NIST SPECIAL PUBLICATION 1800-29C

Data Confidentiality: Detect, Respond to, and Recover from 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 Corporatio

The MITRE Corporation McLean, Virginia

February 2024

FINAL

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-29

The first draft of this publication is available free of charge from: <u>https://www.nccoe.nist.gov/data-confidentiality-identifying-and-protecting-assets-against-data-breaches</u>



DISCLAIMER

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

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

National Institute of Standards and Technology Special Publication 1800-29C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-29C, 67 pages, (February 2024), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at <u>ds-nccoe@nist.gov</u>.

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Attacks that target data are of concern to companies and organizations across many industries. Data breaches represent a threat that can have monetary, reputational, and legal impacts. This guide seeks to provide guidance around the threat of data breaches, exemplifying standards and technologies that are useful for a variety of organizations defending against this threat. Specifically, this guide identifies standards and technologies that are relevant in the detection, response, and recovery phases of a data breach.

KEYWORDS

asset management; cybersecurity framework; data breach; detect; data confidentiality; data protection; malicious actor; malware; ransomware; recover; respond

ACKNOWLEDGMENTS

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

Name	Organization
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
Spike Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation

Name	Organization
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

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

Technology Partner/Collaborator	Build Involvement
Cisco Systems	DUO, Stealthwatch
Dispel	Dispel
FireEye	FireEye Helix
PKWARE	PKWARE PKProtect

DOCUMENT CONVENTIONS

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

PATENT DISCLOSURE NOTICE

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Contents

1	Intr	oduct	tion	1
	1.1	How t	o Use this Guide	1
	1.2	Build	Overview	2
	1.3	Турод	raphic Conventions	2
	1.4	Logica	al Architecture Summary	3
2	Pro	duct I	nstallation Guides	4
	2.1	FireEv	ve Helix	4
		2.1.1	Installing the Communications Broker	4
		2.1.2	Forwarding Event Logs from Windows 2012 R2	6
	2.2	PKWA	ARE PKProtect	9
		2.2.1	Configure PKWARE with Active Directory	9
		2.2.2	Create a New Administrative User	11
		2.2.3	Install Prerequisites	12
		2.2.4	Install the PKProtect Agent	15
		2.2.5	Configure Discovery and Reporting	18
	2.3	Cisco	Duo	23
		2.3.1	Installing Cisco Duo	23
		2.3.2	Registering a Duo User	30
	2.4	Cisco	Stealthwatch	31
		2.4.1	Configure Stealthwatch Flow Collector	31
		2.4.2	Configure Stealthwatch Management Console	34
		2.4.3	Add Stealthwatch Flow Collector to the Management Console	43
	2.5	Dispel	l	49
		2.5.1	Installation	49
		2.5.2	Configuring IP Addresses	52
		2.5.3	Configuring Network	54
		2.5.4	Adding a Device	55
	2.6	Integr	ation: FireEye Helix and Cisco Stealthwatch	58
		2.6.1	Configure the Helix Communications Broker	58
		2.6.2	Configure Stealthwatch to Forward Events	59
	2.7	Integr	ation: FireEye Helix and PKWARE PKProtect	61
		2.7.1	Configure the Helix Communications Broker	62

	2.7.2	Configure PKWARE PKProtect to Forward Events	.62
2.8	Integr	ation: FireEye Helix and Dispel	.64
2.9	Integr	ation: Dispel and Cisco DUO	.64
Append	A xib	List of Acronyms	65

List of Figures

1 Introduction

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 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 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.

1.1 How to Use this Guide

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 ability to detect, respond to, and recover from a loss of data confidentiality. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-29A: *Executive Summary*
- NIST SP 1800-29B: Approach, Architecture, and Security Characteristics what we built and why
- NIST SP 1800-29C: How-To Guides instructions for building the example solution (you are here)

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 1800-29A*, which describes the following topics:

- challenges that enterprises face in data confidentiality
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-29B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.5, Risk Assessment, describes the risk analysis we performed.
- Appendix D, Security Controls Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary, NIST SP 1800-29A*, with your leadership team members to help them understand the importance of adopting standards-based ability to detect, respond to, and recover from a loss of data confidentiality.

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-29C*, to replicate all or parts of the build 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 manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of the ability to detect, respond to, and recover from a loss of data confidentiality. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to <u>ds-nccoe@nist.gov</u>.

1.2 Build Overview

The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively detect, respond to, and recover from a loss of data confidentiality in various Information Technology (IT) enterprise environments. This work also highlights standards and technologies that are useful for a variety of organizations defending against this threat. The servers in the virtual environment were built to the hardware specifications of their specific software components.

The NCCoE worked with members of the Data Confidentiality Community of Interest to develop a diverse (but non-comprehensive) set of security scenarios against which to test the reference implementation. These are detailed in Volume B, Section 5.2.

1.3 Typographic Conventions

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the NCCoE Style Guide.
Bold	names of menus, options, command buttons, and fields	Choose File > Edit.
Monospace	command-line input, on- screen computer output, sample code examples, and status codes	mkdir

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Monospace Bold	command-line user input contrasted with computer output	service sshd start
<u>blue text</u>	link to other parts of the doc- ument, a web Uniform Re- source Locator (URL) or an email address	All publications from NIST's NCCoE are available at <u>https://www.nccoe.nist.gov</u> .

1.4 Logical Architecture Summary

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



Figure 1-1 Data Confidentiality Detect, Respond, and Recover High-Level Architecture

- **Data Protection (PKWARE)** involves maintaining the confidentiality and integrity of proprietary data, even in the event of a security breach or outright theft.
- Event Detection and Monitoring (Stealthwatch) focuses on becoming aware of potential intrusions by tracking the events that may indicate a breach of security and alerting the relevant administrators.
- Log collection, collation and correlation (FireEye) refers to the proper monitoring of activity on a system, and the analysis of that activity for any potential anomalous patterns or events.

- User access controls (Cisco Duo) work to regulate and restrict the level of access different users have, so that they can perform their work without providing unnecessary access that can be turned to more malicious ends.
- 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.

2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution. This implementation guide is split into 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 their own risk assessments and data protection requirements.

2.1 FireEye Helix

FireEye Helix is a security incident and event management system used for collecting and managing logs 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, much of the documentation provided will be integrating a cloud deployment with various products and components of the enterprise.

In this setup, we detail the installation of a communications broker that will be used to collect logs from the enterprise and forward them to the cloud deployment. This installation took place on a CentOS 7 Virtual Machine.

2.1.1 Installing the Communications Broker

- 1. Acquire the Helix Communications Broker for CentOS 7.
- 2. Navigate to the folder containing the installer and run the following.
 - > sudo yum localinstall ./cbs-installer_1.4.2-9.x86_64.rpm
- 3. Log on to the Helix web console.
- 4. Navigate to **Dashboards > Operational**.
- 5. Click Download Certificate.
- 6. Click Download. This will download a "bootstrap.zip" file.
- 7. Copy the zip file to the Helix Communications Broker certificate directory.
 - > sudo cp bootstrap.zip /opt/tap-nxlog/cert
- 8. Navigate to the certificate directory.

- > cd /opt/tap-nxlog/cert
- 9. Extract the zip file you just copied.
 - > sudo unzip ./bootstrap.zip
- 10. If prompted, select "Yes" to overwrite any previous certificate files.
- 11. Navigate to one folder above.
 - > sudo cd ..
- 12. Run the setup script.
 - > sudo ./setup.sh
- 13. Enter the name of the CentOS machine.
- 14. Enter the receiver URL provided in the Helix welcome email.



- 15. Select Add Routes and press Enter.
- 16. Select syslog.
- 17. Select tcp.
- 18. Select the Internet Protocol (IP) address of the machine where logs should be sent.
- 19. Enter 512 for the port number where logs should be sent.

				adı	ministrator@	plocalhos	t:/opt/tap	o-nxlog		-	۰	×
File	Edit	View	Search	Terminal	Help							
[IN	PUT S	OURCE	SETUR	•::ADD —								
In			() (() syslo) json) bsd	g							
Pr			e (() () udp () tcp) ssl								
IU			ace () ()) 192.1 () 192.1) 127.0	68.122.1 68.1.206 .0.1							
In			51	.2								
									 Cancel		OK	

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

2.1.2 Forwarding Event Logs from Windows 2012 R2

- 1. Acquire **nxlog-ce-2.10.2150.msi** from <u>http://nxlog.org/products/nxlog-community-edi-tion/download</u>.
- 2. Run nxlog-ce-2.10.2150.msi.



