

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 Coclinn
DigiCert
Lehi, UT

Ryan Johnson
Dung Lam
F5
Seattle, WA

Neal Lucier
Tom May
Forescout
San Jose, CA

Tim Knudsen
Google Cloud
Mill Valley, CA

Harmeet Singh
Krishna Yellepeddy
IBM
Armonk, NY

Corey Lund
Farhan Saifudin
Ivanti
South Jordan, UT

Hashim Khan
Tim LeMaster
Lookout
Reston, VA

James Elliott
David Pricer
Mandiant
Reston, VA

Clay Taylor
Tarek Dawoud
Microsoft
Redmond, WA

Vinu Panicker
Okta
San Francisco, CA

Andrew Keffalas
Norman Wong
Palo Alto Networks
Santa Clara, CA

Rob Woodworth
Shawn Higgins
PC Matic
Myrtle Beach, SC

Bryan Rosensteel
Ivan Anderson
Ping Identity
Denver, CO

Wade Ellery
John Petrutiu
Radiant Logic
Novato, CA

Frank Briguglio
Ryan Tighe
SailPoint
Austin, TX

Chris Jensen
Joshua Moll
Tenable
Columbia, MD

Jason White
Trellix, Public Sector
Reston, VA

Jacob Rapp
Paul Mancuso
VMware
Palo Alto, CA

Joe Brown
Jim Kovach
Zimperium
Dallas, TX

Bob Smith
Syed Ali
Zscaler
San Jose, CA

August 2022

PRELIMINARY DRAFT

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



DISCLAIMER

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

8 While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk
9 through outreach and application of standards and best practices, it is the stakeholder's responsibility to
10 fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise,
11 and the impact should the threat be realized before adopting cybersecurity measures such as this
12 recommendation.

13 National Institute of Standards and Technology Special Publication 1800-35C, Natl. Inst. Stand. Technol.
14 Spec. Publ. 1800-35C, 83 pages, (August 2022), CODEN: NSPUE2

15 FEEDBACK

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

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

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

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

27 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

43 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

53 **ABSTRACT**

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

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

66 **KEYWORDS**

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

69 **ACKNOWLEDGMENTS**

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

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

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

Name	Organization
Ken Durbin	Mandiant
Earl Matthews	Mandiant
Joey Cruz	Microsoft
Janet Jones	Microsoft
Carmichael Patton	Microsoft
Hemma Prafullchandra	Microsoft
Brandon Stephenson	Microsoft
Sarah Young	Microsoft
Spike Dog	MITRE
Ayayidjin Gabiam	MITRE
Karri Meldorf	MITRE
Kenneth Sandlin	MITRE
Jessica Walton	MITRE
Mike Bartock	NIST
Oliver Borchert	NIST
Gini Khalsa	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
Bill Baz	Radiant Logic
Rusty Deaton	Radiant Logic
Deborah McGinn	Radiant Logic
Lauren Selby	Radiant Logic
Peter Amaral	SailPoint
Jim Russell	SailPoint
Esteban Soto	SailPoint
Jeremiah Stallcup	Tenable
Andrew Babakian	VMware
Dennis Moreau	VMware

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

71 The Technology Partners/Collaborators who participated in this build submitted their capabilities in
 72 response to a notice in the Federal Register. Respondents with relevant capabilities or product
 73 components were invited to sign a Cooperative Research and Development Agreement (CRADA) with
 74 NIST, allowing them to participate in a consortium to build this example solution. We worked with:

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

75 DOCUMENT CONVENTIONS

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

83 **CALL FOR PATENT CLAIMS**

84 This public review includes a call for information on essential patent claims (claims whose use would be
85 required for compliance with the guidance or requirements in this Information Technology Laboratory
86 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication
87 or by reference to another publication. This call also includes disclosure, where known, of the existence
88 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant
89 unexpired U.S. or foreign patents.

90 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in writ-
91 ten or electronic form, either:

92 a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not
93 currently intend holding any essential patent claim(s); or

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

97 1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination;
98 or

99 2. without compensation and under reasonable terms and conditions that are demonstrably free
100 of any unfair discrimination.

101 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
102 behalf) will include in any documents transferring ownership of patents subject to the assurance, provi-
103 sions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that
104 the transferee will similarly include appropriate provisions in the event of future transfers with the goal
105 of binding each successor-in-interest.

106 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of
107 whether such provisions are included in the relevant transfer documents.

108 Such statements should be addressed to: nccoe-zta-project@list.nist.gov

109	Contents	
110	1 Introduction.....	1
111	1.1 How to Use this Guide.....	1
112	1.2 Build Overview	3
113	1.2.1 EIG Crawl Phase Build Features	3
114	1.2.2 Physical Architecture Overview	4
115	1.3 Typographic Conventions.....	6
116	2 Enterprise 1 Build 1 (EIG E1B1) Product Guides	6
117	2.1 Okta Identity Cloud	7
118	2.1.1 Configuration and Integration	7
119	2.1.2 Okta Verify App.....	10
120	2.1.3 Okta Access Gateway.....	10
121	2.2 Radiant Logic RadiantOne	11
122	2.2.1 Installation	11
123	2.2.2 Configuration	11
124	2.2.3 Integration	15
125	2.3 SailPoint IdentityIQ.....	16
126	2.3.1 Installation and Configuration	16
127	2.3.2 Integration with Radiant Logic.....	26
128	2.3.3 Integration with AD.....	27
129	2.3.4 Integration with Okta.....	28
130	2.4 Ivanti Neurons for UEM.....	29
131	2.4.1 Installation and Configuration	29
132	2.4.2 Integration with Ivanti Connector	34
133	2.4.3 Integration with Okta.....	35
134	2.5 Ivanti Sentry.....	36
135	2.5.1 Installation and Configuration	36
136	2.5.2 Ivanti Tunnel Configuration and Deployment	36
137	2.6 Ivanti Access ZSO	37

138	2.6.1 Integration with Ivanti Neurons for UEM	37
139	2.6.2 Integration with Okta.....	38
140	2.7 Zimperium Mobile Threat Defense (MTD)	38
141	2.7.1 Installation, Configuration, and Integration	38
142	2.8 IBM Cloud Pak for Security.....	42
143	2.9 IBM Security QRadar XDR.....	43
144	2.10 Tenable.io	43
145	2.10.1 Installation and Configuration	43
146	2.10.2 Integration with QRadar	44
147	2.11 Tenable.ad	45
148	2.12 Mandiant Security Validation (MSV).....	45
149	2.12.1 MSV Director Installation/Configuration	45
150	2.12.2 MSV Network Actor Installation/Configuration.....	46
151	2.12.3 MSV Endpoint Actor Installation/Configuration	46
152	2.12.4 MSV Evaluation Configuration.....	47
153	2.12.5 MSV Evaluation Execution	48
154	2.13 DigiCert CertCentral	49
155	2.14 AWS IaaS.....	49
156	3 Enterprise 3 Build 1 (EIG E3B1) Product Guides	49
157	3.1 Microsoft Azure Active Directory (AD).....	49
158	3.2 Microsoft Endpoint Manager	50
159	3.2.1 Configuration and Integration	50
160	3.3 Microsoft Defender for Endpoint.....	55
161	3.3.1 Configuration and Integration	55
162	3.3.2 Microsoft Defender Antivirus	59
163	3.4 Microsoft Sentinel	60
164	3.5 F5 BIG-IP	60
165	3.5.1 Installation, Configuration, and Integration	61
166	3.6 Lookout Mobile Endpoint Security (MES)	62
167	3.6.1 Configuration and Integration	62

168	3.6.2 Create MTD device compliance policy with Intune	64
169	3.7 PC Matic Pro	65
170	3.8 Tenable.io	66
171	3.8.1 Integration with Microsoft Sentinel.....	66
172	3.9 Tenable.ad	66
173	3.10 Mandiant Security Validation (MSV).....	67
174	3.11 Forescout eyeSight	67
175	3.11.1 Integration with AD.....	67
176	3.11.2 Integration with Cisco Switch	67
177	3.11.3 Integration with Cisco Wireless Controller.....	67
178	3.11.4 Integration with Microsoft Sentinel.....	67
179	3.11.5 Integration with Palo Alto Networks NGFW	68
180	3.11.6 Integration with Tenable.io	68
181	3.12 Palo Alto Next Generation Firewall.....	68
182	3.13 DigiCert CertCentral	68
183	Appendix A List of Acronyms	69
184	List of Figures	
185	Figure 1-1 Laboratory Infrastructure for the EIG Builds.....	5

186 1 Introduction

187 The following volumes of this guide show information technology (IT) professionals and security
188 engineers how we implemented two example zero trust architecture (ZTA) solutions. We cover all of the
189 products employed in this reference design. We do not recreate the product manufacturers'
190 documentation, which is presumed to be widely available. Rather, these volumes show how we
191 incorporated the products together in our environment to create two example solutions.

192 *Note: These are not comprehensive tutorials. There are many possible service and security configurations
193 for these products that are out of scope for this reference design.*

194 1.1 How to Use this Guide

195 This NIST Cybersecurity Practice Guide will help users develop a plan for migrating to ZTA. It
196 demonstrates a standards-based reference design for implementing a ZTA and provides users with the
197 information they need to replicate two different implementations of this reference design. Each of these
198 implementations, which are known as *builds*, are standards-based and align to the concepts and
199 principles in NIST Special Publication (SP) 800-27, *Zero Trust Architecture*. The reference design
200 described in this practice guide is modular and can be deployed in whole or in part, enabling
201 organizations to incorporate ZTA into their legacy environments gradually, in a process of continuous
202 improvement that brings them closer and closer to achieving the ZTA goals that they have prioritized
203 based on risk, cost, and resources.

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

208 When complete, this guide will contain four volumes:

- 209 ■ NIST SP 1800-35A: *Executive Summary* – why we wrote this guide, the challenge we address,
210 why it could be important to your organization, and our approach to solving this challenge
- 211 ■ NIST SP 1800-35B: *Approach, Architecture, and Security Characteristics* – what we built and why
- 212 ■ NIST SP 1800-35C: *How-To Guides* – instructions for building the example implementations,
213 including all the security-relevant details that would allow you to replicate all or parts of this
214 project (**you are here**)
- 215 ■ NIST SP 1800-35D: *Functional Demonstrations* – use cases that have been defined to showcase
216 ZTA security capabilities and the results of demonstrating them with each of the example
217 implementations

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

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

- 221 ▪ challenges that enterprises face in migrating to the use of ZTA
222 ▪ example solution built at the National Cybersecurity Center of Excellence (NCCoE)
223 ▪ benefits of adopting the example solution

224 **Technology or security program managers** who are concerned with how to identify, understand, assess,
225 and mitigate risk will be interested in this part of the guide, NIST SP 1800-35B, which describes what we
226 did and why.

227 You might share the *Executive Summary*, NIST SP 1800-35A, with your leadership team members to help
228 them understand the importance of migrating toward standards-based ZTA implementations that align
229 to the concepts and principles in NIST SP 800-207, *Zero Trust Architecture*.

230 **IT professionals** who want to implement similar solutions will find the whole practice guide useful. You
231 can use the how-to portion of the guide, NIST SP 1800-35C, to replicate all or parts of the builds created
232 in our lab. The how-to portion of the guide provides specific product installation, configuration, and
233 integration instructions for implementing the example solution. We do not re-create the product
234 manufacturers' documentation, which is generally widely available. Rather, we show how we
235 incorporated the products together in our environment to create an example solution. Also, you can use
236 *Functional Demonstrations*, NIST SP 1800-35D, which provides the use cases that have been defined to
237 showcase ZTA security capabilities and the results of demonstrating them with each of the example
238 implementations.

239 This guide assumes that IT professionals have experience implementing security products within the
240 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
241 not endorse these particular products. Your organization can adopt this solution or one that adheres to
242 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
243 parts of a ZTA. Your organization's security experts should identify the products that will best integrate
244 with your existing tools and IT system infrastructure. We hope that you will seek products that are
245 congruent with applicable standards and best practices.

246 A NIST Cybersecurity Practice Guide does not describe "the" solution, but example solutions. This is a
247 preliminary draft guide. As the project progresses, the preliminary draft will be updated, and additional
248 volumes will also be released for comment. We seek feedback on the publication's contents and
249 welcome your input. Comments, suggestions, and success stories will improve subsequent versions of
250 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, 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. After completing the EIG crawl phase builds, our plan is to gradually enhance these implementations by adding specialized PE and PA components, as well as capabilities such as software defined perimeter and micro-segmentation.

This practice guide provides instructions for reproducing the two EIG crawl phase builds that we have implemented so far: EIG Enterprise 1 Build 1 (E1B1) and EIG Enterprise 3 Build 1 (E3B1). 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 two builds are as follows:

- EIG E1B1 uses products from IBM, Ivanti, Mandiant, Okta, Radiant Logic, SailPoint, Tenable, and Zimperium. Certificates from DigiCert are also used.

