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

## **Peter Gallagher**

**Aaron Palermo** Appgate Coral Gables, FL

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

Kyle Black **Sunjeet Randhawa** Broadcom Software San Jose, CA

July 2023

THIRD PRELIMINARY DRAFT

**Mike Delaguardia Matthew Hyatt** Cisco Herndon, VA

**Corey Bonnell** Dean Coclin DigiCert Lehi, UT

Ryan Johnson **Dung Lam** F5 Seattle, WA

#### **Neal Lucier** Tom May Forescout San Jose, CA

**Christopher Altman** Marco Genovese Google Cloud Mill Valley, CA

#### **Harmeet Singh** Priti Patil IRM Armonk, NY

**Corey Lund** Farhan Saifudin Ivanti South Jordan, UT

Hashim Khan **Tim LeMaster** Lookout Reston, VA

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

**Carmichael Patton Brandon Stephenson** Microsoft Redmond, WA

Vinu Panicker Okta San Francisco, CA

Seetal Patel **Norman Wong** Palo Alto Networks Santa Clara, CA

#### **Shawn Higgins Rob Woodworth** PC Matic

Myrtle Beach, SC

**Mitchell Lewars Bryan Rosensteel** Ping Identity Denver, CO

#### **Don Coltrain** Wade Ellery

Radiant Logic Novato, CA

#### **Frank Briguglio Ryan Tighe** SailPoint

Austin, TX

#### **Chris Jensen** Joshua Moll

Tenable Columbia, MD

**Jason White** Trellix, Public Sector Reston, VA

**Peter Bjork Genc Domi** VMware Palo Alto, CA

Joe Brown Jim Kovach Zimperium Dallas, TX

Syed Ali **Bob Smith** Zscaler San Jose, CA

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



#### 1 **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,
- 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, 97 pages, (July 2023), 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: <u>nccoe-zta-project@list.nist.gov.</u>
- 19 Public comment period: July 19, 2023 through September 4, 2023
- 20 All comments are subject to release under the Freedom of Information Act.

21	National Cybersecurity Center of Excellence
22	National Institute of Standards and Technology
23	100 Bureau Drive
24	Mailstop 2002
25	Gaithersburg, MD 20899
26	Email: <u>nccoe@nist.gov</u>

## 27 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards
and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and
academic institutions work together to address businesses' most pressing cybersecurity issues. This
public-private partnership enables the creation of practical cybersecurity solutions for specific
industries, as well as for broad, cross-sector technology challenges. Through consortia under
Cooperative Research and Development Agreements (CRADAs), including technology collaborators—
from Fortune 50 market leaders to smaller companies specializing in information technology security—

- 1011 Fortune 50 market leaders to smaller companies specializing in mormation technology security
- 35 the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity
- solutions using commercially available technology. The NCCoE documents these example solutions in
   the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework
- and details the steps needed for another entity to re-create the example solution. The NCCoE was
- established in 2012 by NIST in partnership with the State of Maryland and Montgomery County,
- 40 Maryland.

To learn more about the NCCoE, visit <u>https://www.nccoe.nist.gov/</u>. To learn more about NIST, visit 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
- 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);
- 68 *microsegmentation; software-defined perimeter (SDP); zero trust; zero trust architecture (ZTA).*

#### 69 **ACKNOWLEDGMENTS**

70	We are grateful to the following	o individuals for their	generous contributions of	f expertise and time.
/0	we are graterur to the following	g inulviduals for their	generous contributions c	expertise and time.

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

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

Name	Organization
Sharath Math	IBM
Naveen Murthy	IBM
Nikhil Shah	IBM
Deepa Shetty	IBM
Harishkumar Somashekaraiah	IBM
Mike Spisak	IBM
Krishna Yellepeddy	IBM
Vahid Esfahani	IT Coalition
Ebadullah Siddiqui	IT Coalition
Musumani Woods	IT Coalition
Tyler Croak	Lookout
Madhu Dodda	Lookout
Jeff Gilhool	Lookout
Ken Durbin	Mandiant
Earl Matthews	Mandiant
Joey Cruz	Microsoft
Tarek Dawoud	Microsoft
Janet Jones	Microsoft

Name	Organization
Hemma Prafullchandra	Microsoft
Enrique Saggese	Microsoft
Clay Taylor	Microsoft
Sarah Young	Microsoft
Spike Dog	MITRE
Sallie Edwards	MITRE
Ayayidjin Gabiam	MITRE
Jolene Loveless	MITRE
Karri Meldorf	MITRE
Kenneth Sandlin	MITRE
Lauren Swan	MITRE
Jessica Walton	MITRE
Mike Bartock	NIST
Oliver Borchert	NIST
Douglas Montgomery	NIST
Scott Rose	NIST
Kevin Stine	NIST
Sean Frazier	Okta

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

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

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

72 The Technology Partners/Collaborators who participated in this build submitted their capabilities in

response to a notice in the Federal Register. Respondents with relevant capabilities or product

components were invited to sign a Cooperative Research and Development Agreement (CRADA) with

75 NIST, allowing them to participate in a consortium to build this example solution. We worked with:

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

#### 76 **DOCUMENT CONVENTIONS**

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

#### 84 CALL FOR PATENT CLAIMS

- 85 This public review includes a call for information on essential patent claims (claims whose use would be
- 86 required for compliance with the guidance or requirements in this Information Technology Laboratory
- 87 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication
- 88 or by reference to another publication. This call also includes disclosure, where known, of the existence
- 89 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant
- 90 unexpired U.S. or foreign patents.
- 91 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in 92 written or electronic form, either:
- a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not
   currently intend holding any essential patent claim(s); or
- 95 b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring
- to utilize the license for the purpose of complying with the guidance or requirements in this ITL draftpublication either:
- under reasonable terms and conditions that are demonstrably free of any unfair discrimination;
   or
- without compensation and under reasonable terms and conditions that are demonstrably free
   of any unfair discrimination.
- 102 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
- 103 behalf) will include in any documents transferring ownership of patents subject to the assurance,
- 104 provisions sufficient to ensure that the commitments in the assurance are binding on the transferee,
- and that the transferee will similarly include appropriate provisions in the event of future transfers with
- 106 the goal of binding each successor-in-interest.
- 107 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of 108 whether such provisions are included in the relevant transfer documents.

THIRD PRELIMINARY DRAFT

109 Such statements should be addressed to: <u>nccoe-zta-project@list.nist.gov</u>

# 110 **Contents**

111	1	Intr	oduct	ion	1
112		1.1	How to	o Use this Guide	1
113		1.2	Build (	Dverview	
114			1.2.1	EIG Crawl Phase Build Features	4
115			1.2.2	EIG Run Phase Build Features	4
116			1.2.3	SDP and Microsegmentation Phase Build Features	5
117			1.2.4	Physical Architecture Overview	5
118		1.3	Турод	raphic Conventions	10
119	2	Ente	erprise	e 1 Build 1 (E1B1) Product Guides	10
120		2.1	Okta lo	dentity Cloud	10
121			2.1.1	Configuration and Integration	10
122			2.1.2	Okta Verify App	11
123			2.1.3	Okta Access Gateway	12
124		2.2	Radiar	nt Logic RadiantOne	12
125			2.2.1	Installation	12
126			2.2.2	Configuration	12
127			2.2.3	Integration	16
128		2.3	SailPoi	int IdentityIQ	16
129			2.3.1	Installation and Configuration	16
130			2.3.2	Integration with Radiant Logic	20
131			2.3.3	Integration with AD	21
132			2.3.4	Integration with Okta	22
133		2.4	Ivanti	Neurons for UEM	23
134			2.4.1	Installation and Configuration	23
135			2.4.2	Integration with Ivanti Connector	29
136			2.4.3	Integration with Okta	29
137			2.4.4	Integration with QRadar	30
138		2.5	Ivanti	Sentry	32

139			2.5.1	Installation and Configuration	32
140			2.5.2	Ivanti Tunnel Configuration and Deployment	32
141		2.6	lvanti /	Access ZSO	. 32
142			2.6.1	Integration with Ivanti Neurons for UEM	33
143			2.6.2	Integration with Okta	33
144		2.7	Zimpe	rium Mobile Threat Defense (MTD)	. 34
145			2.7.1	Installation, Configuration, and Integration	34
146		2.8	IBM Cl	oud Pak for Security	. 38
147		2.9	IBM Se	ecurity QRadar XDR	. 38
148		2.10	Tenabl	e.io	. 39
149			2.10.1	Installation and Configuration	39
150			2.10.2	Integration with QRadar	40
151		2.11	Tenabl	e.ad	.40
152		2.12	Tenabl	e NNM	. 40
153			2.12.1	Deploy a Tenable NNM instance	40
154		2.13	Mandi	ant Security Validation (MSV)	.41
155			2.13.1	MSV Director Installation/Configuration	41
156			2.13.2	MSV Network Actor Installation/Configuration	42
157			2.13.3	MSV Endpoint Actor Installation/Configuration	42
158			2.13.4	MSV Evaluation Configuration	43
159			2.13.5	MSV Evaluation Execution	44
160		2.14	DigiCe	rt CertCentral	. 45
161			2.14.1	Requesting a certificate	45
162			2.14.2	Obtaining and implementing a certificate	46
163	3	Ente	erprise	e 2 Build 1 (E2B1) Product Guides	.46
164		3.1	Ping Id	entity PingOne	. 46
165			3.1.1	Configuration: PingOne and PingFederate	46
166			3.1.2	Integration with Radiant Logic	47
167			3.1.3	Integration with Cisco Duo	48
168		3.2	Radian	t Logic RadiantOne	. 48

		3.2.1 Installation and Configuration	48
		3.2.2 Configuration	48
		3.2.3 Integration	48
	3.3	SailPoint IdentityIQ	48
		3.3.1 Installation and Configuration	48
		3.3.2 Integration with Radiant Logic	48
		3.3.3 Integration with AD	49
		3.3.4 Integration with Ping Identity	49
	3.4	Cisco Duo	49
		3.4.1 Configuration	49
		3.4.2 Integration	49
	3.5	Palo Alto Networks Next Generation Firewall	50
	3.6	IBM Security QRadar XDR	50
	3.7	Tenable.io	50
	3.8	Tenable.ad	50
	3.9	Tenable NNM	50
	3.10	Mandiant Security Validation (MSV)	50
	3.11	DigiCert CertCentral	50
4	Ente	erprise 3 Build 1 (E3B1) Product Guides	50
	4.1	Microsoft Azure Active Directory (AD)	51
	4.2	Microsoft Endpoint Manager	51
		4.2.1 Configuration and Integration	52
	4.3	Microsoft Defender for Endpoint	53
		4.3.1 Configuration and Integration	53
		4.3.2 Microsoft Defender Antivirus	54
	4.4	Microsoft Sentinel	54
	4.5	Microsoft Office 365	54
	4.6	F5 BIG-IP	55
		4.6.1 Installation, Configuration, and Integration	55
	4.7	Lookout Mobile Endpoint Security (MES)	56
	4	3.3 3.4 3.4 3.5 3.6 3.7 3.8 3.9 3.10 3.11 4 Ent 4.1 4.2 4.3 4.3 4.4 4.5 4.6 4.7	<ul> <li>3.2.1 Installation and Configuration</li> <li>3.2.2 Configuration</li> <li>3.2.3 Integration</li> <li>3.3 SailPoint IdentityIQ</li> <li>3.3.1 Installation and Configuration</li> <li>3.3.2 Integration with Radiant Logic</li> <li>3.3.3 Integration with AD</li> <li>3.3.4 Integration with AD</li> <li>3.4.1 Integration with Ping Identity</li> <li>3.4 Cisco Duo</li> <li>3.4.1 Configuration</li> <li>3.4.2 Integration</li> <li>3.5 Palo Alto Networks Next Generation Firewall</li> <li>3.6 IBM Security QRadar XDR</li> <li>3.7 Tenable.io</li> <li>3.8 Tenable.ad</li> <li>3.9 Tenable NNM</li> <li>3.10 Mandiant Security Validation (MSV)</li> <li>3.11 DigiCert CertCentral</li> <li>4 Enterprise 3 Build 1 (E3B1) Product Guides</li> <li>4.1 Microsoft Azure Active Directory (AD)</li> <li>4.2 Microsoft Defender for Endpoint</li> <li>4.3.1 Configuration and Integration</li> <li>4.3.2 Microsoft Defender Antivirus</li> <li>4.4 Microsoft Defender Antivirus</li> <li>4.4 Microsoft Defender for Endpoint</li> <li>4.3.2 Microsoft Defender Antivirus</li> <li>4.4 Microsoft Defender for Endpoint</li> <li>4.5 Microsoft Defender Antivirus</li> <li>4.6 Installation, Configuration, and Integration</li> <li>4.7 Lookout Mobile Endpoint Security (MES)</li> </ul>

199			4.7.1	Configuration and Integration	57
200			4.7.2	Create MTD Device Compliance Policy with Intune	59
201		4.8	PC Ma	tic Pro	59
202		4.9	Tenabl	e.io	60
203			4.9.1	Integration with Microsoft Sentinel	60
204		4.10	Tenabl	e.ad	61
205		4.11	Tenabl	e NNM	61
206		4.12	Mandi	ant Security Validation (MSV)	61
207		4.13	Foresc	out eyeSight	61
208			4.13.1	Integration with AD	61
209			4.13.2	Integration with Cisco Switch	62
210			4.13.3	Integration with Cisco Wireless Controller	62
211			4.13.4	Integration with Microsoft Sentinel	62
212			4.13.5	Integration with Palo Alto Networks NGFW	62
213			4.13.6	Integration with Tenable.io	62
214		4.14	Palo A	Ito Networks Next Generation Firewall	62
215		4.15	DigiCe	rt CertCentral	62
216	5	Ente	erprise	e 1 Build 2 (E1B2) Product Guides	62
217		5.1	Zscale	r	63
218			5.1.1	Zscaler ZPA Configuration and Integration	63
219			5.1.2	Zscaler ZIA Configuration	64
220			5.1.3	Zscaler Client Connector	64
221			5.1.4	Zscaler Application Connector	64
222		5.2	Okta lo	dentity Cloud	64
223		5.3	Radian	t Logic RadiantOne	64
224		5.4	SailPoi	nt IdentityIQ	65
225		5.5	Ivanti I	Neurons for UEM	65
226		5.6	IBM Se	ecurity QRadar XDR	65
227		5.7	Tenabl	e.io	65
228		5.8	Tenabl	e.ad	65

229		5.9	Tenable NNM65		
230		5.10	Mandi	ant Security Validation (MSV)	65
231		5.11	DigiCert CertCentral		
232		5.12	AWS la	aaS	65
233			5.12.1	Configuration	66
234	6	Ente	erprise	e 3 Build 2 (E3B2) Product Guides	.66
235		6.1	Micros	oft Azure AD Identity Protection	66
236		6.2	Micros	oft Azure AD Identity Governance	67
237		6.3	Micros	oft Defender for Cloud Apps	67
238		6.4	Micros	oft Azure AD Application Proxy	68
239		6.5	Micros	oft Defender for Cloud	68
240		6.6	Foresc	out eyeSight	68
241		6.7	Foresc	out eyeControl	69
242			6.7.1	Configuring a policy	69
243		6.8	Foresc	out eyeSegment	69
244			6.8.1	Access the eyeSegment Dashboard	69
245		6.9	Foresc	out eyeExtend	70
246			6.9.1	Integration with Microsoft Endpoint Manager	70
247		6.10	Micros	oft Azure IaaS	70
248	7	Ente	erprise	e 1 Build 3 (E1B3) Product Guides	.71
249	8	Ente	erprise	e 2 Build 3 (E2B3) Product Guides	.71
250		8.1	Ping Id	entity PingOne	71
251			8.1.1	Configuration: PingOne and PingFederate	71
252			8.1.2	Integrations	71
253		8.2	Radian	t Logic RadiantOne	72
254			8.2.1	Installation and Configuration	72
255			8.2.2	Integrations	72
256		8.3	SailPoi	nt IdentityIQ	72
257			8.3.1	Installation and Configuration	72

258		8.3.2	Integration with Radiant Logic	. 72	
259		8.3.3	Integration with AD	. 73	
260		8.3.4	Integration with Ping Identity	. 73	
261	8.4	VMwai	e Workspace ONE	. 73	
262		8.4.1	VMware Workspace ONE Access	. 73	
263		8.4.2	Setup	. 73	
264		8.4.3	Integration with RadiantOne	. 73	
265		8.4.4	Integration with PingFederate	. 74	
266		8.4.5	VMware Workspace ONE UEM	. 75	
267		8.4.6	Setup	. 75	
268		8.4.7	Integration with Certificate Authority	. 75	
269	8.5	Cisco D	9uo	. 75	
270		8.5.1	Configuration	. 76	
271		8.5.2	Integration	. 76	
272	8.6	Palo Al	to Networks Next Generation Firewall	. 76	
273	8.7	IBM Se	curity QRadar XDR	. 76	
274	8.8	Tenabl	e.io	. 76	
275	8.9	Tenabl	e.ad	. 76	
276	8.10	Tenabl	Tenable NNM		
277	8.11	Mandia	ant Security Validation (MSV)	.76	
278	8.12	DigiCer	t CertCentral	.76	
279	8.13	Cisco lo	dentity Services Engine (ISE)	. 76	
280		8.13.1	Integrations	. 77	
281	8.14	Cisco S	ecure Workload (CSW – Formerly Tetration)	. 77	
282		8.14.1	Configuration	. 78	
283	8.15	Cisco S	ecure Network Analytics (SNA – Formerly Stealthwatch)	. 78	
284		8.15.1	Installation	. 79	
285		8.15.2	Configuration	. 79	
286		8.15.3	Integration	. 79	
287	8.16	Cisco S	ecure Endpoint (CSE – Formerly AMP)	. 79	

288			8.16.1 Integrations	80
289		8.17	Palo Alto Networks - Panorama	80
290			8.17.1 Integration with Cisco ISE	
291	9	Ente	erprise 3 Build 3 (E3B3) Product Guides	81
292		9.1	Microsoft Defender for Identity	81
293		9.2	Microsoft Defender for Office	81
294		9.3	Purview Information Protection	82
295			9.3.1 Information Protection Scanner	82
296			9.3.2 Purview DLP	82
297		9.4	Entra Permissions Management	82
298		9.5	Azure Virtual Desktop	83
299		9.6	Intune VPN Tunnel	83
300		9.7	Azure Arc	83
301		9.8	Azure Automanage	83
302		9.9	Microsoft Sentinel Playbooks	
303		9.10	Microsoft Privileged Access Workstation	
304	10	Ente	erprise 4 Build 3 (E4B3) Product Guides	84
305		10.1	IBM Security Verify	
306			10.1.1 Setup	
307			10.1.2 Integration with Active Directory	
308			10.1.3 Configuration	
309		10.2	IBM Security Trusteer	
310			10.2.1 Integration with IBM Security Verify	85
311		10.3	IBM Security MaaS360	85
312			10.3.1 Setup	85
313			10.3.2 Configuration	85
314		10.4	IBM Security QRadar XDR	
315			10.4.1 Integration with IBM Security MaaS360	86
316			10.4.2 Integration with IBM Security Verify	

317	10.5	IBM Security Guardium	86
318		10.5.1 IBM Security Guardium Data Protection	86
319		10.5.2 IBM Security Guardium Data Encryption	87
320	10.6	IBM Cloud Pak for Security (CP4S)	89
321		10.6.1 Installation	89
322		10.6.2 CP4S and QRadar Integration	89
323		10.6.3 CP4S Playbooks	89
324	10.1	IBM Cloud	89
325	10.2	Tenable.io	90
326	10.3	Tenable.ad	90
327	10.4	Tenable NNM	90
328	10.5	Mandiant Security Validation (MSV)	90
329	10.6	DigiCert CertCentral	90
330	10.7	Palo Alto Networks Next Generation Firewall	90
		\/\\	00
331	10.8	Vivivare	90
331 332	10.8 11 Ent	erprise 1 Build 4 (E1B4) Product Guides	90
331 332 333	10.8 <b>11 Ent</b> 11.1	erprise 1 Build 4 (E1B4) Product Guides Appgate	90
<ul><li>331</li><li>332</li><li>333</li><li>334</li></ul>	10.8 <b>11 Ent</b> 11.1	erprise 1 Build 4 (E1B4) Product Guides         Appgate         11.1.1 Appgate Installation and Configuration	90 90 
<ul> <li>331</li> <li>332</li> <li>333</li> <li>334</li> <li>335</li> </ul>	10.8 11 Ent 11.1	erprise 1 Build 4 (E1B4) Product Guides         Appgate         11.1.1 Appgate Installation and Configuration         11.1.2 Appgate Clients	90 90 91 91 91
<ul> <li>331</li> <li>332</li> <li>333</li> <li>334</li> <li>335</li> <li>336</li> </ul>	10.8 11 Ent 11.1	erprise 1 Build 4 (E1B4) Product Guides Appgate 11.1.1 Appgate Installation and Configuration 11.1.2 Appgate Clients 11.1.3 Appgate Integrations	90 91 91 91 92 92
<ul> <li>331</li> <li>332</li> <li>333</li> <li>334</li> <li>335</li> <li>336</li> <li>337</li> </ul>	10.8 11 Ent 11.1 11.2	erprise 1 Build 4 (E1B4) Product Guides Appgate 11.1.1 Appgate Installation and Configuration 11.1.2 Appgate Clients 11.1.3 Appgate Integrations Okta Identity Cloud	
<ul> <li>331</li> <li>332</li> <li>333</li> <li>334</li> <li>335</li> <li>336</li> <li>337</li> <li>338</li> </ul>	10.8 <b>11 Ent</b> 11.1 11.2 11.2 11.3	erprise 1 Build 4 (E1B4) Product Guides Appgate 11.1.1 Appgate Installation and Configuration 11.1.2 Appgate Clients 11.1.3 Appgate Integrations Okta Identity Cloud Radiant Logic RadiantOne	
<ul> <li>331</li> <li>332</li> <li>333</li> <li>334</li> <li>335</li> <li>336</li> <li>337</li> <li>338</li> <li>339</li> </ul>	10.8 <b>11 Ent</b> 11.1 11.2 11.3 11.4	erprise 1 Build 4 (E1B4) Product Guides Appgate 11.1.1 Appgate Installation and Configuration 11.1.2 Appgate Clients 11.1.3 Appgate Integrations Okta Identity Cloud Radiant Logic RadiantOne SailPoint IdentityIQ	
<ul> <li>331</li> <li>332</li> <li>333</li> <li>334</li> <li>335</li> <li>336</li> <li>337</li> <li>338</li> <li>339</li> <li>340</li> </ul>	10.8 <b>11 Ent</b> 11.1 11.2 11.3 11.4 11.5	erprise 1 Build 4 (E1B4) Product Guides Appgate 11.1.1 Appgate Installation and Configuration 11.1.2 Appgate Clients 11.1.3 Appgate Integrations Okta Identity Cloud Radiant Logic RadiantOne SailPoint IdentityIQ Ivanti Neurons for UEM	
<ul> <li>331</li> <li>332</li> <li>333</li> <li>334</li> <li>335</li> <li>336</li> <li>337</li> <li>338</li> <li>339</li> <li>340</li> <li>341</li> </ul>	10.8 <b>11 Ent</b> 11.1 11.2 11.3 11.4 11.5 11.6	erprise 1 Build 4 (E1B4) Product Guides	
<ul> <li>331</li> <li>332</li> <li>333</li> <li>334</li> <li>335</li> <li>336</li> <li>337</li> <li>338</li> <li>339</li> <li>340</li> <li>341</li> <li>342</li> </ul>	10.8 <b>11 Ent</b> 11.1 11.2 11.3 11.4 11.5 11.6 11.7	erprise 1 Build 4 (E1B4) Product Guides Appgate 11.1.1 Appgate Installation and Configuration 11.1.2 Appgate Clients 11.1.3 Appgate Integrations Okta Identity Cloud Radiant Logic RadiantOne SailPoint IdentityIQ Ivanti Neurons for UEM IBM Security QRadar XDR Tenable.io	
<ul> <li>331</li> <li>332</li> <li>333</li> <li>334</li> <li>335</li> <li>336</li> <li>337</li> <li>338</li> <li>339</li> <li>340</li> <li>341</li> <li>342</li> <li>343</li> </ul>	10.8 <b>11 Ent</b> 11.1 11.2 11.3 11.4 11.5 11.6 11.7 11.8	erprise 1 Build 4 (E1B4) Product Guides Appgate 11.1.1 Appgate Installation and Configuration 11.1.2 Appgate Clients 11.1.3 Appgate Integrations Okta Identity Cloud Radiant Logic RadiantOne SailPoint IdentityIQ Ivanti Neurons for UEM IBM Security QRadar XDR Tenable.io Tenable.ad	
<ul> <li>331</li> <li>332</li> <li>333</li> <li>334</li> <li>335</li> <li>336</li> <li>337</li> <li>338</li> <li>339</li> <li>340</li> <li>341</li> <li>342</li> <li>343</li> <li>344</li> </ul>	10.8 <b>11 Ent</b> 11.1 11.2 11.3 11.4 11.5 11.6 11.7 11.8 11.9	erprise 1 Build 4 (E1B4) Product Guides         Appgate         11.1.1 Appgate Installation and Configuration         11.1.2 Appgate Clients         11.1.3 Appgate Integrations         Okta Identity Cloud         Radiant Logic RadiantOne         SailPoint IdentityIQ         Ivanti Neurons for UEM         IBM Security QRadar XDR         Tenable.io         Tenable.ad	