- 3. Click Next.
- 4. Check the box next to I accept the terms in the License Agreement.

18	NXLog-CE Setup
End- Ple	User License Agreement ase read the following license agreement carefully
	NXLOG PUBLIC LICENSE v1.0
1. "	DEFINITIONS License" shall mean version 1.0 of the NXLOG PUBLIC LICENSE, i.e. the terms and conditions set forth in this document; Software" shall mean the source code and object code form, all associated media, printed materials, and "online" or electronic documentation. All such software and materials are
I	accept the terms in the License Agreement Print Back Rest Cancel

5. Click Next.



6. Click Next.



7. Click Install.

1 6	NXLog-CE Setup	_ 🗆 🗙
	Completed the NXLog-CE	Setup Wizard
	✓ Open README.bt to read important	installation notes
	Back	h Cancel

- 8. Click Finish.
- 9. Navigate to C:\Program Files (x86)\nxlog\conf and open nxlog.conf.
- 10. 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>
   Path
             in => out
</Route>
```

11. Restart the **nxlog** service.

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

2.2 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.

2.2.1 Configure PKWARE with Active Directory

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

🖻 🖅 🗖 Login	\times + \sim $>$		-		×
\leftrightarrow \rightarrow \circlearrowright \bigstar	▲ Certificate error https://192.168.1.43/mds/SuperUser/Login	☆	l~	È	
	DE			ŀ	lelp
PAVZ					
Authorization R	lequired				
	Username:				
	Password:				
	Login				
	PKWARE Enterprise Manager 18.5.203 - <u>About</u> - pkwarevm 6/20/20 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.
- 3. Navigate to **System > Domain**.

System - Domain × + ∨			-		×
\leftarrow \rightarrow \circlearrowright \land Certificate error https://192.168.1.43/mds/SuperUser/System/Domain	☆	∿≡	h	ß	
DI/IA/ADE® Actions ² System Basics Advanced				I	Help
Dashboard Archive Events ¹				Log	out
Status Database Elasticsearch Network				Passv	vord
Domain SNMP SSL Package Log					
Danain					
Domain					
This system is not currently joined to a domain Join Domain					
PKWARE Enterprise Manager 18.5.203 • <u>About</u> • pkwarevm 8/20/20 11:02:01 AM					

4. Click Join Domain.

5. Enter the **Kerberos Realm, NetBIOS Domain**, as well as the **username** and **password** of an administrative user on the domain.

\blacksquare \blacksquare System - Domain \times + \vee				-		×
\leftarrow \rightarrow \circlearrowright \land \land Certificate error https://192	2.168.1.43/mds/SuperUser/System/Domain	□ ☆	☆	h	ß	
PKWARE Actions Dashboa Status Domain	 System Basics Advanced and Archive Events Database Elasticsearch Network SNMP SSL Package Log 				H Log Cha Passw	łelp out nge /ord
Join Windows Domain						
Kerberos Realm	dc.ipdrr					
NetBIOS Domain	dc					
User	Administator					
Password	•••••					
	Debug Output					
	Join Domain Cancel		P			
PKWARE Ente	prise Manager 18.5.203 - <u>About</u> - pkwarevm 8/20/20 11:02:01 AM					

6. Click Join Domain.

2.2.2 Create a New Administrative User

1. Navigate to **Advanced > Admins**.

Advanced - Admins ×	Discovery	× +						_ 0
→ C ▲ Not secure 192.16	8.1.43/mds/SuperUser/Ad	vanced/Admins					☆ 8	Upda
KWARE [*]	ctions System Basics A censes Admins Data Ce	kdvanced Dashboard Archiv Inter Cluster MFA Perform	ve Events ance Reports				Cha	Help Li inge Pas
lmins						Search:		
Username/UPN	🕆 Туре	Role	• MFA	API	Last API	🕴 Last Login		
Itimate Sys Admin	Local User	Super Sys Admin	n/a	n/a	n/a	n/a		
dministrator@DC.IPDRR	Domain User	Super Sys Admin	No	No	(never)	2/10/21 12:47:00 PM	Edit EnableAPI Delete	
		POUL	ARE Enterprise Manager 18.5.21	3 - <u>About</u> - pikwarevm	2/10/21 2:45:12 PM			

2. Click Add Domain User.

- 3. 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).
- 4. Select the level of permissions the user should have.

S Advanced - Admins X III Disc	covery X +	_ 🗆 X
← → C ▲ Not secure 192.168.1.43,	/mds/SuperUser/Advanced/Admins	🖈 😫 Update 🔅
PKWARE ^{* Actions}	System Basics Advanced Dashboard Archive Events	Help Log out Change Password
Add Domain User		
Domain Use	Administrator (Administrator@DCJPDRR)	
Rol	escurity Admin Save Cancel	
	0	
	POWARE Enterprise Manager 16.5203 - <u>about</u> - pixemerer 2/10/21 246/12 PM	

5. Click Save.

2.2.3 Install Prerequisites

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



3. Click Install Certificate.

4. Select Current User.



- 5. Click Next.
- 6. Click **Browse**.
- 7. Select Trusted Root Certification Authorities.

⑥ ₽ 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.	
\bigcirc 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	
Next Cancel	1

8. Click Next.

📀 🗟 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 Contributed Root Certification Authorities Content Certificate	
Finish Cancel	

9. Click Finish.



- 10. Click **OK**.
- 11. Repeat steps 1 through 10 but select **Personal** instead of **Trusted Root Certification Au**thorities.
- 12. Repeat steps 1 through 11 for each certificate that needs to be installed.

📜 l ⊋ 🖺 = l	Application Tools	PKWAI	RE		_ 🗆 X
File Home Share	View Manage				v 😲
💿 💿 – 🕆 👢 🕨 РКМ	/ARE ►		~ Č	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	s 1 KB	
🖗 This PC 🚱 Network					
2 items 1 item selected 1	92 bytes				

13. Rename *agent-registry.txt* to *agent-registry.reg*.

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?
K Yes No

15. Click Yes.

0	Registry Editor
0	The keys and values contained in C:\Users\Administrator.DC\Desktop\PKWARE\agent-registry.reg have been successfully added to the registry.
	Суок

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

2.2.4 Install the PKProtect Agent

1. Run the PKProtect Installation executable.

🕼 Smartcryp	ot 16.40.0010 - InstallShield Wizard
	Welcome to the InstallShield Wizard for Smartcrypt 16.40.0010
4.	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

- 2. Click Next.
- 3. Select I accept the terms in the license agreement.

🕼 Smartcrypt 16.40.0010 - InstallShield Wizard	X
License Agreement	
Please read the following license agreement carefully.	
PKWARE, INC.	<u>^</u>
PKWARE LICENSE AGREEMENT	Ξ
(Software Subscription/ Products)	
This PKWARE Agreement ("Agreement") is made by and between Licensor and Licensee, as defined below. This Agreement governs the subscription licensing of Software, the sale of Products and the provision of services related to the Licensor's PKWARE solution. For perpetual license terms for PKWARE software, visit https://legal.pkware.com.	
BY ACCESSING, USING, OR INSTALLING ALL OR ANY PART OF THE SOFTWARE, PRODUCTS, OR SERVICES AS APPLICABLE, LICENSEE EXPRESSLY AGREES TO AND CONSENTS TO BE BOUND BY ALL O THE TERMS OF THIS AGREEMENT. INCLUSIVE OF ALL SCHEDULES AND EXHIBITS HERETO. IE	DF ~
I accept the terms in the license agreement	
\bigcirc I do not accept the terms in the license agreement	
InstallShield	
< Back Next > Cancel	

- 4. Click Next.
- 5. Select Typical.

1 6	Smartcrypt 16.40.0010 - InstallShield Wizard
Setup Type Choose the s	setup type that best suits your needs.
Please selec	t a setup type.
• Typical	All program features will be installed. (Requires the most disk space.)
Custom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield ——	< Back Next > Cancel

6. Click Next.



7. Click Install.

Smartcrypt 16.40	0.0010 - InstallShield Wizard	X
Insta	allShield Wizard Completed	
The In 16.40.4	stallShield Wizard has successfully installed Smartcrypt 0010.	
	< Back Finish Cancel	

8. Click Finish.



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

8	Smartcrypt: Smartcrypt Manager Entry
Enter the a	dress of your Smartcrypt Manager:
https://pk	arevm.dc.ipdrr/mds
	k,
	OK Cancel

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

2.2.5 Configure Discovery and Reporting

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

0	A Net common 1 103 16	0 1 42 /m da /	Comment Lanar (Aparhiana (D)					
701	A Not secure 192.10	6.1.45/mus/	superoser/Archive/Di	scovery	_			
жи	/ARE° î	ctions Syst	em Basics Advance	d Dashboard Archi	ve Events			Change Pass
		olicies Disc	overy Remediations	Classification Com	nunities Assignments Lockers Accounts			
	U	epioyments	Devices Reporting	Support				
mart Filte	er Bundles							
							Search:	
Туре 🔺	Filter Name		Bundle Patterns					
Discovery	HIPAA - Diagnosis Lexio	on and	Social Security Nu	imber US (1 or more)	National Insurance Number UK (1 or more)	FDA Drugs Dictiona	ry (5 or more)	Edit Clone Delete
Jiscovery	Social Security Number	s	FDA Firms Diction	ary (5 or more) ICD	-9 Codes Dictionary (5 or more) CD-10 Cod	es Dictionary (5 or mo	ore)	Lun cione pelete
Discourse	PCI-DSS - Credit Cards	and Social	All Supported Cre	dit Cards (1 or more)	International Bank Account Number (1 or mo	ore) Social Security	Number US (1 or more)	Edit Class Delate
Discovery	Security Numbers		National Insurance	e Number UK (1 or me	ore)			Luit Cione Delete
