d	Real Request Keep Access, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.e, B-3.4.e, B-3.5.e	Hostile Request Successful	Hostile Request Successful	Success: Hostile Request successfully authenticated.
B-3.1.f, B-3.4.f, B-3.5.f	Hostile Request Unsuccessful	Hostile Request Unsuccessful	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.g, B-3.4.g, B-3.5.g	Real Request Fail, Hostile Request Access Limited	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.h, B-3.4.h, B-3.5.h	Real Request Fail, Hostile Request remains authenticated	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.i, B-3.4.i, B-3.5.i	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.
B-3.1.j, B-3.4.j, B-3.5.j	Real Request remains authenticated, Hostile Request Fail	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-3.1.k, B-3.4.k, B-3.5.k	Hostile Request Fail	Hostile Request Fail	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.l, B-3.4.l, B-3.5.l	Real Request Access Successful	Real Request Access Successful	Success: Real Request successfully reauthenticated.
B-3.1.m, B-3.4.m, B-3.5.m	Hostile Request Access Denied	Hostile Request Access Denied	Success: Hostile Request reauthentication fails.
B-3.1.n, B-3.4.n, B-3.5.n	Hostile Request Session Terminated	Hostile Request Session Terminated	Success: Azure AD sessions terminated.
B-3.1.o, B-3.4.o, B-3.5.o	Real Request Session Terminated	Real Request Session Terminated	Success: Azure AD sessions terminated.
B-3.2, B-3.3	N/A	N/A	Branch office is not included in Build 3.
B-4			All demonstrations here are the same as B-1 since the device is both authenticated and compliant.
B-5			All demonstrations here are the same as B-2 since the device is both authenticated and compliant.
B-6			All demonstrations here are the same as B-3 since the device is both authenticated and compliant.
B-7	Success	Partial Success	Partial Success: Just-in-time privileges were demonstrated. The enterprise was configured to allow a subset of users to gain privileges necessary to perform specific tasks within the Azure cloud environment. This build does not have the capabilities that allow just-in-

Demo ID	Expected Outcome	Observed Outcome	Comments
			time access to extend beyond the cloud to the on-premises environment.
B-7.1.h, j, l, af, ah, aj	Access Successful	Access Successful	Success: Demonstration successful to IaaS, PaaS, and SaaS services.
B-7.1.g, i, k, ae, ag, ai	Access Not Successful	Access Not successful	Success: Demonstration successful to IaaS, PaaS, and SaaS services.
B-7.1.a-b, B-7.1.e-f, B-7.1.y-z, B-7.1.ac-ad	N/A	N/A	Unable to complete demonstration. Current build does not have the capability to extend just-in-time privileges beyond cloud environment.
B-7.1.c, d, m, n, o, p, q, r, s, t, u, v, w, x, aa, ab	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
B-8.1.a-r	N/A	N/A	Unable to complete demonstration. Current build could not extend step-up authentication capability to third-party on-prem applications or services.
B-8.2.a-r	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
B-8.3.a-r	N/A	N/A	Unable to complete demonstration. Current build could not extend step-up authentication capability to third-party IaaS services.
B-8.4.a-c	Session Continues	Session Continues	Success: Demonstration successful for connections to PaaS service.
B-8.4.d-f	Session Terminates	Session Terminates	Success: Demonstration successful for connections to PaaS service.
B-8.4.g-l	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
B-8.4.m-o	Session Continues	Session Continues	Success: Demonstration successful for connections to PaaS service.
B-8.4.p-r	Session Terminated	Session Terminated	Success: Demonstration successful for connections to PaaS service.
B-8.5.a-c	Session Continues	Session Continues	Success: Demonstration successful for connections to SaaS service.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-8.5.d-f	Session Terminated	Session Terminated	Success: Demonstration successful for connections to SaaS service.
B-8.5.g-l	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
B-8.5.m-o	Session Continues	Session Continues	Success: Demonstration successful for connections to SaaS service.
B-8.5.p-r	Session Terminated	Session Terminated	Success: Demonstration successful for connections to SaaS service.
All C Use Cases	N/A	N/A	Demonstrations cannot be performed. Currently, no federation configuration has been set up between Ent3 and Ent4.
All D Use Cases			All demonstrations here are the same as B since the device is both authenticated and compliant. Note that the user is a contractor.
E-1.1.a,b	Access Successful	Access Successful	Success: Guests can access public resources and internet in accordance with policy using Forescout.
