# **NIST SPECIAL PUBLICATION 1800-28C**

# Data Confidentiality: Identifying and Protecting Data Against Data Breaches

Volume C: How-To Guides

William Fisher National Cybersecurity Center of Excellence NIST

R. Eugene Craft Michael Ekstrom Julian Sexton John Sweetnam The MITRE Corporation

McLean, Virginia

December 2023

DRAFT

This publication is available free of charge from <a href="https://www.nccoe.nist.gov/data-confidentiality-identifying-and-protecting-assets-against-data-breaches">https://www.nccoe.nist.gov/data-confidentiality-identifying-and-protecting-assets-against-data-breaches</a>



# 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 sta-
- 5 tus or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it in-
- 6 tended 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 1800-28C, Natl. Inst. Stand. Technol.
- 14 Spec. Publ. 1800-28C, 86 pages, (December 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>ds-nccoe@nist.gov</u>
- 19 Public comment period: December 13, 2023 through January 15, 2024
- 20 As a private-public partnership, we are always seeking feedback on our practice guides. We are
- 21 particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you
- 22 have implemented the reference design, or have questions about applying it in your environment,
- 23 please email us at ds-nccoe@nist.gov.
- 24 All comments are subject to release under the Freedom of Information Act.

25	National Cybersecurity Center of Excellence
26	National Institute of Standards and Technology
27	100 Bureau Drive
28	Mailstop 2002
29	Gaithersburg, MD 20899
30	Email: <u>nccoe@nist.gov</u>

# 31 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

46 <u>https://www.nist.gov.</u>

# 47 NIST CYBERSECURITY PRACTICE GUIDES

- 48 NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity
- 49 challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the
- 50 adoption of standards-based approaches to cybersecurity. They show members of the information
- 51 security community how to implement example solutions that help them align with relevant standards
- and best practices, and provide users with the materials lists, configuration files, and other information
- 53 they need to implement a similar approach.
- 54 The documents in this series describe example implementations of cybersecurity practices that
- 55 businesses and other organizations may voluntarily adopt. These documents do not describe regulations
- 56 or mandatory practices, nor do they carry statutory authority.

# 57 ABSTRACT

- 58 Attacks that target data are of concern to companies and organizations across many industries. Data
- 59 breaches represent a threat that can have monetary, reputational, and legal impacts. This guide seeks to
- 60 provide guidance around the threat of data breaches, exemplifying standards and technologies that are
- 61 useful for a variety of organizations defending against this threat. Specifically, this guide identifies risks
- 62 associated with the loss of data confidentiality, and mitigations to protect against those risks.

### 63 **KEYWORDS**

- 64 asset management; cybersecurity framework; data breach; data confidentiality; data protection;
- 65 *identify; malicious actor; malware; protect; ransomware*

# 66 **ACKNOWLEDGMENTS**

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

Name	Organization
Jason Winder	Avrio Software (now known as Aerstone)
Trey Doré	Cisco
Matthew Hyatt	Cisco
Randy Martin	Cisco
Peter Romness	Cisco
Bryan Rosensteel	Cisco
Micah Wilson	Cisco
Ben Burke	Dispel
Fred Chang	Dispel
Matt Fulk	Dispel
lan Schmertzler	Dispel
Kenneth Durbin	FireEye
Tom Los	FireEye
J.R. Wikes	FireEye
Jennifer Cawthra	NIST
Joe Faxlanger	PKWARE
Victor Ortiz	PKWARE
Jim Wyne	PKWARE
Steve Petruzzo	Qcor

Name	Organization
Billy Stewart	Qcor
Norman Field	StrongKey
Patrick Leung	StrongKey
Arshad Noor	StrongKey
Dylan Buel	Symantec, a division of Broadcom
Sunjeet Randhawa	Symantec, a division of Broadcom
Paul Swinton	Symantec, a division of Broadcom
Spike Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Brian Johnson	The MITRE Corporation
Lauren Lusty	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Julie Snyder	The MITRE Corporation
Lauren Swan	The MITRE Corporation
Anne Townsend	The MITRE Corporation
Jessica Walton	The MITRE Corporation

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

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

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

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

Technology Partner/Collaborator	Build Involvement
Avrio	Avrio SIFT
Cisco Systems	DUO
Dispel	Dispel
FireEye	FireEye Helix
Qcor	Qcor ForceField
PKWARE	PKWARE PKProtect
StrongKey	StrongKey Tellaro
Symantec, a Division of Broadcom	Symantec Web Isolation

# 72 **DOCUMENT CONVENTIONS**

73 The terms "shall" and "shall not" indicate requirements to be followed strictly to conform to the

74 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

76 excluding others, or that a certain course of action is preferred but not necessarily required, or that (in

the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms

78 "may" and "need not" indicate a course of action permissible within the limits of the publication. The

terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

# 80 CALL FOR PATENT CLAIMS

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

86 unexpired U.S. or foreign patents.

87 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in writ-88 ten 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
- 90 currently intend holding any essential patent claim(s); or

- b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring
- to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft
- 93 publication either:
- under reasonable terms and conditions that are demonstrably free of any unfair discrimination;
   or
- 96
   97
   2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

98 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its 99 behalf) will include in any documents transferring ownership of patents subject to the assurance, provi-100 sions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that 101 the transferee will similarly include appropriate provisions in the event of future transfers with the goal 102 of binding each successor-in-interest.

- 103 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of 104 whether such provisions are included in the relevant transfer documents.
- 105 Such statements should be addressed to: <u>ds-nccoe@nist.gov</u>

# 106 **Contents**

107	1	Intr	oduction	1
108		1.1	How to Use this Guide	1
109		1.2	Build Overview	2
110		1.3	Typographic Conventions	3
111		1.4	Logical Architecture Summary	3
112	2	Pro	duct Installation Guides	5
113		2.1	FireEye Helix	5
114			Installing the Communications Broker - CentOS 7	5
115			Forwarding Event Logs from Windows 2012 R2	6
116		2.2	Symantec Cloud Secure Web Gateway	9
117			Configure Web Security Service	9
118			Install Proxy Certificates and enabling TLS/SSL Interception	13
119			Configure Symantec Web Security Service Proxy	17
120		2.3	PKWARE PKProtect	23
121			Configure PKWARE with Active Directory	24
122			Create a New Administrative User	25
123			Install Prerequisites	26
124			Install the PKProtect Agent	29
125			Configure Discovery and Reporting	31
126		2.4	StrongKey Tellaro	35
127			Python Client for StrongKey – Windows Executable Creation and Use	36
128		2.5	Qcor ForceField	40
129			Installation and Usage of ForceField	40
130		2.6	Avrio SIFT	43
131			Configuring Avrio SIFT	43
132		2.7	Cisco Duo	46
133			Installing Cisco Duo	46
134			Registering a Duo User	53
135		2.8	Dispel	53
136			Installation	54
137			Configuring IP Addresses	56
138			Configuring Network	57

139		Adding a Device	57
140	2.9	Integration: FireEye Helix and Symantec SWG	60
141		Configure Fireye Helix to Collect Logs from Symantec SWG	60
142	2.10	Integration: FireEye Helix and PKWARE PKProtect	64
143		Configure the Helix Communications Broker	64
144		Configure PKWARE PKProtect to Forward Events	65
145	2.11	Integration: FireEye Helix and Cisco Duo	66
146		Configure Fireye Helix to Collect Logs from Cisco Duo	66
147	2.12	Integration: FireEye Helix and QCOR ForceField	70
148		Configure an SFTP server on Windows	70
149 150		Configure the Linux Machine to Download and Send Logs to the Helix Communications Broker	71
151	2.13	Integration: FireEye Helix and Dispel	72
152	2.14	Integration: Avrio SIFT and PKWARE PKProtect	73
153		Configuring PKWARE PKProtect	73
154	2.15	Integration: Dispel and Cisco Duo	76
155	Append	lix A List of Acronyms	77

# 156 **1** Introduction

- 157 The following volumes of this guide show information technology (IT) professionals and security
- engineers how we implemented this example solution. We cover all of the products employed in this
- 159 reference design. We do not re-create the product manufacturers' documentation, which is presumed
- to be widely available. Rather, these volumes show how we incorporated the products together in our
- 161 lab environment.
- Note: These are not comprehensive tutorials. There are many possible service and security configurations
   for these products that are out of scope for this reference design.

# 164 **1.1 How to Use this Guide**

- 165 This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a
- standards-based reference design and provides users with the information they need to replicate the
- ability to identify threats to and protect from a loss of data confidentiality. This reference design is
- 168 modular and can be deployed in whole or in part.
- 169 This guide contains three volumes:
- 170 NIST SP 1800-28A: Executive Summary
- 171 NIST SP 1800-28B: Approach, Architecture, and Security Characteristics what we built and why
- NIST SP 1800-28C: *How-To Guides* instructions for building the example solution (you are here)
- 174 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 1800-28A*, which describes the following topics:
- challenges that enterprises face in identifying vulnerable assets and protecting them from data
   breaches
- 179 example solution built at the NCCoE
- 180 benefits of adopting the example solution
- 181 Technology or security program managers who are concerned with how to identify, understand, assess,
- and mitigate risk will be interested in *NIST SP 1800-28B*, which describes what we did and why. The
   following sections will be of particular interest:
- 184 Section 3.4.1, Risk, describes the risk analysis we performed.
- Appendix D, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.
- 187 You might share the *Executive Summary, NIST SP 1800-28A*, with your leadership team members to help
- 188 them understand the importance of adopting a standards-based solution to identify threats to and
- 189 protect from a loss of data confidentiality

- 190 IT professionals who want to implement an approach like this will find this whole practice guide useful.
- 191 You can use this How-To portion of the guide, *NIST SP 1800-28C*, to replicate all or parts of the build
- 192 created in our lab. This How-To portion of the guide provides specific product installation, configuration,
- and integration instructions for implementing the example solution. We do not recreate the product
- 194 manufacturers' documentation, which is generally widely available. Rather, we show how we
- incorporated the products together in our environment to create an example solution.
- 196 This guide assumes that IT professionals have experience implementing security products within the
- 197 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
- 198 not endorse these particular products. Your organization can adopt this solution or one that adheres to
- 199 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
- 200 parts of a solution to identify threats to and protect from a loss of data confidentiality. Your
- 201 organization's security experts should identify the products that will best integrate with your existing
- tools and IT system infrastructure. We hope that you will seek products that are congruent with
- applicable standards and best practices. Section 3.6 Technologies, lists the products that we used and
- 204 maps them to the cybersecurity controls provided by this reference solution.
- 205 A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a
- 206 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and
- success stories will improve subsequent versions of this guide. Please contribute your thoughts to <u>ds-</u>
   nccoe@nist.gov .

# 209 1.2 Build Overview

- 210 The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively
- 211 identify sensitive data and protect against a loss of data confidentiality in various Information
- 212 Technology (IT) enterprise environments. This work also highlights standards and technologies that are
- 213 useful for a variety of organizations defending against this threat. The servers in the virtual environment
- 214 were built to the hardware specifications of their specific software components.
- 215 The NCCoE worked with members of the Data Confidentiality Community of Interest to develop a
- 216 diverse (but non-comprehensive) set of security scenarios against which to test the reference
- 217 implementation. These are detailed in Volume B, Section 5.2.

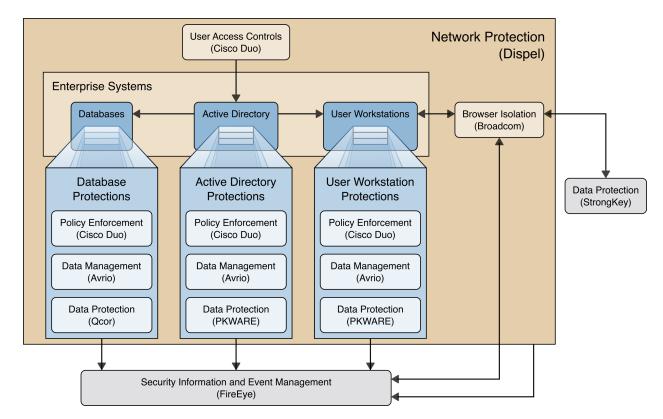
# 218 **1.3 Typographic Conventions**

219 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,
	references to documents that	see the NCCoE Style Guide.
	are not hyperlinks; new	
	terms; and placeholders	
Bold	names of menus, options,	Choose File > Edit.
	command buttons, and fields	
Monospace	command-line input,	mkdir
	onscreen computer output,	
	sample code examples, and	
	status codes	
Monospace Bold	command-line user input	service sshd start
	contrasted with computer	
	output	
<u>blue text</u>	link to other parts of the	All publications from NIST's NCCoE
	document, a web URL, or an	are available at
	email address	https://www.nccoe.nist.gov.

# 220 **1.4 Logical Architecture Summary**

- 221 The architecture described is built within the NCCoE lab environment. Organizations will need to
- 222 consider how the technologies in this architecture will align technologies their existing infrastructure. In
- addition to network management resources, such as a border firewall, the architecture assumes the
- 224 presence of user workstations, an active directory system, and databases. The diagram below shows the
- 225 components of the architecture and how they interact with enterprise resources.



- Data Management (Avrio) allows discovery and tracking of files throughout the enterprise.
- Data Protection (GreenTec, StrongKey, PKWARE) involves encryption and protection against
   disclosure of sensitive files.
- User Access Controls (Cisco Duo) allows organizations to enforce access control policies,
   ensuring that only authorized users have access to sensitive files.
- Browser Isolation (Symantec SWG) protects endpoints in the organization from malicious
   web-based threats by utilizing multi-layered content inspection to block threats and remote
   isolation of content from high-risk and unknown sites.
- Policy Enforcement (Cisco Duo) ensures that endpoints in the organization conform to specified
   security policies, which can include certificate verification, installed programs, and machine
   posture.
- Security Information and Event Management (FireEye Helix) creates a baseline of a normal enterprise activity for comparison in the event of a data confidentiality event. This function includes the collection, aggregation, and analysis of logs throughout the enterprise, including logs from other security tools, to provide a better picture of the overall health of the enterprise before a breach should occur.
- Network Protection (Dispel) ensures that hosts on the network only communicate in allowed
   ways, preventing side-channel attacks and attacks that rely on direct communication between
   hosts. Furthermore, it protects against potentially malicious hosts joining or observing traffic
   (encrypted or decrypted) traversing the network.
- For a more detailed description of our architecture, see Volume B, Section 4.

# 247 **2 Product Installation Guides**

- 248 This section of the practice guide contains detailed instructions for installing and configuring all of the
- 249 products used to build an instance of the example solution. This implementation guide is split into
- 250 sections for each product and integrations between these products, aiming to present a modular
- architecture where individual capabilities and products can be swapped out or excluded depending on
- the needs of the organization. Organizations can choose to implement a partial architecture based on
- 253 their own risk assessments and data protection requirements.

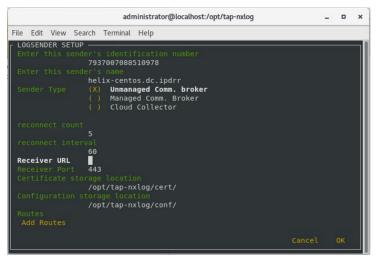
# 254 2.1 FireEye Helix

- 255 FireEye Helix is a security incident and event management system used for collecting and managing logs
- 256 from various sources. In this build, Helix is primarily used to manage events and alerts generated by data
- collected from across the enterprise. This build implemented a cloud deployment of Helix, and as such,
- 258 much of the documentation provided will be integrating a cloud deployment with various products and
- 259 components of the enterprise.
- 260 In this setup, we detail the installation of a communications broker which will be used to collect logs
- 261 from the enterprise and forward them to the cloud deployment. This installation took place on a CentOS
- 262 7 Virtual Machine.

# 263 Installing the Communications Broker- CentOS 7

264	1.	Acquire the Helix Communications Broker for CentOS 7.
265	2.	Navigate to the folder containing the installer, and run
266		<pre>&gt; sudo yum localinstall ./cbs-installer_1.4.2-9.x86_64.rpm</pre>
267	3.	Log on to the Helix web console.
268	4.	Navigate to Dashboards > Operational.
269	5.	Click Download Certificate.
270	6.	Click <b>Download</b> . This will download a "bootstrap.zip" file.
271	7.	Copy the zip file to the Helix Communications Broker certificate directory.
272		<pre>&gt; sudo cp bootstrap.zip /opt/tap-nxlog/cert</pre>
273	8.	Navigate to the certificate directory.
274		<pre>&gt; cd /opt/tap-nxlog/cert</pre>
275	9.	Extract the zip file you just copied.
276		> sudo unzip ./bootstrap.zip
277	10.	If prompted, select "Yes" to overwrite any previous certificate files.
278	11.	Navigate to one folder above.
279		> sudo cd
280	12.	Run the setup script.
281		> sudo ./setup.sh
282	13.	Enter the name of the CentOS machine.
202		

283 14. Enter the receiver URL provided in the Helix welcome email.



- 284 15. Select Add Routes and press Enter.
- 285 16. Select **syslog**.
- 286 17. Select **tcp**.
- 287 18. Select the IP address of the machine where logs should be sent.
- 19. Enter 512 for the port number where logs should be sent.

administrator@localhost:/opt/tap-nxlog	7-	-		×
File Edit View Search Terminal Help				
<pre>INPUT SOURCE SETUP::ADD Input Type () json () bsd Protocol Type () udp (X) tcp () ssl Input Interface () 192.168.122.1 (X) 192.168.1.206 () 127.0.0.1</pre>				
Input Port 512	Cancel		рк	

- 289 20. Select **OK** and press **Enter**.
- 290 21. Review the configuration, then select **OK** and press **Enter**.

### 291 Forwarding Event Logs from Windows 2012 R2

- 292 22. Acquire nxlog-ce-2.10.2150.msi from <a href="http://nxlog.org/products/nxlog-community-edition/download">http://nxlog.org/products/nxlog-community-edition/download</a>.
- 294 23. Run **nxlog-ce-2.10.2150.msi**.

ß	NXLog-CE Setup	_ 🗆 🗙
	Welcome to the NXLog	g-CE on your computer. Click
	Back	Next Cancel

#### 24. Click Next.

295

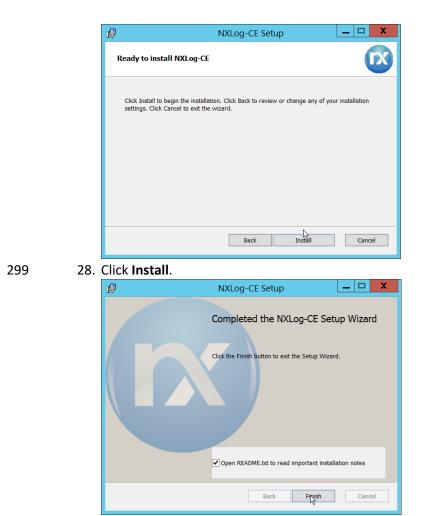
296

297

25. Check the box next to I accept the terms in the License Agreement.

	1 <sup>6</sup>	NXLog-CE Setup	
	End-User License A	greement	
	Please read the follow	ing license agreement carefully	
		DG PUBLIC LICENSE	v1.0
		Il mean version 1.0 of the NXLOG : e. the terms and conditions set forth	
		all mean the source code and objec media, printed materials, and "onl	
		cumentation. All such software and	
	✓ I accept the terms in	n the License Agreement	
		Print Back Ne	xt Cancel
26.	Click <b>Next</b> .		
	ß	NXLog-CE Setup	_ 🗆 X
	Destination Folder	NXLog-CE Setup	
	Destination Folder		
	Destination Folder Click Next to install to t	the default folder or click Change to choose anot	
	Destination Folder Click Next to install to I Install NXLog-CE to:	the default folder or click Change to choose anot	
	Destination Folder Click Next to install to I Install NXLog-CE to: C:\Program Files (x86)	the default folder or click Change to choose anot	
	Destination Folder Click Next to install to I Install NXLog-CE to: C:\Program Files (x86)	the default folder or click Change to choose anot	
	Destination Folder Click Next to install to I Install NXLog-CE to: C:\Program Files (x86)	the default folder or click Change to choose anot	
	Destination Folder Click Next to install to I Install NXLog-CE to: C:\Program Files (x86)	the default folder or click Change to choose anot	
	Destination Folder Click Next to install to I Install NXLog-CE to: C:\Program Files (x86)	the default folder or click Change to choose anot	her.

