NIST SPECIAL PUBLICATION 1800-35C

Implementing a Zero Trust Architecture

Volume C:
How-To Guides

Gema Howell
Alper Kerman
Murugiah Souppaya
National Institute of
Standards and Technology
Gaithersburg, MD

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

Peter Gallagher
Aaron Palermo
Appgate
Coral Gables, FL

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

Kyle Black
Sunjeet Randhawa
Broadcom Software
San Jose, CA

Aaron Rodriguez
Micah Wilson
Cisco
Herndon, VA

Corey Bonnell
Dean Coclin
DigiCert
Lehi, UT

Ryan Johnson
Dung Lam
F5
Seattle, WA

Neal Lucier
Tom May
Forescout
San Jose, CA

Tim Knudsen
Google Cloud
Mill Valley, CA

Harmeet Singh
Krishna Yellepeddy
IBM
Armonk, NY

Corey Lund
Farhan Saifudin
Ivanti
South Jordan, UT

Hashim Khan
Tim LeMaster
Lookout
Reston, VA

James Elliott
David Pricer
Mandiant
Reston, VA

Carmichael Patton
Brandon Stephenson
Microsoft
Redmond, WA

Vinu Panicker
Okta
San Francisco, CA

Andrew Keffalas
Norman Wong
Palo Alto Networks
Santa Clara, CA

Rob Woodworth
Shawn Higgins
PC Matic
Myrtle Beach, SC

Bryan Rosensteel
Mitchell Lewars
Ping Identity
Denver, CO

Wade Ellery
Don Coltrain
Radiant Logic
Novato, CA

Frank Briguglio
Ryan Tighe
SailPoint
Austin, TX

Chris Jensen
Joshua Moll
Tenable
Columbia, MD

Jason White
Trellix, Public Sector
Reston, VA

Jacob Rapp
Paul Mancuso
VMware
Palo Alto, CA

Joe Brown
Jim Kovach
Zimperium
Dallas, TX

Bob Smith
Syed Ali
Zscaler
San Jose, CA

December 2022

SECOND 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 1800-35C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-35C, 90 pages, (December 2022), CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

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

Public comment period: December 21, 2022 through February 6, 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 collaborators—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 the requester's identity and role, the requesting device's health and credentials, and the sensitivity of the resource. 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
Quint Van Deman	Amazon Web Services
Jason Garbis	Appgate
Adam Rose	Appgate
Jonathan Roy	Appgate
Eric Michael	Broadcom Software
Ken Andrews	Cisco
Matthew Hyatt	Cisco
Leo Lebel	Cisco
Tom Oast	Cisco
Peter Romness	Cisco
Steve Vetter	Cisco
Daniel Cayer	F5

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

Name	Organization
Joey Cruz	Microsoft
Tarek Dawoud	Microsoft
Janet Jones	Microsoft
Hemma Prafullchandra	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
Oliver Borchert	NIST
Douglas Montgomery	NIST
Scott Rose	NIST

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

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

** 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 Figures

1 Introduction

The following volume of this guide shows information technology (IT) professionals and security engineers how we implemented five example zero trust architecture (ZTA) solutions. We cover all of the products employed in this reference design.

Note: This is not comprehensive documentation. There are many possible service and security configurations for these products that are out of scope for these demonstrations.

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

When complete, this guide will contain 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 **(you are here)**
- NIST SP 1800-35D: *Functional Demonstrations* – use cases that have been defined to showcase ZTA security capabilities and the results of demonstrating them with each of the example implementations
- 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 National Cybersecurity Center of Excellence (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*.

IT professionals 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 solutions. 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 *Functional Demonstrations,* 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 best practices.

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

1.2 Build Overview

This NIST Cybersecurity Practice Guide addresses the challenge of using standards-based protocols and available technologies to build a ZTA. In our lab at the NCCoE and using our collaborator’s cloud infrastructure, we plan to implement and demonstrate a variety of builds that serve as example ZTA solutions, each of which is designed to dynamically and securely manage access to resources across a set of use cases that a medium or large enterprise might typically deploy. Our plan is to implement these builds in a series of phases, starting with a baseline enterprise architecture that represents the typical legacy components that an enterprise might start with when deciding to begin adding zero trust capabilities.

We began with builds for enhanced identity governance (EIG) that were restricted to a limited set of capabilities. We call these *EIG crawl phase builds*. The central capabilities of these builds are identity, credential, and access management (ICAM) and endpoint protection. In particular, these EIG crawl phase builds do not include the separate, centralized policy engine (PE) or policy administration (PA) components. Instead, these initial EIG crawl phase builds rely upon the PE and PA capabilities provided by their ICAM components. We did not perform an EIG walk phase. After completing the EIG crawl phase builds, we enhanced these implementations by adding specialized PE and PA components, device discovery, and cloud-based resources in the EIG run phase. In future phases, we plan to introduce capabilities such as software-defined perimeter and micro-segmentation.

This practice guide provides instructions for reproducing the builds that we have implemented so far:

- EIG crawl phase builds:
    - EIG Enterprise 1 Build 1 (E1B1)
    - EIG Enterprise 2 Build 1 (E2B1)
    - EIG Enterprise 3 Build 1 (E3B1)
- EIG run phase builds:
    - EIG Enterprise 1 Build 2 (E1B2)
    - EIG Enterprise 3 Build 2 (E3B2)

The NCCoE worked with members of the ZTA community of interest to develop a diverse but non-comprehensive set of use cases and scenarios to demonstrate the capabilities of the builds. The use cases are summarized in NIST SP 1800-35D, *Functional Demonstrations*.

1.2.1 EIG Crawl Phase Build Features

A general ZTA reference design is depicted in Figure 4-1 of Volume B. It consists of ZTA core components: a policy decision point (PDP), which includes both a PE and a PA, and one or more policy enforcement points (PEPs); and ZTA functional components for ICAM, security analytics, data security, and endpoint security. The EIG crawl phase builds that have been created so far differ from this reference design insofar as they do not include separate, dedicated PDP components. Their ICAM component serves as their PDP, and they include very limited data security and security analytics functionality. These limitations were intentionally placed on the initial builds in an attempt to demonstrate the ZTA functionality that an enterprise that currently has ICAM and endpoint protection solutions deployed will be able to support without having to add additional ZTA-specific capabilities.

Each EIG crawl phase build is instantiated in a unique way, depending on the equipment used and the capabilities supported. Briefly, the three builds are as follows:

- E1B1 uses products from IBM, Ivanti, Mandiant, Okta, Radiant Logic, SailPoint, Tenable, and Zimperium. Certificates from DigiCert are also used.
- E2B1 uses products from Cisco Systems, IBM, Mandiant, Palo Alto Networks, Ping Identity, Radiant Logic, SailPoint, and Tenable. Certificates from DigiCert are also used.
- E3B1 uses products from F5, Forescout, Lookout, Mandiant, Microsoft, Palo Alto Networks, PC Matic, and Tenable. Certificates from DigiCert are also used.

1.2.2 EIG Run Phase Build Features

The EIG run phase, as its name suggests, builds upon the EIG crawl phase architecture. The EIG run phase no longer imposes the requirement that the PE and PA components must be provided by the ICAM products used in the build. It also adds capabilities to the EIG crawl phase. In addition to protecting access to resources that are located on-premises, the run phase also protects access to some resources that are hosted in the cloud. The EIG run phase includes a device discovery capability, which is performed as part of the baseline. In addition to monitoring and alerting when new devices are detected, enforcement can be enabled to deny access to devices that are not compliant. The run phase also includes the capability to establish a tunnel between the requesting endpoint and the resource being accessed over which access to the resource can be brokered.

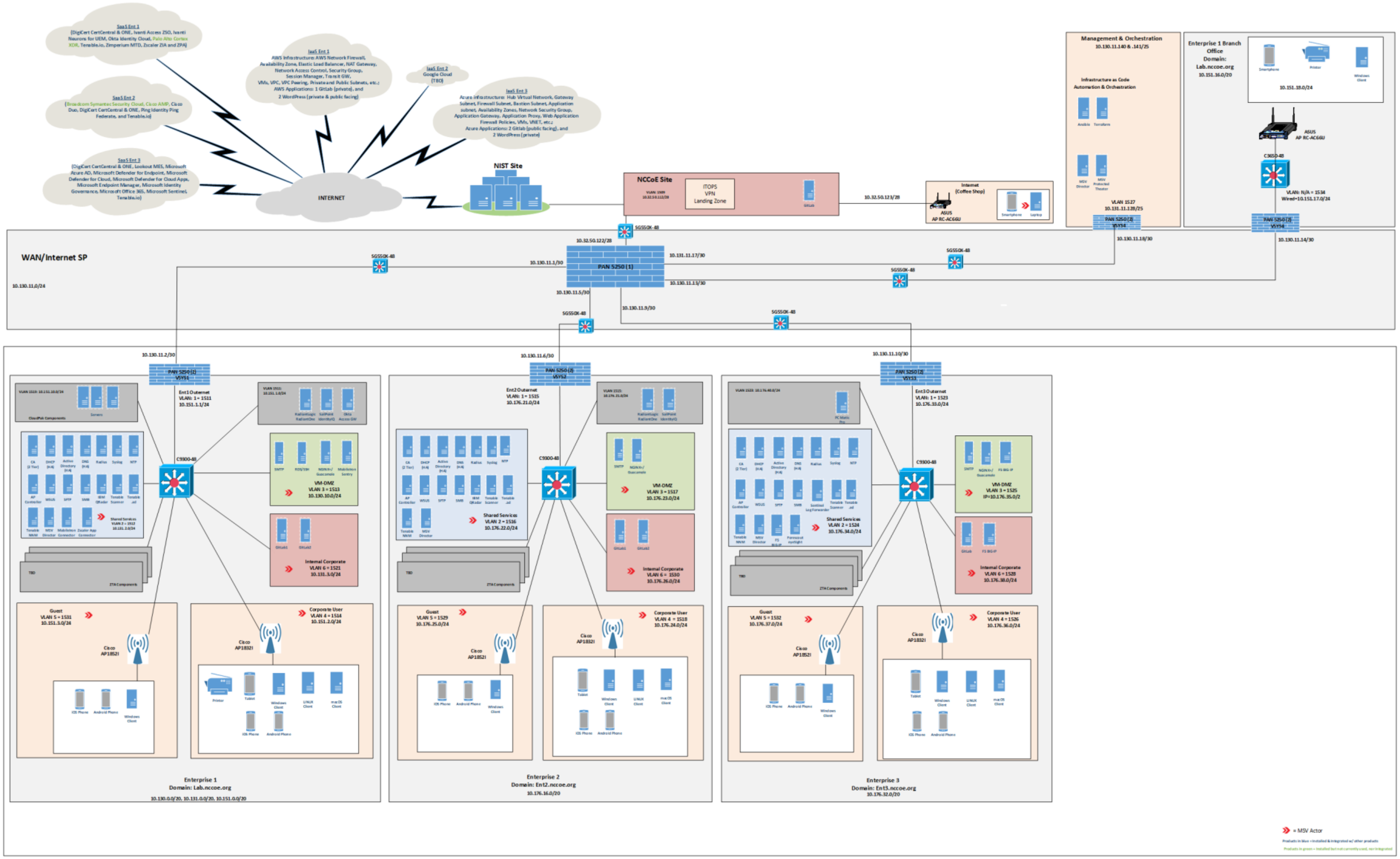
Each EIG run phase build is instantiated in a unique way, depending on the equipment used and the capabilities supported. Briefly, the two builds are as follows:

- E1B2 uses products from Amazon Web Services, IBM, Ivanti, Mandiant, Okta, Radiant Logic, SailPoint, Tenable, and Zscaler. Certificates from DigiCert are also used.
- E3B2 uses products from F5, Forescout, Mandiant, Microsoft, Palo Alto Networks, PC Matic, and Tenable. Certificates from DigiCert are also used.

1.2.3 Physical Architecture Overview

The laboratory environment in which the builds have been implemented is depicted and described in detail in Section 4.3 of Volume B. The laboratory architecture drawing from that volume is reproduced here in Figure 1-1. As shown, this laboratory environment includes three separate enterprise environments, each hosting its own distinct implementation of a ZTA architecture. The enterprises may interoperate as needed by a given use case, and the baseline enterprise environments have the flexibility to support enhancements. The laboratory environment also includes a management virtual local area network (VLAN) on which the following components are installed: Ansible, Terraform, MSV Director, and MSV Protected Theater. These management components support infrastructure as code (IaC) automation and orchestration.

Figure 1-1 Laboratory Infrastructure for the EIG Builds



The following EIG phase builds are supported within the physical architecture depicted in Figure 1-1 and documented in the remainder of this guide:

- EIG E1B1 components consist of DigiCert CertCentral, IBM Cloud Pak for Security, IBM Security QRadar XDR, Ivanti Access ZSO, Ivanti Neurons for UEM, Ivanti Sentry, Ivanti Tunnel, Mandiant Security Validation (MSV), Okta Identity Cloud, Okta Verify App, Radiant Logic RadiantOne Intelligent Identity Data Platform, SailPoint IdentityIQ, Tenable.ad, Tenable.io, and Zimperium MTD.
- EIG E2B1 components consist of Cisco Duo, DigiCert CertCentral, IBM Security QRadar XDR, Mandiant MSV, Palo Alto Networks Next Generation Firewall (NGFW), PingFederate, which is a service in the Ping Identity Software as a Service (SaaS) offering of PingOne, Radiant Logic RadiantOne Intelligent Identity Data Platform, SailPoint IdentityIQ, Tenable.ad, Tenable.io, and Tenable Nessus Network Monitor (NNM).
- EIG E3B1 components consist of DigiCert CertCentral, F5 BIG-IP, Forescout eyeSight, Lookout MES, Mandiant MSV, Microsoft Azure AD, Microsoft Defender for Endpoint, Microsoft Endpoint Manager, Microsoft Sentinel, Palo Alto Networks NGFW, PC Matic Pro, Tenable.ad, and Tenable.io.
- EIG E1B2 components consist of AWS Infrastructure as a Service (IaaS), DigiCert CertCentral, IBM Cloud Pak for Security, IBM Security QRadar XDR, Mandiant MSV, Okta Identity Cloud, Okta Verify App, Radiant Logic RadiantOne Intelligent Identity Data Platform, SailPoint IdentityIQ, Tenable.ad, Tenable.io, Tenable NNM, Zscaler Admin Portal, Zscaler Application Connector, Zscaler Central Authority, Zscaler Client Connector, Zscaler Internet Access (ZIA) Public Service Edges, and Zscaler Private Access (ZPA) Public Service Edges.
- EIG E3B2 components consist of DigiCert CertCentral, F5 BIG-IP, Forescout eyeControl, Forescout eyeExtend, Forescout eyeSegment, Forescout eyeSight, Mandiant MSV, Microsoft AD, Microsoft Azure AD, Microsoft Azure AD (Conditional Access), Microsoft Azure AD Identity Protection, Microsoft Azure (IaaS), Microsoft Defender for Cloud, Microsoft Defender for Cloud Apps, Microsoft Defender for Endpoint, Microsoft Intune, Microsoft Office 365 (SaaS), Microsoft Sentinel, Palo Alto Networks NGFW, PC Matic Pro, Tenable.ad, Tenable.io, and Tenable NNM.

For a detailed description of the architecture of each build, see Volume B, Appendices D, E, F, H and J. The remainder of this guide describes how to implement the EIG crawl and run phase builds E1B1, E2B1, E3B1, E1B2, and E3B2.

1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide*.
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit.**
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

2 Enterprise 1 Build 1 (EIG E1B1) Technology Guides

This section of the practice guide contains detailed instructions for installing, configuring, and integrating all of the products used to implement EIG E1B1. For additional details on EIG E1B1's logical and physical architectures, please refer to Volume B.

2.1 Okta Identity Cloud

The Okta Identity Cloud is a SaaS solution that provide ICAM capabilities to an enterprise. The following sections describe the setup of the Okta Identity Cloud, the Okta Access Gateway, and the Okta Verify application. Okta integrates with Radiant Logic for identity information, SailPoint to receive governance information, and Ivanti to delegate authentication for users accessing resources using mobile devices.

2.1.1 Configuration and Integration

The purpose of this subsection is to set up NCCoE's own instance of the Okta cloud so it can integrate with other ICAM tools so Okta can manage authentication and authorization of users accessing resources. Most configurations are completed within this instance of the Okta cloud.

1. Sign up for an account with Okta (okta.com) and follow steps to set up an admin account, along with configuring Okta Verify for the admin account. This will allow the admin to start configuring integrations and services.

2. Set up directory integration with Radiant Logic. User identity information is pulled from Radiant Logic into Okta for authentication and authorization. An Okta LDAP agent is installed on the Radiant Logic server for integration. Note: This step should be completed after Radiant Logic is configured.

3. Create Groups for Okta to apply a specific set of users to specific services or applications. This allows for automation of user governance at a large scale rather than manual configuration of individual users.
4. Create API tokens to be used by SailPoint and Radiant Logic for communication. These tokens will allow Okta to give specific read/write privileges to other applications.
5. Create a delegated authentication for Okta to be able to import users from Radiant Logic via LDAP. This allows Okta to delegate the actual authentication to Radiant Logic. Okta does not store or know the password of the user. Note that a service account, created in the Radiant Logic Integration section of this document, needs to be created and used in this configuration.
6. Create application integration via Security Assertion Markup Language (SAML). We have Ivanti Neurons for UEM and 2 GitLab instances in Enterprise 1. Okta Access Gateway (AG) needs to be installed in order to configure on-premises applications. The Okta AG gives the Okta Identity Cloud visibility to the resources inside the enterprise. See Section 2.1.3 for installation instructions, which include information on configuring on-premises applications.
7. Create Identity Provider integration for Ivanti Access ZSO. This will allow delegated authentication for Ivanti for mobile devices. This involves creating a custom application using SAML and then creating a SAML Identity Provider.
8. Configure Device Trust on iOS and Android devices to create device integrations.
9. Create authentication policies. These policies define how users will authenticate. By default, a "Catch All" policy is created when an application is created. We are creating an authentication policy that will allow Okta to trust Ivanti Access ZSO to be the delegated Identity Provider (IdP). To do this, when Okta checks that Okta Verify is a managed application on a device, it will delegate authentication to Ivanti Access ZSO.

2.1.2 Okta Verify App

The Okta Verify app is installed, usually on a mobile device, when a new user is onboarded. It serves as a tool to provide a second factor for authentication. The user can log in to the Okta Identity Cloud for the first time. For this setup, the user will be asked to change their password and perform setup. After the password update, the user can set up Okta Verify. Follow the instructions for Android or iOS devices to install Okta Verify and complete the process.

2.1.3 Okta Access Gateway

The Okta Access Gateway (AG) is part of the Okta Identity Cloud. It can be leveraged to integrate legacy, on-prem applications into the Okta Identity Cloud. Since the Okta Identity Cloud cannot communicate with Enterprise 1 resources directly, the Okta AG acts as a proxy to facilitate that communication. More information on installing and configuring the Okta AG is available online.

2.2 Radiant Logic RadiantOne

Radiant Logic RadiantOne is an ICAM solution that unifies identity data, making access reusable and scalable for the enterprise.

2.2.1 Installation

RadiantOne is to be installed on a Microsoft Windows 2019 server. See the RadiantOne v7.4.1 documentation from the Radiant Logic website for system specifications. Prerequisites are in Chapter 1 of the *RadiantOne Installation Guide*. Note: You need to create an account within the Radiant Logic website in order to access the installation and configuration documentation.

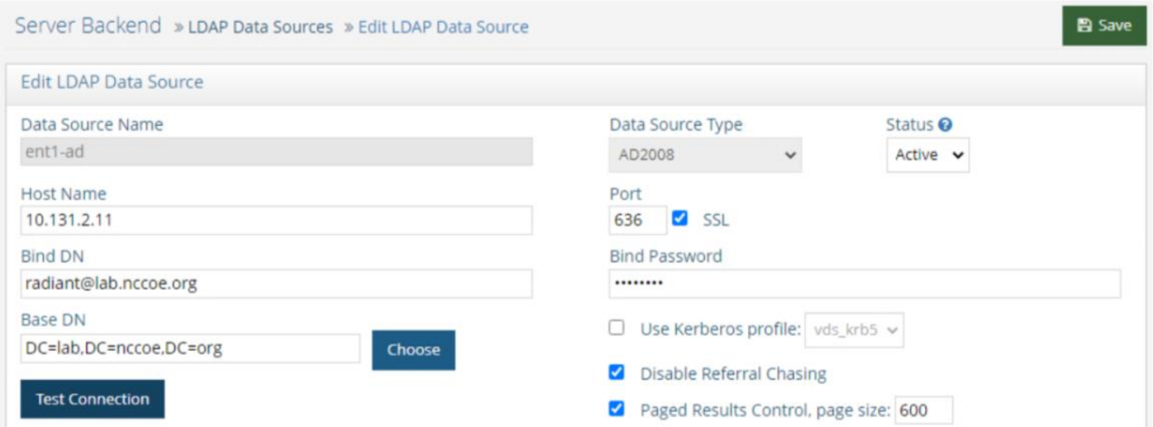
Once you download and launch the executable for a Windows server installation, follow the step-by-step instructions provided on the screen. We used default settings unless specified below. Instructions can also be found in Chapter 2 of the *RadiantOne Installation Guide*.

- Choose **RadiantOne Federated Identity Suite New Cluster/Standalone** for the **Install Set.**
- Provide a name and password for the **Cluster settings.**
- For the **Server Configuration** step, use the following ports: LDAP = 389, LDAPS = 636, and Scheduler Port = 1099.

2.2.2 Configuration

2.2.2.1 Sync with an LDAP server

1. Once installation is complete, log in to RadiantOne from a web browser on the Radiant Logic server, https://localhost:7171. Note: ensure the proper SSL certificate is on the server for HTTPS.
2. Initial configuration is to sync up with an LDAP server. Go to **Settings > Server Backend > LDAP Data Sources.** The screenshot below shows the information created for Enterprise 1 AD. See the *RadiantOne Namespace Configuration Guide* Chapter 3 for details.