E-1.2.a,b	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
F-1.1.a, F-1.3.a	Session stays active	Session stays active	Success: If a user successfully reauthenticates when prompted, session remains active. If reauthentication fails, user will lose access to resources. Note: Default reauthentication period is 1 hour and is configurable to a shorter duration. However, Microsoft does not endorse short reauthentication periods. An alternative is to prompt for reauthentication to specific resources that are of higher sensitivity.
F-1.1.b, F-1.3.b	Session Terminated	Session Terminated	Success: If a user fails reauthentication, the user will lose access to resources.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-1.2, F-1.5	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
F-1.4.a, F-1.6.a	Session stays active	Session stays active	Success: If a user successfully reauthenticates when prompted, session remains active. If reauthentication fails, user will lose access to resources. Note: Default reauthentication period is 1 hour and is configurable to a shorter duration. However, Microsoft does not endorse short reauthentication periods. An alternative is to prompt for reauthentication to specific resources that are of higher sensitivity.
F-1.4.b, F-1.6.b	Session Terminated	Session Terminated	Success: If a user fails reauthentication, the user will lose access to resources.
F-2.1.a, F-2.3.1a, F-2.4.a, F-2.6.a	Session stays active	Session stays active	Success: Session stayed active with device reauthentication.
F-2.1.b, F-2.3.1b, F-2.4.b, F-2.6.b	Session Terminated	Session Terminated	Success: Once device reauthentication fails, access to resources from the endpoint is lost.
F-2.2, F-2.5	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-3	N/A	N/A	For this build, resource authentication was not tested; if time permits we can test in the future.
F-4.1.a, F-4.3.a, F-4.4.a, F-4.6.a	Session stays active	Session stays active	Success: Requestor can continue with already established sessions with devices that remain compliant.
F-4.1.b, F-4.3.b, F-4.4.b, F-4.6.b	Session Terminated	N/A	Partial Success: While session may not be immediately terminated, continued access to resource was blocked once compliance determination performed at intervals was made.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-4.2.a-b, F-4.5.a-b,	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-5.1.a, F-5.3.a, F-5.4.a, F-5.6.a	Access Not Successful	Access Not Successful	Success: Access was denied with requestor's noncompliant endpoints.
F-5.1.b, F-5.3.b, F-5.4.b, F-5.6.b	Access Successful	Access Successful	Success: Requestors were allowed access to resource with positive compliance determination.
F-5.2, F-5.5	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-6	N/A	N/A	For this build, this use case was not tested; if time permits we can test in the future.
F-7	N/A	N/A	For this build, this use case was not tested; if time permits we can test in the future.
F-8.1.a, c, d, f, g, i, j, l	Access Stopped	Access Stopped	Success: Demonstration successful. Resource access blocked.
F-8.1.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-8.2.a, c, d, f, g, i, j, l	Access Stopped	Access Stopped	Success: Demonstration successful. Resource access blocked.
F-8.2.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-8.3.a-l	Access Stopped	N/A	Unable to stop resource access on an unmanaged endpoint since the endpoint is guest and doesn't have any management software.
F-9.1.a, c, d, f, g, i, j, l,	Access Stopped	Access Stopped	Success: Demonstration successful. Resource access blocked.
F-9.1.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-9.2.a, c, d, f, g, i, j, l	Access Stopped	Access Stopped	Success: Demonstration successful. Resource access blocked.
F-9.2.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-9.3	N/A	N/A	Unable to stop resource access on an unmanaged endpoint since the endpoint is guest and doesn't have any managemt software.
F-10.1.a-d, i-p, u-z, aa, ab, ag-an, as-av	Access Not Successful	Access Not Successful	Success: Demonstration successful. Enterprise user's access disabled.
F-10.1.e-h, q-t, ac-af, ao-ar	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-10.2.a-d, i-p, u-z, aa, ab, ag-an, as-av	Access Not Successful	Access Not Successful	Success: Demonstration successful. Enterprise user's access disabled.
F-10.2.e-h, q-t, ac-af, ao-ar	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-10.3.a-d, i-p, u-z, aa, ab, ag-an, as-av	Access Not Successful	Access Not Successful	Success: Demonstration successful. Enterprise user's access disabled.
F-10.3.e-h, q-t, ac-af, ao-ar	N/A	N/A	Success: Demonstration successful. Enterprise user's access disabled.
F-11.1.a-d, i-p, u-z, aa, ab, ag-an, as-av	Active Session Terminated	Active Session Terminated	Success: Demonstration successful. Enterprise user's active session terminated.