346	11.11DigiCert CertCentral	94
347	11.12AWS laaS	94
348	11.12.1 AppGate Controller Configuration	94
349	11.13Zimperium Mobile Threat Defense (MTD)	94
350	Appendix A List of Acronyms	95

# 351 List of Figures

352 Figure 1-1 Laboratory Infrastructure for the EIG Builds
---

# 353 **1** Introduction

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

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

#### 359 **1.1** How to Use this Guide

360 This NIST Cybersecurity Practice Guide will help users develop a plan for migrating to ZTA. It

- 361 demonstrates a standards-based reference design for implementing a ZTA and provides users with the
- information they need to replicate ten different implementations of this reference design. Each of these
- implementations, which are known as *builds*, are standards-based and align to the concepts and
   principles in NIST Special Publication (SP) 800-207, *Zero Trust Architecture*. The reference design
- 365 described in this practice guide is modular and can be deployed in whole or in part, enabling
- 366 organizations to incorporate ZTA into their legacy environments gradually, in a process of continuous
- 367 improvement that brings them closer and closer to achieving the ZTA goals that they have prioritized
- 368 based on risk, cost, and resources.
- 369 NIST is adopting an agile process to publish this content. Each volume is being made available as soon as
- 370 possible rather than delaying release until all volumes are completed. Work continues on implementing
- 371 the example solutions and developing other parts of the content. As a third preliminary draft, we will
- 372 publish at least one additional draft for public comment before it is finalized.
- 373 When complete, this guide will contain five volumes:
- NIST SP 1800-35A: *Executive Summary* why we wrote this guide, the challenge we address,
   why it could be important to your organization, and our approach to solving this challenge
- NIST SP 1800-35B: Approach, Architecture, and Security Characteristics what we built and why
- NIST SP 1800-35C: *How-To Guides* instructions for building the example implementations,
   including all the security-relevant details that would allow you to replicate all or parts of this
   project (you are here)
- NIST SP 1800-35D: *Functional Demonstrations* use cases that have been defined to showcase
   ZTA security capabilities and the results of demonstrating them with each of the example
   implementations
- NIST SP 1800-35E: *Risk and Compliance Management* risk analysis and mapping of ZTA security
   characteristics to cybersecurity standards and recommended practices

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

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

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

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

Also, Section 3 of *Risk and Compliance Management*, *NIST SP 1800-35E*, will be of particular interest.

395 Section 3, ZTA Reference Architecture Security Mappings, maps logical components of the general ZTA

396 reference design to security characteristics listed in various cybersecurity guidelines and recommended

397 practices documents, including *Framework for Improving Critical Infrastructure Cybersecurity* (NIST

398 Cybersecurity Framework), Security and Privacy Controls for Information Systems and Organizations

399 (NIST SP 800-53), and Security Measures for "EO-Critical Software" Use Under Executive Order (EO)

400 *14028*.

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

402 them understand the importance of migrating toward standards-based ZTA implementations that align

to the concepts and principles in NIST SP 800-207, *Zero Trust Architecture*.

404 **IT professionals** who want to implement similar solutions will find the whole practice guide useful. You

405 can use the how-to portion of the guide, NIST SP 1800-35C, to replicate all or parts of the builds created

in our lab. The how-to portion of the guide provides specific product installation, configuration, and

- 407 integration instructions for implementing the example solutions. We do not re-create the product
- 408 manufacturers' documentation, which is generally widely available. Rather, we show how we
- 409 incorporated the products together in our environment to create an example solution. Also, you can use
- 410 *Functional Demonstrations,* NIST SP 1800-35D, which provides the use cases that have been defined to
- showcase ZTA security capabilities and the results of demonstrating them with each of the exampleimplementations.
- 413 This guide assumes that IT professionals have experience implementing security products within the
- 414 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
- 415 not endorse these particular products. Your organization can adopt this solution or one that adheres to
- 416 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
- 417 parts of a ZTA. Your organization's security experts should identify the products that will best integrate
- 418 with your existing tools and IT system infrastructure. We hope that you will seek products that are
- 419 congruent with applicable standards and best practices.

420 A NIST Cybersecurity Practice Guide does not describe "the" solution, but example solutions. This is a

421 third preliminary draft guide. As the project progresses, the third preliminary draft will be updated, and

422 additional volumes will also be released for comment. We seek feedback on the publication's contents

423 and welcome your input. Comments, suggestions, and success stories will improve subsequent versions

424 of this guide. Please contribute your thoughts to <u>nccoe-zta-project@list.nist.gov</u>.

## 425 1.2 Build Overview

426 This NIST Cybersecurity Practice Guide addresses the challenge of using standards-based protocols and

427 available technologies to build a ZTA. In our lab at the NCCoE and using our collaborators' cloud

428 infrastructure, we plan to implement and demonstrate a variety of builds that serve as example ZTA

solutions, each of which is designed to dynamically and securely manage access to resources across a set

430 of use cases that a medium or large enterprise might typically deploy. Our plan is to implement these

- 431 builds in a series of phases, starting with a baseline enterprise architecture that represents the typical
- 432 legacy components that an enterprise might start with when deciding to begin adding zero trust
- 433 capabilities.

434 We began with builds for enhanced identity governance (EIG) that were restricted to a limited set of

435 capabilities. We call these *EIG crawl phase builds*. The central capabilities of these builds are identity,

- 436 credential, and access management (ICAM) and endpoint protection. In particular, these EIG crawl
- 437 phase builds do not include separate, centralized policy engine (PE) or policy administration (PA)
- 438 components. Instead, these initial EIG crawl phase builds rely upon the PE and PA capabilities provided
- 439 by their ICAM components. We did not perform an EIG walk phase. After completing the EIG crawl
- 440 phase builds, we enhanced these implementations by adding specialized PE and PA components, device
- discovery, and cloud-based resources in the EIG run phase. Next, we began the software-defined

442 perimeter (SDP) and microsegmentation phase of the project. As its name suggests, this phase involved

- integrating ZTA components that support one or both of the SDP and microsegmentation deployment
- 444 models. It also integrated additional supporting components and features to provide an increasingly rich445 set of ZTA functionalities.
- 446 This practice guide provides instructions for reproducing the builds that we have implemented so far:
- 447 EIG crawl phase builds:
- Enterprise 1 Build 1 (E1B1)
- Enterprise 2 Build 1 (E2B1)
- 450 Enterprise 3 Build 1 (E3B1)
- 451 EIG run phase builds:
- 452 Enterprise 1 Build 2 (E1B2)
- 453 Enterprise 3 Build 2 (E3B2)

454	<ul> <li>Enterprise 4 Build 3 (E4B3)</li> </ul>
455	SDP and microsegmentation builds:
456	• Enterprise 1 Build 3 (E1B3)
457	• Enterprise 2 Build 3 (E2B3)
458	• Enterprise 3 Build 3 (E3B3)
459	<ul> <li>Enterprise 1 Build 4 (E1B4)</li> </ul>

460 The NCCoE worked with members of the ZTA community of interest to develop a diverse but non-461 comprehensive set of use cases and scenarios to demonstrate the capabilities of the builds. The use 462 cases are summarized in NIST SP 1800-35D, *Functional Demonstrations*.

#### 463 1.2.1 EIG Crawl Phase Build Features

464 A general ZTA reference design is depicted in Figure 4-1 of Volume B. It consists of ZTA core 465 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, 466 467 and endpoint security. The EIG crawl phase builds that have been created so far differ from this 468 reference design insofar as they do not include separate, dedicated PDP components. Their ICAM 469 component serves as their PDP, and they include very limited data security and security analytics 470 functionality. These limitations were intentionally placed on the initial builds in an attempt to 471 demonstrate the ZTA functionality that an enterprise that currently has ICAM and endpoint protection 472 solutions deployed will be able to support without having to add additional ZTA-specific capabilities. 473 Each EIG crawl phase build is instantiated in a unique way, depending on the equipment used and the 474 capabilities supported. Briefly, the three builds are as follows:

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

#### 481 1.2.2 EIG Run Phase Build Features

The EIG run phase, as its name suggests, builds upon the EIG crawl phase architecture. The EIG run
phase no longer imposes the requirement that the PE and PA components must be provided by the
ICAM products used in the build. It also adds capabilities to the EIG crawl phase. In addition to
protecting access to resources that are located on-premises, the run phase also protects access to some
resources that are hosted in the cloud. The EIG run phase includes a device discovery capability, which is

- 487 performed as part of the baseline. In addition to monitoring and alerting when new devices are
- detected, enforcement can be enabled to deny access to devices that are not compliant. The run phase
- also includes the capability to establish a tunnel between the requesting endpoint and the resource
- 490 being accessed over which access to the resource can be brokered.
- 491 Each EIG run phase build is instantiated in a unique way, depending on the equipment used and the492 capabilities supported. Briefly, the three builds are as follows:
- 493 E1B2 uses products from Amazon Web Services, IBM, Ivanti, Mandiant, Okta, Radiant Logic,
   494 SailPoint, Tenable, and Zscaler. Certificates from DigiCert are also used.
- 495 E3B2 uses products from F5, Forescout, Mandiant, Microsoft, Palo Alto Networks, PC Matic, and
   496 Tenable. Certificates from DigiCert are also used.
- 497 E4B3 uses products from IBM, Mandiant, Palo Alto Networks, Tenable, and VMware. Certificates
   498 from DigiCert are also used.

### 499 1.2.3 SDP and Microsegmentation Phase Build Features

- 500 The SDP and microsegmentation phase builds are based on the general ZTA reference design that is 501 depicted in Figure 4-1 of Volume B. It consists of ZTA core components: a PDP, which includes both a PE 502 and a PA, and one or more PEPs; and ZTA functional components for ICAM, security analytics, data 503 security, and endpoint security. The builds implemented in the SDP and microsegmentation phase of the 504 project each deploy elements of either the SDP deployment model, the microsegmentation deployment 505 model, or both.
- Each SDP and microsegmentation phase build is instantiated in a unique way, depending on theequipment used and the capabilities supported. Briefly, the four builds are as follows:
- E1B3 uses all of the same products and technologies as E1B2, so there is no separate section for
   E1B3 in this document.
- E2B3 uses products from Cisco Systems, IBM, Mandiant, Palo Alto Networks, Ping Identity,
   Radiant Logic, SailPoint, Tenable, and VMware. Certificates from DigiCert are also used.
- E3B3 uses products from F5, Forescout, Mandiant, Microsoft, Palo Alto Networks, PC Matic, and
   Tenable. Certificates from DigiCert are also used.
- E1B4 uses products from Amazon Web Services, Appgate, IBM, Ivanti, Mandiant, Okta, Radiant
   Logic, SailPoint, Tenable, and Zimperium. Certificates from DigiCert are also used.

#### 516 1.2.4 Physical Architecture Overview

- 517 The laboratory environment in which the builds have been implemented is depicted and described in
- 518 detail in Section 4.3 of Volume B. The laboratory architecture drawing from that volume is reproduced
- 519 here in Figure 1-1. As shown, this laboratory environment includes four separate enterprise

- 520 environments, each hosting its own distinct implementation of a ZTA architecture. The enterprises may
- 521 interoperate as needed by a given use case, and the baseline enterprise environments have the
- 522 flexibility to support enhancements. The laboratory environment also includes a management virtual
- 523 local area network (VLAN) on which the following components are installed: Ansible, Terraform, MSV
- 524 Director, and MSV Protected Theater. These management components support infrastructure as code
- 525 (laC) automation and orchestration.

#### THIRD PRELIMINARY DRAFT

526 Figure 1-1 Laboratory Infrastructure for the EIG Builds



527 The following builds are supported within the physical architecture depicted in Figure 1-1 and 528 documented in the remainder of this guide:

- E1B1 components consist of DigiCert CertCentral, IBM Cloud Pak for Security (CP4S), IBM
   Security QRadar XDR, Ivanti Access Zero Sign-On (ZSO), Ivanti Neurons for Unified Endpoint
   Management (UEM), Ivanti Sentry, Ivanti Tunnel, Mandiant Security Validation (MSV), Okta
   Identity Cloud, Okta Verify App, Radiant Logic RadiantOne Intelligent Identity Data Platform,
   SailPoint IdentityIQ, Tenable.ad, Tenable.io, and Zimperium Mobile Threat Defense (MTD).
- E2B1 components consist of Cisco Duo, DigiCert CertCentral, IBM Security QRadar XDR,
   Mandiant MSV, Palo Alto Networks Next Generation Firewall (NGFW), PingFederate, which is a
   service in the Ping Identity Software as a Service (SaaS) offering of PingOne, Radiant Logic
   RadiantOne Intelligent Identity Data Platform, SailPoint IdentityIQ, Tenable.ad, Tenable.io, and
   Tenable Nessus Network Monitor (NNM).
- E3B1 components consist of DigiCert CertCentral, F5 BIG-IP, Forescout eyeSight, Lookout Mobile
   Endpoint Security (MES), Mandiant MSV, Microsoft Azure Active Directory (AD), Microsoft
   Defender for Endpoint, Microsoft Endpoint Manager, Microsoft Sentinel, Palo Alto Networks
   NGFW, PC Matic Pro, Tenable.ad, and Tenable.io.
- E1B2 and E1B3 components consist of Amazon Web Services (AWS) Infrastructure as a Service (IaaS), DigiCert CertCentral, IBM CP4S, IBM Security QRadar XDR, Mandiant MSV, Okta Identity
   Cloud, Okta Verify App, Radiant Logic RadiantOne Intelligent Identity Data Platform, SailPoint IdentityIQ, Tenable.ad, Tenable.io, Tenable NNM, Zscaler Admin Portal, Zscaler Application
   Connector, Zscaler Central Authority, Zscaler Client Connector (ZCC), Zscaler Internet Access
   (ZIA) Public Service Edges, and Zscaler Private Access (ZPA) Public Service Edges.
- E3B2 components consist of DigiCert CertCentral, F5 BIG-IP, Forescout eyeControl, Forescout eyeExtend, Forescout eyeSegment, Forescout eyeSight, Mandiant MSV, Microsoft AD, Microsoft Azure AD, Microsoft Azure AD (Conditional Access), Microsoft Azure AD Identity Protection, Microsoft Azure (IaaS), Microsoft Defender for Cloud, Microsoft Defender for Cloud Apps, Microsoft Defender for Endpoint, Microsoft Intune, Microsoft Office 365 (SaaS), Microsoft Sentinel, Palo Alto Networks NGFW, PC Matic Pro, Tenable.ad, Tenable.io, and Tenable NNM.
- E2B3 components consist of Cisco Duo, Cisco Identity Services Engine (ISE), Cisco network
   devices, Cisco Secure Endpoint (CSE), Cisco Secure Network Analytics (SNA), Cisco Secure
   Workload, DigiCert CertCentral, IBM Security QRadar XDR, Mandiant MSV, Palo Alto Networks
   NGFW, Ping Identity PingOne, Radiant Logic RadiantOne Intelligent Identity Data Platform,
   SailPoint IdentityIQ, Tenable.ad, Tenable.io, Tenable NNM, VMware Workspace ONE UEM and
   Access.
- E3B3 components consist of DigiCert CertCentral, F5 BIG-IP, Forescout eyeControl, Forescout eyeExtend, Forescout eyeSight, Forescout eyeSegment, Mandiant MSV, Microsoft AD, Microsoft Azure AD, Microsoft Azure AD (Conditional Access), Microsoft Azure AD Identity Governance, Microsoft Intune, Microsoft Sentinel, Microsoft Azure App Proxy, Microsoft Defender for Endpoint, Microsoft Azure AD Identity Protection, Microsoft Defender for Identity, Microsoft

- Defender for Office, Microsoft Entra Permissions Management, Microsoft Defender for Cloud
  Apps, Microsoft Purview Data Loss Prevention (DLP), Microsoft Purview Information
  Protection, Microsoft Purview Information Protection Scanner, Microsoft Intune VPN Tunnel,
  Microsoft Azure Arc, Microsoft Azure Automanage, Microsoft Intune Privilege Access
  Workstation, Microsoft Azure Virtual Desktop Windows 365, Microsoft Defender for Cloud,
  Microsoft Azure (IaaS), Microsoft Office 365 (SaaS), Palo Alto Networks NGFW, PC Matic Pro,
  Tenable.io, Tenable.ad, and Tenable NNM.
- E4B3 components consist of DigiCert CertCentral, IBM CP4S, IBM QRadar XDR, IBM Security
   Guardium Data Encryption, IBM Security MaaS360 (for both laptops and mobile devices), IBM
   Security Verify, Mandiant MSV, Palo Alto Networks GlobalProtect VPN, Tenable.ad, Tenable.io,
   Tenable NNM, and VMware infrastructure.
- E1B4 components consist of Appgate SDP Controller, Appgate SDP Gateway, Appgate SDP client,
   Appgate Portal, AWS IaaS and SaaS, DigiCert CertCentral, IBM CP4S, IBM Security QRadar XDR,
   Ivanti Neurons for UEM Platform, Mandiant MSV, Okta Identity Cloud, Okta Verify App, Radiant
   Logic RadiantOne Intelligent Identity Data Platform, SailPoint IdentityIQ, Tenable.ad, Tenable.io,
   Tenable NNM, and Zimperium MTD.
- 582 For a detailed description of the architecture of each build, see Volume B, Appendices D to M. The
- remainder of this guide describes how to implement the EIG crawl, EIG run, and SDP and

584 microsegmentation phase builds.

# 585 **1.3 Typographic Conventions**

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

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

# 587 2 Enterprise 1 Build 1 (E1B1) Product Guides

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

## 591 2.1 Okta Identity Cloud

592 The Okta Identity Cloud is a SaaS solution that provides ICAM capabilities to an enterprise. The following 593 sections describe the setup of the Okta Identity Cloud, the Okta Access Gateway, and the Okta Verify 594 application. Okta integrates with Radiant Logic for identity information, SailPoint to receive governance 595 information, and Ivanti to delegate authentication for users accessing resources using mobile devices.

## 596 2.1.1 Configuration and Integration

- 597 The purpose of this subsection is to set up NCCoE's own instance of the Okta cloud so it can integrate 598 with other ICAM tools and enable Okta to manage authentication and authorization of users accessing 599 resources. Most configurations are completed within this instance of the Okta cloud.
- Sign up for an account with Okta (okta.com) and follow steps to set up an admin account, along
   with configuring Okta Verify for the admin account. This will allow the admin to start configuring
   integrations and services.

- Set up directory integration with Radiant Logic. User identity information is pulled from Radiant
   Logic into Okta for authentication and authorization. An Okta Lightweight Directory Access
   Protocol (LDAP) agent is installed on the Radiant Logic server for integration. Note: This step
   should be completed after Radiant Logic is configured.
- 607 3. Create Groups for Okta to apply a specific set of users to specific services or applications. This
   608 allows for automation of user governance at a large scale rather than manual configuration of
   609 individual users.
- 610
   611
   611
   612
   612
   613
   614
   615
   616
   617
   618
   619
   619
   610
   610
   611
   611
   611
   612
   612
   612
   613
   614
   615
   615
   616
   617
   618
   619
   619
   610
   611
   611
   612
   612
   612
   613
   614
   615
   614
   615
   615
   616
   617
   618
   619
   619
   610
   610
   611
   612
   612
   612
   612
   614
   615
   615
   616
   617
   618
   619
   619
   610
   610
   611
   612
   611
   612
   612
   612
   612
   612
   614
   615
   615
   616
   617
   618
   619
   619
   610
   610
   610
   610
   610
   611
   612
   612
   612
   612
   614
   615
   614
   615
   614
   615
   614
   614
   614
   614
   615
   614
   614
   614
   614
   614
   614
   614
   614
   614
   614
   614
   614
   614
   614
   614
   614
   614
   614
   614
- 613 5. <u>Create a delegated authentication for Okta to be able to import users from Radiant Logic via</u>
  614 <u>LDAP.</u> This allows Okta to delegate the actual authentication to Radiant Logic. Okta does not
  615 store or know the password of the user. Note that a service account, created in the Radiant
  616 Logic Integration section 2.2.3, needs to be created and used in this configuration.
- 6. Create application integration via Security Assertion Markup Language (SAML). We have Ivanti
  618 Neurons for UEM and 2 GitLab instances in Enterprise 1. Okta Access Gateway (AG) needs to be
  619 installed in order to configure on-premises applications. The Okta AG gives the Okta Identity
  620 Cloud visibility to the resources inside the enterprise. See Section 2.1.3 for installation
  621 instructions, which include information on configuring on-premises applications.
- 622 7. Create Identity Provider integration for Ivanti Access ZSO. This will allow delegated
  623 authentication for Ivanti for mobile devices. This involves <u>creating a custom application using</u>
  624 SAML and then creating a SAML Identity Provider.
- 625 8. <u>Configure Device Trust on iOS and Android devices to create device integrations.</u>
- 626 9. <u>Create authentication policies.</u> These policies define how users will authenticate. By default, a
  627 "Catch All" policy is created when an application is created. We are creating an authentication
  628 policy that will allow Okta to trust Ivanti Access ZSO to be the delegated Identity Provider (IdP).
  629 To do this, when Okta checks that Okta Verify is a managed application on a device, it will
  630 delegate authentication to Ivanti Access ZSO.

#### 631 2.1.2 Okta Verify App

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

#### 637 2.1.3 Okta Access Gateway

638 The Okta Access Gateway (AG) is part of the Okta Identity Cloud. It can be leveraged to integrate legacy, 639 on-prem applications into the Okta Identity Cloud. Since the Okta Identity Cloud cannot communicate 640 with Enterprise 1 resources directly, the Okta AG acts as a proxy to facilitate that communication. <u>More</u>

641 information on installing and configuring the Okta AG is available online.