Server Backend » LDAP Data Sources » Edit LDAP Data Source

Edit LDAP Data Source

Data Source Name: ent1-ad

Data Source Type: AD2008

Status: Active

Host Name: 10.131.2.11

Port: 636 ☑ SSL

Bind DN: radiant@lab.nccoe.org

Bind Password: ••••••••

Base DN: DC=lab,DC=nccoe,DC=org

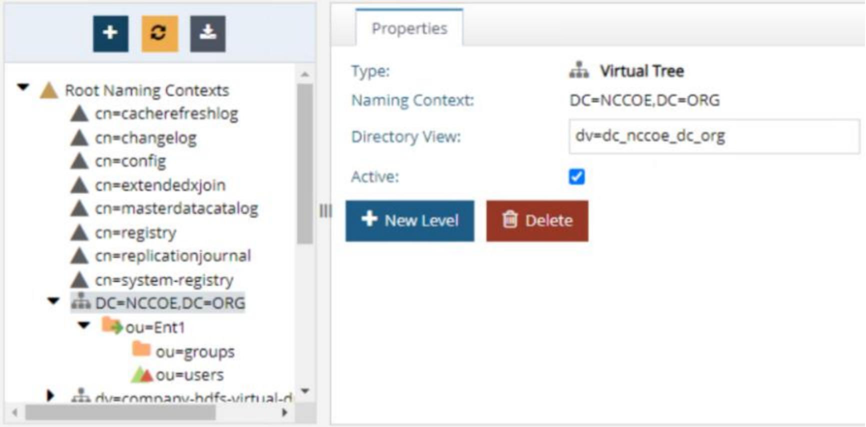
□ Use Kerberos profile: vds_krb5

☑ Disable Referral Chasing

☑ Paged Results Control, page size: 600

3. Once the connection is tested and successful, the integration is completed.

4. Next, create a Directory Namespace by going to **Directory Namespace** and selecting **Create New Naming Context.** Click **Next** and click **OK.**



Root Naming Contexts
- cn=cacherefreshlog
- cn=changelog
- cn=config
- cn=extendedxjoin
- cn=masterdatacatalog
- cn=registry
- cn=replicationjournal
- cn=system-registry
- DC=NCCOE,DC=ORG
  - ou=Ent1
    - ou=groups
    - ou=users
- dv=company-hdfs-virtual-d

Properties

Type: Virtual Tree

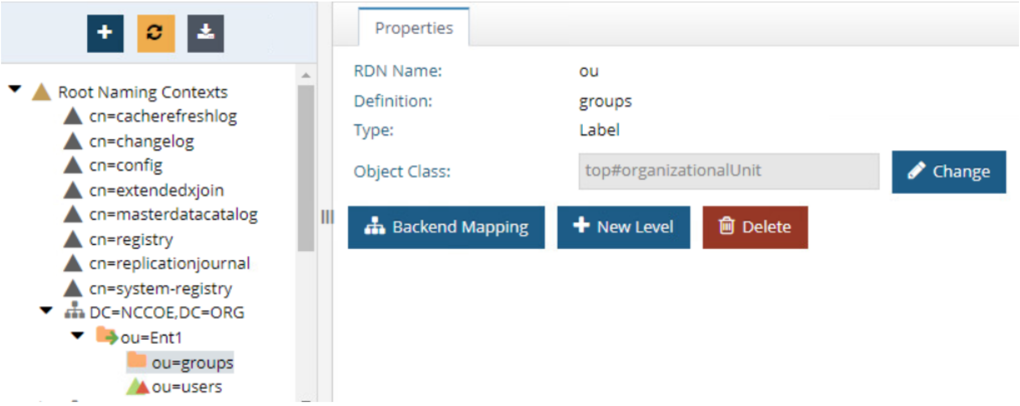
Naming Context: DC=NCCOE,DC=ORG

Directory View: dv=dc_nccoe_dc_org

Active: ☑

5. Find **DC=NCCOE,DC=ORG** under **Root Naming Contexts** on the left side of the screen. Click the **New Level** button. Enter **ent1** as the name for the **OU** and click **OK.**

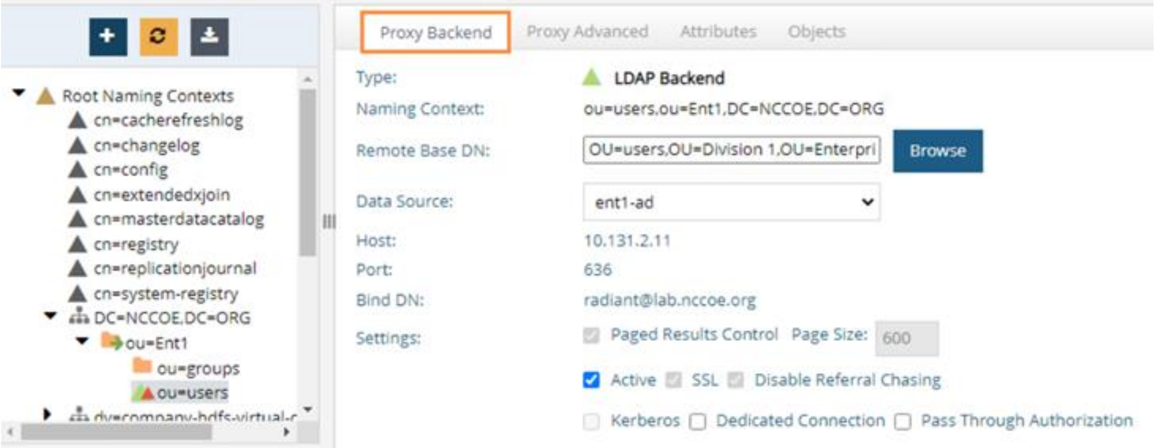
6. Click on **ou=ent1** on the left side and click the **New Level** button on the right to create a sub-ou called **groups.**



RDN Name: ou
Definition: groups
Type: Label
Object Class: top#organizationalUnit

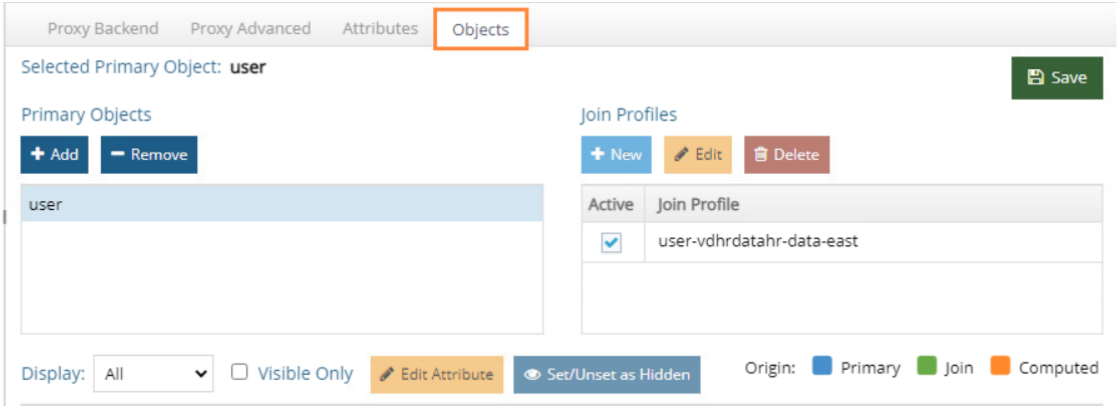
7. Click on **ou=ent1** on the left side as shown below and click the **New Level** button on the right to create a sub-ou called **users.**

8. Once configured and saved, click on **ou=users** and click on **Backend Mapping** on the right. Select **LDAP Backend.** Click **Next** and **Browse** for the proper **Remote Base DN.** Then click **OK.** The screenshot is the completed configuration for the sub-ou users Proxy Backend.



Type: LDAP Backend
Naming Context: ou=users,ou=Ent1,DC=NCCOE,DC=ORG
Remote Base DN: OU=users,OU=Division 1,OU=Enterpri
Data Source: ent1-ad
Host: 10.131.2.11
Port: 636
Bind DN: radiant@lab.nccoe.org
Settings: ☑ Paged Results Control Page Size: 600
☑ Active ☑ SSL ☑ Disable Referral Chasing
□ Kerberos □ Dedicated Connection □ Pass Through Authorization

9. Go to **Objects** and create a primary object and Join Profile by clicking **Add** on each. Click **Save.** Now we have data sources from LDAP and our database.



Selected Primary Object: user

user

Active	Join Profile
☑	user-vdhrdatahr-data-east

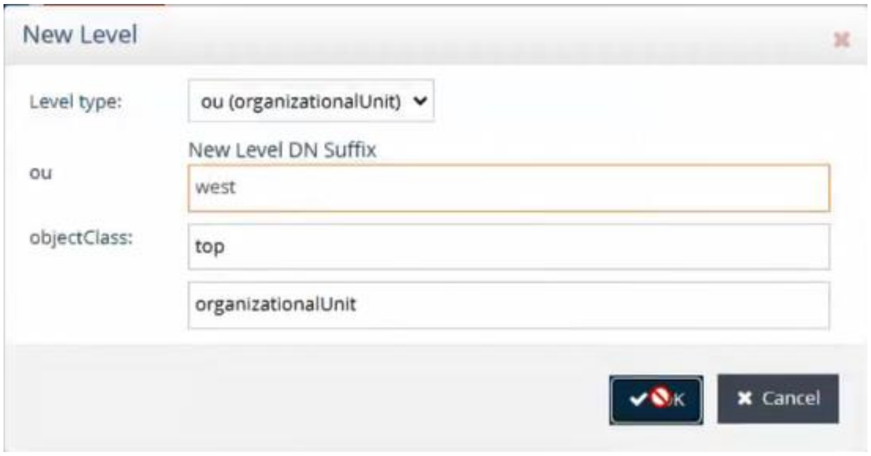
Display: All □ Visible Only

2.2.2.2 Create a namespace to bring in users

1. In **Directory Namespace**, click the **+** sign. Create a naming context: `ou=hr,ou=lab,ou=nccoe,ou=org` and select **Virtual Tree** for the naming context type, then click **Next.**

2. Configure the Virtual Tree by choosing **Create a new view (.dvx),** setting the **Directory View** to `dv=ou_hr_ou_lab_ou_nccoe_ou_org` and clicking **OK**.

3. Next, create a sub-Namespace by clicking the **+ New level** button and entering the information depicted below.



Level type: ou (organizationalUnit)

New Level DN Suffix

ou: west

objectClass: top

organizationalUnit

4. Click on the sub-Namespace that was just created and click on **Backend Mapping**. Specify `ou=east,ou=hr,ou=lab,ou=nccoe,ou=org` as the naming context and select **HDAP Store** as the type, then click **Next**. Note: Instead of having an actual HR database, we are importing sample users from a text file.

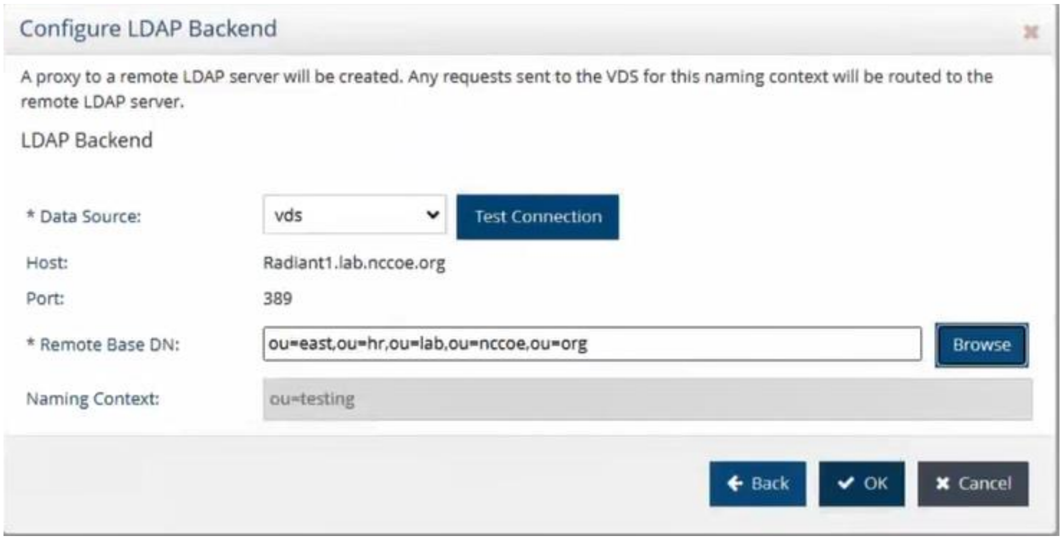
5. Click on **ou=east** to edit properties. Scroll down to the bottom of the screen and click on the **Initialize** button. Then select a file with database users to import for initializing the HDAP store. Note: We are emulating an HR database with this file.

6. Go to the **Directory Browser** tab and refresh the data by clicking the **Refresh Tree** button.

7. Go to the OU that you just configured and expand it. The new users should now be available.

8. Go to **Directory Namespace** and click the **+** button to add new naming context (in our build, we used `ou=testing`). This is used to map to the LDAP backend the database information that was imported.

9. Click on the OU that was created. Click **OK** and **Save**.



Configure LDAP Backend

A proxy to a remote LDAP server will be created. Any requests sent to the VDS for this naming context will be routed to the remote LDAP server.

LDAP Backend

* Data Source: vds

Host: Radiant1.lab.nccoe.org

Port: 389

* Remote Base DN: ou=east,ou=hr,ou=lab,ou=nccoe,ou=org

Naming Context: ou=testing

10. Go to **Directory Browser** and hit the **Refresh** button.

11. Go to **Settings > Configuration > ORX Schema**, and find **OU=Testing** and check it. Click on **Generate LDAP Schema** at the bottom of the screen and click **OK**.

2.2.3 Integration

Other applications, including SailPoint and Okta, will need the following information in order to integrate with Radiant Logic and pull information from it:

- Hostname: radiant1.lab.nccoe.org (hostname of the Radiant Logic server)
- Port: 389 (LDAP) and 636 (LDAPS)

Also, a service account and password need to be created on Radiant Logic for each application to be integrated. The service account is in the form of: `uid=sailpointadmin,ou=globalusers,cn=config`. Follow these steps to create each service account for SailPoint, Okta, and any other desired applications:

1. Go to **Directory Browser.**
2. On the left, go to **cn=config,** then **ou=globalusers** underneath it. Right-click on **ou=globalusers,** click **Add,** then click **New InetOrgPerson.**
3. Fill in the necessary entries. Click **Confirm** to save the configuration.

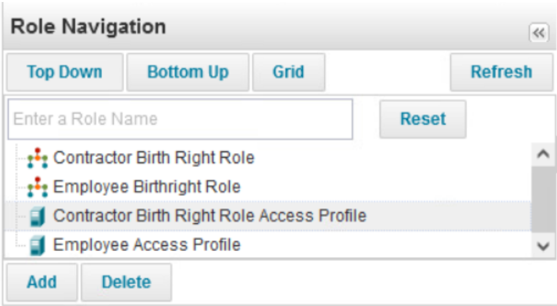
2.3 SailPoint IdentityIQ

SailPoint IdentityIQ is the identity and access management software platform for governing the lifecycle of the enterprise user's identity.

2.3.1 Installation and Configuration

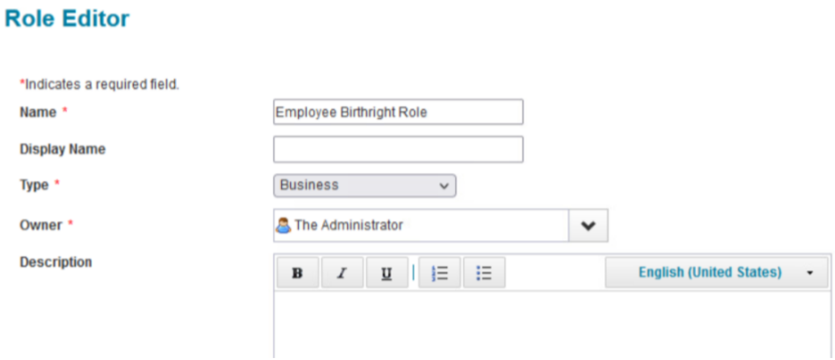
The steps below explain the installation of the IdentityIQ server, initial configuration to import users from the Radiant Logic identity store, and configuration to manage the lifecycle of users.

1. To install IdentityIQ, first identify the platform and prerequisites. For this build, we used Windows 2019 with Apache Tomcat 9.0 and MS SQL Server 2019 as recommended requirements for release 8.2. Download the installation file from the SailPoint website and follow the installation instructions.
2. Login into IdentityIQ from a web browser (http://localhost:8080) using the default login and password identified in the IdentityIQ Installation Guide. Make sure to change the default password by following the instructions provided in the Guide.
3. Configure IQService. This is needed in order to set up integration with AD.
4. Govern permissions by pushing both employee and contractor users and groups to AD and Okta. Note: This step should be completed after the integration with AD and Okta is completed. Steps to configure integration are in Sections 2.3.3 and 2.3.4. After integration with AD and Okta is completed, navigate to the **Setup** drop-down menu and select **Roles**. Here we will create a birthright role and access profile for employees and contractors.
    a. Select **New Role** drop-down button and select **Role**. The screenshot lists the four roles that are created for this build.



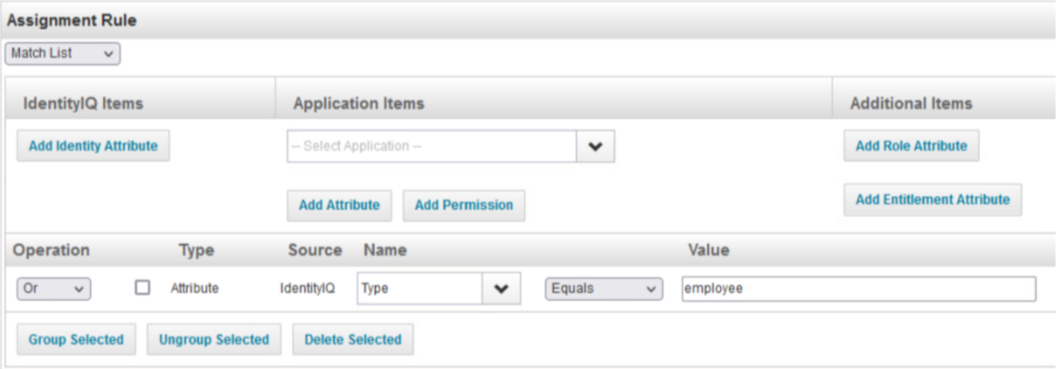
- Contractor Birth Right Role
- Employee Birthright Role
- Contractor Birth Right Role Access Profile
- Employee Access Profile

b. For the **Employee Birthright Role**, use the configuration shown in the next two screenshots. Note that the **Assignment Rule** is where the value of **employee** is used to identify the users. This will push users into AD as a birthright. Once that role is configured, configure the corresponding contractor role the same way. Note that the **Assignment Rule** should be different for the contractor based on user information in SailPoint.



*Indicates a required field.

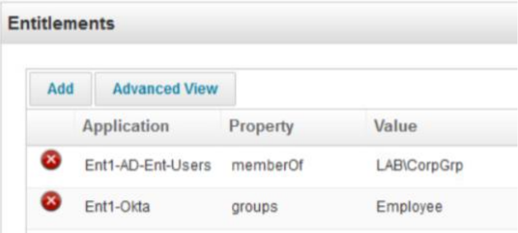
Name *	Employee Birthright Role
Display Name	
Type *	Business
Owner *	The Administrator
Description	



Match List

Operation	Type	Source	Name		Value
Or	□ Attribute	IdentityIQ	Type	Equals	employee

c. For the **Employee Access Profile** role, add the groups that the employees belong to. This means that these users will have access to these groups as a birthright. Perform the same for the corresponding contractor role. Note that the **Entitlements** should be different for the contractor based on group information in Okta and AD.

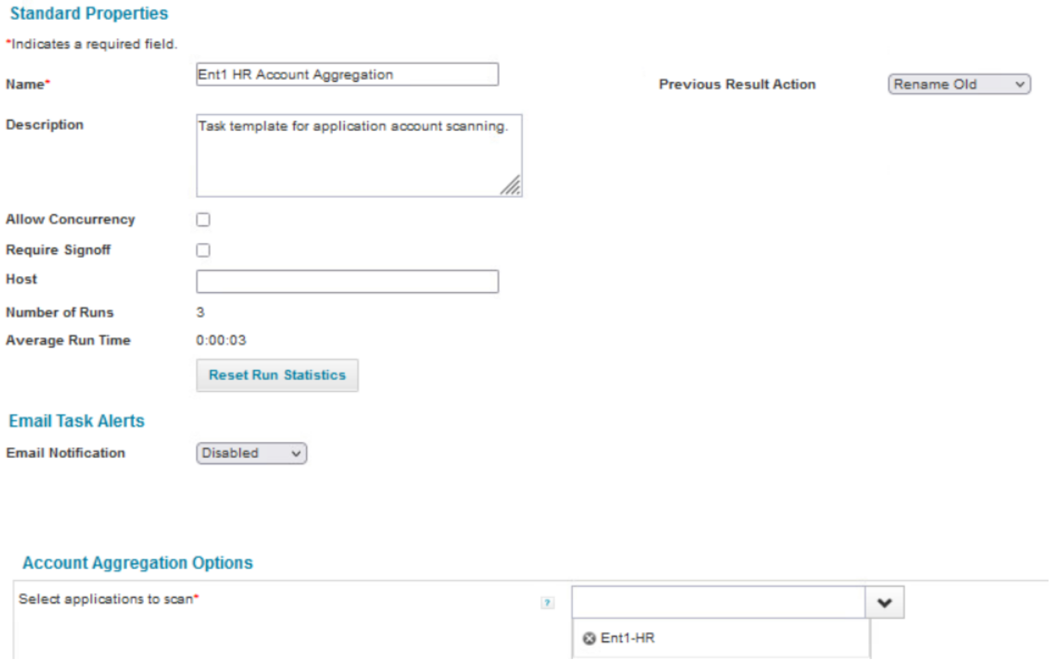


Entitlements

	Application	Property	Value
⊗	Ent1-AD-Ent-Users	memberOf	LAB\CorpGrp
⊗	Ent1-Okta	groups	Employee

5. The next step is to synchronize users and groups. To begin, navigate to the **Setup** tab and select **Tasks**.

   a. To create user aggregation, select the **New Task** drop down button and select **Account Aggregation**. The screenshot below depicts the aggregation configuration for Radiant Logic. This allows SailPoint to sync with Radiant Logic on any updates made to users. Repeat this step for AD and Okta accounts. Note that the **Account Aggregation Options** section is where the AD and Okta applications need to be selected to create the proper account aggregation.