298 27. Click Next.



- 300 29. Click **Finish**.
- 301 30. Navigate to *C*:\*Program Files* (*x86*)\*nxlog*\*conf* and open **nxlog.conf**.
- 302 31. Copy the **nxlog.conf** file provided below.

```
Panic Soft
#NoFreeOnExit TRUE
define ROOT C:\Program Files (x86)\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
<Extension syslog>
   Module xm syslog
</Extension>
<Input in>
  Module im msvistalog
# For windows 2003 and earlier use the following:
# Module im mseventlog
</Input>
<Output out>
   Module om_tcp
            192.168.1.206
   Host
            512
   Port
            to syslog snare();
   Exec
</Output>
<Route 1>
             in => out
   Path
</Route>
```

303 32. Restart the **nxlog** service.

304 33. You can verify that this connection is working by checking the logs in *data\nxlog.log*, and by
 305 noting an increase in events on the Helix Dashboard.

# 306 2.2 Symantec Cloud Secure Web Gateway

This installation and configuration guide for Symantec SWG uses a cloud instance of Web Isolation. In this guide, Web Isolation is used to isolate threats to the user through the browser. It does this through

the use of a web proxy, which captures traffic and assigns a threat level to it, and based on

administrative policy decides whether to serve the page to the user. In doing so, threats from the web

can be mitigated through shared intelligence and isolated execution of the page before it reaches the

312 user's desktop.

### 313 Configure Web Security Service

1. Login to the Symantec portal by navigating to <u>https://portal.threatpulse.com/</u>.

S Web Security Service - Product S × +		~		X
$\leftrightarrow$ $\rightarrow$ C ( $$ portal.threatpulse.com		Ŕ	* .	) :
Neb Security Service				
Product Configuration				
Products will be available for use after completion of their initial configuration. Please select a product to configure.				
Product 1	Configuration Status	Action	Progres	55
Web Security	Not Configured	Configure	0%	
Protection Suite	🕌 Not Purchased			
Hosted Reporting	🞽 Not Purchased			
CASB	🕌 Not Purchased			
Exit / Logout			Contir	nue

315 2. Click **Configure** next to Protection Suite.

#### 316 3. Select WSS Portal.

#### 317 4. Select Monitor.

Web Security Service - Prod	luct Sc × +		v <mark>-</mark>	
÷ → C 🔒 portal.ti	hreatpulse.com		🖻 🛧	<b>2</b> :
left Web Securit	-			
Default Policy	Privacy	Mobile Users Static Location	Auth Connector Setup On-boarding Confirma	tion
Where do you plar	n to manage your clou	id policy?		*
Policy Source:	• WSS Portal	Configure and manage your policy from the WSS portal		Ь.
	O Management Center	Configure and manage your policy from your Management Center and deplo points	y your policy to your appliances and to WSS as enforcemen	t
What policy profile	do you want to use?			
Choose the policy profi	ile that corresponds with y	our security requirements. You can fully customize your policy behavior after t	he On-Boarding process.	
Default Policy Profile:	<ul> <li>Monitor</li> </ul>	Protects against security threats, monitors all other traffic.		
	O Standard	Protects against security threats, adult content and illegal activity.	L <sub>6</sub>	Ŀ
	O High	Protects against all <b>Standard</b> plus additional legal liability and security risks.		Ŧ
Cancel			Back	lext

- 318 5. Click **Next**.
- Select Suppress User/Group, Device Info, Client IP, Geolocation. (Note: If you are planning to
   use this tool for network monitoring of organizational users, a less strict privacy policy may be
   preferable; however, for this build, we are using Web Isolation primarily for external threats.)

S Web Security Service - Product 5 X +	X
$\leftarrow$ $\rightarrow$ C $\stackrel{\text{a portal threatpulse.com}}{}$	<b>.</b> ()
left Web Security Service	
System Configuration: Privacy	
Default Policy Privacy Mobile Users Static Location Auth Connector Setup On-boarding Confirmatic Completed	on
Default policy added successfully.	
Configure Privacy What data do you want to log?	Î.
To address privacy requirements, Personally Identifiable Information (PII) can be suppressed in access logs. Specific traffic reporting is not available for any data that is suppressed.	
Choose what data is collected in your access logs by setting the Default Privacy Setting, which applies to all traffic. You can configure different privacy settings for specific users, groups, IPs, and locations after the On-Boarding process.	L
Default Privacy Setting: Suppress User/Group, Device Info, Client IP, Geolocation V Note: User, Client IP, and Geolocation reporting is not available with this setting	L
Who can access your account?	
Control whether Support Operators from Symantec can access your account to assist with troubleshooting and support.	-
Cancel	ext

322 7. Click **Next**.

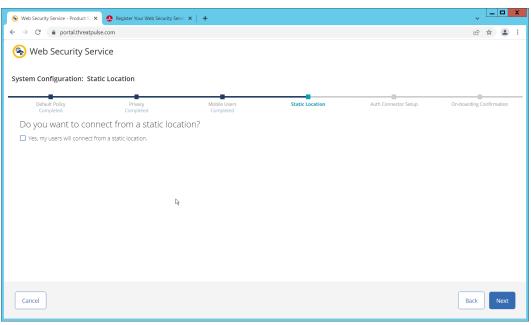
323

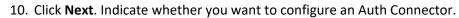
# 8. Indicate whether you have mobile users.

⊗ Web Security Service - Product S⊢ ×	+				~ <u> </u>
$\leftarrow$ $\rightarrow$ C $\bullet$ portal.threatput	lse.com				@☆ 😩 :
leb Security Ser	vice				
System Configuration: Mo	bile Users				
Default Policy Completed	Privacy Completed	Mobile Users	Static Location	Auth Connector Setup	On-boarding Confirmation
Privacy Setting added s	successfully.				
Do you have roamin	ng mobile users?				
□ I have roaming users who w	ill connect using the Symantec Mc	bile Client.			
		R			
Cancel					Back

324

9. Click **Next**. Indicate whether your users connect from a static location.

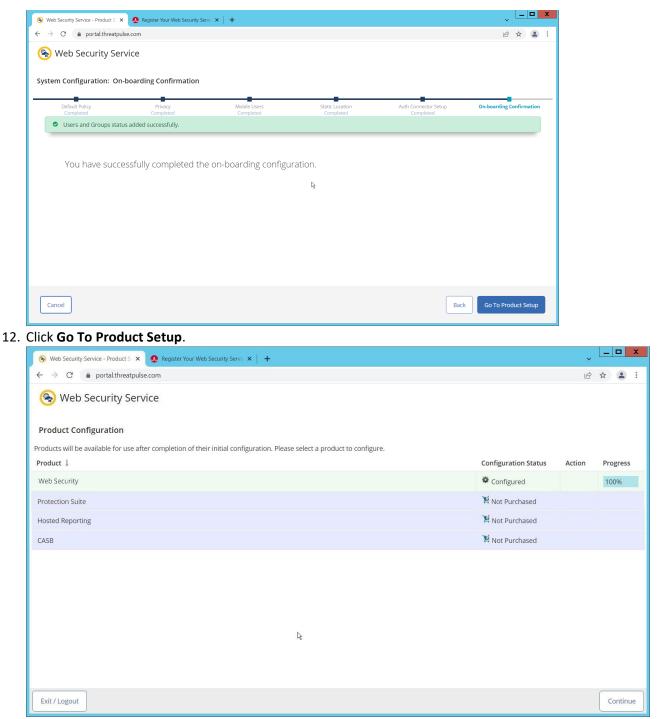




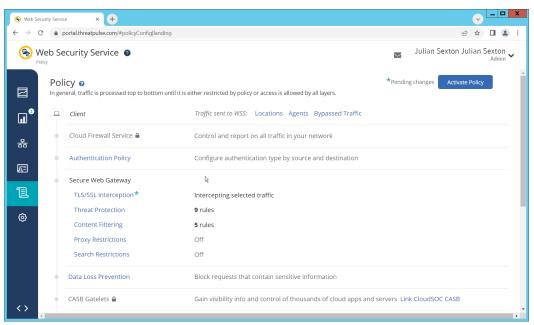
S Web Security Service - Product S	K 👧 Register Your Web Security Ser	rvic ×   +			~ <u> </u>
← → C 🌲 portal.threatpu	ulse.com				☞ ☆ 😩 :
left Security Set Security Set	rvice				
System Configuration: Au	th Connector Setup				
Default Policy Completed	Privacy Completed	Mobile Users Completed	Static Location Completed	Auth Connector Setup	On-boarding Confirmation
Do you want to con	figure an Auth Conne	ctor to automatically ir	mport Users and Gro	ups from your Active D	irectory?
Yes, I want to configure an .	Auth Connector				
		k₀			
		v			
Cancel					Back Next

326 11. Click **Next**.

NIST SP 1800-28C: Data Confidentiality: Identifying and Protecting Data Against Data Breaches



- 328 13. Click **Continue**.
- 329 Install Proxy Certificates and enabling TLS/SSL Interception
- 330 1. Click the **Policy** tab.



#### 331 2. Click TLS/SSL Interception.

332 3. Enable TLS/SSL interception by clicking the toggle.

🛞 Web S	ecurity Service × +		~ <u> </u>
$\leftarrow \   \rightarrow$	C 🍵 portal.threatpulse.com/#policyConfig ssl		🖻 🎓 🔲 😩 🗄
	Neb Security Service		Julian Sexton Julian Sexton
	TLS/SSL Interception  Carbing TLS/SSL Interception allows you to cont encrypted traffic that is not intercepted.	rol and report on encrypted traffic. Some policy, including content analysis	Activate Policy s and web application controls, cannot be applied to
윪	TLS/SSL Interception Certificate	lnstall on endpoint browsers	0 🔺
E 1	-	on all endpoint browsers in your network before enabling TLS/SSL Interce	ption for the best end-user experience.
¢	TLS/SSL Interception Policy	5 rules	0 -
	OCSP Validation	Disabled	0 -
<>			

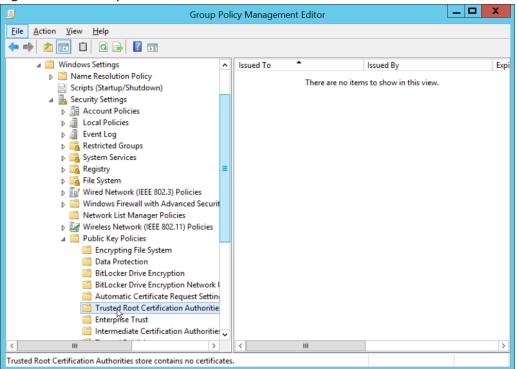
- 4. Download the certificate here. You can either install this individually in the Trusted Root
- Certification Authorities store on individual machines or follow the below steps to distribute the certificate via Group Policy.
- 336 5. Open the **Group Policy Management Console**.
- 337 6. Right click the **Domain** and select **Create a GPO in this domain, and Link it here...**.

	New GPO
Name: WSS Certificate	
Source Starter GPO:	
(inite)	OK Cancel

#### 7. Enter a name and click **OK**.

#### 338 339

#### 8. Right click the newly created GPO and click Edit....



- 340 9. Navigate to Computer Configuration > Policies > Window Settings > Security Settings > Public
   341 Key Policies, and right click Trusted Root Certification Authorities.
- 342 10. Click **Import**.
- 343 11. Click **Next**.
- 344 12. Select the certificate you just downloaded.

File to Import         Specify the file you want to import.         File name:         C:'Users'Administrator'Documents'(CertEmulationCA crt         Note: More than one certificate can be stored in a single file in the following formats:         Personal Information Exchange-PKCS #12 (PFX, P12)         Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P78)         Microsoft Serialized Certificate Store (.SST)         Itek Next.         Itek Next.         Certificate Import Wizard         Certificate Store         Certificate Stores are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for the certificate store         Q Place all certificates in the following store         Certificate store:         Trusted Root Certification Authorities       Browse		
File name:       C:\Users\uddininistrator\Documents\CertEnulationCA\crt       Browse         Note: More than one certificate can be stored in a single file in the following formats:       Personal Information Exchange- PKCS #12 (.PFX,.P12)         Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)       Microsoft Serialized Certificate Store (.SST)         Incosoft Serialized Certificate Store (.SST)       Nett       Certificate Import Wizard         Certificate Store       Certificate stores are system areas where certificates are kept.       Microsoft serialized certificate store, or you can specify a location for the certificate store based on the type of certificate         Windows can automatically select a certificate store based on the type of certificate store:       Outomatically select the certificate store based on the type of certificate store:	File	
C: Users \Administrator \Documents \CertEmulationCA\crt       Browse         Note: More than one certificate can be stored in a single file in the following formats:       Personal Information Exchange-PKCS #12 (.PFX,.P12)         Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P78)       Microsoft Serialized Certificate Store (.SST)         Microsoft Serialized Certificate Store (.SST)       Next       Ca         Ick Next.       Ca         Certificate Import Wizard       Ca         Windows can automatically select a certificate store, or you can specify a location for the certificate.       Automatically select the certificate store based on the type of certificate store         Inconstructing store       Certificate store:       Certificate store:		
Note: More than one certificate can be stored in a single file in the following formats:         Personal Information Exchange-PKCS #12 (PFX, P12)         Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)         Microsoft Serialized Certificate Store (.SST)         Intersection         Microsoft Serialized Certificate Store (.SST)         Intersection         Next         Cather Store         Cather Store         Certificate Import Wizard         Certificate Store         Certificate Store         Certificate Stores are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for the certificate.         Place all certificates in the following store         Certificate store:		File name:
Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P76) Microsoft Serialized Certificate Store (.SST) Next Ca Next Ca Next Ca Certificate Import Wizard Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate Microsoft Serialized Certificates in the following store Certificate store:		C:\Users\Administrator\Documents\CertEmulationCAl.crt Browse
Personal Information Exchange- PKCS #12 (.PFX,.P12)         Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P78)         Microsoft Serialized Certificate Store (.SST)         Incomposition Certificate Store (.SST)         Incomposition Certificate Import Wizard         Certificate Store         Certificate Store         Certificate Store are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for the certificate.         Place all certificates in the following store         Certificate store:		Note: More than one certificate can be stored in a single file in the following formats:
Microsoft Serialized Certificate Store (.SST)  Next Ca  Next Ca  ick Next.  Certificate Import Wizard  Certificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Mundows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store: Ceri		Personal Information Exchange- PKCS #12 (.PFX,.P12)
Next Ca Next.  Next Certificate Import Wizard  Certificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Windows can automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store:		Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Next       Cartificate Import Wizard         Certificate Store       Certificate stores are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for the certificate.       Numatically select the certificate store, or you can specify a location for the certificate.         Place all certificates in the following store       Certificate store:		Microsoft Serialized Certificate Store (.SST)
Next       Cartificate Import Wizard         Certificate Store       Certificate stores are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for the certificate.         Automatically select the certificate store based on the type of certificate         Place all certificates in the following store         Certificate store:		
Next       Call         Iick Next.       Certificate Import Wizard         Certificate Store       Certificate stores are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for the certificate.       Nutomatically select the certificate store based on the type of certificate         Image: Place all certificates in the following store       Certificate store:		
Next       Cartificate Import Wizard         Certificate Store       Certificate stores are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for the certificate.       Automatically select the certificate store based on the type of certificate         Image: Place all certificates in the following store       Certificate store:		Ν
Certificate Import Wizard         Certificate Store         Certificate stores are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for the certificate.         O Automatically select the certificate store based on the type of certificate         Image: Place all certificates in the following store         Certificate store:		r,
Certificate Import Wizard         Certificate Store         Certificate stores are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for the certificate.         O Automatically select the certificate store based on the type of certificate         Image: Place all certificates in the following store         Certificate store:		
Certificate Import Wizard  Certificate Store Certificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store:		
Certificate Import Wizard Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store:		Next C
<ul> <li>Certificate Import Wizard</li> <li>Certificate Store         <ul> <li>Certificate stores are system areas where certificates are kept.</li> </ul> </li> <li>Windows can automatically select a certificate store, or you can specify a location for the certificate.         <ul> <li>Automatically select the certificate store based on the type of certificate</li> <li>Place all certificates in the following store             <ul> <li>Certificate store:</li> <li>Certificate store:</li> </ul> </li> </ul></li></ul>		
Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store:		
Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store:		
<ul> <li>the certificate.</li> <li>Automatically select the certificate store based on the type of certificate</li> <li>Place all certificates in the following store</li> <li>Certificate store:</li> </ul>	€ <i>₿</i> с	Certificate Import Wizard
the certificate. <ul> <li>Automatically select the certificate store based on the type of certificate</li> <li>Place all certificates in the following store</li> <li>Certificate store:</li> </ul>	-) 💆 C	Certificate Import Wizard
<ul> <li>Automatically select the certificate store based on the type of certificate</li> <li>Place all certificates in the following store</li> <li>Certificate store:</li> </ul>	₿ C	Certificate Import Wizard
Place all certificates in the following store     Certificate store:	je c	Certificate Import Wizard tificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for
Certificate store:	) 🍠 C	Certificate Import Wizard tificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.
Trusted Root Certification Authorities Browse	-) 🖉 C	Certificate Import Wizard tificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate
	₿ C	Certificate Import Wizard tificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate © Place all certificates in the following store
	) 🍠 C	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store:
	€ <i>₿</i> с	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store:
	€ <i>₿</i> с	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store:
	€ <i>₿</i> с	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store:
	€ <i>₿</i> с	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse
R	€ <i>₿</i> с	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse
L <sub>3</sub>	€ <i>₿</i> с	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse
ß	9 C	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse



14. Click Next.

) 🔄 🛃 Certificate Import Wizar	rd
Completing the Cert	ificate Import Wizard
The certificate will be imported a	fter you dick Finish.
You have specified the following	settings:
Certificate Store Selected by U	ser Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\Administrator\Documents\CertEmulationCA
<	III >
	R
	Finish Cancel

- 347 15. Click **Finish**.
- 348 16. Click **OK**.