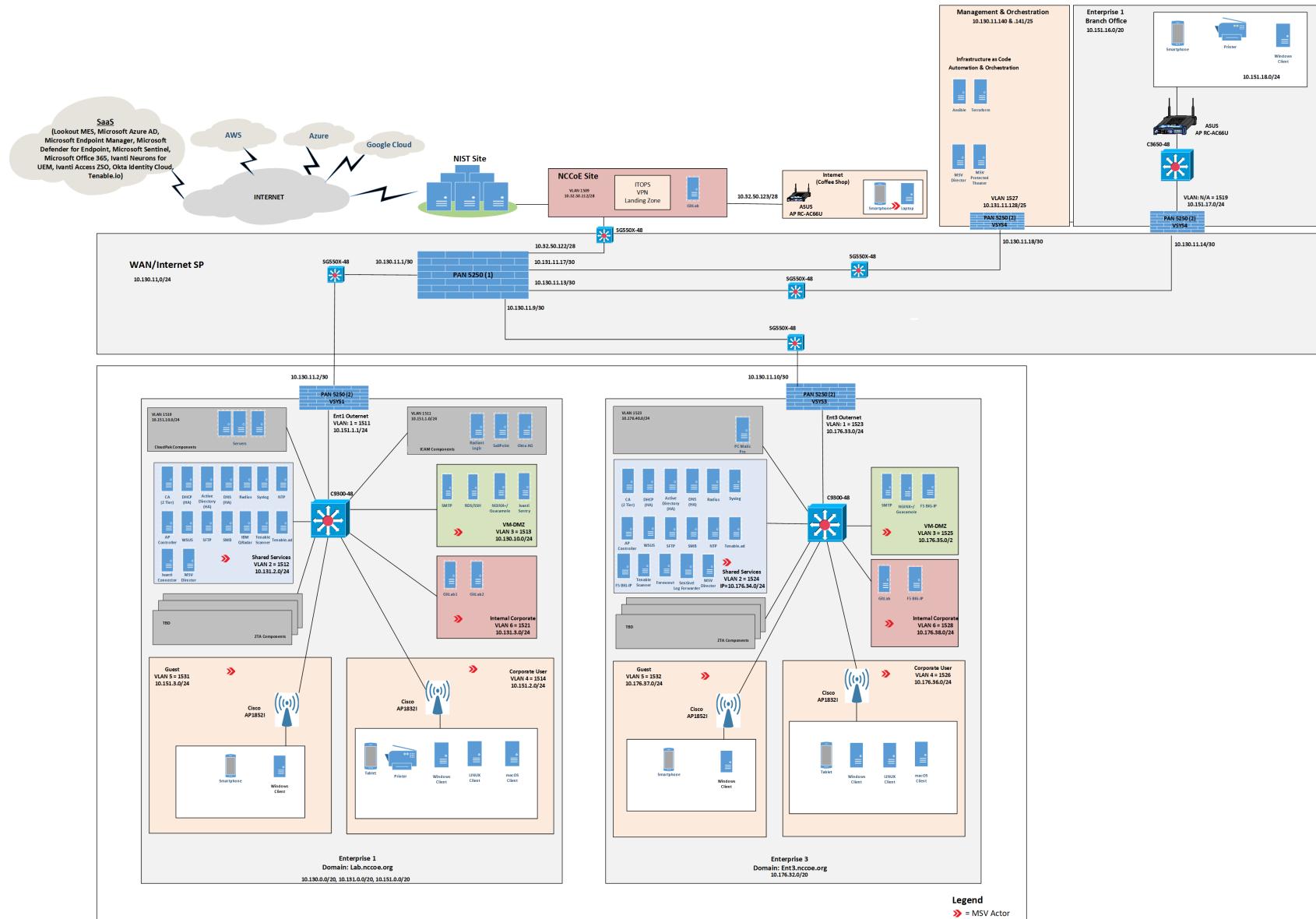
- 286 ■ EIG E3B1 uses products from F5, Forescout, Lookout, Mandiant, Microsoft, Palo Alto Networks,
287 PC Matic, and Tenable. Certificates from DigiCert are also used.

288

1.2.2 Physical Architecture Overview

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

298 Figure 1-1 Laboratory Infrastructure for the EIG Builds



299 The following two EIG crawl phase builds are supported within the physical architecture depicted in
 300 [Figure 1-1](#) and documented in the remainder of this guide:

- 301 ▪ EIG E1B1 components consist of DigiCert CertCentral, IBM Cloud Pak for Security, IBM Security
 302 QRadar XDR, Ivanti Access ZSO, Ivanti Neurons for UEM, Ivanti Sentry, Ivanti Tunnel, Mandiant
 303 Advantage Security Validation (MSV), Okta Identity Cloud, Okta Verify App, Radiant Logic
 304 RadiantOne Intelligent Identity Data Platform, SailPoint IdentityIQ, Tenable.ad, Tenable.io, and
 305 Zimperium MTD.
- 306 ▪ EIG E3B1 components consist of DigiCert CertCentral, F5 BIG-IP, Forescout eyeSight, Lookout
 307 MES, Mandiant MSV, Microsoft Azure AD, Microsoft Defender for Endpoint, Microsoft Endpoint
 308 Manager, Microsoft Sentinel, Palo Alto Networks NGFW, PC Matic Pro, Tenable.ad, and
 309 Tenable.io.

310 For a detailed description of the architecture of each build, see Volume B, Appendices D and F. The
 311 remainder of this guide describes how to implement the EIG crawl phase builds E1B1 and E3B1.

312 **1.3 Typographic Conventions**

313 The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
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	<code>mkdir</code>
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 .

314 **2 Enterprise 1 Build 1 (EIG E1B1) Product Guides**

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

318 **2.1 Okta Identity Cloud**

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

324 **2.1.1 Configuration and Integration**

325 The purpose is to set up integrations with other ICAM tools so Okta can manage authentication and
326 authorization of users accessing resources.

- 327 1. Sign up for an account with Okta (okta.com).
- 328 2. Set up an admin account, then set up Okta Verify for the admin account. (Repeat this step if
329 needed so each administrator has a unique account.)
- 330 3. Log in to the Okta instance that was just created and into the admin account.
- 331 4. Set up directory integration with Radiant Logic. User identity information is pulled from Radiant
332 Logic into Okta for authentication and authorization. Note: This step should be completed after
333 Radiant Logic is configured.
 - 334 a. [Review the background information and check the prerequisites](#).
 - 335 b. [Install the Okta LDAP Agent on the Radiant Logic server and configure LDAP integration settings](#).
 - 336 c. [Configure the LDAP Interface](#). Note that the service account and password that was created in Radiant Logic is used in this step.
 - 337 d. [Once LDAP integration is successful, users from Radiant Logic can be imported into Okta](#).
- 341 5. Create Groups for Okta to apply a specific set of users to specific services or applications. From
342 the main menu, navigate to **Directory > Groups** and click on the **Add Group** button. Create the
343 name and description of the group and click **Save**.
- 344 6. Create API tokens to be used by SailPoint and Radiant Logic for communication.
 - 345 a. From the main menu, navigate to **Security > API** and click on the **Create Token** button.
346 Type in the name for SailPoint and click **Create Token**.

- 347 b. Copy the token. It will be used in the SailPoint configuration. Once we configure Sail-
348 Point, the integration is complete. Please refer to the “Integration with Okta” subsection
349 within SailPoint for integration configuration.
- 350 c. Repeat these steps to [create a token for Radiant Logic](#).
- 351 7. [Create a delegated authentication for Okta to be able to import users from Radiant Logic via](#)
352 [LDAP](#). Note that a service account, created in the Radiant Logic Integration section of this docu-
353 ment, needs to be created and used in this configuration.
- 354 8. Okta Access Gateway needs to be installed in order to configure on-premises applications. See
355 Section 2.1.3 for installation instructions, which include information on configuring on-premises
356 applications.
- 357 9. Create application integration for Ivanti Neurons for UEM.
- 358 a. From the Okta admin page, select **Applications** from the **Application** drop-down menu.
- 359 b. Click on the **Browse App Catalog** button. Type “MobileIron” and select the “MobileIron
360 Cloud” app.
- 361 c. Follow the step-by-step instructions to configure the app.
- 362 10. Create Identity Provider integration for Ivanti Access ZSO. This involves [creating a custom appli-](#)
363 [cation using SAML](#) and then [creating a SAML Identity Provider](#).
- 364 11. [Configure Device Trust on iOS and Android devices to create device integrations](#).
- 365 12. [Create authentication policies](#). By default, a “Catch All” policy is created when an application is
366 created. We are creating an authentication policy that will allow Okta to trust Ivanti Access ZSO
367 to be the delegated Identity Provider (IdP). To do this, when Okta checks that Okta Verify is a
368 managed application on a device, it will delegate authentication to Ivanti Access ZSO. The
369 screenshots below show the current policy created for the GitLab1 application. Note that iOS
370 and Android devices are managed in the first policy.

1 For-MobileIron

ENABLED Actions ▾

IF

- User type: Any
- Group: Any
- User Is: Any
- Zone: Any
- Risk: Any
- Device: Registered, Managed
- Platform: iOS, Android

⋮

THEN

Access:

- Allowed after successful authentication

User must authenticate with:

- Any 2 factor types

Access with Okta FastPass is granted:

If the user approves a prompt in Okta Verify or provides biometrics (meets NIST AAL2 requirements)

Available Authenticators:

- Knowledge / Biometric factor types
- Okta Verify* or Password / IdP or Security Question**

AND

Additional factor types

- Okta Verify*

*authenticator that may satisfy multiple factor requirements

**Security Questions can't be used with passwordless authentication. [Learn more.](#)

2 For Desktops	ENABLED Actions ▾
<p>IF</p> <ul style="list-style-type: none"> User type: Any Group: Any User Is: Any Zone: Any Risk: Any Device: Registered, Not managed Platform: MacOS, Windows 	<p>THEN</p> <p>Access:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Allowed after successful authentication <p>User must authenticate with:</p> <p>Password / IdP + Another factor</p> <p>Access with Okta FastPass is granted:</p> <p>If the user approves a prompt in Okta Verify or provides biometrics (meets NIST AAL2 requirements)</p> <p>Available Authenticators:</p> <ul style="list-style-type: none"> Password / IdP <p>AND</p> <p>Additional factor types</p> <ul style="list-style-type: none"> Okta Verify

3 Catch-all Rule	ENABLED Actions ▾
<p>IF</p> <ul style="list-style-type: none"> User type: Any Group: Any User Is: Any Zone: Any Device: Any Platform: Any 	<p>THEN</p> <p>Access:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Denied

371 2.1.2 Okta Verify App

372 The Okta Verify app is installed when a new user is onboarded. The user can log in to the Okta Identity
 373 Cloud for the first time. For this setup, the user will be asked to change their password and perform
 374 setup. After the password update, the user can set up Okta Verify. [Follow the instructions for Android or](#)
 375 [iOS devices to install Okta Verify and complete the process.](#)

376 2.1.3 Okta Access Gateway

377 The Okta Access Gateway is part of the Okta Identity Cloud. It can be leveraged to integrate legacy, on-
 378 prem applications into the Okta Identity Cloud. [More information on installing and configuring the Okta](#)
 379 [Access Gateway \(AG\) is available online.](#) Tasks to perform include:

- 380 1. First, [download and deploy the latest OVA image](#).
- 381 2. Once installed, start the server, log in to the Okta AG, and [configure the Okta AG](#).

- 382 3. Next, log into the Okta admin console via a web browser (i.e.: <https://zta-eig1-admin.okta.com/>). [Configure Okta as the Identity Provider for the AG](#).
- 383 4. Log into Okta AG via a web browser and [configure enterprise applications in Okta AG](#).

385 2.2 Radiant Logic RadiantOne

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

388 2.2.1 Installation

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

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

- 396
 - 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.

400 2.2.2 Configuration

401 2.2.2.1 Sync with an LDAP server

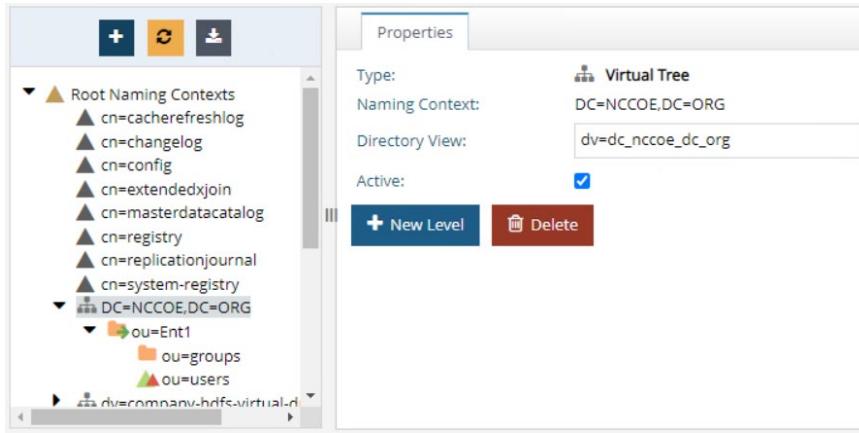
- 402 1. Once installation is complete, log in to RadiantOne from a web browser on the Radiant Logic
403 server, <https://localhost:7171>. Note: ensure the proper SSL certificate is on the server for
404 HTTPS.
- 405 2. Initial configuration is to sync up with an LDAP server. Go to **Settings > Server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

Server Backend » LDAP Data Sources » Edit LDAP Data Source

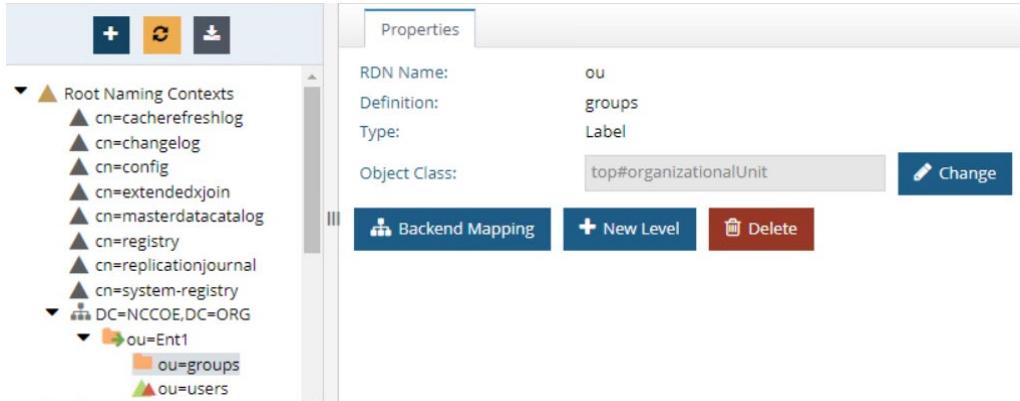
Edit LDAP Data Source

Data Source Name	ent1-ad	Data Source Type	AD2008	Status	Active
Host Name	10.131.2.11	Port	636	<input checked="" type="checkbox"/> SSL	
Bind DN	radiant@lab.nccoe.org	Bind Password		
Base DN	DC=lab,DC=nccoe,DC=org	<input type="checkbox"/> Use Kerberos profile:	vds_krb5		
	Choose	<input checked="" type="checkbox"/> Disable Referral Chasing			
	Test Connection	<input checked="" type="checkbox"/> Paged Results Control, page size: 600			

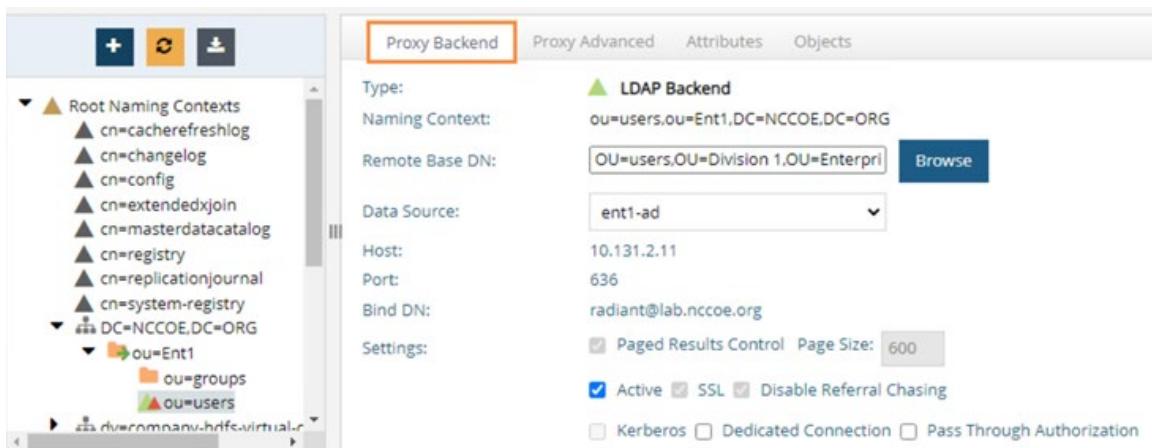
- 408 3. Once the connection is tested and successful, the integration is completed.
- 409 4. Next, create a Directory Namespace by going to **Directory Namespace** and selecting **Create New Naming Context**. Click **Next** and click **OK**.
- 410