#### 642 2.2 Radiant Logic RadiantOne

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

#### 645 2.2.1 Installation

- 646 RadiantOne is to be installed on a Microsoft Windows 2019 server. See the RadiantOne v7.4.1
- 647 documentation from the <u>Radiant Logic website</u> for system specifications. Prerequisites are in Chapter 1
- 648 of the RadiantOne Installation Guide. Note: You need to create an account within the Radiant Logic
- 649 website in order to access the installation and configuration documentation.
- 650 Once you download and launch the executable for a Windows server installation, follow the step-by-
- 651 step instructions provided on the screen. We used default settings unless specified below. Instructions 652 can also be found in Chapter 2 of the *RadiantOne Installation Guide*.
- 653 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.
- 657 2.2.2 Configuration
- 658 2.2.2.1 Sync with an LDAP server
- Once installation is complete, log in to RadiantOne from a web browser on the Radiant Logic
   server, https://localhost:7171. Note: ensure the proper SSL certificate is on the server for
   HTTPS.
- Initial configuration is to sync up with an LDAP server. Go to Settings > Server Backend > LDAP
   Data Sources. The screenshot below shows the information created for Enterprise 1 AD. See the
   *RadiantOne Namespace Configuration Guide* Chapter 3 for details.

Edit LDAP Data Source		
Data Source Name	Data Source Type	Status 🚱
ent1-ad	AD2008 🗸	Active 🗸
Host Name	Port	
10.131.2.11	636 🗹 SSL	
Bind DN	Bind Password	
radiant@lab.nccoe.org		
Base DN	Use Kerberos profile: vds	krb5 v
DC=lab.DC=nccoe.DC=org Choose		

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

Root Naming Contexts       Type:       Image: Virtual Tree         A cn=cacherefreshlog       Naming Context:       DC=NCCOE,DC=ORG         A cn=config       Directory View:       dv=dc_nccoe_dc_org         A cn=extendedxjoin       Active:       Image: View:         A cn=registry       Image: View:       Image: View:         A cn=replicationjournal       Image: View:       Image: View:
Cn=System-registry  Cn=Sy

- 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.
- 670 6. Click on ou=ent1 on the left side and click the New Level button on the right to create a sub-ou
  671 called groups.
- 672 7. Click on ou=ent1 on the left side and click the New Level button on the right to create a sub-ou
  673 called users.
- 674 8. Once configured and saved, click on ou=users and click on Backend Mapping on the right. Select
   675 LDAP Backend. Click Next and Browse for the proper Remote Base DN. Then click OK. The
   676 screenshot is the completed configuration for the sub-ou users Proxy Backend.



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

Proxy Backend Proxy Advanced Attributes	Objects	
Selected Primary Object: <b>user</b>		🖺 Save
Primary Objects		Join Profiles
+ Add - Remove		+ New / Edit
user		Active Join Profile
		✓ user-vdhrdatahr-data-east
Display: All 🗸 🖸 Visible Only 🧳 Edit /	Attribute	Set/Unset as Hidden Origin: Primary Join Computed

#### 679 2.2.2.2 Create a namespace to bring in users

- In Directory Namespace, click the + sign. Create a naming context:
   ou=hr,ou=lab,ou=nccoe,ou=org and select Virtual Tree for the naming context type, then click
   Next.
- 683 2. Configure the Virtual Tree by choosing Create a new view (.dvx), setting the Directory View to
   684 dv=ou\_hr\_ou\_lab\_ou\_nccoe\_ou\_org and clicking OK.
- 885 3. Next, create a sub-Namespace by clicking the + New level button and entering the information
   686 depicted below.

New Level		3
Level type:	ou (organizationalUnit) 🗸	
ou	New Level DN Suffix	
	west	
objectClass:	top	
	organizationalUnit	

- 687
   687
   688
   688
   689
   689
   689
   680
   680
   680
   681
   682
   683
   684
   685
   685
   686
   686
   687
   688
   689
   689
   680
   680
   680
   680
   680
   680
   681
   682
   683
   684
   684
   685
   685
   686
   686
   687
   688
   688
   689
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
   690
- 691 5. Click on ou=east to edit properties. Scroll down to the bottom of the screen and click on the
  692 Initialize button. Then select a file with database users to import for initializing the High693 Availability Directory Access Protocol (HDAP) store. Note: We are emulating an HR database
  694 with this file.
- 695 6. Go to the **Directory Browser** tab and refresh the data by clicking the **Refresh Tree** button.
- 696 7. Go to the OU that you just configured and expand it. The new users should now be available.
- 697 8. Go to Directory Namespace and click the + button to add new naming context (in our build, we
   698 used ou=testing). This is used to map to the LDAP backend the database information that was
   699 imported.
- 700 9. Click on the OU that was created. Click **OK** and **Save**.

Configure LDAP Bac	kend	ж
A proxy to a remote LDAP remote LDAP server.	server will be created. Any requests sent to the VDS for this naming context will be routed to the	
LDAP Backend		
* Data Source:	vds   Test Connection	
Host:	Radiant1.lab.nccoe.org	
Port:	389	
* Remote Base DN:	ou=east,ou=hr,ou=lab,ou=nccoe,ou=org	•
Naming Context:	ou~testing	

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

The section is a setting in the section in the section in the section is a setting in the section in the section in the section is a setting in the section in the section in the section is a setting in the section in the section in the section is a setting in the section in the section in the section is a setting in the section in the section in the section is a setting in the section in the section in the section is a setting in the section in the section in the section is a setting in the section in the section in the section is a set of the section in the section in the section in the section is a set of the section in the s

#### 704 2.2.3 Integration

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

- 707 Hostname: radiant1.lab.nccoe.org (hostname of the Radiant Logic server)
- 708 Port: 389 (LDAP) and 636 (LDAPS)
- Also, a service account and password need to be created on Radiant Logic for each application to be
- 710 integrated. The service account is in the form of: uid=sailpointadmin,ou=globalusers,cn=config.
- Follow these steps to create each service account for SailPoint, Okta, and any other desired applications:
- 712 1. Go to Directory Browser.
- On the left, go to cn=config, then ou=globalusers underneath it. Right-click on ou=globalusers,
   click Add, then click New InetOrgPerson.
- 715 3. Fill in the necessary entries. Click **Confirm** to save the configuration.

#### 716 2.3 SailPoint IdentityIQ

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

#### 719 2.3.1 Installation and Configuration

- The steps below explain the installation of the IdentityIQ server, initial configuration to import usersfrom the Radiant Logic identity store, and configuration to manage the lifecycle of users.
- To install IdentityIQ, first identify the platform and prerequisites. For this build, we used
   Windows 2019 with Apache Tomcat 9.0 and MS SQL Server 2019 as recommended
   requirements for release 8.2. Download the installation file from the SailPoint website and
   follow the installation instructions.
- Login into IdentityIQ from a web browser (http://localhost:8080) using the default login and
   password identified in the IdentityIQ Installation Guide. Make sure to change the default
   password by following the instructions provided in the Guide.
- 729 3. <u>Configure IQService</u>. This is needed in order to set up integration with AD.
- Govern permissions by pushing employee and contractor users and groups to AD and Okta.
  Note: This step should be completed after the integration with AD and Okta is completed. Steps
to configure integration are in Sections 2.3.3 and 2.3.4. After integration with AD and Okta is
completed, navigate to the Setup drop-down menu and select Roles. Here we will create a
birthright role and access profile for employees and contractors.

- 735 736
- a. Select the **New Role** drop-down button and select **Role**. The screenshot lists the four roles that are created for this build.



737b.For the Employee Birthright Role, use the configuration shown in the next two738screenshots. Note that the Assignment Rule is where the value of employee is used to739identify the users. This will push users into AD as a birthright. Once that role is740configured, configure the corresponding contractor role the same way. Note that the741Assignment Rule should be different for the contractor based on user information in742SailPoint.

#### **Role Editor**

Indicates a required field.			
Name *	Employee Birthright Role		
Display Name			
Type *	Business v		
Owner *	a The Administrator	*	
Description	B⊥∐		English (United States) •

Match List		
IdentityIQ Items	Application Items	Additional Items
Add Identity Attribute	Select Application	Add Role Attribute
	Add Attribute Add Permission	Add Entitlement Attribute
Operation Type	Source Name Value	
Or v Attribute	IdentityIQ Type 💙 Equals 🗸 employee	
Group Selected Ungroup Selected	Delete Selected	

- 743 c. For the Employee Access Profile role, add the groups that the employees belong to. This
  744 means that these users will have access to these groups as a birthright. Perform the
  745 same for the corresponding contractor role. Note that the Entitlements should be
  746 different for the contractor based on group information in Okta and AD.
- 747 5. The next step is to synchronize users and groups. To begin, navigate to the Setup tab and select
   748 Tasks.
- 749a.To create user aggregation, select the New Task drop down button and select Account750Aggregation. The screenshot below depicts the aggregation configuration for Radiant751Logic. This allows SailPoint to sync with Radiant Logic on any updates made to users.752Repeat this step for AD and Okta accounts. Note that the Account Aggregation Options753section is where the AD and Okta applications need to be selected to create the proper754account aggregation.

Standard Properties					
*Indicates a required field.					
Name*	Ent1 HR Account Aggregation		Previous Result Action	Rename Old	×)
Description	Task template for application account scanning				
Allow Concurrency	0				
Require Signoff					
Host					
Number of Runs	3				
Average Run Time	0:00:03				
	Reset Run Statistics				
Email Task Alerts					
Email Notification	Disabled v				
Account Aggregation	Options				
Select applications to sca	n*	2		*	
			© Ent1-HR		

755	h	To create group aggregation, solect the New Tack drep down button and solect Account
/ 55	υ.	To create group aggregation, select the <b>New Task</b> drop down button and select <b>Account</b>
756		Aggregation. This allows SailPoint to sync with AD on any updates made to users in the
757		groups. Repeat this step for the Okta account. Note that the Account Group
758		Aggregation Options section is where the Okta applications need to be selected to
759		create the proper account aggregation.

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

## 772 2.3.2 Integration with Radiant Logic

LDAP Configuration

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

Use TLS	7	
Authorization Type		Simple V
User *	$ \hat{\mathbf{p}} $	uid=ailpointadmin,ou=globalusers,cn=config
Password *	7	•••••
Host *	2	radiant1.lab.nccoe.org
Port *	7	389
Page Size	7	100
Authentication Search Attributes	2	cn uid mail
		lin.

- 4. Scroll down the screen and under the Account tab, add the Search DN, which is the one createdfrom Radiant Logic.
- 781 5. Click on **Test Connection** to make sure that SailPoint is able to connect to Radiant Logic. Click
  782 Save.
- 783
  6. You can go back into the **Configuration** tab and **Schema** sub-tab. Toward the bottom of the
  784
  785
  785
  786
  786
  786
  786
  786
  786
  786
- 787 7. To complete the setup, click **Save** to finish and import users from Radiant Logic.
- 8. Go to the Setup tab and click Tasks. Once in the new tab, click on the New Task button at the top right corner to create the account aggregation for Radiant Logic.
- 9. Perform identity attribute mapping. The screenshot shows mappings specific to this build only.

#### **Identity Attributes**

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

## 791 2.3.3 Integration with AD

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

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

Ap	plication Ent1	-AD-Ent-Use	ers								
ils	Configuration Cor	relation Accourt	nts Risk Act	ivity Data Sources	Unstructured Targ	ets Rules Passwo	rd Policy				
ings	Schema Provis	ioning Policies									
tive I QSer	Directory - Direct Co rvice Configuration	nfiguration									
IQ	Service Host 🕠		IQService Po	ort 🔸	IQService User •		IQService P	assword +		Use	TLS +
10.	.151.1.20		5050		LAB\allen						0
ores	st Configuration* (*)	Global Catalog	Server 1	User •	Password	Aut	hentication Security	Use TLS 🕠	Resource Forest	Manage All Domains	Discover Doma
ores	Forest Name > Enterprise Users	Global Catalog	Server •	User 🔸	Password	Aut and Simpl	hentication Security +	Use TLS •	Resource Forest	Manage All Domains	Discover Domai Discover

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

Dor	nain	Configuration* 2							
		Forest Name 🔹	Domain DN 🔹	NetBIOS Name	User	Password	Servers	Authentication and Security	Use TLS 🔹
							10.131.2.11		
0		Enterprise Users	do=lab,do=nccoe,do=org	LAB	allen	•••••		Simple v	
									_
								Simple v	0

- 800
   4. Scroll down to the User Search Scope section and input the Search DN information. This should
   801
   be the AD domain location for your enterprise.
- 802 5. Navigate to the Schema and Provisioning Policies sub-tabs, and update information as
   803 necessary.
- 8046. Then navigate to the **Correlation** tab to configure the correlation for application and identity805 attributes between SailPoint and AD.

To Edit the currently assigned	I configuration click	Edit. If you want to create a	New Correlation config click New.
Ent1-AD-Correlation	✓ Edit	New	
Attribute Based Correl	ation		Identity Attribute
Attribute Based Correls Application Attribute	ation		Identity Attribute

- 806 7. Click **Save** to complete the configuration.
- 807 8. Go to **Setup** tab and click **Tasks**. Once in the new tab, click on the **New Task** button at the top 808 right corner to create the account aggregation for AD.

#### 809 2.3.4 Integration with Okta

- Go into the Applications tab and select Application Definition. When the screen comes up, click
   on the Add New Application button.
- Fill out the Name (e.g., "Ent1-Okta") and Owner ("The Administrator"), select Okta as the
   Application Type, and enable the Authoritative Application option.
- 814
   3. In the **Configuration** settings tab, the Okta URL and API token are needed. Note that the API token is created in Okta. Click **Save** to finish the setup.

Settings Schema Provisioning Policie	5
Okta Connection Settings	
URL *	1 https://zta-eig1.okta.com
Authentiation Type	API Token
API Token *	2
Page Size	200
Aggregation Filter Settings	
Filter Condition for Accounts	2
Filter Condition for Groups	type eq "BUILT_IN" or type eq "OKTA_GROUP"
Filter Condition for Applications	2
Test Connection	

## 816 **2.4** Ivanti Neurons for UEM

- 817 Ivanti Neurons for UEM is a unified endpoint management (UEM) solution which is used to provision
- endpoints, grant access to enterprise resources, protect data, distribute applications, and enforcemeasures as required.
- 820 2.4.1 Installation and Configuration
- 821 2.4.1.1 Install an MDM certificate for Apple devices
- 822 The Apple Push Notification service (APNs) certificate needs to be installed in Ivanti Neurons for UEM to
- communicate with Apple devices. Apple devices use an APNs certificate to learn about updates, MDMpolicies, and incoming messages.
- 825 To acquire and install the MDM certificate:
- 826 1. Open the Ivanti Neurons for UEM console and go to Admin > Apple > MDM Certificate page to
   827 download a certificate signing request (CSR).
- 2. Upload the CSR to the <u>Apple Push Certificates Portal</u> to create a new certificate.
- 829 3. Save the resulting certificate.
- 830 4. Install the certificate for the Ivanti Neurons for UEM tenant.

## 831 2.4.1.2 Configure Android Enterprise

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

834 documentation to <u>set up the integration</u>.

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

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

#### 842 2.4.1.3 Add a certificate authority

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

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

Download	Certificate				
Combined Co	ertificate Files				
Server Platform			A single pem file c	ontaining all the certs	•
Microsoft IIS 10		•			
			Download		
Download			102		
ndividual Ce	ertificate Files				
ndividual Ce ertificate	ertificate Files	Intermediate Certificate		Root Certificate	
ndividual Ce ertificate nobileironsentry.lab.m	ertificate Files	Intermediate Certificate DigiCert TLS RSA SHA2	56 2020 CA1	Root Certificate DigiCert Global Root CA	
ndividual Ce ertificate poblieironsentry.lab.ne Download	ertificate Files ccoe.org Click Text to Copy	Intermediate Certificate DigiCert TLS RSA SHA21	56 2020 CA1 Click Text to Copy	Root Certificate DigiCert Global Root CA	Click Text to Co

## 852 2.4.1.4 Configure user settings

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

#### 855 2.4.1.5 Add a policy

- Policies define requirements for devices and compliance actions (what happens if the rule is violated).To add a policy:
- 1. Go to **Policies** and click **+Add** (upper right).
- Select a policy type and complete the settings. Policy types include Compromised Devices, Data
   Protection/Encryption Disabled, MDM/Device Administration Disabled, Out of Contact, and
   Allowed Apps.
- 862 3. Select the device groups that will receive this policy.
- The following screenshots show an example of a Data Protection policy to be distributed to a custom group of devices.

#### THIRD PRELIMINARY DRAFT

Policies / Details		
Edit Policy C	Data Protection/Encryption I Choose the actions to take if a device does not have a p	Disabled passcode or encryption enabled.
2 Distribute	Policies and Compliance Setup	
	Data Protection/Encryption Disabled	
	Description	
	Checks for devices which do not have a passcode or en	cryption enabled.
	Compliance Action Monitor Block via Sentry	
	This will be applicable only for registered/managed device	в (
	Quarantine Quarantine removes access to apps and content distribute	ed to the user, and it prevents the user from downloading new apps and content. This setting also applies to AppConnect apps:
html#!/		Next →
Policies / Details		
Edit Policy Carcel	The Data Protection/Encryption Disabled	
Settings	Choose the actions to take if a device does not have a passcode or encryption e	nabled.
2 Distribute	Choose one of these options	
		*
	All Devices No Devices	Custom
	All compatible devices will have this Stage this configuration for later configuration sent to them distribution	Distribute the Policy to specific Devices/Device Foruge of Uners/User Groups
	Choose one of these Custom Distribution Option You can specify distribution of this Configuration to either Users/User Group O Users/User Groups © Devices/Device Groups	s -or- Devicet/Device Groups
	Select below to distribute this Policy	Distribution Summary
	select below to distribute this rolley	
	Users User Groups Devices Device Groups	This configuration will be sent to:
	Device         Device         Device         Composition           User         User Kame         Q	This configuration will be sent to:

## 865 2.4.1.6 Add a configuration for managed devices

- 866 Configurations are collections of settings that Ivanti Neurons for UEM sends to devices. To add a867 configuration:
- 868 1. Click Add.
- 2. Select the type of configuration. There are numerous types of configurations available, including
- 870 Privacy, Certificate, Default App Runtime Permissions, Passcode, Exchange, Wi-Fi, VPN,
- 871 iOS/macOS/Windows Restrictions, and Software Updates.

Privacy Define Privacy settings.	Certificate Adding certificates allows devices to establish trust with servers and networks.	Default App Runtime Permissions     Set defaults for application     runtime permissions (Android     enterprise)	Identity Certificate       Add certificates to allow devices       to authenticate to server and       network resources.	Passcode           Define the passcode requirements for devices.           Image: Control of the second secon
Android Work Challenge Set the work profile password.	Content Caching Create Content-Caching configuration.	S Custom Import and distribute a predefined configuration file.	Exchange Configure ActiveSync/EWS based email for devices.	Configure the Wi-Fi network that devices can connect to.
۲	mac	<ul><li>(i) (ii) (iii) (</li></ul>	() (03 (mac) ()	(a) (108) (mac) (a)
Create Per-App VPN Configuration to use with the MobileIron Tunnel app.	VPN Configure VPN that devices can use to connect to specified apps.	Office 365 Auto Account Creation Configure Office 365 applications	Controls restrictions and settings for loading User Approved Kernel Extensions.	Privacy Preference     Create Privacy Preference     configuration
(105) (mac) (11)	(*) (*) (**) (*)	mac	mac	mao
iOS Restrictions Define which features are enabled on iOS devices.	macOS Restrictions Define which features are enabled on macOS devices.	Windows Restrictions Define which features are enabled on Windows devices.	App Control Create allowed and disallowed rules for apps.	• Software Updates Create rules for Software Updates.
	mac	۲	۱	(08) mai ( <b>1</b>
() Anti-phishing Protection	AppConnect Device	G Google Account	MobileIron Threat Defense	MobileIron Threat

- 872 3. Click **Next.**
- 4. Select a distribution level for the configuration.
- 874 Here is an example of a Privacy configuration:

Name	
Privacy policy	
+ Add Description	
Configuration Set	Jp (IOS) (mac) ( 🏟 ) 貫
	<ul> <li>Collect Location Data Collect the device's last known location based on check-in.</li> <li>Disable Device Wipe Action (User Owned Devices Only) Prevent admins and users from wiping the device</li> <li>Prompt user to enable location services if WiFi/MTD configuration is pushed (Fully Managed and Work profile for Company Owned Devices)         <ul> <li>①</li> </ul> </li> </ul>
Collect App Inventory	<ul> <li>For Apps on the Device that are in the App Catalog</li> <li>For All Apps on the Device This must be selected in order to use the Allowed Apps Policy</li> </ul>
Note: Device Wipe acti	on and option to collect App Inventory for all Apps on device is not applicable for User Enrollment

#### 875 This is an example of an iOS AppConnect configuration:



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

0	Configurations	Installed Apps	Available Apps	Policies	Certificates	Sentry	Attributes	Logs	Updates	Bios	Hardware				
Configu	onfigurations anfigurations 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.														
Dist	Distributed Configurations (10) Excluded Configurations (0)														
Distribu	istributed 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.														
Pus	h Profiles Exclude Pro	files													
	NAME				TYPE				STATUS		DISTRIBUTI	ON METHOD	ACTIONS		
	250 Identity Certificate				Identity Certificate (Dynamically Generated)			Error		Assignmen		(Push) Exclude			
	250 Certificate (Tunnel)				Certificate			Installed		Assignmen		(Push) Exclude)			
	Sentry DigiCert Certificates				Identity Certificate (Dynamically Generated)			Pending Ins	tall	Assignmen	:	(Push) Exclude			
	Identity issued by MobileIron Ag	ent CA			Identity Certificate (Dynamically Generated) Inst			Installed		Assignmen		(Push) (Exclude)			
	Windows Apps@Work Identity is	sued by MobileIron Ager	nt CA		Identity Certificate (Dynamically Generated)			Installed		Assignmen		(Push) (Exclude)			
	Passcode Requirements				Passcode				Installed		Assignment		(Push) Exclude)		
	DigiCert Global Root CA				Certificate				Installed		Assignment		(Push) Exclude)		
	Privacy				Privacy				Active (?)		Assignment		(Push) (Exclude)		
	MobileIron Agent CA Certificate				Certificate				Installed		Assignmen		(Push) (Exclude)		
0	DigiCert TLS RSA SHA256 2020 C	AI			Certificate				Installed		Assignmen		(Push) Exclude		
									_						

## 877 2.4.2 Integration with Ivanti Connector

- 878 Ivanti Connector provides access from Ivanti Neurons for UEM to corporate resources, such as an LDAP
   879 server. For the latest Connector installation instructions, select the appropriate version of the <u>Cloud</u>
   880 Connector Guide.
- Once the Ivanti Connector has been set up and configured, navigate to the Ivanti Neurons for
   UEM console.
- 2. Connect to an LDAP Server to import users and groups. Navigate to Admin > Infrastructure >
   LDAP > Add Server. Complete configurations and save. Users can now be imported from the
   LDAP server.
- 886 2.4.3 Integration with Okta
- 887 2.4.3.1 *IdP setup*
- 888 1. Go to Admin > Infrastructure > Identity > Add IdP.
- 889 2. Generate a key for uploading to Okta IdP.
- 3. Log in to Okta IdP. Search IdP for the **MobileIron Cloud App** and add it to the IdP account.
- 891 4. Configure the MobileIron Cloud App on the IdP by pasting the above-generated key and the892 host information.
- 5. Export metadata from Okta to the Ivanti Neurons for UEM console.
- 894 6. In Admin > Infrastructure > Identity > Add IdP, select Choose File to import the downloaded
   895 metadata file to Ivanti Neurons for UEM and complete the setup.
- 896 7. When an IdP is added, user authentication automatically switches from LDAP to IdP.
- 897 2.4.3.2 Okta Verify app configuration preparation
- 1. In the Okta Admin console, navigate to **Security > Device Integrations** and click **Add Platform**.
- 899 2. Select platform and click Next.
- Secret Key for later usage and enter Device Management Provider and Enrollment Link
   settings.
- 902 4. Repeat for any other device platforms.
- 903 2.4.3.3 Okta Verify app configuration Android
- 904 1. In the Ivanti Neurons for UEM console, navigate to **Apps > App Catalog.** Click **Add.**

- 905 2. Select the Google Play Store and search for **Okta Verify.** Select the official **Okta Verify** app.
- Solution
   Solution
   Continue through the wizard until you reach the App Configurations page. Click the + button in the Managed Configurations for Android section.
- Add desired settings. Under Managed Configurations, add the Org URL and Management Hint
   from the Okta Admin console. The Management hint will be the Secret Key you saved from the
   Okta console during preparation.
- 911 5. Click **Next**, then click **Done**.
- 912 2.4.3.4 Okta Verify app configuration iOS
- 913 1. In the Ivanti Neurons for UEM console, navigate to Apps > App Catalog. Click Add.
- 914 2. Select the iOS Store and search for **Okta Verify**. Select the official **Okta Verify** app.
- 915 3. Continue through the wizard until you reach the App Configurations page. Click the + button in
  916 the Apple Managed App Configuration section.
- 917 4. Add desired settings. Under Apple Managed App Settings, click Add and add two items.
- 918a. For the first item, the key will be **domainName**, the value will be your Org URL, and the919type will be STRING.
- b. For the second item, the key will be managementHint, the value will be the Secret Key
  you saved from the Okta console during preparation, and the type will be STRING.
- 922 5. Click **Next**, then click **Done**.
- 923 2.4.4 Integration with QRadar
- 924 2.4.4.1 Ivanti log transfer setup
- Set up an SSH server to host log files. Create a user account that can be used to host/transfer
   Ivanti Log Files.
- 927 2. In the Ivanti Neurons for UEM console, navigate to Admin > Infrastructure > Audit Trails.
- 928 3. Turn on Audit Trails Export and Device Check-in Trails.
- 929 4. Under Export Format, select **CEF** (Common Event Format).
- 930 5. Enter the IP address or hostname for the SSH server you set up previously.
- 931 6. Enter the username and password for the user you set up previously.
- 932 7. Enter the server path for where you would like the Ivanti log files to be stored on the SSH server.