# 349 Configure Symantec Web Security Service Proxy

# 350 1. Navigate to the **Connectivity** tab.

🛞 Web Secu	rrity Service × +						
$\leftarrow \rightarrow c$	🗧 🔶 C 👔 portal.threatpulse.com/#connectivity landing						
	eb Security Service 2	Julian Sexton Julian Sexton Admin					
	Connectivity 🛛						
ū	Locations	1 location					
윦	Agents	Agents that send traffic to the service					
æ	Setup and Configuration	k					
E	Bypassed Traffic	8 domains					
¢	PAC Files	Configure PAC files to facilitate Explicit Proxy and SEP connections					
	WSS Agent	WSS Agent settings and installer for Windows & Mac devices					
	Symantec Endpoint Security	Setup instructions for SEP with Seamless identification and agents for both iOS and Android					
<>							

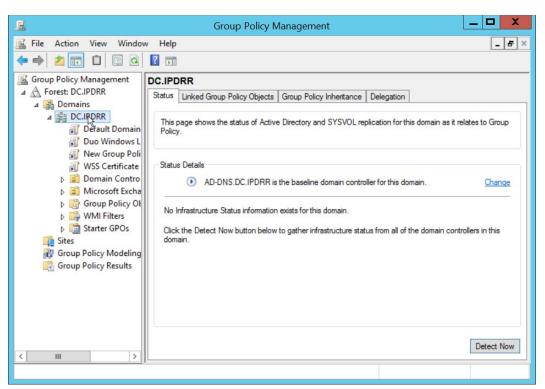
351 2. Click Locations.

🛞 Web S	Security Service × +						~	_ <b>D</b> X
$\leftrightarrow$ $\rightarrow$	C   portal.threatpulse.com/#	#connectivity locations					6 \$	□ 😩 :
	Web Security Service     Julian Sexton Julian Sexton       Connectivity     / Locations ~							Sexton Admin
	Locations 🧕							
	In order to direct traffic https://pfms.wss.syman		is, please set your browser'	s PAC file to:				
ᇔ	+ Add Location	Edit Delete	7/15/2022, 1	2:49:15 PM		Search		Q
	□ Location Name ↓	IP Address / Device ID	Access Method	Agent Configuration	References		Data Center Conn	ections
æ			Explicit Proxy	Inactive	1 reference(	s)	오 gusas1	
1	≪ <   Page 1	of1 > »	0				Displaying locat	tions 1 - 1 of 1
ŵ								
<>								

- 352 3. Click Add Location.
- 353 4. Enter a name for the **Location**.
- 354 5. Select **Proxy Forwarding** for **Access Method**.
- Enter any public IP addresses of your organization, to ensure that traffic sent through the WSS
   proxy is redirected to the proper dashboard.

🛞 Web Security Se	ervice × +			
$\leftrightarrow$ $\rightarrow$ C	portal.threatpulse.com/#connectivity locations			🖻 ☆ 🗖 🏝 :
Web S	Add Location 6			Julian Sexton 🗸
	Location Name: * DC IPDRR	Estimated Users: *	Less than 50 🔹	
	In or Access Method: * Proxy Forwarding	Country: 🍁	United States 👻	
	+ Add	Time Zone: 🌞	Eastern Time (America/New_Yc 🔹	Q
	We've noticed that your IP address is: Local If this IP address is the location you wish to add click here	Address Line 1:		er Connections
	P N	Address Line 2:		
	0 0	Zip / Postal Code:		ying locations 1 - 1 of 1
	The following options require WSS Agent v7.x or higher Keep agents active at this location	Comments:		
	Selective intercept		255 of 255 characters left	
			Cancel Save	

- 357 7. Click **Save**.
- This page will now provide a URL to a PAC file which can be distributed to browsers across the
   organization via GPO. If you wish to create a custom PAC file, you can navigate to **Connectivity** >
   **PAC Files**.
- 361 9. Open the **Group Policy Management Console**.



10. Right click the **Domain** and select **Create a GPO in this domain, and Link it here...**.

	New GPO	X
Name: WSS Proxy		
Source Starter GPO: (none)		~
	ОК	Cancel

363 11. Enter a name and click **OK**.

L	Group Policy Manageme	ent		_ 0	X
🔜 File Action View Windo	W Help				- 8 ×
Group Policy Management Construction Const	The following sites, domains, and OUs are linked to	this GPO:			~
<ul> <li>New Group Pol</li> <li>WSS Certificate</li> <li>WSS Proxy</li> <li>Domain Contro</li> <li>Microsoft Excha</li> <li>Group Policy O</li> </ul>	Location DC.IPDRR	Enforced No	Link Enabled Yes	Path DC.IPDRR	>
<ul> <li>WMI Filters</li> <li>Starter GPOs</li> <li>Sites</li> <li>Group Policy Modeling</li> <li>Group Policy Results</li> </ul>	The settings in this GPO can only apply to the follow Name	ving groups, use	ers, and computers:		
< III >	Add Remove WMI Filtering This GPO is linked to the following WMI filter: (none>	Properties	Open		

- 364 12. Right click the newly created GPO and click **Edit...**.
- 365 13. Navigate to User Configuration > Preferences > Control Panel Settings.

<b>I</b>	Group Policy Mana	gement Editor	
File Action View Help			
🗢 🄿 🙍 🖬 🖬 🖨 🧔	🗟 🚺 🖬 🔯 🗣		
<ul> <li>WSS Proxy [AD-DNS.DC.IPDRR]</li> <li>Computer Configuration</li> <li>Policies</li> <li>Preferences</li> <li>Viser Configuration</li> <li>Policies</li> <li>Policies</li> <li>Preferences</li> <li>Windows Settings</li> <li>Control Panel Setting</li> <li>Control Panel Setting</li> <li>Devices</li> <li>Folder Options</li> <li>Local Users and C</li> <li>Network Options</li> <li>Power Options</li> <li>Scheduled Tasks</li> <li>Start Menu</li> </ul>	Processing       Image: Constraint of the second seco	Name Order	ns to show in this view.
< III > \	Preferences (Extended ) Standard /		

- 366
- 14. Right click Internet Settings and select New > Internet Explorer 10 Properties.
- 367 15. Click the **Connections** Tab.

16.

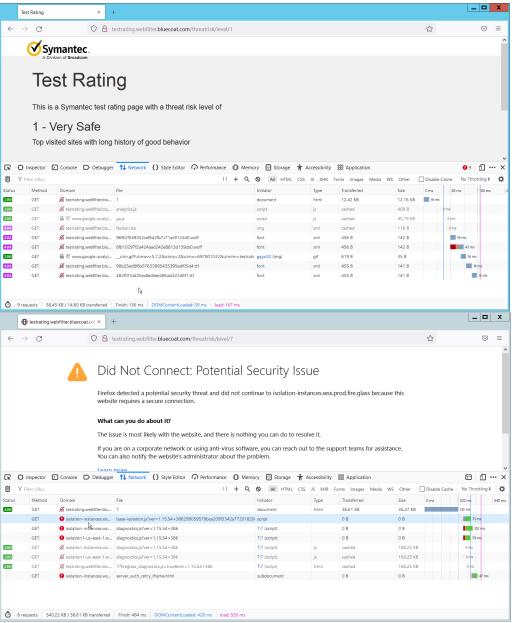
	New Inte	ernet Explorer	10 Prop	erties
Progra	ims	Advanced		Common
General	Security	Privacy	Conten	t Connections
	set up an Int tup.	ternet connection,	dick	Setup
Dial-up and	Virtual Privat	e Network setting:	s —	
				Add
				Add VPN
				Remove
	ttings if you n a connection.	need to configure a	a proxy	Settings
O Never	dial a connect	tion		
Dial wh	enever a net	work connection is	not preser	nt
Always	dial my defa	ult connection		
Current	None	2		Set default
		0		
	Network (LAN			
		ply to dial-up conn for dial-up setting		LAN settings
				$\searrow$
	OK	Cancel	Ар	ply Help
ck <b>Local</b> /	Area Ne	twork (LAN	l Settin	igs).
	Local A	rea Network (L	AN) Setti	ings
Automatic cor	C			

Local Area Network (LAN) Settings
Automatic configuration Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address:
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: Port: Advanced
Bypass proxy server for local addresses
OK

- 369 17. Select the **Address** field.
- 18. Press **F6** to enable it (it is enabled if the box has a solid green underline.
- 19. Enter the PAC file URL from earlier in the **Address** field.

	Local Area Network (LAN) Settings
	Automatic configuration         Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.         Automatically detect settings         Use automatic configuration script         Address:       https://pfms.lwss.symantec.com/v1/pac;         Proxy server         Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).         Address:       Port:         Address:       Port:         Address:       Bypass proxy server for local addresses
20 0	OK Cancel
20. C	lick OK.
	New Internet Explorer 10 Properties
	Programs Advanced Common
	General Security Privacy Content Connections
	To set up an Internet connection, dick     Setup       Dial-up and Virtual Private Network settings
	Add VPN Remove
	Choose Settings if you need to configure a proxy Settings server for a connection.
	O Never dial a connection
	Dial whenever a network connection is not present
	Always dial my default connection     Current None Set default
	Current None Set default
	Local Area Network (LAN) settings LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.
	OK Cancel Apply Help

- 373 21. Click **OK**.
- 22. To verify that traffic is going through Isolation, you can visit the following test website, and
- 375 substitute 1-10 for the threat level: <u>http://testrating.webfilter.bluecoat.com/threatrisk/level/7</u>.



376 23. On this test URL (tested July 2022), levels 5-7 will go through isolation, and you will be able to
377 see the isolation traffic from the network tab in developer mode (F12) on the browser. Levels 8378 10 will be blocked by the content filter, and levels 1-4 will not go through isolation or content
379 filtering.

### 380 2.3 PKWARE PKProtect

This installation and configuration guide for PKWARE PKProtect uses a physical PKWARE server, and as such will not delve into the installation of server components. In this guide, PKWARE is used to automatically perform data inventory and data protection functions. PKWARE provides users with the ability to store encrypted files for retrieval later, requiring the use of user credentials to access them.

# 385 Configure PKWARE with Active Directory

386 1. Login to the PKWARE web portal using the administrative credentials.

PKWA					
Authorization	Required				
	Username:				
	Password:				
		Login			
		PKWARE Enterprise Manager 18.5.203 - <u>About</u> - pkwarevm	n 8/20/20 11:00:04 AM		

- 2. Once logged in, you can and should change the password to this administrative account by clicking **Change Password** in the top right corner.
- 388 clicking Change Password in the top389 3. Navigate to System > Domain.

PKWARE*     Actions*     System     Basics     Advanced       Dashboard     Archive     Events*     Dashboard	→ … Help .og out Change ssword
Dashboard Archive Events Dashboard Archive Events Control Dashboar	.og out Thange
Status Database Elasticsearch Network Pa	Change
Status Database Elasticsearch Network Pa	
Domain SNMP SSL Package Log	
Domain	
This system is not currently joined to a domain Join Domain	
PKWARE Enterprise Manager 18.5.203 - <u>About</u> - pikwarevm 8/20/20 11:02:01 AM	

- 390 4. Click Join Domain.
- 391 5. Enter the Kerberos Realm, NetBIOS Domain, as well as the username and password of an
   392 administrative user on the domain.

g +5 ☐ System - Domain × + ∨				-		>
$\leftrightarrow$ $\rightarrow$ $\circlearrowright$ $\land$ $\land$ Certificate error https://192	.168.1.43/mds/SuperUser/System/Domain	□ ☆	չ⊨	h	È	•
PKWARE <sup>*</sup> Actions <sup>®</sup> Dashboa					l Log	He J O
	rd Archive Events				Cha	
Status [	Database Elasticsearch Network				Passv	VOI
Domain	SNMP SSL Package Log					
Join Windows Domain						
Kerberos Realm	dc.ipdrr					
NetBIOS Domain	dc					
User	Administator					
Password	•••••					
	Debug Output					
	Join Domain Cancel		$\mathbf{v}$			
PKWARE Enten	orise Manager 18.5.203 - <u>About</u> - pkwarevm 8/20/20 11:02:01 AM					

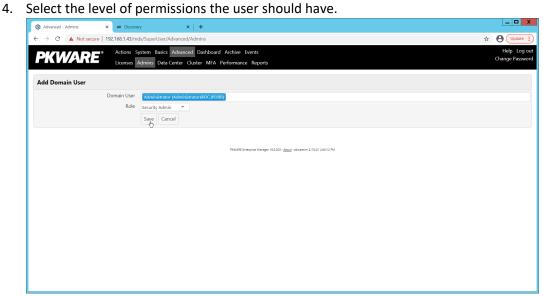
393 6. Click Join Domain.

### 394 Create a New Administrative User

395 1. Navigate to Advanced > Admins.

								Search:	
Administrator@DCJPDRR Domain User Sys Admin No No (never) 2/10/21 12:47:00 PM Edit EnableAPI Delete howing 1 to 2 of 2 entries Add Domain Group Add Local User	Username/UPN	Туре	Role		MFA	API	Last API	Last Login	
howing 1 to 2 of 2 entries Add Domain Group Add Local User Add Local User	Ultimate Sys Admin	Local User	Super Sys Admin		n/a	n/a	n/a	n/a	
Add Domain User Add Domain Group Add Local User	Administrator@DC.IPDRR	Domain User	Super Sys Admin		No	No	(never)	2/10/21 12:47:00 PM	Edit EnableAPI Delete
			,	NWARE Ente	rprise Manager 18.5.20	8 - <u>About</u> - pkwarevm 2/1	10/21 2:45:12 PM		

- 396 2. Click Add Domain User.
- Enter the username of a user on the domain that should be able to login through the PKWARE
   management portal (this is meant for administrators only).



#### 400 5. Click **Save.**

### 401 Install Prerequisites

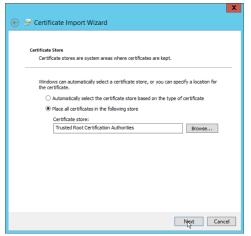
- If needed for your environment, you may need to install certificates locally before agents can
   connect to PKProtect ask your PKWARE representative if this is necessary for your
   environment.
- 405 2. Double click the certificate you wish to install.

<b>R</b>	Certificate
Ge	neral Details Certification Path
	Certificate Information
	This certificate is intended for the following purpose(s): • All issuance policies • All application policies
	Issued to: PKWARE NIST-NCCoE Lab
	Issued by: PKWARE NIST-NCCoE Lab Root Authority
	Valid from 8/17/2020 to 8/17/2022
	Instal Certificate Issuer Statement
	OK

- 406 3. Click Install Certificate....
- 407 4. Select Current User.



- 408
- 409 6. Click **Browse**.
- 410 7. Select Trusted Root Certification Authorities.



. C	Click <b>Next.</b>	
(	🛞 🍜 Certificate Import Wizard	X
	Completing the Certificate Import Wizard	
	The certificate will be imported after you click Finish.	
	You have specified the following settings:	
	Certificate Store Selected by User Trusted Root Certification Authorities Content Certificate	
	Finish Can	cel

- 412
- 9. Click Finish.

#### DRAFT



- 413 10. Click **OK**.
- 414 11. Repeat steps 1 through 10 but select **Personal** instead of **Trusted Root Certification Authorities.**
- 415 12. Repeat steps 1 through 11 for each certificate which needs to be installed.

👢   ⊋ 📜 =	Application Tools	PKWAR	RE		_ 🗆 X
File Home Share	View Manage				v 😮
🍥 🍥 - 🛧 🎩 🕨 PK	WARE •		~ C	Search PKWARE	Ą
☆ Favorites	Name	Date modified	Туре	Size	
Desktop	l certificates	2/15/2021 9:22 AM	File folder		
Downloads	agent-registry.reg	8/17/2020 8:00 AM	Registration Entries	1 KB	
laces 😓 Recent places					
🖗 This PC					
Network					
2 items 1 item selected	192 bytes				

- 416 13. Rename agent-registry.txt to agent-registry.reg.
- 417 14. Double click the file (must have administrator privileges).

Registry Editor
Adding information can unintentionally change or delete values and cause components to stop working correctly. If you do not trust the source of this information in C:\Users\Administrator.DC\Desktop\PKWARE\agent-registry.reg, do not add it to the registry. Are you sure you want to continue?
Le Yes No

418 15. Click **Yes.** 

NIST SP 1800-28C: Data Confidentiality: Identifying and Protecting Data Against Data Breaches



- 419 16. Click OK.
- 420 17. Restart the machine to apply these changes.

#### Install the PKProtect Agent 421

422 1. Run the PKProtect Installation executable.

🗗 Smartcryp	ot 16.40.0010 - InstallShield Wizard
	Welcome to the InstallShield Wizard for Smartcrypt 16.40.0010
	The InstallShield(R) Wizard will install Smartcrypt 16.40.0010 on your computer. To continue, click Next. WARNING: This program is protected by copyright law and international treaties.
	< Back Next > Cancel

- 423
- 424
- 2. Click Next.

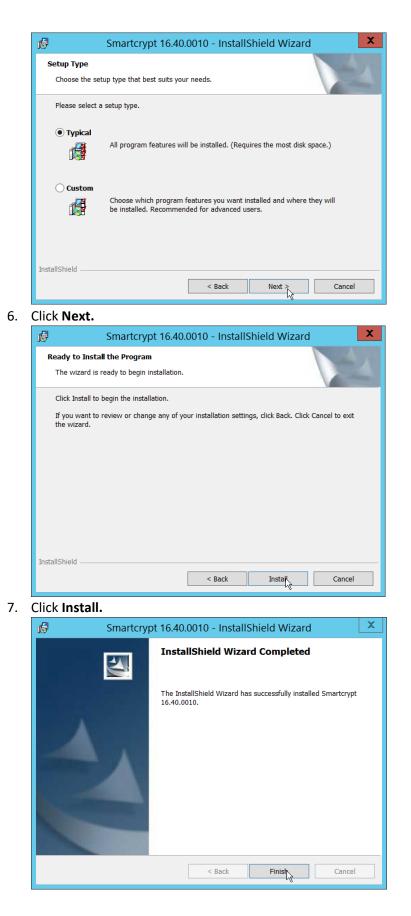
## 3. Select I accept the terms in the license agreement.

ß	Smar	tcrypt 16.40	.0010 - InstallS	hield Wizard	
	e Agreement e read the following	ng license agreem	ent carefully.		
		PKWARE L	WARE, INC. ICENSE AGREEMI ubscription/ Prod		
below. provisio PKWAR BY ACCI SERVICI	This Agreement go of services related software, visit htt SSING, USING, OR S AS APPLICABLE, I	overns the subscrip d to the Licensor's :ps://legal.pkware INSTALLING ALL ( LICENSEE EXPRES:	nade by and between otion licensing of Softy PKWARE solution. Fo .com. DR ANY PART OF THE SLY AGREES TO AND ( F OF ALL SCHEDULES	ware, the sale of Pro r perpetual license SOFTWARE, PRODI CONSENTS TO BE BO	oducts and the terms for UCTS, OR DUND BY ALL OF
-	pt the terms in the ot accept the term				
InstallShie	ld				
			< Back	Next >	Cancel

425 426

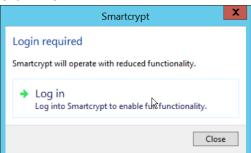
5. Select Typical.

428



433

### 429 8. Click Finish.



- 430
  430
  9. If a window to login is not automatically shown, you can right click the PKProtect icon in the
  431
  431
  Windows taskbar and click Login... If a window is automatically shown, click Log in.
  - Login using the username of the account in the domain, in email format (such as administrator@domain.id).

8	Smartcrypt: Smartcrypt Manager Entry
Enter t	e address of your Smartcrypt Manager:
https:	/pkwarevm.dc.ipdrr/mds
	$\triangleright$
	OK Cancel

- 434 11. Enter the address of the PKWARE server.
- 435 12. The PKWARE agent will now run in the background.