Standard Properties

*Indicates a required field.

Name*	Ent1 HR Account Aggregation	Previous Result Action	Rename Old
Description	Task template for application account scanning.		
Allow Concurrency	□		
Require Signoff	□		
Host			
Number of Runs	3		
Average Run Time	0:00:03		

Email Task Alerts

Email Notification: Disabled

Account Aggregation Options

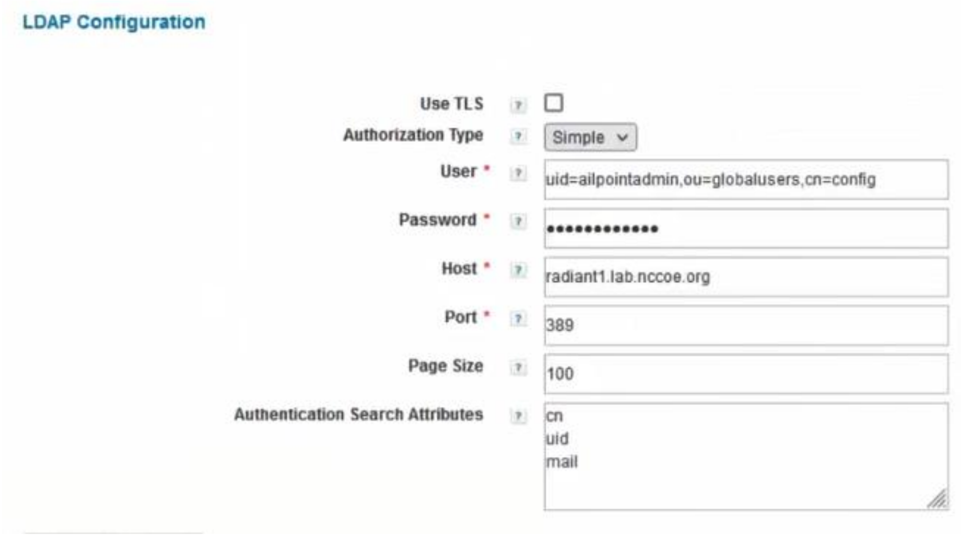
Select applications to scan*: Ent1-HR

   b. To create group aggregation, select the **New Task** drop down button and select **Account Aggregation**. This allows SailPoint to sync with AD on any updates made to users. Repeat this step for the Okta account. Note that the **Account Group Aggregation Options** section is where the Okta applications need to be selected to create the proper account aggregation.

6. Configure lifecycle processes through Rapid Setup Configuration. Click on the **Setup** cog and select **Rapid Setup** to begin. The Rapid Setup Configuration process allows onboarding of applications and manage functions such as joiner, mover, and leaver of identities. Use the "Using Rapid Setup" section of the IdentityIQ Rapid Setup Guide to guide the configuration.
    a. Configure **Joiner**, **Mover,** and **Leaver.**
    b. Configure **Identity Operations**.
    c. Configure Rapid Setup specific to AD users: Aggregation, Joiner, Mover, and Leaver.
7. Govern user permissions to applications on an individual basis. Configure procedures to provision and approve user access to resources. For Enterprise 1, the process is for an administrator or user to request approval to access an application. That request goes to the user's manager for review and approval. Once the manager approves the request, SailPoint kicks off an API call to Okta to configure access for that user.

2.3.2 Integration with Radiant Logic

1. In the **Applications** tab, select **Application Definition.** When the screen comes up, click on the **Add New Application** button.
2. Enter values for the **Name** (e.g., "Ent1-HR") and **Owner** (e.g., "The Administrator") fields. Select **LDAP** as the **Application Type** and ensure that **Authoritative Application** is enabled.
3. Click on the **Configuration** tab next to the current tab. The credentials that were created in Radiant Logic will need to be added.



LDAP Configuration

Use TLS	☐
Authorization Type	Simple
User *	uid=ailpointadmin,ou=globalusers,cn=config
Password *	••••••••••••
Host *	radiant1.lab.nccoe.org
Port *	389
Page Size	100
Authentication Search Attributes	cn uid mail

4. Scroll down the screen and under the **Account** tab, add the Search DN, which is the one created from Radiant Logic.

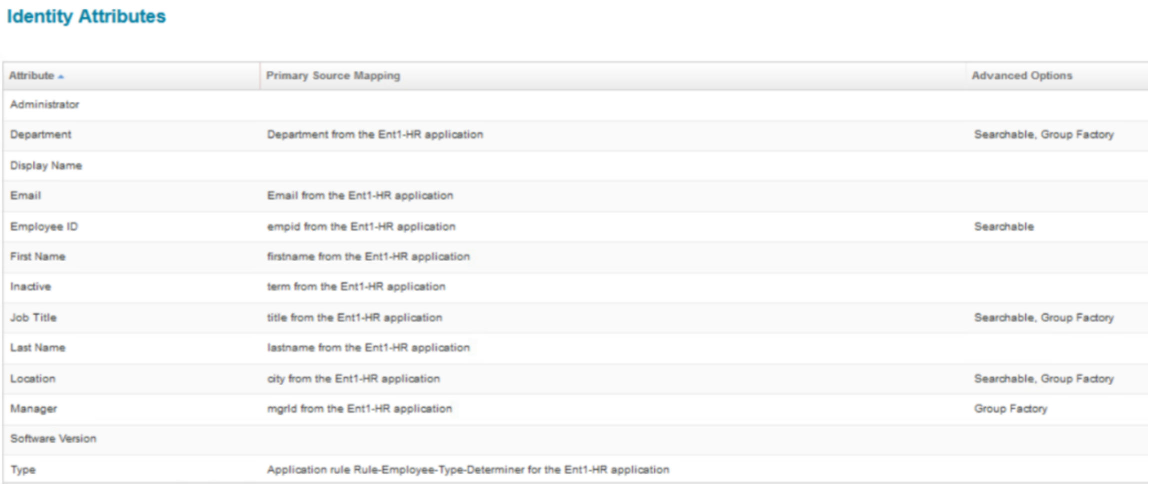
5. Click on **Test Connection** to make sure that SailPoint is able to connect to Radiant Logic. Click **Save.**

6. You can go back into the **Configuration** tab and **Schema** sub-tab. Toward the bottom of the screen, there is a **Preview** button. You can click on that to preview the imported attributes. Note: We manually added schema attributes. This can be completed from Radiant Logic and imported. Please ensure that you have the correct attributes to integrate this.

7. To complete the setup, click **Save** to finish and import users from Radiant Logic.

8. Go to the **Setup** tab and click **Tasks.** Once in the new tab, click on the **New Task** button at the top right corner to create the account aggregation for Radiant Logic.

9. Perform identity attribute mapping. The screenshot shows mappings specific to this build only.



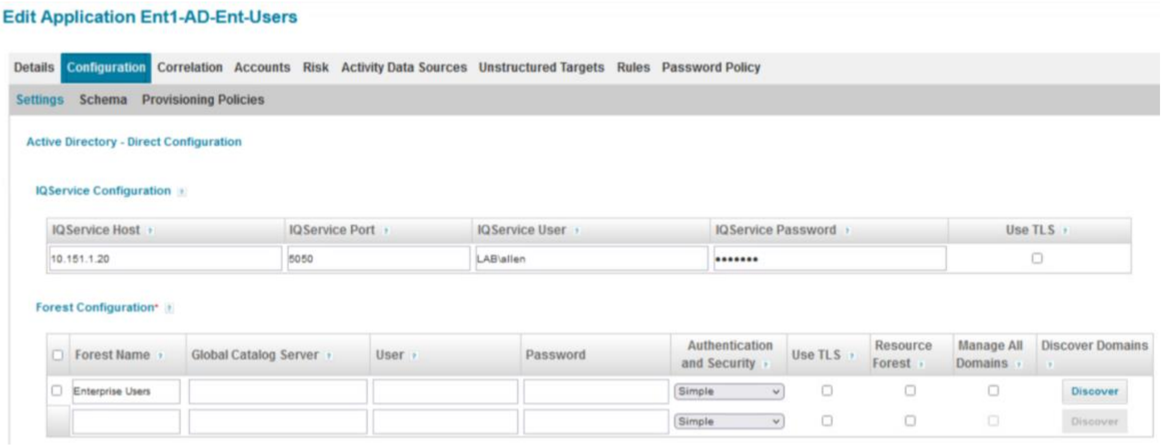
Identity Attributes

Attribute ▴	Primary Source Mapping	Advanced Options
Administrator		
Department	Department from the Ent1-HR application	Searchable, Group Factory
Display Name		
Email	Email from the Ent1-HR application	
Employee ID	empid from the Ent1-HR application	Searchable
First Name	firstname from the Ent1-HR application	
Inactive	term from the Ent1-HR application	
Job Title	title from the Ent1-HR application	Searchable, Group Factory
Last Name	lastname from the Ent1-HR application	
Location	city from the Ent1-HR application	Searchable, Group Factory
Manager	mgrId from the Ent1-HR application	Group Factory
Software Version		
Type	Application rule Rule-Employee-Type-Determiner for the Ent1-HR application	

2.3.3 Integration with AD

1. Navigate to the **Applications** tab, click on **Application Definition**, then click the **Add New Application** button. Fill out the **Name** (e.g., "Ent1-AD-Ent-Users"), **Owner** (e.g., "The Administrator"), and **Application Type** ("Active Directory – Direct").

2. Navigate to the **Configuration** tab. From here, input information for the IQ Service Host. The IP address is this server, the IdentityIQ server. IQ Service User is a user that was created in AD for this integration.



Edit Application Ent1-AD-Ent-Users

Active Directory - Direct Configuration

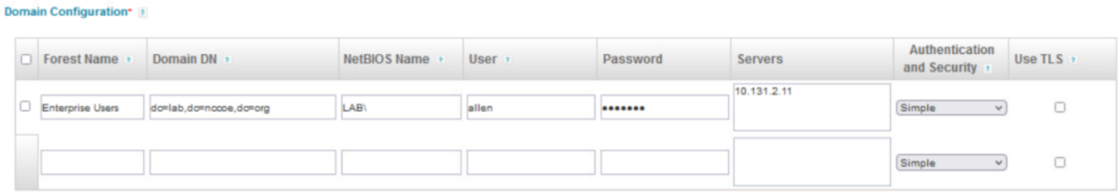
IQService Configuration

IQService Host	IQService Port	IQService User	IQService Password	Use TLS
10.151.1.20	5050	LAB\allen	•••••••	□

Forest Configuration*

□	Forest Name	Global Catalog Server	User	Password	Authentication and Security	Use TLS	Resource Forest	Manage All Domains	Discover Domains
□	Enterprise Users				Simple	□	□	□	Discover
					Simple	□	□	□	Discover

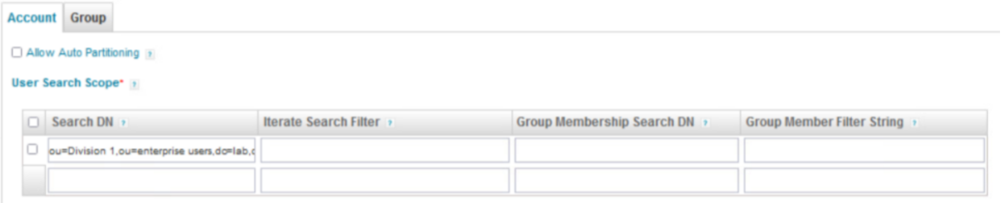
3. Scroll down to the **Domain Configuration** section. Input the domain information for where the users will be provisioned.



Domain Configuration*

□	Forest Name	Domain DN	NetBIOS Name	User	Password	Servers	Authentication and Security	Use TLS
□	Enterprise Users	dc=lab,dc=nccoe,dc=org	LAB\	allen	•••••••	10.131.2.11	Simple	□
							Simple	□

4. Scroll down to the **User Search Scope** section and input the Search DN information. This should be the AD domain location for your enterprise.



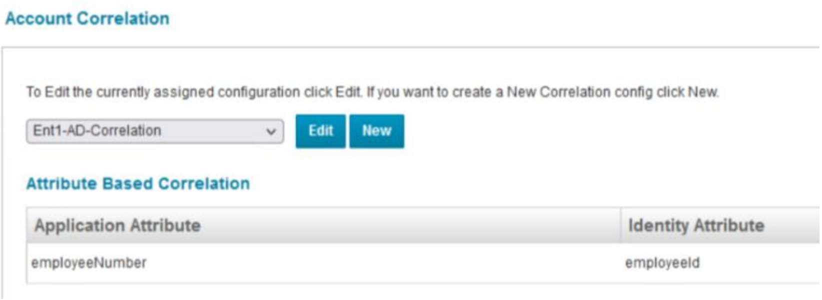
□ Allow Auto Partitioning

User Search Scope*

□	Search DN	Iterate Search Filter	Group Membership Search DN	Group Member Filter String
□	ou=Division 1,ou=enterprise users,dc=lab,c			

5. Navigate to the **Schema** and **Provisioning Policies** sub-tabs, and update information as necessary.

6. Then navigate to the **Correlation** tab to configure the correlation for application and identity attributes between SailPoint and AD.



Account Correlation

To Edit the currently assigned configuration click Edit. If you want to create a New Correlation config click New.

Ent1-AD-Correlation

Attribute Based Correlation

Application Attribute	Identity Attribute
employeeNumber	employeeId

7. Click **Save** to complete the configuration.

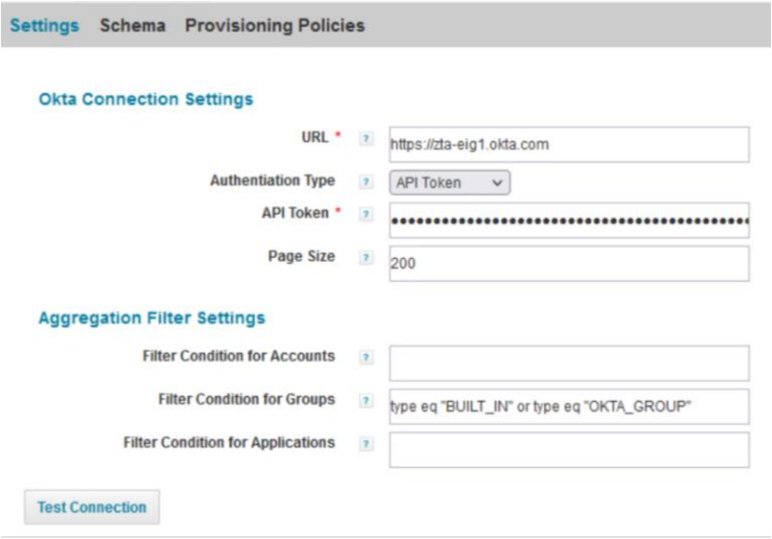
8. Go to **Setup** tab and click **Tasks**. Once in the new tab, click on the **New Task** button at the top right corner to create the account aggregation for AD.

2.3.4 Integration with Okta

1. Go into the **Applications** tab and select **Application Definition.** When the screen comes up, click on the **Add New Application** button.

2. Fill out the **Name** (e.g., "Ent1-Okta") and **Owner** ("The Administrator"), select **Okta** as the **Application Type,** and enable the **Authoritative Application** option.

3. In the **Configuration** settings tab, the Okta URL and API token are needed. Note that the API token is created in Okta. Click **Save** to finish the setup.



Okta Connection Settings

URL * https://zta-eig1.okta.com

Authentiation Type API Token

API Token * ••

Page Size 200

Aggregation Filter Settings

Filter Condition for Accounts

Filter Condition for Groups type eq "BUILT_IN" or type eq "OKTA_GROUP"

Filter Condition for Applications

2.4 Ivanti Neurons for UEM

Ivanti Neurons for UEM is a unified endpoint management (UEM) solution which is used to provision endpoints, grant access to enterprise resources, protect data, distribute applications, and enforce measures as required.

2.4.1 Installation and Configuration

2.4.1.1 Install an MDM certificate for Apple devices

The Apple Push Notification service (APNs) certificate needs to be installed in Ivanti Neurons for UEM to communicate with Apple devices. Apple devices use an APNs certificate to learn about updates, MDM policies, and incoming messages.

To acquire and install the MDM certificate:

1. Open the Ivanti Neurons for UEM console and go to **Admin > Apple > MDM Certificate** page to download a certificate signing request (CSR).
2. Upload the CSR to the Apple Push Certificates Portal to create a new certificate.
3. Save the resulting certificate.
4. Install the certificate for the Ivanti Neurons for UEM tenant.

2.4.1.2 Configure Android Enterprise

Android Enterprise allows personal and corporate applications on the same Android device. Android Enterprise configuration depends on the type of Google subscription. Please follow Ivanti documentation to set up the integration.

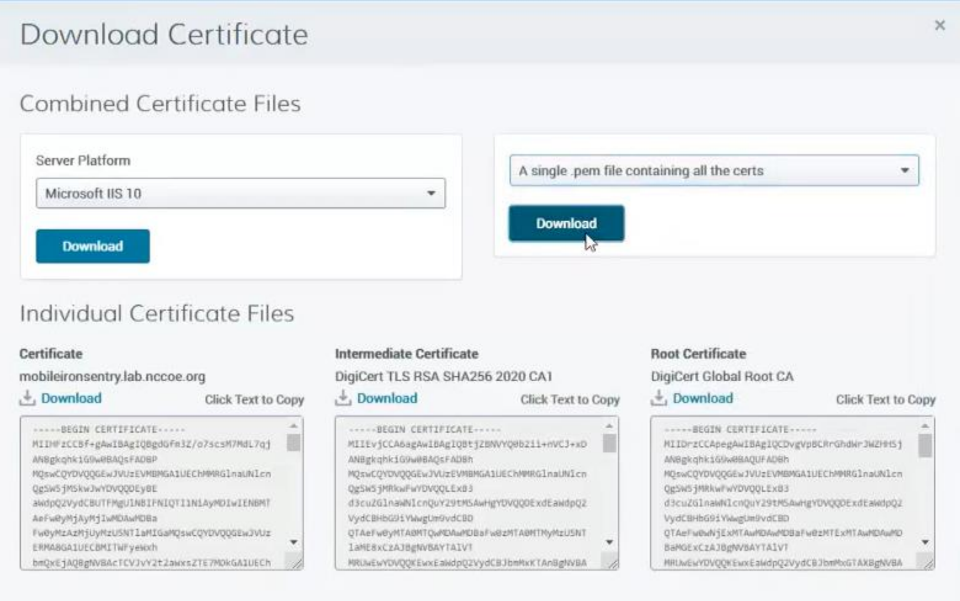
The Android Enterprise Work Profile configuration defines which features and apps are allowed, and which are restricted on Android enterprise devices. Do the following to configure the profile:

1. In the Cloud portal, go to **Configurations** and click **Add.**
2. Select the **Lockdown & Kiosk: Android Enterprise** configuration.
3. Enter a configuration name and description.
4. Click the **Work Profile** lockdown type.
5. Select the lockdown settings for Android devices.

2.4.1.3 Add a certificate authority

A certificate authority (CA) generates self-signed certificates to be used by the devices that Ivanti Neurons for UEM manages. For this implementation we used an external certificate authority (DigiCert) and a Connector to access it. Ivanti Cloud Connector provides access from the Ivanti Neurons for UEM service to corporate resources, such as an LDAP server or CA.

1. Install and configure a Connector (**Admin > Connector**).
2. In the **Certificate Management** page, click **Add** under the **Certificate Authority** section.
3. Choose **Connect to a publicly-trusted Cloud Certificate Authority.**
4. Enter a name for the CA.
5. Download the certificate from DigiCert and upload it to Ivanti Neurons for UEM.



Download Certificate

Combined Certificate Files

Server Platform: Microsoft IIS 10

A single .pem file containing all the certs

Individual Certificate Files

Certificate
mobileironsentry.lab.nccoe.org

-----BEGIN CERTIFICATE-----
MIIHFzCCBf+gAwIBAgIQBgdGfm3Z/o7scsM7MdL7qj
ANBgkqhkiG9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcn
QgSW5jMSkwJwYDVQQDEyBE
aWdpQ2VydCBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMT
AeFw0yMjAyMjIwMDAwMDBa
Fw0yMzAzMjUyMzU5NTlaMIGaMQswCQYDVQQGEwJVUz
ERMA8GA1UECBMITWFyeWxh
bmQxEjAQBgNVBAcTCVJvY2t2aWxsZTE7MDkGA1UECh

Intermediate Certificate
DigiCert TLS RSA SHA256 2020 CA1

-----BEGIN CERTIFICATE-----
MIIEvjCCA6agAwIBAgIQBtjZBNVYQ0b2ii+nVCJ+xD
ANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcn
QgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2
VydCBHbG9iYWwgUm9vdCBD
QTAeFw0yMTA0MTQwMDAwMDBaFw0zMTA0MTMyMzU5NT
laME8xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBA

Root Certificate
DigiCert Global Root CA

-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSj
ANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcn
QgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2
VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMD
BaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBA

2.4.1.4 Configure user settings

User settings define device registration options. Access them by opening Ivanti Neurons for UEM and going to **Users** > **User Settings**. Configure device and password settings there.