933 934	8.	Click <b>Test Connection and Save</b> . Ivanti log files will now be transferred to the SSH server on a regular basis.
935	2.4.4.	2 QRadar setup
936	1.	In the QRadar console, navigate to Admin > Extensions Management. Click Add.
937	2.	Select the Ivanti extension file provided by IBM. Click Add.
938	3.	Continue through the wizard until you completed the extension installation.
939	4.	In the QRadar console, navigate to Admin > Log Sources. Click +New Log Source.
940 941	5.	In the search box, type <b>Ivanti</b> . Make sure <b>Ivanti</b> is selected in the menu and click <b>Step 2: Select</b> <b>Protocol Type</b> .
942 943	6.	In the search box, type Log File. Make sure Log File is selected in the menu and click Step 3: Configure Log Source Parameters.
944 945	7.	Enter a name for the log source and turn off <b>Coalescing Events</b> . Click <b>Step 4: Configure Protocol Parameters</b> . The settings are as follows:
946		a. Log Source Identifier: MobileIron Cloud
947		b. Service Type: SFTP
948		c. Remote IP or Hostname: <log previously="" server="" set="" up="" you=""></log>
949		d. Remote port: 22
950 951		<ul> <li>Remote User/Password: <credentials created="" earlier,="" file<br="" if="" key="" not="" using="">authentication&gt;</credentials></li> </ul>
952		f. SSH Key File: < Credentials created earlier, if not using password authentication>
953		g. Remote directory: Directory where Ivanti logs are being stored
954		h. Recursive: On
955		i. FTP File Type Pattern (Regex for Ivanti log files): ^.*\.(zip ZIP)\$
956		j. Processor: ZIP
957		k. All other settings can be left as default
958	8.	Click Step 5: Test Protocol Parameters. Run the tests and ensure the configuration is valid.
959	9.	From the QRadar console, navigate to the <b>Admin</b> tab. Click <b>Deploy Changes</b> .

## 960 2.5 Ivanti Sentry

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

## 964 2.5.1 Installation and Configuration

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

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

## 972 2.5.2 Ivanti Tunnel Configuration and Deployment

- 973 Ivanti Tunnel is an application that connects a mobile device to the Ivanti Sentry. The process to deploy
  974 this app is similar to the deployment of the Okta Verify app in Section 2.1.2.
- 975 1. On the **App Configurations** page for the Tunnel app, create a Managed Configuration.
- 976 2. Set the **Tunnel Profile Mode** to **MobileIron Sentry + Access**.
- 977 3. Set the **Sentry Server** to the Sentry instance you created previously.
- 978 4. Set the **SentryService** to the name of the IP Tunnel defined on the Sentry.
- 979 5. Set the **ClientCertAlias** to the Sentry certificates you defined during Sentry configuration.
- 980 6. Set any other options as needed.
- 981 7. Save the Managed Configuration and deploy to devices as needed.

#### 982 2.6 Ivanti Access ZSO

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

## 986 2.6.1 Integration with Ivanti Neurons for UEM

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

Admin / Infrastructure / Access										
MobileIron Access Show Description										
STATUS	ACCESS ADMIN URL	USERNAME	LAST SYNCED	ACTIONS						
$\oslash$	https://access-na1.mobileiron.com/	@nist.gov	3/08/22 2:07 pm	$\odot \ominus$						

#### 997 2.6.2 Integration with Okta

- In the Okta Admin console, navigate to Security > API and generate an API token. Save this
   token for use in Access.
- 1000 2. In the Ivanti Access ZSO console, navigate to **Profile > Federation.**
- 1001 3. Select Add Pair > Delegated IDP and choose Okta.
- 1002 4. Enter the Okta Domain URL and the Okta API Token you generated in Step 1. Click Verify.
- 1003 5. Once the verification is complete, select the routing rules you'd like configured and click **Next**.
- 1004 6. Verify the Signing Certificate settings and Encryption Certificate settings are correct and click
   1005 Next.
- 1006 7. Choose the desired **Unmanaged Device Authentication** setting and click **Done**.
- You will see Okta in the Delegated IDP section. Okta will route authentication requests based on
   your settings.

## **2.7 Zimperium Mobile Threat Defense (MTD)**

Zimperium MTD 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.

- 1013 2.7.1 Installation, Configuration, and Integration
- 1014 2.7.1.1 Create an API user
- 1015 To configure a Zimperium MTD console to work with Ivanti Neurons for UEM, an API user needs to be 1016 created and assigned a few roles.
- 1017 1. In the Ivanti Neurons for UEM admin console, select **Users.**
- 1018 2. Click + Add > API user. The Add API User dialog page opens.
- Enter the following details: Username, Email, First Name, Last Name, Display Name, and
   Password.
- 1021 4. Confirm the password.
- 1022 5. Deselect the **Cisco ISE Operations** option.
- 1023 6. Click **Done.**
- 1024 2.7.1.2 Assign roles to the API user
- 1025 1. From the admin console, go to Users.
- 1026 2. Select the new API user created previously.
- 1027 3. Click Actions.
- 1028 4. From the User details page, select Assign Roles.
- 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.
- 1032 2.7.1.3 Add an MDM server to the Zimperium console
- 1033 1. Log in to the Zimperium MTD console.
- 1034 2. Navigate to Manage > Integrations > Add MDM.
- 1035 3. Select **Cloud** to add it to the MTD console as an MDM server.

1036 1037	4.	Enter the following required information: URL, Username/Password, MDM Name, and Background Sync.
1038	5.	Click Finish.
1039	2.7.1.4	4 Activate MTD on Ivanti Neurons for UEM
1040	1.	From the Ivanti Neurons for UEM admin console, go to <b>Configurations.</b>
1041	2.	Click <b>+Add.</b>
1042	3.	Click Mobile Threat Defense Activation.
1043	4.	In the Create Mobile Threat Defense Configuration page, enter a name for the configuration.
1044	5.	In the Configuration Setup section, select the vendor <b>Zimperium</b> .
1045	6.	In the License Key field, enter a unique encrypted Mobile Threat Defense activation code.
1046	7.	In the Wake up Intervals (mins) field, set a time.
1047	8.	Click Next.
1048	9.	Select the Enable this configuration option.
1049	10.	Select All Devices.
1050	11.	Click <b>Done.</b>
1051	2.7.1.5	5 Add custom attributes in Ivanti Neurons for UEM
1052	Custom	device attributes will be applied to both Android and iOS devices based on threat severity.
1053 1054	1.	To create custom attributes, in the Ivanti Neurons for UEM admin console go to Admin > System > Attributes. Enter each attribute name in lower case.
1055	2.	Create the custom attribute mtdnotify for Low or Normal severity threats:
1056		a. Click Add New. The Attribute Name and Attribute Type fields are displayed.
1057		b. Select <b>Device</b> as the attribute type.
1058		c. Name the custom attribute <b>mtdnotify.</b>
1059		d. Click <b>Save</b> to monitor and notify.
1060	3.	Create the custom attribute mtdblock for Elevated or Critical severity threats:
1061		a. Click Add New.

1062	b. Select <b>Device</b> as the attribute type.
1063	c. Name the custom attribute <b>mtdblock.</b>
1064	d. Click <b>Save</b> to monitor and notify.
1065	4. Create the custom attribute <b>mtdquarantine</b> for <b>Elevated</b> or <b>Critical</b> severity threats:
1066	a. Click Add New.
1067	b. Select <b>Device</b> as the attribute type.
1068	c. Name the custom attribute <b>mtdquarantine.</b>
1069	d. Click <b>Save</b> to monitor, notify, and quarantine.
1070 1071	<ol> <li>Create the custom attribute mtdtiered4hours for Low, Normal, Elevated, or Critical severity threats:</li> </ol>
1072	a. Click Add New.
1073	b. Select <b>Device</b> as the attribute type.
1074	c. Name the custom attribute <b>mtdtiered4hours.</b>
1075 1076	d. Click <b>Save</b> to monitor and notify, wait for four hours, block, wait for another four hours, and quarantine.
1077	2.7.1.6 Create compliance policy
1078	Create compliance actions using custom policies based on the MTD custom attributes created above.
1079	1. In Ivanti Neurons for UEM admin console, go to <b>Policies.</b>
1080	2. Click <b>+ Add.</b>
1081	3. Select Custom Policy.
1082	4. Enter <b>mtdnotify</b> as the policy name.
1083	5. Under Conditions, select Custom Device Attribute.
1084	6. Select <b>mtdnotify</b> from the drop-down box and set the condition <b>is equal to</b> 1.
1085	7. Under Choose Actions, select Monitor and Send Email and Push Notification.
1086	8. Under Email Message fields, enter the subject and body text.
1087	9. Under <b>Push Notification,</b> enter message text.

- 1088 10. Click **Yes, Next,** and **Done.**
- 1089 11. Repeat this procedure to add the following policies: mtdblock, mtdquarantine,
   1090 mtdtiered4hours.
- 1091 12. Add other policies if needed.

NAME	ТҮРЕ	DISTRIBUTION	ACTIVE VIOLATIONS -	COMPLIANCE ACTION
Data Protection/Encryption Disabled	E 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	S Custom Policy	6	0	Monitor, Send Push Notification, Block, Send Push Notification
MTD-Notify	Custom Policy	б	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	б	1	Monitor only
Test Block	S Custom Policy	2	2	Monitor only

# 1092 2.7.1.7 Create device groups and match with custom policies and custom device 1093 attributes created above

- 1094 1. In Ivanti Neurons for UEM admin console, go to **Devices > Device Groups.**
- 1095 2. Click **+ Add.**
- 1096 3. Enter **mtdNotify** as the device group name.
- 1097 4. Under Dynamically Managed groups, select **Custom Device Attribute.**
- 1098 5. Select **mtdnotify** from the drop-down box and set the condition **is equal to** 1.
- 1099 6. Click Save.
- Repeat this procedure to add the following groups: mtdBlock, mtdQuarantine,
   mtdTiered4hours.
- 1102 2.7.1.8 Configure Zimperium MTD management console
- 1103 Set up, configure, and use the MTD console for supported MTD activities. When configuring policies in
- 1104 the Zimperium admin console, use the available MDM actions and mitigation actions.

) Enable	Type 👘	Severity	Thre	at 1	Ŧ	Set User Alert	Device Action	MDM Action	Mitigation Action	Notify M
	Singular	Elevated~	0	Abnormal Process Activity		0 ¢	0	Select an Opt*	Unavailable	
	Singular	Elevated ~	0	Always-on VPN App Set		• •	¢	Q.	Select an Opt	
	Singular	Elevated ~	0	Android Debug Bridge (ADB) Apps Not Verified		•	¢	Remove	Select an Opt*	-
	Singular	Low 👻	0	Android Device - Compatibility Not Tested By Goo	ogle	0 0	0	MTD-Notify	Select an Opt *	-
53	Singular	Critical 🛩	0	Android Device - Possible Tampering		0 ¢	¢	MTD-Block MTD-Quarantine	Select an Opt *	
2	Singular	Elevated ~	0	App Debug Enabled		0 0	٥	MTD-Tiered4hours	Unavailable	
	Singular	Low 💌	0	App Pending Activation		•	٥	Select an Opt	Select an Opt *	80
53	Singular	Critical ~	0	App Tampering		•	0	Select an Opt	Unavailable	-
	Singular		0	ARP Scan		0 ¢	0	Select an Opt.	Unavailable	-
2	Singular	Elevated~	0	BlueBorne Vulnerability		•	0	Select an Opt	Select an Opt	-
	Singular		0	Captive Portal			0	Select an Ont	Colent on Out	

## 1105 2.8 IBM Cloud Pak for Security

1106 IBM Cloud Pak for Security platform enables the integration of existing security tools and provides1107 understanding and management of threats in the environment.

- 11081. Deploy an OpenShift cluster. OpenShift needs to be in place before Cloud Pak for Security can be1109installed.
- 1110 2. Install Cloud Pak for Security.
- Configure LDAP authentication so Cloud Pak for Security can leverage an existing LDAP directory
   server for authentication.
- 1113 Once those steps are complete, open a web browser and navigate to the DNS name for Cloud Pak for
- 1114 Security. Additional documentation can be found at <u>Cloud Pak for Security Documentation</u>.

## 1115 2.9 IBM Security QRadar XDR

- 1116 IBM Security QRadar platform provides various security capabilities including threat detection and
- response, security information and event management (SIEM), and security orchestration, automation,and response (SOAR).
- 1119 Install and configure QRadar following IBM's QRadar Installation and Configuration Guide.
- 1120 Once that is complete, open a web browser and navigate to the QRadar server web interface by using its
- 1121 IP address or DNS name.

#### 1122 **2.10 Tenable.io**

1123 Tenable.io is a cloud-based platform that is used in this build to provide network discovery, vulnerability, 1124 and scanning capabilities for enterprise components.

1125 2.10.1 Installation and Configuration

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

- 1129 *2.10.1.1 Deploy an agent*
- In Tenable.io, click the hamburger menu (Ξ) in the top left corner and navigate to Settings >
   Sensors > Nessus Agents.
- 1132 2. Click Add Nessus Agent and save the Linking Key.
- 11333. On the target endpoint, download the agent from <a href="https://downloads.tenable.com">https://downloads.tenable.com</a>. When the1134download completes, run the executable file.
- In the setup window, fill in the key from step 2, the server (in our case, cloud.tenable.com:443),
   and the agent groups that this agent will be part of (in our case, Default). Click Next.
- 1137 5. Click **Install** and approve the request if User Account Control (UAC) comes up.
- 6. When installation completes, updates will continue running in the background. The update andconnection process may take some time. The endpoint will then be shown in the cloud tenant.

Linke	Agents Age	ent Groups Freez	e Windows Settings	Networks						
Filt	ers v S	earch	م	14 Agents						
	14 Items							1 to 14	of 14 🛩 💠 🤄 Page 1	of1 > >
	NAME	STATUS	IP ADDRESS	PLATFORM (DI	VERSION	GROUPS	NETWORK	LAST PLUGIN U	LAST SCANN ↑≡	ACTIONS
	IDENTITYIQ	<ul> <li>Online</li> </ul>	10.176.21.20	Windows (win	10.1.3	Default	Default	N/A	February 3 at	:
	MAIL	<ul> <li>Online</li> </ul>	10.176.23.93	Windows (win	10.1.3	Default	Default	N/A	February 3 at	:
	RADIANT2	<ul> <li>Online</li> </ul>	10.176.21.32	Windows (win	10.1.3	Default	Default	N/A	February 3 at	:
	RADIUS	<ul> <li>Online</li> </ul>	10.176.22.20	Windows (win	10.1.3	Default	Default	N/A	February 3 at	:

#### 1140 2.10.1.2 Deploy a scanner

- 1141 1. In Tenable.io, navigate to **Settings > Sensors > Cloud Scanners.**
- 1142 2. Click Add Nessus Scanner and save the Linking Key.
- 1143 3. Download the Nessus Scanner .ova file from <u>https://downloads.tenable.com</u>.
- 1144 4. Deploy the .ova file in your virtual environment.

- 5. Once the scanner is running, navigate to the IP address shown in the console in a web browser.
- 1146 6. Login with the default username *wizard* and default password *admin*.
- 1147 7. Enter new administrator credentials and click **Create Account.**
- 1148 8. Click **Finish Setup** and authenticate with the new administrator credentials.
- 1149 9. On the left-side navigation pane, click **Nessus.**
- 1150 10. Click the URL shown in the *Nessus Installation Info* pane.
- 1151 11. Click the radio button next to *Managed Scanner* and click **Continue**.
- 1152 12. Enter the Linking Key from step 2 and click **Continue.**
- 1153 13. Enter credentials for a new administrator account and click **Submit.**
- 1154 14. The scanner will initialize and be visible on tenable.io. Scans can now be scheduled.
- 1155 2.10.2 Integration with QRadar
- 1156 For Tenable.io and QRadar integration, follow the <u>Tenable and IBM QRadar SIEM Integration Guide</u>.

#### 1157 **2.11 Tenable.ad**

- 1158 Tenable.ad provides AD monitoring to detect attacks and identify vulnerabilities. In this build,
- 1159 Tenable.ad is integrated with the on-premises AD installation and configured to forward alerts to the1160 IBM QRadar SIEM.
- 1161 For Tenable.ad installation and configuration, follow the <u>Tenable.ad On-Premise Installation Guide.</u>
- 1162 For Tenable.ad and QRadar integration, follow the <u>Tenable and IBM QRadar SIEM Integration Guide</u>.

#### 1163 **2.12 Tenable NNM**

- Tenable Nessus Network Monitoring (NNM) monitors network traffic at the packet level to provide
  visibility into both server and client-side vulnerabilities. In this build, NNM was set to Asset Discovery
  mode and linked to Tenable.io in order to provide visibility into all network actors.
- 1167 For Tenable.ad installation and configuration, follow the <u>Tenable NNM Documentation</u>.

#### 1168 2.12.1 Deploy a Tenable NNM instance

- 1169 1. In Tenable.io, navigate to **Settings > Sensors > Nessus Network Monitors.**
- 1170 2. Click Add Nessus Network Monitor and save the Linking Key.

- 1171 3. Download the NNM .ova file from <u>https://downloads.tenable.com</u>.
- 1172 4. Deploy the .ova file in your virtual environment.
- 5. Once the NNM instance is running, navigate to the IP address shown in the console in a webbrowser on port 8835.
- 1175 6. Enter credentials for a new administrator account and click **Submit.**
- 1176 7. Enter the Linking Key from step 2 and click **Continue.**
- 1177 8. The NNM instance will initialize and be visible on Tenable.io. Additional NNM configuration can1178 now occur if needed.

## 1179 2.13 Mandiant Security Validation (MSV)

1180 Mandiant Security Validation (MSV) allows organizations to continuously validate the effectiveness of 1181 their cybersecurity controls by running actions that may conflict with the organization's policy and 1182 determining if those actions are detected and/or blocked. In this build, MSV is configured to regularly

- 1183 test the build's zero trust policies and report on the results.
- 1184 2.13.1 MSV Director Installation/Configuration
- 11851. Download the MSV Director software from the Mandiant web portal and deploy it in a virtual1186environment.
- 1187 2. Log into the MSV command line interface using credentials provided by Mandiant.
- 1188 3. Run the command sudo vsetnet to apply network configuration.
- Run the command sudo vsetdb --password new\_password to set a new password for the
   Director database.
- 1191 5. Use a web browser to access the MSV Director web interface at https://Director IP/.
- 1192 6. Sign into the web interface using credentials provided by Mandiant.
- 11937. Review and accept the End User Licensing Agreement, and apply the license provide by1194Mandiant.
- 1195 8. Configure the DNS settings by navigating to **Settings > Director Settings > DNS Servers.**
- 1196 9. Configure the NTP settings by navigating to **Settings > Director Settings > NTP Servers.**
- 10. Add Security Zones corresponding with the enterprise's network segments by navigating to
   Environment > Security Zones.

- 1199 11. Download security content from the Mandiant web portal.
- 1200 12. Navigate to Settings > Director Settings > Content.
- 1201 13. Select **Import**, browse to the downloaded security content, and select the content files.
- 1202 14. Click **Upload Import** and upload the files into the MSV Director web interface.
- 1203 15. Once the upload is complete, click **Apply Import** to import the content files into MSV.

#### 1204 2.13.2 MSV Network Actor Installation/Configuration

- 1205 1. Download the MSV Network Actor software from the Mandiant web portal and deploy it in a 1206 virtual environment.
- 1207 2. Log into the MSV command line interface using credentials provided by Mandiant.
- 1208 3. Run the command sudo vsetnet to apply network configuration.
- 1209 4. In the MSV Director web interface, navigate to **Environment > Actors.**
- 1210 5. Click **Add Network Actors** and fill out the new **Actor** form.
- 1211 6. Identify the Actor you just created in the **Pending Actors** table, expand the **Actions** menu, and
   1212 click **Connect** to initiate a Director-to-Actor registration.
- 1213 7. Enter the Actor's fully qualified domain name (FQDN) or IP address.

#### 1214 2.13.3 MSV Endpoint Actor Installation/Configuration

- 1215 1. Deploy an endpoint machine running Windows, macOS, or Linux.
- In the MSV Director web interface, navigate to Library > Actor Installer Files and download the
   relevant installer onto the endpoint.
- 1218 3. Navigate to **Environment > Actors,** click **Add Endpoint Actors,** and fill out the new Actor form.
- 1219 4. Execute the Actor installer on the endpoint and proceed through the install process.
- 1220 5. At the end of the install process, identify the actor you just created in the **Pending Actors** table 1221 and enter the value from the **Code** field into the Actor configuration field.

P	Pending Actors										
	Name	Desc	Security Zone	Code	Туре	Status	Actions				
	Test		Internet	3N9J-70YY-A3CZ	Endpoint	Unregistered	i				

1222 6. The endpoint will register itself with the MSV Director, and setup will be complete.

#### 1223 2.13.4 MSV Evaluation Configuration

- 12241. Once the MSV Director and Actors have been configured, evaluations can be created to test1225security controls and policies. In the MSV Director web interface, navigate to Library > Actions.
- Find the action(s) you would like to use for the evaluation and select the +Queue button to add
   the action to the Queue. Repeat this process until you have added all needed actions to the
   Queue.