## 436 Configure Discovery and Reporting

437 1. On the PKWARE dashboard, log in as an administrative user, and navigate to Archive >

438 Discovery.

	Policies Disco Deployments	m Basics Advanced Dashboard Archive Events very Remediations Classification Communities Assignments Lockers Accounts Devices Reporting Support	Help Change
Smart Filt	er Bundles	Search	
Туре 🔺	Filter Name	Bundle Patterns	
Discovery	HIPAA - Diagnosis Lexicon and Social Security Numbers	Social Security Number US (1 or more)         National Insurance Number UK (1 or more)         FDA Drugs Dictionary (5 or more)           FDA Firms Dictionary (5 or more)         ICD-9 Codes Dictionary (5 or more)         ICD-10 Codes Dictionary (5 or more)	Edit Clone De
Discovery	PCI-DSS - Credit Cards and Social Security Numbers	All Supported Credit Cards (1 or more) International Bank Account Number (1 or more) Social Security Number US (1 or more) National Insurance Number UK (1 or more)	Edit Clone De
Discovery	Personally Identifiable Information	Social Security Number US (1 or more) National Insurance Number UK (1 or more) Tax ID US (1 or more) Address US (10 or more)	Edit Clone De
Add Biscov Discovery	o 3 of 3 entries ery Add Redaction Patterns In Global Settings Under Scanning Priority Low Detection Time Frame 1 (Days) 1	nport Bundle Pack Export Bundle Pack	

439 440

3. Enter a **name** for the discovery rule.

- 441 4. Select a **pattern** for the rule to discover. In this case, we are setting up a rule to detect social
- security numbers in files for reporting/remediation.
- 443 5. The **Threshold** field refers to how many of those patterns must be present in a document for the444 rule to be applied.

	<ul> <li>Actions System Bas</li> </ul>	cs Advanced Dashboard	d Archive Events	н
PKWA	Policies Discovery R	emediations Classificatio	n Communities Assignments Lockers Accounts	Chan
	Deployments Device	Reporting Support		
Discovery Smart	Filter Bundle			
	Filter Name SSN Discovery			
Pattern		Threshold		
Social Security Number	US	· 1		
Add	L <sub>6</sub>			
Exclusions				
	Patterns			
Inclusions				
	Patterns			
Save Cancel				
			PKWARE Enterprise Manager 18.5.203 - <u>About</u> - pkwarevm 2/10/21 2:20:36 PM	
			<ul> <li>Contract of the processing of the second of <u>House</u> ("providents" of the 1 second pro- ter second second processing of the second s</li></ul>	

## 445 6. Click **Save.**

446

### 7. Navigate to Archive > Remediations.

S Archive - Remediations x = Discovery x +	_ <b>D</b> X
← → C 🔺 Not secure   192.168.1.43/mds/SuperUser/Archive/Remediations	☆ 🛛 Update 🔅
PKVVARE         Actions         System         Basics         Advanced         Dashboard         Archive         Events           Policies         Discovery         Remediations         Classification         Communities         Assignments         Lockers         Accounts           Deployments         Devices         Reporting         Support	Help Log out Change Password
Remediation Actions	
None Add Dc	
POINARE Enterprise Manager 18.5203 - <u>About</u> - perameters 2/10/21 22/50 PM	

#### 447 8. Click **Add.**

448 9. Enter a name for the remediation.

Archive - Remediations	x = Discovery x +	_ □
→ C A Not secure	e   192.168.1.43/mds/SuperUser/Archive/Remediations	🖈 \varTheta Updat
<b>YKWARE</b>	Actions System Basics Advanced Dashboard Archive Events Searching Policies Discovery Remediations Classification Communities Assignments Lockers Accounts Deployments Devices Reporting Support	Help Log o Change Passwo
Remediation Action	Report and Encrypt	
Comment		
	Report Discovery Events     Report Discovery Events     Report Successful Encryptions     Report Encryption Failures     Algorithm As (256-bit)     Key(s)     This list is prioritized from left to right. The first key a user has access to will be used for encryption operations.     If a user does not have access to any of the keys in the list, their Personal SmartKey will be used.     Classify     Delete     Delete     Do Nothing	
Pre Command 🗟		
Command		1.

- 10. Check the box next to **Report Discovery Events.**
- 450 11. Check the box next to **Encrypt.**
- 451 12. Ensure that **AES (256-bit)** is selected.

#### 452 13. Click **Save.**

PKWARE     Actions System Basics Advanced Dashboard Archive Events     Help Lor       Policies Discovery Remediations     Classification Communities Assignments Lockers Accounts     Change Pass       Deployments Devices Reporting Support     Support	Archive - Remediations ×		×   +				
Operation Actions         Support           Remediation Actions         Search:				ents			Help Log o
Name     Comment     Types     Smartleys       Report and Encrypt     Report, Encrypt     (none)     Edit Delete	PRWARE	· · · ·		es Assignments Lockers Accounts			Change Passwo
Name     Comment     Types     Smartkeys       Report and Encrypt     Report, Encrypt     (none)     Edit Delete	Remediation Actions						
Showing 1 to 1 of 1 entries Add	Name	*	Comment	Types			٥
Showing 1 to 1 of 1 entries Add	Report and Encrypt	6		Report, Encrypt	(none)	Edit Delete	
	Add		POWARE Inte	price Manager 185300 - <u>Appur</u> - picerem 2/1021 22947 PM			

453 14. Navigate to **Archive > Assignments.** 

	← → C ▲ Not secure   192.16	8.1.43/mds/SuperUser/Arch	ive/Assignments						\$ <b>8</b> 🖤
	PKWARE R	ctions System Basics Ad olicies Discovery Remedia eployments Devices Repu	ations Classificat		Events Assignments Lockers Account	ls			Help Change P
	Assignments								
							Searc	h:	
	Order 🔦 Name	Users / Groups	Platform	Mode	Locations	Re- Encryption	Compliant	Not Compliant	
	= 1 Domain Users Desktop Encrypt	Domain Users [DC.IPDRR]	Windows	Encrypt	\${USERPROFILE}\Desktop\Encrypt	Disabled	1	Q	Status Edit Reset Delete Disa
	Showing 1 to 1 of 1 entries								
	Add								
				PKWARE E	interprise Manager 18.5.203 - <u>About</u> - pixwarevm 2/10/21 2:295	55 PM			
15									
15.	Click <b>Add.</b>								
15.		Discovery	×   +						
15.	S Archive - Assignments		1 A 4 A 4 A 4 A 4 A 4 A 4 A 4 A 4 A 4 A						
15.		8.1.43/mds/SuperUser/Arch	ive/Assignments						¢ <b>8</b> ₪
15.	<ul> <li>⊗ Archive - Assignments ×</li> <li>← → C ▲ Not secure   192.16</li> </ul>	8.1.43/mds/SuperUser/Arch ctions System Basics Ad	ive/Assignments Ivanced Dashboa						★ e ur Help La
15.	Image: Second secon	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia	ive/Assignments Ivanced Dashboa ations Classificat		Events hities Assignments Lockers Account	ls			★ e ur Help La
15.	Image: Second secon	8.1.43/mds/SuperUser/Arch ctions System Basics Ad	ive/Assignments Ivanced Dashboa ations Classificat			s			★ e ur Help La
15.	© Archive - Assignments × ← → C ▲ Not secure   192.16 PKWARE ▲ P	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia	ive/Assignments Ivanced Dashboa ations Classificat			5			ہے ۔ ۲۵ کو لیے Heip Lo Change Pass
15.	Image: Second secon	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia	ive/Assignments Ivanced Dashboa ations Classificat			s			☆ 😫 Up Help La
15.	© Archive - Assignments × ← → C ▲ Not secure   192.16 PKWARE ▲ P	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia eployments Devices Repe	ive/Assignments Ivanced Dashboa ations Classificat orting Support			5			☆ 😫 Up Help La
15.	<ul> <li>③ Archive - Assignments</li> <li>×</li> <li>×</li> <li>C</li> <li>▲ Not secure</li> <li>192.16</li> <li>PKCWAREE</li> <li>A</li> <li>A</li> <li>Assignment</li> </ul>	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia eployments Devices Repe me Report and Encrypt SSI	ive/Assignments Ivanced Dashboa ations Classificat orting Support			5			☆ 😫 Up Help La
15.	③ Archive - Assignments x ← → C ▲ Not secure 192.16 PKWAREE ▲ D Assignment Nar	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia eployments Devices Rep ene Report and Encrypt SS m Windows	ive/Assignments Ivanced Dashboa ations Classificat orting Support	ion Commur		5			☆ 😫 Up Help La
15.	<ul> <li>③ Archive - Assignments</li> <li>×</li> <li>×</li> <li>A Not secure</li> <li>192.16</li> <li>PKWARE</li> <li>A</li> <li>A</li></ul>	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia eployments Devices Repu Report and Encrypt SSI M Windows de Discovery	ive/Assignments Ivanced Dashboo ations Classificat orting Support N	ion Commur		5			☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     Assignment 192.16     PK(WAREE A. R.	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia eployments Devices Repr me Report and Encrypt SS mm Windows de Discovery ps Dumain Users (DCJDD7	ive/Assignments Ivanced Dashboo ations Classificat orting Support N	ion Commur		5			☆ 😫 Up Help La
15.	Archive - Assignments x     Assignment x     Ass	8.1.43/mds/SuperUser/Arch ctions System Basics Ad dicies Discovery Remedia eployments Devices Repr m Windows de Discovery P Comain Users (DC/IPDL SUSERPROFILE)	ive/Assignments Ivanced Dashboo ations Classificat orting Support N	ion Commur		5			☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     A solution of the solution o	8.1.43/mds/SuperUser/Arch ctions System Basics Ad dicies Discovery Remedic eployments Devices Reper me Report and Encrypt SS m Windows de Discovery p Comain Users (DIC/IPO) 5 (SUSERPROFILE] list	ive/Assignments Ivanced Dashboa ations Classificat orting Support N	ion Commur		s			☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     A solution of the solution o	8.1.43/mds/SuperUser/Arch ctions System Basics Ad ficies Discovery Remedia eployments Devices Repr me Report and Encrypt SS m Windows de Discovery ps Domain Users (DCJPDP () \$USERPROFILE) ist	ive/Assignments Ivanced Dashboo ations Classificat orting Support N	ion Commur		5 *jpg *jpeg *g	( 5mov 5mp3 (	ng4 (1993) (19	☆ 🕑 🕞 telp Lt Help Lt Change Pas
15.	Archive - Assignments x     A solution of the solution o	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia eployments Devices Repr Windows de Discovery ps Domain Users [DC:IP0] (s) <u>\$1USEDPROFILE</u> ist <u>\$1APEDATAIN</u> <u>\$10000</u>	ive/Assignments Weanced Dashboo attions Classificat attions Classificat N N N	ion Commur		5 ] *.jpg *.jpeg *.gj	1 Smov Smp3 .	mp4 <u>2003</u> 201	☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     A solution of the solution o	8.1.43/mds/SuperUser/Arch ctions System Basics Ad dicies Discovery Remedic eployments Devices Repr m Windows de Discovery P Opmain Users [DC:IPD] 5 (SUSTREMORTE] list 5 (APEDATA)(* 5(BC)) 5 (SUSTREMORTE) list 5 (SUSTREMORTE) 1 (STORE) 5	ive/Assignments Wanced Dashboc ations Classifications Classifications onting Support N RE RIAPPDATATY: *.a Mode	ion Commun	•httes         Assignments         Lockers         Account           •https://www.second/secon	s Tipg Tipeg Tig	1 Smov Smp3 4	npa sus se	☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     A solution of the solution o	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia eployments Devices Repe  Windows de Discovery P Osmain Users [DC:IPD5 ist SUASERROFE] ist SUASERROFE[ ist SUASERROFE]	ive/Asignments Wareed Dashboota ations Classificat orting Support N N ALAPPICATALY Mode	ion Commun	Hites         Assignments         Lockers         Account           *.hmg         *.dll         *.epe         *.eee         *.fle         *.inidd           her in the Agent.         *.         *.         *.         *.         *.         *.	tipa tipea tai	( smoy smp3 (	ngd (1903) (19	☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     A solution of the solution o	8.1.43/mds/SuperUser/Arch etcions System Basics Ad olicies Discovery Remedia eployments Devices Repr Windows de Discovery P5 Domain Users [DC:IP07 (4) <u>\$USERPROFILT</u> ] ist <u>\$IAPEDATAIN</u> {10:0C <u>\$USERPROFILT</u> } ist <u>\$IAPEDATAIN</u> {10:0C <u>\$USERPROFILT</u> } <u>\$Can-Only</u> Made dia Instead of reacting	ive/Assignments Ivenced Dashboxations Classificat orting Support N ALAPPDATAYC 2-a Mode to real-time file sy	ion Commun	attes         Assignments         Lockers         Account           *hmp         *dll         *eps         *exe         #fiv         *indd           *hmp         *dll         *eps         *exe         #fiv         *indd           her in the Agent.         the Agent will perform traditional folder         the Agent will perform traditional folder         *indd	tipa tipea tai	f smov smp3 s	mpd tons to	☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     A solution of the solution o	8.1.43/mds/SuperUser/Arch ctions System Basics Ad locics Discovery Remedic eployments Devices Repr eployments Devices Repr (indows de Discovery p <u>Domain Users [DC:IPD</u> (ist <u>SUUSERPROFILE</u> ] list <u>SUUSERPROFILE</u> list <u>Subsection</u> <u>Subsection</u> <u>Canable Scan-Only</u> 1 <u>Scan-only mode</u> dia <u>Agents earlier than</u> <u>Agents earlier than</u>	ive/Assignments Ivenced Dashboxations Classificat orting Support N ALAPPDATAYC 2-a Mode to real-time file sy	ion Commun	attes         Assignments         Lockers         Account           *hmp         *dll         *eps         *exe         #fiv         *indd           *hmp         *dll         *eps         *exe         #fiv         *indd           her in the Agent.         the Agent will perform traditional folder         the Agent will perform traditional folder         *indd	tipa tipea tai	1 Smov Smp3 *	mp4 spay spr	☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     A solution of the solution o	8.1.43/mds/SuperUser/Arch       ctions     System       Basics     Ad       olicies     Discovery       Remoti     Devices       Report and Encrypt SS       mm     Windows       de     Discovery       ps     Osmain Users (DC1005       ist     SURSERVORTE1       ist     SURSERVORTE1       ist     Surser-Only 1       intend of reacting     Agents carlier than       Agents     Secon-Only 1       Agents     Secon-Only 1	ive/Asignments Wanced Dashbaoka ations Classificat orting Support N N ALARPIOATA(12) Mode Mode to real-time file sp 1630 do not supp	ion Commun	attes         Assignments         Lockers         Account           *hmp         *dll         *eps         *exe         #fiv         *indd           *hmp         *dll         *eps         *exe         #fiv         *indd           her in the Agent.         the Agent will perform traditional folder         the Agent will perform traditional folder         *indd	tipa tipea tai	( 1.mov 1.mp3 (	npå (sm) sp	☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     A solution - Assignments x     A solution - Assignment x     Assignment	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia eployments Devices Repr windows de Discovery ps Domain Users [Dic1019] ist studews ist state="color:phase">State: Color:	ive/Assignments Wanced Dashbas ations Classificat orting Support N N ALAPPDATAGY ••• Mode Stotes the local fill stote sell-time file sp 16.30 do not supp e and Status	ion Commun	attes         Assignments         Lockers         Account           *hmp         *dll         *eps         *exe         #fiv         *indd           *hmp         *dll         *eps         *exe         #fiv         *indd           her in the Agent.         the Agent will perform traditional folder         the Agent will perform traditional folder         *indd	tipa tipea tai	1 *mov *mp3 *.	mp4 *pn3 *pr	☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     A solution - Assignments x     A solution - Assignment x     Assignment	8.1.43/mds/SuperUser/Arch ctions System Basics Ad ctions Statement exploring Statement (Statement Statement Statement (Statement Statement Statement Statement (Statement Statement Statement Statement (Statement Statement Statement Statement (Statement Statement Sta	IVE/Assignments Vanced Dashbot Stations Classificat N N N N ALARPICATAR ALARPI	ion Commun	attes         Assignments         Lockers         Account           *hmp         *dll         *eps         *exe         #fiv         *indd           *hmp         *dll         *eps         *exe         #fiv         *indd           her in the Agent.         the Agent will perform traditional folder         the Agent will perform traditional folder         *indd	tipa tipea tai	1 Smov Smp3 4	np4 spn3 spr	☆ 💽 Up Help Lo Change Pas
15.	Archive - Assignments x     A signments x     A Not secure 192.16     PK(WAREE A Regiment Reg	8.1.43/mds/SuperUser/Arch ctions System Basics Ad olicies Discovery Remedia eployments Devices Repr windows de Discovery ps Domain Users [Dic1019] ist studews ist state="basics.com" s	ive/Assignments IverAc	ion Commun	attes         Assignments         Lockers         Account           *hmp         *dll         *eps         *exe         #fiv         *indd           *hmp         *dll         *eps         *exe         #fiv         *indd           her in the Agent.         the Agent will perform traditional folder         the Agent will perform traditional folder         *indd	tipa tipea tai	( tmo) tmp3 (	nud Sung Sp	☆ 💽 Up Help Lo Change Pas

- 455 16. Enter a **name** for the Assignment.
- 456 17. Select the **Platform** for this assignment to run on.
- 457 18. Select **Discovery** for the **Mode**.
- 458 19. Enter the names of the Active Directory users or groups this rule should apply to.
- 459 20. Enter the folders for this rule to search in **Local Paths.**
- 460 21. Use **Whitelist** and **Blacklist** to specify file types which should or should not be considered.
- 461 22. Enter the interval for this rule to run in **Sweep Interval**.

S Archive - Assignments X	Discovery ×   +		_ <b>D</b> X
← → C ▲ Not secure   192.168.1	.43/mds/SuperUser/Archive/Assignments	\$	<b>O</b> Update
Whitelist			
Blacklist	\${APPDATA}\* \${LOCALAPPDATA}\* *.acm *.ai *.avi *.bmp *.dll *.eps *.tmp *.wav	*exe "tflv *indd *jpg *jpeg *gif *.mov *.mp3 *.mp4 *.png *.psd *.pst *.raw *.ocx *.os	
	Enable Scan-Only Mode		
	Scan-only mode disables the local file system watcher in the Agent.		
	Instead of reacting to real-time file system events, the Agent will perforr	n traditional folder scans.	
	Agents earlier than 16.30 do not support scan-only mode.		
Sweep Interval (seconds)	3600		
	Report Compliance and Status		
	Report Advanced File Attributes		
	Z Exclude Hidden Files		
	Z Exclude System Files		
Remediation Actions  Smart Filter Bur	dies	Remediation Action	
	No data availabl	e in table	
Showing 0 to 0 of 0 entries Agents earlier than 15.70 will only use t	he first Remediation Action shown above		
Save Cancel			
	PKWARE Enterprise Manager 183.203 - <u>Abbo</u>	g. = Skaween 2/10/21 20355 PM	

- 462 23. Under **Remediation Actions**, click **Add**.
- 463 24. Select the **Discovery** rule created earlier under **Smart Filter Bundles**.
- 464 25. Select the **Remediation Action** created earlier under **Remediation Action**.