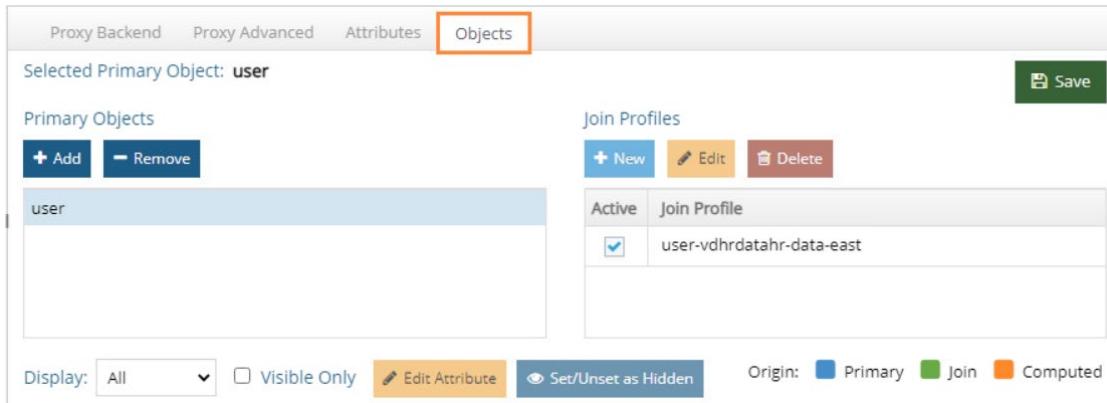
- 411 5. Find **DC=NCCOE,DC=ORG** under **Root Naming Contexts** on the left side of the screen. Click the **New Level** button. Enter **ent1** as the name for the **OU** and click **OK**.
- 412
- 413 6. Click on **ou=ent1** on the left side and click the **New Level** button on the right to create a sub-ou called **groups**.
- 414



- 415 7. Click on **ou=ent1** on the left side as shown below and click the **New Level** button on the right to
416 create a sub-ou called **users**.
- 417 8. Once configured and saved, click on **ou=users** and click on **Backend Mapping** on the right. Select
418 **LDAP Backend**. Click **Next** and **Browse** for the proper **Remote Base DN**. Then click **OK**. The
419 screenshot is the completed configuration for the sub-ou users Proxy Backend.



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

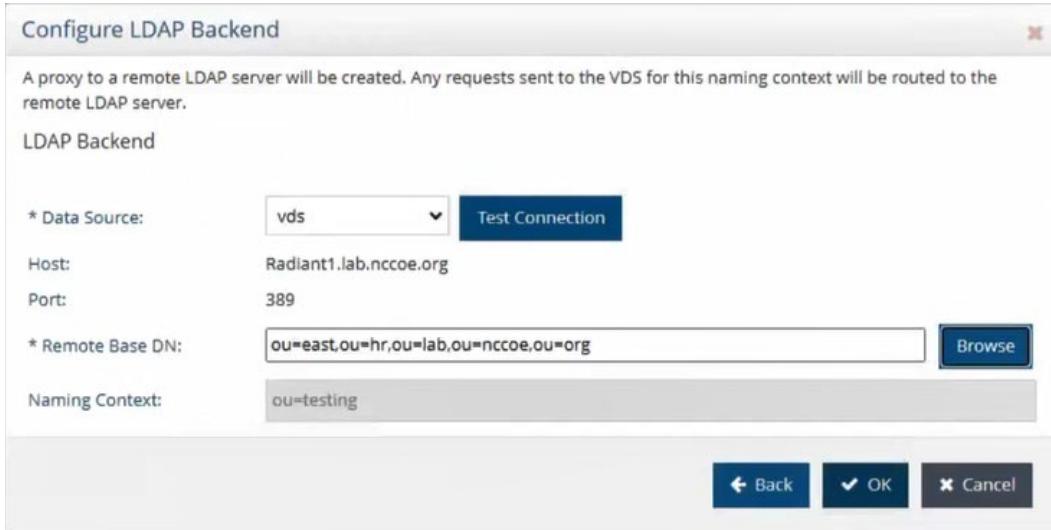


422 **2.2.2.2 Create a namespace to bring in users**

- 423 1. In **Directory Namespace**, click the + sign. Create a naming context:
 424 `ou=hr,ou=lab,ou=nccoe,ou=org` and select **Virtual Tree** for the naming context type, then click
 425 **Next**.
- 426 2. Configure the Virtual Tree by choosing **Create a new view (.dvx)**, setting the **Directory View** to
 427 `dv=ou_hr_ou_lab_ou_nccoe_ou_org` and clicking **OK**.
- 428 3. Next, create a sub-Namespace by clicking the **+ New level** button and entering the information
 429 depicted below.

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

- 434 5. Click on **ou=east** to edit properties. Scroll down to the bottom of the screen and click on the
 435 **Initialize** button. Then select a file with database users to import for initializing the HDAP store.
 436 Note: We are emulating an HR database with this file.
- 437 6. Go to the **Directory Browser** tab and refresh the data by clicking the **Refresh Tree** button.
- 438 7. Go to the OU that you just configured and expand it. The new users should now be available.
- 439 8. Go to **Directory Namespace** and click the + button to add new naming context (in our build, we
 440 used **ou=testing**). This is used to map to the LDAP backend the database information that was
 441 imported.
- 442 9. Click on the OU that was created. Click **OK** and **Save**.



- 443 10. Go to **Directory Browser** and hit the **Refresh** button.
- 444 11. Go to **Settings > Configuration > ORX Schema**, and find **OU=Testing** and check it. Click on
 445 **Generate LDAP Schema** at the bottom of the screen and click **OK**.

446 2.2.3 Integration

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

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

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

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

458 **2.3 SailPoint IdentityIQ**

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

461 **2.3.1 Installation and Configuration**

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

- 464 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
465 for release 8.2. Download the installation file from the SailPoint website and [follow the installation instructions](#).
- 466 2. Login into IdentityIQ from a web browser (<http://localhost:8080>) using the default login and
467 password. Make sure to change the default password.
- 468 3. [Configure IQService](#). This is needed in order to set up integration with AD.
- 469 4. Govern permissions by pushing both employee and contractor users and groups to AD and Okta.
470 Note: This step should be completed after the integration with AD and Okta is completed. Steps
471 to configure integration are in [Sections 2.3.3](#) and [2.3.4](#). After integration with AD and Okta is
472 completed, navigate to the **Setup** drop-down menu and select **Roles**. Here we will create birth-
473 right role and access profile for employees and contractors.
- 474 a. Select **New Role** drop-down button and select Role. The screenshot lists the four roles
475 that are created for this build.



- 478 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
 479 the users. This will push users into AD as a birthright. Once that role is configured, con-
 480 figure the corresponding contractor role the same way. Note that the **Assignment Rule**
 481 should be different for the contractor based on user information in SailPoint.
 482

Role Editor

*Indicates a required field.

Name *	Employee Birthright Role
Display Name	
Type *	Business
Owner *	The Administrator
Description	<p style="font-size: small;">B I U </p> English (United States)

Assignment Rule

IdentityIQ Items		Application Items		Additional Items	
Add Identity Attribute	– Select Application –	Add Attribute	Add Permission	Add Role Attribute	Add Entitlement Attribute
Operation	Type	Source	Name	Value	
Or	<input type="checkbox"/>	IdentityIQ	Type	Equals	employee
Group Selected		Ungroup Selected		Delete Selected	

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

487

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

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

Standard Properties	
<small>*Indicates a required field.</small>	
Name*	<input type="text" value="Ent1 HR Account Aggregation"/>
Description	<input type="text" value="Task template for application account scanning."/>
Allow Concurrency	<input type="checkbox"/>
Require Signoff	<input type="checkbox"/>
Host	<input type="text"/>
Number of Runs	3
Average Run Time	0:00:03
<input type="button" value="Reset Run Statistics"/>	
Email Task Alerts	
Email Notification	<input type="button" value="Disabled"/>
Account Aggregation Options	
Select applications to scan*	<input type="button" value=""/>
<input type="checkbox"/> Ent1-HR	

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

- 501 6. Configure lifecycle processes through Rapid Setup Configuration. Click on the **Setup** cog and se-
 502 lect **Rapid Setup** to begin. The Rapid Setup Configuration process allows onboarding of applica-
 503 tions and manage functions such as joiner, mover, and leaver of identities. Use the “Using Rapid
 504 Setup” section of the [IdentityIQ Rapid Setup Guide](#) to guide the configuration.

505 a. The following screen captures show the configuration we used for **Joiner**.

The image contains two screenshots of the IdentityIQ Rapid Setup Configuration interface, both titled "Joiner".

Screenshot 1: Joiner Processing

- Joiner Processing:** A toggle switch is turned on.
- Generate Approvals:** A toggle switch is turned off.
- Automatically Join New Empty Identities:** A toggle switch is turned off.
- Exclude Uncorrelated Identities:** A toggle switch is turned on.
- Alternative Workgroup for Joiner Completed Notification Email:** A dropdown menu is open, showing a list of options.
- Joiner Completed Notification Email Template:** A dropdown menu is open, showing a list of options. The selected option is "Joiner Completed Notification".

Screenshot 2: Identity Processing Threshold

- Identity Processing Threshold:**
 - Threshold Type:** Options are "Fixed" and "Percentage".
 - Threshold:** An input field is present.
- Joiner Business Process:** A dropdown menu is open, showing a list of options. The selected option is "RapidSetup - Joiner".
- Trigger Filter:**
 - Logic:** Options are "AND" and "OR".
 - Filter Rows:** Two rows are defined:

Type	String	Equals	employee	<input type="checkbox"/>
Type	String	Equals	contractor	<input type="checkbox"/>
 - Buttons:** "+ Add Row", "+ Add Group".

506

b. The following screen captures show the configuration we used for **Mover**.

The image displays two screenshots of a software interface for configuring the Mover process. Both screenshots have a header with tabs: Joiner, Mover (which is selected), Leaver, Identity Operations, and Miscellaneous.

Top Screenshot (Mover Processing):

- Mover Processing: Enabled (switch is blue)
- Generate Approvals: Disabled (switch is grey)
- Exclude Uncorrelated Identities: Enabled (switch is blue)
- Launch a Targeted Certification: Enabled (switch is blue)
- Stage the Certification: Disabled (switch is grey)
- Include Birthright Roles: Disabled (switch is grey)

Bottom Screenshot (Mover Configuration):

- Certification Owner: The Administrator
- Backup Certifier: The Administrator
- Include Previous Manager as a Certifier: Enabled (switch is blue)
- Joiner Processing: Enabled (switch is blue)
- Post Mover Rule: Select Rule ... (dropdown menu)
- Identity Processing Threshold:
 - Threshold Type: Fixed (radio button selected)
 - Percentage: Percentage (radio button)
 - Threshold: [Input field]

The screenshot shows the 'Mover' tab selected in a top navigation bar. Below the tabs are two radio button options: 'Fixed' and 'Percentage'. A 'Threshold' input field is present. A 'Mover Business Process' dropdown menu is set to 'RapidSetup - Mover'. Under 'Trigger Filter', there is an 'AND' logic operator and a row editor for 'Job Title' (String) and 'Changed' (String). Buttons for '+ Add Row' and '+ Add Group' are available. At the bottom right are 'Return to Global Settings' and 'Save' buttons.

507

- c. The following screen captures show the configuration we used for **Leaver**.

The screenshot shows the 'Leaver' tab selected in a top navigation bar. It includes several toggle switches: 'Leaver Processing' (on), 'Generate Approvals' (off), 'Exclude Uncorrelated Identities' (on), 'Remove Assigned Roles' (on), and 'Reassign Artifacts' (on). A note at the bottom states: 'Reassignment controls are prioritized as follows, the first to return a result is used: Assign to manager, Assign by rule, Assign to alternative.'.

PRELIMINARY DRAFT

Joiner	Mover	Leaver	Identity Operations	Miscellaneous
Reassign Artifact Types *				
<input type="checkbox"/> Application				
<input type="checkbox"/> Certification Schedule				
<input type="checkbox"/> Entitlement				
<input type="checkbox"/> Group/Population				
<input type="checkbox"/> Policy				
Show 4 More...				
Reassign Artifacts To Manager				
<input checked="" type="checkbox"/>				
Reassign Artifacts Rule				
<input type="button" value="Select Rule ..."/>				
Reassign Artifacts Alternate * ?				
<input type="button" value="The Administrator"/>				
Reassignment controls are prioritized as follows, the first to return a result is used: Assign to manager, Assign by rule, Assign to alternative.				
Reassign Identities ?				
<input checked="" type="checkbox"/>				
Reassign Identities To Manager ?				
<input checked="" type="checkbox"/>				
Reassign Identities Rule ?				
<input type="button" value="Select Rule ..."/>				
Reassign Identities Alternate * ?				
<input type="button" value="The Administrator"/>				
Send Leaver Notification to this Workgroup ?				
<input type="button"/>				
Ownership Reassignment Notification Email Template *				
<input type="button" value="Leaver Ownership Reassignment Notification"/>				
Leaver Completed Notification Email Template *				
<input type="button" value="Leaver Completed Notification"/>				

Joiner Mover **Leaver** Identity Operations Miscellaneous

Identity Processing Threshold

Threshold Type ?
 Fixed
 Percentage

Threshold ?

Leaver Business Process *

Trigger Filter * ?

AND **OR**

<input type="text" value="Inactive"/>	<input type="text" value="Equals"/>	<input type="text" value="True"/>
<input type="text" value="Inactive"/>	<input type="text" value="Changed"/>	
+ Add Row	+ Add Group	

Return to Global Settings **Save**

© Copyright 2021 BellPoint Technologies - All rights reserved.

508

- d. The following screen captures show the configuration we used for **Identity Operations**.

Joiner Mover Leaver **Identity Operations** Miscellaneous

Terminate Processing

Generate Approvals

Remove Assigned Roles

Reassignment controls are prioritized as follows, the first to return a result is used: Assign to manager, Assign by rule, Assign to alternative.