2.4.1.5 Add a policy

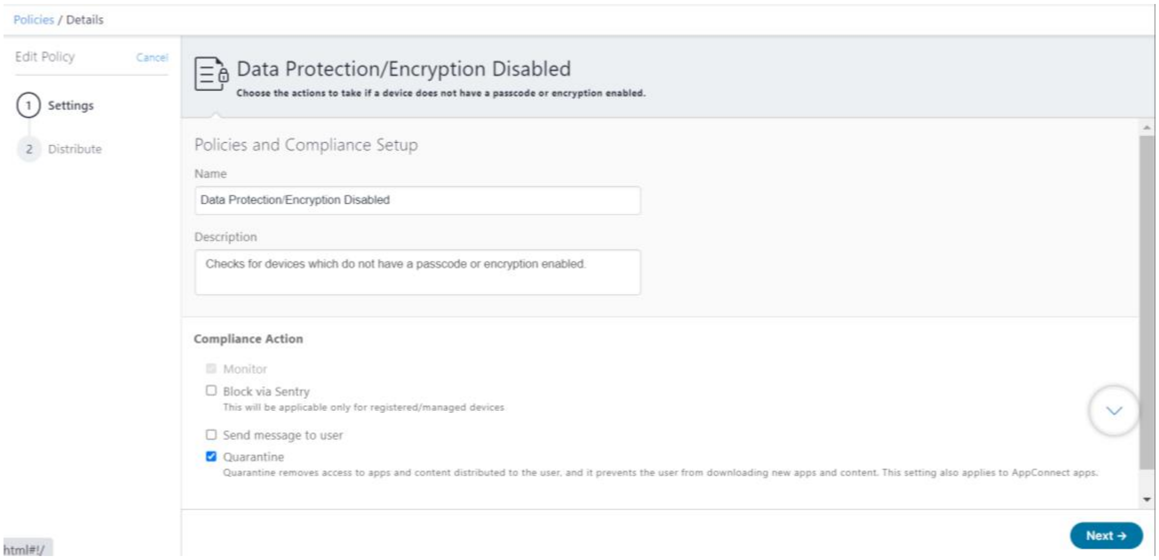
Policies define requirements for devices and compliance actions (what happens if the rule is violated). To add a policy:

1. Go to **Policies** and click **+Add** (upper right).

2. Select a policy type and complete the settings. Policy types include Compromised Devices, Data Protection/Encryption Disabled, MDM/Device Administration Disabled, Out of Contact, and Allowed Apps.

3. Select the device groups that will receive this policy.

The following screenshots show an example of a Data Protection policy to be distributed to a custom group of devices.



Policies / Details

Edit Policy Cancel

1 Settings

2 Distribute

Data Protection/Encryption Disabled

Choose the actions to take if a device does not have a passcode or encryption enabled.

Policies and Compliance Setup

Name: Data Protection/Encryption Disabled

Description: Checks for devices which do not have a passcode or encryption enabled.

Compliance Action

☑ Monitor

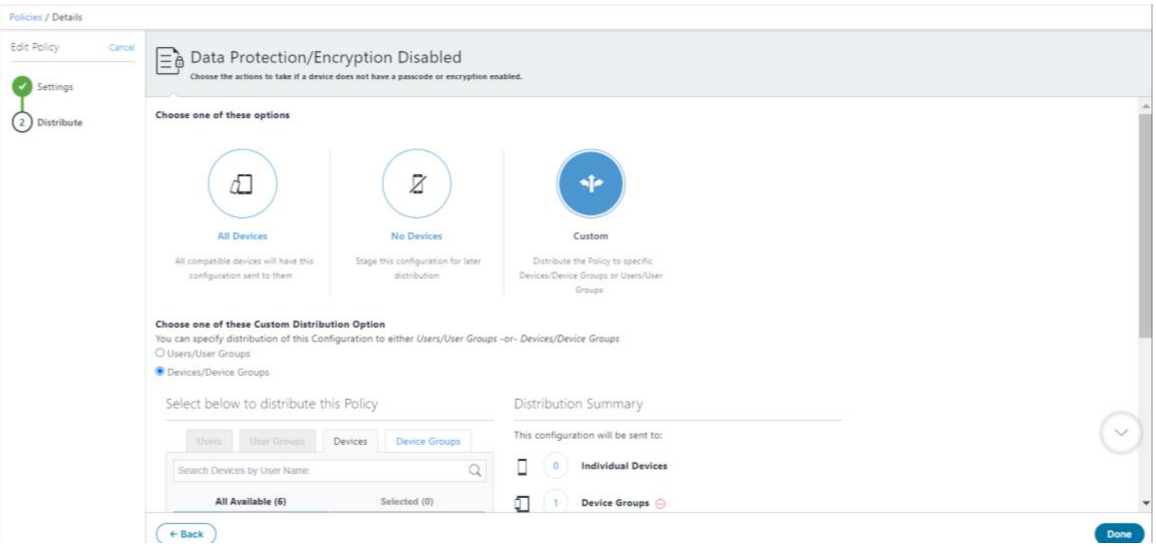
☐ Block via Sentry
This will be applicable only for registered/managed devices

☐ Send message to user

☑ Quarantine
Quarantine removes access to apps and content distributed to the user, and it prevents the user from downloading new apps and content. This setting also applies to AppConnect apps.

Next →

html#!/



Policies / Details

Edit Policy Cancel

✓ Settings

2 Distribute

Data Protection/Encryption Disabled

Choose the actions to take if a device does not have a passcode or encryption enabled.

Choose one of these options

All Devices: All compatible devices will have this configuration sent to them

No Devices: Stage this configuration for later distribution

Custom: Distribute the Policy to specific Devices/Device Groups or Users/User Groups

Choose one of these Custom Distribution Option

You can specify distribution of this Configuration to either *Users/User Groups* -or- *Devices/Device Groups*

○ Users/User Groups

● Devices/Device Groups

Select below to distribute this Policy

Users | User Groups | Devices | Device Groups

Search Devices by User Name

All Available (6) Selected (0)

Distribution Summary

This configuration will be sent to:

0 Individual Devices

1 Device Groups

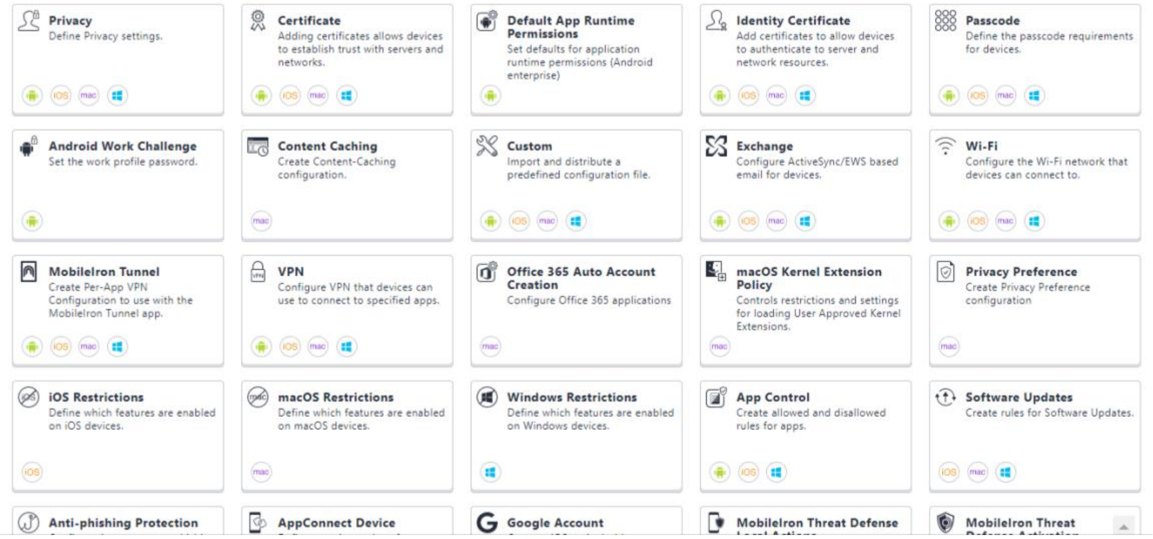
← Back

Done

2.4.1.6 Add a configuration for managed devices

Configurations are collections of settings that Ivanti Neurons for UEM sends to devices. To add a configuration:

1. Click **Add.**
2. Select the type of configuration. There are numerous types of configurations available, including Privacy, Certificate, Default App Runtime Permissions, Passcode, Exchange, Wi-Fi, VPN, iOS/macOS/Windows Restrictions, and Software Updates.



Privacy Define Privacy settings.

Certificate Adding certificates allows devices to establish trust with servers and networks.

Default App Runtime Permissions Set defaults for application runtime permissions (Android enterprise)

Identity Certificate Add certificates to allow devices to authenticate to server and network resources.

Passcode Define the passcode requirements for devices.

Android Work Challenge Set the work profile password.

Content Caching Create Content-Caching configuration.

Custom Import and distribute a predefined configuration file.

Exchange Configure ActiveSync/EWS based email for devices.

Wi-Fi Configure the Wi-Fi network that devices can connect to.

MobileIron Tunnel Create Per-App VPN Configuration to use with the MobileIron Tunnel app.

VPN Configure VPN that devices can use to connect to specified apps.

Office 365 Auto Account Creation Configure Office 365 applications

macOS Kernel Extension Policy Controls restrictions and settings for loading User Approved Kernel Extensions.

Privacy Preference Create Privacy Preference configuration

iOS Restrictions Define which features are enabled on iOS devices.

macOS Restrictions Define which features are enabled on macOS devices.

Windows Restrictions Define which features are enabled on Windows devices.

App Control Create allowed and disallowed rules for apps.

Software Updates Create rules for Software Updates.

Anti-phishing Protection

AppConnect Device

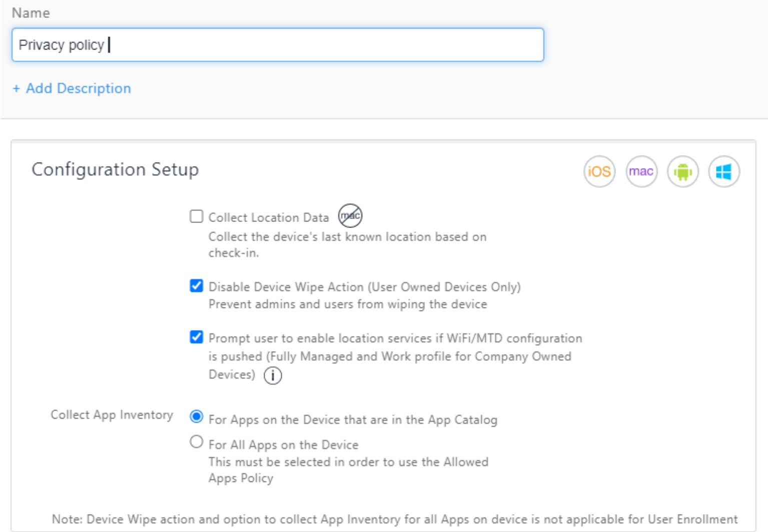
Google Account

MobileIron Threat Defense

MobileIron Threat

3. Click **Next.**
4. Select a distribution level for the configuration.

Here is an example of a Privacy configuration:



Name

Privacy policy

+ Add Description

Configuration Setup

☐ Collect Location Data
Collect the device's last known location based on check-in.

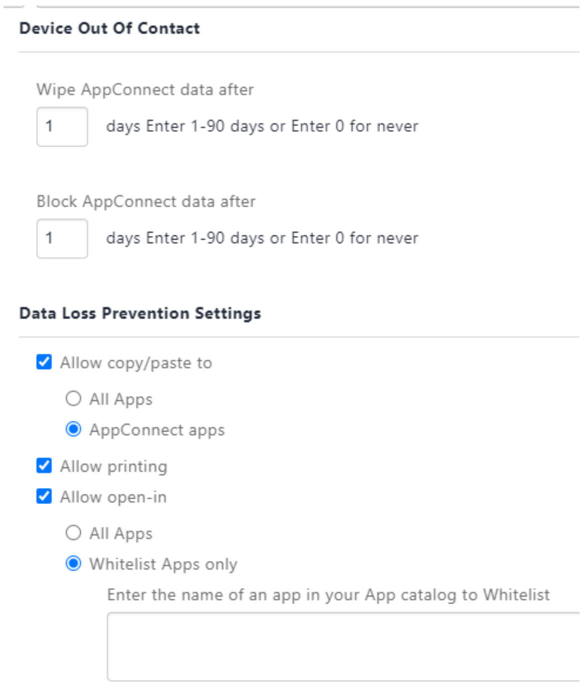
☑ Disable Device Wipe Action (User Owned Devices Only)
Prevent admins and users from wiping the device

☑ Prompt user to enable location services if WiFi/MTD configuration is pushed (Fully Managed and Work profile for Company Owned Devices)

Collect App Inventory
● For Apps on the Device that are in the App Catalog
○ For All Apps on the Device
This must be selected in order to use the Allowed Apps Policy

Note: Device Wipe action and option to collect App Inventory for all Apps on device is not applicable for User Enrollment

This is an example of an iOS AppConnect configuration:



Device Out Of Contact

Wipe AppConnect data after
1 days Enter 1-90 days or Enter 0 for never

Block AppConnect data after
1 days Enter 1-90 days or Enter 0 for never

Data Loss Prevention Settings

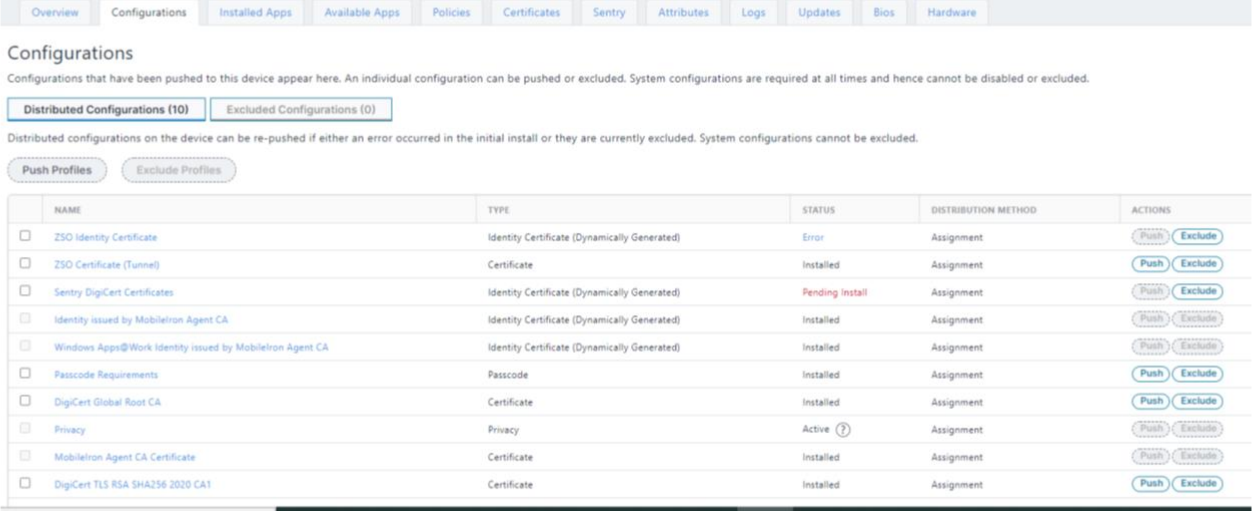
☑ Allow copy/paste to
- ○ All Apps
- ● AppConnect apps

☑ Allow printing

☑ Allow open-in
- ○ All Apps
- ● Whitelist Apps only

Enter the name of an app in your App catalog to Whitelist

This screenshot shows a list of configurations pushed to a device:



Configurations

Configurations that have been pushed to this device appear here. An individual configuration can be pushed or excluded. System configurations are required at all times and hence cannot be disabled or excluded.

Distributed configurations on the device can be re-pushed if either an error occurred in the initial install or they are currently excluded. System configurations cannot be excluded.

	NAME	TYPE	STATUS	DISTRIBUTION METHOD	ACTIONS
□	ZSO Identity Certificate	Identity Certificate (Dynamically Generated)	Error	Assignment	Push Exclude
□	ZSO Certificate (Tunnel)	Certificate	Installed	Assignment	Push Exclude
□	Sentry DigiCert Certificates	Identity Certificate (Dynamically Generated)	Pending Install	Assignment	Push Exclude
□	Identity issued by MobileIron Agent CA	Identity Certificate (Dynamically Generated)	Installed	Assignment	Push Exclude
□	Windows Apps@Work Identity issued by MobileIron Agent CA	Identity Certificate (Dynamically Generated)	Installed	Assignment	Push Exclude
□	Passcode Requirements	Passcode	Installed	Assignment	Push Exclude
□	DigiCert Global Root CA	Certificate	Installed	Assignment	Push Exclude
□	Privacy	Privacy	Active ?	Assignment	Push Exclude
□	MobileIron Agent CA Certificate	Certificate	Installed	Assignment	Push Exclude
□	DigiCert TLS RSA SHA256 2020 CA1	Certificate	Installed	Assignment	Push Exclude

2.4.2 Integration with Ivanti Connector

Ivanti Connector provides access from Ivanti Neurons for UEM to corporate resources, such as an LDAP server. For the latest Connector installation instructions, select the appropriate version of the Cloud Connector Guide.

1. Once the Ivanti Connector has been set up and configured, navigate to the Ivanti Neurons for UEM console.
2. Connect to an LDAP Server to import users and groups. Navigate to **Admin > Infrastructure > LDAP > Add Server.** Complete configurations and save. Users can now be imported from the LDAP server.

2.4.3 Integration with Okta

2.4.3.1 IdP setup

1. Go to **Admin > Infrastructure > Identity > Add IdP.**
2. Generate a key for uploading to Okta IdP.
3. Log in to Okta IdP. Search IdP for the **MobileIron Cloud App** and add it to the IdP account.
4. Configure the **MobileIron Cloud App** on the IdP by pasting the above-generated key and the host information.
5. Export metadata from Okta to the Ivanti Neurons for UEM console.

6. In **Admin > Infrastructure > Identity > Add IdP,** select **Choose File** to import the downloaded metadata file to Ivanti Neurons for UEM and complete the setup.
7. When an IdP is added, user authentication automatically switches from LDAP to IdP.

2.4.3.2 Okta Verify app configuration preparation

1. In the Okta Admin console, navigate to **Security > Device Integrations** and click **Add Platform.**
2. Select platform and click **Next.**
3. Copy the **Secret Key** for later usage and enter Device Management Provider and Enrollment Link settings.
4. Repeat for any other device platforms.

2.4.3.3 Okta Verify app configuration - Android

1. In the Ivanti Neurons for UEM console, navigate to **Apps > App Catalog.** Click **Add.**
2. Select the Google Play Store and search for **Okta Verify.** Select the official **Okta Verify** app.
3. Continue through the wizard until you reach the App Configurations page. Click the **+** button in the Managed Configurations for Android section.
4. Add desired settings. Under **Managed Configurations,** add the **Org URL** and **Management Hint** from the Okta Admin console. The Management hint will be the **Secret Key** you saved from the Okta console during preparation.
5. Click **Next,** then click **Done.**

2.4.3.4 Okta Verify app configuration - iOS

1. In the Ivanti Neurons for UEM console, navigate to **Apps > App Catalog**. Click **Add**.
2. Select the iOS Store and search for **Okta Verify**. Select the official **Okta Verify** app.
3. Continue through the wizard until you reach the App Configurations page. Click the **+** button in the Apple Managed App Configuration section.
4. Add desired settings. Under **Apple Managed App Settings**, click **Add** and add two items.
    a. For the first item, the key will be **domainName**, the value will be your Org URL, and the type will be STRING.
    b. For the second item, the key will be **managementHint**, the value will be the **Secret Key** you saved from the Okta console during preparation, and the type will be STRING.

5. Click **Next,** then click **Done**.

2.4.4 Integration with QRadar

2.4.4.1 Ivanti log transfer setup

1. Set up an SSH server to host log files. Create a user account that can be used to host/transfer Ivanti Log Files.
2. In the Ivanti Neurons for UEM console, navigate to **Admin > Infrastructure > Audit Trails**.
3. Turn on **Audit Trails Export** and **Device Check-in Trails.**
4. Under Export Format, select **CEF**.
5. Enter the IP address or hostname for the SSH server you set up previously.
6. Enter the username and password for the user you set up previously.
7. Enter the server path for where you would like the Ivanti log files to be stored on the SSH server.
8. Click **Test Connection and Save**. Ivanti log files will now be transferred to the SSH server on a regular basis.

2.4.4.2 QRadar setup

1. In the QRadar console, navigate to **Admin > Extensions Management**. Click **Add**.
2. Select the Ivanti extension file provided by IBM. Click **Add**.
3. Continue through the wizard until you completed the extension installation.
4. In the QRadar console, navigate to **Admin > Log Sources.** Click +**New Log Source.**
5. In the search box, type **Ivanti**. Make sure **Ivanti** is selected in the menu and click **Step 2: Select Protocol Type**.
6. In the search box, type **Log File**. Make sure **Log File** is selected in the menu and click **Step 3: Configure Log Source Parameters**.
7. Enter a name for the log source and turn off **Coalescing Events**. Click **Step 4: Configure Protocol Parameters**. The settings are as follows:
    a. Log Source Identifier: **MobileIron Cloud**
    b. Service Type: SFTP
    c. Remote IP or Hostname: <Log server you set up previously>

   d. Remote port: 22
   e. Remote User/Password: <Credentials created earlier, if not using key file authentication>
   f. SSH Key File: <Credentials created earlier, if not using password authentication>
   g. Remote directory: Directory where Ivanti logs are being stored
   h. Recursive: On
   i. FTP File Type Pattern (Regex for Ivanti log files): ^.*\.(zip|ZIP)$
   j. Processor: ZIP
   k. All other settings can be left as default

8. Click **Step 5: Test Protocol Parameters**. Run the tests and ensure the configuration is valid.
9. From the QRadar console, navigate to the **Admin** tab. Click **Deploy Changes**.