Discovery	Personally Identifiable I	nformation	Social Security Nu	imber US (1 or more)	National Insurance Number UK (1 or more)	Tax ID US (1 or mor	e) Address US (10 or more)	Edit Clone Delete
showing 1 to	3 of 3 entries							
Add Discove	ery Add Redaction	Patterns I	mport Bundle Pack	Export Bundle Pack				
0								
Discovery	Global Settings							
Discovery A	gent Scanning Priority	Low						
Version	Detection Time Frame (Davs)	1						
	(0.0)0)	Scan Metad	ata					
		Scan Alterna	ate Data Streams					

- 2. Click Add Discovery.
- 3. Enter a **name** for the discovery rule.
- 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.
- 5. The **Threshold** field refers to how many of those patterns must be present in a document for the rule to be applied.

S Archive - Discovery	x a Discovery x +	_ D X
\leftrightarrow \rightarrow C \blacktriangle Not	t secure 192.168.1.43/mds/SuperUser/Archive/Discovery	🖈 😫 Update 🔅
PKWA	Actions System Basics Advanced Dashboard Archive Events Policies Discovery Remediations Classification Communities Assignments Lockers Accounts Deployments Devices Reporting Support	Help Log out Change Password
Discovery Smart	Filter Bundle	
	Filter Name SSN Discovery	
Pattern	Threshold	
Social Security Number	us vita in the second s	
Exclusions		
	Patterns	
Inclusions		
	Patterns	
Save Cancel		
	POINARE Entergine Manager (18.323 - <u>4000</u> - pownerum 2/1021 22009 PM	

- 6. Click Save.
- 7 . Navigate to **Archive > Remediations**.

S Archive - Remediations	× an Discovery >	< +	
← → C ▲ Not se	cure 192.168.1.43/mds/SuperUser/Archive/Re	emediations	☆ 😫 Update 🔋
PKWAR	Actions System Basics Advance Policies Discovery Remediation: Deployments Devices Reporting	ed Dashboard Archive Events 5 Classification Communities Assignments Lockers Accounts 5 Support	Help Log out Change Password
Remediation Action	s		
None Add	D ₆		
		POINAE Enterprise Manager 183.203 - <u>About</u> - privareum 2/10/21 22753 PM	

- 8. Click Add.
- 9. Enter a name for the remediation.

Archive - Remediations	x = Discovery x +	_ 🗆
→ C ▲ Not secur	e 192.168.1.43/mds/SuperUser/Archive/Remediations	🖈 😝 Update
PKWARE	Actions System Basics Advanced Dashboard Archive Events Searching - Policies Discovery Remediations Classification Communities Assignments Lockers Accounts	Help Log o Change Passwo
	Deployments Devices Reporting Support	
Remediation Action		
Name	Report and Encrypt	
Comment		
Remediations	Report Discovery Events Report Discovery Events Report Discovery Events Report Successful Encryptions Report Encryption Failures Algorithm AES (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 Smarkey will be used. Classify Before you can use redaction, you must add at least one Redaction Smart Filter Bundle Delete Do Nothing	
Pre Command 🗟		
Command		
	□ Ignore Filesystem Events	
Post Command		

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

Archive - Remediations ×	Discovery	× +			
→ C A Not secure 192.168	8.1.43/mds/SuperUs	er/Archive/Remediations			🖈 😫 Update
PKWARE Ac Pro De	tions System Bas licies Discovery f ployments Device	sics Advanced Dashboard Archive E Remediations Classification Communi es Reporting Support	vents ies Assignments Lockers Accounts		Help Log Change Passw
Remediation Actions					
				Search:	٥
Name	*	Comment	Types	Smartkeys	
Report and Encrypt	5		Report, Encrypt	(none)	Edit Delete
Add		PKWARE Ero	rprise Manager 185.203 - <u>2001</u> - pixanesm 2/10/21 2:2947 PM		

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

ssignme	nts						(and		1.
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 Disable
idd	o i oi i entriës								
				PKWARE E	nterprise Manager 18.5.203 - <u>Algous</u> - pixvarevm 2/10/21 2:29:5	5 PM			

15. Click Add.

Archive - Assignments 🗙 🚥 C	iscovery X +	_ □
→ C ▲ Not secure 192.168.1.	43/mds/SuperUser/Archive/Assignments	🖈 😫 🗘
PKWARE [®] Action Polici Deple	ns System Basics Advanced Dashboard Archive Events es Discovery Remediations Classification Communities <mark>Assignments</mark> Lockers Accounts syments Devices Reporting Support	Help Log Change Passw
ssignment		
Name	Report and Encrypt SSN	
Platform	Windows	
Mode	Discovery	
Users / Groups	Domain Users [DC.IPDRR]	4>
Local Path(s)	\$[USERPROFILE]	
Whitelist		
Blacklist	SAPPOATAY: SLOCALAPPOATAYY taom fai tawi tamp tali tops tow the tindd typ type tagit town tops tops tops tops the tra	w *.ocx *.ost
	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 scans.	
Sween Interval (seconds)	Agents earlier than 16.30 do not support scan-only mode.	
sweep interval (seconds)	Report Compliance and Status	
	Report Advanced File Attributes	
	Z Exclude Hidden Files	
	✓ Exclude System Files	
emediation Actions		

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

S Archive - Assignments × 🚥 C	Discovery × +		_ 🗆 X
← → C ▲ Not secure 192.168.1.	.43/mds/SuperUser/Archive/Assignments	\$	O Update :
Whitelist			
Blacklist	\$(APPDATA)* \$(LOCALAPPDATA)* *.acm *.ai *.avi *.bmp *.dll *.e *.tmp *.wav	ps *exe *flv *indd *jpg *jpeg *gif *mov *mp3 *mp4 *png *psd *pst *zaw *.occ *	ost
	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 per	form 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		
	ZExclude Hidden Files		
	Exclude System Files		
Smart Filter Bun	dles	Remediation Action	
	No data avail	able in table	
Showing 0 to 0 of 0 entries			
Agents earlier than 15.70 will only use the	he first Remediation Action shown above		
Albe			
Save Cancel			
	PIOWARE Enterprise Manager 18:5:203 -	About - pionerem 2/10/21 228-55 PM	

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

25.	Select the Remediation Action created earlier under Remediation Action .

🕲 Archive - Assignments 🛛 🗙 🚥 🕻	Discovery × +				_ □ X
← → C ▲ Not secure 192.168.1.	43/mds/SuperUser/Archive/Assignments			☆	O Update
Local Path(s)	\$(USERPROFILE)				
Whitelist					
Blacklist	\$IAPPDATAIY* \$ILOCALAPPDATAIY* *.acm *.ai *.avi *.bmp *.dll *.eps *.exe *.flv *.indd *.jp *.mp *.wav	ig *.jpeç	l_*.gif_*.mov_*.mp3_*.mp4_*.png_*.psd_*.pst_*.raw	*.ocx *	ost
	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 scan	s.			
	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				
Remediation Actions					
Smart Filter Bundles			Remediation Action		
SSN Discovery		4>	Report and Encrypt	Delete	
Showing 1 to 1 of 1 entries					
Add					
Save Cancel					
	NUMBER Formation Management (1977) Alter & International States (1977)				

26. Click Save.

27. This rule will now run automatically, reporting and encrypting files that match its discovery conditions.

2.3 Cisco Duo

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 becomes compromised, there is still significant access control between that machine and the internal enterprise machines.

In the following section, we demonstrate the installation of Cisco Duo on an internal system in such a way that Remote Desktop Protocol (RDP) and local login to that system are protected by multifactor authentication.

2.3.1 Installing Cisco Duo

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

Admin Login
Enter your admin credentials
Save my email address for next time Not recommended for public or shared computers
Continue
Want to protect your organization with Duo? Start a free tri

3. Login with your admin credentials and dual factor authentication to reach the administrator dashboard.

DUO	Q Search for us	ers, groups, applic	ations, or devices		MITRE	MITRE I	D: 2636-3111-77	Michael Ekstrom 🗸
Dashboard	Dachbo	ard						Add Now
Policies	Dashbu	Jaru						Add New V
Applications	Users							
Users	0	0	5	1	Administrators			
Groups	U Bypass Users	Locked Out	Inactive					
2FA Devices	View	View	View	2	2FA Devices			
Administrators	4 Licenses	Remaining		1	Groups			
Reports	6 Total Use	rs		471	Pompining Telephony Cred	to		
Settings				4/1	Remaining Telephony Cred	15		
Billing								
Need Help?								
<u>Upgrade your plan</u> for support.								

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

DUƏ	Q. Search for users,	groups, applications, or devices	MITRE MIT	TRE ID: 2636-3111	-77 Michael Ekstrom 🗸
Dashboard	Dashboard > Applicat	ons			
Policies	Applicati	0.000			Destant og Angligeting
Applications	Applicat	ons			Protect an Application
Protect an Application					
Users					\sim
Groups	Manage your	Ipdate to the new Universal Prompt			
2FA Devices	experience, a	in one place.			
Administrators	See My Progress	Get More Information			
Reports				•	_
Settings	4	0			
Billing	All Applications	End of Support			
Need Help?			Export	Q Search	

- 6. Search for, or scroll down to, Microsoft RDP.
- 7. Click **Protect**.

DUO	Q Search for users, groups, applications, or devices	MITRE	MITRE ID: 2636-3111-77	Michael Ekstrom 🗸
Dashboard	Dashboard > Applications > Protect an Application			
Policies	Protect an Application			
Applications				
Protect an Application	RDP			