Reassign Artifacts

The image displays two screenshots of the Identity Operations configuration interface, specifically for the Leaver tab.

Screenshot 1: Reassign Artifact Types

- Reassign Artifact Types ***: A list of artifact types:
 - Application
 - Certification Schedule
 - Entitlement
 - Group/Population
 - Policy
- Show 4 More...**: A link to view additional artifact types.
- Reassign Artifacts To Manager**: A toggle switch that is currently turned on (blue).

Screenshot 2: Send Terminate Complete Notification

- Send Terminate Complete Notification to this Workgroup**: A dropdown menu.
- Ownership Reassignment Notification Email Template ***: A dropdown menu set to "Terminate Ownership Reassignment Notification".
- Terminate Completed Notification Email Template ***: A dropdown menu set to "Terminate Completed Notification".
- Post Terminate Rule**: A dropdown menu set to "Select Rule ...".
- Terminate Business Process ***: A dropdown menu set to "RapidSetup - Leaver".

At the bottom right of the interface are two buttons: "Return to Global Settings" and a blue "Save" button.

- 509 e. Configure Rapid Setup specific to AD users: Aggregation, Joiner, Mover, and Leaver
 510 based on the following screenshots. Note: The Joiner setup used the default configura-
 511 tion, so it is not included in the screenshots.

Rapid Setup: Ent1-AD-Ent-Users

Aggregation

- Joiner
- Mover
- Leaver

Account Correlation

Changes made here will be reflected for all applications which share this configuration.

employeeNumber Equals Employee ID

+ Add Filter

Mover

Include Additional Entitlements in a Certification for This Application

Include Targeted Permissions in a Certification for This Application

Perform Account-Only Provisioning

Leaver Options

Set the actions and timing of account operations during leaver operations.

Delete Account

Now Later

Days to Delay Deleting Accounts * 30

Leaver

Disable Account

Now Later

Scramble Password

Remove Entitlements

Add Comment

Now Later

Comment Attribute * description

Comment * Disabled by IdentityIQ as p

Cancel Previous Save Next

- 512 7. Govern user permissions to applications on an individual basis. Configure procedures to provision
 513 and approve user access to resources. For Enterprise 1, the process is for an administrator
 514 or user to request approval to access an application. That request goes to the user's manager

515 for review and approval. Once the manager approves the request, SailPoint kicks off an API call
 516 to Okta to configure access for that user.

517 2.3.2 Integration with Radiant Logic

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

The screenshot shows the 'LDAP Configuration' page. It has several input fields:
 - 'Use TLS': A checkbox that is not checked.
 - 'Authorization Type': A dropdown menu set to 'Simple'.
 - 'User': A text input field containing 'uid=ailpointadmin,ou=globalusers,cn=config'.
 - 'Password': A text input field with redacted content.
 - 'Host': A text input field containing 'radian1.lab.nccoe.org'.
 - 'Port': A text input field containing '389'.
 - 'Page Size': A text input field containing '100'.
 - 'Authentication Search Attributes': A text input field containing 'cn', 'uid', and 'mail'.

- 524 4. Scroll down the screen and under the **Account** tab, add the Search DN, which is the one created
 525 from Radiant Logic.
- 526 5. Click on **Test Connection** to make sure that SailPoint is able to connect to Radiant Logic. Click
 527 **Save**.
- 528 6. You can go back into the **Configuration** tab and **Schema** sub-tab. Toward the bottom of the
 529 screen, there is a **Preview** button. You can click on that to preview attributes imported. Note:
 530 We manually added schema attributes. This can be completed from Radiant Logic and imported.
 531 Please ensure that you have the correct attributes to integrate this.
- 532 7. To complete the setup, click **Save** to finish and import users from Radiant Logic.
- 533 8. Go to the **Setup** tab and click **Tasks**. Once in the new tab, click on the **New Task** button at the
 534 top right corner to create the account aggregation for Radiant Logic.

- 535 9. Perform identity attribute mapping. The screen capture shows mappings specific to this build
 536 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

- 537 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”).
- 538 2. Navigate to the **Configuration** tab. From here, input information for the IQ Service Host. The IP
 539 address is this server, the IdentityIQ server. IQ Service User is a user that was created in AD for
 540 this integration.
- 541 2. Navigate to the **Configuration** tab. From here, input information for the IQ Service Host. The IP
 542 address is this server, the IdentityIQ server. IQ Service User is a user that was created in AD for
 543 this integration.

Edit Application Ent1-AD-Ent-Users

Details	Configuration	Correlation	Accounts	Risk	Activity	Data Sources	Unstructured Targets	Rules	Password Policy																																																				
	Settings	Schema	Provisioning Policies																																																										
Active Directory - Direct Configuration <table border="1"> <tr> <td colspan="2">IQService Configuration</td> </tr> <tr> <td>IQService Host</td> <td>IQService Port</td> <td>IQService User</td> <td>IQService Password</td> <td>Use TLS</td> </tr> <tr> <td>10.151.1.20</td> <td>5050</td> <td>LABialien</td> <td>*****</td> <td><input type="checkbox"/></td> </tr> </table> <table border="1"> <tr> <td colspan="10">Forest Configuration</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Forest Name</td> <td>Global Catalog Server</td> <td>User</td> <td>Password</td> <td>Authentication and Security</td> <td>Use TLS</td> <td>Resource Forest</td> <td>Manage All Domains</td> <td>Discover Domains</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Enterprise Users</td> <td></td> <td></td> <td></td> <td>Simple</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/> Discover</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td>Simple</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/> Discover</td> </tr> </table>										IQService Configuration		IQService Host	IQService Port	IQService User	IQService Password	Use TLS	10.151.1.20	5050	LABialien	*****	<input type="checkbox"/>	Forest Configuration										<input type="checkbox"/>	Forest Name	Global Catalog Server	User	Password	Authentication and Security	Use TLS	Resource Forest	Manage All Domains	Discover Domains	<input type="checkbox"/>	Enterprise Users				Simple	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Discover						Simple	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Discover
IQService Configuration																																																													
IQService Host	IQService Port	IQService User	IQService Password	Use TLS																																																									
10.151.1.20	5050	LABialien	*****	<input type="checkbox"/>																																																									
Forest Configuration																																																													
<input type="checkbox"/>	Forest Name	Global Catalog Server	User	Password	Authentication and Security	Use TLS	Resource Forest	Manage All Domains	Discover Domains																																																				
<input type="checkbox"/>	Enterprise Users				Simple	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Discover																																																				
					Simple	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Discover																																																				

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

Domain Configuration*

<input type="checkbox"/> Forest Name	Domain DN	NetBIOS Name	User	Password	Servers	Authentication and Security	Use TLS
<input type="checkbox"/> Enterprise Users	dc=lab,dc=ncoco,dc=org	LAB1	allen	*****	10.131.2.11	Simple	<input type="checkbox"/>
						Simple	<input type="checkbox"/>
						Simple	<input type="checkbox"/>

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

Account Group

Allow Auto Partitioning

User Search Scope*

<input type="checkbox"/> Search DN	Iterate Search Filter	Group Membership Search DN	Group Member Filter String
<input type="checkbox"/> ou=Division 1,ou=enterprise users,dc=lab,dc=org			

- 548 5. Navigate to the **Schema** and **Provisioning Policies** sub-tabs, and update information as necessary.
 549
 550 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

- 552 7. Click **Save** to complete the configuration.
 553 8. Go to **Setup** tab and click **Tasks**. Once in the new tab, click on the **New Task** button at the top
 554 right corner to create the account aggregation for AD.

2.3.4 Integration with Okta

- 556 1. Go into the **Applications** tab and select **Application Definition**. When the screen comes up, click
 557 on the **Add New Application** button.
 558 2. Fill out the **Name** (e.g., “Ent1-Okta”) and **Owner** (“The Administrator”), select **Okta** as the **Appli-**
 559 **cation Type**, and enable the **Authoritative Application** option.

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

Okta Connection Settings

URL *	<input type="text" value="https://zta-eig1.okta.com"/>
Authentication Type	<input type="button" value="API Token"/>
API Token *	<input type="text" value="*****"/>
Page Size	<input type="text" value="200"/>

Aggregation Filter Settings

Filter Condition for Accounts	<input type="text"/>
Filter Condition for Groups	<input \"okta_group\""="" built_in\"="" eq="" or="" type="" value="type eq \"/>
Filter Condition for Applications	<input type="text"/>

Test Connection

562

2.4 Ivanti Neurons for UEM

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

566

2.4.1 Installation and Configuration

567

2.4.1.1 Install an MDM certificate for Apple devices

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

571 To acquire and install the MDM certificate:

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

577 *2.4.1.2 Configure Android Enterprise*

578 Android Enterprise allows personal and corporate applications on the same Android device. Android
579 Enterprise configuration depends on the type of Google subscription. Please follow Ivanti
580 documentation to [set up the integration](#).

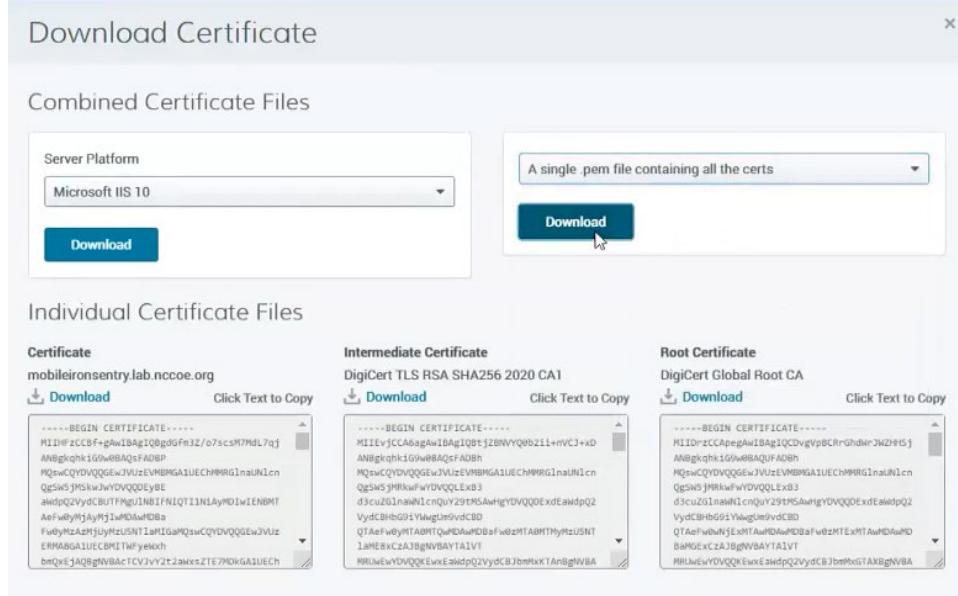
581 The Android Enterprise Work Profile configuration defines which features and apps are allowed, and
582 which are restricted on Android enterprise devices. Do the following to configure the profile:

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

588 *2.4.1.3 Add a Certificate Authority*

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

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



598 *2.4.1.4 Configure user settings*

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

601 *2.4.1.5 Add a policy*

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

- 604 1. Go to **Policies** and click **+Add** (upper right).
 - 605 2. Select a policy type and complete the settings. Policy types include Compromised Devices, Data
606 Protection/Encryption Disabled, MDM/Device Administration Disabled, Out of Contact, and Al-
607 lowed Apps.
 - 608 3. Select the device groups that will receive this policy.
- 609 The following screenshots show an example of a Data Protection policy to be distributed to a custom
610 group of devices.

PRELIMINARY DRAFT

The screenshot shows two consecutive configuration screens from the Ivanti Neurons for UEM software.

Step 1: Policies / Details

This screen is titled "Data Protection/Encryption Disabled". It includes a sub-section "Policies and Compliance Setup" with fields for "Name" (set to "Data Protection/Encryption Disabled") and "Description" (set to "Checks for devices which do not have a passcode or encryption enabled"). Below this is a "Compliance Action" section containing several options:

- 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.

A "Next →" button is visible at the bottom right.

Step 2: Policies / Details

This screen continues the configuration. It shows the "Data Protection/Encryption Disabled" policy again. The "Distribute" step is selected, indicated by a green checkmark icon. The "Choose one of these options" section offers three choices:

- All Devices
- No Devices
- Custom

Under the "Custom" option, there is a note: "Distribute the Policy to specific Devices/Device Groups or Users/User Groups".

The "Choose one of these Custom Distribution Option" section allows specifying distribution to either "Users/User Groups" or "Devices/Device Groups". The "Devices/Device Groups" option is selected.

The "Select below to distribute this Policy" section contains a search bar "Search Devices by User Name" and a table showing "All Available (6)" and "Selected (0)".

The "Distribution Summary" section indicates the configuration will be sent to "Individual Devices" (0) and "Device Groups" (1).

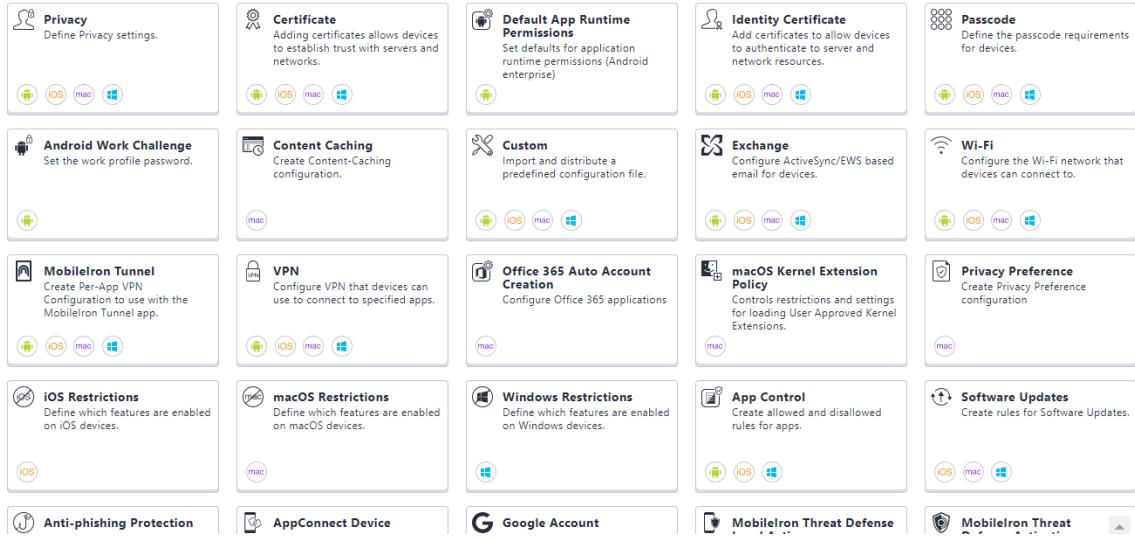
A "Done" button is located at the bottom right of this screen.