F-11.1.e-h, q-t, ac-af, ao-ar	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-11.2.a-d, i-p, u-z, aa, ab, ag-an, as-av	Active Session Terminated	Active Session Terminated	Success: Demonstration successful. Enterprise user's active session terminated.
F-11.2.e-h, q-t, ac-af, ao-ar	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-11.3.a-d, i-p, u-z, aa, ab, ag-an, as-av	Active Session Terminated	Active Session Terminated	Success: Demonstration successful. Enterprise user's active session terminated.
F-11.3.e-h, q-t, ac-af, ao-ar	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-12.1.a-d, i-p, u-z, aa, ab, ag-an, as-av	Access not Successful	Access not Successful	Success: Demonstration successful. User's access disabled.
F-12.1.e-h, q-t, ac-af, ao-ar	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-12.2.a-d, i-p, u-z, aa, ab, ag-an, as-av	Access not successful	Access not successful	Success: Demonstration successful. User's access disabled.
F-12.2.e-h, q-t, ac-af, ao-ar	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-12.3.a-d, i-p, u-z, aa, ab, ag-an, as-av	Access not successful	Access not successful	Success: Demonstration successful. User's access disabled.
F-12.3.e-h, q-t, ac-af, ao-ar	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-13.1.a-d, i-p, u-z, aa, ab, ag-an, as-av	Active Session Terminated	Active Session Terminated	Success: Demonstration successful. User's active session terminated.
F-13.2.e-h, q-t, ac-af, ao-ar	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-13.3.a-d, i-p, u-z, aa, ab, ag-an, as-av	Active Session Terminated	Active Session Terminated	Success: Demonstration successful. User's active session terminated.
F-14.1.a, c, d, f, g, i, j, l	Access Not Successful	Access Not Successful	Success: Access to resource was denied from endpoints identified as high risk.
F-14.1.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-14.2.a, c, d, f, g, i, j, l	Access Not Successful	Access Not Successful	Success: Access to resource was denied from endpoints identified as high risk.
F-14.2.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-14.3	N/A	N/A	Unable to classify an unmanaged endpoint as high risk based on detected suspicious activity, since the endpoint is guest and doesn't have any management software.
F-15.1.a, c, d, f, g, i, j, l	Access Not Successful	Access Not Successful	Success: Access to resource was denied from endpoints identified as high risk.
F-15.1.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-15.2.a, c, d, f, g, i, j, l	Access Not Successful	Access Not Successful	Success: Access to resource was denied from endpoints identified as high risk.
F-15.2.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-15.3	N/A	N/A	Unable to classify an unmanaged endpoint as high risk based on detected suspicious activity, since the endpoint is guest and doesn't have any management software.
F-16.1.a, c, d, f, g, i, j, l	Access Stopped	Access Stopped	Success: Session was terminated from an endpoint with suspicious activity.
F-16.1.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-16.2.a, c, d, f, g, i, j	Access Stopped	Access Stopped	Success: Session was terminated from an endpoint with suspicious activity.
F-16.2.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.

Demo ID	Expected Outcome	Observed Outcome	Comments
F-16.3	N/A	N/A	Unable to classify an unmanaged endpoint as high risk based on detected suspicious activity, since the endpoint is guest and doesn’t have any management software.
F-17.1.a, c, d, f, g, i, j, l	Access Stopped	Access Stopped	Success: Session was terminated from an endpoint with suspicious activity.
F-17.1.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-17.2.a, c, d, f, g, i, j, l	Access Stopped	Access Stopped	Success: Session was terminated from an endpoint with suspicious activity.
F-17.2.b, e, h, k	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
F-17.3	N/A	N/A	Unable to classify an unmanaged endpoint as high risk based on detected suspicious activity, since the endpoint is guest and doesn’t have any management software.
G-1.1	N/A	N/A	Demonstration could not be completed. Chosen on-premises application in the lab does not provide authenticated API access to client applications using access tokens issued by an external authorization server.
G-1.2	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
G-2.1.a, e	Access successful	Access successful	Success: API calls made using the appropriate Azure roles were successfully made to Azure IaaS.
G-2.1.b, f	Access not successful	Access not successful	Success: API calls from client apps without the right Azure roles were denied

Demo ID	Expected Outcome	Observed Outcome	Comments
G-2.1.c, d	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
G-2.2.a, e	Access successful	Access successful	Success: API calls from client apps leveraging Azure AD as authorization server were successfully made to read Azure AD user profiles.