Users				
Groups	Application	Protection Type		
2FA Devices				
Administrators	Microsoft RDP	2FA	Documentation 🗗	Protect
Reports				

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 Users Groups	Dashboard > Applications > M Microsoft RI See the RDP documentation	licrosoft RDP 3 DP 3 E ^r to integrate Duo into your Microsoft RDP deployment.		Authentication Log	Bemove Application
2FA Devices Administrators Reports	Details	DIZQ2S5DXMVCA2FBVEMM	Сору		Reset Secret Key
Settings Billing	Secret key	T88F	Сору		
Need Help? <u>Upgrade your plan</u> for support. Versioning Core Authentication Service:	API hostname	Don't write down your secret key or share it with anyone.	Сору		

- 9. Download the **Duo Authentication for Windows Logon** installer package, located at <u>https://dl.duosecurity.com/duo-win-login-latest.exe</u>.
- 10. Run the downloaded EXE file.



- 11. Click Next.
- 12. Copy the **API Hostname** into the labeled field.

	and the megrate bas me your merson rear depoyment.	Duo Connectivity Check Please enter the hostname for your integration to verify connectivity
Details		API Hostname:
Integration key	DI8SZS91SLPZGWEEHZWG Copy	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	Copy Don't write down your secret key or share it with anyone.	Configure manual proxy for Duo traffic (Uses System settings if unspecified) Proxy Hosts Proxy Port:
API hostname	api-9d22ea89.duosecurity.com	
		InstalShield <gadk next=""> Cancel</gadk>

13. Click Next.

14. Copy in the Integration and Secret Keys into the relevant fields and click Next.

🖶 Duo Authentication for Windows Logon x64 - InstallShield Wizard 🛛 🗙
Duo Security Account Details
Please enter the keys provided by Duo Security
Integration Key:
DI8SZS91SLPZGWEEHZWG
Secret Key:
These keys can be found in the <u>Duo Admin Panel</u> under Applications, configure or select a Microsoft RDP application.
Please refer to the Duo Windows Logon <u>documentation</u> for more information. nstallShield
< Back Next > Cancel

15. Click Next.

16. Configure Duo's integration options according to the needs of your organization. Note that **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	\times
Duo integration options	
Configure the integration below	
Bypass Duo authentication when offline (FailOpen)	
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>documentation</u> for more information.	
< Back Next > Cance	el

17. Click Next.

18. Leave Enable Smart Card support unchecked.

Enable Smart Card support	
O Protect smart card log Both smart card and use two-factor authenticatio	i n with Duo rname/password primary login is followed by Duo m.
 Enable smart card logi Allow use of the Window password login with Duo 	n without Duo as smart card login provider as an alternative to two-factor authentication.

19. Click Next.
| Di | Configure User Elevation Protection |
|----|--|
| | Enable UAC Elevation Protection
Enable Duo two-factor authentication for password protected UAC prompts. |
| | Protect User Elevation only
Protect UAC Prompts Only. Disables MFA for Local and RDP sessions |
| | Protect User Elevation while offline
Enable Duo two-factor authentication for password protected UAC prompts
when Offline access is enabled. |
| | Allow Offline enrollment during User Elevation
Allow for offline access enrollment during password protected UAC prompts
when Offline access is enabled. |
| | Please refer to the Duo Windows Logon documentation for more information. |

滑 Duo Authentication for Windows Log	on x64 - InstallSl	hield Wizard	×
Ready to Install the Program			
The wizard is ready to begin installation.			
Click Install to begin the installation.			
If you want to review or change any of exit the wizard.	your installation se	ettings, click Back	. Click Cancel to
7			
Instalioniela	< Back	Install	Cancel

22. Click Install.



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.

2.3.2 Registering a Duo User

1. Login to the Duo Admin Dashboard.

	arch for users, groups, applic	ations, or devices		MITRI	MITRE I	D: 2636-3111-77	Michael Ekstrom $ \mathbf{v} $
Dashboard Da Policies Applications	shboard						Add New V
Users 0 Groups Dusc		5	1 A	dministrators			User Application Group
2FA Devices View	View	View	2 21	A Devices			
Administrators 4 Reports	Licenses Remaining		1 G	roups			
6 Settings Billing	Total Users		463	Remaining Telephony Crec	its		

- 2. Click **Add New > User** from the drop-down menu on the right.
- 3. Enter a username for the user.

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

- 4 . Click Add User.
- 5. This will lead you to that user's information page, where additional information (full name, email, phone number) and Duo authenticators (phone numbers, Two-Factor Authentication (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.*

2.4 Cisco Stealthwatch

This section will describe the setup and configuration of Cisco Stealthwatch, a network monitoring solution. Cisco Stealthwatch provides insight into the networking activity of the organization, allowing for the detection of malicious network activity, as well as the ability to review user activity for the source of breaches, and intentional or unintentional data egress. This guide assumes the use of the Stealthwatch virtual machines.

2.4.1 Configure Stealthwatch Flow Collector

- 1 . Log in to the console of the Stealthwatch Flow Collector.
- 2. Enter the networking information for the machine.

StealthWatcl	h FlowCollector	for NetFlow VE ve	rsion 7.3.2 build	20210409.0329-58b666896	1ea-0 serial
	Future the second			1	
	IP Address: Netmask: Netmask: Broadcast: Host Name: Domain:	192.168.1.64 255.255.255.0 192.168.1.1 192.168.1.255 swfc dc.ipdrr			
	_	<u>< 0</u> K >	<cancel></cancel>		

- 3. Select OK and press Enter.
- 4. Navigate the menu to highlight **Management** and **Select**.
- 5. Confirm the settings.

StealthWatch	FlowCollector	for NetFlow	VE version	7.3.2 build	20210409.032	29-58b66668961e	ea-O serial
,	IP Address: 11 Netmask: 255.3 Gateway: 192.3 Broadcast: 193 Host Name: swi Domain: dc.ip FQDN: swfc.dc Are these the d	92.168.1.64 155.255.0 168.1.1 2.168.1.255 Te trr .ipdrr correct setti	ngs?				
		K <u>Y</u> es	>	< No >			

6. Select **Yes** and press **Enter**.



7. Select **OK** and press **Enter**.

	Main Menu		
Select a menu:			
	Network Security Recovery Advanced		
	naouneca		
L			
(Select)	<about></about>	< Exit >	

8. Once the machine restarts, navigate to **Security**, and press **Enter**.

althwatch fic	MC011ettur für Hetrium ve Gersion 7.5.2 milia 20210405.0325-300000	0.0169-0.261.
Sele	Security ect a menu: Password CSRF Protection Manage CSRF protection.	
	<pre></pre>	

- 9. Select Password and press Enter.
- 10. Change the password from the default password to a secure password.

2.4.2 Configure Stealthwatch Management Console

- 1. Log in to the console of the Stealthwatch Management Console.
- 2. Enter the networking information for the machine.

Enter the new IP Address: Netmask: Gateway: Broadcast: Host Name: Domain:	network informatio 192.168.1.63 255.255.255.0 192.168.1.1 192.168.1.255 swmc di.ipdrr_	m:		
	< 0K >	«C an	cel>	_

3. Select **OK** and press **Enter**.

lthWatch Management	Console VE version 7.3.	2 build 20210409.03	29-5866668961ea-0 se	erial SMO
			1	
IP Address Netnask: 2 Gateway: 1 Broadcast: Host Nane: Domain: di FQDN: swnc	: 192.168.1.63 55.255.255.0 22.168.1.1 192.168.1.255 sumc .ipdrr .di.ipdrr			
Are these t	he correct settings?			
	< Yes >	< No >		

4 . Select **Yes** and press **Enter**.



5. Select **OK** and press **Enter**.

Select a menu:	Main Menu]
	Network Security Recovery Advanced		
Select>	<about></about>	< Exit >	

6. Once the machine restarts, navigate to **Security**, and press **Enter**.

Select a menu:	Security		
Password CSRF Protection	Change the password f Manage CSRF protectio	or the current user. m.	
	Select> < Exi	t >	

- 7. Select **Password** and press **Enter**.
- 8. Change the password from the default password to a secure password.
- 9. Navigate to the Stealthwatch Management Console from a web browser. The URL will be <a href="https://<<a href="https://.

🚱 Stealthwatch Management Cons 🗙 🕂		• - • ×
← → C ▲ Not secure 192.168.1.63/sw-login/		x 😩 I
		•
	cisco	
	Stealthwatch	
	admin Password *	
	Sign In	
	Copyright © 2021 Cisco Systems Inc. All rights reserved. Privacy Statement	

10. Login using the default username and password (should be provided by product vendor).



11. Click **Continue**.

12. Change the password for the admin account (this is the account used to log in to the web interface).

Stealthwatch Management Co Appliance Setup Serial Number: SMCVE-VMware-422d278c2e7886 Version: 7.3.2 Build: 20210409 0329 986668961ea 0	nsole VE 3-670756294103856#	STE	ALTH WATCH
Step 1: Change Default Password	Change Default Passwor	ds	