611 2.4.1.6 Add a configuration for managed devices

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

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

PRELIMINARY DRAFT



618 3. Click **Next**.

619 4. Select a distribution level for the configuration.

620 Here is an example of a Privacy configuration:

Name
Privacy policy |

+ Add Description

Configuration Setup

Collect Location Data (iOS)
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) (i)

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

621 This is an example of an iOS AppConnect configuration:

PRELIMINARY DRAFT

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

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

Overview	Configurations	Installed Apps	Available Apps	Policies	Certificates	Sentry	Attributes	Logs	Updates	Bios	Hardware
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 (10) Excluded Configurations (0)											
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.											
Push Profiles Exclude Profiles											
NAME	TYPE	STATUS	DISTRIBUTION METHOD	ACTIONS							
<input type="checkbox"/> ZSO Identity Certificate	Identity Certificate (Dynamically Generated)	Error	Assignment	Push Exclude							
<input type="checkbox"/> ZSO Certificate (Tunnel)	Certificate	Installed	Assignment	Push Exclude							
<input type="checkbox"/> Sentry DigiCert Certificates	Identity Certificate (Dynamically Generated)	Pending Install	Assignment	Push Exclude							
<input type="checkbox"/> Identity issued by MobileIron Agent CA	Identity Certificate (Dynamically Generated)	Installed	Assignment	Push Exclude							
<input type="checkbox"/> Windows Apps@Work Identity issued by MobileIron Agent CA	Identity Certificate (Dynamically Generated)	Installed	Assignment	Push Exclude							
<input type="checkbox"/> Passcode Requirements	Passcode	Installed	Assignment	Push Exclude							
<input type="checkbox"/> DigiCert Global Root CA	Certificate	Installed	Assignment	Push Exclude							
<input type="checkbox"/> Privacy	Privacy	Active ?	Assignment	Push Exclude							
<input type="checkbox"/> MobileIron Agent CA Certificate	Certificate	Installed	Assignment	Push Exclude							
<input type="checkbox"/> DigiCert TLS RSA SHA256 2020 CA1	Certificate	Installed	Assignment	Push Exclude							

623 [2.4.2 Integration with Ivanti Connector](#)

624 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](#).

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

632 **2.4.3 Integration with Okta**

633 **2.4.3.1 IdP setup**

- 634 1. Go to **Admin > Infrastructure > Identity > Add IdP**.
- 635 2. Generate a key for uploading to Okta IdP.
- 636 3. Log in to Okta IdP. Search IdP for the **MobileIron Cloud App** and add it to the IdP account.
- 637 4. Configure the **MobileIron Cloud App** on the IdP by pasting the above-generated key and the
638 host information.
- 639 5. Export metadata from Okta to the Ivanti Neurons for UEM console.
- 640 6. In **Admin > Infrastructure > Identity > Add IdP**, select **Choose File** to import the downloaded
641 metadata file to Ivanti Neurons for UEM and complete the setup.
- 642 7. When an IdP is added, user authentication automatically switches from LDAP to IdP.

643 **2.4.3.2 Okta Verify app configuration preparation**

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

649 **2.4.3.3 Okta Verify app configuration - Android**

- 650 1. In the Ivanti Neurons for UEM console, navigate to **Apps > App Catalog**. Click **Add**.
- 651 2. Select the Google Play Store and search for **Okta Verify**. Select the official **Okta Verify** app.
- 652 3. Continue through the wizard until you reach the App Configurations page. Click the + button in
653 the Managed Configurations for Android section.

- 654 4. Add desired settings. Under **Managed Configurations**, add the **Org URL** and **Management Hint**
655 from the Okta Admin console. The Management hint will be the **Secret Key** you saved from the
656 Okta console during preparation.
- 657 5. Click **Next**, then click **Done**.

658 **2.4.3.4 Okta Verify app configuration - iOS**

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

669 **2.5 Ivanti Sentry**

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

673 **2.5.1 Installation and Configuration**

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

677 Next, create a profile for Standalone Sentry in the Ivanti Neurons for UEM console. For information on
678 how to create a profile for Standalone Sentry and configure Standalone Sentry for ActiveSync and
679 AppTunnel, see the [*Sentry Guide for Cloud*](#).

680 **2.5.2 Ivanti Tunnel Configuration and Deployment**

681 Ivanti Tunnel is an application that connects a mobile device to the Ivanti Sentry. The process to deploy
682 this app is similar to the deployment of the Okta Verify app in [*Section 2.1.2*](#).

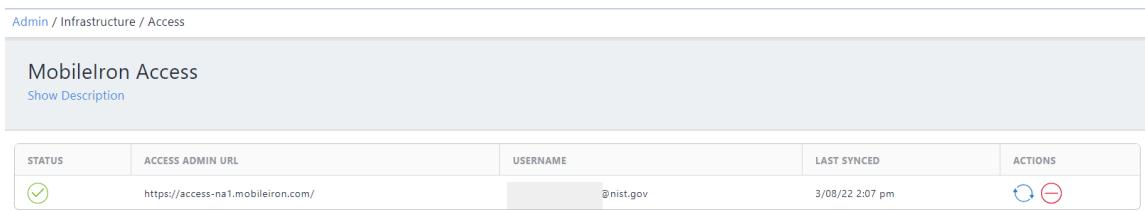
- 683 1. On the **App Configurations** page for the Tunnel app, create a Managed Configuration.
- 684 2. Set the **Tunnel Profile Mode** to **MobileIron Sentry + Access**.
- 685 3. Set the **Sentry Server** to the Sentry instance you created previously.
- 686 4. Set the **SentryService** to the name of the IP Tunnel defined on the Sentry.
- 687 5. Set the **ClientCertAlias** to the Sentry certificates you defined during Sentry configuration.
- 688 6. Set any other options as needed.
- 689 7. Save the Managed Configuration and deploy to devices as needed.

690 **2.6 Ivanti Access ZSO**

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

694 **2.6.1 Integration with Ivanti Neurons for UEM**

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



The screenshot shows the 'Access' section of the Ivanti Neurons for UEM interface. At the top, there's a header bar with 'Admin / Infrastructure / Access'. Below it, a title 'MobileIron Access' with a 'Show Description' link. A table follows, with columns: STATUS, ACCESS ADMIN URL, USERNAME, LAST SYNCED, and ACTIONS. The first row contains: a green checkmark icon, 'https://access-na1.mobileiron.com/', '@nist.gov', '3/08/22 2:07 pm', and two small circular icons (blue with white arrow, red with white minus sign).

STATUS	ACCESS ADMIN URL	USERNAME	LAST SYNCED	ACTIONS
✓	https://access-na1.mobileiron.com/	@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, and 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**.

732 *2.7.1.2 Assign roles to the API user*

- 733 1. From the admin console, go to **Users**.
- 734 2. Select the new API user created previously.
- 735 3. Click **Actions**.
- 736 4. From the User details page, select **Assign Roles**.
- 737 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**.

740 *2.7.1.3 Add an MDM server to the Zimperium console*

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

747 *2.7.1.4 Activate MTD on Ivanti Neurons for UEM*

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

758 11. Click **Done**.

759 *2.7.1.5 Add custom attributes in Ivanti Neurons for UEM*

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

761 1. To create custom attributes, in the Ivanti Neurons for UEM admin console go to **Admin > System**
762 > **Attributes**. Enter each attribute name in lower case.

763 2. Create the custom attribute **mtdnotify** for **Low or Normal** severity threats:

764 a. Click **Add New**. The **Attribute Name** and **Attribute Type** fields are displayed.

765 b. Select **Device** as the attribute type.

766 c. Name the custom attribute **mtdnotify**.

767 d. Click **Save** to monitor and notify.

768 3. Create the custom attribute **mtdblock** for **Elevated** or **Critical** severity threats:

769 a. Click **Add New**.

770 b. Select **Device** as the attribute type.

771 c. Name the custom attribute **mtdblock**.

772 d. Click **Save** to monitor and notify.

773 4. Create the custom attribute **mtdquarantine** for **Elevated** or **Critical** severity threats:

774 a. Click **Add New**.

775 b. Select **Device** as the attribute type.

776 c. Name the custom attribute **mtdquarantine**.

777 d. Click **Save** to monitor, notify, and quarantine.

778 5. Create the custom attribute **mtdtiered4hours** for **Low**, **Normal**, **Elevated**, or **Critical** severity
779 threats:

780 a. Click **Add New**.

781 b. Select **Device** as the attribute type.

782 c. Name the custom attribute **mtdtiered4hours**.

783 d. Click **Save** to monitor and notify, wait for four hours, block, wait for another four hours,
784 and quarantine.

785 *[2.7.1.6 Create Compliance Policy](#)*

- 786 Create compliance actions using custom policies based on the MTD custom attributes created above.
- 787 1. In Ivanti Neurons for UEM admin console, go to **Policies**.
 - 788 2. Click **+ Add**.
 - 789 3. Select **Custom Policy**.
 - 790 4. Enter **mtdnotify** as the policy name.
 - 791 5. Under **Conditions**, select **Custom Device Attribute**.
 - 792 6. Select **mtdnotify** from the drop-down box and set the condition **is equal to 1**.
 - 793 7. Under **Choose Actions**, select **Monitor** and **Send Email and Push Notification**.
 - 794 8. Under **Email Message** fields, enter the subject and body text.
 - 795 9. Under **Push Notification**, enter message text.
 - 796 10. Click **Yes, Next, and Done**.
 - 797 11. Repeat this procedure to add the following policies: **mtdblock**, **mtdquarantine**, **mtdtiered4hours**.
 - 799 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

800 ***2.7.1.7 Create device groups and match with custom policies and custom device attributes created above***

- 801
- 802 1. In Ivanti Neurons for UEM admin console, go to **Devices > Device Groups**.
 - 803 2. Click **+ Add**.
 - 804 3. Enter **mtdNotify** as the device group name.
 - 805 4. Under Dynamically Managed groups, select **Custom Device Attribute**.
 - 806 5. Select **mtdnotify** from the drop-down box and set the condition **is equal to 1**.
 - 807 6. Click **Save**.
 - 808 7. Repeat this procedure to add the following groups: **mtdBlock**, **mtdQuarantine**, **mtdTiered4hours**.

810 ***2.7.1.8 Configure Zimperium MTD management console***

811 [Set up, configure, and use the MTD console for supported MTD activities](#). When configuring policies in
812 the Zimperium admin console, use the available MDM actions and Mitigation actions.

The screenshot shows a table interface for managing threats. The columns include: Enable, Type, Severity, Threat, Set User Alert, Device Action, MDM Action, Mitigation Action, and Notify Me. A dropdown menu for 'MDM Action' is open over the third row, showing options like 'Select an Opt...', 'No Action', 'Remove', 'Lock Device', 'MTD-Notify', 'MTD-Block', 'MTD-Quarantine', and 'MTD-Tiered4hours'. The 'No Action' option is currently selected. The 'Mitigation Action' column also has a dropdown menu with similar options, many of which are labeled 'Unavailable'.

Enable	Type	Severity	Threat	Set User Alert	Device Action	MDM Action	Mitigation Action	Notify Me
<input checked="" type="checkbox"/>	Singular	Elevated	Abnormal Process Activity	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Singular	Elevated	Always-on VPN App Set	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Singular	Elevated	Android Debug Bridge (ADB) Apps Not Verified	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Singular	Low	Android Device - Compatibility Not Tested By Google	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>
<input type="checkbox"/>	Singular	Critical	Android Device - Possible Tampering	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Singular	Elevated	App Debug Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Singular	Low	App Pending Activation	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>
<input type="checkbox"/>	Singular	Critical	App Tampering	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Singular	Medium	ARP Scan	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Singular	Elevated	BlueBorne Vulnerability	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Singular	Medium	Captive Portal	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select an Opt...	<input type="checkbox"/>

813 ***2.8 IBM Cloud Pak for Security***

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

816 1. [Deploy an OpenShift cluster](#). OpenShift needs to be in place before Cloud Pak for Security can be
817 installed.

818 2. [Install Cloud Pak for Security](#).

819 3. [Configure LDAP authentication](#) so Cloud Pak for Security can leverage an existing LDAP directory
820 server for authentication.

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

823 2.9 IBM Security QRadar XDR

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

827 Install and configure QRadar following IBM's [QRadar Installation and Configuration Guide](#).

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

830 2.10 Tenable.io

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

833 2.10.1 Installation and Configuration

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

837 2.10.1.1 Deploy an agent

838 1. In Tenable.io, click the hamburger menu (☰) in the top left corner and navigate to **Settings >**
839 **Sensors > Nessus Agents**.

840 2. Click **Add Nessus Agent** and save the Linking Key.

841 3. On the target endpoint, download the agent from <https://downloads.tenable.com>. When the
842 download completes, run the executable file.

843 4. In the setup window, fill in the key from step 2, the server (in our case, cloud.tenable.com:443),
844 and the agent groups that this agent will be part of (in our case, Default). Click **Next**.

- 845 5. Click **Install** and approve the request if User Account Control (UAC) comes up.
- 846 6. When installation completes, updates will continue running in the background. The update and
847 connection process may take some time. The endpoint will then be shown in the cloud tenant.

Linked Agents								
	NAME	STATUS	IP ADDRESS	PLATFORM (D...)	VERSION	GROUPS	NETWORK	LAST PLUGIN U...
<input type="checkbox"/>	IDENTITYIQ	Online	10.176.21.20	Windows (win...)	10.1.3	Default	Default	N/A
<input type="checkbox"/>	MAIL	Online	10.176.23.93	Windows (win...)	10.1.3	Default	Default	N/A
<input type="checkbox"/>	RADIANT2	Online	10.176.21.32	Windows (win...)	10.1.3	Default	Default	N/A
<input type="checkbox"/>	RADIUS	Online	10.176.22.20	Windows (win...)	10.1.3	Default	Default	N/A

2.10.1.2 Deploy a scanner

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

2.10.2 Integration with QRadar

- 864 For Tenable.io and QRadar integration, follow the [Tenable and IBM QRadar SIEM Integration Guide](#).