2.5 Ivanti Sentry

Ivanti Sentry is an in-line gateway that manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems. In this build, Ivanti Sentry acts as a PEP that controls access to enterprise resources.

2.5.1 Installation and Configuration

For this implementation we used a Standalone Sentry installation on-premises. For the latest Sentry installation instructions, select the appropriate version of the *Standalone Sentry On-Premises Installation Guide* at https://www.ivanti.com/support/product-documentation.

Next, create a profile for Standalone Sentry in the Ivanti Neurons for UEM console. For information on how to create a profile for Standalone Sentry and configure Standalone Sentry for ActiveSync and AppTunnel, see the *Sentry Guide for Cloud*. For the latest Sentry installation instructions, click on Sentry, then select the appropriate version of the Standalone Sentry On-Premises Installation Guide.

2.5.2 Ivanti Tunnel Configuration and Deployment

Ivanti Tunnel is an application that connects a mobile device to the Ivanti Sentry. The process to deploy this app is similar to the deployment of the Okta Verify app in Section 2.1.2.

1. On the **App Configurations** page for the Tunnel app, create a Managed Configuration.
2. Set the **Tunnel Profile Mode** to **MobileIron Sentry + Access.**

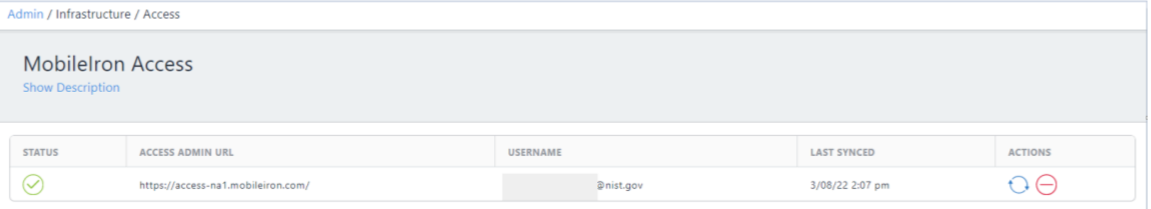
3. Set the **Sentry Server** to the Sentry instance you created previously.
4. Set the **SentryService** to the name of the IP Tunnel defined on the Sentry.
5. Set the **ClientCertAlias** to the Sentry certificates you defined during Sentry configuration.
6. Set any other options as needed.
7. Save the Managed Configuration and deploy to devices as needed.

2.6 Ivanti Access ZSO

Ivanti Access ZSO is a cloud-based service that allows access to enterprise cloud resources based on user and device posture, and whether apps are managed or not. In this build, Ivanti Access ZSO functions as a delegated IdP, with Okta passing certain responsibilities to Ivanti Access ZSO.

2.6.1 Integration with Ivanti Neurons for UEM

1. Ensure that you have the **Manage MobileIron Access Integration** role in Ivanti Neurons for UEM enabled at **Admin > System > Roles Management.**
2. Navigate to **Users > Users** and click **Add > API User.**
3. Next, navigate to **Users > Users** and click on the username of the user you just created. Navigate to the **Roles** tab of that user and add the **Manage MobileIron Access Integration** role.
4. In the Ivanti Neurons for UEM console, go to **Admin > Infrastructure > Access.**
5. Enter the following: **Access Admin URL, Access Admin Username** (username for the Access administrator account created for Access integration), and **Access Admin Password.**
6. Click **Register.**
7. When Access is registered with Ivanti Neurons for UEM, you should see the following:



Admin / Infrastructure / Access

MobileIron Access

Show Description

STATUS	ACCESS ADMIN URL	USERNAME	LAST SYNCED	ACTIONS
✓	https://access-na1.mobileiron.com/	[redacted]@nist.gov	3/08/22 2:07 pm	⟳ ⊖

2.6.2 Integration with Okta

1. In the Okta Admin console, navigate to **Security > API** and generate an API token. Save this token for use in Access.

2. In the Ivanti Access ZSO console, navigate to **Profile > Federation.**
3. Select **Add Pair > Delegated IDP** and choose **Okta.**
4. Enter the Okta Domain URL and the Okta API Token you generated in Step 1. Click **Verify.**
5. Once the verification is complete, select the routing rules you'd like configured and click **Next.**
6. Verify the Signing Certificate settings and Encryption Certificate settings are correct, and click **Next.**
7. Choose the desired **Unmanaged Device Authentication** setting and click **Done.**
8. You will see Okta in the Delegated IDP section. Okta will route authentication requests based on your settings.

2.7 Zimperium Mobile Threat Defense (MTD)

Zimperium can retrieve various device attributes, such as device name, model, OS, OS version, and owner's email address. It then continuously monitors the device's risk posture and reports any changes in the posture to Ivanti Neurons for UEM.

2.7.1 Installation, Configuration, and Integration

2.7.1.1 Create an API user

To configure a Zimperium MTD console to work with Ivanti Neurons for UEM, an API user needs to be created and assigned a few roles.

1. In the Ivanti Neurons for UEM admin console, select **Users.**
2. Click **+ Add > API user.** The Add API User dialog page opens.
3. Enter the following details: **Username, Email, First Name, Last Name, Display Name,** and **Password.**
4. Confirm the password.
5. Deselect the **Cisco ISE Operations** option.
6. Click **Done.**

2.7.1.2 Assign roles to the API user

1. From the admin console, go to **Users.**
2. Select the new API user created previously.

3. Click **Actions.**
4. From the User details page, select **Assign Roles.**
5. Select the following roles: **App & Content Management, App & Content Read Only, Common Platform Services (CPS), Device Actions, Device Management, Device Read Only, System Read Only,** and **User Read Only.**

2.7.1.3 Add an MDM server to the Zimperium console

1. Log in to the Zimperium MTD console.
2. Navigate to **Manage > Integrations > Add MDM.**
3. Select **Cloud** to add it to the MTD console as an MDM server.
4. Enter the following required information: **URL, Username/Password, MDM Name,** and **Background Sync.**
5. Click **Finish.**

2.7.1.4 Activate MTD on Ivanti Neurons for UEM

1. From the Ivanti Neurons for UEM admin console, go to **Configurations.**
2. Click **+Add.**
3. Click **Mobile Threat Defense Activation.**
4. In the **Create Mobile Threat Defense Configuration** page, enter a name for the configuration.
5. In the Configuration Setup section, select the vendor **Zimperium.**
6. In the **License Key** field, enter a unique encrypted Mobile Threat Defense activation code.
7. In the **Wake up Intervals (mins)** field, set a time.
8. Click **Next.**
9. Select the **Enable this configuration** option.
10. Select **All Devices.**
11. Click **Done.**

2.7.1.5 Add custom attributes in Ivanti Neurons for UEM

Custom device attributes will be applied to both Android and iOS devices based on threat severity.

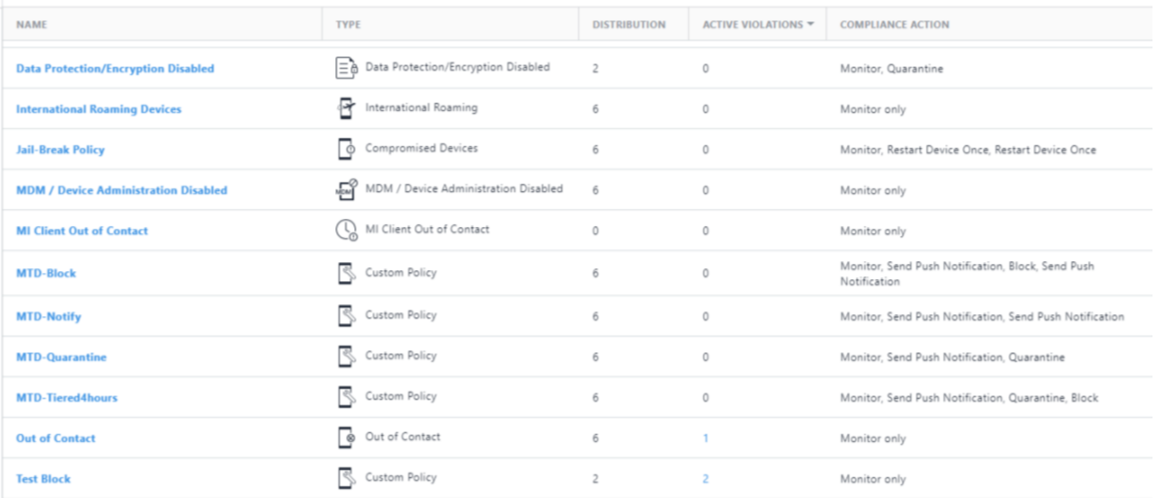
1. To create custom attributes, in the Ivanti Neurons for UEM admin console go to **Admin > System > Attributes.** Enter each attribute name in lower case.
2. Create the custom attribute **mtdnotify** for **Low or Normal** severity threats:
    a. Click **Add New.** The **Attribute Name** and **Attribute Type** fields are displayed.
    b. Select **Device** as the attribute type.
    c. Name the custom attribute **mtdnotify.**
    d. Click **Save** to monitor and notify.
3. Create the custom attribute **mtdblock** for **Elevated** or **Critical** severity threats:
    a. Click **Add New.**
    b. Select **Device** as the attribute type.
    c. Name the custom attribute **mtdblock.**
    d. Click **Save** to monitor and notify.
4. Create the custom attribute **mtdquarantine** for **Elevated** or **Critical** severity threats:
    a. Click **Add New.**
    b. Select **Device** as the attribute type.
    c. Name the custom attribute **mtdquarantine.**
    d. Click **Save** to monitor, notify, and quarantine.
5. Create the custom attribute **mtdtiered4hours** for **Low, Normal, Elevated,** or **Critical** severity threats:
    a. Click **Add New.**
    b. Select **Device** as the attribute type.
    c. Name the custom attribute **mtdtiered4hours.**
    d. Click **Save** to monitor and notify, wait for four hours, block, wait for another four hours, and quarantine.

2.7.1.6 Create compliance policy

Create compliance actions using custom policies based on the MTD custom attributes created above.

1. In Ivanti Neurons for UEM admin console, go to **Policies.**

2. Click **+ Add.**
3. Select **Custom Policy.**
4. Enter **mtdnotify** as the policy name.
5. Under **Conditions,** select **Custom Device Attribute.**
6. Select **mtdnotify** from the drop-down box and set the condition **is equal to** 1.
7. Under **Choose Actions,** select **Monitor** and **Send Email and Push Notification.**
8. Under **Email Message** fields, enter the subject and body text.
9. Under **Push Notification,** enter message text.
10. Click **Yes, Next,** and **Done.**
11. Repeat this procedure to add the following policies: **mtdblock, mtdquarantine, mtdtiered4hours.**
12. Add other policies if needed.



NAME	TYPE	DISTRIBUTION	ACTIVE VIOLATIONS ▾	COMPLIANCE ACTION
Data Protection/Encryption Disabled	Data Protection/Encryption Disabled	2	0	Monitor, Quarantine
International Roaming Devices	International Roaming	6	0	Monitor only
Jail-Break Policy	Compromised Devices	6	0	Monitor, Restart Device Once, Restart Device Once
MDM / Device Administration Disabled	MDM / Device Administration Disabled	6	0	Monitor only
MI Client Out of Contact	MI Client Out of Contact	0	0	Monitor only
MTD-Block	Custom Policy	6	0	Monitor, Send Push Notification, Block, Send Push Notification
MTD-Notify	Custom Policy	6	0	Monitor, Send Push Notification, Send Push Notification
MTD-Quarantine	Custom Policy	6	0	Monitor, Send Push Notification, Quarantine
MTD-Tiered4hours	Custom Policy	6	0	Monitor, Send Push Notification, Quarantine, Block
Out of Contact	Out of Contact	6	1	Monitor only
Test Block	Custom Policy	2	2	Monitor only

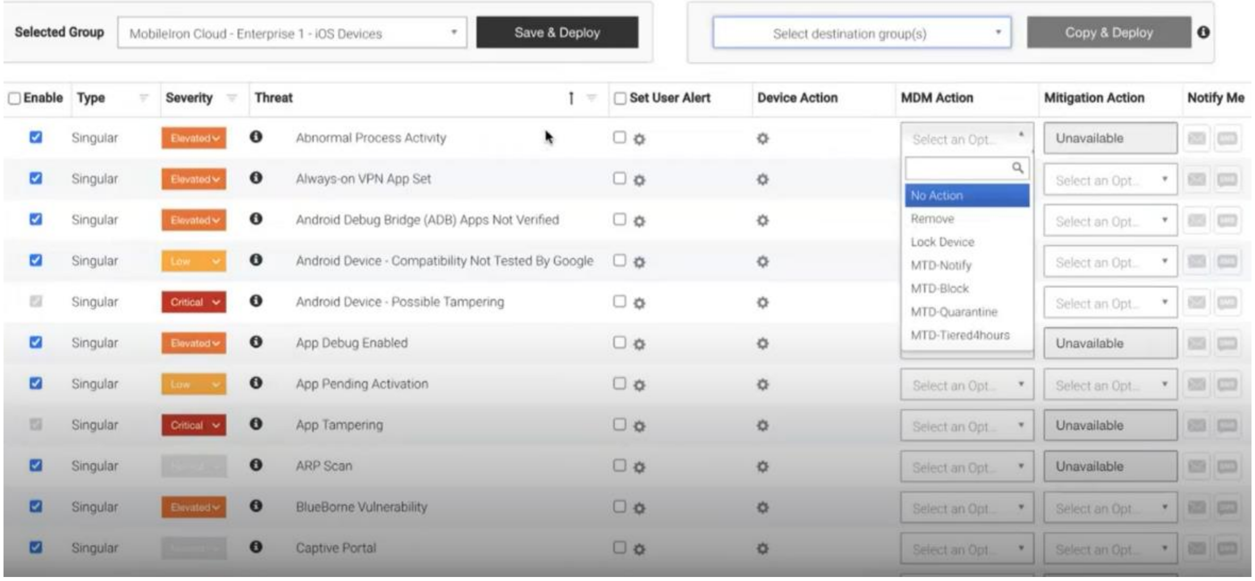
2.7.1.7 Create device groups and match with custom policies and custom device attributes created above

1. In Ivanti Neurons for UEM admin console, go to **Devices > Device Groups.**
2. Click **+ Add.**
3. Enter **mtdNotify** as the device group name.

4. Under Dynamically Managed groups, select **Custom Device Attribute.**
5. Select **mtdnotify** from the drop-down box and set the condition **is equal to** 1.
6. Click **Save.**
7. Repeat this procedure to add the following groups: **mtdBlock, mtdQuarantine, mtdTiered4hours.**

2.7.1.8 Configure Zimperium MTD management console

Set up, configure, and use the MTD console for supported MTD activities. When configuring policies in the Zimperium admin console, use the available MDM actions and mitigation actions.



□ Enable	Type	Severity	Threat	□ Set User Alert	Device Action	MDM Action	Mitigation Action	Notify Me
☑	Singular	Elevated	Abnormal Process Activity	□		Select an Opt...	Unavailable	
☑	Singular	Elevated	Always-on VPN App Set	□			Select an Opt...	
☑	Singular	Elevated	Android Debug Bridge (ADB) Apps Not Verified	□			Select an Opt...	
☑	Singular	Low	Android Device - Compatibility Not Tested By Google	□			Select an Opt...	
☑	Singular	Critical	Android Device - Possible Tampering	□			Select an Opt...	
☑	Singular	Elevated	App Debug Enabled	□			Unavailable	
☑	Singular	Low	App Pending Activation	□		Select an Opt...	Select an Opt...	
☑	Singular	Critical	App Tampering	□		Select an Opt...	Unavailable	
☑	Singular	[illegible]	ARP Scan	□		Select an Opt...	Unavailable	
☑	Singular	Elevated	BlueBorne Vulnerability	□		Select an Opt...	Select an Opt...	
☑	Singular	[illegible]	Captive Portal	□		Select an Opt...	Select an Opt...	

2.8 IBM Cloud Pak for Security

IBM Cloud Pak for Security platform enables the integration of existing security tools and provides understanding and management of threats in the environment.

1. Deploy an OpenShift cluster. OpenShift needs to be in place before Cloud Pak for Security can be installed.
2. Install Cloud Pak for Security.
3. Configure LDAP authentication so Cloud Pak for Security can leverage an existing LDAP directory server for authentication.

Once those steps are complete, open a web browser and navigate to the DNS name for Cloud Pak for Security. Additional documentation can be found at Cloud Pak for Security Documentation.

2.9 IBM Security QRadar XDR

IBM Security QRadar platform provides various security capabilities including threat detection and response, security information and event management (SIEM), and security orchestration, automation, and response (SOAR).

Install and configure QRadar following IBM's QRadar Installation and Configuration Guide.

Once that is complete, open a web browser and navigate to the QRadar server web interface by using its IP address or DNS name.

2.10 Tenable.io

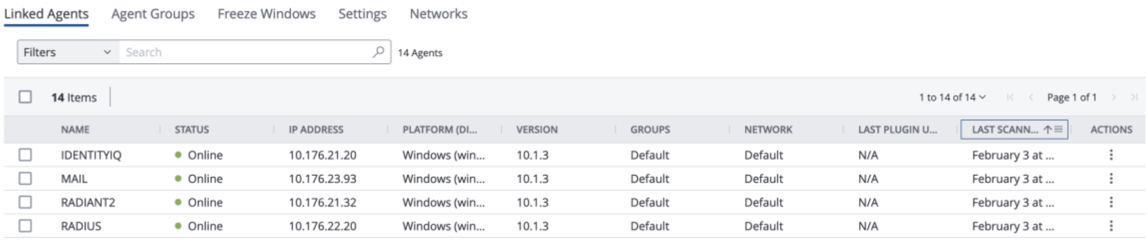
Tenable.io is a cloud-based platform that is used in this build to provide network discovery, vulnerability, and scanning capabilities for on-premises components.

2.10.1 Installation and Configuration

As a cloud-based platform, a license must first be obtained, and a cloud instance deployed by Tenable. Once deployed by a Tenable representative, Tenable.io can be accessed through the web interface located at https://cloud.tenable.com.

2.10.1.1 Deploy an agent

1. In Tenable.io, click the hamburger menu (☰) in the top left corner and navigate to **Settings > Sensors > Nessus Agents.**
2. Click **Add Nessus Agent** and save the Linking Key.
3. On the target endpoint, download the agent from https://downloads.tenable.com. When the download completes, run the executable file.
4. In the setup window, fill in the key from step 2, the server (in our case, cloud.tenable.com:443), and the agent groups that this agent will be part of (in our case, Default). Click **Next.**
5. Click **Install** and approve the request if User Account Control (UAC) comes up.
6. When installation completes, updates will continue running in the background. The update and connection process may take some time. The endpoint will then be shown in the cloud tenant.



	NAME	STATUS	IP ADDRESS	PLATFORM (DI...	VERSION	GROUPS	NETWORK	LAST PLUGIN U...	LAST SCANN...	ACTIONS
□	IDENTITYIQ	● Online	10.176.21.20	Windows (win...	10.1.3	Default	Default	N/A	February 3 at ...	⋮
□	MAIL	● Online	10.176.23.93	Windows (win...	10.1.3	Default	Default	N/A	February 3 at ...	⋮
□	RADIANT2	● Online	10.176.21.32	Windows (win...	10.1.3	Default	Default	N/A	February 3 at ...	⋮
□	RADIUS	● Online	10.176.22.20	Windows (win...	10.1.3	Default	Default	N/A	February 3 at ...	⋮

2.10.1.2 Deploy a scanner

1. In Tenable.io, navigate to **Settings > Sensors > Cloud Scanners.**
2. Click **Add Nessus Scanner** and save the Linking Key.
3. Download the Nessus Scanner .ova file from https://downloads.tenable.com.
4. Deploy the .ova file in your virtual environment.
5. Once the scanner is running, navigate to the IP address shown in the console in a web browser.
6. Login with the default username *wizard* and default password *admin*.
7. Enter new administrator credentials and click **Create Account.**
8. Click **Finish Setup** and authenticate with the new administrator credentials.
9. On the left-side navigation pane, click **Nessus.**
10. Click the URL shown in the *Nessus Installation Info* pane.
11. Click the radio button next to *Managed Scanner* and click **Continue**.
12. Enter the Linking Key from step 2 and click **Continue.**
13. Enter credentials for a new administrator account and click **Submit.**
14. The scanner will initialize and be visible on tenable.io. Scans can now be scheduled.

2.10.2 Integration with QRadar

For Tenable.io and QRadar integration, follow the Tenable and IBM QRadar SIEM Integration Guide.

2.11 Tenable.ad

Tenable.ad provides AD monitoring to detect attacks and identify vulnerabilities. In this build, Tenable.ad is integrated with the on-premises AD installation and configured to forward alerts to the IBM QRadar SIEM.

For Tenable.ad installation and configuration, follow the Tenable.ad On-Premise Installation Guide.

For Tenable.ad and QRadar integration, follow the Tenable and IBM QRadar SIEM Integration Guide.

2.12 Tenable NNM

Tenable Nessus Network Monitoring (NNM) monitors network traffic at the packet level to provide visibility into both server and client-side vulnerabilities. In this build, NNM was set to Asset Discovery mode and linked to Tenable.io in order to provide visibility into all network actors.

For Tenable.ad installation and configuration, follow the Tenable NNM Documentation.

2.12.1Deploy a Tenable NNM instance

1. In Tenable.io, navigate to **Settings > Sensors > Nessus Network Monitors.**
2. Click **Add Nessus Network Monitor** and save the Linking Key.
3. Download the NNM .ova file from https://downloads.tenable.com.
4. Deploy the .ova file in your virtual environment.
5. Once the NNM instance is running, navigate to the IP address shown in the console in a web browser on port 8835.
6. Enter credentials for a new administrator account and click **Submit.**
7. Enter the Linking Key from step 2 and click **Continue.**
8. The NNM instance will initialize and be visible on Tenable.io. Additional NNM configuration can now occur if needed.