Step 2: Management Network Interface	Password Format (Case Sensitive)	_	
Step 3: Host Name and Domains	Must be different from the previous p Must be different from the previous p Must not be the same as the previo Must not be similar or the same as y	ers. password by at least 4 characters. Is 12 password(s). our username.	
Step 4: DNS Settings	Must exclude dictionary words and r	epeated or sequential characters.	
Step 5: NTP Settings	Note: You must change the pass © ADMIN	word for all the users before continuir	g.
Register Your Appliance	Current Password:		
Register Your Appliance	New Password:	Generate Passwor	1
Step 6: Register Your Appliance	New Password:	Generate Passwor	1

13. Click Next.

14. Change the password for the root account (this is the account used to log in to the command line console).

Stealthwatch Management C Appliance Setup Serial Number: SMCVE-VMware-422d27552976 Version: 7.9.2 Build: 20210/09.0329-58b6666991ea-0	ionsole VE 183-67075e2arina885r	STE.	
Step 1: Change Default Password	Change Default Passwords		
Step 2: Management Network Interface	Password Format (Case Sensitive) Must be between 8 and 256 characters.		
Step 3: Host Name and Domains	Must be different from the previous pase Must not be the same as the previous 1 Must not be similar or the same as your	sword by at least 4 characters. (2 password(s) r username.	
Step 4: DNS Settings	Must exclude dictionary words and repe	sated or sequential characters.	
Step 5: NTP Settings	Note: You must change the passwo	ord for all the users before continuing १ ROOT	
Register Your Appliance	Current Password:		
Complete	Current Password:	root Generate Password	
Complete	Current Password: Incorrect Password for New Password: Password Steegh- Tea Confirm New Password:	root Generate Password	

16. Confirm the networking information is correct and click **Next**.

🖅 Appliance Setup Tool 🛛 🗙 🕂				0
← → C ▲ Not secure 192.168.1.63/lc-ast/steps	ntml#!/managementInterface			☆ 😩
Appliance Setup Serial Number: SMCVE-VMware-4220 Version: 7.3 2 Build: 20210409.0329-58b6668961ea			STEALTH WATCH	
Step 1: Change Default Password	Management N	letwork Inte	erface	
Step 2: Management Network Interface	Enable communication b below. Before changing a	etween this appliance ar my of these settings, cor	d the network. Default network settings for this appliance appear fer with your network administrator	
Step 3: Host Name and Domains	Warning! If you change replaced automatically, these fields so you don'	your IP address, host na If you have a custom cer I lose data.	me, or network domain name, the appliance identity certificate is fificate, save the certificate and private key before you change	
Step 4: DNS Settings	Interface Name:	eth0	Interface MAC Address: 00:50:56 ad ca:9d	
Step 5: NTP Settings		IPv4	IPv6	
Step 6: Register Your Appliance	IP Address:			
Complete	Subnet Mask:			
	Default Gateway:			
	Broadcast Address:		K	
			Next →	

17. Enter the domain for Stealthwatch, and the IP addresses Stealthwatch will be monitoring.

Pppliance Setup Tool x +			• <u> </u>
← → C ▲ Not secure 192.168.1.63/lc-ast/steps.html#!/host	nameDomain		☆ 😩 :
Stealthwatch Management Con Appliance Setup Serial Number: SMCVE-VMware-42202755/287853-4 Version: 3.3 Build: 20210408 0528-5886666961ea-0	sole VE 17075e29f103855f	STEALT	Ъ.
Step 1: Change Default Password	Host Name and	Domains	
Step 2: Management Network Interface			
Step 3: Host Name and Domains	Warning! If you change yo replaced automatically. If these fields so you don't i	wr IP address, hest name, or network domain name, the appliance identity certificate i you have a custom certificate, save the certificate and private key before you change use data.	5
Step 4: DNS Settings	Host Name:		
Step 5: NTP Settings	Network Domain:		
Sten 6:			
Register Your Appliance	Stealthwatch Domain:		
Complete	IP Address Ranges:		
		here and the second sec	

19. Add the Domain Name System (DNS) server(s) Stealthwatch should be using.

۵	Stealthwatch Management Co Appliance Setup Serial Number: SMCVE VMware-422d27f5c2e780 Version: 7.3.2 Build: 20210409.0329-58b6668961ea-0	onsole VE 183-67075e29f103855f			STEALTH	
	Step 1: Change Default Password	DNS S	ettings			
ŗ	Step 2: Management Network Interface	Enter t the cor	e IP address(es) of your de esponding checkbox, and t	omain name server(s). hen click the - button.	m. To delete a server, select	
5	Step 3: Host Name and Domains	De	te DNS Server			
<u></u>	Step 4: DNS Settings					
	Step 5: NTP Settings					
	Step 6; Register Your Appliance					
	Complete					
		← B	ick		Next	

- 20. Click Next.
- 21. Enter the Network Time Protocol (NTP) server(s) Stealthwatch should use.

State: 2010/00 0028-30000000000000000000000000000000000	
Step 2: Management Network Interface Imagement Network Interface Select or enter the IP address(es) or name(s) of your network Interprotocol server(s). Choose the same NTP server(s) used for other devices server, select the carresponding checkbox, and then click the - button. To delete a server, select the carresponding checkbox, and then click the - button. Imagement Network Interface Imagement Network Interface Imagement Network Imagement Network Imagement Network Imagement Network	
Step 3: Delete NTP Server Step 4: 1097 74 8 Image: Constraints Step 5: NTP Server	
Step 4: DNS Settings	
Step 5: NTP Settings	
Register Your Appliance	
Complete	
← Back Next →	

★ Appliance Setup 1001 ★ T ★ → C ▲ Not secure 192.168.163 Ø Stealthwatch Appliance Setup Setup 1001 ★ 1000 Stealthwatch Appliance Setup Setup 1001 ★ 1000 Setup 1001 ★ 1000 File 1000 <pfile< th=""><th>rlc-ast/steps.html#i/ntpSe Management Con IC VMware 4224571522e70104 seasesesses</th><th>ttings sole VE storsesmosee</th><th></th><th></th><th>STEALTH</th><th>☆ 2</th></pfile<>	rlc-ast/steps.html#i/ntpSe Management Con IC VMware 4224571522e70104 seasesesses	ttings sole VE storsesmosee			STEALTH	☆ 2
Step 1: Charge Detail	Review and Res	start				
Step 2: Management	Step 2 View Management to update with the below changes, you need to restart your machine. Upon returning to the Application, you will be brought to Step 6 to continue setup of your Appliance.					
Step 3: Host Name or	Management Networ Name: MAC Address: IP Address:	eth0 00 50 56 ad.ca.9d 192 168 1 63	Host Name and Net Host Name: Network Domain:	work Domain swmc di.lpdrr		
Step 4: DNS Settings	Subnet Mask: Default Gateway: Broadcast Address: IPv6 Address: IPv6 Pretry Length:	255 255 255 0 192 168 1.1 192 168 1.255				
Step 5: NTP Settings	IPv6 Gateway: DNS Settings		NTP Settings			
Step 6: Register Your						
Complete	Cancel			Restart and Proceed		

23. Click Restart and Proceed.

Stealthwatch Setup Tool × +		• - • ×
← → C ▲ Not secure 192.168.1.63/lc-ast/		☆ 🚨 :
	Welcome to the Stealthwatch Appliance Setup Tool!	
		1000
	K Continue 🔸	
이 아이에는 그가도 것 것 것 같아요.		

24. After it restarts, log in again, and click **Continue**.

I Appliance Setup Tool × +			• - • ×
← → C ▲ Not secure 192.168.1.63/Ic-ast/steps.html#!/r	egister		☆ 😩 :
Stealthwatch Management C Appliance Setup Serial Number: SMCVE-VMware-42202755/2e7 Version: 7.3 Build: 202104/00 0329-5859568961ea-0	Console VE eres 67076/29H03888	STEALT	н сн
Step 1: Change Default Password	Register your appliance		
Step 2: Management Network Interface		anager that you will be using to configure and manage this applian	ce.
Step 3:	IP Address		
Host Name and Domains		Save	
Step 4: DNS Settings			
Step 5: NTP Settings			
Step 6: Register Your Appliance			
Complete			
	- Back	Next →	

25. Confirm the IP address is correct and click Next.

SW Appliance Setup Tool	× +		• <u> </u>
← → C ▲ Not s	ecure 192.168.1.63/lc-ast/steps.html#!/revi	2W	☆ 🚨 ፤
	Stealthwatch Management Co Appliance Setup Serial Number: SMCVE-VMwate-42242775-28785 Version: 7.9.2 Build: 20210409 (325-386666951es-0	nsole VE 670756281038551	STEALTH
	Step 1: Change Default Password	Appliance Setup Complete!	
	Step 2: Management Network Interface		
	Step 3: Host Name and Domains	Your appliance setup is complete.	
	Step 4: DNS Settings	Go to Dashboard	
	Step 5: NTP Settings		
	Step 6: Register Your Appliance		
	Complete		
			Next

26. Click **Go to Dashboard**.

2.4.3 Add Stealthwatch Flow Collector to the Management Console

- 1. Navigate to the Stealthwatch Flow Collector Console from a web browser. The URL will be <a href="https://<<a href="https://.
- 2. Login using the default username and password (should be provided by product vendor).

Welcome to the Stealthwatch Appliance Setup Too!! The tool will help you configure your Stealthwatch appliance steep by step
For more information, refer to your Stealthwatch System documentation.

3. Click Continue.

\$ Flow Collector for NetFlow VE Appliance Setup Serial Number: FCNPVE: VMvare-422459e566dctc39a-d6e5 Wersian: 732 Build: 202104/09.0329-58b6668661ea.0	0405833e22466			STEA				