865 2.11 Tenable.ad

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

869 For Tenable.ad installation and configuration, follow the [Tenable.ad On-Premise Installation Guide](#).

870 For Tenable.ad and QRadar integration, follow the [Tenable and IBM QRadar SIEM Integration Guide](#).

871 2.12 Mandiant Security Validation (MSV)

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

876 2.12.1 MSV Director Installation/Configuration

- 877 1. Download the MSV Director software from the Mandiant web portal and deploy it in a virtual
878 environment.
- 879 2. Log into the MSV command line interface using credentials provided by Mandiant.
- 880 3. Run the command `sudo vsetnet` to apply network configuration.
- 881 4. Run the command `sudo vsetdb --password new_password` to set a new password for the Di-
882 rector database.
- 883 5. Use a web browser to access the MSV Director web interface at <https://Director IP/>.
- 884 6. Sign into the web interface using credentials provided by Mandiant.
- 885 7. Accept the End User Licensing Agreement and apply the license provide by Mandiant.
- 886 8. Configure the DNS settings by navigating to **Settings > Director Settings > DNS Servers**.
- 887 9. Configure the NTP settings by navigating to **Settings > Director Settings > NTP Servers**.
- 888 10. Add Security Zones corresponding with the enterprise's network segments by navigating to
889 **Environment > Security Zones**.
- 890 11. Download security content from the Mandiant web portal.
- 891 12. Navigate to **Settings > Director Settings > Content**.
- 892 13. Select **Import**, browse to the downloaded security content, and select the content files.

- 893 14. Click **Upload Import** and upload the files into the MSV Director web interface.
- 894 15. Once the upload is complete, click **Apply Import** to import the content files into MSV.

895 2.12.2 MSV Network Actor Installation/Configuration

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

905 2.12.3 MSV Endpoint Actor Installation/Configuration

- 906 1. Deploy an endpoint machine running Windows, macOS, or Linux.
- 907 2. In the MSV Director web interface, navigate to **Library > Actor Installer Files** and download the
908 relevant installer onto the endpoint.
- 909 3. Navigate to **Environment > Actors**, click **Add Endpoint Actors**, and fill out the new Actor form.
- 910 4. Execute the Actor installer on the endpoint and proceed through the install process.
- 911 5. At the end of the install process, identify the actor you just created in the **Pending Actors** table
912 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	

- 913 6. The endpoint will register itself with the MSV director and setup will be complete.

914 **2.12.4 MSV Evaluation Configuration**

- 915 1. Once the MSV Director and Actors have been configured, evaluations can be created to test se-
 916 curity controls and policies. In the MSV Director web interface, navigate to **Library > Actions**.
- 917 2. Find the action(s) you would like to use for the evaluation and select the **+Queue** button to add
 918 the action to the Queue. Repeat this process until you have added all needed actions to the
 919 Queue.

The screenshot shows the 'View Action' dialog box. At the top, there are several buttons: a play icon, '+ Monitor', '+ Queue' (which is highlighted in blue), a refresh icon, and an eye icon. To the right is the MANDIANT logo. Below the buttons, the action details are listed:

- 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:** A table showing the action's relationship to ATT&CK tactics:

Name	ID	Actions
Remote Desktop Protocol	T1021.001	Ø
- Run As Tags:** None
- Source/Destination Tags:** None

At the bottom right of the dialog is a 'Close' button.

- 920 3. After actions have been added to the Queue, click the **Queue** button in the upper right side of
 921 the web interface.
- 922 4. Select each of the actions in the **Unassigned** section and drag them to the **Current Actions**
 923 section.
- 924 5. Scroll up to the top of the page and click the **Save** button.
- 925 6. Under the **Test Type** dropdown, choose **Evaluation**.

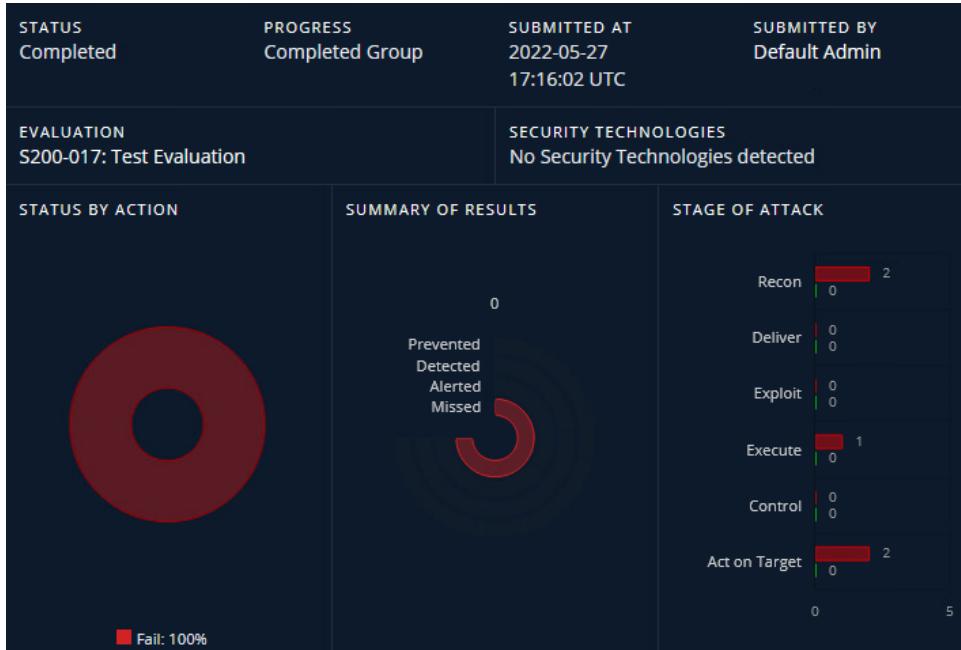
- 926 7. Under the **Name** section, enter a name.
- 927 8. Under the **Description** section, enter a description.
- 928 9. Select the **Save** button to save the evaluation.
- 929 10. Your new evaluation can be found by navigating to **Library > Evaluations** and filtering on **User
Created**.
- 930

931 2.12.5 MSV Evaluation Execution

- 932 1. Navigate to **Library > Evaluations** and select the evaluation you'd like to run. Click the **Run**
933 button.
- 934 2. From the Evaluation screen, press the **Run Evaluation** button.



- 935 3. Select the **Source Actor** and **Destination Actor** from the dropdown menus. Click **Run Now**.
- 936 4. The evaluation will run, providing results once the actions have been attempted/completed.



937 **2.13 DigiCert CertCentral**

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

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

942 **2.14 AWS IaaS**

943 This section will be part of the EIG run phase and will be included in the next version of the practice
 944 guide.

945 **3 Enterprise 3 Build 1 (EIG E3B1) Product Guides**

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

949 **3.1 Microsoft Azure Active Directory (AD)**

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

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

975 3.2 Microsoft Endpoint Manager

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

978 3.2.1 Configuration and Integration

979 3.2.1.1 Add and verify a custom domain

980 To connect an organization's domain name with Intune, a DNS registration needs to be configured. This
981 gives users a familiar domain when connecting to Intune and using resources.

- 982 1. Go to the Microsoft 365 Admin Center (admin.microsoft.com) and sign into your administrator
983 account.

- 984 2. Choose **Setup > Domains**.
- 985 3. Choose **Add domain** and type a custom domain name. Select **Next**.
- 986 4. The **Verify domain** dialog box opens, giving the values to create the TXT record with the DNS
- 987 hosting provider.

988 *[3.2.1.2 Add users](#)*

989 Once you sign into Microsoft Intune, you can add users directly or synchronize users from an on-

990 premises AD. Once added, users can enroll devices and access company resources.

Home > Users >

New user ...

ent3nccoe

Got feedback?

Create user

Create a new user in your organization. This user will have a user name like alice@ent3.nccoe.org.
[I want to create users in bulk](#)

Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

Identity

User name * Example: chris @

991 *[3.2.1.3 Enroll devices in Microsoft Intune](#)*

992 Enrolling devices allows them to receive configuration profiles and compliance policies. Configuration

993 profiles configure features and settings on devices. Compliance policies help devices meet an

994 organization's rules.

- 995 1. [Get an Apple MDM push certificate and add it to Endpoint Manager](#). This certificate is required
- 996 to enroll iOS/iPadOS devices. Then enroll iOS devices in Microsoft Intune.
- 997 2. [Create an iOS enrollment profile](#). An enrollment profile defines the settings applied to a group of
- 998 devices during enrollment.

- 999 3. [Enroll Android devices in Microsoft Intune](#). To enable Android Enterprise, an administrative
1000 Google account needs to be connected to the Intune tenant.
- 1001 4. [Create an iOS compliance policy in Microsoft Intune](#). It will be evaluated before access is allowed
1002 from iOS devices.
- 1003 5. [Create an Android compliance policy in Microsoft Intune](#). It will be evaluated before access is
1004 allowed from Android devices.
- 1005 6. [Create an iOS/macOS configuration profile](#) for iOS or Mac devices.

The screenshot shows the Microsoft Intune interface. On the left, there's a navigation sidebar with links like Home, Devices, Search (Ctrl+), Create profile, and Collection. Under Devices, there are sections for macOS, Android, Device enrollment (with Enroll devices), Provisioning (Windows 365), Policy (Compliance policies, Conditional access, Configuration profiles, Scripts, Group Policy analytics (preview)), and Configuration profiles. The Configuration profiles link is highlighted. On the right, a 'Create a profile' dialog box is open. It has fields for Platform (set to iOS/iPadOS) and Profile type (set to Device restrictions). A list of profile names includes AEWorkProfileRestrictions, Defender IOS, Defender VPN - Android, Intune data collection policy, IOS-Device-Restrictions, MacOSDeviceRestrictions, MacOSEndpointProtection, and URL Protection. At the bottom of the dialog is a 'Create' button.

- 1006 7. [Create an Android configuration profile](#).
- 1007 8. [Create a Windows configuration profile](#).

3.2.1.4 Configure Conditional Access rules

1009 Conditional Access is used to control the devices and apps that can connect to company resources.

- 1010 1. Go to **Devices > Conditional Access** and click **New Policy**. Choose cloud apps or actions, conditions, and access controls to create a policy. The screenshot below illustrates this.
- 1012 2. The multi-factor authentication rule enabled in the screenshot will require MFA before granting
1013 access to enterprise Office 365 apps.

The screenshot shows the 'Conditional Access' section of the Microsoft Azure portal. On the left, under 'Access controls', there is a 'Grant' tab selected. The 'Grant' section contains several configuration options:

- Block access
- Grant access
- Require multi-factor authentication
- Require device to be marked as compliant
- Require Hybrid Azure AD joined device
- Require approved client app
 - See list of approved client apps
- Require app protection policy
 - See list of policy protected client apps

At the bottom right of the 'Grant' section is a blue 'Select' button.

- 1014 3. The Conditional Access Device Access Policy is enabled in the screenshot. It requires devices to
1015 be marked as compliant in order to get access to enterprise resources.

The screenshot shows the 'Conditional Access' section of the Microsoft Azure portal. On the left, under 'Access controls', there is a 'Grant' tab selected. The 'Grant' section contains several configuration options:

- Block access
- Grant access
- Require multi-factor authentication
- Require device to be marked as compliant
 - A warning message: '⚠️ Don't lock yourself out! Make sure that your device is compliant.'
- Require Hybrid Azure AD joined device
- Require approved client app

At the bottom right of the 'Grant' section is a blue 'Select' button.

1016 3.2.1.5 Managing Applications

- 1017 **iOS/iPadOS:** Use the instructions at [Add iOS Store Apps](#) to select apps from the iOS/iPadOS store that
1018 will be approved for installation on your managed iOS or iPadOS devices.

1019 **Android:** For this build we added Managed Google Play apps. Managed Google Play is Google's
 1020 enterprise app store which serves as a source of applications for Android Enterprise in Intune. Use the
 1021 instructions at [Add Android Store Apps](#) to select apps that will be approved for installation and made
 1022 available to your managed devices.

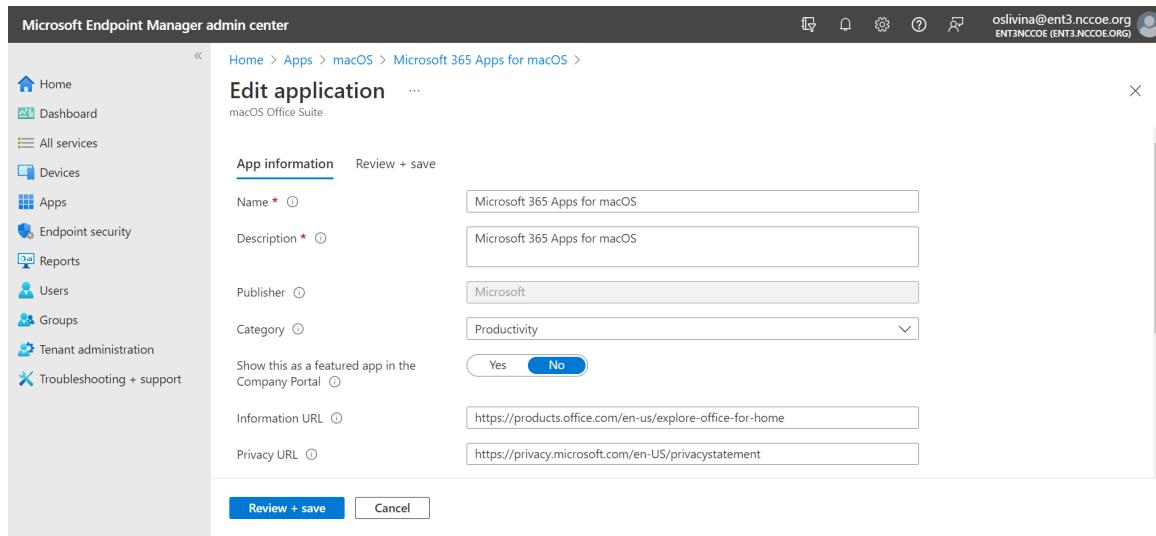
1023 **Windows:** We tested this build with Microsoft 365 Apps for Windows 10 and later. To add Windows
 1024 apps:

- 1025 1. Open the Microsoft Endpoint Manager admin center.
- 1026 2. Select **Apps > All apps > Add**.
- 1027 3. Select **Windows 10 and later** in the **Microsoft 365 Apps** section of the **Select app type** pane.
- 1028 4. Click **Select**. The **Add Microsoft 365 Apps** steps are displayed.

1029 There is more than one way to configure Windows apps in Intune. We configured the app using App
 1030 suite information. For other ways, [refer to the Microsoft documentation](#).

1031 **macOS:** Follow these steps to add macOS apps:

- 1032 1. Open the Microsoft Endpoint Manager admin center.
- 1033 2. Select **Apps > All apps > Add**.
- 1034 3. Select **macOS** in the **Microsoft 365 Apps** section of the **Select app type** pane.
- 1035 4. Click **Select**. The **Add Microsoft 365 Apps** steps are displayed.
- 1036 5. Confirm or modify the default values in the **App suite information** page.