2.13 Mandiant Security Validation (MSV)

Mandiant Security Validation (MSV) allows organizations to continuously validate the effectiveness of their cybersecurity controls by running actions that may conflict with the organization’s policy and determining if those actions are detected and/or blocked. In this build, MSV is configured to regularly test the build’s zero trust policies and report on the results.

2.13.1 MSV Director Installation/Configuration

1. Download the MSV Director software from the Mandiant web portal and deploy it in a virtual environment.
2. Log into the MSV command line interface using credentials provided by Mandiant.

3. Run the command `sudo vsetnet` to apply network configuration.
4. Run the command `sudo vsetdb --password new_password` to set a new password for the Director database.
5. Use a web browser to access the MSV Director web interface at `https://Director IP/`.
6. Sign into the web interface using credentials provided by Mandiant.
7. Accept the End User Licensing Agreement and apply the license provide by Mandiant.
8. Configure the DNS settings by navigating to **Settings > Director Settings > DNS Servers.**
9. Configure the NTP settings by navigating to **Settings > Director Settings > NTP Servers.**
10. Add Security Zones corresponding with the enterprise's network segments by navigating to **Environment > Security Zones.**
11. Download security content from the Mandiant web portal.
12. Navigate to **Settings > Director Settings > Content.**
13. Select **Import,** browse to the downloaded security content, and select the content files.
14. Click **Upload Import** and upload the files into the MSV Director web interface.
15. Once the upload is complete, click **Apply Import** to import the content files into MSV.

2.13.2 MSV Network Actor Installation/Configuration

1. Download the MSV Network Actor software from the Mandiant web portal and deploy it in a virtual environment.
2. Log into the MSV command line interface using credentials provided by Mandiant.
3. Run the command `sudo vsetnet` to apply network configuration.
4. In the MSV Director web interface, navigate to **Environment > Actors.**
5. Click **Add Network Actors** and fill out the new **Actor** form.
6. Identify the Actor you just created in the **Pending Actors** table, expand the **Actions** menu, and click **Connect** to initiate a Director-to-Actor registration.
7. Enter the Actor's FQDN or IP address.

2.13.3 MSV Endpoint Actor Installation/Configuration

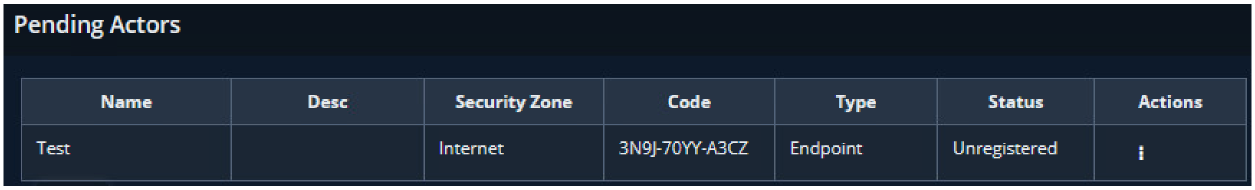
1. Deploy an endpoint machine running Windows, macOS, or Linux.

2. In the MSV Director web interface, navigate to **Library > Actor Installer Files** and download the relevant installer onto the endpoint.

3. Navigate to **Environment > Actors,** click **Add Endpoint Actors,** and fill out the new Actor form.

4. Execute the Actor installer on the endpoint and proceed through the install process.

5. At the end of the install process, identify the actor you just created in the **Pending Actors** table and enter the value from the **Code** field into the Actor configuration field.



Pending Actors

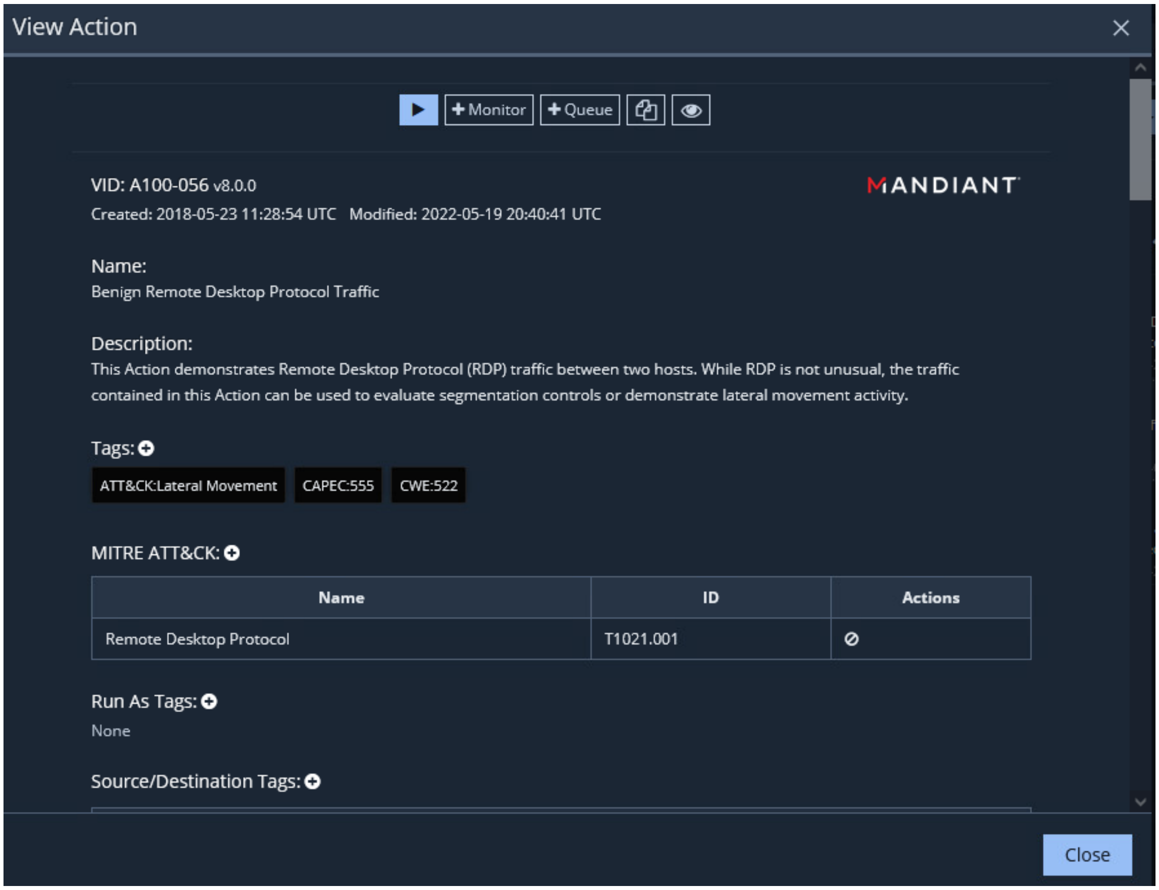
Name	Desc	Security Zone	Code	Type	Status	Actions
Test		Internet	3N9J-70YY-A3CZ	Endpoint	Unregistered	⋮

6. The endpoint will register itself with the MSV Director, and setup will be complete.

2.13.4 MSV Evaluation Configuration

1. Once the MSV Director and Actors have been configured, evaluations can be created to test security controls and policies. In the MSV Director web interface, navigate to **Library > Actions.**

2. Find the action(s) you would like to use for the evaluation and select the **+Queue** button to add the action to the Queue. Repeat this process until you have added all needed actions to the Queue.



VID: A100-056 v8.0.0

Created: 2018-05-23 11:28:54 UTC Modified: 2022-05-19 20:40:41 UTC

Name:
Benign Remote Desktop Protocol Traffic

Description:
This Action demonstrates Remote Desktop Protocol (RDP) traffic between two hosts. While RDP is not unusual, the traffic contained in this Action can be used to evaluate segmentation controls or demonstrate lateral movement activity.

Tags: ⊕
ATT&CK:Lateral Movement | CAPEC:555 | CWE:522

MITRE ATT&CK: ⊕

Name	ID	Actions
Remote Desktop Protocol	T1021.001	⊘

Run As Tags: ⊕
None

Source/Destination Tags: ⊕

3. After actions have been added to the Queue, click the **Queue** button in the upper right side of the web interface.

4. Select each of the actions in the **Unassigned** section and drag them to the **Current Actions** section.

5. Scroll up to the top of the page and click the **Save** button.

6. Under the **Test Type** dropdown, choose **Evaluation.**

7. Under the **Name** section, enter a name.

8. Under the **Description** section, enter a description.

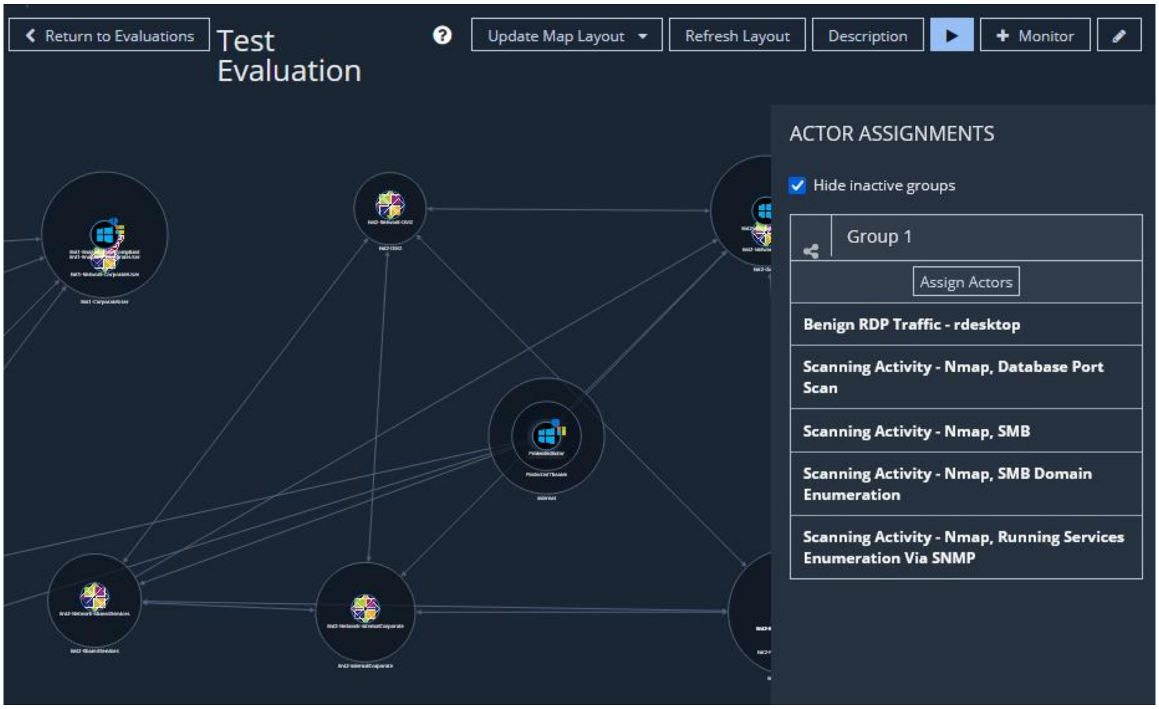
9. Select the **Save** button to save the evaluation.

10. Your new evaluation can be found by navigating to **Library > Evaluations** and filtering on **User Created.**

2.13.5 MSV Evaluation Execution

1. Navigate to **Library > Evaluations** and select the evaluation you'd like to run. Click the **Run** button.

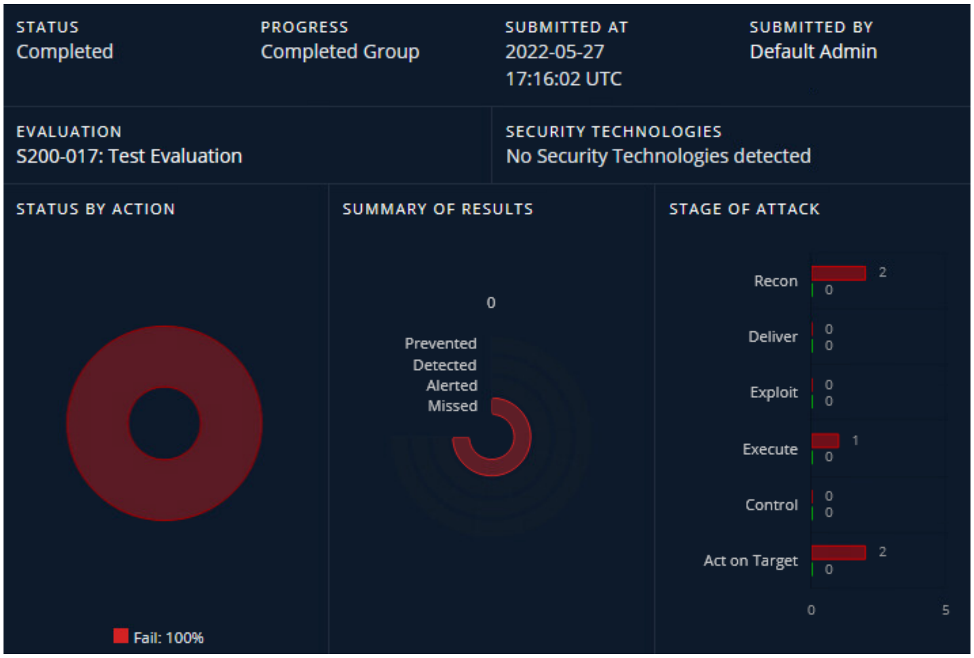
2. From the Evaluation screen, press the **Run Evaluation** button.



- Benign RDP Traffic - rdesktop
- Scanning Activity - Nmap, Database Port Scan
- Scanning Activity - Nmap, SMB
- Scanning Activity - Nmap, SMB Domain Enumeration
- Scanning Activity - Nmap, Running Services Enumeration Via SNMP

3. Select the **Source Actor** and **Destination Actor** from the dropdown menus. Click **Run Now.**

4. The evaluation will run, providing results once the actions have been attempted/completed.



STATUS
Completed

PROGRESS
Completed Group

SUBMITTED AT
2022-05-27
17:16:02 UTC

SUBMITTED BY
Default Admin

EVALUATION
S200-017: Test Evaluation

SECURITY TECHNOLOGIES
No Security Technologies detected

2.14 DigiCert CertCentral

CertCentral simplifies digital trust and automates certificate management by consolidating tasks for issuing, installing, inspecting, remediating, and renewing TLS/SSL certificates in one place. In this build, CertCentral provided TLS/SSL certificates to any system needing those services.

For the latest CertCentral setup and usage instructions, see https://docs.digicert.com/get-started/.

2.14.1 Requesting a certificate

1. Generate a Certificate Signing Request. This can be done with OpenSSL or DigiCert's Certificate Utility. Save the private key for later use.

2. In the DigiCert CertCentral dashboard, navigate to **Certificates > Requests** and click **Request a Certificate**. Select the certificate type.

3. Upload or paste the Certificate Signing Request in the provided field.

4. Select the coverage length, and add any other additional options as needed.

5. Click **Submit Request**.

2.14.2 Obtaining and implementing a certificate

1. In the DigiCert CertCentral dashboard, navigate to **Certificates > Orders** and select the request that you previously created.
2. Click **Download certificate as** and select **More Options…**
3. You will be presented with a list of certificate format options. Select the option/format that best pertains to the platform you will be using the certificate on. Click **Download**.
4. Obtain the private key that was originally generated with your Certificate Signing Request. If using DigiCert's Certificate Utility, this can be found using the Export function.
5. The certificate and private key can now be imported/installed and used on the intended platform.

3 Enterprise 2 Build 1 (EIG E2B1) Product Guides

This section of the practice guide contains detailed instructions for installing, configuring, and integrating all of the products used to implement EIG E2B1. For additional details on EIG E2B1's logical and physical architectures, please refer to Volume B.

3.1 Ping Identity PingOne

Ping Identity PingOne is a SaaS solution that provides ICAM capabilities to an enterprise. The following sections describe the setup of PingOne and its PingFederate service, and various integrations to other products. Ping Identity integrates with Radiant Logic for identity information, and with Cisco Duo to delegate the second authentication factor for users accessing resources.

3.1.1 Configuration: PingOne and PingFederate

1. PingOne setup: From your web browser, type pingone.com and click the "Try Ping" at the top right of the screen. Follow the instructions to sign up.
2. Once the PingOne environment is set up and functioning, scroll down the screen and click on the PingFederate service. A new browser tab will open. Most of the configuration will be performed on PingFederate for this build.
3. Create an IDP adaptor. This configuration should include some required values like mail and group membership (these will be mapped in steps below to the policy contract) and it is used as the first authentication factor and will be applied in the policy in the next step.

4. Create a policy contract as a list to map values to the connection(s). They will use a policy to fulfill the mappings from sources (such as LDAP or Third-Party Identity Provider using a Federated Hub).

5. Create an authentication policy that will be used to dictate application authentication. For our policies, we are using user ID and password for the first authentication factor (step 2 above) and Duo as the second authentication factor (step 2 in the Integration with Cisco Duo section).

6. Create a policy contract to connect that uses the above policy.

7. Configure SAML application integrations. Note that all applications are different. For our resources (applications), certain SAML formats and attributes are used. Follow the linked documentation above to configure the specific setup of your own application.

8. For this build, we developed policies that allow employees to access all resources (resource 1 and resource 2) and contractors to access resource 2 only. In order to do that, we leveraged the "memberof" attribute from Radiant Logic to identify employees and contractors. Once this information is identified, refer to:

    a. Authentication Policies to define the attribute mappings using this information, Policy Contract

    b. SAML applications to configure issuance criteria to information retrieved from Radiant Logic

3.1.2 Integration with Radiant Logic

1. For this build we installed a PingOne Gateway, which is "on-premise software that allows PingOne to communicate with other systems like LDAP servers," to communicate with RadiantOne. The PingOne Gateway was installed on a Windows Server on the same subnet as the RadiantOne server. We used the PingOne Gateway due to restrictions of multiple firewalls and NAT rules within our lab environments (some are not under our control) from allowing PingOne from the Internet to reach RadiantOne in Enterprise 2. In many environments, the LDAP gateway is not needed if NAT is not used, and opening the proper TCP/UDP ports on the enterprise firewalls will allow communication between PingOne and the on-prem resource. Note: Prerequisites and instructions to install the gateway are available under **Connections/Gateway** in the PingOne console.

2. Once the Gateway is configured, click the **Add** button within the Connections/Gateway screen. Follow instructions on the screen to complete the integration with Radiant Logic. Note: A service account and other information from Radiant Logic is needed for the setup. Ensure this service account is created within Radiant Logic prior to configuring the PingOne Gateway.

3. From PingFederate, go to **Data Stores** and create a **New Data Store** for Radiant Logic. Select **LDAP** for your **LDAP Type** and fill in the variables to complete the configuration.

3.1.3 Integration with Cisco Duo

Make sure that configuration from Cisco Duo is completed before performing the integration.

For IDP application integration, from the **Authentication** tab, select **IDP Adaptors**, and click **Create New Instance** to create the integration with Cisco Duo to use Duo MFA as the second authentication factor. Specific API configuration information that was created from Cisco Duo is needed here to complete the setup.

Note: For this build, we are using Duo although Ping Identity has its own MFA.

3.2 Radiant Logic RadiantOne

3.2.1 Installation and Configuration

Refer to Section 2.2.1.

3.2.2 Configuration

Refer to Section 2.2.2.

3.2.3 Integration

Refer to Section 2.2.3 for integration with SailPoint.

For integration with Ping Identity, a service account was created in RadiantOne. This service account, along with various credential information is used by PingFederate to communicate with RadiantOne to authenticate users. The communication between RadiantOne and PingFederate is through the Ping Gateway, which was installed on the same subnet as RadiantOne.

3.3 SailPoint IdentityIQ

3.3.1 Installation and Configuration

Refer to Section 2.3.1.

3.3.2 Integration with Radiant Logic

Refer to Section 2.3.2.

3.3.3 Integration with AD

Refer to Section 2.3.3.

3.3.4 Integration with Ping Identity

There is no integration with Ping Identity. For this build, SailPoint provides AD user information and Duo pulls from AD.

3.4 Cisco Duo

Cisco Duo is a SaaS solution that implements and enforces security policies and processes, using strong authentication to reduce the risk of data breaches due to compromised credentials and access from unauthorized devices. For this build, we use Cisco Duo as the second authentication factor for resources.

3.4.1 Configuration

Sign up with Cisco Duo to create a Duo instance. Once you have admin access, create policies and integration with AD and Ping Identity.

Create a policy to enable MFA for users. Navigate to **Policy** and click **Edit Global Policy**. In the Global Policy, there are many sub-policies that can be applied. For this build, we enabled the following:

- New User policy: prompt any user without the Duo app to enroll
- Authentication policy: require two-factor
- Authentication methods: Duo Mobile app (Duo Push)
- Device Health application: enable macOS and Windows (note: these are the only operating systems that are capable of device health monitoring)
- Custom Policies: Create a policy to monitor device health if the authentication request comes from PingFederate. Self-enrollment is enabled so users will be prompted to install a Duo client on the end device for health monitoring. For this build, users will not be given access to a resource if their macOS or Windows firewall is turned off. There are other health checks available.

3.4.2 Integration

For integration with PingFederate, navigate to **Applications** and click **Protect an application**. Follow the instructions to complete the configuration. Note the three pieces of information provided: Client ID, Client secret, and API hostname. This information will be used to configure the integration within PingFederate to communicate with Duo.

For integration with Microsoft Active Directory, navigate to **Users** and click on **Directory Sync**. Follow the instructions to configure the AD integration. A Duo Authentication Proxy is needed for this build since the Enterprise 2 AD is not visible to the Internet.

3.5 Palo Alto Networks Next Generation Firewall

In this build, a virtualized Palo Alto Next Generation Firewall (NGFW) was deployed on-premises as a security and access control device. The firewall provides zone-based network filtering for both inbound and outbound traffic, including remote access virtual private networks (VPNs) using the GlobalProtect clients. For GlobalProtect VPN access installation instructions, visit: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFbCAK

3.6 IBM Security QRadar XDR

For installation, configuration, and integration instructions, refer to Section 2.9.