View Action ×							
÷	► + Monitor + Queue 2						
	VID: A100-056 v8.0.0 Created: 2018-05-23 11:28:54 UTC Modified: 2022-05-19 20:40:41 UT	rc	MANDIANT				
	Name: Benign Remote Desktop Protocol Traffic						
	Description: This Action demonstrates Remote Desktop Protocol (RDP) traffic between two hosts. While RDP is not unusual, the traffic contained in this Action can be used to evaluate segmentation controls or demonstrate lateral movement activity.						
	Tags: ● ATT&CK:Lateral Movement CAPEC:555 CWE:522						
	MITRE ATT&CK: •						
	Name	ID	Actions				
	Remote Desktop Protocol	T1021.001	0				
	Run As Tags: 🔿 None						
	Source/Destination Tags: ↔						
				Close			

- 3. After actions have been added to the Queue, click the **Queue** button in the upper right side ofthe web interface.
- Select each of the actions in the Unassigned section and drag them to the Current Actions
   section.
- 1233 5. Scroll up to the top of the page and click the **Save** button.

- 1234 6. Under the **Test Type** dropdown, choose **Evaluation**.
- 1235 7. Enter a name and a description, then select the **Save** button to save the evaluation.
- 1236 8. Your new evaluation can be found by navigating to Library > Evaluations and filtering on User
   1237 Created.

#### 1238 2.13.5 MSV Evaluation Execution

- Navigate to Library > Evaluations and select the evaluation you'd like to run. Click the Run
   button.
- 1241 2. From the Evaluation screen, press the **Run Evaluation** button.



- 1242 3. Select the **Source Actor** and **Destination Actor** from the dropdown menus. Click **Run Now.**
- 1243 4. The evaluation will run, providing results once the actions have been attempted/completed.

STATUS PROGR Completed Compl		ss ted Group	SUBMITTED AT 2022-05-27 17:16:02 UTC	SUBMI Defaul	SUBMITTED BY Default Admin	
EVALUATION S200-017: Test Evaluation		SECURITY TECHNOLOGIES No Security Technologies detected				
STATUS BY ACTION		SUMMARY OF RESULTS		STAGE OF ATTAC	к	
		o		Recon		
		Prevented		Deliver		
		Alerted Missed		Exploit		
				Execute		
				Control		
			Act on Target			
<b>F</b> ail: 100%					0	5

## 1244 2.14 DigiCert CertCentral

1245 CertCentral simplifies digital trust and automates certificate management by consolidating tasks for
 1246 issuing, installing, inspecting, remediating, and renewing TLS/SSL certificates in one place. In this build,
 1247 CertCentral provided TLS/SSL certificates to any system needing those services.

1248 For the latest CertCentral setup and usage instructions, see <u>https://docs.digicert.com/get-started/</u>.

## 1249 2.14.1 Requesting a certificate

- Generate a Certificate Signing Request. This can be done with OpenSSL or DigiCert's Certificate
   Utility. Save the private key for later use.
- In the DigiCert CertCentral dashboard, navigate to Certificates > Requests and click Request a
   Certificate. Select the certificate type.
- 1254 3. Upload or paste the Certificate Signing Request in the provided field.
- 1255 4. Select the coverage length, and add any other additional options as needed.
- 1256 5. Click **Submit Request**.

## 1257 2.14.2 Obtaining and implementing a certificate

- In the DigiCert CertCentral dashboard, navigate to Certificates > Orders and select the request
   that you previously created.
- 1260 2. Click **Download certificate as** and select **More Options...**
- 12613. You will be presented with a list of certificate format options. Select the option/format that best1262pertains to the platform you will be using the certificate on. Click **Download**.
- 4. Obtain the private key that was originally generated with your Certificate Signing Request. If
  using DigiCert's Certificate Utility, this can be found using the Export function.
- 12655. The certificate and private key can now be imported/installed and used on the intended1266platform.

# 1267 **3 Enterprise 2 Build 1 (E2B1) Product Guides**

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

## 1271 3.1 Ping Identity PingOne

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

## 1276 3.1.1 Configuration: PingOne and PingFederate

- 12771. PingOne setup: From your web browser, type pingone.com and click the "Try Ping" at the top1278right of the screen. Follow the instructions to sign up.
- Once the PingOne environment is set up and functioning, scroll down the screen and click on the
   PingFederate service. A new browser tab will open. Most of the configuration will be performed
   on PingFederate for this build.
- 12823. Create an IDP adaptor. This configuration should include some required values like mail and1283group membership (these will be mapped in steps below to the policy contract) and this adaptor1284is used as the first authentication factor and will be applied in the policy in the next step.

1285 1286 1287	4.	<u>Create a policy</u> contract as a list to map values to the connection(s). The policy contract will use a policy to fulfill the mappings from sources (such as LDAP or Third-Party Identity Provider using a Federated Hub).		
1288 1289 1290	5.	Create an authentication policy that will be used to dictate application authentication. For our policies, we are using user ID and password for the first authentication factor (step 3 above) and Duo as the second authentication factor (Integration with Cisco Duo section).		
1291	6.	Create a policy contract to connect that uses the above policy.		
1292 1293 1294	7.	Configure <u>SAML application</u> integrations. Note that all applications are different. For our resources (applications), certain SAML formats and attributes are used. Follow the linked documentation above to configure the specific setup of your own application.		
1295 1296 1297 1298	8.	For this build, we developed policies that allow employees to access all resources (resource 1 and resource 2) and contractors to access resource 2 only. In order to do that, we leveraged the "memberof" attribute from Radiant Logic to identify employees and contractors. Once this information is identified, refer to:		
1299		a. <u>Authentication Policies</u> to define the attribute mappings using this information		
1300 1301		b. <u>SAML applications</u> to configure issuance criteria to information retrieved from Radiant Logic		
_				

- 1302 3.1.2 Integration with Radiant Logic
- 1303 1. For this build we installed a PingOne Gateway, which is "on-premise software that allows 1304 PingOne to communicate with other systems like LDAP servers," to communicate with 1305 RadiantOne. The PingOne Gateway was installed on a Windows Server on the same subnet as 1306 the RadiantOne server. We used the PingOne Gateway due to restrictions of multiple firewalls 1307 and NAT rules within our lab environments (some are not under our control) from allowing 1308 PingOne from the Internet to reach RadiantOne in Enterprise 2. In many environments, the LDAP gateway is not needed if NAT is not used, and opening the proper TCP/UDP ports on the 1309 enterprise firewalls will allow communication between PingOne and the on-prem resource. 1310 Note: Prerequisites and instructions for installing the gateway are available under 1311 **Connections/Gateway** in the PingOne console. 1312
- Once the Gateway is configured, click the Add button within the Connections/Gateway screen.
   Follow instructions on the screen to complete the integration with Radiant Logic. Note: A service account and other information from Radiant Logic is needed for the setup. Ensure this service account is created within Radiant Logic prior to configuring the PingOne Gateway.

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

#### 1319 3.1.3 Integration with Cisco Duo

- 1320 Make sure that configuration from Cisco Duo is completed before performing the integration.
- 1321 For IDP application integration, from the Authentication tab, select IDP Adaptors, and click Create New
- **Instance** to create the integration with Cisco Duo to use Duo MFA as the second authentication factor.
   Specific API configuration information that was created from Cisco Duo is needed here to complete the
- 1324 setup.
- 1325 Note: For this build, we are using Duo, although Ping Identity has its own MFA.
- 1326 **3.2** Radiant Logic RadiantOne
- 1327 3.2.1 Installation and Configuration
- 1328 Refer to Section <u>2.2.1</u>.
- 1329 3.2.2 Configuration
- 1330 Refer to Section <u>2.2.2</u>.
- 1331 3.2.3 Integration
- 1332 Refer to Section 2.2.3 for integration with SailPoint.
- 1333 For integration with Ping Identity, a service account was created in RadiantOne. This service account,
- along with various credential information is used by PingFederate to communicate with RadiantOne toauthenticate users. The communication between RadiantOne and PingFederate is through the Ping
- 1336 Gateway, which was installed on the same subnet as RadiantOne.
- 1337 3.3 SailPoint IdentityIQ
- 1338 3.3.1 Installation and Configuration
- 1339 Refer to Section <u>2.3.1</u>.
- 1340 3.3.2 Integration with Radiant Logic
- 1341 Refer to Section <u>2.3.2</u>.

#### 1342 3.3.3 Integration with AD

- 1343 Refer to Section <u>2.3.3</u>.
- 1344 3.3.4 Integration with Ping Identity
- There is no integration with Ping Identity. For this build, SailPoint provides AD user information and Duopulls from AD.

#### 1347 **3.4 Cisco Duo**

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

## 1351 3.4.1 Configuration

- 1352 Sign up with Cisco Duo to create a Duo instance. Once you have admin access, create policies and1353 integration with AD and Ping Identity.
- <u>Create a policy</u> to enable MFA for users. Navigate to **Policy** and click **Edit Global Policy**. In the Global
   Policy, there are many sub-policies that can be applied. For this build, we enabled the following:
- 1356 New User policy: prompt any user without the Duo app to enroll
- 1357 Authentication policy: require two-factor
- 1358 Authentication methods: Duo Mobile app (Duo Push)
- 1359Device Health application: enable macOS and Windows (note: these are the only operating<br/>systems that are capable of device health monitoring when installed with Cisco Duo.)
- Custom Policies: create a policy to monitor device health if the authentication request comes from PingFederate. Self-enrollment is enabled so users will be prompted to install a Duo client on the end device for health monitoring. For this build, users will not be given access to a resource if their macOS or Windows firewall is turned off. There are other health checks available.

#### 1366 3.4.2 Integration

- 1367 For integration with PingFederate, navigate to **Applications** and <u>click **Protect an application**</u>. Follow the
- instructions to complete the configuration. Note the three pieces of information provided: Client ID,Client secret, and API hostname. This information will be used to configure the integration within
- 1370 PingFederate to communicate with Duo.

- 1371 For integration with Microsoft Active Directory, navigate to Users and click on Directory Sync. Follow
- 1372 the instructions to configure the AD integration. A <u>Duo Authentication Proxy</u> is needed for this build
- 1373 since the Enterprise 2 AD is not visible to the Internet.

## **3.5 Palo Alto Networks Next Generation Firewall**

- 1375 In this build, a virtualized Palo Alto Networks Next Generation Firewall (NGFW) was deployed on-
- 1376 premises as a security and access control device. The firewall provides zone-based network filtering for
- 1377 both inbound and outbound traffic, including remote access VPNs using the GlobalProtect clients. For
- 1378 GlobalProtect VPN access installation instructions, visit:
- 1379 <u>https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFbCAK</u>
- 1380 3.6 IBM Security QRadar XDR
- 1381 For installation, configuration, and integration instructions, refer to <u>Section 2.9</u>.
- 1382 **3.7 Tenable.io**
- 1383 For installation, configuration, and integration instructions, refer to Section <u>2.10</u>.
- 1384 **3.8 Tenable.ad**
- 1385 For installation, configuration, and integration instructions, refer to <u>Section 2.11</u>.
- 1386 **3.9 Tenable NNM**
- 1387 For installation, configuration, and integration instructions, refer to <u>Section 2.12</u>.
- 1388 **3.10** Mandiant Security Validation (MSV)
- 1389 For installation, configuration, and integration instructions, refer to <u>Section 2.13</u>.
- 1390 3.11 DigiCert CertCentral
- 1391 For installation, configuration, and integration instructions, refer to <u>Section 2.14</u>.

## 1392 **4 Enterprise 3 Build 1 (E3B1) Product Guides**

- 1393 This section of the practice guide contains detailed instructions for installing, configuring, and
- 1394 integrating all of the products used to implement E3B1. For additional details on E3B1's logical and
- 1395 physical architectures, please refer to NIST SP 1800-35B.

## 1396 4.1 Microsoft Azure Active Directory (AD)

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

- 1400 1. After logging in to portal.azure.com, <u>create an Azure AD Tenant</u>.
- Create a connection between your on-premises AD and Azure AD to replicate user, group, and authentication information from your AD to Azure AD.
- Configure the Azure AD Tenant to enable Single Sign-On Password Reset (SSPR). This gives users
   the ability to reset their passwords from <u>https://aka.ms/sspr</u> or from within their profile in
   Azure AD. This will be effective for both their AD and Azure AD accounts.
- 1406
   4. <u>Configure password writeback</u>, which enables password changes in Azure AD to be replicated back to the on-premises AD.
- 14085. The conditional access feature in Azure AD specifies conditions under which a user would be1409given access to a resource or application that uses Azure AD for authentication. MFA was1410configured as a requirement for access to all applications. Configure MFA for all users.
- Access to resources based on device compliance was implemented as an essential feature in this
   solution. Access would only be granted to a user if the client device is compliant. Compliance is
   reported to Azure AD by Microsoft Endpoint Manager. Enable this feature, Conditional Access
   Device Compliance.
- 1415 7. Configure an enterprise application, GitLab, to use Azure AD for authentication:
- 1416a. GitLab was configured to directly authenticate to Azure AD using the SAML protocol.1417GitLab must first be registered in Azure AD before Azure AD can be configured as the1418application's IdP.
- b. <u>Configure Azure AD as a SAML IdP for the GitLab application.</u> Once that is implemented,
  access attempts to the target application will be redirected to Azure AD for
  authentication and authorization.

#### 1422 4.2 Microsoft Endpoint Manager

- 1423 Microsoft Endpoint Manager is a cloud-based service that focuses on mobile device management
- 1424 (MDM) and mobile application management (MAM).

## 1425 4.2.1 Configuration and Integration

#### 1426 4.2.1.1 Add and verify a custom domain

1427 To connect an organization's domain name with Intune, a DNS registration needs to be configured. This 1428 gives users a familiar domain when connecting to Intune and using resources. Use the information found 1429 at the hyperlink to create a custom domain.

- 1430 4.2.1.2 Add users
- 1431 Use the information at the hyperlink to <u>add users to Intune</u>.
- 1432 4.2.1.3 Enroll devices in Microsoft Intune
- Enrolling devices allows them to receive configuration profiles and compliance policies. Configuration
  profiles configure features and settings on devices. Compliance policies help devices meet an
  organization's rules.
- 1436 1. <u>Get an Apple MDM push certificate and add it to Endpoint Manager</u>. This certificate is required 1437 to enroll iOS/iPadOS devices. Then enroll iOS devices in Microsoft Intune.
- <u>Create an iOS enrollment profile</u>. An enrollment profile defines the settings applied to a group of devices during enrollment.
- <u>Enroll Android devices in Microsoft Intune</u>. To enable Android Enterprise, an administrative
   Google account needs to be connected to the Intune tenant.
- <u>Create an iOS compliance policy in Microsoft Intune</u>. It will be evaluated before access is allowed
   from iOS devices.
- 1444 5. <u>Create an Android compliance policy in Microsoft Intune</u>. It will be evaluated before access is
   1445 allowed from Android devices.
- 1446 6. <u>Create an iOS/macOS configuration profile</u> for iOS or Mac devices.
- 1447 4.2.1.4 Configure conditional access rules
- 1448 Conditional access is used to control the devices and apps that can connect to company resources. Use 1449 the information in the hyperlink to <u>create device-based conditional access policies</u>.
- 1450 4.2.1.5 Manage applications
- iOS/iPadOS: Use the instructions at <u>Add iOS Store Apps</u> to select apps from the iOS/iPadOS store that
   will be approved for installation on your managed iOS or iPadOS devices.
- 1453 Android: For this build we added Managed Google Play apps. Managed Google Play is Google's
- 1454 enterprise app store which serves as a source of applications for Android Enterprise in Intune. Use the
- instructions at <u>Add Android Store Apps</u> to select apps that will be approved for installation and made
   available to your managed devices.
- 1457 Windows: Use the information provided at <u>select approved apps</u> to choose which apps should be added
  1458 to your Windows devices.
- 1459 There is more than one way to configure Windows apps in Intune. We configured the app using App 1460 suite information. For other ways, <u>refer to the Microsoft documentation</u>.
- 1461 **4.3** Microsoft Defender for Endpoint
- 1462 Microsoft Defender for Endpoint provides endpoint protection, detection, and response to threats.
- 1463 4.3.1 Configuration and Integration
- 1464 4.3.1.1 Enable Microsoft Defender for Endpoint
- 1465 Use the information at <u>Configure Microsoft Defender for Endpoint in Microsoft Intune | Microsoft Learn</u>
  1466 to enable Defender for Endpoint.
- 1467 1. Use the information in the provided hyperlink to <u>onboard devices</u>. Once devices are onboarded, 1468 threat signals and vulnerability information are automatically collected from them.
- You can optionally <u>enable supervised mode on iOS devices</u> using information at the hyperlink.
   Supervised mode gives administrators greater control over corporate-owned devices.
- Alerts and security incidents can be viewed and responded to by accessing the Defender for
   Endpoint cloud component. Use the information in the hyperlink to view and respond to
   discovered threats.
- 1474 4.3.1.2 Create Endpoint Detection and Response policy (Windows 10 and later)
- 1475 Endpoint detection and response (EDR) policies are used to detect advanced attacks in near real-time.1476 Use the information in the hyperlink to <u>create an EDR policy</u>.
- 1477 4.3.1.3 Create an antivirus policy
- 1478 An antivirus policy defines the behavior of the antivirus software agent on the endpoint. Use the
- 1479 information in the hyperlinks to <u>create an antivirus policy</u> and <u>configure antivirus policy settings</u>.

#### 1480 4.3.1.4 Create Defender compliance policy

1481 Compliance policies can help protect organizational data by requiring users and devices to meet defined

security requirements. Use the information in the hyperlink to <u>create a Defender for Endpoint</u>
 <u>compliance policy</u>.

#### 1484 4.3.2 Microsoft Defender Antivirus

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

- 1488 1. <u>Check the status of real-time protection</u> to ensure it's on.
- 1489 2. <u>Turn real-time protection on or off.</u>

#### 1490 4.4 Microsoft Sentinel

1491 Microsoft Sentinel is a cloud-native SIEM and SOAR system. It can be used for security analytics, threat 1492 intelligence, attack detection, and threat response.

- 1493 There is no need to install Sentinel, as it is a managed service. Instead, it needs to be enabled and 1494 configured in your Azure environment. It also needs a workspace to store and correlate ingested data.
- 1495 1. Enable Sentinel and configure a workspace.
- Use the general instructions found at <u>Connector to Data Sources</u> to enable log forwarding to
   Sentinel from various devices, systems, and services. Each data source will have to be connected
   independently from other data sources, so you must perform this step once per data source. In
   this build, Azure AD, Endpoint Manager, Defender for Endpoint, Office365, and Tenable.io were
   configured to send logs using this method.
- 15013. The Log Analytics Agent is a log forwarder that accepts syslog and Common Event Format (CEF)1502formatted logs and then forwards the logs to Sentinel. If you have a product or device without a1503native Sentinel integration, install and configure the Log Analytics Agent on a virtual machine.1504Once completed, the log forwarder will be able to receive syslog data on UDP port 514. Then1505configure the product or device that will be the data source to send logs via syslog to the log1506forwarder using the product's instructions.

#### 1507 **4.5 Microsoft Office 365**

1508 Microsoft Office 365 is a suite of SaaS-based productivity applications used for a variety of activities such 1509 as word processing, accounting, creating presentations, email, and others. Office 365 was enabled in the

- 1510 environment and was used as a set of protected target applications. Use the information at Activate
- 1511 <u>Microsoft Office 365</u> to activate your Office 365 subscription.
- 1512 Use the Office 365 Sign-in link to log on to Microsoft Office 365. Use your email address and password.
- 1513 You will be required to authenticate using multi-factor authentication.
- 1514 Once authentication is complete, you will see the various office applications, such as Word, Excel,
- 1515 PowerPoint, and Outlook in your dashboard.

#### 1516 **4.6 F5 BIG-IP**

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

#### 1520 4.6.1 Installation, Configuration, and Integration

- BIG-IP was deployed into the environment using a virtual machine image or open virtual appliance
  (OVA) file. Once this OVA import operation is complete, log into the virtual machine console and assign
  an IP address to a network interface, then continue configuration by connecting to its web interface.
  This BIG-IP image has both the Access Policy Manager (APM) and the Local Traffic Manager modules
  installed.
- 1526 1. <u>Deploy BIG-IP OVA</u> into your VMware environment.
- Access the BIG-IP web interface by entering the IP address or DNS name into a web browser.
   Then complete the initial setup and configuration of BIG-IP.
- Create virtual servers which map to back-end protected applications—in this build, to our
   Guacamole application server.
- 15314. Configure BIG-IP to use Azure AD as the SAML IdP for external authentication to access back-end1532applications. The instructions at Configure BIG-IP Easy Button for Header Based SSO and the1533video at Azure AD and BIG-IP APM Integration Video provide additional references.
- Once these instructions are completed, BIG-IP, leveraging Azure AD for external authentication,
   will only allow successfully authenticated and authorized users to access Guacamole. Access to
   the backend application is either done by connecting directly via the DNS name of the
   application or by going to myapps.microsoft.com and selecting the backend application icon,
   such as F5 Guacamole\_SSO as shown below.

 $\gg$ 



1539 1540 6. For this build, <u>configure BIG-IP to send logs to Microsoft Sentinel</u>. Then you can observe BIG-IP logs in Sentinel, as shown below.

₽ N	ew Query 1* $ imes$ +	
₽ S	ecOps	▶ Run Time range : Last 3 days
*	1 F5Telemetry_AVR_CL	
	Results     Chart     Image: Add       Image: Showing the first 30,000 results	bookmark ults. <u>Learn more</u> on how to narrow down the resu
	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
Sch	TimeGenerated [UTC]	2022-06-03T14:35:05.884Z
lema	hostname_s	ENT3-BIGIP.ent3.nccoe.org
an	SlotId_s	0
E D	errdefs_msgno_s	22323218
ter	STAT_SRC_s	TMSTAT
	Entity_s	ProcessCpuUtil
	EOCTimestamp_s	1654266900

### 1541 4.7 Lookout Mobile Endpoint Security (MES)

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

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

#### 1546 4.7.1 Configuration and Integration

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

- 1549 1. Go to Azure Active Directory > Properties and locate Tenant ID. Copy and save it to the text file.
- 1550 2. Go to Azure Active Directory > Groups to open the Groups | All groups pane.
- 1551 3. Select the group with full access *rights* (Lookout Admin group).
- 1552 4. Copy the (group) **Object Id**, and then save it in a text file.
- 1553 The following steps are to be completed in the Lookout Enterprise admin console and will enable a 1554 connection to Lookout's service for Intune enrolled devices.
- 1555 1. Sign in to the Lookout for Work console and go to **System** > **Integrations**, and then select
- 1556 **Choose a product to set up**. Select **Microsoft Azure**. Copy and paste the Azure AD (AAD) tenant 1557 ID and group object ID from the text file that was created in previous steps.

IDP Settings



Lookout Role Permissions

00720000 571	3b-46e9-be89-4ce0509b3f73	
Restricted acc	ess	
Unique AAD	group ID (optional)	
Read only		
Read only Unique AAD	group ID (optional)	
Read only Unique AAD g invites only	group ID (optional)	

# Stay in System > Integrations, and then select Choose a product to set up. Select Microsoft Intune.

1560 3. Configure Intune connector settings.

Connector	Settings		
Label	for this MDM cor	nection ?	
ENT	3NCCOE		
Heart	beat Frequency (	required) ?	
10	minute(s)		

- 1561 After Lookout MES is enabled, a connection to Lookout in Intune needs to be set up.
- 1562 1. Go back to Microsoft Endpoint Manager and enable the Mobile Threat Defense connector there.
- 1563 2. Select **Tenant administration > Connectors and tokens > Mobile Threat Defense.**
- 1564 3. On the **Mobile Threat Defense** pane, select **Add.**
- For Mobile Threat Defense connector to setup, select Lookout MTD solution from the drop down list.
- 1567 5. Configure the toggle options according to the organization's requirements. This screenshot1568 shows examples.