G-2.2.b, f	Access not successful	Access not successful	Success: API calls to update Azure AD user profiles from client apps without the right permissions were denied.
G-2.2.c, d	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
G-2.3.a, e	Access successful	Access successful	Success: API calls from client apps leveraging Azure AD as authorization server were successfully made to Outlook Online.
G-2.3.b, f	Access not successful	Access not successful	Success: API calls to Outlook Online from client apps without the correct permissions were denied.
G-2.3.c, d	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
G-3.1.a, c	Access successful	Access successful	Success: API calls from client apps leveraging Azure AD as authorization server and hosted on Azure VMs or Azure Functions were successfully made to manage Azure AD users and VMs.
G-3.1.b, d	Access not successful	Access not successful	Success: API calls from client apps hosted on Azure VMs or Azure Functions attempting to manage Azure AD users or Azure VMs without authorization were denied access.
G-3.1.e, f	N/A	N/A	For this build, this use case was not tested; if time permits we can test in the future.

Demo ID	Expected Outcome	Observed Outcome	Comments
G-3.2.a, c	Access successful	Access successful	Success: API calls from client apps leveraging Azure AD as authorization server and hosted on Azure VMs or Azure Functions were successfully made to manage Azure AD users and VMs.
G-3.2.b, d	Access not successful	Access not successful	Success: API calls from client apps hosted on Azure VMs or Azure Functions attempting to manage Azure AD users or Azure VMs without authorization were denied access.
G-3.2.e	Access successful	Access successful	Success: Microsoft Sentinel playbooks were used to make successful API calls to Azure AD.
G-3.2.f	N/A	N/A	For this build, this use case was not tested; if time permits we can test in the future.
G-3.3.a, c	Access successful	Access successful	Success: API calls from client apps leveraging Azure AD as authorization server and hosted on Azure VMs or Azure Functions were successfully made to manage Outlook online mail.
G-3.3.b, d	Access not successful	Access not successful	Success: API calls from client apps hosted on Azure VMs or Azure Functions attempting to manage mailboxes in Outlook Online without authorization were denied access.
G-3.3.e	Access Successful	Access Successful	Success: Microsoft 365 Defender Portal forwards alerts and incidents to Microsoft Sentinel.
G-3.3.f	N/A	N/A	For this build, this use case was not tested; if time permits we can test in the future.
G-5.1.a, c, d, f, m, o, p, r	Access Successful	Access Successful	Success: Microsoft Intune initiates various actions to endpoints.

Demo ID	Expected Outcome	Observed Outcome	Comments
G-5.1.b, e, n, q	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
G-5.1.g-l	N/A	N/A	In this build, services used to communicate with endpoints are SaaS and not PaaS.

E.4 Enterprise 1 Build 4 (E1B4) Detailed Demonstration Results

Table E-4 lists the full demonstration results for SDP phase demonstrations run in Enterprise 1 Build 4 (E1B4). In all demonstrations that we attempted to conduct, the ZTA functionality included in the build performed as expected. The technology deployed in E1B4 was able to determine endpoint compliance for Windows, Linux, macOS, and mobile devices and prevent noncompliant endpoints from accessing private resources.

Table E-4 Detailed Demonstration Results for E1B4 SDP Phase

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.a, A-1.4.a	Access to Network	Access to specific resources	Success: Once a headless client is installed on a resource and policies are applied to it, Appgate can control communications to and from that resource. “Ring fencing,” which denies access to the resource via the resource’s firewall can be configured. Note: headless clients are leveraged to control outbound traffic, although inbound control is possible via “ring fencing.” Also note that headless clients are revalidated every five minutes for compliance.
A-1.1.b-d, A-1.4.b-d	No Access to Network	No Access to Network	Success: If onboarding is not completed, authentication failed, or compliance failed, resource will not have access. Note: while policies can be applied to the resource to deny access to the network or other resources, Appgate recommends using server management technology to perform server health and security. This technology can then feed information about the resource to Appgate to make policy decision about a user and endpoint access to that resource.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.e, i, A-1.2.e, i, A-1.3.a, d, A-1.4.e	Access to Network	Access to Network	Success: EP logs on to Appgate agent. User is given access to specific resources that it is allowed to access, not the entire corporate network. Note: EP and BYOD are onboarded the same way by installing and logging onto an Appgate client.
A-1.1.f, j, A-1.2.f, j, A-1.3.b, e, A-1.4.f	Max. Limited Access to Network	Max. Limited Access to Network	Success: If compliance is not met, user will have access to limited resources. Once compliance is met, user will have access to all resources that are assigned based on policy. Note: EP and BYOD are onboarded the same way by installing and logging onto an Appgate client.