3.7 Tenable.io

For installation, configuration, and integration instructions, refer to Section 2.10.

3.8 Tenable.ad

For installation, configuration, and integration instructions, refer to Section 2.11.

3.9 Tenable NNM

For installation, configuration, and integration instructions, refer to Section 2.12.

3.10 Mandiant Security Validation (MSV)

For installation, configuration, and integration instructions, refer to Section 2.13.

3.11 DigiCert CertCentral

For installation, configuration, and integration instructions, refer to Section 2.14.

4 Enterprise 3 Build 1 (EIG E3B1) Product Guides

This section of the practice guide contains detailed instructions for installing, configuring, and integrating all of the products used to implement EIG E3B1. For additional details on EIG E3B1's logical and physical architectures, please refer to NIST SP 1800-35B.

4.1 Microsoft Azure Active Directory (AD)

Azure AD is a SaaS identity and access management platform. No installation steps are required. You will need to create your organization's instance of Azure AD and configure it to allow your users access to applications that use it for authentication and authorization.

1. After logging in to portal.azure.com, create an Azure AD Tenant.
2. Create a connection between your on-premises AD and Azure AD to replicate user, group, and authentication information from your AD to Azure AD.
3. Configure the Azure AD Tenant to enable Single Sign-On Password Reset (SSPR). This gives users the ability to reset their passwords from https://aka.ms/sspr or from within their profile in Azure AD. This will be effective for both their AD and Azure AD accounts.
4. Configure password writeback, which enables password changes in Azure AD to be replicated back to the on-premises AD.
5. The conditional access feature in Azure AD specifies conditions under which a user would be given access to a resource or application that uses Azure AD for authentication. MFA was configured as a requirement for access to all applications. Configure MFA for all users.
6. Access to resources based on device compliance was implemented as an essential feature in this solution. Access would only be granted to a user if the client device is compliant. Compliance is reported to Azure AD by Microsoft Endpoint Manager. Enable this feature, Conditional Access Device Compliance.
7. Configure an enterprise application, GitLab, to use Azure AD for authentication:
    a. GitLab was configured to directly authenticate to Azure AD using the SAML protocol. GitLab must first be registered in Azure AD before Azure AD can be configured as the application's IdP.
    b. Configure Azure AD as a SAML IdP for the GitLab application. Once that is implemented, access attempts to the target application will be redirected to Azure AD for authentication and authorization.

4.2 Microsoft Endpoint Manager

Microsoft Endpoint Manager is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM).

4.2.1 Configuration and Integration

4.2.1.1 Add and verify a custom domain

To connect an organization's domain name with Intune, a DNS registration needs to be configured. This gives users a familiar domain when connecting to Intune and using resources. Use the information found at the hyperlink to create a custom domain.

4.2.1.2 Add users

Use the information at the hyperlink to add users to Intune.

4.2.1.3 Enroll devices in Microsoft Intune

Enrolling devices allows them to receive configuration profiles and compliance policies. Configuration profiles configure features and settings on devices. Compliance policies help devices meet an organization's rules.

1. Get an Apple MDM push certificate and add it to Endpoint Manager. This certificate is required to enroll iOS/iPadOS devices. Then enroll iOS devices in Microsoft Intune.
2. Create an iOS enrollment profile. An enrollment profile defines the settings applied to a group of devices during enrollment.
3. Enroll Android devices in Microsoft Intune. To enable Android Enterprise, an administrative Google account needs to be connected to the Intune tenant.
4. Create an iOS compliance policy in Microsoft Intune. It will be evaluated before access is allowed from iOS devices.
5. Create an Android compliance policy in Microsoft Intune. It will be evaluated before access is allowed from Android devices.
6. Create an iOS/macOS configuration profile for iOS or Mac devices.

4.2.1.4 Configure conditional access rules

Conditional access is used to control the devices and apps that can connect to company resources. Use the information in the hyperlink to create device based conditional access policies.

4.2.1.5 Manage applications

iOS/iPadOS: Use the instructions at Add iOS Store Apps to select apps from the iOS/iPadOS store that will be approved for installation on your managed iOS or iPadOS devices.

Android: For this build we added Managed Google Play apps. Managed Google Play is Google's enterprise app store which serves as a source of applications for Android Enterprise in Intune. Use the instructions at Add Android Store Apps to select apps that will be approved for installation and made available to your managed devices.

Windows: Use the information provided at select approved apps to choose which apps should be added to your Windows devices.

There is more than one way to configure Windows apps in Intune. We configured the app using App suite information. For other ways, refer to the Microsoft documentation.

4.3 Microsoft Defender for Endpoint

Microsoft Defender for Endpoint provides endpoint protection, detection, and response to threats.

4.3.1 Configuration and Integration

4.3.1.1 Enable Microsoft Defender for Endpoint

Use the information at Configure Microsoft Defender for Endpoint in Microsoft Intune | Microsoft Learn to enable Defender for Endpoint.

1. Use the information in the provided hyperlink to onboard devices. Once devices are onboarded, threat signals and vulnerability information are automatically collected from them.

2. You can optionally enable supervised mode on iOS devices using information at the hyperlink. Supervised mode gives administrators greater control over corporate-owned devices.

3. Alerts and security incidents can be viewed and responded to by accessing the Defender for Endpoint cloud component. Use the information in the hyperlink to view and respond to discovered threats.

4.3.1.2 Create Endpoint Detection and Response policy (Windows 10 and later)

Endpoint detection and response (EDR) policies are used to detect advanced attacks in near real-time. Use the information in the hyperlink to create an EDR policy.

4.3.1.3 Create an antivirus policy

An antivirus policy defines the behavior of the antivirus software agent on the endpoint. Use the information in the hyperlinks to create an antivirus policy and configure antivirus policy settings.

4.3.1.4 Create Defender compliance policy

Compliance policies can help protect organizational data by requiring users and devices to meet defined security requirements. Use the information in the hyperlink to create a Defender for Endpoint compliance policy.

4.3.2 Microsoft Defender Antivirus

Microsoft Defender Antivirus is leveraged by Microsoft Defender by Endpoint. It is anti-malware software built into Windows client devices that detects threats and malware on client devices and quarantines infected files. Defender Antivirus is enabled by default.

1. Check the status of real-time protection to ensure it's on.
2. Turn real-time protection on or off.

4.4 Microsoft Sentinel

Microsoft Sentinel is a cloud-native SIEM and SOAR system. It can be used for security analytics, threat intelligence, attack detection, and threat response.

There is no need to install Sentinel, as it is a managed service. Instead, it needs to be enabled and configured in your Azure environment. It also needs a workspace to store and correlate ingested data.

1. Enable Sentinel and configure a workspace.
2. Use the general instructions found at Connector to Data Sources to enable log forwarding to Sentinel from various devices, systems, and services. Each data source will have to be connected independently from other data sources, so you must perform this step once per data source. In this build, Azure AD, Endpoint Manager, Defender for Endpoint, Office365, and Tenable.io were configured to send logs using this method.
3. The Log Analytics Agent is a log forwarder that accepts syslog and common event format (CEF) formatted logs and then forwards the logs to Sentinel. If you have a product or device without a native Sentinel integration, install and configure the Log Analytics Agent on a virtual machine. Once completed, the log forwarder will be able to receive syslog data on UDP port 514. Then configure the product or device that will be the data source to send logs via syslog to the log forwarder using the product's instructions.

4.5 Microsoft Office 365

Microsoft Office 365 is a suite of SaaS-based productivity applications used for a variety of activities such as word processing, accounting, creating presentations, email, and others. Office 365 was enabled in the environment and was used as a set of protected target applications. Use the information at Activate Microsoft Office 365 to activate your office 365 subscription.

Use Office 365 Sign-in link to log on to Microsoft Office 365. Use your email address and password. You will be required to authenticate using multi-factor authentication.

Once authentication is complete, you will see the various office applications, such as Word, Excel, PowerPoint, and Outlook in your dashboard.

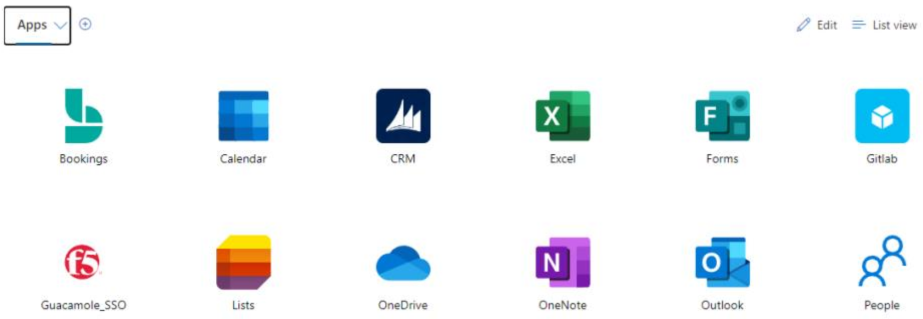
4.6 F5 BIG-IP

BIG-IP is both a load balancer and an identity-aware proxy. In this phase of the build, it was primarily used as an identity-aware reverse proxy that forwarded or denied traffic to protected back-end applications.

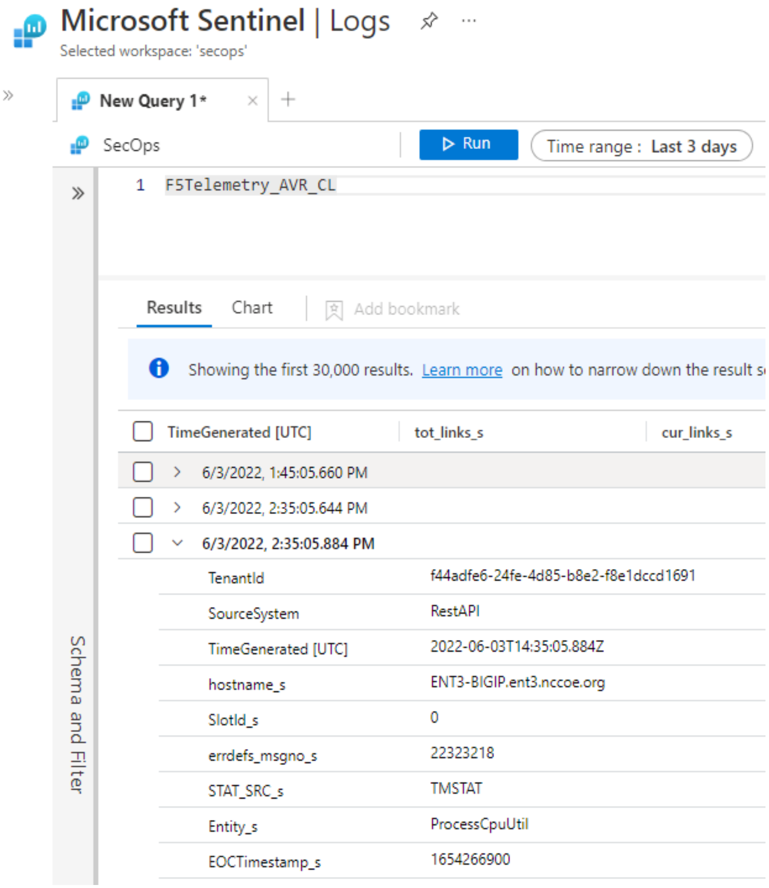
4.6.1 Installation, Configuration, and Integration

BIG-IP was deployed into the environment using a virtual machine image or open virtual appliance (OVA) file. Once this OVA import operation is complete, log into the virtual machine console and assign an IP address to a network interface, then continue configuration by connecting to its web interface. This BIG-IP image has both the Access Policy Manager (APM) and the Local Traffic Manager modules installed.

1. Deploy BIG-IP OVA into your VMWare environment.
2. Access the BIG-IP web interface by entering the IP address or DNS name into a web browser. Then complete the initial setup and configuration of BIG-IP.
3. Create virtual servers which map to back-end protected applications—in this build, to our Guacamole application server.
4. Configure BIG-IP to use Azure AD as the SAML IdP for external authentication to access back-end applications. The instructions at Configure BIG-IP Easy Button for Header Based SSO and the video at Azure AD and BIG-IP APM Integration Video provide additional references.
5. Once these instructions are completed, BIG-IP, leveraging Azure AD for external authentication, will only allow successfully authenticated and authorized users to access Guacamole. Access to the backend application is either done by connecting directly via the DNS name of the application or by going to **myapps.microsoft.com** and selecting the backend application icon, such as **F5 Guacamole_SSO** as shown below.



6. For this build, configure BIG-IP to send logs to Microsoft Sentinel. Then you can observe BIG-IP logs in Sentinel, as shown below.



```
1  F5Telemetry_AVR_CL
```

Showing the first 30,000 results. Learn more on how to narrow down the result s

TimeGenerated [UTC]	tot_links_s	cur_links_s
6/3/2022, 1:45:05.660 PM		
6/3/2022, 2:35:05.644 PM		
6/3/2022, 2:35:05.884 PM		

TenantId	f44adfe6-24fe-4d85-b8e2-f8e1dccd1691
SourceSystem	RestAPI
TimeGenerated [UTC]	2022-06-03T14:35:05.884Z
hostname_s	ENT3-BIGIP.ent3.nccoe.org
SlotId_s	0
errdefs_msgno_s	22323218
STAT_SRC_s	TMSTAT
Entity_s	ProcessCpuUtil
EOCTimestamp_s	1654266900

4.7 Lookout Mobile Endpoint Security (MES)

Lookout Mobile Endpoint Security (MES) solution is used to control mobile device access to corporate resources based on risk assessment. Risk is assessed based on information collected from devices by the

Lookout service. Lookout then communicates this risk level to the MDM (Microsoft Endpoint Manager (Intune)) which determines whether the device is compliant or not.

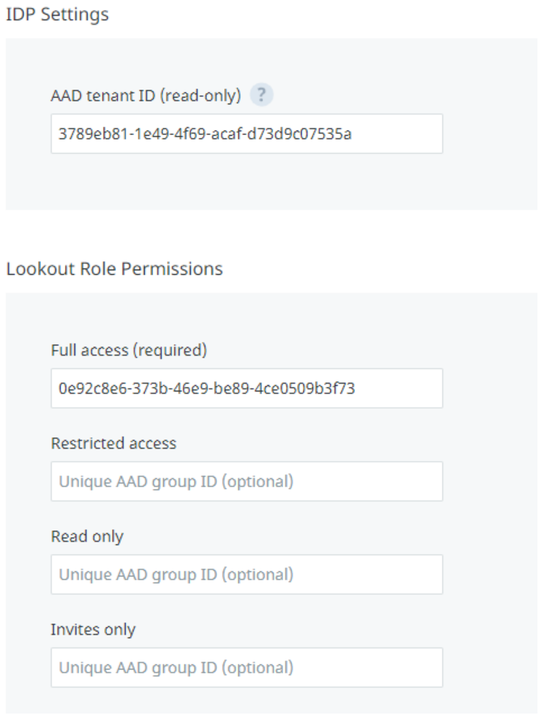
4.7.1 Configuration and Integration

Before configuring Lookout, collect the following information from Azure AD: **Azure AD tenant ID** and **Azure AD group object ID**.

1. Go to **Azure Active Directory** > **Properties** and locate **Tenant ID.** Copy and save it to the text file.
2. Go to **Azure Active Directory** > **Groups** to open the **Groups | All groups** pane.
3. Select the group with full access *rights* (Lookout Admin group).
4. Copy the (group) **Object Id,** and then save it in a text file.

The following steps are to be completed in the Lookout Enterprise admin console and will enable a connection to Lookout's service for Intune enrolled devices.

1. Sign in to the Lookout for Work console and go to **System** > **Integrations**, and then select **Choose a product to set up**. Select **Microsoft Azure**. Copy and paste the Azure AD (AAD) tenant ID and group object ID from the text file that was created in previous steps.



IDP Settings

AAD tenant ID (read-only): 3789eb81-1e49-4f69-acaf-d73d9c07535a

Lookout Role Permissions

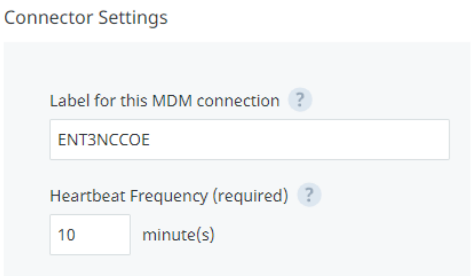
Full access (required): 0e92c8e6-373b-46e9-be89-4ce0509b3f73

Restricted access: Unique AAD group ID (optional)

Read only: Unique AAD group ID (optional)

Invites only: Unique AAD group ID (optional)

2. Stay in **System** > **Integrations**, and then select **Choose a product to set up.** Select Microsoft **Intune**.
3. Configure Intune connector settings.



Connector Settings

Label for this MDM connection ?

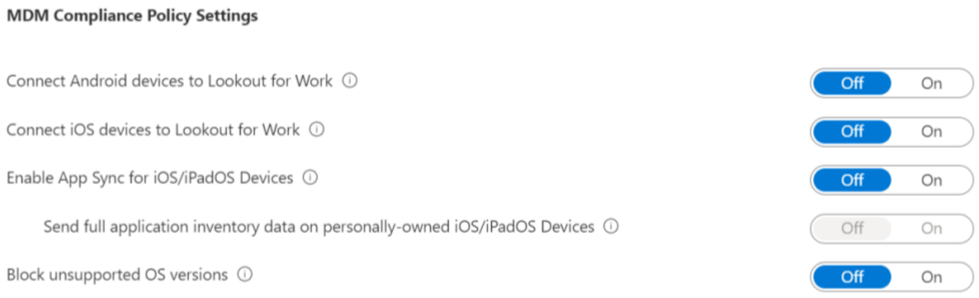
ENT3NCCOE

Heartbeat Frequency (required) ?

10 minute(s)

After Lookout MES is enabled, a connection to Lookout in Intune needs to be set up.

1. Go back to Microsoft Endpoint Manager and enable the Mobile Threat Defense connector there.
2. Select **Tenant administration > Connectors and tokens > Mobile Threat Defense.**
3. On the **Mobile Threat Defense** pane, select **Add.**
4. For **Mobile Threat Defense connector to setup,** select **Lookout** MTD solution from the drop-down list.
5. Configure the toggle options according to the organization's requirements. This screenshot shows examples.



MDM Compliance Policy Settings

Connect Android devices to Lookout for Work ⓘ [✓ Off] On

Connect iOS devices to Lookout for Work ⓘ [✓ Off] On

Enable App Sync for iOS/iPadOS Devices ⓘ [✓ Off] On

Send full application inventory data on personally-owned iOS/iPadOS Devices ⓘ Off On

Block unsupported OS versions ⓘ [✓ Off] On

When Lookout is integrated with Intune MTD and the connection to Intune is enabled, Intune creates a classic conditional access policy in Azure AD. To view classic conditional access policy, go to **Azure Active Directory > Conditional Access > Classic policies**. Classic conditional access policy is used by Intune MTD to require that devices are registered in Azure AD so that they have a device ID before communicating to Lookout MTD. The ID is required so that devices can report their status to Intune.

4.7.2 Create MTD Device Compliance Policy with Intune

Compliance policy is needed to detect threats and assess risks on mobile devices to determine if a device is compliant or not.

1. Open the Microsoft Endpoint Manager admin center.
2. Select **Endpoint security > Device Compliance > Create Policy.**
3. Select the **Platform,** and then **Create.**
4. On **Basics,** provide **Name** and **Description.** Select **Next** to continue.
5. On **Compliance settings,** expand and configure **Device Health.** Choose the Mobile Threat Level from the drop-down list for **Require the device to be at or under the Device Threat Level.** Choose the level for compliance.
6. Select **Next** to go to **Assignments.** Select the groups or users to which this policy should be assigned.

4.8 PC Matic Pro

PC Matic Pro is an endpoint protection system that consists of a server for centralized management and agents installed on endpoints. In addition to scanning for malware, it uses a default-deny approach in preventing malicious or unauthorized programs and processes from executing. To configure PC Matic Pro, you will need to install the server, install the agents, and configure a list of allowed software.

PC Matic Pro Server needs to be installed on a server with Windows 2019 Server and SQL server preinstalled.

1. Obtain the *OnPremInstallerRun.ps1* installation script from the vendor and open an elevated PowerShell window.
2. Execute the *OnPremInstallerRun.ps1* script by entering `.\OnPremInstallerRun.ps1 registryUser pcmatic -registryPwd <insert_password_here> -localDBUser pcm-app` to install docker, pull down the container images, and deploy the container instances that make up the PC Matic Pro server.
3. Navigate to the PC Matic web server and verify that it is operational by opening a web browser and going to *https://<pcmaticDNSName>/web_portal.* In this build, the DNS name is nist.pcmaticfederal.com; as such, to access the server’s web interface, we would go to https://nist.pcmaticfederal.com/web_portal.

Follow these steps to install PC Matic Endpoint Agents:

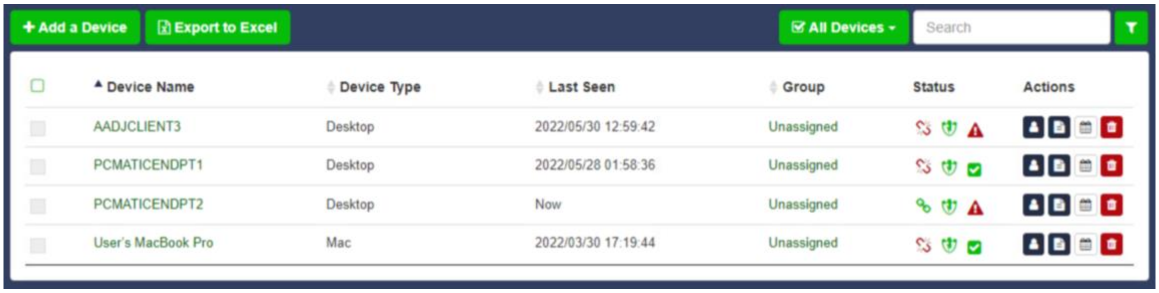
1. Open a web browser on a Windows or macOS client device. Navigate to the PC Matic Server web interface by browsing to https://nist.pcmaticfederal.com from the client device and log on with your credentials.