MDM Compliance Policy Settings	
Connect Android devices to Lookout for Work ①	Off On
Connect iOS devices to Lookout for Work $\odot$	Off On
Enable App Sync for iOS/iPadOS Devices ①	Off On
Send full application inventory data on personally-owned iOS/iPadOS Devices $\odot$	Off On
Block unsupported OS versions $\odot$	Off On

- 1569 When Lookout is integrated with Intune MTD and the connection to Intune is enabled, Intune creates a
- 1570 classic conditional access policy in Azure AD. To view classic conditional access policy, go to Azure Active
- 1571 Directory > Conditional Access > Classic policies. Classic conditional access policy is used by Intune MTD
- to require that devices are registered in Azure AD so that they have a device ID before communicating to
- 1573 Lookout MTD. The ID is required so that devices can report their status to Intune.

#### 1574 4.7.2 Create MTD Device Compliance Policy with Intune

1575 Compliance policy is needed to detect threats and assess risks on mobile devices to determine if a1576 device is compliant or not.

- 1577 1. Open the Microsoft Endpoint Manager admin center.
- 1578 2. Select Endpoint security > Device Compliance > Create Policy.
- 1579 3. Select the **Platform,** and then **Create.**
- 1580 4. On **Basics**, provide **Name** and **Description**. Select **Next** to continue.
- On Compliance settings, expand and configure Device Health. Choose the Mobile Threat Level
   from the drop-down list for Require the device to be at or under the Device Threat Level.
   Choose the level for compliance.
- Select Next to go to Assignments. Select the groups or users to which this policy should be assigned.

#### 1586 **4.8 PC Matic Pro**

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

- PC Matic Pro Server needs to be installed on a server with Windows 2019 Server and SQL Serverpreinstalled.
- 15931. Obtain the OnPremInstallerRun.ps1 installation script from the vendor and open an elevated1594PowerShell window.
- **2.** Execute the OnPremInstallerRun.ps1 script by entering .\OnPremInstallerRun.ps1
- 1596registryUser pcmatic -registryPwd <insert\_password\_here> -localDBUser pcm-app to1597install docker, pull down the container images, and deploy the container instances that make up1598the PC Matic Pro server.
- Navigate to the PC Matic web server and verify that it is operational by opening a web browser and going to *https://<pcmaticDNSName>/web\_portal*. In this build, the DNS name is nist.pcmaticfederal.com; as such, to access the server's web interface, we would go to https://nist.pcmaticfederal.com/web\_portal.

- 1603 Follow these steps to install PC Matic Endpoint Agents:
- Open a web browser on a Windows or macOS client device. Navigate to the PC Matic Server
   web interface by browsing to https://nist.pcmaticfederal.com from the client device and log on
   with your credentials.
- Click Add a Device and then click Windows Installer or Mac Installer, as appropriate, to
   download the PC Matic Endpoint Agent.
- 1609 3. Install the agent.
- 4. Once installed, the agent will establish communications with the server and show up on the listof managed devices once you log on to the server as previously described.
- 1612 5. Devices with an agent will register and come online.

+ Add	a Device 🖹 Export to Excel			All Devices -	Search	۲
0	A Device Name	Device Type	0 Last Seen	4 Group	Status	Actions
	AADJCLIENT3	Desktop	2022/05/30 12:59:42	Unassigned	SS 🐮 🔺	🔺 🗈 🖮 🚺
	PCMATICENDPT1	Desktop	2022/05/28 01:58:36	Unassigned	SS 🐮 🖬	🔺 🗈 🖿 🚺
	PCMATICENDPT2	Desktop	Now	Unassigned	8 🛡 🛦	🔺 🗈 😁 🚺
	User's MacBook Pro	Mac	2022/03/30 17:19:44	Unassigned	SS 🙂 🖬	🔺 🗈 📾 🚺

#### 1613 **4.9 Tenable.io**

1614 For installation, configuration, and integration instructions, refer to Section <u>2.10</u>.

#### 1615 4.9.1 Integration with Microsoft Sentinel

- In Tenable.io, click the hamburger menu (Ξ) in the top left corner and navigate to Settings >
   Access Control > Users.
- 1618
   2. (Optional) Click Create User and create a new API user for Microsoft Sentinel. In this
   1619 implementation, a standard administrator account was used.
- 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.
- In Microsoft Sentinel, navigate to Data Connectors. Search *tenable* and click Tenable.io
   Vulnerability Management (Preview) > Open Connector Page.
- 1624 5. Scroll down in the Instructions panel and save the Workspace ID and Primary Key.
- 1625 6. Click **Deploy to Azure.**

- 1626 7. Select the appropriate resource group.
- 1627 8. In the Workspace ID and Workspace Key fields, enter the values obtained in step 5.
- 1628 9. In the Tenable Access Key and Tenable Secret Key fields, enter the values obtained in step 3.
- 1629 10. Click **Review + create.**
- 1630 11. Click Create. Function deployment will begin. Once deployment is complete, it will take some1631 time before Sentinel begins making calls to Tenable.io.

#### 1632 **4.10 Tenable.ad**

1633 For installation, configuration, and integration instructions, refer to Section 2.11.

#### 1634 **4.11 Tenable NNM**

1635 For installation, configuration, and integration instructions, refer to Section 2.12.

#### 1636 4.12 Mandiant Security Validation (MSV)

1637 For installation, configuration, and integration instructions, refer to Section 2.13.

#### 1638 4.13 Forescout eyeSight

- Forescout eyeSight provides asset discovery with both active and passive techniques, and through
   integrations with network and security infrastructure. In this build, Forescout was deployed on-premises
   in two virtual hosts: an Enterprise Manager and Forescout Appliance.
- 1642 For Forescout installation instructions, visit the Forescout Installation Overview.

#### 1643 4.13.1 Integration with AD

- 1644 1. In AD, create a domain administrator service account for Forescout and save the credentials.
- 1645 2. In the Forescout console, navigate to **Tools > Options > HPS Inspection Engine.**
- 1646 3. In the **Domain Credentials** section, click the **Add** button.
- 1647 4. Enter the domain information and credentials you saved earlier. Click **OK**.
- 1648 5. Click **Apply.** After the new configuration is saved, click **Test** to verify that the credentials are 1649 working as expected.

- 1650 4.13.2 Integration with Cisco Switch
- 1651 For Cisco Switch integration instructions, visit the <u>Switch Plugin Configuration Guide</u>.
- 1652 4.13.3 Integration with Cisco Wireless Controller
- 1653 For Cisco Wireless Controller integration instructions, visit the Wireless Plugin Configuration Guide.
- 1654 4.13.4 Integration with Microsoft Sentinel
- 1655 1. In the Forescout console, navigate to **Tools > Options > CEF.**
- 1656 2. Click Add.
- In the Add Server dialog, enter a Name, select Use UDP for Connection, and enter the IP address
   of the Sentinel Log Forwarder. Click Next.
- Click the Assign CounterACT Devices radio button, and check all of the checkboxes next to the
   listed devices.
- 1661 5. Click **Finish.** Verify that logs are being received by the Sentinel Log Forwarder.
- 1662 4.13.5 Integration with Palo Alto Networks NGFW
- For Palo Alto Networks NGFW integration instructions, visit the <u>eyeExtend for Palo Alto Networks Next-</u>
   Generation Firewall Configuration Guide.
- 1665 4.13.6 Integration with Tenable.io
- For Tenable.io integration instructions, visit the <u>eyeExtend for Tenable.io Vulnerability Management</u>
   <u>Configuration Guide</u>.
- 1668 4.14 Palo Alto Networks Next Generation Firewall
- 1669 For installation, configuration, and integration instructions, refer to <u>3.5</u>.

#### 1670 4.15 DigiCert CertCentral

1671 For setup and usage instructions, refer to Section 2.14.

### 1672 **5 Enterprise 1 Build 2 (E1B2) Product Guides**

- 1673 This section of the practice guide contains detailed instructions for installing, configuring, and
- 1674 integrating all of the products used to implement E1B2. For additional details on E1B2's logical and

1675 physical architectures, please refer to Volume B.

#### 1676 **5.1 Zscaler**

I677 Zscaler provides secure user access to public-facing sites and on- or off-premises private applications via
 the Zscaler Zero Trust Exchange, a cloud-delivered security service edge technology. The Zscaler Internet
 Access (ZIA) manages user access to the internet. Zscaler Private Access (ZPA) manages user access to
 applications within an enterprise. Zscaler integrates with Okta for authentication and authorization of
 users.

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

#### 1685 5.1.1 Zscaler ZPA Configuration and Integration

- 1686 Once admin access is available, log in to ZPA to perform the following:
- 1687 1. Create additional <u>admin accounts</u> as needed.
- 16882. Create a Zscaler App Connector Group and Zscaler App Connector in the ZPA portal. Note: App1689Connector Groups are recommended by Zscaler for availability and scaling. Note: This build has1690two App Connector Groups, one for on-prem applications and one for cloud applications in1691AWS.
- Once the App Connector is configured in the ZPA portal, install the actual Zscaler App connector.
   Refer to the Zscaler Application Connector section below. Note: This build has two App
   Connectors, one for on-prem applications and one for cloud applications in AWS.
- 1695
   4. <u>Create integration with Okta</u>. All users accessing resources within the enterprise will use twofactor authentication when logging into the Zscaler Client Connector. Note: Step 1 of
   1697
   1698
   completed in the Okta cloud. Refer to Section 5.2. Step 2 of configuration is completed on the ZPA admin portal.
- Deploy Zscaler Client Connectors (ZCCs) for various endpoints, including configuring ZCC policies
   to control the settings and behavior of ZCC. Refer to the Zscaler Client Connector section below.
- Set up <u>ZPA Application configuration</u> for access to resources. In this step, applications are
   defined and applied to segments so that the proper App Connector can perform PEP functions.
- Configure <u>Access Policies</u> to control user access to various applications. For our policies, we
   defined specific App Segments, configured specific IDP authentication parameters, and
   configured client posture checks.
- 1706 8. Configure a <u>log receiver</u> for the IBM QRadar SIEM tool to receive logs for ZPA.

#### 1707 5.1.2 Zscaler ZIA Configuration

- 1708 Once admin access is available, log in to ZIA to perform the following:
- 1709 1. Create additional <u>admin accounts</u> as needed.
- 1710 2. Set up <u>IdP integration</u> with Okta.
- 17113. Create policies to manage user access to various resources on the internet. For this build, we1712used many of the defaults built into ZIA. We created policies to allow certain users access to a1713resource on the internet and to block certain users based on their role and time of day.
- 1714 4. Integrate ZIA Nanolog Streaming Service with IBM QRadar SIEM tool to receive ZIA logs.

#### 1715 5.1.3 Zscaler Client Connector

1716 <u>Zscaler Client Connectors (ZCCs)</u> are available for Windows, macOS, Linux, iOS, and Android endpoints.
 1717 Deployment of ZCC includes configuring ZCC policies to control the settings and behavior of ZCC. For all

1718 these endpoints, a device manager can be leveraged to push the ZCC. For this build, we tested the use of

1719 Ivanti to push ZCC to Windows, iOS, and Android endpoints. For other devices we manually installed

1720 ZCC. Once ZCC is installed, users are prompted to log in, which allows the user and device to be

managed by ZPA and ZIA, depending on the type of resource the user is accessing.

#### 1722 5.1.4 Zscaler Application Connector

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

### 1728 5.2 Okta Identity Cloud

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

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

#### 1734 5.3 Radiant Logic RadiantOne

1735 No changes were made from Build 1. Refer to Section <u>2.2</u>.

#### SailPoint IdentityIQ 5.4 1736

1737 No changes were made from Build 1. Refer to Section 2.3.

#### **Ivanti Neurons for UEM** 5.5 1738

1739 No significant changes were made from Build 1. Ivanti Neurons for UEM was configured to deploy the

- 1740 Zscaler Client Connector to managed devices. For information, configuration, and integration 1741
- instructions, refer to Section 2.4.
- 5.6 **IBM Security QRadar XDR** 1742
- 1743 For installation, configuration, and integration instructions, refer to Section 2.9.

#### 5.7 Tenable.io 1744

- 1745 For installation, configuration, and integration instructions, refer to Section 2.10.
- **Tenable.ad** 5.8 1746
- 1747 For installation, configuration, and integration instructions, refer to Section 2.11.

#### 1748 5.9 Tenable NNM

1749 For installation, configuration, and integration instructions, refer to Section 2.12.

#### 5.10 Mandiant Security Validation (MSV) 1750

1751 For installation, configuration, and integration instructions, refer to Section 2.13.

#### 5.11 **DigiCert CertCentral** 1752

1753 For setup and usage instructions, refer to Section 2.14.

#### **AWS laaS** 5.12 1754

- 1755 Amazon Web Services is a cloud computing platform provided by Amazon that includes a mixture of
- 1756 laaS, platform as a service (PaaS), and SaaS offerings. The following section describes the setup of AWS 1757 laaS resources to serve as a public/private cloud host.
- 1758 For details on the logical architecture of the AWS environment, please refer to Volume B, Section
- 1759 4.4.9.1.

#### 1760 5.12.1 Configuration

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

- Create and activate an AWS account. Use the root account to create administrative accounts
   with rights to create necessary resources for the project.
- Create a Production and Management Virtual Private Cloud (VPC). Configure ingress and egress
   Security Group rules for each VPC.
- Create Transit gateways to attach on-prem networks to the AWS environment. Create Internet
   gateways for access to the internet.
- 17714. Within the Prod VPC, configure redundant public subnets in different Availability Zones for fault1772tolerance. Configure redundant private subnets for Web, Application, and Database tiers.
- Set up resources for testing in the Prod VPC. For demonstration purposes, a private WordPress and GitLab server pair and a public WordPress server were built. Configure auto scaling and Elastic Load Balancing for servers/services set up on the Web, Application, and Database tiers.
- Within the Mgmt VPC, configure redundant public subnets in different Availability Zones for
   fault tolerance. Configure private subnets for Satellite, Domain Controller, and Security
   Management Tiers.
- 1779 7. Set up AWS Session Manager access for remote admins.
- 1780 8. For shared AWS services, configure VPC endpoints with ICAM policies to control access.

## 1781 6 Enterprise 3 Build 2 (E3B2) Product Guides

This section of the practice guide contains detailed instructions for installing, configuring, and
integrating all the products used to implement E3B2. For additional details on E3B2's logical and physical
architectures, please refer to Volume B. Build 2 was built on top of Build 1 and all the components in
Build 1 were used in this build. For E3B1's configuration please refer to Section <u>4</u>. Below are the
additional components added to Build 2.

### 1787 6.1 Microsoft Azure AD Identity Protection

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

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

#### 1798 6.2 Microsoft Azure AD Identity Governance

- Azure AD Identity Governance enables organizations to manage access to resources applying access
   request and approval workflows, access assignments and removals, access expiration, and access
   reviews.
- 1802 1. <u>Create an access package</u> to encapsulate the target resources in a single object.
- 1803 2. <u>Create policies</u> to define approvers and eligible requestors.
- 18043. Requesting access to the access package can be done using the information found at <a href="Request\_access">Request\_access</a>.1805access</a>.
- 1806 4. To approve or deny access requests, use the information found at <u>Approve or deny request</u>.

#### 1807 6.3 Microsoft Defender for Cloud Apps

- 1808 Microsoft Defender for Cloud Apps is a cloud access broker solution that protects cloud applications and
   1809 on-premises web applications by monitoring session activity to those applications, ensuring compliance
   1810 to defined policy and mitigating detected threats.
- 1811 1. Login to the portal and activate your Defender for Cloud Apps tenant.
- Connect your apps to Defender for Cloud Apps. For custom web applications including on premises web applications, use the information on connecting a custom app to Defender for
   Cloud Apps to integrate your custom web applications.
- 1815
   3. Use the information on <u>creating and assigning policies</u> to provide security controls to apps,
   1816
   ensuring compliance and mitigating threats.
- 1817
   4. <u>Deploy Conditional Access App Control</u>, which leverages Azure AD conditional access policies and enforcement for connected apps.

#### 1819 6.4 Microsoft Azure AD Application Proxy

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

- 1823 1. Configure <u>Application Proxy deployment prerequisites</u>.
- 1824 2. <u>Install and register the Application Proxy connectors</u>. Once the application proxy connectors are 1825 successfully installed and registered, the Application Proxy service will be enabled automatically.
- 1826 3. <u>Add your application</u> to Application Proxy.

#### 1827 6.5 Microsoft Defender for Cloud

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

- 1834 1. <u>Enable Defender for Cloud</u> for your subscription.
- To receive a secure score, which provides a numeric value indicating your point-in-time security posture, you must ensure that the Azure Security Benchmark initiative or at least one other listed regulation is selected and applied to your subscription. Azure Security Benchmark should automatically apply to your subscription. Examples of regulations include PCI DSS, HIPAA, and NIST SP 800-53. Azure Security Benchmark is comprised of a set of controls that detect security misconfigurations based on best practices from common compliance frameworks.
- 1841 3. <u>Apply regulations to your subscription</u>.
- Defender for Cloud will list recommendations for your environment to improve the security
   posture. <u>Apply the listed security recommendations</u>.

#### 1844 6.6 Forescout eyeSight

- Forescout eyeSight provides asset discovery with both active and passive techniques, and throughintegrations with network and security infrastructure.
- 1847 For installation, configuration, and integration instructions, refer to <u>Section 4.13</u>.

#### 1848 6.7 Forescout eyeControl

- 1849 Forescout eyeControl enforces and automates network policies across the enterprise.
- 1850 For Forescout eyeControl installation instructions, visit the <u>Forescout Installation Overview</u>.
- 1851 6.7.1 Configuring a policy
- 1852 1. In the Forescout Console, choose a policy.
- 1853 2. Select the network segment to which the policy will be applied.
- 1854 3. Add **Conditions** to select the attributes of the hosts that the policy will be applied to.
- 1855 4. Add **Actions** that will be applied to the selected hosts.
- 1856 5. Add any additional rules that will be used in the policy.
- 1857 6. Run the policy.

#### 1858 6.8 Forescout eyeSegment

- Forescout eyeSegment accelerates zero trust segmentation through visibility into traffic and transactionflows.
- 1861 For Forescout eyeSegment installation instructions, visit the <u>Forescout Installation Overview</u>. After
- 1862 installation has been completed, visit the <u>eyeSegment Application How-to Guide</u> to configure and use
- 1863 eyeSegment to analyze your network traffic from a dynamic zone perspective, simplify segmentation
- 1864 planning, and automate access control list (ACL)/VLAN assignment.
- 1865 6.8.1 Access the eyeSegment Dashboard
- From the Forescout Console, click **Dashboards**. This will launch a web browser and authenticate
   to the Forescout Web Client.
- 1868 2. At the top of the Forescout Web Client, click **Segmentation**.
- 18693. The initial dashboard is the eyeSegment Matrix. This dashboard can be used to analyze traffic1870and transaction flows between different network hosts, segments, and groups.
- Open the eyeSegment Policy dashboard, which can be used to apply proposed zero trust rules.
   The effect of these rules can be seen in the eyeSegment Matrix.
- 1873 5. Open the eyeSegment Health dashboard, which provides information about Reporting
   1874 Appliances, Traffic Sensors, Endpoint Coverage, and the connection to the eyeSegment cloud.

#### 1875 6.9 Forescout eyeExtend

- 1876 Forescout eyeExtend automates security workflows across disparate products through integration with1877 other security technologies.
- 1878 For Forescout eyeExtend installation instructions, visit the <u>Forescout Installation Overview</u>. Once
- 1879 installation has been completed, visit the <u>Connect Plugin Configuration Guide</u>, which provides the
- 1880 capability to build custom integrations with products that are not already provided. However, Forescout
- also provides a wide range of integrations at the official <u>Forescout eyeExtend repository</u>.

#### 1882 6.9.1 Integration with Microsoft Endpoint Manager

1883 Integration instructions for Microsoft Endpoint Manager can be found at Forescout's official GitHub 1884 repository: <u>https://github.com/Forescout/eyeExtend-Connect/tree/master/Intune</u>.

#### 1885 6.10 Microsoft Azure laaS

- Azure IaaS provides compute, networking, and storage services that enable the creation of an enterprise
  IT infrastructure by subscribers. The following section describes the Azure IaaS components that were
  deployed in this build.
- 18891. Virtual Networks (VNETs) are isolated customer networks. They contain subnets and are built in<br/>Azure. We have three VNETs: a hub VNET, which provides central connectivity for other VNETs,<br/>and a GitLab VNET and a WordPress VNET, which are both designed to protect individual apps<br/>and their associated resources. Use the information at <u>Create a VNET</u> to create and configure a<br/>virtual network. To enable communication between the hub and other VNETs, <u>establish peering</u><br/>between them.
- Public VNETs are regular VNETs that have hosts with public IP addresses. The GitLab VNET is
   configured as a public subnet with a public IP address attached to the Application Gateway
   which was configured to provide load balancing and protection against common web attacks.
- Private VNETs are regular VNETs that have hosts with only private IP addresses and are
   reachable only by internal users by default. WordPress VNET was configured as a private VNET.
- Configure Azure Bastion to enable web-based SSH and remote desktop-based access to servers and virtual machines.
- 1902 5. <u>Instantiate and configure Azure Firewall</u> in the hub VNET to provide protection for incoming
   1903 traffic from both the Internet and the VPN traffic from on-prem clients.
- 1904 6. <u>Use network security groups (NSGs) to filter inbound or outbound traffic</u> to or from Azure
   1905 resources. Enable only ports that are necessary for appropriate access.

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

## 1910 7 Enterprise 1 Build 3 (E1B3) Product Guides

1911 E1B3 uses all of the same products and technologies as E1B2. (See Section 5.)

## 1912 8 Enterprise 2 Build 3 (E2B3) Product Guides

1913 This section of the practice guide contains detailed instructions for installing, configuring, and 1914 integrating all of the products used to implement Microsegmentation (Network) E2B3. For additional

1915 details on E2B3's logical and physical architectures, please refer to Volume B.

### 1916 8.1 Ping Identity PingOne

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

### 1921 8.1.1 Configuration: PingOne and PingFederate

1922 Refer to Section <u>3.1.1</u>.

#### 1923 8.1.2 Integrations

1924 Refer to Sections <u>3.1.2</u> and <u>3.1.3</u> for integrations of Ping Identity with Radiant Logic and Cisco Duo.

1925 VMware Workspace ONE Access's Integration with PingFederate was achieved using a SAML redirect

1926 (Workspace ONE Access is configured as a third-party SAML IdP in PING). When users on mobile devices

1927 attempt to authenticate through PingFederate, they will be redirected to Workspace ONE Access.

- 1928 Workspace ONE Access performs seamless passwordless user and device authentication using
- 1929 certificates, as well as checking the device's compliance status in Workspace ONE UEM. The result of the
- 1930 compliance check and authentication is passed back to PING as a SAML Assertion.
- 1931 1. To integrate with VMware Workspace ONE Access, navigate to the Authentication -> IdP
- 1932Connections menu and click Create Connection to create an IdP connection. The steps below1933describe the information needed to configure this IdP connection.