Change Default Password	Change Default Passwords							
Step 2: Management Network Interface	Password Format (Ca • Must be between	ise Sensitive) 8 and 256 characters.						
Step 3: Host Name and Domains	Studs be different from the previous password by at least 4 characters. Used note the same as the previous 12 passwords) Must not be similar of the same as you uncername.							
Step 4: DNS Settings	Must exclude dictionary words and repeated or sequential characters							
Step 5: NTP Settings	• ADMIN	nge trie password to	© ROOT	erore conunuing.				
Step 6: Central Management								
Complete	New Password:			enerate Password				
	Confirm New Password:	Password Strength - Fair						
	- Back	Show Password		Next →				

- 4 . Change the passwords for the admin and root accounts.
- 5. Click Next.

Flow C Applian Seria Nun Versien: 7 Build: 202	Collector for NetFlow VE ce Setup http://CNFVE-VMware-422d59e06d4c39a-diceSof .3.2 10409-0529-5866668961ea-0	SESSIONEZAGE					
Ste	ep 1: Inge Default Password	lanagement Network Interface					
Ste	ep 2: agement Network Interface	Enable communication between this appliance and the induced. Default network settings for this appliance appear below. Before changing any of these settings, conter with your network administrator.					
Ste	ep 3: t Name and Domains	Warning If you change your IP address, hod name, or network domain name, the appliance identity certificate is replaced automatically. If you have a custom certificate, save the certificate and private key before you change these fields so you down load edit.					
Ste	ep 4: S Settings	Interface Name: ct	h0 Inti	terface MAC Address: 00.	50.56 ad.63.1d		
E Ste	ep 5: • Settings	IPν	4	IPv6			
🥰 Ste	ap 6: tral Management	IP Address:					
~ Co	mplete	Subnet Mask:					
		Default Gateway:					
동 영상 방송 같은 것이 같은 것이 같이 많이		Broadcast Address:					
					Next 🔿		

- 6. Confirm the networking information is correct and click **Next**.
- 7 . Confirm the domain name for Flow Collector is correct.

Flow Collector for NetFlow VE Appliance Setup Senai Number: FCNYE VMware 422d59e0660423 Version: 7.3.2 Build: 20210409.0029-58586895166-0	9a d6e50fd583e22466		STEALTH			
Step 1: Change Default Password	Host Name and	l Domains				
Step 2: Management Network Interface						
Step 3: Host Name and Domains	Warning! If you change yo replaced automatically. If these fields so you don't le	our IP address, host name, or network domain name you have a custom certificate, save the certificate at ose data.	; the appliance identity certificate is nd private key before you change			
Step 4: DNS Settings	Host Name:	swic				
Step 5: NTP Settings	Network Domain:					
Step 6: Central Management						
Complete						
			Next 🔿			

- 8. Click Next.
- 9. Add the DNS server(s) Stealthwatch should be using.

Flow Collector for NetFlow VE Appliance Setup sena Number ("NINV-VMware-4220960504c6" Version: 7.3.2 Bune: 20270409 0029-5656669651ee.0	STEALTH WATCH
Step 1: Change Default Password	DNS Settings
Step 2: Management Network Interface	Enter the IP address(es) of your domain name server(s). To add a server, click the + button. To delete a server, select the corresponding checkbox, and then click the - button.
Step 3: Host Name and Domains	Delete DNS Server
Step 4: DNS Settings	
Step 5: NTP Settings	
Step 6: Central Management	· · · · · · · · · · · · · · · · · · ·
Complete	
	Hext Hext
김 소리는 영상 이 것 수 같은 것이 없는 것이 같다.	동안 모님 동안 방법을 다 같은 것이 집에 가지 않는 것이 같이 많이 있는 것이 같이 없다. 것이 같이 많이

- 10. Click Next.
- 11. Enter the NTP server(s) Stealthwatch should use.

Flow Collector for NetFlow Appliance Setup serva twoets: COVEY Manuse-420056000 version: 7.3.3 Build: 22(19)(0) 0220-350056006/read	
Step 1: Change Default Password	NTP Settings
Step 2: Management Network Interface	Select or only the IP address(es) or name(s) of your network time protocol serve(s). Choose the same NTP serve(s) used to other devices that teed information to the Statifhinkh TheoColector to helf/two. To add a server, cick the + bottom. To device a server, select the ecorresponding chocked, unit denic data. He - bottom.
Step 3: Host Name and Domains	Delete NTP Server
Step 4: DNS Settings	
Step 5: NTP Settings	•
Step 6: Central Management	
Complete	•
	← Back Next →

Step 1: Revie	w and Restart				
Step 2 Miningentia	r to update with the b tion, you will be broug	slow changes, you need ght to Step 6 to continue	I to restart your mach setup of your Applia	ine. Upon returning to the nce.	
Manag	ement Network Interfac		Host Name and Netw	vork Domain	
Step 3: Half Name MAC A	: eth0 Address: 00.50.5 Iress: 192.168	5.ad.63.1d	Host Name: Network Domain:	swfc dc.lpdrr	
Step 4 Defaul DNS School Broad	et Mask: 255.252 It Gateway: 192.162 cast Address: 192.163 iddress:	255.0 1.1 1.255			
Step 5: NTP Setting	refix Length: Sateway:				
DNS S	ettings		NTP Settings		
Cance	1			Restart and Proceed	

13. Click Restart and Proceed.

STEALTH	
Welcome to the Stealthwatch Appliance Setup Tool! This tool will help you configure your Stealthwatch appliance step by step	
Editore you begin.	
For more information, refer to your Stealthwatch System documentation.	
Continue -	

- 14. After it restarts, log in again, and click **Continue**.
- 15. Enter the IP of the Stealthwatch Management Console.

Build: 20210409.0329-58b6668961ea-0	
Step 1: Change Default Password	Central Management Settings
Step 2: Management Network Interface	Enter the IP address of the Central Manager that you will be using to configure and manage this appliance. Note: By default, this will be the IP address of your SMC. If you have SMCs in a failover pair, enter the IP address of your primary SMC. Also, provide security events will be sent to the SMC you enter here.
Step 3: Host Name and Domains	IP Address
Step 4: DNS Settings	192.168.1.63 Save
Step 5: NTP Settings	Entranal for the spin and manage of the spin and based on your environment.
Step 6: Central Management	
Complete	
	← Back

16. Click Save.

Plane Collector for NetFlow VE Appliance Stag Density of the Collector for NetFlow VE Appliance Stag Density of the Collector of the	A A CONTRACT ON	rendigure and manager this applance. BIOS in a failwayer part, enter the tP address of your enter them.

- 17. Accept the certificate by clicking **Yes**.
- 18. Enter the username and password for the Stealthwatch Management Console.

Flow Collector for NetFlow VE Appliance Setup serial Number: FCNP/G-VMArate-422059e66de3c9a-d664 Version: 7.32 Built: 20210420.0029-5696689061ea-0	5010583e22	166	STEALTH WATCH
		al Management Settings	
Step 2: Management Network Interface		Please enter your administration credentials below.	
Step 3: Hort Name and Domains		our In order to be added for management you must enter your SMC administration credentials below.	
		admin 1 Password:	
NTP Settings			
Step 6: Central Management		Cancel Next 🕈	

- 19. Click Next.
- 20. Enter the **Domain** and **Flow Collection Port**.

Flow Collector for NetFlow VE Appliance Setup Serial Number: FCNFVE: VMware-42/85905064-8/3 Version: 7.3 Build: 20215409 0329 6866686961ea 0	STEALTH
Step 1: Change Default Password	Central Management Settings
Step 2: V= Management Network Interface	IP Address
Step 3: Host Name and Domains	
Step 4: DNS Settings	Staalthwatch Domain: dl.ipdrr 👻
Step 5: NTP Settings	Flow Collection Port:
Step 8: Central Management	Note: The default netflow port for the Flow Collector is 2055, and the default sFlow port is 6343.
Complete	
	← Back Next →

Flow Collector 1 Appliance Setup Serial Number: TONY V-V Version: 7.3.2 Built: 2021/04/9 0029-588	or NetFlow VE Name = 2720/000/004/238a d/se/078/0386/2466 860/6/1e=0	STEALTH WATCH
Step 1: Change Default Pa	Appliance Setup Complete!	
Step 2: V= Management Netw		
Step 3: Host Name and Do	Your appliance setup is complete.	
Step 4: DNS Settings	Use your Central Manager to manage your applian edit configuration settings, and update software.	ces,
Step 5: NTP Settings	Go to Central Management	
Step 6: Central Manageme		
Complete		

22. Click **Go to Central Management** to be redirected to the dashboard.

2.5 Dispel

Dispel is a network protection and user access tool that we used to provide a Virtual Desktop 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 north and south-facing network interfaces, placing the device in-line between the enterprise systems and the external network.

2.5.1 Installation

1. Deploy an Ubuntu machine with the provided specifications, ensuring that a provided optical disk image is attached to the device.

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 Vy0S!
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.
Vy0S is a free software distribution that includes multiple components,
you can check individual component licenses under /usr/share/doc/*/copyright
dispel@dispelwicket:~$
```