S Archive - Assignments X Dis	scovery × +						
← → C ▲ Not secure   192.168.1.4	3/mds/SuperUser/Archive/Assignments			☆	O Update		
Local Path(s)	\$(USERPROFILE)						
Whitelist							
Blacklist	\$(APPDATA)\^ \$(LOCALAPPDATA)\* *.acm *.ai *.avi *.bmp *.dll *.eps *.exe *.flv *.indd *.j	ipg *.jpe	g *.gif *.mov *.mp3 *.mp4 *.png *.psd *.pst *.raw	*.ocx *.	ost		
	t.mp t.wav						
	Enable Scan-Only Mode						
	Scan-only mode disables the local file system watcher in the Agent.						
	Instead of reacting to real-time file system events, the Agent will perform traditional folder sca	ns.					
	Agents earlier than 16.30 do not support scan-only mode.						
Sweep Interval (seconds)	3600						
	Report Compliance and Status     Report Advanced File Attributes						
	Exclude Hidden Files						
	ZExclude System Files						
Remediation Actions							
Smart Filter Bundles			Remediation Action				
SSN Discovery		<b>\$</b>	Report and Encrypt	Delete			
Showing 1 to 1 of 1 entries							
Add							
Save Cancel							
R0044E Enterprise Manager 163.201 - dog.rprivaterim 2110.211 2355 PM							

- 465 26. Click **Save.**
- 466 27. This rule will now run automatically, reporting and encrypting files which match its discovery 467 conditions.

## 468 **2.4 StrongKey Tellaro**

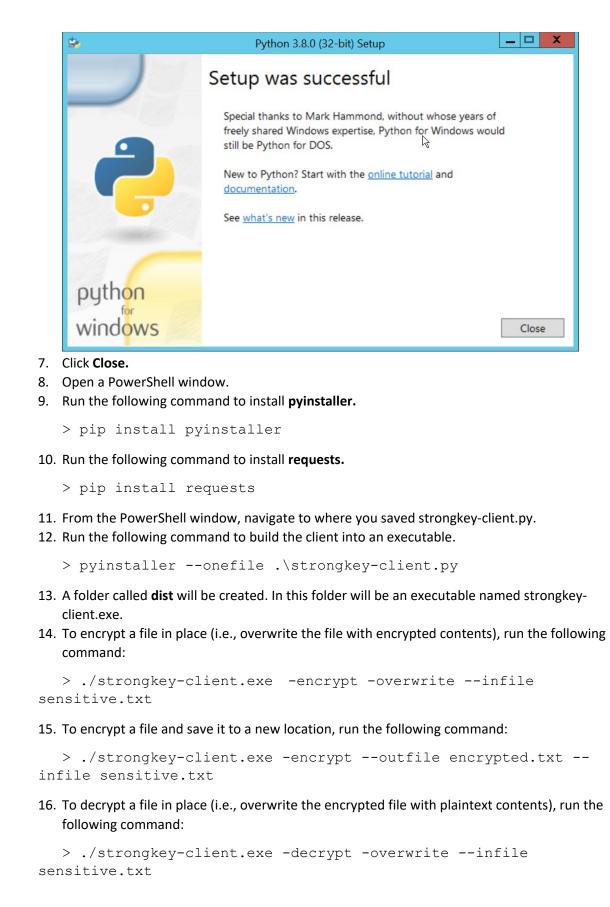
StrongKey is a REST API providing various security services. In this project, we primarily make use of its file encryption capabilities in the context of data protection. Because it is a web service, there is not much installation required on the enterprise side, and the bulk of the setup is acquiring credentials to communicate safely with the API. In this build, Strongkey will primarily be used for integration with other products, to encrypt sensitive data generated by products in formats which may be otherwise difficult to encrypt.

# 476 Python Client for StrongKey – Windows Executable Creation and Use

- 477
  478
  478 Ensure that the following script (see end of section) is filled out with information specific to your enterprise, including the variables **skdid**, **skuser**, and **skpass**.
- 479 2. Save the file as **strongkey-client.py**.
- This example will demonstrate how to create an executable from the script below. Download
   Python 3.8.0 from the Python website: <u>https://www.python.org/downloads/release/python-</u>
   380/. Specifically, download the Windows x86 executable installer. The 32-bit version will
- 483 provide better access to Active Directory packages and interfaces.
- 484 4. Run the installer.
- 485 5. Check the box next to Add Python 3.8 to PATH.



- 486
- 6. Click Install Now.



```
DRAFT
```

509 17. To decrypt a file and save it to a new location, run the following command: 510 > ./strongkey-client.exe -decrypt --outfile decrypted.txt --511 infile encrypted.txt 512 18. This client can be configured to run on a schedule, or be iterated over a directory of files, 513 depending on the needs of the organization. Because the client is Python and StrongKey is REST 514 API based, the script is adaptable to various architectures and can be deployed widely across the 515 enterprises, to fill in gaps that the enterprise may have in its data protection capabilities. 516 import requests 517 import json 518 import argparse 519 520 skdid = # Note: Users should reference a separate file for this ID 521 skuser = # Note: Users should reference a separate file for the username 522 skpass = # Note: Users should reference a separate file for the password 523 encurl = "https://demo4.strongkey.com/skee/rest/encrypt" 524 decurl = "https://demo4.strongkey.com/skee/rest/decrypt" 525 526 def buildrequest(fname, encrypt): 527  $req = \{\}$ 528 req["svcinfo"] = { 529 "did": skdid, 530 "svcusername":skuser, 531 "svcpassword":skpass 532 } 533 534 if (encrypt): 535 req["encinfo"] = { 536 "algorithm": "AES", 537 "keysize":256, 538 "uniquekey":True 539 } 540 541 req["fileinfo"] = { 542 543 "filename": name 544 } 545 546 reg["authzinfo"] = { "username": "encryptdecrypt", 547 #"userdn": "cn=encryptdecrypt,did="+skdid+",ou=us-548 549 ers,ou=v2,ou=SKCE,ou=StrongAuth,ou=Applications,dc=strongauth,dc=com", "authgroups": "cn=EncryptionAuthor-550 551 ized, did="+skdid+", ou=groups, ou=v2, ou=SKCE, ou=StrongAuth, ou=Applica-552 tions, dc=strongauth, dc=com", 553 "requiredauthorization": 0 554 } 555 556 req["svcinfo"] = json.dumps(req["svcinfo"]) 557 req["fileinfo"] = json.dumps(req["fileinfo"]) 558 if (encrypt): 559 reg["encinfo"] = json.dumps(reg["encinfo"]) 560 req["authzinfo"] = json.dumps(req["authzinfo"]) 561

```
562
             return req
563
564
         def encrypt(filename,output,overwrite):
565
             req = buildrequest(filename, True)
566
             with open(filename, mode='rb') as f:
567
                 files = [('filedata', f)]
568
                 p = requests.request("POST", encurl, headers={}, data=req,
569
         files=files)
570
             print(p)
571
             p.raise for status()
572
             if (p.status code == 200):
573
                 output = filename if overwrite else output
574
                 with open (output, mode='wb') as o:
575
                     o.write(p.content)
576
577
         def decrypt(filename,out,overwrite):
578
             req = buildrequest(filename, False)
579
             with open(filename, mode='rb') as f:
580
                 files = [('filedata', f)]
581
                 p = requests.request("POST", decurl, headers={}, data=req,
582
         files=files)
583
             p.raise for status()
584
             if (p.status code == 200):
585
                 output = filename if overwrite else out
586
                 with open(output, mode='wb') as o:
587
                     o.write(p.content)
588
589
590
         parser = argparse.ArgumentParser(description='Encrypt or decrypt a file
591
         using Strongkey.')
592
593
         group = parser.add mutually exclusive group(required=True)
594
         group.add argument("-encrypt", action='store true')
595
         group.add argument("-decrypt", action='store true')
596
597
         group = parser.add mutually exclusive group(required=True)
598
         group.add argument("-overwrite", action='store true')
599
         group.add argument("--outfile", type=str)
600
601
         parser.add argument ("--infile", type=str, required=True)
602
603
         a = parser.parse args()
604
605
         if (a.overwrite is True):
606
              overwrite = True
              out = ""
607
608
         elif (a.outfile is not None):
609
              out = a.outfile
610
              overwrite = False
611
612
         if (a.encrypt is True):
613
              encrypt(a.infile, out, overwrite)
614
         elif (a.decrypt is True):
615
             decrypt(a.infile, out, overwrite)
```

## 616 2.5 Qcor ForceField

- 617 ForceField is a Write-Protected File System (WFS) combining hardware device security and encryption.
- 618 In this build, ForceField is primarily used to backup data while maintaining confidentiality through
- 619 encryption. In this build, we used ForceField is for the protection of a transactional database which
- 620 needs to maintain both the confidentiality and integrity of prior transactions, while still affording the
- ability to use that data in new transactions.

## 622 Installation and Usage of ForceField

- 623 1. Either a CD or zip file will be provided by Qcor containing the WFS API and associate utilities.
- 624 Copy the contents of \*GreenTec*\*Release* onto the C: drive of the Qcor ForceField server.
- Add the destination folder to the command line PATH variable if necessary. To do this, from thestart menu search for **Environment Variables**.

			Edit User Variable		
Variable	Value				
Path	;C:\Program Files\Azure Data Studio\bi	Variable name:	Path		
TEMP	%USERPROFILE%\AppData\Local\Temp				
TMP	%USERPROFILE%\AppData\Local\Temp	Variable value:	Studio\bin;C:\GreenTec\ForceField;C:\Pro		
			OK Cancel		
	New Edit Delete				
ystem variables					
·	Value				
Variable	, and a				
Variable CLASSPATH	. Ξ				
Variable CLASSPATH ComSpec	C:\Windows\system32\cmd.exe				
Variable CLASSPATH ComSpec FP_NO_HOST_C	C:\Windows\system32\cmd.exe . NO				
Variable CLASSPATH ComSpec	C:\Windows\system32\cmd.exe . NO				
Variable CLASSPATH ComSpec FP_NO_HOST_C NUMBER_OF_PR	. = C:\Windows\system32\cmd.exe . NO . 32 ~				

627 3. Double click the **Path** variable and add the path to the WFS API.

6 <b>%.</b>	Administra	tor: Comma	nd Prompt			
C:\Users\Administrator.DC>wfsdir 2						
*						
h, Apr 9 2022 at	20-2021. All Right		ted File Syste	m (WFS) Vers	ion 1.9	
Note: Must be e (Linux))	executed with eleva	ted permissi	ons (e.g. admi	n (Windows)	or root =	
ST_Parms: * Warn	ing * Unable to l	ocate wfs.co	nf file, takin	g default pa	PMS	
ForceField(tm) - FS VOLUME <	> <del>***</del> HARDWARE-:	ENFORCED DAT	A SECURITY ★★→	⊧ ACTIVE ON	THIS W	
*						
* SerialNum S2ZW 25167	J9JG300194 has NOT J9JG300194 has BEE Enforced or Finali:	N ENFORCED f	rom 99904 to 1			
t be applied.	x (-fix) Option NOT : VERIFIED OK. Sea:					
CrDate CrTim Ver Ext FIL	e FileSize ENAME 	Blocks	Start	End	Dir 	
 20210520	08 213	8	100008	100015	99984	
20210520 14:59:	46 213 Users_Administrato:	8 NDC Deskton	100016 Pinates! Ann	100023	99976	
20210630 12:16:	20 26 ate_Mottos.txt	8	100024	100031	99968	
20221017 12:52:		8	100032	100039	99960	
20221017 12:56:	23 242	8	100040	100047	99952	
20221017 12:58:	47 157	8	100048	100055	99944	
20221026 11:42:	00 157	8	100056	100063	99936	
20221116 12:20:		8	100064	100071	99928	
20221116 12:21:		8	100072	100079	99920	
20221116 12:22:	tings.txt 01 157	8	100080	100087	99912	
20221116 12:26:	tings.txt 30 157 tings.txt	8	100088	100095	99904	
 USAGE STATISTICS: Num Extents= 11, Total Disk Size=1.0002 (TB), Used=0.0001 ( TB), Remaining=1.0002 (TB)						
Drive 2	DATA:	IB B	locks Per	cent		
	USED : 0.000 AVAIL: 1.000 TOTAL: 1.000	15 19534				
				cent		
	USED : 0.000 AVAIL: 0.006 TOTAL: 0.006	01 39	11 0.088 12482 99.91 12493	 105		
	1011131 01000				$\sim$	

4. Verify that the drives of the Qcor WFS server have been formatted to work with ForceField with wfsdir command line utility that was just installed. The drives may be pre-formatted. Use the

630 631 632		following command to determine whether a drive is formatted. In place of "N", enter the number of the drive to check.
633		> wfsdir N
634 635 636 637 638	5.	<i>If the hard drive(s) have not been formatted</i> , use the wfsx command line tool to format your drive. <b>Note:</b> Once performed, the formatting cannot be undone. The following instructions are copied from the WFS User Guide.
639 640		> wfsfx <devicename> <options></options></devicename>
641 642 643 644 645		<b>devicename</b> is the device identifier of the disk to be formatted. For Windows, this is the Windows disk number that may be found via the Windows Disk Manager (e.g. 1, 2, etc.). For Linux, this is the physical device name (e.g. /dev/sdb/).
646 647		<pre>options may be:     -DirX or -x <power 10="" of=""> (optional power of 10 for max number</power></pre>
648 649		of files, default is 10) 1 will format for 1,243 files, 10 will allow 12,489 files, 100
650 651 652		<pre>allows 124,993 files, 1000 allows 1,249,930 files    -vuser <username> specifies a volume user name, DO NOT FORGET THIS USE NAME IF USED!</username></pre>
653 654		<pre>-vpass <password> specifies a volume password, DO NOT FORGET THIS PASSWORD IF USED!</password></pre>
655 656 657		<pre>-cache ON OFF will turn on or off the disk drive internal cache (default is ON)verifywrite ON OFF will turn write verify on or off for the</pre>
658 659 660		WFS volume (default is OFF). The write verify status may be toggled ON or OFF using the WFScache utility. NOTE: turning write verify ON may significantly degradeI/O performance.
661 662 663	6.	Files can then be copied into or out of the designated drives using the wfscopy command line tool. The following instructions are copied from the WFS User Guide.
664		<pre>&gt; wfscopy <source-file> <destination-file> <count></count></destination-file></source-file></pre>

665 One of the files must be a native OS file system file, and the other file must be a WFS file. **source-file** is 666 the name of the input file and may be a native OS filename, or a WFS filename. **destination-file** is the 667 name of the input file and may be a native OS filename, or a WFS filename. **count** is the optional num-668 ber of bytes to copied. count defaults to all records.

#### DRAFT

## 669 Examples of wfscopy using Windows:

## 670 > wfscopy testfile.txt 1:\*

The above command will copy the file named testfile.txt from the local directory to disk number 1 with
the same name. If the WFS file does not previously exist, then it is created. If the WFS file does
previously exist, then the data is appended to the existing WFS file as a new file extension.

## 674 > wfscopy 2:Contracts.pdf c:\myfolder\Contracts.pdf

The above command will copy all records from all extensions of the WFS file named Contract.pdf from
the disk, as identified as 2 by the Windows Disk Manager, to the Windows file C:\myfolder\Contracts.pdf
record by record

677 record by record.

## 678 > wfscopy 4:myfile.txt con:

The above command will display the contents of the WFS file myfile.txt from disk 4 onto the console.This is similar to using the type command in the Windows command line.

## 681 2.6 Avrio SIFT

682 Avrio SIFT is a data inventory and management capability designed to enforce data policies. The

- 683 installation of Avrio SIFT is typically done in a managed fashion by the vendor, and the deployment seen
- 684 in the NCCoE lab may not resemble other deployments. In the case of a Docker deployment,
- configuration to the base Avrio installation can be made by modifying the docker-compose file.
- Otherwise, it will be assumed that Avrio has been installed and configured properly for the enterprise by
- 687 the vendor.

## 688 Configuring Avrio SIFT

- 1. Navigate to the SIFT dashboard (default address: http://IP-address:8080/sift/) and login.
- 690 2. Click **Configuration**.
- G91 3. Under Enclaves, enter two locations. First, the path to the public Windows share, and second,
  the path to the one protected by PKProtect. We will use this second path later in the integration
  between PKProtect and SIFT. In this example, DCIPDRR is the path to the public share, and
  PROTECTED is the path to the one protected by PKProtect. Enter user accounts that can access
  each share. In production, it is recommended to create a separate user account for SIFT to use
  to access these shares.

	SIFT   Secure Integrated File Tagg × S Archiv	ve - Lockers ×   +					~ <sup>[</sup>	_ 0	X
÷	→ C A Not secure   192.168.1.198:	8080/sift/blacklist/networks					12 ☆		) E
	🔗 SIFT Request 🗸 Confi	iguration Reports Analyze	Acces				👤 User, Admi		Î
	Configuration Enclaves	Enclaves							
	Keywords	SMB S3 Sharepo	oint						
	File Types	Name		UNC Path	Username	Password			
	Classifications	DCIPDRR	×	\\AD-DNS\TOP-SECRET-SH	DC\Administrator	••••••			
	Rich Text	PROTECTED	×	\\192.168.1.80\SECRET	DC\Administrator				
	Batch Scanning	+ Add new enclave							
	Video	+ Add new enclave							
	Scan Mode	SAVE CHANGES							
	Profiles								
	Language								
	Import/Export								
	Machine Learning								
	File Status								
									-

- 697 4. Click Save Changes.
- 698 5. Click **Keywords** on the left menu.
- 699 6. Click Add new keyword.
- 700 7. Enter the keyword under Name, and an Alias (if desired). Check the box next to any enclaves
  701 which are allowed to have this keyword SIFT will be able to move files matching it to the
  702 enclaves you check the box for.
- 703 8. Select the PROTECTED enclave under **Move To**.

SIFT   Secure Integrated File Tagg × S An	rchive - Lockers ×   +				~ <u> </u>	D X
← → C ▲ Not secure   192.168.1.1	98:8080/sift/blacklist/keywords				ዸ ☆ 🛛	<b>a</b> =
🧭 SIFT Request 🗸 Co	onfiguration Reports Analyze	Access ~			👤 User, Admin 🗸	
Configuration	Keyword Restrictions					
Enclaves	Word List	Alias	Move To	Enclaves		
Keywords		, 440	more to	DCIPDRR	PROTECTED	
File Types	Select All					
Classifications	MALABAR	alias	PROTECTED ~		2	
Rich Text						
Batch Scanning		R				
Video						
Scan Mode						
Profiles						
Language						
Import/Export						
Machine Learning						
File Status	+ Add new keyword					

- 704 9. Click Save Changes.
- 705 10. Click **File Types**.
- 11. Designate file types which are allowed to exist under each enclave.

🔗 SIFT Request 🗸 Config	uration Reports Analyze Access -	L User, Admin ∽
	PNG	2
	PPT	
	PPTX	
	RTF	
	TAR	
	TIFF 12	
	ТХТ	
	XLS	
	XLSX	
	XML	
	ZIP	
	SAVE CHANGES	

#### 707 12. Click Save Changes.

709

#### 708 13. Click Classifications.

#### 14. Designate the classifications which are allowed to exist under each enclave.

🕷 SIFT   Secure Integrated File Tag: X 🕲 Archive - Lockers X   +							
← → C ▲ Not secure   192.168.1.198:808	0/sift/blacklist/classifications		🖻 🖈 🔲 😩 i				
🧭 SIFT Request 🗸 Configu	ration Reports Analyze Access -		👤 User, Admin 🗸				
Configuration	Classification Restrictions						
Enclaves	Classification	Encl	aves				
Keywords		DCIPDRR	PROTECTED				
File Types	Select All						
Classifications	TOP SECRE						
Rich Text	SECRET	0					
Batch Scanning							
Video	UNCLASSIFIED						
Scan Mode	+ Add new classification						
Profiles	SAVE CHANGES						
Import/Export Machine Learning							
File Status							
File Status							

- 710 15. Click **Save Changes**.
- 711 16. On the top click **Request > New Request**.
- 712 17. Click **Batch**.
- 713 18. Select **UNC Path** for **Source Type**.
- 714 19. Select the enclave to scan for sensitive files.
- 20. Select Move for Scan Type. (Note that if you select Scan for Scan Type, it will scan files and tell
  you they are sensitive and whether they can be moved, but will not attempt to move them. This
  is useful for debugging.)
- 718 21. Select **Delete** for **Move Action**, or another action depending on the needs of your organization.
  719 Selecting **Delete** will remove the sensitive file from the public share and move it to the
  720 protected one.