1037 3.3 Microsoft Defender for Endpoint

1038 Microsoft Defender is an enterprise defense suite. Its main role is to detect and prevent threats and to
1039 provide protection to endpoints, identities, email, and applications. Microsoft Defender can provide
1040 device health information to the Microsoft Endpoint Manager (Intune).

1041 3.3.1 Configuration and Integration

1042 3.3.1.1 Enable Microsoft Defender for Endpoint

- 1043 1. Open the Microsoft Endpoint Manager admin center.
- 1044 2. Select **Endpoint security > Microsoft Defender for Endpoint**, and then select **Open the Mi-**
1045 **crosoft Defender for Endpoint admin console**. This opens the **Microsoft 365 Defender** portal.
- 1046 3. Select **Settings > Endpoints > Advanced features**.
- 1047 4. For **Microsoft Intune connection**, choose **On**.
- 1048 5. Return to the **Microsoft Defender for Endpoint** page in the Microsoft Endpoint Manager admin
1049 center.
- 1050 6. Under **MDM Compliance Policy Settings**, enable Microsoft Defender connections for Android,
1051 iOS, and Windows devices. To be guided through the steps on licensing validation, tenant config-
1052 uration, and network configuration, [follow Microsoft's documentation](#).
- 1053 7. Onboard devices that run Android, iOS/iPadOS, and Windows 10/11.

1054 3.3.1.2 Create Endpoint Detection and Response policy (Windows 10 and Later)

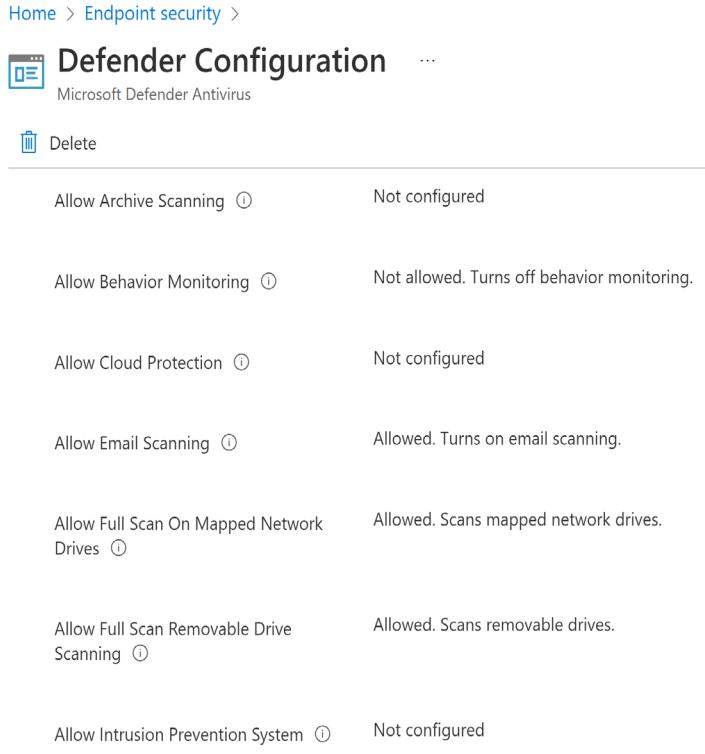
- 1055 1. Open the Microsoft Endpoint Manager portal.
- 1056 2. Navigate to **Endpoint security > Endpoint detection and response**. Click on **Create Profile**.
- 1057 3. Under **Platform**, select **Windows 10 and Later**, **Profile - Endpoint detection and response >**
1058 **Create**.
- 1059 4. Enter a name and description, then select **Next**.
- 1060 5. Select settings as required, then select **Next**.
- 1061 6. Add scope tags if necessary, then select **Next**.
- 1062 7. Click on **Select groups to include** and choose a group, then select **Next**.
- 1063 8. Review and accept and select **Create**.
- 1064 9. The completed policy appears in **Endpoint detection and response**.

Policy name	Policy type	Assigned	Platform	Target	Last modified
Defender Setup	Endpoint detection and response	Yes	Windows 10 and later	mdm,microsoftSense	04/20/22, 3:23 PM

1065 3.3.1.3 *Create an antivirus policy*

- 1066 1. Open the Microsoft Endpoint Manager portal.
- 1067 2. Navigate to **Endpoint security > Antivirus > Create Policy**.
- 1068 3. Select **Platform - Windows 10 and Later - Windows and Profile – Microsoft Defender Antivirus > Create**. Enter name and description, then select **Next**.
- 1069
- 1070 4. On the **Configuration settings page**, set the configurations for Microsoft Defender Antivirus
- 1071 5. Add scope tags and select **Next**.
- 1072 6. Select and assign groups to include, then select **Next**.
- 1073 7. Review and then select **Create**.
- 1074 8. The completed policy appears in **Endpoint security**.

Home > Endpoint security >



Defender Configuration

Microsoft Defender Antivirus

Delete

Allow Archive Scanning ⓘ	Not configured
Allow Behavior Monitoring ⓘ	Not allowed. Turns off behavior monitoring.
Allow Cloud Protection ⓘ	Not configured
Allow Email Scanning ⓘ	Allowed. Turns on email scanning.
Allow Full Scan On Mapped Network Drives ⓘ	Allowed. Scans mapped network drives.
Allow Full Scan Removable Drive Scanning ⓘ	Allowed. Scans removable drives.
Allow Intrusion Prevention System ⓘ	Not configured

1075 *3.3.1.4 Create Microsoft Defender compliance policy*

- 1076 Compliance policies can help protect organizational data by requiring users and devices to meet some requirements.
- 1077
- 1078 1. Open the Microsoft Endpoint Manager admin center.
- 1079 2. Select **Devices > Compliance policies > Policies > Create Policy**.
- 1080 3. Select a **Platform** for this policy.
- 1081 4. On the **Basics** tab, specify a **Name for the Policy**.
- 1082 5. On the **Compliance settings** tab, expand the available categories, and configure settings for the policy.
- 1083

[Home](#) > [Endpoint security](#) > [Compliance policies](#) > [WindowsComplianceDefenderPolicy](#) >

Windows 10/11 compliance policy

Windows 10 and later

- ▽ Custom Compliance
- ▽ Device Health
- ▽ Device Properties
- ▽ Configuration Manager Compliance
- ▽ System Security
- △ Microsoft Defender for Endpoint

Microsoft Defender for Endpoint rules

Require the device to be at or under the machine risk score: ⓘ

Medium

[Review + save](#) [Cancel](#)

1084 [3.3.1.5 Deploy Defender for Endpoint on iOS via Intune company portal](#)

- 1085 1. In the Microsoft Endpoint Manager admin center, go to **Apps > iOS/iPadOS > Add > iOS store app** and click **Select**.
- 1086 2. On the **Add app** page, click on **Search the App Store**, type **Microsoft Defender for Endpoint** in the search bar, and click **Select**.
- 1087 3. Select the desired value for the **Minimum operating system**. Review the rest of information about the app and click **Next**.
- 1088 4. In the **Assignments** section, go to the **Required** section and select **Add group**. Click **Select** and then **Next**.
- 1089 5. In the **Review + Create** section, verify that all the information entered is correct and then select **Create**.
- 1090
- 1091
- 1092
- 1093
- 1094

1095 [3.3.1.6 Configure supervised mode for iOS devices via Intune](#)

- 1096 1. Open Microsoft Endpoint Manager admin center and go to **Apps > App configuration policies > Add**. Select **Managed devices**.
- 1097 2. In the **Create app configuration policy** page, provide **Policy Name, Platform: iOS/iPadOS, Targeted app: Microsoft Defender for Endpoint**.
- 1098
- 1099

- 1100 3. In the next screen, select **Use configuration designer** as the configuration settings format. Spec-
1101 ify the following property:
- 1102 a. **Configuration key:** issupervised
1103 b. **Value type:** String
1104 c. **Configuration value:** {{issupervised}}

3.3.1.7 Deploy Microsoft Defender for Endpoint on Android with Microsoft Intune

- 1106 1. In the Microsoft Endpoint Manager admin center, go to **Apps > Android Apps > Add > Android**
1107 **store app** and choose **Select**.
- 1108 2. On the **Add app** page enter: **Name, Description, Publisher** as Microsoft, **App store URL** as
1109 <https://play.google.com/store/apps/details?id=com.microsoft.scmx> (Defender for Endpoint app
1110 Google Play Store URL).
- 1111 3. Select **Next**.
- 1112 4. In the **Assignments** section, go to the **Required** section and select **Add group, Select group** and
1113 click **Next**.
- 1114 5. The completed Android app configuration policy appears under **All services > Apps**.
- 1115 6. On the Android mobile device, tap the Microsoft Defender for Endpoint app icon and follow the
1116 on-screen instructions to complete onboarding the app.

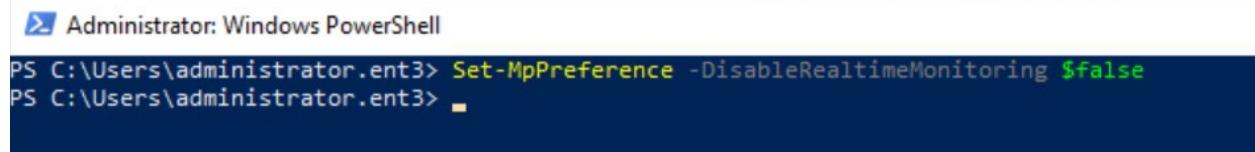
3.3.2 Microsoft Defender Antivirus

1118 Microsoft Defender Antivirus is leveraged by Microsoft Defender by Endpoint, which is anti-malware
1119 software built into Windows client devices. It detects threats and malware on client devices and
1120 quarantines infected files. Defender Antivirus is enabled by default.

1121 Ensure that real-time protection is enabled by running
1122 `(Get-MpComputerStatus).RealtimeProtectionEnabled`
1123 at an elevated PowerShell prompt as shown in the screenshot below.

```
Administrator: Windows PowerShell
PS C:\Users\administrator.ent3> (Get-MpComputerStatus).RealtimeProtectionEnabled
True
PS C:\Users\administrator.ent3>
```

1124 If real-time protection is off, it can be turned back on by executing
1125 Set-MpPreference -DisableRealtimeMonitoring \$false
1126 at an elevated PowerShell prompt as shown in the screenshot below.



```
Administrator: Windows PowerShell
PS C:\Users\administrator.ent3> Set-MpPreference -DisableRealtimeMonitoring $false
PS C:\Users\administrator.ent3> -
```

1127 Verify that real-time protection is on by going to **Control Panel > System and Security > Security and**
1128 **Maintenance > Security > Virus Protection.**

1129 3.4 Microsoft Sentinel

1130 Microsoft Sentinel is a cloud-native SIEM and SOAR system. It can be used for security analytics, threat
1131 intelligence, attack detection, and threat response.

1132 There is no need to install Sentinel, as it is a managed service. Instead, it needs to be enabled and
1133 configured in your Azure environment. It also needs a workspace to store and correlate ingested data.

- 1134 1. [Enable Sentinel and configure a workspace.](#)
- 1135 2. Use the general instructions found at [Connector to Data Sources](#) to enable log forwarding to
1136 Sentinel from various devices, systems, and services. Each data source will have to be connected
1137 independently from other data sources, so you must perform this step once per data source. In
1138 this build, Azure AD, Endpoint Manager, Defender for Endpoint, Office365, and Tenable.io were
1139 configured to send logs using this method.
- 1140 3. The Log Analytics Agent is a log forwarder that accepts syslog and common event format (CEF)
1141 formatted logs and then forwards the logs to Sentinel. If you have a product or device without a
1142 native Sentinel integration, [install and configure the Log Analytics Agent on a virtual machine](#).
1143 Once completed, the log forwarder will be able to receive syslog data on UDP port 514. Then
1144 configure the product or device that will be the data source to send logs via syslog to the log for-
1145 warder using the product's instructions.

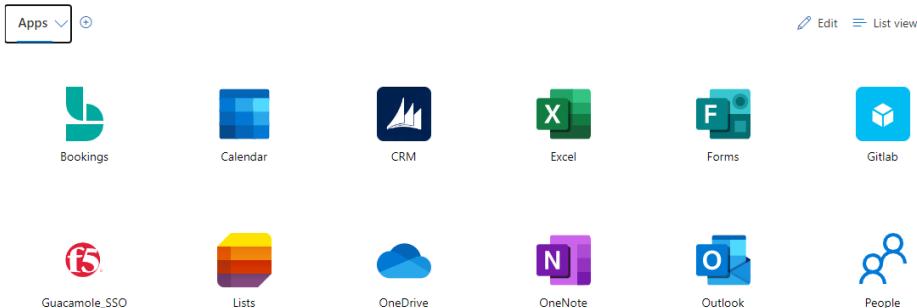
1146 3.5 F5 BIG-IP

1147 BIG-IP is both a load balancer and an identity-aware proxy. In this phase of the build, it was primarily
1148 used as an identity-aware reverse proxy that forwarded or denied traffic to protected back-end
1149 applications.

1150 3.5.1 Installation, Configuration, and Integration

1151 BIG-IP was deployed into the environment using a virtual machine image or open virtual appliance
 1152 (OVA) file. Once this OVA import operation is complete, you would log into the virtual machine console
 1153 and assign an IP address to a network interface, then continue configuration by connecting to its web
 1154 interface. This BIG-IP image has both the Access Policy Manager (APM) and the Local Traffic Manager
 1155 modules installed.

- 1156 1. [Deploy BIG-IP OVA](#) into your VMWare environment.
- 1157 2. Access the BIG-IP web interface by entering the IP address or DNS name into a web browser.
 1158 Then [complete the initial setup and configuration of BIG-IP](#).
- 1159 3. [Create virtual servers which map to back-end protected applications](#)—in this build, to our Guacamole application server.
- 1161 4. [Configure BIG-IP to use Azure AD as the SAML IdP for external authentication to access back-end](#)
 1162 [applications](#). The instructions at [Configure BIG-IP Easy Button for Header Based SSO](#) and the
 1163 video at [Azure AD and BIG-IP APM Integration Video](#) provide additional references.
- 1164 5. Once these instructions are completed, BIG-IP, leveraging Azure AD for external authentication,
 1165 will only allow successfully authenticated and authorized users to access Guacamole. Access to
 1166 the backend application is either done by connecting directly via the DNS name of the applica-
 1167 tion or by going to **myapps.microsoft.com** and selecting the backend application icon, such as
 1168 **F5 Guacamole_SSO** as shown below.



- 1169 6. For this build, [configure BIG-IP to send logs to Microsoft Sentinel](#). Then you can observe BIG-IP
 1170 logs in Sentinel, as shown below.