- 3. Begin the installation process.
 - > 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.

```
Would you like to continue? (Yes/No) [Yes]:
Probing drives: OK
Looking for pre-existing RAID groups...none found.
The image will require a minimum 2000MB root.
Would you like me to try to partition a drive automatically
or would you rather partition it manually with parted? If
you have already setup your partitions, you may skip this step
Partition (Auto/Parted/Skip) [Auto]:
I found the following drives on your system:
sda 150323MB
Install the image on? [sda]:
This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]:
```

5. Type yes before pressing enter to rewrite the current volume.

```
This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]: yes
How big of a root partition should I create? (2000MB – 150323MB) [150323]MB: _
```

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.boot]: Copying /opt/vyatta/etc/config/config.boot to sda. Enter password for administrator account Enter password for user 'dispel':

7. Enter and re-enter a new password for the user dispel.



8. Press enter one final time to finish the installation.



- 9. Power off the machine, remove the provided optical disk image, and power it back on.
- 10. 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:~% _
```

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.

```
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:~$
```

2.5.2 Configuring IP Addresses

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# _
```

7. Type in the command > exit.



2.5.3 Configuring Network

The following instructions are to modify a Dispel wicket device to forward traffic to a different routing device. This may be desirable for some network setups.

1. Type in the command > configure to the Dispel wicket device after logging in.



2. Type in the command > set protocols static route 0.0.0/0 next-hop 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#
```

3. Type in the command > commit.

```
dispel@dispelwicket# commit
[edit]
dispel@dispelwicket#
```

4. Type in the command > save.

```
dispel@dispelwicket# save
Saving configuration to '/config/config.boot'...
Done
[edit]
dispel@dispelwicket# _
```

5. Type in the command > exit.