- 721 22. Set **Scan Subfolders** to **ON**.
- 722 23. Enter a **description** for the scan.
- 24. Set the frequency of the scan. Note that the efficiency of the scan will likely depend on the size
- 724of the organization, and it may be more desirable to scan once an hour rather than once a725minute.

SIFT   Secure Integrated File Tagg × SIFT   Secure Integrated File Tagg ×	Lockers ×   +		× _ □ X
← → C ▲ Not secure   192.168.1.198:808	30/sift/batch/create		년 🏚 🖬 😩 🗄
🔗 SIFT Request 🗸 Configu	ration Reports Analyze		L User, Admin ∽
New Request Type	Initiate Batch Request		
File	Source Type	UNC Path ~	
Batch	Source Enclave	DCIPDRR ~	
Rescan	Scan Type	Move ~	
	Move Action	Delete ~	
	Scan Subfolders	ON	
	Description*	Move Files	
	Scheduled Time	Every minute  0 0/1 *** ?	
		SUBMIT .	
			-

## 726 25. Click **Submit**.

727 26. Now, you can verify that files which are added to the public share with sensitive keywords are728 moved to the share designed to hold sensitive files.

## 729 **2.7 Cisco Duo**

- 730 Cisco Duo is a Multi-Factor Authentication and Single Sign-On tool. In this project, Dispel is used to
- control access to internal systems through virtualization, and Duo is used as a multifactor authentication
- solution between Dispel and those internal systems. This ensures that even if a Dispel virtual machine
- 733 becomes compromised, there is still significant access control between that machine and the internal
- 734 enterprise machines.
- In the following section, we demonstrate the installation of Cisco Duo on an internal system in such a
   way that RDP and local login to that system is protected by multifactor authentication.

## 737 Installing Cisco Duo

- 7381. Begin by logging into the system you wish to protect with Duo.
- 739 2. Then connect to the internet, if not connected already, and go to the Duo Admin login page at
   740 <u>https://admin.duosecurity.com/</u>.

	Admin Login
Enter you	r admin credentials
Email address	
	email address for next time lended for public or shared computers
	Continue
	your organization with Duo? Start a free trial

741 3. Login with your admin credentials and dual factor authentication until the admin dashboard is742 reached.

Dashboard	Deckher	l					
Policies	Dashboa	ara					Add Nev
Applications	Users						
Users	0	0	5	1	Administrators		
Groups	-	U Locked Out	Inactive				
2FA Devices		View	View	2	2FA Devices		
Administrators	4 Licenses Rei	maining		1	Groups		
Reports							
Settings	6 Total Users			471	Remaining Telephony Cred	its	
Billing							

- 743 4. Click **Applications** in the sidebar.
- 7445. Click Protect an Application.

<b>DUC</b>	Q Search for users, groups, applications, or devices	MITRE MITRE   ID: 2636-3111-77 Michael Ekstrom ~
Dashboard	Dashboard > Applications	
Policies	Applications	Protect an Application
Applications	Applications	
Protect an Application		
Users	Manage your update to the new Universal Prompt	
Groups	experience, all in one place.	
2FA Devices		
Administrators	See My Progress Get More Information	
Reports		
Settings	4 0	
Billing	All Applications End of Support	
Need Help?		Export ~

745 6. Search for, or scroll down to, **Microsoft RDP**.

## 746 7. Click **Protect**

<b>DU</b> O	<b>Q</b> Search for users, groups, applications, or devices	MITRE	MITRE   ID: 2636-3111-77	Michael Ekstrom 🗸
Dashboard	Dashboard > Applications > Protect an Application			
Policies	Protoct on Application			
Applications	Protect an Application			
Protect an Application	RDP			
Users				
Groups	Application	Protection Type		
2FA Devices				
Administrators	Microsoft RDP	2FA	Documentation 🗹	Protect
Reports				

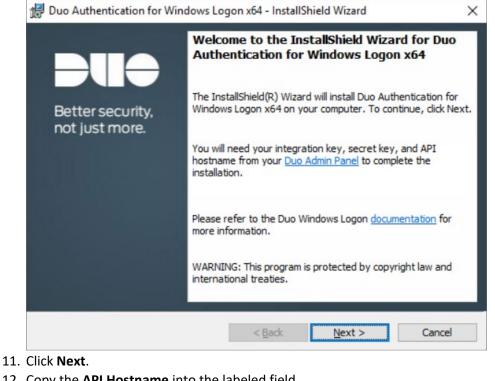
747 748 749 8. The next screen will provide policy configuration options, as well as the **Integration Key**, **Secret Key**, and **API hostname**, which are required information for the next step. Either keep this window open or copy down those three pieces of information.

Applications Protect an Application	Dashboard > Applications > M	icrosoft RDP 3			
Users	Microsoft RI	DP 3		Authentication Log	Remove Application
Groups	See the RDP documentation	to integrate Duo into your Microsoft RDP deployment.			
2FA Devices					
Administrators	Details				Reset Secret Key
Reports	Integration key	DIZQ2S5DXMVCA2FBVEMM	Сору		
Settings					
Billing	Secret key	T88F	Сору		
		Don't write down your secret key or share it with anyone.			
Need Help?					
Upgrade your plan for support.	API hostname	api-9d22ea89.duosecurity.com	Сору		
Versioning Core Authentication Service:					

753

750 9. Download the Duo Authentication for Windows Logon installer package, located at 751 https://dl.duosecurity.com/duo-win-login-latest.exe.

#### 10. Run the downloaded EXE file.



		Duo Connectivity Check Please enter the hostname for your integration to verify connectivity
Details		API Hostname:
Integration key	DI8SZS91SLPZGWEEHZWG	api-9d22ea89.duosecurity.com This hostname can be found in the <u>Duo Admin Panel</u> under Applications, configure or select a Microsoft RDP application.
Secret key	Don't write down your secret key or share it with anyone.	Copy Proxy Host: Proxy Host: Proxy Port:
API hostname	api-9d22ea89.duosecurity.com	Сору
		InstallShield

- 754 13. Click Next.
- 755 14. Copy in the Integration and Secret Keys into the relevant fields and click Next.

🛃 Duo Authentication for Windov	vs Logon x64 - InstallShield Wizard	×
Duo Security Account Details		
Please enter the keys provided by	y Duo Security	
Integration Key:		
DI8SZS91SLPZGWEEHZWG		
Secret Key:		
These keys can be found in the D a Microsoft RDP application.	<u>uo Admin Panel</u> under Applications, co	nfigure or select
Please refer to the Duo Windows	Logon <u>documentation</u> for more inform	ation.
	< Back Next >	Cancel
	C DOCK NEXT >	Cancer
lick <b>Next</b> .		

15. Clic

756

759

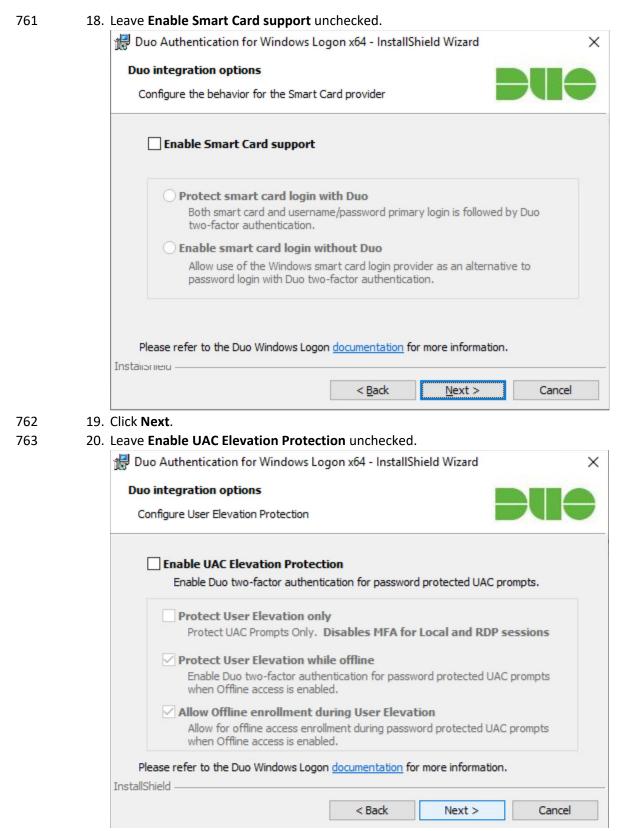
757 16. Configure Duo's integration options according to the needs of your organization. Note that 758

Bypass Duo authentication when offline will allow users to skip the two-factor authentication

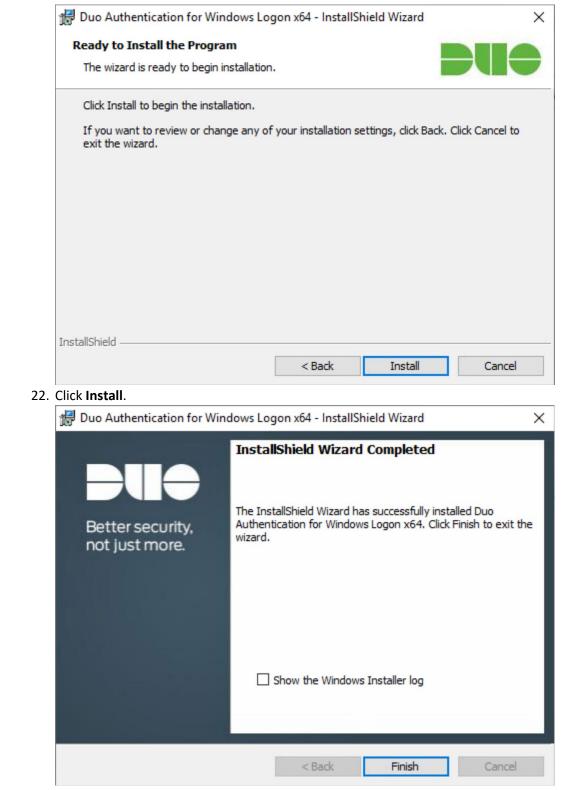
when offline, which increases the availability of their files but may increase risk.

🖟 Duo Authentication for Windows Logon x64 - InstallShield Wizard									
Duo integration options									
Configure the integration below									
Bypass Duo authentication when	n offline (Fai	Open)							
Enable this option to allow user logon without completing two-factor authentication if the Duo Security cloud service is unreachable. If you plan to enable offline access with MFA consider disabling FailOpen to prevent un-enrolled users from logging in.									
	Use auto push to authenticate if available Automatically send a Duo Push or phone call authentication request after primary credential validation.								
Only prompt for Duo authentication when logging in via RDP Leave this option unchecked to require Duo two-factor authentication for local logon and RDP sessions. If enabled, local logons do not require 2FA approval.									
Please refer to the Duo Windows Logon <u>doc.</u> InstallShield	<u>imentation</u> for	more informatior	۱.						
	< Back	Next >	Cancel						

#### 760 17. Click Next.



#### 764 21. Click **Next**.



768

765

- 23. Click Finish.
- 24. Installation should now be complete. Users registered on the Duo Dashboard with a linked phone will be allowed access to the system.

## 769 Registering a Duo User

1. Login to the Duo Admin Dashboard.

DUO	Q Search for use	ers, groups, applic	ations, or devices			MITRE	MITRE   ID	2636-3111-77	Michael Ekstrom 🗸
Dashboard	Deebbe	ard							
Policies	Dashbo	Dashboard							Add New 🗸
Applications	Users	Users							User
Users			_						Application
Groups	0	0	5	1	Administrators				Group
2FA Devices	Bypass Users View	Locked Out View	Inactive View	2	2FA Devices				
Administrators	4 Licenses	Remaining		1	Groups				
Reports									
Settings	6 Total Use	rs		463	Remaining Telephon	y Credits			
Billing									

2. Click **Add New > User** from the drop-down menu on the right.

## 7723. Enter a username for the user.

Policies	Add User									
Applications		Most applications allow users to enroll themselves after they complete primary authentication.								
Users		Learn more about adding users 🗗								
Add User										
Pending Enrollments										
Bulk Enroll Users	Username	userName								
Import Users		Should match the primary authentication username.								
Directory Sync										
Bypass Codes										
Groups		Add User								
2FA Devices										

#### 773 4. Click **Add User**.

This will lead you to that user's information page, where additional information (full name, email, phone number) and Duo authenticators (phone numbers, 2FA hardware tokens, WebAuthn, etc.) can be associated with that username. Note: A user will not be able to log into a Duo protected system unless the user is registered and has an authentication device associated with their username.

## 779 **2.8 Dispel**

- 780 Dispel is a network protection and user access tool that we used to provide a Virtual Desktop
- 781 Infrastructure (VDI) capability. A typical deployment of Dispel is done in a largely managed fashion, with
- a specific deployment being tailored to a network setup. The deployment in the NCCoE laboratory may
- not be the best setup for any given network. The NCCoE deployment was done on an Ubuntu host with
- 784 WAN and LAN interfaces, placing the device in-line between the enterprise systems and the external
- 785 network.

### 786 Installation

Deploy an Ubuntu machine with the provided specifications, ensuring that a provided ISO is
 attached to the device.

#### 789 2. Login with username "dispel" and the password provided.

dispelwicket login: dispel Password: Linux dispelwicket 4.19.195–amd64–vyos #1 SMP Thu Feb 17 12:52:59 UTC 2022 x86\_6 4 Welcome to VyOS!

Check out project news at https://blog.vyos.io and feel free to report bugs at https://phabricator.vyos.net

You can change this banner using "set system login banner post-login" command.

VyOS is a free software distribution that includes multiple components, you can check individual component licenses under /usr/share/doc/\*/copyright

## dispel@dispelwicket:~\$

```
7903. Being the installation process
```

```
791 > install image
```

```
dispel@dispelwicket:~$ install image
Welcome to the Dispel Wicket ESI install program. This script
will walk you through the process of installing the
Dispel Wicket ESI image to a local hard drive.
Would you like to continue? (Yes/No) [Yes]:
```

#### 4. Press enter on the following three prompts, modifying any default options as desired.

6. Press enter on the remaining prompts, modifying any default options as desired.

		How big of a root partition should I create? (2000MB – 150323MB) [150323]MB:
		Creating filesystem on /dev/sda1: OK Done!
		Mounting /dev/sda1 What would you like to name this image? [999.202203220259]: OK. This image will be named: 999.202203220259 Copying squashfs image Copying kernel and initrd images
		Done! I found the following configuration files: /opt/vyatta/etc/config/config.boot /opt/vyatta/etc/config.boot.default Which one should I copy to sda? [/opt/vyatta/etc/config/config.boot]:
		Copying /opt/vyatta/etc/config/config.boot to sda. Enter password for administrator account Enter password for user 'dispel':
795	7.	Enter and re-enter a new password for the user dispel
		Enter password for administrator account Enter password for user 'dispel': Retype password for user 'dispel': I need to install the GRUB boot loader. I found the following drives on your system: sda 150323MB
		Which drive should GRUB modify the boot partition on? [sda]:
796	8.	Press enter one final time to finish the installation
		Which drive should GRUB modify the boot partition on? [sda]:
		Setting up grub: OK Done!
797	۵	dispel@dispelwicket: ~*\$
798		Log in with the user "dispel" and the new password set in step 9.
		UNAUTHORIZED USE OF THIS SYSTEM IS PROHIBITED!
		Hint: Num Lock on
		dispelwicket login: dispel
		Password: Linux dispelwicket 4.19.195–amd64–vyos #1 SMP Thu Feb 17 12:52:59 UTC 2022 x86_6 4
		∀ Welcome to VyOS!
		Check out project news at https://blog.vyos.io and feel free to report bugs at https://phabricator.vyos.net
		You can change this banner using "set system login banner post-login" command.
		VyOS is a free software distribution that includes multiple components, you can check individual component licenses under /usr/share/doc/*/copyright
		dispel@dispelwicket:~\$
		Turne in the common deal is for an firm to success the start Marifest the partment to make sure it motoles

11. Type in the command > ifconfig | grep inet. Verify the output to make sure it matches the desired network configuration. If not, see the next section.

804 805

806 807

808

809

dispel@dispelwicket:~\$ ifconfig | grep inet inet addr:10.33.53.194 Bcast:10.33.53.207 Mask:255.255.255.240 inet6 addr: fe80::250:56ff:fead:223e/64 Scope:Link inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host dispel@dispelwicket:~\$

## 801 Configuring IP Addresses

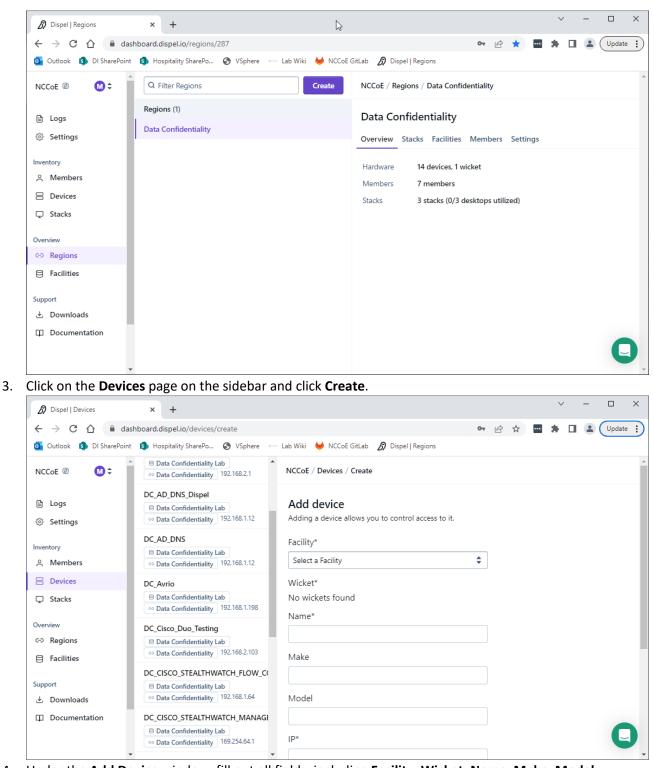
802 1. Login to the device with the user "dispel".