The screenshot shows the Microsoft Sentinel Log Analytics interface. At the top, it says "Microsoft Sentinel | Logs" and "Selected workspace: 'secops'". Below that is a search bar labeled "New Query 1*" with a "Run" button and a time range selector set to "Last 3 days". The main area displays a query result titled "1 F5Telemetry_AVR_CL". The results table has columns for TimeGenerated [UTC], tot_links_s, and cur_links_s. The first row shows a timestamp of 6/3/2022, 1:45:05.660 PM. Subsequent rows show timestamps at 6/3/2022, 2:35:05.644 PM and 6/3/2022, 2:35:05.884 PM, each with detailed log entries below it. A vertical sidebar on the left is labeled "Schema and Filter".

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	

1171 3.6 Lookout Mobile Endpoint Security (MES)

1172 Lookout Mobile Endpoint Security (MES) solution is used to control mobile device access to corporate
 1173 resources based on risk assessment. Risk is assessed based on information collected from devices by the
 1174 Lookout service. Lookout then communicates this risk level to Mobile Device Management (Microsoft
 1175 Endpoint Manager (Intune)) which determines whether the device is compliant or not.

1176 3.6.1 Configuration and Integration

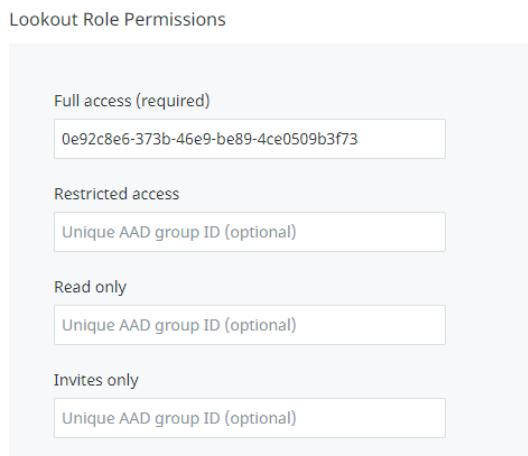
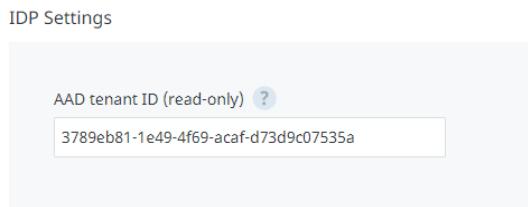
1177 Before configuring Lookout, collect the following information from Azure AD: **Azure AD tenant ID** and
 1178 **Azure AD group object ID**.

- 1179 1. Go to **Azure Active Directory > Properties** and locate **Tenant ID**. Copy and save it to the text file.
- 1180 2. Go to **Azure Active Directory > Groups** to open the **Groups | All groups** pane.
- 1181 3. Select the group with full access *rights* (Lookout Admin group).

1182 4. Copy the (group) **Object Id**, and then save it in a text file.

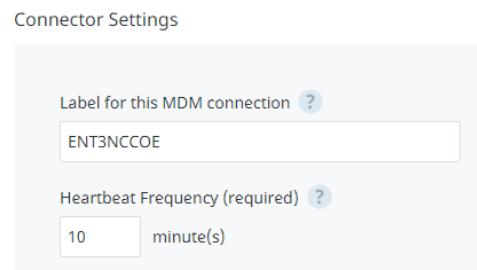
1183 The following steps are to be completed in the Lookout Enterprise admin console and will enable a
1184 connection to Lookout's service for Intune enrolled devices.

1185 1. Sign in to the Lookout for Work console and go to **System > Integrations**, and then select
1186 **Choose a product to set up**. Select **Microsoft Azure**. Copy and paste the Azure AD (AAD) tenant
1187 ID and group object ID from the text file that was created in previous steps.

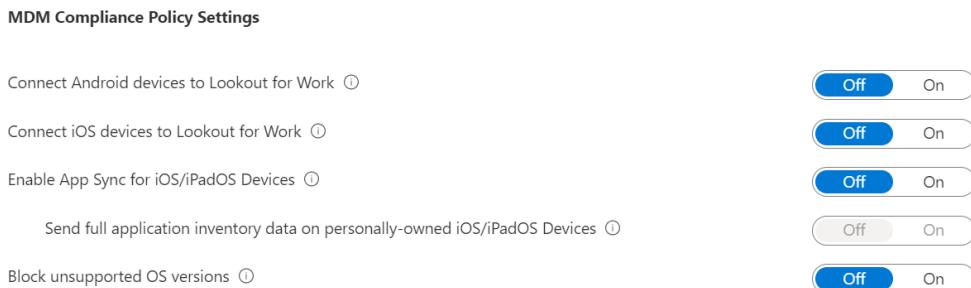


1188 2. Stay in **System > Integrations**, and then select **Choose a product to set up**. Select Microsoft
1189 **Intune**.

1190 3. Configure Intune connector settings.



- 1191 After Lookout MES is enabled, a connection to Lookout in Intune needs to be set up.
- 1192 1. Go back to Microsoft Endpoint Manager and enable the Mobile Threat Defense connector there.
- 1193 2. Select **Tenant administration > Connectors and tokens > Mobile Threat Defense**.
- 1194 3. On the **Mobile Threat Defense** pane, select **Add**.
- 1195 4. For **Mobile Threat Defense connector to setup**, select **Lookout** MTD solution from the drop-down list.
- 1196
- 1197 5. Configure the toggle options according to the organization's requirements. This screenshot shows examples.
- 1198



- 1199 When Lookout is integrated with Intune MTD and the connection to Intune is enabled, Intune creates a
 1200 classic conditional access policy in Azure AD. To view classic conditional access policy, go to **Azure Active**
 1201 **Directory > Conditional Access > Classic policies**. Classic conditional access policy is used by Intune MTD
 1202 to require that devices are registered in Azure AD so that they have a device ID before communicating to
 1203 Lookout MTD. The ID is required so that devices can report their status to Intune.

1204 3.6.2 Create MTD device compliance policy with Intune

1205 Compliance policy is needed to detect threats and assess risks on mobile devices to determine if the
 1206 device is compliant or not.

- 1207 1. Open the Microsoft Endpoint Manager admin center.
- 1208 2. Select **Endpoint security > Device Compliance > Create Policy**.
- 1209 3. Select the **Platform**, and then **Create**.
- 1210 4. On **Basics**, provide **Name**, and **Description**. Select **Next** to continue.
- 1211 5. On **Compliance settings**, expand and configure **Device Health**. Choose the Mobile Threat Level
 1212 from the drop-down list for **Require the device to be at or under the Device Threat Level**.
 1213 Choose the level for compliance.

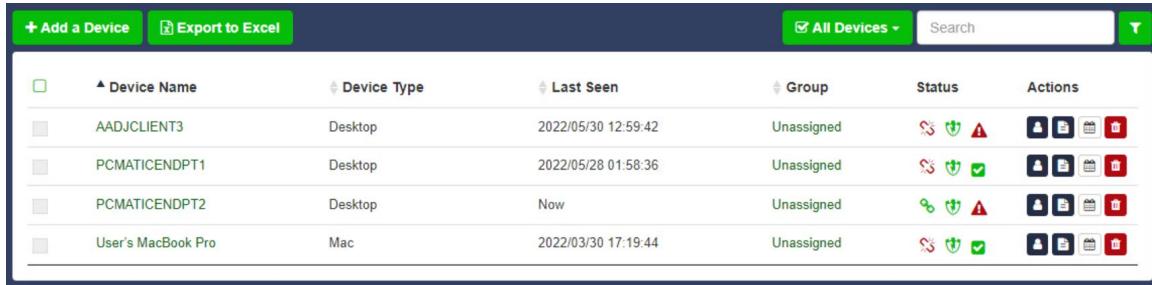
1214 6. Select **Next** to go to **Assignments**. Select the groups or users to assign this policy.

1215 **3.7 PC Matic Pro**

1216 PC Matic Pro is an endpoint protection system that consists of a server for centralized management and
1217 agents installed on endpoints. In addition to scanning for malware, it uses a default-deny approach in
1218 preventing malicious or unauthorized programs and processes from executing. To configure PC Matic
1219 Pro, you will need to install the server, install the agents, and configure a list of allowed software.

1220 PC Matic Pro Server needs to be installed on a server with Windows 2019 Server and SQL server
1221 preinstalled.

- 1222 1. Obtain the *OnPremInstallerRun.ps1* installation script from the vendor and open an elevated
1223 PowerShell window.
 - 1224 2. Execute the *OnPremInstallerRun.ps1* script by entering `.\OnPremInstallerRun.ps1 registerUser pcmatic -registryPwd <insert_password_here> -localDBUser pcm-app` to install
1225 docker, pull down the container images, and deploy the container instances that make up the
1226 PC Matic Pro server.
 - 1228 3. Navigate to the PC Matic web server and verify that it is operational by opening a web browser
1229 and going to https://<pcmaticDNSName>/web_portal. In this build, the DNS name is
1230 nist.pcmaticfederal.com; as such, to access the server's web interface, we would go to
1231 https://nist.pcmaticfederal.com/web_portal.
- 1232 Follow these steps to install PC Matic Endpoint Agents:
- 1233 1. Open a web browser on a Windows or macOS client device. Navigate to the PC Matic Server
1234 web interface by browsing to <https://nist.pcmaticfederal.com> from the client device and log on
1235 with your credentials.
 - 1236 2. Click **Add a Device** and then click **Windows Installer** or **Mac Installer**, as appropriate, to download
1237 the PC Matic Endpoint Agent.
 - 1238 3. Install the agent.
 - 1239 4. Once installed, the agent will establish communications with the server and show up on the list
1240 of managed devices once you log on to the server as previously described.
 - 1241 5. Devices with an agent will register and come online.



The screenshot shows a web-based interface for managing devices. At the top, there are buttons for '+ Add a Device' and 'Export to Excel'. A dropdown menu shows 'All Devices' with a checkmark. A search bar is next to it, and a green 'T' icon is on the far right. Below this is a table with columns: Device Name, Device Type, Last Seen, Group, Status, and Actions. The table contains four rows of data:

	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	! ! ✓	! ! ✓

1242 **3.8 Tenable.io**

1243 For installation, configuration, and integration instructions, refer to [Section 2.10](#).

1244 **3.8.1 Integration with Microsoft Sentinel**

- 1245 1. In Tenable.io, click the hamburger menu (☰) in the top left corner and navigate to **Settings > Access Control > Users**.
- 1246 2. (Optional) Click **Create User** and create a new API user for Microsoft Sentinel. In this implementation, a standard administrator account was used.
- 1247 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.
- 1248 4. In Microsoft Sentinel, navigate to **Data Connectors**. Search *tenable* and click **Tenable.io Vulnerability Management (Preview) > Open Connector Page**.
- 1249 5. Scroll down in the Instructions panel and save the Workspace ID and Primary Key.
- 1250 6. Click **Deploy to Azure**.
- 1251 7. Select the appropriate resource group.
- 1252 8. In the Workspace ID and Workspace Key fields, enter the values obtained in step 5.
- 1253 9. In the Tenable Access Key and Tenable Secret Key fields, enter the values obtained in step 3.
- 1254 10. Click **Review + create**.
- 1255 11. Click **Create**. Function deployment will begin. Once deployment is complete, it will take some time before Sentinel begins making calls to Tenable.io.

1261 **3.9 Tenable.ad**

1262 For installation, configuration, and integration instructions, refer to [Section 2.11](#).

1263 **3.10 Mandiant Security Validation (MSV)**

1264 For installation, configuration, and integration instructions, refer to [Section 2.12](#).

1265 **3.11 Forescout eyeSight**

1266 Forescout eyeSight provides asset discovery with both active and passive techniques, and through
1267 integrations with network and security infrastructure. In this build, Forescout eyeSight was deployed on-
1268 premises in two virtual hosts: an Enterprise Manager and Forescout Appliance.

1269 For Forescout eyeSight installation instructions, visit the [Forescout Installation Overview](#).

1270 **3.11.1 Integration with AD**

- 1271 1. In AD, create a domain administrator service account for Forescout and save the credentials.
- 1272 2. In the Forescout console, navigate to **Tools > Options > HPS Inspection Engine**.
- 1273 3. In the **Domain Credentials** section, click the **Add** button.
- 1274 4. Enter the domain information and credentials you saved earlier. Click **OK**.
- 1275 5. Click **Apply**. After the new configuration is saved, click **Test** to verify that the credentials are
1276 working as expected.

1277 **3.11.2 Integration with Cisco Switch**

1278 For Cisco Switch integration instructions, visit the [Switch Plugin Configuration Guide](#).

1279 **3.11.3 Integration with Cisco Wireless Controller**

1280 For Cisco Wireless Controller integration instructions, visit the [Wireless Plugin Configuration Guide](#).

1281 **3.11.4 Integration with Microsoft Sentinel**

- 1282 1. In the Forescout console, navigate to **Tools > Options > CEF**.
- 1283 2. Click **Add**.
- 1284 3. In the Add Server dialog, enter a Name, select **Use UDP for Connection**, and enter the IP address
1285 of the Sentinel Log Forwarder. Click **Next**.
- 1286 4. Click the **Assign CounterACT Devices** radio button, and check all of the checkboxes next to the
1287 listed devices.
- 1288 5. Click **Finish**. Verify that logs are being received by the Sentinel Log Forwarder.

1289 **3.11.5 Integration with Palo Alto Networks NGFW**

1290 For Palo Alto Networks Next-Generation Firewall (NGFW) integration instructions, visit the [eyeExtend](#)
1291 [for Palo Alto Networks Next-Generation Firewall Configuration Guide.](#)

1292 **3.11.6 Integration with Tenable.io**

1293 For Tenable.io integration instructions, visit the [eyeExtend for Tenable.io Vulnerability Management](#)
1294 [Configuration Guide.](#)

1295 **3.12 Palo Alto Next Generation Firewall**

1296 In this build, a virtualized Palo Alto Next Generation Firewall was deployed on-premises as a security and
1297 access control device. The firewall provides zone-based network filtering for both inbound and
1298 outbound traffic, including remote access virtual private networks (VPNs) using the GlobalProtect
1299 clients.

1300 For GlobalProtect VPN access installation instructions, visit:

1301 <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIFbCAK>

1302 **3.13 DigiCert CertCentral**

1303 For setup and usage instructions, refer to [Section 2.13.](#)

1304 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
E3B1	EIG Enterprise 3 Build 1
EIG	Enhanced Identity Governance
FQDN	Fully Qualified Domain Name
HDAP	High-Availability Directory Access Protocol
HR	Human Resources
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
NTP	Network Time Protocol
OS	Operating System
OU	Organizational Unit
OVA	Okta Verify App, Open Virtual Appliance
PA	Policy Administration
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
VPN	Virtual Private Network
ZSO	Zero Sign-On
ZTA	Zero Trust Architecture