A-1.1.g, k, A-1.2.g, k, A-1.3.c, f, A-1.4.g	No Access to Network	No Access to Network	Success: If user does not successfully authenticate to Appgate, there is no access to network resources. Note: EP and BYOD are onboarded the same way by installing and logging onto an Appgate client.
A-1.1.h, l, m, A-1.2.h, l, m	Access to Public Network	Access to Public Network	Success: User who is not onboarded will have access to the guest Wi-Fi, which allows public network access. All devices that are not onboarded are treated as guests. These devices will have access to the public network.
A-1.2.a-d	N/A	N/A	Currently, there are no resources in the branch office. However, configuration would be identical to resources that are on-prem.
A-2.1.a-c, A-2.2.a-c, A-2.4.a-c	N/A	N/A	Note: reauthentication is not needed, as a headless client for Appgate stays authenticated after initial connection. However, headless clients are re-evaluated every five minutes for compliance.
A-2.1.d, g, A-2.2.d, g, A-2.3.a, d, A-2.4.d	Access to Network	Access to Network	Success: EP logs on to Appgate agent again after it expires. User is given access to resources that it is allowed once reauthentication is successful.
A-2.1.e, h, A-2.2.f, j, A-2.3.b, e, A-2.4.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: After reauthentication, if compliance is not met, user will have access to limited resources only. Once compliance is met, user will have access to all resources that are assigned based on policy. Note: compliance validation is performed when user reauthenticates and it is set to five minutes. If compliance fails, EP will have limited access.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-2.1.f, i, A-2.2.f, i, A-2.3.c, f, A-2.4.f	Terminate Access to Network	No Access to Network	Success: If user does not successfully reauthenticate to Appgate, there is no access to network resources.
A-2.1.h, A-2.2.h	Access to Public Network	Access to Public Network	Success: User who is not onboarded will have access to the guest Wi-Fi, which allows public network access.
All of A-3	API call is recorded	Logs contain relevant API information	Success: Appgate sends all logs to IBM QRadar.
B-1.1-6.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	Success: For both laptop and mobile endpoints, user access to resource RSS1 was successful, with user and endpoint passing authN/authZ and compliance. RSS1 is compliant. A policy is set to check RSS1's compliance prior to allowing access for E1. If RSS1 is not compliant, E1 is denied access to RSS1. Note: For all B-1 use cases, it does not matter where the user's device resides; Appgate policies dictate what resources a user can access. In our use cases, user devices will function the same way on-prem, at a branch office, or a remote site.
B-1.1-6.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	Success: For both laptop and mobile endpoints, user access to resource RSS1 was successful, with user and endpoint passing authN/authZ and compliance. RSS2 is compliant. A policy is set to check RSS2's compliance prior to allowing access for E1. If RSS2 is not compliant, E1 is denied access to RSS2. For E1 access to RSS1, there is no route to RSS1 from E1. A user would not have access out of its device to RSS2.
B-1.1-6.c, B-4.1.c, B-4.2.c, B-4.3.c, D-1.1.c, D-1.2.c, D-1.3.c, D-4.1.c, D-4.2.c, D-4.3.c	Access Not Successful	Access Not Successful	Success: Demonstration completed with user not able to log in to Appgate due to a failed authentication.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1-6.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	Success: For both laptop and mobile endpoints, user access for E2 to resource RSS1 was not successful. Since there is no policy for E2 to access resource RSS1, there is no route out of E2. If E2 tries to reach RSS1, browser will show "This site cannot be reached" because browser traffic was not able to leave E2.
B-1.1-6.e, B-4.1.e, B-4.2.e, B-4.3.e, D-1.1.e, D-1.2.e, D-1.3.e, D-4.1.e, D-4.2.e, D-4.3.e	Access Successful	Access Successful	Success: For both laptop and mobile endpoints, user access to resource RSS1 was successful, with user and endpoint passing authN/authZ and compliance. Policies applied to RSS2 allows access from the user.
B-1.1-6.f, B-4.1.f, B-4.2.f, B-4.3.f, D-1.1.f, D-1.2.f, D-1.3.f, D-4.1.f, D-4.2.f, D-4.3.f	Access Not Successful	Access Not Successful	Success: Demonstration completed with user not able to log in to resource with a failed authentication.