- For the IDP Connection settings, the connection role is IdP using SAML 2.0. General information needed is Partner's Entity ID, Connection Name, and Base URL. All this information is provided by Workspace ONE Access.
- 1937 3. Browser SSO properties include IdP-Initiated SSO and SP-Initiated SSO.
- 1938 4. For **User-Session Creation** information, leverage the contract that was created in Section <u>3.1</u>.
- 1939 5. For **Protocol Settings, SSO Service URLs** need to include a Redirect URL and a POST URL.
- 1940 6. Lastly, a certificate that is provided by Workspace ONE Access is needed for **Credentials.**
- 1941 Refer to the <u>PingFederate Administrator's Reference Guide</u> for detailed configuration steps.
- 1942 8.2 Radiant Logic RadiantOne
- 1943 8.2.1 Installation and Configuration
- 1944 Refer to Section <u>2.2.1</u> and Section <u>2.2.2</u>.
- Additional attributes were added to the RadiantOne solution. These attributes allow other ZT tools to
  create more granular policies for access. Within the Directory Namespace, we created namespaces
  (HDAP) for Clearance, Data Governance, Risk, and Training. Information pertaining to these categories
  was imported via flat files for the purpose of this build. For configuration instructions, refer to
  RadiantOne v7.4.4 Namespace Configuration Guide. We also updated RadiantOne's configuration with a
  global Identity view of users combining these attributes with the AD directory and HR database. We
  leveraged the <u>Global Identity Builder</u> to perform this.
- 1952 8.2.2 Integrations
- 1953 Refer to Section 2.2.3 for integration of Radiant Logic with SailPoint.
- 1954 To integrate with Cisco ISE and VMware Workspace ONE Access, follow the instructions in the 1955 Integration sub-section of Section 2.2 to create unique service accounts for the integration.
- 1956 8.3 SailPoint IdentityIQ
- 1957 8.3.1 Installation and Configuration
- 1958 Refer to Section <u>2.3.1</u>.
- 1959 8.3.2 Integration with Radiant Logic
- 1960 Refer to Section <u>2.3.2</u>.

#### 1961 8.3.3 Integration with AD

- 1962 Refer to Section <u>2.3.3</u>.
- 1963 8.3.4 Integration with Ping Identity
- 1964 There is no integration with Ping Identity. For this build, SailPoint provides AD user information and Duo 1965 pulls from AD.

#### 1966 **8.4 VMware Workspace ONE**

- 1967 VMware Workspace ONE Access is a cloud-based service that provides a variety of management
  1968 functions to support enterprise operations. For this build, two VMware services were utilized to support
  1969 endpoint management functionality: Workspace ONE Access and Workspace ONE UEM.
- 1970 8.4.1 VMware Workspace ONE Access
- Workspace ONE Access can serve as an IdP and integrate with a large range of enterprise identity
  components. For this build, Workspace ONE Access was integrated with PingFederate and RadiantOne
  to provide certificate-based authentication for endpoints.

#### 1974 8.4.2 Setup

1975 Each instance of Workspace ONE Access must be provisioned by VMware. After this has been1976 completed, VMware provides access and setup instructions.

#### 1977 8.4.3 Integration with RadiantOne

- 1978 To integrate with RadiantOne, an on-premises agent was installed on a Microsoft Windows Server 2019 1979 system and connected to Workspace ONE Access. After this, Workspace ONE Access was configured to 1980 pull user, group, and attribute information.
- The step-by-step guide to adding the on-prem connector can be triggered in the Workspace ONE
   Access console by navigating to Integrations -> Connectors and clicking New.
- After the on-prem agent is installed and connected to Workspace ONE Access, follow the <u>official</u>
   <u>VMware documentation</u> to add a new LDAP Directory and point Workspace ONE Access to your
   RadiantOne installation.
- Once these two steps are completed, RadiantOne's users, groups, and attributes are available for usewithin Workspace ONE.

## 1988 8.4.4 Integration with PingFederate

1989 1990 1991	Integration with PingFederate was achieved using a SAML redirect. When users with mobile devices attempt to authenticate through PingFederate, they will be redirected to Workspace ONE Access if certificate authentication is available.			
1992 1993	1.	In the Workspace ONE Access console, navigate to Integrations -> Identity Providers and click Add -> SAML IdP.		
1994 1995	2.	Fill out details in the form pertaining to your installation. For the binding protocol, select <b>HTTP Redirect</b> .		
1996	3.	Under Users, select the directory that you created in your previous integration with RadiantOne.		
1997 1998	4.	Under Authentication Methods, add a new authentication method name and select urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport for the SAML Context.		
1999	5.	Click <b>Save</b> in the bottom right corner.		
2000 2001	Now that the configuration on the Workspace ONE Access side has been completed, navigate to the PingFederate console.			
2002	1.	Navigate to Authentication -> IdP Connections and click Create Connection.		
2003 2004	2.	Check the <b>BROWSER SSO Profiles</b> checkbox and select <b>SAML 2.0</b> from the dropdown menu that appears. Click <b>Next</b> .		
2005	3.	Select the Browser SSO checkbox and click Next.		
2006	4.	On the <b>Metadata URL</b> page, click <b>Next</b> .		
2007 2008	5.	Under the <b>Partner's Entity ID (Connection ID)</b> section, paste your Workspace ONE Access metadata URL. It should look something like		
2009	C	<pre>nttps://<workspaceoneaccessurl>/SAAS/AP1/1.0/GET/metadata/idp.xml.</workspaceoneaccessurl></pre>		
2010	6.	Under BASE URL, add the base URL for your Workspace ONE Access Instance. Click Save.		
2011 2012	Workspace ONE Access can also be configured as a Service Provider (SP) for PingFederate. This proce is very similar to the IdP configuration.			
2013 2014	1.	In the PingFederate console, navigate to <b>Applications -&gt; SP Connections</b> and click <b>Create</b> <b>Connection</b> .		
2015 2016	2.	Check the <b>BROWSER SSO Profiles</b> checkbox and select <b>SAML 2.0</b> from the dropdown menu that appears. Click <b>Next</b> .		

2017 3. Select the **Browser SSO** checkbox and click **Next**.

- 2018 4. On the Metadata URL page, click **Next**.
- 20195. Under the Partner's Entity ID (Connection ID) section, paste your Workspace ONE Access2020metadata URL. It should look something like
- 2021 https://<WorkspaceONEAccessURL>/SAAS/API/1.0/GET/metadata/idp.xml.
- 2022 6. Under **BASE URL**, add the base URL for your Workspace ONE Access instance. Click **Next**.
- 2023 7. Under Browser SSO, select the checkboxes next to IdP-Initiated SSO and SP-Initiated SSO.
- 8. For Assertion Creation, select the checkbox next to Enable Standard Identifier. Select the
   PingFederate contract to use for this connection.
- 20269. Under Protocol Settings, set the Assertion Consumer Service URL to2027/SAAS/auth/saml/response. Click Save.

Initial setup for this integration has now been completed. To utilize this integration, you can set policies
 on either Workspace ONE Access or PingFederate to point to the other IdP or SP. In PingFederate, this
 can be found under Authentication -> Policies. In Workspace ONE Access, this can be found under
 Resources -> Policies.

- 2032 8.4.5 VMware Workspace ONE UEM
- 2033 Workspace ONE UEM provides endpoint management capabilities for this build and allows certificates2034 to be provisioned for user authentication.

#### 2035 8.4.6 Setup

The cloud-based Workspace ONE UEM instance must be provisioned by VMware. After this has been
 completed, follow the <u>official Workspace ONE UEM documentation</u> to deploy agents to each of your
 managed endpoints. Instructions for deploying profiles and compliance requirements to devices can also
 be found in the link above.

#### 2040 8.4.7 Integration with Certificate Authority

To provide certificates with custom attributes, Workspace ONE UEM was integrated with the on-prem
 Certificate Authority hosted in Enterprise 4. Instructions on how to complete this process can be found
 in the official Workspace ONE UEM documentation.

#### 2044 **8.5 Cisco Duo**

2045 Cisco Duo is a SaaS solution that implements and enforces security policies and processes, using strong
2046 authentication to reduce the risk of data breaches due to compromised credentials and access from
2047 unauthorized devices. For this build, we use Cisco Duo as the second authentication factor for resources.

- 2048 8.5.1 Configuration
- 2049 Refer to Section <u>3.4.1</u>.
- 2050 8.5.2 Integration
- 2051 Refer to Section <u>3.4.2</u>.
- 2052 8.6 Palo Alto Networks Next Generation Firewall
- 2053 For installation, configuration, and integration instructions, refer to Section <u>3.5</u>.
- 2054 8.7 IBM Security QRadar XDR
- 2055 For installation, configuration, and integration instructions, refer to <u>Section 2.9</u>.
- 2056 **8.8 Tenable.io**
- 2057 For installation, configuration, and integration instructions, refer to Section 2.10.
- 2058 **8.9 Tenable.ad**
- 2059 For installation, configuration, and integration instructions, refer to <u>Section 2.11</u>.
- 2060 8.10 Tenable NNM
- 2061 For installation, configuration, and integration instructions, refer to <u>Section 2.12</u>.
- 2062 8.11 Mandiant Security Validation (MSV)
- 2063 For installation, configuration, and integration instructions, refer to <u>Section 2.13</u>.
- 2064 8.12 DigiCert CertCentral
- 2065 For installation, configuration, and integration instructions, refer to <u>Section 2.14</u>.

#### 2066 8.13 Cisco Identity Services Engine (ISE)

Cisco ISE is a network central PDP that includes both PE and PA to help organizations provide secure access to users, their devices, and the other resources in their network environment. It simplifies the delivery of consistent and secure access control to PEPs across wired and wireless multi-vendor

2070 networks, as well as remote VPN connections.

2071 To deploy ISE, use the following steps:

2072	1.	Install (	Cisco ISE ADE-OS-Version 3.1.0.010 Patch 5 using Cisco ISE Installation Guide.
2073	2.	Continu	ue configuration using Cisco ISE configuration information.
2074	3.	Key cor	nfiguration features used at the NCCoE lab are as follows:
2075		a.	Basic setup: Cisco ISE Deployment model used is the "Stand Alone" as shown here.
2076 2077 2078		b.	Maintain and Monitor: System recovery, syslog settings, backups/recovery, advance filtering, and reporting, including endpoint purging and quarantining used as shown <u>here.</u>
2079 2080		C.	Secure Access: Cisco ISE User Identity is supported by Integration with Microsoft Active Directory as the user identity source as shown <u>here.</u>
2081 2082 2083		d.	Profiling and Compliance: Configuration of posture policies to mandate allowance of specific applications is shown <u>here</u> . For NCCoE lab configuration, AnyConnect is enabled on endpoints in order to achieve accurate posture on enterprise-supplied endpoints.
2084		e.	Segmentation: Cisco ISE supports configuration for segmentations as shown here.
2085 2086 2087 2088		f.	BYOD: Cisco ISE is used as a tool that allow employees to securely use either employer- provided or personal devices on the enterprise network. Cisco ISE is used to protect network services and enterprise data by authenticating and authorizing users (employees and contractors) and their devices. The BYOD configuration is shown <u>here</u> .

#### 2089 8.13.1 Integrations

- 2090 Cisco ISE was provisioned with a service account to pull user and device attributes from Workspace ONE
- 2091 UEM for use in policy decisions. Configure this integration in **Administration/Network**
- 2092 **Resources/External MDM** using the <u>ISE Admin Guide</u>.
- 2093 Cisco ISE and Cisco Secure Network Analytics (SNA) are integrated to allow SNA to provide network
- visibility information to ISE to enforce policies. Integration configuration was completed by creating a
   client for SNA under Administration/pxGrid Services/Client Management.

### 2096 8.14 Cisco Secure Workload (CSW – Formerly Tetration)

Cisco Secure Workload (formerly known as Cisco Tetration) is designed to address application security
 challenges by providing comprehensive workload protection and bringing security closer to applications
 and tailoring the security posture based on the application behavior. For configuration, this document
 references specific sections of the <u>Cisco Secure Workload User Guide</u>.

#### 2101 8.14.1 Configuration

For this build, the NCCoE used the SaaS-based version of CSW. To start, contact a Cisco representative to procure an instance of CSW.

- A prerequisite for CSW is to gather and document the organizational layout of your enterprise in the form of security boundaries. Leverage the <u>Cisco Secure Workload Quick Start Guide</u> to
   familiarize the CSW design using scopes and labels.
- 2107
   2. Once a basic understanding of CSW is achieved, a CSW administrator can leverage <u>labels</u> to
   2108
   2109
   additional metadata tags within the inventory database in CSW.
- Once logged into CSW, leverage the first-time user-experience (FTUE) wizard to define the scope and inventory. Note: This step was not necessary, but it was leveraged to have a baseline understanding of how scopes and inventory function.
- 4. In parallel to a scope tree being defined in CSW, users can begin installing <u>software agents</u> on all workloads (resources) to be managed by CSW. Once in the "Software Agents Installer" page, the user will be guided through the process of selecting the OS platform to download. See the 
  Deploying Software Agents page for support platforms, requirements, and install instructions.
- 5. With agent installations completed on the workloads, CSW will begin collecting network flow
  data along with OS information about these resources. Ensure a minimum of at least a week or
  so if you want to take advantage of CSW's ability to auto-generate microsegmentation policies
  using the solution's built-in machine learning algorithms.
- 6. Once agents are installed and your scope tree is set up properly, <u>create policies</u>. The policy
  analysis phase is intended to be an iterative process that allows a CSW user to adjust policies as
  necessary.
- 2124 7. Once you feel the policies are good enough to enforce, <u>enable enforcement</u> of those policies.
  2125 Alerts should be created for escaped policies. CSW can, at a minimum, generate internal alerts,
  2126 but best practice suggests that these alerts should also be sent to a northbound platform like a
  2127 SIEM.

### 2128 8.15 Cisco Secure Network Analytics (SNA – Formerly Stealthwatch)

2129 Cisco Secure Network Analytics (SNA) uses machine learning, behavioral modeling, and threat

intelligence to provide network visibility. For this build, we mainly leverage NetFlow data collected fromnetwork devices to feed to SNA.

#### 2132 8.15.1 Installation

- 2133 The components of SNA are installed on-premises in the virtual environment for Enterprise 2.
- Installation is completed using the <u>Virtual Edition Appliance Installation Guide 7.4.1</u>. Specific sections
   from that guide are noted below.
- 21361. Prior to installing SNA, check all resource requirements and prerequisites (General Deployment2137Requirements and Section 1).
- 2138 2. Install the virtual edition for VMware vCenter (Section 3a).
- 2139 3. Configure the SNA manager and the Flow Sensor (Section 4).
- 2140 8.15.2 Configuration
- 2141 Use the <u>Cisco Secure Network Analytics System Configuration Guide</u> to configure the SNA.
- 21421. Configure SNA to retrieve information for network appliances. This is performed by the Flow2143Sensor, which is a separate appliance managed by the SNA manager.
- Configure network components to send NetFlow data to the SNA Flow Sensor. Note: There are
   tools that can build the configuration for network devices.
- 2146 3. Configure hosts and host groups to be used by policies and response management.
- 2147 4. Configure policies to monitor various host groups.
- 21485. Configure response management to perform specific actions based on policies. Response2149management configuration provides information to Cisco ISE to act on those policies.

#### 2150 8.15.3 Integration

Integrate with Cisco ISE to inform ISE of actions it needs to take to allow or deny communications based
 on the policies. To integrate with ISE, follow the configuration instructions shown here.

### 2153 8.16 Cisco Secure Endpoint (CSE – Formerly AMP)

- Cisco Secure Endpoint (CSE) is a cloud-based solution that leverages connectors that are deployed on
   endpoints to protect against vulnerabilities. The configuration steps below leverage the <u>Cisco Secure</u>
   Endpoint User Guide.
- 2157 1. Work with your Cisco representative to procure an instance of Cisco Secure Endpoint.
- 2158 2. Ensure administrator accounts are created and users have access to the AMP portal.

2159	3.	Develop policies for all your different endpoints. For this build, endpoints include Windows,
2160		macOS, Linux, iOS, and Android devices. By default, CSE has various default policies that can be
2161		applied to endpoints once these endpoints are configured. For this build, we began by
2162		leveraging the Audit mode to allow CSE to gather information and learn about the endpoints.
2163		After several weeks, we enabled the Enforce mode to block malicious traffic. Refer to Chapter 5
2164		of the User Guide.

- Note that Groups can be configured to apply policies for different types of endpoints. Refer to
   Chapter 6.
- 2167 5. Exclusions for the types of applications that you want to exclude from policies can be
  2168 configured. You can create custom exclusions or view the Cisco-maintained exclusions list. Refer
  2169 to Chapter 4.
- 6. Download connectors from CSE and deploy them to endpoints. Once in the
  Management/Download Connector page, links will be available for download or for a URL for
  the various endpoints that CSE supports. The URL can be provided to the user to download, or it
  can be downloaded and deployed via an enterprise tool. Refer to Chapters 8-12 for connector
  installation.

#### 2175 8.16.1 Integrations

2176 CSE integrates with ISE to provide endpoint threat detection information to ISE to act on. The process

- 2177 for integration begins with Cisco ISE. From the ISE Administration menu, click on the Third Party
- 2178 Vendors link. Click Add and click Cisco AMP as the vendor. Input all information. Once added, there will
- 2179 be a status link stating "Ready to configure." Click on it and follow instructions to configure CSE.

#### 2180 8.17 Palo Alto Networks - Panorama

- Palo Alto Networks' Panorama provides centralized management and monitoring of the Palo Alto
  Networks NGFWs. For this build, it was leveraged to integrate with Cisco ISE in addition to managing the
  NGFWs.
- 21841.Deploy Panorama in the virtual environment using Palo Alto Networks' prerequisite2185recommendations. Follow each step of the deployment to install the VM, register Panorama and2186install licenses, perform updates, add firewalls as managed devices, and create templates and2187device groups.
- 2188 2. Complete all configuration of the firewalls on Panorama's console.
- For remote access, the NGFW is leveraged to check compliance of user devices. <u>Create the</u>
   <u>configuration</u> for compliance checks and add it to the VPN policy created for users. Note:
   Integration with ISE needs to be completed prior to this step.

#### 2192 8.17.1 Integration with Cisco ISE

For this integration, the user logging onto the Palo Alto Networks VPN will leverage ISE for
authentication. The Palo Alto Networks NGFW will perform device compliance checks prior to
completing the authentication. To integrate with Cisco ISE, leverage the instructions to <u>enable delivery</u>
of vendor-specific attributes to RADIUS server.

## 2197 9 Enterprise 3 Build 3 (E3B3) Product Guides

This section of the practice guide contains detailed instructions for installing, configuring, and
integrating all the products used to implement E3B3. For additional details on E3B3's logical and physical
architectures, please refer to Volume B. Build 3 was built on top of Build 2 and all the components in
Build 2 were used in this build. For E3B2's configuration, please refer to Section <u>6</u>. Below are the
additional components added to Build 3.

### 2203 9.1 Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based solution that detects identity-based threats in hybrid
 environments. Using signals collected from AD, it will discover compromised identities and alert on
 suspicious user actions. To deploy Defender for Identity, use the following steps:

- 2207 1. Review the <u>prerequisites</u> before deploying Defender for Identity.
- 2208 2. <u>Configure the necessary Windows event logs</u> to enable appropriate detections.
- 2209 3. <u>Create a directory service account</u> that will be used by Defender for Identity in the domain.
- 2210 4. <u>Download</u> and install the <u>Defender for Identity sensor</u>.
- 2211 5. <u>Configure sensor settings</u> and <u>validate installation</u>.

#### 2212 9.2 Microsoft Defender for Office

2213 Microsoft Defender for Office 365 provides protection from malware, phishing, spam, unsafe links and 2214 attachments, and other related threats. To configure Defender for Office 365, use the following steps:

- 2215 1. Configure the Standard Preset Security Policy for Defender for Office 365.
- 2216 2. <u>Configure anti-phishing policies</u>.
- 2217 3. <u>Configure anti-malware policies</u>.
- 2218 4. <u>Configure safe attachment protections in Office 365</u>.
- 2219 5. <u>Set up safe links protections</u>.

#### 2220 9.3 Purview Information Protection

- Purview Information Protection discovers, labels, classifies, and protects data in the cloud and onpremises. It aims to provide data governance and protection throughout the enterprise.
- 2223 <u>Discover your sensitive data</u> using the <u>examples shown here</u>. To discover sensitive data on-premises,
   2224 you will need to deploy the Information Protection Scanner.

#### 2225 9.3.1 Information Protection Scanner

- 2226 Information Protection Scanner is used to discover sensitive data in an on-premises environment.
- 2227 Use the information here to install and configure the Information Protection Scanner.

#### 2228 9.3.2 Purview DLP

- Purview Data Loss Prevention (DLP) reduces the risk of unauthorized information disclosure and reduces
  the likelihood that sensitive data will be shared inappropriately. Data loss prevention policies specify the
  category of data to protect and the type of restrictions that are applicable.
- 2232 Use the information here to create and deploy DLP policies.

#### 2233 9.4 Entra Permissions Management

- Entra Permissions Management provides visibility and control of an identity's permissions in Amazon
  Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). It identifies a user's
  permissions across all three cloud platforms, determines which permissions are not required based on
  usage, and can be configured to reduce the permissions to only those being used.
- 2238 1. Enable Entra Permissions Management.
- 2239 2. Onboard an AWS Account.
- 2240 3. <u>Onboard an Azure Subscription</u>.
- 2241 4. <u>Onboard a GCP Project</u>.
- 5. Add an AWS Account, Azure Subscription, and GCP Project after onboarding is complete.
- 2243 6. To view inactive users or users with overprovisioned permissions, click <u>here</u>.
- 2244 7. To revoke unused permissions, click <u>here</u>.

#### 2245 9.5 Azure Virtual Desktop

Azure Virtual Desktop is a desktop and application virtualization service that delivers the full Windows experience over HTTPS to a connecting client. Use the following steps to set up Azure Virtual Desktop:

- 1. Understand prerequisites prior to deployment.
- 2249 2. Create and connect to an Azure Virtual Desktop.

#### 2250 9.6 Intune VPN Tunnel

- The Intune VPN Tunnel is a VPN solution that provides access to internal network resources from
   iOS/iPad and Android devices using modern authentication and conditional access. Use the following
   steps to set up the Intune VPN Tunnel:
- 2254 1. <u>Understand the prerequisites</u> prior to deployment.
- 2255 2. Install and configure Intune VPN Tunnel.

#### 2256 9.7 Azure Arc

- Azure Arc is an Azure cloud platform that provides governance and management of on-premises servers,
   containers, and other related infrastructure components using Azure policies and management tools. It
   essentially extends governance to resources existing in on-premises environments. Use the following
   steps to set up Azure Arc:
- 2261 1. <u>Understand network requirements</u>.
- 2262 2. <u>Understand Azure Arc-enabled servers</u>.
- 2263 3. <u>Onboard a Windows server</u>.
- 2264 4. <u>Onboard a Linux server</u>.

#### 2265 9.8 Azure Automanage

- Azure Automanage automatically configures onboarded servers with Azure best practices, monitors
  those servers, and remediates them when any configuration drift occurs. With Automanage, you must
  create a configuration profile for the server.
- 2269 Enable Azure Automanage for VMs in Azure portal.

#### 2270 9.9 Microsoft Sentinel Playbooks

- 2271 Playbooks in SOAR systems enable automated responses to address detected threats in an environment.
- 2272 In this build, a Sentinel playbook was created to revoke or terminate sessions of users when the risk

evaluated for that session was deemed high. You can create playbooks with the information found atthe create a playbook link.

#### 2275 9.10 Microsoft Privileged Access Workstation

- 2276 A privileged access workstation is a hardened workstation that includes security controls that lock down
- local administrative access and tools to only what is required for performing sensitive tasks. Use the
- 2278 information at <u>configure a privileged access workstation</u> to do so.

## **10 Enterprise 4 Build 3 (E4B3) Product Guides**

- 2280 This section of the practice guide contains detailed instructions for installing, configuring, and
- 2281 integrating all the products used to implement E4B3. For additional details on E4B3's logical and physical
- architectures, please refer to Volume B.