	UNAUTHORIZED USE OF THIS SYSTEM IS PROHIBITED!
	Hint: Num Lock on
	dispelwicket login: dispel Password: Linux dispelwicket 4.19.195–amd64–vyos #1 SMP Thu Feb 17 12:52:59 UTC 2022 x86_6
	4 Welcome to VyOS!
	Check out project news at https://blog.vyos.io and feel free to report bugs at https://phabricator.vyos.net
	You can change this banner using "set system login banner post–login" command.
	VyOS is a free software distribution that includes multiple components, you can check individual component licenses under /usr/share/doc/*/copyright
	dispel@dispelwicket:~\$
2.	Type in the command > configure.
	dispel@dispelwicket:~\$ configure [edit] dispel@dispelwicket# _
3.	Type in the command > del interfaces ethernet eth0, or whichever interface you
	are currently modifying. dispel@dispelwicket# del interfaces ethernet eth0
	[edit] dispel@dispelwicket# _
4.	Type in the command > set interfaces ethernet eth0 address followed by the
	desired IP address in CIDR notation, modifying for the desired interface as appropriate.
	dispel@dispelwicket# set interfaces ethernet eth0 address 192.168.2.213/28 [edit] dispel@dispelwicket# _
5.	Type in the command > commit.
	dispel@dispelwicket# commit [edit] dispel@dispelwicket#
6.	Type in the command > save.

		dispel@dispelwicket# save Saving configuration to '/config/config.boot' Done [edit] dispel@dispelwicket# _
810	7.	Type in the command > exit.
		dispel@dispelwicket# exit
811		exit dispel@dispelwicket:~\$
812	Config	guring Network
813	The foll	owing instructions are to modify a Dispel wicket device to forward traffic to a different routing
814	device.	This may be desirable for some network setups.
815	1.	Type in the command > configure to the Dispel wicket device after logging in.
010		dispel@dispelwicket:~\$ ifconfig   grep inet
		inet addr:10.33.53.194 Bcast:10.33.53.207 Mask:255.255.255.240 inet6 addr: fe80::250:56ff:fead:223e/64 Scope:Link inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host dispel@dispelwicket:~\$ configure
		[edit] dispel@dispelwicket#
816	2.	Type in the command > set protocols static route 0.0.0/0 next-hop
817		followed by the IP address of the router you wish to forward to.
		dispel@dispelwicket# set protocols static route 0.0.0.0/0 next-hop 192.168.1.1 [edit] dispel@dispelwicket#
818	3.	Type in the command > commit.
		dispel@dispelwicket# commit [edit] dispel@dispelwicket#
819	4.	Type in the command > save.
		dispel@dispelwicket# save Saving configuration to '/config/config.boot' Done [edit] dispel@dispelwicket# _
820	5.	Type in the command > exit.
		dispel@dispelwicket# exit exit dispel@dispelwicket:~\$
821	6.	On the designated router or firewall, ensure UDP is allowed from the Dispel device on the
822		provided port. For the NCCoE deployment, port 1194 was utilized. A target destination for the
823		traffic will be provided by Dispel.
824	7.	Modify the IP addresses of the south-side network interface to properly align with your
825		network. See the "Configuring IP Addresses" section above.

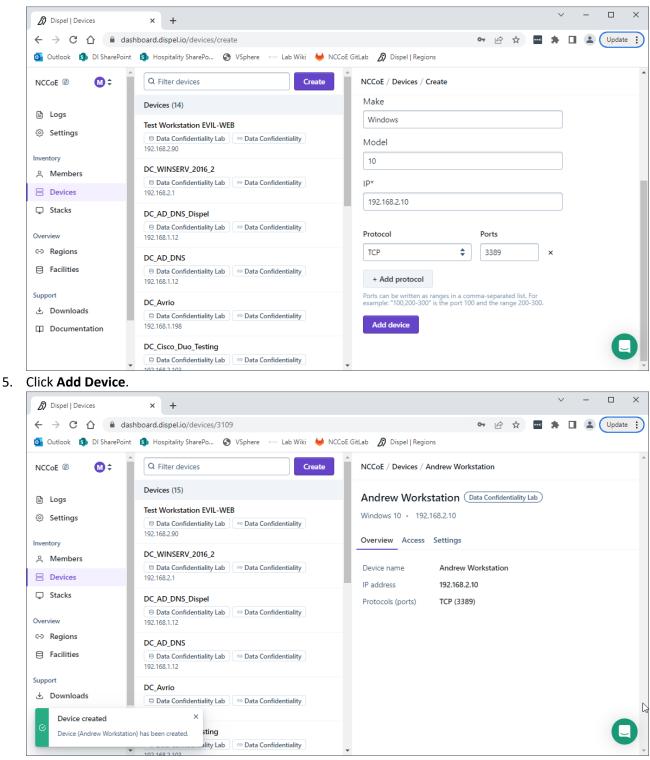
## 826 Adding a Device

- 827
   1. On the workstation in question, ensure that ping and RDP are accessible, including allowing such
   828
   connections through a local firewall.
- 829 2. Authenticate to the Dispel webpage with the provided credentials.



830

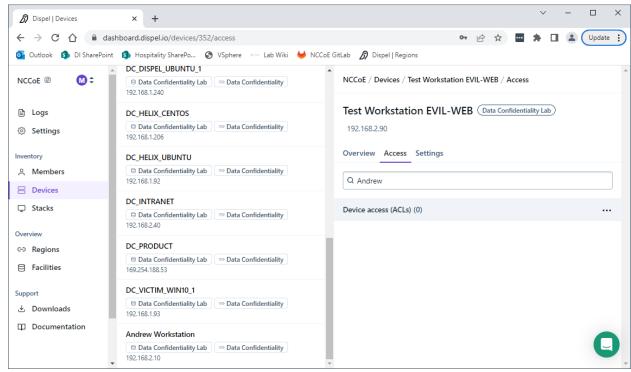
4. Under the Add Device window, fill out all fields, including Facility, Wicket, Name, Make, Model, IP, and Protocol.



833

Under Access for that device, search for the user(s) that will have access to that device. Verify they have the correct access settings.

#### DRAFT



836
 7. If a user is not already a member of the region, click **Members** in the sidebar and click **Invite.** Fill
 837 out relevant information for this individual and click **Invite this Member.**

## 838 2.9 Integration: FireEye Helix and Symantec SWG

839 In this integration the output of the web isolation tool, Symantec SWG, will be forwarded to our SIEM,

840 FireEye Helix. In this guide, we will aim to forward most logs to our SIEM, which can collect, analyze, and

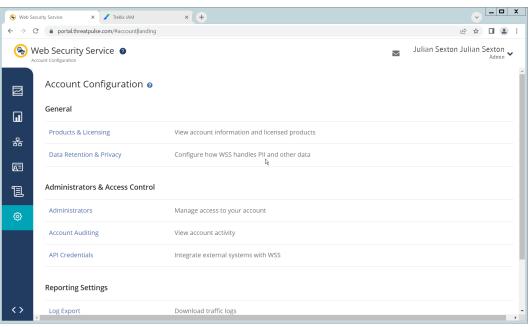
841 report on these logs to better maintain awareness of our systems and provide a single interface for

analyzing the health of the system. Logs from WSS will allow us to see statistics on the number of

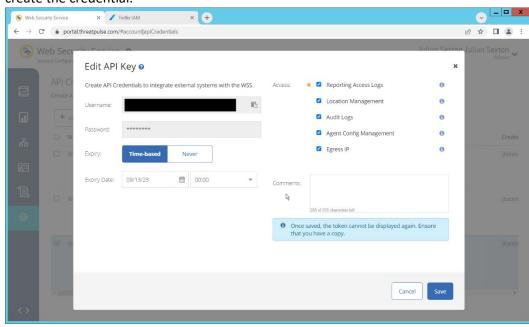
843 threats which have been blocked, as well as any administrative changes made to the WSS product.

## 844 Configure Fireye Helix to Collect Logs from Symantec SWG

- 1. Navigate to the Symantec dashboard, and login.
- 2. Navigate to **Account Configuration** by clicking the gear icon on the left sidebar.



- 847 3. Click API Credentials.
- 848 4. Click **Add**.
- 849 5. Check the boxes next to Reporting Access Logs, Location Management, Audit Logs, Agent Con 850 fig Management, and Egress IP.
- 851 6. Set an **Expiration Date** for the credential (1 year recommended).
- 852 7. Copy the Username and Password provided, as you will not be able to retrieve these once you853 create the credential.



854

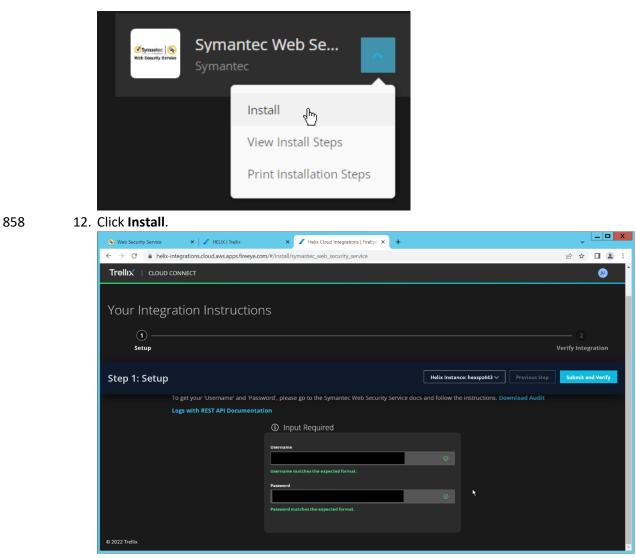
8. Click Save.

Neb Security S	iervice ×	HELIX   Trellix	×	+						•		X
· ·	apps.fireeye.com/heli		~	Ŧ						IR 🕇		
_		IX/10/11EX3p2445/										
Trellix	HELIX			Dashboards 🛩	Investigate 💙	Explore 🛩	Configure 🔨	Manage	<ul> <li>DOC-NIST-NC.</li> </ul>	15 Q	<u>+</u> (	<u> </u>
							Lists					
Summa	ary Dashboa	ard					Rules			ē.	rint As PD	F
A dashboard	tailored to all users.	Use this view t	o get a quick s	ynopsis of what	's going on in y	our environme	Rule Packs	Trellix	dashboard, it is n	ot editable. L	earn More	
			Overall Risk Sco	•			Searches					
	lert Correlations	View All	Overall Risk Sco	ore 💔			Network	œ		View All	Correlatior	ıs
Asset		Risk Score										
	No Entities to display.						Cloud Conn	. &				
								Ŭ				
			0	3/17 08/18 08/19 08/20 0	B/21 0B/22 0B/23 0B/24	08/25 08/26 08/27 08/2	28 08/29 08/30 08/3	31 09/01 09/02 09	03 09/04 09/05 09/06 09/07	09/08 09/09 09/10 0	av11 09v12 0	- <b>•</b> 9/13
Recent Alerts							View Alerts	s Index	Recent Alerts			
Risk	Name			Origin	Events	Last Updated						
<ul> <li>Medium</li> </ul>	SYSTEM MONITORING [	Events Missing for I	Day - ms_windo	fireeye rule	1 hit	a year ago						x

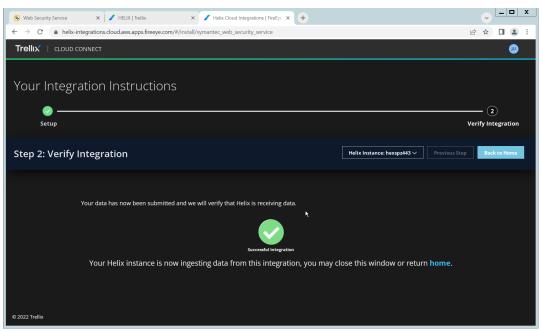
9. On the Helix Dashboard, click **Configure > Cloud Connect**.

🛞 Web !	Security Service	× / HELIX   Trell	ix ×	/ Helix Cloud Integra	tions   FireEye × +	)			-□
← →	C 🌲 helix-integ	grations.cloud.aws.apps		=%5B%5D					e ☆ □ 🏝
Trelli	🗙 🕴 CLOUD CON	INECT							
Clou	ud Conne	ect							
Add and Helix.	l manage cloud con	nnections for			• • •	• •	Last Update: 2022-09-12T13:0	5:22-04:00 🍤 🕀 A	dd Cloud Connection
	Name All ~	Vendor All ~	Identifier Search 1 records	Sensor ID Search 1 records	Helix ID Search 1 records	Status All	Created <sup>®</sup> ∽	Last Event <sup>③</sup>	Last Poll <sup>®</sup>
	Duo Auth	Duo Security	DI4ERNLR0C3L2I	1654094729300	hexspz443	•	3 months ago	3 months ago	an hour ago
Rows per	Page 10 25 <b>50</b>							1 - 1 of 1	
2022 Tr	ellix								

- 856 10. Click Add Cloud Connection.
- 857 11. Click the arrow next to Symantec Web Security Service.



- 859
  - 9 13. Enter the username and password from the credential created earlier.



- 860 14. Click **Submit and Verify**.
- 15. Click **Back to Home**. You will now be able to see events from Symantec WSS in Helix.

# 862 2.10 Integration: FireEye Helix and PKWARE PKProtect

863 In the following section, PKWARE PKProtect, which has been configured to identify and encrypt sensitive

data, will be configured to forward these events to FireEye Helix. Logs from PKWARE PKProtect will

allow us to monitor the use of encryption throughout the enterprise, and catch any suspicious

866 decryptions which may indicate a breach. This section assumes the Helix Communications Broker has

867 already been installed.

#### 868 Configure the Helix Communications Broker

- 869 1. On the CentOS system with the Helix Communications Broker installed, run the following
   870 commands:
- 871 > cd /opt/tap-nxlog
- 872 > sudo ./setup.sh
- 873 2. Select Add Routes and press Enter.
- 874 3. Select **bsd**.
- 875 4. Select **tcp**.
- 5. Select the IP address of the network interface which should receive logs.
- 877 6. Enter 513 for the port.

administrator@localhost:/opt/tap-nxlog	-		×
File Edit View Search Terminal Help			
INPUT SOURCE SETUP::ADD			
Input Type () syslog () json (X) bsd			
Protocol Type () udp (X) tcp () ssl Input Interface			
() 192.168.122.1 (X) 192.168.1.206 () 127.0.0.1			
Input Port <b>513</b>			
Cancel		OK	

- 878 7. Select **OK** and press **Enter**.
- 879 8. Select **OK** and press **Enter**.

#### 880 Configure PKWARE PKProtect to Forward Events

- 1. Navigate to the PKWARE PKProtect web portal.
- 2. Click the **Basics** link at the top of the page.
- 3. Scroll down to the **Data Security Intelligence** section.
- 4. Next to Dashboard Elasticsearch Target, click Internal.
- 5. Uncheck the box next to **Use Internal Elasticsearch**.
- 6. Uncheck the box next to **Enable DSI in Dashboard**.

💙 HELIX   FireEye 🗙 🛛 🖬 EdgeF	W-PFS.I0115.Jabs.nccoe.nis × 🛞 Basics	× 🚥 Creating and Deploying Classific: ×   +	• • • • ×
← → C ▲ Not secure   192.168.1.43/m	nds/SuperUser/Basics		🖈 😩 Update 🔅
PKWARE* Actions	System Basics Advanced Dashboard Archive I	Events	Help Log out Change Password
Dashboard Elasticsearch Target			
Enable DSI in Dashboard	Save Cancel		
	PKWARE Enterprise Manager 18.5.2	.203 - <u>About</u> - powereviti 5/25/21 11:13:42 AM	

- 887 7. Click **Save**.
- 888 8. In the **Data Security Intelligence** section, click **Internal** next to **Target**.

- 889 9. Select Syslog TCP RFC-3164 for Target.
- 10. Enter the URL and port of the Helix Communications Broker that was just configured.

C     A     Not sec	ure   192.168.1.43/mi	ds/SuperUser/Basics		🖈 😩 🛛 Upd
KWARI	Actions 5	ystem Basics Advanced Dashbo	oard Archive Events	Help L Change Pa
ta Security Intellig	jence Target			
	Target	Syslog TCP RFC-3164	<b>*</b>	
	Url	192.168.1.206:513		
		Save Cancel		

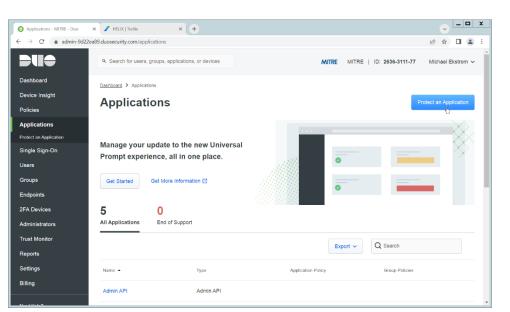
- 891 11. Click **Save**.
- 892 12. Verify that PKWARE logs now show up in Helix.

# 893 **2.11 Integration: FireEye Helix and Cisco Duo**

- In this integration, FireEye Helix will be configured to collect logs from Cisco Duo. Cisco Duo is our multi factor authentication mechanism and acts as source of information both for detecting breaches and for
- detecting insider threats. Information about a login, such as the username, time, location, are all usefulin the event of a breach. Furthermore, they are useful as a baseline for user activity, which can be used
- and the event of a breach. Furthermore, they are useful as a baseline for user activity, which can be use
- as a comparison point for detecting unusual behavior.

#### 899 Configure Fireye Helix to Collect Logs from Cisco Duo

900 1. On the Cisco Duo dashboard navigate to **Applications**.

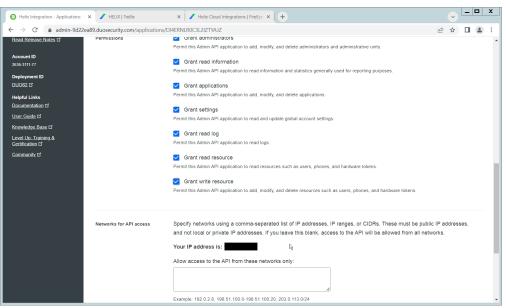


#### 901

2. Click Protect an Application.

Protect an Application - Applicati	HELIX   Trellix × +			✓ _ □ ×	
$\leftrightarrow$ $\rightarrow$ C $(a)$ admin-9d22ea8	39.duosecurity.com/applications/protect/types			🖻 ☆ 🔲 😩 :	
<b>BIIC</b>	Search for users, groups, applications, or devices	MITRE	MITRE   ID: 2636-3111-77	Michael Ekstrom $\checkmark$	•
Dashboard	Dashboard > Applications > Protect an Application				
Device Insight	Protect an Application				
Policies					
Applications	Filter by keywords: VPN, Microsoft, SAML				
Protect an Application					
Single Sign-On	Application	Protection Type			
Users	•				
Groups	1Password	2FA	Documentation Ľ	Protect	
Endpoints					
2FA Devices	AWS Directory Service	2FA	Documentation 🗗	Protect	
Administrators					
Trust Monitor	Admin API	2FA	Documentation 🗗	Protect	
Reports					
Settings					
Billing	Aeries SIS	2FA	Documentation ⊡	Protect	
					Ŧ

#### 902 3. Click Admin API.



- 9034. Scroll down and check the boxes next to Grant administrators, Grant read information, Grant904applications, Grant settings, Grant read log, Grant read resource, and Grant write resource
- 905 5. Click **Save**.
- 906 6. Login to the Helix dashboard.
- 907 7. Navigate to **Configure** > **Cloud Connect**.
- 908 8. Click See Available Connections.
- 909 9. Type "Duo" in the Search box.

O Admin API 1 - Applications - MIT × / HELIX   Trellix × / Helix Cloud Integrations   FireEy: × +	✓ _ □ ×
← → C	🖻 🖈 🖪 😩 i
Trellix   CLOUD CONNECT	
© Back to Installed Connections Add Connection (1 Available)	
due Q	
Jump to Category: Identity and access management (1)	
Identity and access management	
Duo Auth Duo Security	
Install 🚯	
View Install Steps Print Installation Steps	
Print installation steps	
© 2022 Trelix	

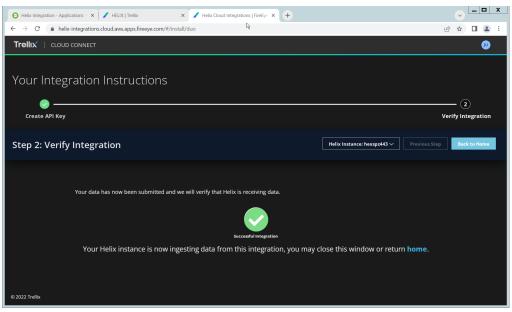
- 910
- 10. Click the Arrow next to the Cisco Duo integration and click Install.