B-1.1-6.g, B-4.1.g, B-4.2.g, B-4.3.g, D-1.1.g, D-1.2.g, D-1.3.g, D-4.1.g, D-4.2.g, D-4.3.g	Access Not Successful	Access Not Successful	Success: Demonstration completed with user not able to log in to resource with a failed authentication.
B-1.1-6.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: Resource session timeout is set to one minute for demonstration purposes. After session timed out, user was reauthenticated.
B-1.1-6.i, B-4.1.i, B-4.2.i, B-4.3.i, D-1.1.i, D-1.2.i, D-1.3.i, D-4.1.i, D-4.2.i, D-4.3.i	Access Not Successful	Access Not Successful	Success: After session timeout, user tried to login with incorrect password and was denied.
B-1.1-6.j, B-4.1.j, B-4.2.j, B-4.3.j, D-1.1.j, D-1.2.j, D-1.3.j, D-4.1.j, D-4.2.j, D-4.3.j	Access Not Successful	Access Not Successful	Success: Device posture failure detected, so access was denied.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1-6.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	Access Not Successful	Partial success: Access to RSS2 is blocked. Currently cannot perform limited access.
B-1.1-6.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 noncompliant. Device posture failure detected. Currently cannot perform limited access.
B-1.1-6.n-p, B-4.1.n-p, B-4.2.n-p, B-4.3.n-p, D-1.1.n-p, D-1.2.n-p, D-1.3.n-p, D-4.1.n-p, D-4.2.n-p, D-4.3.n-p	N/A	N/A	When accessing a resource, resource compliance is checked. If resource is not compliant, Appgate client will deny endpoint access to resource. However, if user does not have a policy to access the resource, the endpoint will be denied access regardless of the resource's compliance state.
B-2	N/A	N/A	For this build, Appgate does not manage access to internet sites. Appgate does not provide secure web gateway (SWG)/cloud access security broker (CASB) functionality, but can control access to public internet sites at the network level. Enterprises that require this capability normally use Appgate Always-On to control/route all egress traffic through Appgate and onsite proxies/inspection tools.
B-3.1.a, B-3.4.a, B-3.5.a	Real Req Success	Real Req Success	Success: Real Request successfully authenticated. Note: For all B3 use cases, unless credentials are reported stolen, a hostile request with correct credentials will have access to the resources.
B-3.1.b, B-3.4.b, B-3.5.b	Real Req Fail	Real Req Fail	Success: Incorrect credentials were entered, and the Real Request failed as expected.
B-3.1.c, B-3.4.c, B-3.5.c	Limit Access for Real Request, Deny Access to	N/A	If the hostile user has the device and credentials, Appgate would not block access. In this case, the user with the stolen credentials needs the Client Profile string to log in to the Appgate client. If a hostile user has both 1st and 2nd factor authentication credentials, access will be successful.

Demo ID	Expected Outcome	Observed Outcome	Comments
	Hostile Request		Appgate can limit new device registration, for example limit to one registered device per user. Note: Appgate has an option to limit the number of logins from a single user. That can be applied. Appgate can limit connections using IP-based geolocation, understanding that GeoIP accuracy may be reduced on WiFi and mobile networks.
B-3.1.d, B-3.4.d, B-3.5.d	Real Request Keep Access, Deny Access to Hostile Request	N/A	Appgate does not stop users from access if all credentials are correct. In this case, since the hostile user failed authentication, there is no access.
B-3.1.e, B-3.4.e, B-3.5.e	Hostile Request Successful	Hostile Request Successful	Success: Hostile Request successfully authenticated.
B-3.1.f, B-3.4.f, B-3.5.f	Hostile Request Unsuccessful	Hostile Request Unsuccessful	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.g, B-3.4.g, B-3.5.g	Real Request Fail, Hostile Request Access Limited	N/A	Appgate does not stop users from access if all credentials are correct. Please see B-3.1.c for capabilities.
B-3.1.h, B-3.4.h, B-3.5.h	Real Request Fail, Hostile Request remains authenticated	N/A	Appgate does not stop users from access if all credentials are correct. Please see B-3.1.c for capabilities.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-3.1.i, B-3.4.i, B-3.5.i	Real Req Success	Real Req Success	Success: Real Request successfully authenticated. In cases where stolen credentials are reported, updates to configuration to change user credentials will deny hostile users.
B-3.1.j, B-3.4.j, B-3.5.j	Real Request remains authenticated, Hostile Request Fail	N/A	Appgate does not stop users from access if all credentials are correct. In cases where stolen credentials are reported, updates to configuration to change user credentials will deny hostile users. Please see B-3.1.c for capabilities.