#### 2283 10.1 IBM Security Verify

- IBM Security Verify is a cloud-based SaaS that operates as the Policy Engine and ICAM for Enterprise 4
   and provides a variety of services including SSO, multifactor and passwordless authentication, adaptive
   access, identity lifecycle management, and identity analytics.
- 2287 10.1.1 Setup
- 2288 IBM provisioned a new instance of IBM Security Verify for this build.

#### 2289 10.1.2 Integration with Active Directory

To integrate with Active Directory, an IBM Security Verify Bridge agent was installed on an on-premises
 server running Microsoft Windows Server 2019. To replicate this process, follow the instructions in the
 <u>official IBM documentation</u>. Completing this integration will add AD as an available identity source in
 IBM Security Verify.

#### 2294 10.1.3 Configuration

2300

- For this build, configuration focused on several areas. First, the integration with applications/resources needed to be configured. With the AD integration completed, users, groups, and attributes can now be managed, and authentication methods can be set up. Finally, access policies can be defined and implemented.
- 2299 1. Add/configure connected applications.
  - a. Begin the application configuration using the official IBM documentation.

- b. In this build, SAML was configured to allow for user authentication. Follow the <u>official</u>
   IBM documentation for instructions on this step.
- Users, groups, and attributes were managed using the <u>official IBM documentation</u>. This allowed
   the configured policies to make decisions using user and group attributes.
- 23053. Create security policies. There are a variety of pre-built policies available that can be utilized in2306different scenarios. For example, one of the pre-built policies will deny access to any device that2307is not in compliance with MaaS360 policy. Custom policies can also be built based on a range of2308criteria, including user and group attributes. Additional information on creating/editing policies2309can be found in the official IBM documentation.

#### 2310 10.2 IBM Security Trusteer

2311 IBM Security Trusteer is a cloud-based SaaS that integrates with IBM Security Verify and uses cloud-

2312 based intelligence, AI, and machine learning (ML) to holistically identify new and existing users while

2313 improving the overall user experience by reducing the friction created with traditional forms of MFA.

2314 Within a ZTA, Trusteer acts as a risk engine that improves the efficacy of policy decisions enforced by

- 2315 various identity and access management solutions.
- 2316 10.2.1 Integration with IBM Security Verify

To act as a risk engine in this build, IBM provisioned a new Trusteer instance and linked it with IBM
Security Verify. This action must be completed by an IBM representative.

#### 2319 **10.3 IBM Security MaaS360**

IBM Security MaaS360 cloud-based SaaS provides endpoint management capabilities for both user
 workstations and user mobile devices through agents installed on each endpoint, supporting both BYOD
 and corporate-owned device usage.

- 2323 10.3.1 Setup
- 2324 IBM provisioned a new cloud-based instance of IBM Security MaaS360 for this build.

#### 2325 10.3.2 Configuration

- The majority of MaaS360 configuration for this build was completed by building policies to apply to useror device groups.
- Configure user and device groups. Group configuration instructions can be found in the <u>official</u>
   <u>IBM documentation</u>.

- Build and apply policies to groups. Instructions for building these policies can be found in the
   official IBM documentation.
- Once these groups have been built and policies have been applied, policy enforcement can
   begin.
- 2334 10.4 IBM Security QRadar XDR
- 2335 For installation, configuration, and integration instructions, refer to <u>Section 2.9</u>.
- 2336 10.4.1 Integration with IBM Security MaaS360
- 2337 QRadar was integrated with MaaS360 using the <u>official IBM documentation</u>.
- 2338 10.4.2 Integration with IBM Security Verify
- 2339 QRadar was integrated with Verify using the official IBM documentation.

#### 2340 10.5 IBM Security Guardium

IBM Security Guardium is a data security platform that protects sensitive and regulated data across with
 compliance enforcement, sensitive data discovery, data encryption, and risk reduction. This build
 utilized two Security Guardium products: Guardium Data Protection and Guardium Data Encryption.

#### 2344 10.5.1 IBM Security Guardium Data Protection

Guardium Data Protection is a unified data security solution that provides data discovery and
classification, data activity monitoring and analytics, real-time response to threats, and automated
compliance auditing and reporting. For this build, a single Guardium Data Protection appliance was
deployed in VMware to serve as a data collector.

- 2349 10.5.1.1 Appliance Installation and Configuration
- 2350 1. Create a new virtual machine using <u>IBM's recommended requirements</u>.
- Boot from the IBM-provided Guardium Data Protection ISO using the <u>IBM Guardium installation</u>
   guide.
- 2353
   3. Choose standard installation at the boot prompt. Once the install completes, on first boot the
   appliance will ask the user to choose Collector or Aggregator mode. Choose Collector.
- 2355 4. After the installer finishes, log into the appliance console using the default credentials.
- 2356 5. Complete the initial setup and configuration for the appliance using the <u>IBM Guardium setup</u>
   2357 <u>guide</u>. Reboot the appliance when configuration changes are complete.

- 2358
   6. Log into the appliance command line and add a QRadar instance as a remote logger with the
   2359
   <u>command</u>.
- **7.** Log into the Guardium Data Protection web console at https://<ip address>:8443
- 2361 8. Confirm remote log forwarders are configured by clicking on Tools | Tools and Views | Remote
   2362 Loggers. Each daemon should have a green checkmark.
- 2363 10.5.2 IBM Security Guardium Data Encryption
- Guardium Data Encryption is a data encryption suite that can safeguard files and databases, provide in application encryption, manage encryption keys, and enforce access policies for data.
- 2366 10.5.2.1 Appliance Installation & Configuration
- The Guardium Data Encryption platform for this build requires a local appliance installation on theEnterprise 4 VMware farm.
- 2369 1. Obtain the latest .ova image from IBM for the IBM Security CipherTrust Manager software.
- 2370
   2. Follow the install guide to deploy the IBM Security CipherTrust Manager on a new virtual machine with the cloud-init configuration enabled to set the static IP address.
- On boot, access the assigned IP address of the CipherTrust Manager with a web browser and
   enter a user's public SSH key for administrator access. The CipherTrust Manager is not functional
   until this key is entered.
- 2375 4. Change the default administrator password.
- 2376 5. Under Admin Settings | Licensing, enter a license key or click on Start CipherTrust Evaluation to
   2377 license the appliance.
- 2378 10.5.2.2 S-TAP Installation and Configuration
- Install the appropriate S-TAP agent on any client machines that require monitoring. For this
   build the Windows S-TAP agent was deployed on the Microsoft SQL Server Express 2019 using
   <u>IBM's install guide</u>. The S-TAP agent appliance IP address used during setup is from the IBM
   Guardium Data Protection Collector configured in the previous section.
- Confirm S-TAP control from the IBM Guardium Data Protection Collector web console by
   accessing the <u>S-TAP control menu</u> and verifying the client machine appears with a green
   checkmark.
- 2386 10.5.2.3 Client Machine Setup and Configuration
- 2387 The client machine for this build is a Windows 2019 Server running Microsoft SQL Server Express 2019.

2388 2389	1.	From the Guardium Data Encryption web console, create a registration token for the client machine <u>following the steps in the CipherTrust Manager Administration Guide</u> .			
2390	2.	Copy and save the registration token created in step 1.			
2391 2392 2393	3.	From the Guardium Data Encryption web console, manually create a new client entry for the client machine following the steps in <u>the CipherTrust Data Encryption Guide</u> . For this build, password registration was used to register the client with a user-generated password.			
2394 2395 2396	4.	Install the CipherTrust Transparent Encryption client software on the client machine. Choose <b>Register CipherTrust Transparent Encryption Now</b> at the end of the installation. These parameters were used for this build:			
2397		a. Components: File System			
2398		b. Host name of key manager: IP/DNS of the Guardium Data Encryption Appliance			
2399		c. Enable hardware association and LDT feature.			
2400 2401		d. On the host screen, paste the ASCII token from Step 2 into the <b>Registration Token</b> field. Leave the remaining fields blank.			
2402		e. Click <b>Next</b> and then <b>Finish</b> once the client is registered. Restart the client machine.			
2403	10.5.2	2.4 GuardPoint Configuration			
2404 2405 2406	A Guar encryp Guardj	dPoint specifies the list of folders that contain paths to be protected. Access to files and tion of files under the GuardPoint are controlled by security policies. More information on points can be found in the <u>Guardium Data Encryption GuardPoint Guide</u> .			
2407 2408 2409	1.	Create two user sets, one for full and one for limited/no access using the <u>CipherTrust</u> <u>Transparent Encryption Guide</u> . For this build, the Admins User Set will have no access to a protected directory while the AppUsers User Set will have full access.			
2410 2411	2.	Create a new Standard Policy using the <u>CipherTrust Transparent Encryption Guide</u> . Name it "File Access Policy" and create Security rules for file access based on a User Set.			
2412 2413	3.	Follow the <u>CipherTrust Transparent Encryption Guide</u> using Step 2 to create a new Key Rule and a new encryption key.			
2414 2415	4.	Once the policy is created, check the order of the Key Rules from the Policies Menu on the web console. If they are out of order, reorder them according to Step 2.			
2416	5.	Create "encrypted" and "unencrypted" folders on the client machine to test access policies.			
- 2417 6. From the web console, create an AutoDirectory GuardPoint using the <u>CipherTrust Transparent</u>
- 2418 <u>Encryption Guide</u>. Use the Policy created in Step 2 and point the GuardPoint to the "encrypted"
   2419 folder created in Step 5.
- 2420 7. Confirm access is restricted by logging into the client machine with a user from each UserSet.

## 2421 **10.6** IBM Cloud Pak for Security (CP4S)

- The IBM Cloud Pak for Security (CP4S) platform enables the integration of existing security tools and provides understanding and management of threats in the environment.
- 2424 10.6.1 Installation
- 2425 Refer to Section <u>2.8</u> for CP4S installation instructions.
- 2426 10.6.2 CP4S and QRadar Integration
- 2427 For this build, QRadar was integrated into CP4S as a data source for events from other resources.
- 2428 1. Install the <u>QRadar SOAR app plugin</u> on the QRadar instance.
- Configure the QRadar SOAR app plugin to connect to the CP4S instance using an API key. Follow
   the instructions in the <u>IBM QRadar SOAR app plugin Configuration Guide</u>.
- An IBM Edge Application Gateway must be installed first to connect CP4S to QRadar. Install the
   Edge Gateway appliance in your virtual environment <u>following the IBM installation guide</u>.
- 2433 4. <u>Pair the IBM Cloud Pak for Security account with the Edge Gateway appliance</u>.
- 2434 5. <u>Finish creating the Edge Gateway with the pairing information from Step 4.</u>
- 2435 6. Follow the <u>IBM guide to add QRadar as a data source</u> to CP4S.

## 2436 10.6.3 CP4S Playbooks

A CP4S Playbook is a set of rules, conditions, business logic, workflows, and tasks used to respond to a
 case/incident. For this build, IBM provided a test playbook to disable accounts in IBM Security Verify
 when multiple failed logins were detected in QRadar. Playbook design suggestions and instructions can
 be found in the IBM Cloud Pak for Security SOAR Guide.

## 2441 **10.7 IBM Cloud**

IBM Cloud provides compute, networking, and storage services that enable the creation of an enterpriseIT infrastructure by subscribers.

- Start with setting up the IPsec tunnel between IBM Cloud and the on-prem data center as
   shown here.
- 2446 2. Build the components in the IBM Cloud using the <u>architecture</u> and <u>configuration guide</u>.
- 2447 **10.8 Tenable.io**
- 2448 For installation, configuration, and integration instructions, refer to Section 2.10.
- 2449 **10.9 Tenable.ad**
- 2450 For installation, configuration, and integration instructions, refer to <u>Section 2.11</u>.

#### 2451 **10.10 Tenable NNM**

- 2452 For installation, configuration, and integration instructions, refer to <u>Section 2.12</u>.
- 2453 10.11 Mandiant Security Validation (MSV)
- 2454 For installation, configuration, and integration instructions, refer to <u>Section 2.13</u>.
- 2455 10.12 DigiCert CertCentral
- 2456 For installation, configuration, and integration instructions, refer to <u>Section 2.14</u>.

#### 2457 10.13 Palo Alto Networks Next Generation Firewall

- 2458 For installation, configuration, and integration instructions, refer to <u>Section 3.5</u>.
- 2459 **10.14 VMware**
- 2460 The VM ware environment was used for on-premises virtualized infrastructure hosting enterprise
- resources and consisted of three vSAN clusters. The VM ware vSAN installation and configuration guidecan be found here.

# 2463 11 Enterprise 1 Build 4 (E1B4) Product Guides

- 2464 This section of the practice guide contains detailed instructions for installing, configuring, and
- integrating all the products used to implement E1B4. For additional details on E1B4's logical and physicalarchitectures, please refer to Volume B.

## 2467 **11.1 Appgate**

The Appgate SDP solution has been designed with the intent to provide all the critical elements of zero trust. The Appgate SDP has a controller that offers PA and PE functionality, and gateways that offer PEP functionality. By providing highly performant, scalable, secure, integrated, and cloaked zero trust access, Appgate SDP is able to ensure that the correct device and user (under the appropriate conditions at that moment in time) are connected.

## 2473 11.1.1 Appgate Installation and Configuration

Appgate components for deployment are the controller and gateway. Prior to installation, admins
 should understand the <u>pre-installation considerations</u> to deploy Appgate. These considerations include
 browser compatibility, network setup, identity providers, and DNS.

- For this build, an Appgate controller and gateway are deployed on-prem as well as in the AWS IaaS cloud. Both the controller and gateway are deployed on the same server on-prem and in AWS.
- For the on-prem installation, we used the instructions in the <u>Appgate SDP Installation from ISO into</u>
  VMware guide.
- 2481 For the Appgate install in AWS, we used the <u>Appgate SDP for AWS Deployment Guide</u>.
- 2482 After installation, the initial configuration is completed via <u>CLI (command-line interface) on the</u>

2483 <u>controller</u>. Note: Gather various information about the network and IP addresses that are needed to

2484 configure the controller. Once the configuration is completed, an administrator can gain access to the

- 2485 GUI via https://"controller-ip-address":8443 on a browser.
- 2486 Gateway configuration: As mentioned earlier, the gateway is deployed on the same server as the 2487 controller. Once logged into the controller, deploy the gateway.
- For this build, policies were created to allow users to access various resources on-premises and in the
   AWS laaS environment for Enterprise 1. We leveraged the following tags, conditions, entitlements, and
   policies to allow employees access to all resources and contractors to certain resources.
- 2491Tags were used to differentiate which users were allowed access. Tags were created for2492employees, contractors, and mobile devices. Tags can be created when configuring a policy.
- 2493 Conditions were created for employees and contractors.
- Check endpoints and resources for compliance
- 2495 Appgate delegates to Ivanti to validate compliance for mobile devices
- 2496 Do a 10-minute reauthentication for high-value resources
- Validate user attributes pulled from Radiant Logic

- An <u>entitlement</u> was created for four resources and applied with the appropriate tags. Resource1
   and Resource2 were on-premises. Resource3 and Resource4 were in AWS. The employee tag
   was applied to all four resources. The contractor tag was applied to Resource2 and Resource4.
   Contractors did not have access to Resource1 and Resource3.
- 2502 Policies were created for employees and contractors.
- The employee policy leveraged an identity provider for authentication, and validated that
   the user was an employee based on information retrieved from Radiant Logic. The
   employee tag was applied to this policy. Therefore, any entitlements and conditions
   applied with the same tag were applied to this policy.
- The same logic was applied to the contractor policy.

#### 2508 11.1.2 Appgate Clients

Appgate has clients for end users logging to desktop, laptop, and mobile devices for different OSes
including Windows, Linux, macOS, iOS, and Android. <u>Installing clients</u> require downloads for all clients'
software, which are available <u>here</u>.

- Headless clients were also installed to protect resources. From the same download page above, the
  Windows client is the same for both workstations/laptops and servers. For Linux clients, use the
  "Ubuntu Headless Client v6.x.x" instead of the full client. Instructions for installing <u>Windows</u> and <u>Linux</u>
- 2515 both use the command line.

#### 2516 11.1.3 Appgate Integrations

- 2517 For this build, Appgate integrates with Okta, Radiant Logic, Ivanti, and IBM.
- 2518 For integration with Okta, which is used for authentication and authorization of the user to log in to the
- 2519 Appgate client, follow the <u>SAML configuration</u> instructions to create an identity provider in Appgate.
- 2520 Note: Certain information will be provided by Okta, so the integration configuration within Okta should
- 2521 be completed prior to this configuration.
- 2522 For integration configuration with Radiant Logic, the purpose is to identify users and additional
- attributes to verify compliance of a user. One attribute being leveraged is the groups attribute so
- 2524 Appgate can identify whether the user is an employee or contractor. We also leveraged several
- 2525 attributes such as BreakGlassScore, ClearanceValue, RiskLevel, and BehavorialRiskScore. A User Claim
- 2526 <u>Script</u> was leveraged to pull these attributes from Radiant Logic. If the user does not meet certain scores
- 2527 for these attributes, the user is denied entitlements to resources.
- 2528 For integration with Ivanti, Appgate is trusting Ivanti's claim of whether a device is complaint or not. To
- 2529 perform this integration, a User Claim Script was created. Note: Knowledge of JavaScript is required for
- this configuration.

To manage Appgate logs for large deployments, Appgate recommends using a LogForwarder to send logs to your log server or SIEM. For integration with IBM QRadar, we <u>configured the LogForwarder</u> to send logs to IBM QRadar.

## 2534 11.2 Okta Identity Cloud

For this build, the integration between Okta and Ivanti was disabled in Okta Identity Cloud. Users logging into a resource are authenticated via Okta with a password for the first factor and Okta Verify for the second factor. Users logging into AppGate SDP also use Okta for authentication. Use the link for <u>integration with AppGate</u> to configure Okta. Note: Information such as Single Sign-on URL, Issuer, and other data created here are needed for the Appgate integration configuration.

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

## 2542 11.3 Radiant Logic RadiantOne

Additional attributes were added to the RadiantOne solution. These attributes allow other zero trust
tools to create more granular policies for access. Within the Directory Namespace, we created
namespaces for Clearance, Data Governance, Risk, and Training. Information pertaining to these
categories was imported via flat files for the purpose of this build. For configuration instructions, refer to
RadiantOne v7.4.4 Namespace Configuration Guide. We also updated RadiantOne's configuration with a
<u>Global Database View</u> of users combining these attributes with the AD directory and HR database. We
leveraged the <u>Global Identity Builder</u> to perform this.

For integration with Appgate, a user ID was created in Radiant Logic as a service account for Appgate to be able to retrieve attributes. To create this, follow the instructions from Section 2.2.3.

## 2552 11.4 SailPoint IdentityIQ

2553 No changes were made from Build 1. Refer to Section 2.3.

#### 2554 **11.5** Ivanti Neurons for UEM

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

#### 2558 11.6 IBM Security QRadar XDR

2559 For installation, configuration, and integration instructions, refer to <u>Section 2.9</u>.

#### 2560 **11.7 Tenable.io**

- 2561 For installation, configuration, and integration instructions, refer to Section <u>2.10</u>.
- 2562 **11.8 Tenable.ad**
- 2563 For installation, configuration, and integration instructions, refer to <u>Section 2.11</u>.
- 2564 **11.9 Tenable NNM**
- 2565 For installation, configuration, and integration instructions, refer to <u>Section 2.12</u>.

## 2566 **11.10** Mandiant Security Validation (MSV)

- 2567 For installation, configuration, and integration instructions, refer to <u>Section 2.13</u>.
- 2568 11.11 DigiCert CertCentral
- 2569 For setup and usage instructions, refer to <u>Section 2.14</u>.

#### 2570 **11.12** AWS laaS

- 2571 Amazon Web Services is a cloud computing platform provided by Amazon that includes a mixture of
- 2572 IaaS, PaaS, and SaaS offerings. This section describes the setup of AWS IaaS resources to serve as a2573 public/private cloud host.
- For details on the logical architecture of the AWS environment, please refer to Volume B, Section4.4.9.1.

## 2576 11.12.1 AppGate Controller Configuration

- 2577 Ensure the on-prem controller can reach the AWS segment on which the new controller will be installed.
- 2578 This controller will need to communicate with the on-prem controller. To install the controller in AWS,
- 2579 follow the prerequisites outlined in the <u>AWS Step by Step guide</u> and the steps to provision AWS resource
- 2580 for a new appliance (up to Step 1 of the guide). Once these steps are completed, log in to the on-prem
- Appgate controller user interface (UI) and follow the <u>Configuring a new appliance</u> instructions to deploy the AWS controller.

## 2583 11.13 Zimperium Mobile Threat Defense (MTD)

2584 For installation, configuration, and integration instructions, refer to Section <u>2.10</u>.

# 2585 Appendix A List of Acronyms

AAD	(Microsoft) Azure Active Directory
ACL	Access Control List
AD	Active Directory
AG	(Okta) Access Gateway
ΑΡΙ	Application Programming Interface
APM	(F5) Access Policy Manager
APNs	Apple Push Notification service
AWS	Amazon Web Services
BYOD	Bring Your Own Device
CA	Certificate Authority
CEF	Common Event Format
CLI	Command Line Interface
CP4S	(IBM) Cloud Pak for Security
CRADA	Cooperative Research and Development Agreement
CSE	Cisco Secure Endpoint
CSR	Certificate Signing Request
CSW	Cisco Secure Workload
DLP	Data Loss Prevention
DN	Domain Name
DNS	Domain Name System
E1B1	Enterprise 1 Build 1
E1B2	Enterprise 1 Build 2
E1B3	Enterprise 1 Build 3
E1B4	Enterprise 1 Build 4
E2B1	Enterprise 2 Build 1

E2B3	Enterprise 2 Build 3
E3B1	Enterprise 3 Build 1
E3B2	Enterprise 3 Build 2
E3B3	Enterprise 3 Build 3
E4B3	Enterprise 4 Build 3
EDR	Endpoint Detection and Response
EIG	Enhanced Identity Governance
EO	Executive Order
FQDN	Fully Qualified Domain Name
FTUE	First-Time User-Experience
GCP	Google Cloud Platform
HDAP	High-Availability Directory Access Protocol
HR	Human Resources
laaS	Infrastructure as a Service
laC	Infrastructure as Code
ICAM	Identity, Credential, and Access Management
IdP	Identity Provider
IP	Internet Protocol
ISE	(Cisco) Identity Services Engine
ІТ	Information Technology
ITL	Information Technology Laboratory
LDAP	Lightweight Directory Access Protocol
MAM	Mobile Application Management
MDM	Mobile Device Management
MES	(Lookout) Mobile Endpoint Security
MFA	Multi-Factor Authentication

ML	Machine Learning
MSV	Mandiant Security Validation
MTD	Mobile Threat Defense
NCCoE	National Cybersecurity Center of Excellence
NGFW	Next-Generation Firewall
NIST	National Institute of Standards and Technology
NNM	(Tenable) Nessus Network Monitor
NSG	Network Security Group
NTP	Network Time Protocol
OS	Operating System
OU	Organizational Unit
OVA	Okta Verify App, Open Virtual Appliance
РА	Policy Administration
PaaS	Platform as a Service
PDP	Policy Decision Point
PE	Policy Engine
PEP	Policy Enforcement Point
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SDP	Software-Defined Perimeter
SIEM	Security Information and Event Management
SNA	(Cisco) Secure Network Analytics
SOAR	Security Orchestration, Automation, and Response
SP	Special Publication, Service Provider
SSH	Secure Shell
SSL	Secure Sockets Layer

SSO	Single Sign-On
SSPR	Single Sign-On Password Reset
ТСР	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Account Control
UDP	User Datagram Protocol
UI	User Interface
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VNET	Virtual Network
VPC	Virtual Private Cloud
VPN	Virtual Private Network
ZCC	Zscaler Client Connector
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access
ZSO	(Ivanti) Zero Sign-On
ZTA	Zero Trust Architecture