Admin API 1 - Applications - MIT	× / HELIX   Trellix	× +				✓ - □ ×	
$\leftarrow$ $\rightarrow$ C $\triangleq$ admin-9d22	ea89.duosecurity.com/application	JDI4ERNLR0C3L2IZTYAJZ				🖻 🖈 🔲 😩 :	
DUO	<ul> <li>Search for users, groups</li> </ul>	applications, or devices		MITRE	MITRE   ID: 2636-3111-77	Michael Ekstrom $ \sim $	Â
Dashboard							
Device Insight	Successfully adde	d Admin API to protected ap	plications. Add another.				I
Policies							I
Applications	Dashboard > Applications >						I
Protect an Application	Admin API	1			La	Remove Application	
Single Sign-On	Setup instructions are in t	ne Admin API documentation	1 <b>2</b> .				
Users	The Admin API allows you t	programmatically create, re	etrieve, update, and delete u	isers, phones, hard	ware tokens, admins, application	a, and more.	
Groups							
Endpoints	Details					Reset Secret Key	
2FA Devices	Integration key			Сору			
Administrators							
Trust Monitor	Secret key			Сору			
Reports		Don't write down your secre	t key or share it with anyone.				
Settings	API hostname			Сору			
Billing							
	Sottings						-

911 11. Copy the Integration Key, Secret Key, and API hostname (not including duosecurity.com) to the
 912 appropriate fields on the Helix Cloud Connect page.

🕒 Admin API 1 - Applications - MIT 🗙 🛛 🖌 HELIX   Trellix	× / Helix Cloud Integrations   FireEye × +		✓ - □ ×
$\leftarrow$ $\rightarrow$ C $($ helix-integrations.cloud.aws.apps.fireeye.cd	pm/#/install/duo		🖻 🖈 🔲 😩 🗄
			•
Your Integration Instruction ① 	าร		2 Verify Integration
Step 1: Create API Key		Helix Instance: hexspz443 V Previous	Step Submit and Verify
Create an API key in the Duo Secu below and click Submit and Verify	rity admin console by following these instructions. Enter A ① Input Required	r the integration key, secret key, and API host	name
	Integration Key Base84 client ID	k	
	Secret Key           Base64 secret           Display hidden value		

913 12. Click **Submit and Verify**.



13. If successful, you should see a screen about the integration being successful.

# 915 2.12 Integration: FireEye Helix and QCOR ForceField

916 In this integration, we will configure the collection of logs from ForceField, our database encryption

- 917 solution, into FireEye Helix. Detailed logs describing encryption and decryption are useful for
- 918 determining how much of an enterprise is encrypted, and statistics and records in this area can prepare

the organization for the event of a breach. For the purposes of this guide, we will assume ForceField is

920 running on a Windows Server, and we would like to transfer files from this server to a Linux server. If

- 921 you are using a Linux server for ForceField, you can skip to the configuration of rsyslog to forward logs
- 922 directly to the Helix Comm Broker.

### 923 Configure an SFTP server on Windows

- 924 In this section, we will configure an SFTP server on the Windows system to allow for encrypted,
- automated download of Forcefield's logs onto a Linux server. We have specifically elected not to use
- 926 Windows SMB for this scenario because we would like to demonstrate an encrypted transfer of logs
- 927 from Windows to Linux. We chose SFTP over FTPS because automation of FTPS would at some point
- 928 require a plaintext password, while SFTP can default to the system's SSH capabilities.
- Once on Linux, rsyslog can be configured to use TLS for encrypted transfer according to the needs of theorganization.
- Download OpenSSH from here (<u>https://github.com/PowerShell/Win32-OpenSSH/releases</u>). During the creation of this guide, version V8.9.1.0p1-Beta was used.
   Extract to C:\Program Files\OpenSSH.
   In a Powershell window, navigate to the folder you extracted it to, and run the following command to install the server.
   powershell.exe -ExecutionPolicy Bypass -File ./install-
- 937 sshd.ps1
- 938 4. Run the following command to open the firewall port for OpenSSH.

020		
939		Run New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH
940		SSH Server' -Enabled True -Direction Inbound -Protocol TCP -
941		Action Allow -LocalPort 22 -Program
942		"C:\Windows\System32\OpenSSH\sshd.exe"
943		Open services.msc and start the OpenSSH SSH server.
944	6.	Create a file called authorized_keys in C:\Users\ <your username="">\.ssh. If needed, create the</your>
945		.ssh folder (Windows will not allow you to create it by default – naming the folder .ssh. will al-
946		low you to bypass this restriction.)
947	7.	Generate a key using ./ssh-keygen. Copy the contents of the generated public key (.pub file)
948		into the <b>authorized_keys</b> file created earlier. The private key should be placed in the <b>~/.ssh</b>
949		folder on the Linux machine.
950	8.	Right click the authorized_keys file and click Properties.
951	9.	Click Disable Inheritance.
952	10	. Select Convert inherited permissions into explicit permissions on this object.
953		. Using the remove button, remove all accounts other than SYSTEM from the list. Ensure that the
954		SYSTEM account has full control.
955	12	. Under C:\ProgramData\ssh, open sshd_config.
956	13	. Comment out these lines by adding '#' characters before each line, like so:
957		#Match Group administrators
958		# AuthorizedKeysFile
959		PROGRAMDATA /ssh/administrators authorized keys
960	14	. Add the following lines to the <b>sshd_config</b> file to ensure that RSA public key authentication is
961		allowed.
962		PubkeyAuthentication yes
963		PubkeyAcceptedKeyTypes=+ssh-rsa
964	15	. Add the directory C:\Program Files\OpenSSH to the system path – this is necessary so that the
965		server can find the sftp-server.exe file.
966	16	. Add the following lines to <b>sshd_config</b> file to configure the SFTP server.
967		ForceCommand internal-sftp
968		ChrootDirectory C:\GreenTec\ForceField\log
969	17	. Alternatively, if it's preferable to set the root directory somewhere else and move the log file,
970		you can also do that. To edit the log file location, simply open C:\GreenTec\Forcefield\wfs.conf
971		and change <b>Logpath</b> to a different directory, and update <b>ChrootDirectory</b> to point to that.
972	18	. After doing this, you should be able to authenticate over SSH to the server. If the authentication
973		fails, you can check the logs in Event Viewer on the server, under <b>Applications and Services Logs</b>
974		> OpenSSH > Operational to see the reason for the failure.
		· ·
975	Confi	gure the Linux Machine to Download and Send Logs to the Helix
070	Com	munications Proker

- 976 Communications Broker
- 977 19. On the Linux server, we can use sftp to download the file. Ensure that you replace the username and hostname of your actual SSH server.
   979 sftp administrator@forcefield.dc.ipdrr:/ForceField.log
   980 /tmp/ForceField.log
   981 20. For automation purposes, we can use cron jobs to automatically download this file at regular
- 982 intervals. Use crontab to edit the list of cron jobs.

983	Crontab -e
984	21. Enter the interval and command for sftp in the crontab file. The following line will download the
985	log file once an hour. Ensure that you replace the username and hostname with the username
986	and hostname of your actual SSH server.
987	0 * * * * sftp
988	administrator@forcefield.dc.ipdrr:/ForceField.log
989	/tmp/ForceField.log
990	22. Next, we will use <b>rsyslog</b> to forward this log file to the Helix Comm Broker.
991	23. Open /etc/rsyslog.conf, and add the following line, using the IP and port of the Helix Comm Bro-
992	ker. (Note that putting a single '@' symbol here indicates UDP. Use two, such as '@@' for TCP.)
993	*.* @192.168.1.206:514
994	24. Create a file <b>/etc/rsyslog.d/forcefield.conf</b> and enter the following lines in it.
995	<pre>sudo nano /etc/rsyslog.d/forcefield.conf</pre>
996	\$ModLoad imfile
997	\$InputFilePollInterval 10
998	\$PrivDropToGroup adm
999	<pre>\$InputFileName /tmp/ForceField.log</pre>
1000	\$InputFileTag FORCEFIELD
1001	\$InputFileStateFile Stat-FORCEFIELD
1002	\$InputFileFacility local8
1003	\$InputRunFileMonitor
1004	\$InputFilePersistStateInterval 1000
	\$ModLoad imfile
	<pre>\$InputFilePollInterval 10</pre>
	\$PrivDropToGroup adm
	<pre>\$InputFileName /tmp/ForceField.log</pre>
	<pre>\$InputFileTag FORCEFIELD</pre>
	<pre>\$InputFileStateFile Stat-FORCEFIELD</pre>
	<pre>\$InputFileSeverity forcefield</pre>
	<pre>\$InputFileFacility local8</pre>
	\$InputRunFileMonitor
	<pre>\$InputFilePersistStateInterval 1000</pre>
1005	25. Restart rsyslog.

1006

sudo service rsyslog restart

# 1007 2.13 Integration: FireEye Helix and Dispel

In this integration, we configure the collection of logs from Dispel, our network protection solution.
Because Dispel controls access from users to enterprise systems it is important to have an overview of
its actions through log collection and reporting. Dispel personnel can perform this integration by simply
providing them with the protocol, port, and IP address of the Helix Communications Broker and allowing
them to configure it on the on-premise Dispel wicket.

# 1013 **2.14 Integration: Avrio SIFT and PKWARE PKProtect**

1014 When used together, SIFT and PKProtect can protect sensitive data accidentally dropped into public

1015 shares on the enterprise. In <u>Section 2.6</u>, we detail how to configure SIFT to detect sensitive data in a

1016 Windows Share and move it to a location designated for sensitive information. Now, we will

1017 demonstrate how to ensure that location is protected by PKProtect, which will automatically encrypt the1018 data.

# 1019 Configuring PKWARE PKProtect

- 1020 1. Navigate to the PKProtect dashboard and login.
- 1021 2. Navigate to Archive > Discovery.

ЖИ	Policies Dis	tern Basics Advanced Dashboard Archive Events <sup>990</sup> covery Remediations Classification Communities Assignments Lockers eployments Devices Support	Help Log o Change Passwor
nart Filte	er Bundles Filter Name	Search: Search:	*
Discovery	HIPAA - Diagnosis Lexicon and Social Security Numbers	Social Security Number US (1 or more)         National Insurance Number UK (1 or more)         FDA Drugs Dictionary (5 or more)           FDA Firms Dictionary (5 or more)         ICD-9 Codes Dictionary (5 or more)         ICD-10 Codes Dictionary (5 or more)	Edit Clone Delete
Discovery	PCI-DSS - Credit Cards and Social Security Numbers	All Supported Credit Cards (1 or more)         International Bank Account Number (1 or more)           Social Security Number US (1 or more)         National Insurance Number UK (1 or more)	Edit Clone Delete
Discovery	Personally Identifiable Information	Social Security Number US (1 or more)         National Insurance Number UK (1 or more)         Tax ID US (1 or more)           Address US (10 or more)	Edit Clone Delete
Discovery	SSN Discovery	Social Security Number US (1 or more)	Edit Clone Delete
	Word Dictionary	Custom: Custom Dictionary Names (1 or more)	Edit Clone Delete

- 1022 3. Click Pattern Dictionary.
- 1023 4. Enter a name for these patterns in the **Name** field.
- 1024 5. Enter keywords to match in the **Keywords** field.

					x
🔀 SIFT   Secure Integrated File Tagg 🗙	S Archive - Discovery × +	~			
← → C ▲ Not secure   http:	r:// <b>pkwarevm.dc.ipdrr</b> /mds/SuperUser/Archive/Discovery	6 \$		-	:
PRVVARE	Actions System Basics Advanced Dashboard Archive Events <sup>999</sup> Policies Discovery Remediations Classification Communities Assignments Lockers Accounts Deployments Devices Support	(	Help Change	Log Passw	
Pattern - Dictionary					
Name Keywords	Custom Dictionary Names       Inalatar     drate     buffab     cakutta       Choose File     No file chosen     Load Dictionary       Match Whole Phrase     Match Case     D       Save     Cancel     D				]
	PCWARE Enterprise Manager 18.5.203 - <u>About</u> - pReament 1/25/23 54834 PM				

- 1025 6. Click **Save**.
- 1026 7. Click Add Discovery.
  - 8. Under **Pattern**, select the name of the **Pattern** you just created.
  - 9. For Threshold, enter the number of matches of this pattern needed to consider the file
- 1028 1029

1027

ensitive.			
😹 SIFT   Secure Integrated F	ile Tagg 🗙 🔇	Archive - Discovery × +	_ <b>_ </b>
← → C ▲ Nots	ecure   https://	pkwarevm.dc.ipdrr/mds/SuperUser/Archive/Discovery	🖻 🛧 🔲 😩 :
<b>PKW</b> AR	Pc	tions System Basics Advanced Dashboard Archive Events <sup>999</sup> licies Discovery Remediations Classification Communities Assignments Lockers counts Deployments Devices Support	Help Log ou Change Password
Discovery Smart Fi	lter Bundle		
	Filter Name	Word Dictionary	
Pattern Custom: Custom Dictiona	ry Names	Threshold	
Add Exclusions			
	Patterns		
Inclusions		Pe	
	Patterns		
Save Cancel			
		PC0XARE Enterprise Manager 18.5.203 - <u>abood</u> - privateum 1/25/23 546/54 PM	

- 1030 10. Click **Save**.
- 1031 11. Navigate to Archive > Lockers.
- 1032 12. Ensure that a PKWARE client is installed on the device which will be monitored for encryption.
- 1033The device should show up in the list. If it doesn't you can search for the device and select it1034from the list.

SIFT   Secure In	tegrated File Tag	g 🗙 🕲 Arc	hive - Lockers	× +					~		
→ C .	Not secure	https://pkwa	revm.dc.ipdrr/mds/S	uperUser/Archive/	Lockers				@ ☆		
evices											
Search											
earcn											
		Device									
Platform			Windows								
Owner											
Owner UPN											
Owner Email Last IP											
Search											
Show 10 entries											
							Last				
Device 🔺	Enabled	Platform	Application	Owner 🕴	Owner UPN	Owner Email	Accessed	Last IP 🔅	URN		
									WIN-	R	
DESKTOP-	Enabled	Windows	Smartcrypt	bob	bob@DC.IPDRR	bob@dc.ipdrr	6/3/21	192.168.1.156	376002ef- 7035-4cad-	Add	a
BN5BE26		Desktop	16.40.0010						90ac- 03508625d5d1		
									WIN-		
RDP1	Enabled	Windows	Smartcrypt	Administrator	Administrator@DC.IPDRR	Administrator@dc.ipdrr	Today at	192.168.1.80	585d6b62- 6cb9-4d3c-	Add	а –
		Server	16.40.0010				12:44:56 PM		9be3- 855028d8bd4f		÷.,
howing 1 to	2 of 2 entries								Previous 1	Nex	đ

- 1035 13. Click **Add** on the device you wish to add a locker for.
- 1036 14. Enter a **Name** for the locker.
- 1037 15. Enter the **path** to the protected folder.
- 1038 16. Select **AES 256** for the **Algorithm**.
- 1039 17. Select the PKWARE Smartkey to use.
- 1040 18. Check all the boxes next to **Encryption Events**.

SIFT   Secure Integrated File Tagg 🗙 🔞 A	rchive - Lockers × +	~	
→ C ▲ Not secure   https://pkw	varevm.dc.ipdrr/mds/SuperUser/Archive/Lockers	<i>Ŀ</i> ☆	
Name	ENCRYPT-STORAGE		
Path	C/Share/SECRET		 1
			 J
Algorithm	AES (256-bit)		
Smartkey	Community: Domain Users Commnity Key		
Whitelist			
Blacklist			
	Enable Scan-Only Mode		
	Scan-only mode disables the local file system watcher in the Locker Service.		
	Instead of reacting to real-time file system events, the Locker Service will perform traditional folder scans.		
Sweep Interval (seconds)	86400		
	Report Compliance and Status		
	Report Advanced File Attributes		
	Z Exclude Hidden Files		
	Z Exclude System Files		
Encryption Events	Report Successful Encryptions		
	Report Encryption Failures		
Discovery	Enable Discovery Mode		
Re-Encryption	Enable Re-Encryption		
Cancel			

- 1041 19. Check the box next to **Enable Discovery Mode**.
- 1042 20. Add the relevant rules to the **Smart Filter Bundles** box.
- 1043 21. Select **Report and Encrypt** for **Remediation Action**.

2	SIFT   Secure Integrate	d File Tag: X 🛞 Archive - Lockers X +		~	-		X		
$\leftarrow$	→ C 🔺 No	t secure   https://pkwarevm.dc.ipdrr/mds/SuperUser/Archive/Lockers	Ē	☆			:		
		<ul> <li>Report Advanced File Attributes</li> <li>Exclude Hidden Files</li> <li>Exclude System Files</li> </ul>					^		
	Discovery	Enable Discovery Mode							
	Remediation Ac	tions							
	*	Smart Filter Bundles Remediation Action							
	=	HIPAA - Diagnosis Lexicon and Social Security Numbers PCI-DSS - Credit Cards and Social Security Numbers Personally Identifiable Information SSN Discovery Word Dictionary N	<u>Del</u> e	<u>ete</u>					
	Showing 1 to 1 of 1 entries Add								
	Re-Encryption     Enable Re-Encryption       Save     Cancel								
	PKINARE Enterprise Manager 16.5.203 - <u>About</u> - privaterum 1/25/23 5/4008 PM								

- 1044 22. Click **Save**.
- 1045 23. Now the folder on the device you selected will be monitored, and files which match the selected1046 rules will be encrypted automatically.

#### 1047 2.15 Integration: Dispel and Cisco Duo

- 1048 In this build, Dispel acts as an intermediary between the user and enterprise systems, by providing
- 1049 temporary remote desktops with access to enterprise systems. In this integration, we primarily installed
- 1050 Cisco Duo on the enterprise systems, to require multifactor authentication over RDP between Dispel's
- 1051 temporary remote desktops and the enterprise systems.
- 1052 In this particular integration, no extra work was required other than installing Cisco Duo (see <u>Section</u>
- 1053 <u>2.7</u>) on systems to control remote desktop access between Dispel machines and the other machines.
- 1054 However, it is important for organizations to check that this integration works and is present, to ensure
- 1055 that multifactor authentication is being applied to users who are logging in remotely.

# 1056 Appendix A List of Acronyms

- 1057 Provide a list of alphabetized acronyms and abbreviations and spell out each one. Use Word Style:
- 1058 Glossary. Bold each acronym to enhance readability.

SIEM	Security Information and Event Management		
RDP	Remote Desktop Protocol		
IP	Internet Protocol		
ТСР	Transmission Control Protocol		
SFTP	Secure File Transfer Protocol		
DNS	Domain Name Service		
NTP	Network Time Protocol		
2FA	Two Factor Authentication		
UDP	User Datagram Protocol		
WSS	Web Security Service		
TLS	Transport Layer Security		
SSL	Secure Sockets Layer		
GPO	Group Policy Object		
PAC	Proxy Auto Configuration		
AES	Advanced Encryption Standard		
REST	Representational State Transfer		
ΑΡΙ	Application Programming Interface		
WFS	Write-protected File System		