B-3.1.k, B-3.4.k, B-3.5.k	Hostile Request Fail	Hostile Request Fail	Success: Incorrect credentials were entered, and the Hostile Request failed as expected. In cases where stolen credentials are reported, updates to configuration to change user credentials will deny hostile users.
B-3.1.l, B-3.4.l, B-3.5.l	Real Request Access Successful	Real Requet Access Successful	Success: Real Request successfully reauthenticated. In cases where stolen credentials are reported, updates to configuration to change user credentials will deny hostile users.
B-3.1.m, B-3.4.m, B-3.5.m	Hostile Request Access Denied	Hostile Request Access Denied	Success: Incorrect credentials were entered for reauthentication, and the Hostile Request failed as expected. In cases where stolen credentials are reported, updates to configuration to change user credentials will deny hostile users.
B-3.1.n, B-3.4.n, B-3.5.n	N/A	N/A	In cases where stolen credentials are reported, updates to configuration to change user credentials will deny hostile users.
B-3.1.o, B-3.4.o, B-3.5.o	N/A	N/A	In cases where stolen credentials are reported, updates to configuration to change user credentials will deny hostile users. Real user should receive new credentials.
B-4			All results for B-4 are the same as B-1.
B-5	N/A	N/A	Appgate does not manage access to internet sites. Other tools are needed to manage access to the internet.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-6			All results for B-6 are the same as B-3.
B-7	Success	Partial Success	Partial Success: Just-in-time privileges can be manually completed in Appgate to allow a user to access a resource. However, just-in-time access privileges with automation are not tested and require integration with other zero trust tools which have the capabilities to manage user attributes and notify the Appgate system.
B-8	N/A	N/A	Appgate does not have the ability to control a resource’s privileges. If a resource is considered sensitive, Appgate can create a policy to prompt the user to provide an extra authentication method prior to accessing the resource.
All C Use Cases	N/A	N/A	No Federated-ID setup yet; will be part of future phase.
All D Use Cases			All D use cases are the same as B use cases.
All E Use Cases	N/A	N/A	Appgate SDP considers this out of scope for their products. Other technologies should be used to perform this.
F-1.1a, F-1.2a, F-1.3a, F-1.4a, F-1.5a, F-1.6a	Success	Success	Success: When Appgate prompts for reauthentication, if user successfully authenticates, session remains active. If authentication fails, user will lose access to resources. Note: Default reauthentication period is 24 hours and is configurable to a shorter duration. However, Appgate does not endorse short reauthentication periods due to user experience. An alternative is to prompt for reauthentication to specific resources that are of higher criticality.
F-1.1b, F-1.2b, F-1.3b, F-1.4b, F-1.5b, F-1.6b	Success	Success	Success: When Appgate prompts for reauthentication, if authentication fails, user will lose access to resources. Appgate client will show the failed authentication and no resources will show up in the client.
F-2	Success	Success	Success: Results are the same as F-1. Appgate authenticates user and validates device when user logs onto Appgate agent, and periodically

Demo ID	Expected Outcome	Observed Outcome	Comments
			revalidates device and user authentication and/or MFA based on configuration.
F-3	Success	Partial Success	Partial Success: Once a headless client is authenticated, it reauthenticates automatically using PKI or stored credentials. However, compliance checks are performed periodically. If compliance fails, user will lose access within five minutes.
F-4	Success	Success	Success: Device compliance is checked periodically (set to every five minutes). If compliance fails, Appgate policies deny access to resources.
F-5	Success	Success	Success: Device compliance is checked periodically. If compliance fails, Appgate policies deny access to resources. Once the endpoint is compliant again, Appgate will allow access. Note: compliance is checked every 5 minutes, so access may take up to 5 minutes after the device becomes compliant again.
F-6, F-7, F-8, F-9	N/A	N/A	Appgate does not have this capability.
F-10, F-12	N/A	N/A	Appgate policies dictate whether a user has access to that resource or not. If there is no policy to allow a user to access a resource and the user attempts to reach that resource, the attempt will not be able to leave the end device or it will be denied by the Appgate gateway. If there is no route to that resource, then the request never leaves the endpoint. For example, if a user types in a URL to a resource on a browser, it will return "This site cannot be reached" because browser traffic was not able to leave the device. If there's a policy to access a resource via HTTPS only and the user tries to SSH to that resource, the gateway will deny the SSH connection.