2. Click **Add a Device** and then click **Windows Installer** or **Mac Installer,** as appropriate, to download the PC Matic Endpoint Agent.

3. Install the agent.

4. Once installed, the agent will establish communications with the server and show up on the list of managed devices once you log on to the server as previously described.

5. Devices with an agent will register and come online.



□	Device Name	Device Type	Last Seen	Group	Status	Actions
□	AADJCLIENT3	Desktop	2022/05/30 12:59:42	Unassigned		
□	PCMATICENDPT1	Desktop	2022/05/28 01:58:36	Unassigned		
□	PCMATICENDPT2	Desktop	Now	Unassigned		
□	User's MacBook Pro	Mac	2022/03/30 17:19:44	Unassigned		

4.9 Tenable.io

For installation, configuration, and integration instructions, refer to Section 2.10.

4.9.1 Integration with Microsoft Sentinel

1. In Tenable.io, click the hamburger menu (☰) in the top left corner and navigate to **Settings > Access Control > Users.**

2. (Optional) Click **Create User** and create a new API user for Microsoft Sentinel. In this implementation, a standard administrator account was used.

3. Click the user who needs API keys generated. Then click **API KEYS > Generate > Continue.** Save the Access and Secret Keys, as they will not be shown again.

4. In Microsoft Sentinel, navigate to **Data Connectors.** Search *tenable* and click **Tenable.io Vulnerability Management (Preview) > Open Connector Page.**

5. Scroll down in the Instructions panel and save the Workspace ID and Primary Key.

6. Click **Deploy to Azure.**

7. Select the appropriate resource group.

8. In the Workspace ID and Workspace Key fields, enter the values obtained in step 5.
9. In the Tenable Access Key and Tenable Secret Key fields, enter the values obtained in step 3.
10. Click **Review + create.**
11. Click **Create.** Function deployment will begin. Once deployment is complete, it will take some time before Sentinel begins making calls to Tenable.io.

4.10 Tenable.ad

For installation, configuration, and integration instructions, refer to Section 2.11.

4.11 Tenable NNM

For installation, configuration, and integration instructions, refer to Section 2.12.

4.12 Mandiant Security Validation (MSV)

For installation, configuration, and integration instructions, refer to Section 2.13.

4.13 Forescout eyeSight

Forescout eyeSight provides asset discovery with both active and passive techniques, and through integrations with network and security infrastructure. In this build, Forescout was deployed on-premises in two virtual hosts: an Enterprise Manager and Forescout Appliance.

For Forescout installation instructions, visit the Forescout Installation Overview.

4.13.1 Integration with AD

1. In AD, create a domain administrator service account for Forescout and save the credentials.
2. In the Forescout console, navigate to **Tools > Options > HPS Inspection Engine.**
3. In the **Domain Credentials** section, click the **Add** button.
4. Enter the domain information and credentials you saved earlier. Click **OK.**
5. Click **Apply.** After the new configuration is saved, click **Test** to verify that the credentials are working as expected.

4.13.2 Integration with Cisco Switch

For Cisco Switch integration instructions, visit the Switch Plugin Configuration Guide.

4.13.3 Integration with Cisco Wireless Controller

For Cisco Wireless Controller integration instructions, visit the Wireless Plugin Configuration Guide.

4.13.4 Integration with Microsoft Sentinel

1. In the Forescout console, navigate to **Tools > Options > CEF.**
2. Click **Add.**
3. In the Add Server dialog, enter a Name, select **Use UDP for Connection,** and enter the IP address of the Sentinel Log Forwarder. Click **Next.**
4. Click the **Assign CounterACT Devices** radio button, and check all of the checkboxes next to the listed devices.
5. Click **Finish.** Verify that logs are being received by the Sentinel Log Forwarder.

4.13.5 Integration with Palo Alto Networks NGFW

For Palo Alto Networks Next-Generation Firewall (NGFW) integration instructions, visit the eyeExtend for Palo Alto Networks Next-Generation Firewall Configuration Guide.

4.13.6 Integration with Tenable.io

For Tenable.io integration instructions, visit the eyeExtend for Tenable.io Vulnerability Management Configuration Guide.

4.14 Palo Alto Networks Next Generation Firewall

For installation, configuration, and integration instructions, refer to Section 3.5.

4.15 DigiCert CertCentral

For setup and usage instructions, refer to Section 2.14.

5 Enterprise 4 Build 1 (EIG E4B1) Product Guides

This section will be completed during the next phase.

6 Enterprise 1 Build 2 (EIG E1B2) Product Guides

This section of the practice guide contains detailed instructions for installing, configuring, and integrating all of the products used to implement EIG E1B2. For additional details on EIG E1B2's logical and physical architectures, please refer to Volume B.

6.1 Zscaler

Zscaler provides secure user access to public-facing sites and on- or off-premises private applications via the Zscaler Zero Trust Exchange, a cloud-delivered security service edge technology. The Zscaler Internet Access (ZIA) manages user access to the internet. Zscaler Private Access (ZPA) manages user access to applications within an enterprise. Zscaler integrates with Okta for authentication and authorization of users.

To begin, contact Zscaler to create an instance of ZIA and ZPA. To do this, Zscaler will need the FQDN of the enterprise using ZIA and ZPA. Admin user information will need to be provided to Zscaler to create admin accounts. Refer to documents for ZIA and ZPA.

6.1.1 Zscaler ZPA Configuration and Integration

Once admin access available, log in to ZPA to perform the following:

1. Create additional admin accounts as needed.
2. Create an Zscaler App Connector Group and Zscaler App Connector in the ZPA portal. Note: App Connector Groups are recommended by Zscaler for availability and scaling. Note: This build has two App Connector Groups, one for on-prem applications and one for cloud applications in AWS.
3. Once the App Connector is configured in the ZPA portal, install the actual Zscaler App connector. Refer to the Zscaler Application Connector section below. Note: This build has two App Connectors, one for on-prem applications and one for cloud applications in AWS.
4. Create integration with Okta. All users accessing resources within the enterprise will use two-factor authentication when logging into the Zscaler Client Connector. Note: Step 1 of configuration is completed in the Okta cloud. Refer to Section 6.2. Step 2 of configuration is completed on the ZPA admin portal.
5. Deploy Zscaler Client Connectors (ZCCs) for various endpoints, including configuring ZCC policies to control the settings and behavior of ZCC. Refer to the Zscaler Client Connector section below.
6. Set up ZPA Application configuration for access to resources. In this step, applications are defined and applied to segments so that the proper App Connector can perform PEP functions.
7. Configure Access Policies to control user access to various applications. For our policies, we defined specific App Segments, configured specific IDP authentication parameters, and configured client posture checks.
8. Configure a log receiver for the IBM QRadar SIEM tool to receive logs for ZPA.

6.1.2 Zscaler ZIA Configuration

Once admin access is available, login to ZIA to perform the following:

1. Create additional admin accounts as needed.
2. Set up IdP integration with Okta.
3. Create policies to manage user access to various resources on the internet. For this build, we used many of the defaults built into ZIA. We created policies to allow certain users access to a resource on the internet and block certain users based on their role and time of day.
4. Integrate ZIA Nanolog Streaming Service with IBM QRadar SIEM tool to receive ZIA logs.

6.1.3 Zscaler Client Connector

Zscaler Client Connectors (ZCCs) are available for Windows, Mac, Linux, iOS, and Android endpoints. Deployment of ZCC includes configuring ZCC policies to control the settings and behavior of ZCC. For all these endpoints, a device manager can be leveraged to push the ZCC. For this build, we tested the use of Ivanti to push ZCC to Windows, iOS, and Android endpoints. For other devices we manually installed ZCC. Once ZCC is installed, users are prompted to login, which allows the user and device to be managed by ZPA and ZIA, depending on the type of resource the user is accessing.

6.1.4 Zscaler Application Connector

The Zscaler Application Connector is installed and configured on the same subnet where the resource will be protected. For this build, we use the documentation for Linux OS to install the App Connector. Zscaler supports other operating systems. Repeat steps 1 and 2 in the configuration section if an application residing in a different subnet segment needs to be protected. If that application is in the same subnet, then only one App Connector is needed to protect both applications.

6.2 Okta Identity Cloud

For this build, the integration between Okta and Ivanti was disabled in Okta Identity Cloud. Users logging into a resource are authenticated via Okta with a password for the first factor and Okta Verify for the second factor. Use the link for integration with Zscaler to configure Okta.

No changes were made from Build 1 Sections 2.1.2 and 2.1.3 (Okta Access Gateway). Refer to those sections for configuration details.

6.3 Radiant Logic RadiantOne

No changes were made from Build 1. Refer to Section 2.2.

6.4 SailPoint IdentityIQ

No changes were made from Build 1. Refer to Section 2.3.

6.5 Ivanti Neurons for UEM

No significant changes were made from Build 1. Ivanti Neurons for UEM was configured to deploy the Zscaler Client Connector to managed devices. For information, configuration and integration instructions, refer to Section 2.4.

6.6 IBM Security QRadar XDR

For installation, configuration, and integration instructions, refer to Section 2.9.

6.7 Tenable.io

For installation, configuration, and integration instructions, refer to Section 2.10.

6.8 Tenable.ad

For installation, configuration, and integration instructions, refer to Section 2.11.

6.9 Tenable NNM

For installation, configuration, and integration instructions, refer to Section 2.12.

6.10 Mandiant Security Validation (MSV)

For installation, configuration, and integration instructions, refer to Section 2.13.

6.11 DigiCert CertCentral

For setup and usage instructions, refer to Section 2.14.

6.12 AWS IaaS

Amazon Web Services is a cloud computing platform provided by Amazon that includes a mixture of IaaS, platform-as-a-service (PaaS), and SaaS offerings. The following section describes the setup of AWS IaaS resources to serve as a public/private cloud host.

For details on the logical architecture the AWS environment, please refer to Volume B, Section 4.4.9.1.

6.12.1Configuration

The purpose of this subsection is to provide an outline of how to set up a cloud infrastructure to provide a platform to host public and private resources which integrate with products from EIG E1B2. AWS CloudFormation templates were used during the build of the AWS IaaS environment but are considered outside of the scope of this document. More information about CloudFormation may be found here.

1. Create and activate an AWS account. Use the root account to create administrative accounts with rights to create necessary resources for the project.
2. Create a Production and Management Virtual Private Cloud (VPC). Configure ingress and egress Security Group rules for each VPC.
3. Create Transit gateways to attach on-prem networks to the AWS environment. Create Internet gateways for access to the internet.
4. Within the Prod VPC, configure redundant public subnets in different Availability Zones for fault tolerance. Configure redundant private subnets for Web, Application, and Database tiers.
5. Set up resources for testing in the Prod VPC. For demonstration purposes, a private WordPress and GitLab server pair and a public WordPress server were built. Configure auto scaling and Elastic Load Balancing for servers/services set up on the Web, Application, and Database tiers.
6. Within the Mgmt VPC, configure redundant public subnets in different Availability Zones for fault tolerance. Configure private subnets for Satellite, Domain Controller, and Security Management Tiers.
7. Set up AWS Session Manager access for remote admins.
8. For shared AWS services, configure VPC endpoints with ICAM policies to control access.

7 Enterprise 3 Build 2 (EIG E3B2) Product Guides

This section of the practice guide contains detailed instructions for installing, configuring, and integrating all the products used to implement EIG E3B2. For additional details on EIG E3B2's logical and physical architectures, please refer to Volume B.

7.1 Microsoft Azure Active Directory (AD)

For setup and usage instructions, refer to Section 4.1.

7.2 Microsoft Azure AD Identity Protection

This section offers a guide for setting up the various components that make up Azure AD Identity Protection in your environment.

1. To ensure that all users register for multifactor authentication, configure Azure AD Multifactor Authentication registration policy using the information found at Configure MFA Registration Policy.
2. Sign-in risk policy enables detection of and response to suspicious logon sessions and unusual logon activity. Use the information found at Configure Sign-in Risk Policy to configure the sign-in risk policy.
3. User-risk policy enables detection of and response to compromised user accounts. To configure this policy, use the information found at Configure User-Risk Policy.

7.3 Microsoft Azure AD Identity Governance

Azure AD Identity Governance enables organizations to manage access to resources applying access request and approval workflows, access assignments and removals, access expiration, and access reviews.

1. Create an access package to encapsulate the target resources in a single object.
2. Create policies to define approvers and eligible requestors.
3. Requesting access to the access package can be done using the information found at Request access.
4. To approve or deny access requests, use the information found at Approve or deny request.

7.4 Microsoft Intune

For setup and usage instructions of Intune (formerly called Endpoint Manager), refer to Section 4.2.

7.5 Microsoft Defender for Endpoint

For setup and usage instructions, refer to Section 4.3.

7.6 Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a cloud access broker solution that protects cloud applications and on-premises web applications by monitoring session activity to those applications, ensuring compliance to defined policy and mitigating detected threats.

1. Login to the portal and activate your Defender for Cloud Apps tenant.
2. Connect your apps to Defender for Cloud Apps. For custom web applications including on-premises web applications, use the information on connecting a custom app to Defender for Cloud Apps to integrate your custom web applications.

3. Use the information on creating and assigning policies to provide security controls to apps, ensuring compliance and mitigating threats.

4. Deploy Conditional Access App Control, which leverages Azure AD conditional access policies and enforcement for connected apps.

7.7 Microsoft Azure AD Application Proxy

Azure AD Application Proxy enables users to securely connect to internal applications via the Internet. It has two components, Application Proxy service and Application Proxy connector, which work together to provide access to the internal application.

1. Configure Application Proxy deployment prerequisites.

2. Install and register the Application Proxy connectors. Once the application proxy connectors are successfully installed and registered, the Application Proxy service will be enabled automatically.

3. Add your application to Application Proxy.

7.8 Microsoft Defender for Cloud

Defender for Cloud is a SaaS-based cloud security posture management and cloud workload protection platform. It enables organizations to monitor their cloud and on-premises resources, determine differences and security issues based on benchmark and regulations, and provide recommendations to help remediate the issues. Within Defender for Cloud, benchmarks and regulations encapsulate policies that are used as baselines to measure how compliant your environment is. This leads to the generation of a secure score.

1. Enable Defender for Cloud for your subscription.

2. To receive a secure score, which provides a numeric value indicating your point-in-time security posture, you must ensure that the Azure Security Benchmark initiative or at least one other listed regulation are selected and applied to your subscription. Azure Security Benchmark should automatically apply to your subscription. Examples of regulations include PCI/DSS, HIPAA, and NIST SP 800-53. Azure Security Benchmark is comprised of a set of controls that detect security misconfigurations based on best practices from common compliance frameworks.

3. Apply regulations to your subscription.

4. Defender for Cloud will list recommendations for your environment to improve the security posture. Apply the listed security recommendations.

7.9 Microsoft Sentinel

For setup and usage instructions, refer to Section 4.4.

7.10 Microsoft Office 365

For setup and usage instructions, refer to Section 4.5.

7.11 F5 BIG-IP

For setup and usage instructions, refer to Section 4.6.

7.12 PC Matic Pro

For setup and usage instructions, refer to Section 4.8.

7.13 Tenable.io

For setup and usage instructions, refer to Section 2.10.

7.14 Tenable.ad

For setup and usage instructions, refer to Section 2.11.

7.15 Tenable NNM

For setup and usage instructions, refer to Section 2.12.

7.16 Mandiant Security Validation (MSV)

For setup and usage instructions, refer to Section 2.13.

7.17 Forescout eyeSight

Forescout eyeSight provides asset discovery with both active and passive techniques, and through integrations with network and security infrastructure.

For installation, configuration, and integration instructions, refer to Section 4.13.

7.18 Forescout eyeControl

Forescout eyeControl enforces and automates network policies across the enterprise.

For Forescout eyeControl installation instructions, visit the Forescout Installation Overview.

7.18.1 Configuring a policy

1. In the Forescout Console, choose a policy.
5. Select the network segment to which the policy will be applied.
6. Add **Conditions** to select the attributes of the hosts that the policy will be applied to.
7. Add **Actions** that will be applied to the selected hosts.
8. Add any additional rules that will be used in the policy.
9. Run the policy.

7.19 Forescout eyeSegment

Forescout eyeSegment accelerates zero trust segmentation through visibility into traffic and transaction flows.

For Forescout eyeSegment installation instructions, visit the Forescout Installation Overview. After installation has been completed, visit the eyeSegment Application How-to Guide to configure and use eyeSegment to analyze your network traffic from a dynamic zone perspective, simplify segmentation planning, and automate ACL/VLAN assignment.

7.19.1 Access the eyeSegment Dashboard

1. From the Forescout Console, click **Dashboards**. This will launch a web browser and authenticate to the Forescout Web Client.
2. At the top of the Forescout Web Client, click **Segmentation**.
3. The initial dashboard is the eyeSegment Matrix. This dashboard can be used to analyze traffic and transaction flows between different network hosts, segments, and groups.
4. Open the eyeSegment Policy dashboard, which can be used to apply proposed Zero Trust rules. The effect of these rules can be seen in the eyeSegment Matrix.
5. Open the eyeSegment Health dashboard, which provides information about Reporting Appliances, Traffic Sensors, Endpoint Coverage, and the connection to the eyeSegment cloud.

7.20 Forescout eyeExtend

Forescout eyeExtend automates security workflows across disparate products through integration with other security technologies.

For Forescout eyeExtend installation instructions, visit the Forescout Installation Overview. Once installation has been completed, visit the Connect Plugin Configuration Guide, which provides the capability to build custom integrations with products that are not already provided. However, Forescout also provides a wide range of integrations at the official Forescout eyeExtend repository.

7.20.1 Integration with Microsoft Endpoint Manager

Integration instructions for Microsoft Endpoint Manager can be found at Forescout's official GitHub repository: https://github.com/Forescout/eyeExtend-Connect/tree/master/Intune.

7.21 Palo Alto Next Generation Firewall

For setup and usage instructions, refer to Section 3.5.

7.22 DigiCert CertCentral

For setup and usage instructions, refer to Section 2.14.

7.23 Microsoft Azure IaaS

Azure IaaS provides compute, networking, and storage services that enable the creation of an enterprise IT infrastructure by subscribers. The following section describes the Azure IaaS components that were deployed in this build.

1. Virtual Networks (VNETs) are isolated customer networks. They contain subnets and are built in Azure. We have three VNETs, hub VNET which provides central connectivity for other VNETs, and two additional VNETs, a GitLab VNET and a WordPress VNET, designed to protect individual apps and their associated resources. Use the information at Create a VNET to create and configure a virtual network. To enable communication between the hub and other VNETs, establish peering between them.

2. Public VNETs are regular VNETs that have hosts with public IP addresses. The GitLab VNET is configured as public subnet with a public IP address attached to the Application Gateway which was configured to provide load balancing and protection against common web attacks.

3. Private VNETs are regular VNETs that have hosts with only private IP addresses and are reachable only by internal users by default. WordPress VNET was configured as a private VNET.

4. Configure Azure Bastion to enable web-based SSH and remote desktop-based access to servers and virtual machines.

5. Instantiate and configure Azure Firewall in the hub VNET to provide protection for incoming traffic from both the Internet and the VPN traffic from on-prem clients.

6. Use network security groups (NSGs) to filter inbound or outbound traffic to or from Azure resources. Enable only ports that are necessary for appropriate access.

7. Azure App Gateway is a web traffic load balancer that can detect and stop common web attacks. The Azure App Gateway was configured to protect the GitLab application servers, as the WordPress servers. Use the information at Application Gateway Quickstart to configure the Application Gateway.

1793 Appendix A List of Acronyms

AAD	(Microsoft) Azure Active Directory
AD	Active Directory
AG	(Okta) Access Gateway
API	Application Programming Interface
APM	Access Policy Manager
APNs	Apple Push Notification service
CA	Certificate Authority
CEF	Common Event Format
CRADA	Cooperative Research and Development Agreement
CSR	Certificate Signing Request
DN	Domain Name
DNS	Domain Name System
E1B1	EIG Enterprise 1 Build 1
E1B2	EIG Enterprise 1 Build 2
E2B1	EIG Enterprise 2 Build 1
E3B1	EIG Enterprise 3 Build 1
E3B2	EIG Enterprise 3 Build 2
EDR	Endpoint Detection and Response
EIG	Enhanced Identity Governance
EO	Executive Order
FQDN	Fully Qualified Domain Name
HDAP	High-Availability Directory Access Protocol
HR	Human Resources
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code

ICAM	Identity, Credential, and Access Management
IdP	Identity Provider
IP	Internet Protocol
IT	Information Technology
ITL	Information Technology Laboratory
LDAP	Lightweight Directory Access Protocol
MAM	Mobile Access Management
MDM	Mobile Device Management
MEM	Microsoft Endpoint Manager
MES	(Lookout) Mobile Endpoint Security
MFA	Multi-Factor Authentication
MSV	Mandiant Security Validation
MTD	Mobile Threat Defense
NCCoE	National Cybersecurity Center of Excellence
NGFW	Next-Generation Firewall
NIST	National Institute of Standards and Technology
NNM	(Tenable) Nessus Network Monitor
NSG	Network Security Group
NTP	Network Time Protocol
OS	Operating System
OU	Organizational Unit
OVA	Okta Verify App, Open Virtual Appliance
PA	Policy Administration
PaaS	Platform as a Service
PDP	Policy Decision Point
PE	Policy Engine

PEP	Policy Enforcement Point
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
SP	Special Publication
SSL	Secure Sockets Layer
SSO	Single Sign-On
SSPR	Single Sign-On Password Reset
TLS	Transport Layer Security
UAC	User Account Control
UDP	User Datagram Protocol
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VNET	Virtual Network
VPC	Virtual Private Cloud
VPN	Virtual Private Network
ZCC	Zscaler Client Connector
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access
ZSO	Zero Sign-On
ZTA	Zero Trust Architecture