F-11, F-13	N/A	N/A	Appgate does not manage access to internet sites. Other tools are needed to manage access to the internet.
F-14, F-15, F-16, F-17	N/A	N/A	Appgate does not allow any traffic past the Appgate gateway if there is no policy to allow that specific access from the user. Logs of these attempts are

Demo ID	Expected Outcome	Observed Outcome	Comments
			provided to the SIEM. Note: The SIEM can trigger a security event, which Appgate can consume to further restrict that user's access by deeming them more risky.
G-1.1.a, e	Access successful	Access successful	Success: For all service-to-service use cases, headless clients are installed on resources to check compliance, risk score and control communication in and out of that resource. Headless client uniquely identifies both the credentials and the workload. Policy on the subject location will allow the subject to reach the resource. Policies on the resource will allow access by the subject.
G-1.1.b, f	Access not successful	Access not successful	Success: Based on policy, subject was denied from communicating with the resource.
G-1.1.c-d	N/A	N/A	There are no resources currently deployed at a branch location. Tests are not performed. However, the results of a subject at a branch location attempting to reach an on-prem resource would be the same as use case G-1.1a because installation and policies are applied the same way.
G-1.1.g	Access successful	Access successful	Success: A PaaS solution was deployed and policies applied. Access was successful.
G-1.1.h	Access not successful	Access not successful	Success: A PaaS solution was deployed and policies applied. Access to the resource was denied based on policy.
G-1.1.i-j	N/A	N/A	SaaS solutions that allow for Conditional Access can be restricted to Appgate-enabled clients. SaaS that has no option for IP whitelisting cannot be protected by Appgate. Enterprise 1 does not have such a SaaS solution. Optionally, “ringfencing” can be applied to the on-prem resource to allow or deny communications from the SaaS solution.
G-1.2.a-j	N/A	N/A	There are no resources at a branch location. Tests are not performed. However, Appgate would deploy policies the same way as on-prem resources to protect resources at a branch location. An Appgate client would be installed on these resources.

Demo ID	Expected Outcome	Observed Outcome	Comments
G-2.1.a	Access successful	Access successful	Success: Policy on the subject location will allow the subject to reach the resource in IaaS.
G-2.1.b	Access not successful	Access not successful	Success: Based on policy, subject was denied from communicating with the resource.
G-2.1.c-f, G-2.2.c-f, G-2.3.c-f	N/A	N/A	There are no resources currently deployed at a branch or remote location. Tests are not performed. However, the results of a subject at a branch or remote location attempting to reach a cloud resource would be the same as use case G-1.1a because installation and policies are applied the same way.
G-2.2	N/A	N/A	A PaaS resource was created within AWS to show communication from PaaS to an on-premesis protected resource. Connections to the PaaS workload from outside the cluster can be protected by the PEP located in AWS. Therefore, G-2.2 results would be the same as G-2.1.
G-2.3	N/A	N/A	These use cases depend on the SaaS provider's ability to enforce IP-based conditional access. If this option is used, SaaS-bound traffic would flow through an Appgate PEP for policy enforcement. In this build we don't currently have a SaaS application to demonstrate.
G-3	Access Successful	Partial Success	Partial Success: Successful for IaaS and PaaS. These use cases depend on the cloud provider's ability to enforce IP-based conditional access. If this option is used, Cloud-bound traffic would flow through an Appgate PEP for policy enforcement. In this build we don't currently have a SaaS application to demonstrate.
G-4.1.a, b, e, f	N/A	N/A	Although this can be done, Appgate does not recommend deploying this solution, as it can add significant latency to intra-cluster communication.
G-4.1.c	Access Successful	Access Successful	Success: A Kubernetes cluster was deployed and an Appgate sidecar enforces policies applied to the cluster. Access was successful.

Demo ID	Expected Outcome	Observed Outcome	Comments
G-4.1.d	Access not successful	Access not successful	Success: A Kubernetes cluster was deployed and an Appgate sidecar enforces policies applied to the cluster. Access was denied due to policy.
G-5.1.a-f	Access Successful	Access Successful	Success: Access was successful by applying policy to allow access from service to the endpoint.
G-5.1.g	Access Successful	Access Successful	Success: Access was successful by applying policy to allow access from service to the endpoint.
G-5.1.h-l	Access Successful	Access Successful	Success: The results are same as G-5.1g since the policy is applied to the resource only.
G-5.1.m-r	N/A	N/A	These use cases cannot be performed. Appgate does not have the capability to protect SaaS-initiated connections to resources.