```
dispel@dispelwicket# exit
exit
dispel@dispelwicket:~$
```

- 6. On the designated router or firewall, ensure User Datagram Protocol (UDP) is allowed from the Dispel device on the provided port. For the NCCoE deployment, port 1194 was utilized. A target destination for the traffic will be provided by Dispel.
- 7. Modify the IP addresses of the south-side network interface to properly align with your network. See the "Configuring IP Addresses" section above.

2.5.4 Adding a Device

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



3. Click on the **Devices** page on the sidebar and click **Create**.

Dispel Devices	× +					~	-		×
\leftrightarrow \rightarrow C \triangle $$ dash	hboard.dispel.io/devices/create	07	Ê	☆	••••]	*		Updat	e :)
outlook 🜖 DI SharePoint	🔹 Hospitality SharePo 🔇 VSphere 🛛 🖙 Lab Wiki 🤟 NCCoE GitLab 💋 Dispel Regions								
NCCoE @ M ¢	B Data Confidentiality Lab								^
🖹 Logs	DC_AD_DNS_Dispel Add device Data Confidentiality Lab Adding a device allows you to control access to it.								
Inventory 은 Members	DC_AD_DNS Facility* □ Data Confidentiality Lab Select a Facility ∞ Data Confidentiality 192.168.1.12	\$							
B Devices	DC_Avrio Wicket*								
Stacks	Data Confidentiality Lab No wickets found Data Confidentiality 192.168.1.198 Name*								
Overview	DC_Cisco_Duo_Testing								
E Facilities	© Data Confidentiality 192.168.2.103 Make								1
Support	DC_CISCO_STEALTHWATCH_FLOW_C								
🕁 Downloads									
Documentation	DC_CISCO_STEALTHWATCH_MANAGI							_	
								C	

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

Dispel Devices	× +	∨ - □ ×
← → C ☆ ●	dashboard.dispel.io/devices/create	🕶 🖻 🖈 🔲 🌲 🗍 😩 Update 🚦
o Outlook 🗿 DI SharePe	oint 🗊 Hospitality SharePo 🔇 VSphere 🚥 Lab Wiki 🦊 N	CCoE GitLab 🔊 Dispel Regions
NCCoE ©	Q Filter devices Create	NCCoE / Devices / Create
	Devices (14)	Make
🖹 Logs	Test Workstation EVIL-WEB	Windows
Settings	☐ Data Confidentiality Lab	Model
Inventory	DC WINSERV 2016 2	10
은 Members	Data Confidentiality Lab So Data Confidentiality	ID*
Devices	192.168.2.1	192 168 2 10
Stacks	DC_AD_DNS_Dispel	152,100,2,10
Overview	 □ Data Confidentiality Lab ○ Data Confidentiality 192.168.1.12 	Protocol Ports
⇔ Regions	DC AD DNS	TCP 💠 3389 ×
Facilities		+ Add protocol
Support	DC Auria	Ports can be written as ranges in a comma-separated list. For
🗄 Downloads	DC_AVIIO D Data Confidentiality Lab So Data Confidentiality	example: 100,200-300 is the port 100 and the range 200-300.
Documentation	192.168.1.198	Add device
	DC_Cisco_Duo_Testing	
	Data Confidentiality Lab So Data Confidentiality	

5. Click Add Device.



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

Dispel Devices	× +	✓ - □ X
\leftrightarrow \rightarrow C \triangle \bigcirc da	shboard.dispel.io/devices/352/access	🕶 🖻 🏚 🖬 🌲 🗍 😩 🗍 Update 🔅
o Outlook 🗊 DI SharePoint	t 🤹 Hospitality SharePo 😵 VSphere 🚥 Lab Wiki 🦊 NCC	CoE GitLab 💋 Dispel Regions
NCCoe 🐵 М 🗢	▲ DC_DISPEL_UBUNTU_1	NCCoE / Devices / Test Workstation EVIL-WEB / Access
🗄 Logs	DC_HELIX_CENTOS	Test Workstation EVIL-WEB (Data Confidentiality Lab)
Settings	□ Data Confidentiality Lab ○ Data Confidentiality 192.168.1.206	192.168.2.90
Inventory	DC_HELIX_UBUNTU	Overview Access Settings
은 Members	Data Confidentiality Lab So Data Confidentiality	O Apdraw
B Devices	152,100,132	
Stacks	DC_INTRANET ☐ Data Confidentiality Lab ↔ Data Confidentiality	Device access (ACLs) (0) ····
Overview	192.168.2.40	
C→ Regions	DC_PRODUCT	
Facilities	☐ Data Confidentiality Lab	
0	105.2.54.100.55	
Support	DC_VICTIM_WIN10_1	
🕁 Downloads	192.168.1.93	
Documentation	Andrew Workstation	
	Data Confidentiality Lab So Data Confidentiality 192.168.2.10	ļ U

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

2.6 Integration: FireEye Helix and Cisco Stealthwatch

In the following section, Cisco Stealthwatch will be configured to forward logs to an on-premise Helix Communications Broker. Cisco Stealthwatch, as a network monitoring solution, can provide logs relevant to malicious network activity, potential data egress, as well as contextual information that can aid in the early detection of confidentiality events and the assessment of damage after an attack on confidentiality has occurred. An integration with the logging capability is useful for contextualizing information provided by other tools, generating alerts, and providing historical archives for reporting and compliance purposes.

2.6.1 Configure the Helix Communications Broker

- 1. On the CentOS system with the Helix Communications Broker installed, run the following commands:
 - > cd /opt/tap-nxlog
 - > sudo ./setup.sh
- 2. Select Add Routes and press Enter.
- 3. Select syslog.
- 4. Select udp.
- 5. Select the IP address of the network interface that should receive logs.
- 6. Enter 514 for the port.

1				adı	ministrator(@locall	host:/opt	/tap-nxlo	g		-		×
File	Edit	View	Search	Terminal	Help								
[IN	PUT S	OURCE	SETUP	::ADD —									
In	put T	ype	(X (() syslo) json) bsd	g								
Pr	otoco [:]	l Typ	e (X (() udp) tcp) ssl									
τn	put II	nteri	ace ((X () 192.1) 192.1) 127.0	68.122.1 68.1.206 .0.1								
In	put P	ort	51	4									
										Cance		0K	

- 7. Select OK and press Enter.
- 8. Select OK and press Enter.

2.6.2 Configure Stealthwatch to Forward Events

- 1. Log on to the Stealthwatch Management Console web interface.
- 2. Navigate to **Configure > Response Management**.
- 3. Click the **Actions** tab.
- 4. Click the three dots next to Send to Syslog and click Edit.
- 5. Set the action to **Enabled**.
- 6. Enter the address of the Helix Communications Broker.
- 7. Enter the port that you selected earlier.

A Not secure https://192.168.1.63/	sw-response-mgmt/		6 \$	
ules Actions Syslog Formats				
yslog Message Action			Cancel	Save
		Description		
Send to Syslog		Sends a message to the syslog server designated in the Syslog Add	fress field using	
		the default Syslog Message format.		
Enabled Disabled actions are not perform	ned for any associated rules.			- 11
Enabled Disabled actions are not performed	med for any associated rules.			4
Enabled Disabled actions are not perfor	med for any associated rules.			11
Enabled Disabled actions are not perfor Syslog Server Address	UDP Port			
Enabled Disabled actions are not perfor Syslog Server Address 192.168.1.206	UDP Port 514			
Enabled Disabled actions are not perfor Syslog Server Address 192.168.1.206	UDP Port			4
Enabled Disabled actions are not perfor Syslog Server Address 192.168.1.206 Message Format	UDP Port			4
Enabled Disabled actions are not perfor Syslog Server Address 192.168.1.206 Message Format Custom CEF	UDP Port			
Enabled Disabled actions are not perfor Syslog Server Address 192.168.1.206 Message Format Custom CEF Syslog Format	UDP Port	4		
Enabled Disabled actions are not perfor Syslog Server Address 192.168.1.206 Message Format Custom CEF Syslog Format Default Format Default Format	UDP Port 514	L		
Enabled Disabled actions are not perfor Syslog Server Address 192.168.1.206 Message Format Custom CEF Syslog Format Default Format	UDP Port	P ₂		
Enabled Disabled actions are not perfor Syslog Server Address 192.168.1.206 Message Format Custom CEF Syslog Format Default Format	UDP Port	Þ		*

8. Click Save.

9. Click the **Rules** tab.

10. On the **Actions** tab, you can use some of the existing rules or create your own.

Response Management Stealthy × +								-
→ C A Not secure https://192.168.1	.63/sw-response-mgmt/					ß	2 🖈 🛛	(
Stealthwatch dc.ipdrr	 Dashboards • 	Monitor • Analyze •	Jobs 🔻	Configure 🔻	Deploy •	۹ 🍂	1 0	+
esponse Management								
soponise management								
Rules Actions Syslog Formats								
Rules						Add N	New Rule	~
Name ↑	Туре	Description			FlowCollector System	n Alarm		
All Exporter or Interface Alarms	Exporter or Interface Alarm	This rule sends an email (E to a designated syslog sen Interface alarm occurs with	mail action) to ver (Syslog M any level of	o designated recip essage action) wh severity. You can e	e Exporter or Interface d Host Alarm	ement Console S Alarm	System Alarm	I
		Specify email recipients an work.	ace alarms a d/or a syslog	s opposed to havin server address if	W Host Group Relations UDP Director Alarm	hip Alarm		
All FlowCollector System Alarms	FlowCollector System Alarm	This rule sends an email (E to a designated syslog sen alarm occurs with any level Flow Collector alarms as op recipients and/or a syslog s	mail action) to ver (Syslog M of severity. Y oposed to har server addres	o designated recip essage action) wh 'ou can edit this ru ving all of them ind s if you want this	ients and a message en any Flow Collector le to specify particular cluded. Specify email ule to work.		•••	
All SMC System Alarms	Stealthwatch Management Console System Alarm	This rule sends an email (E to a designated syslog serv occurs with any level of sev alarms as opposed to havir and/or a syslog server add	mail action) to ver (Syslog M verity. You can ng all of them ress if you wa	o designated recip essage action) wh n edit this rule to s included. Specify ant this rule to wor	ients and a message en any SMC alarms pecify particular SMC email recipients k.		•••	

11. To create your own, click **Add New Rule**. For the purposes of this example, we select **FlowCollector System Alarm**.

- 12. Enter a name for the rule.
- 13. Ensure the rule is **Enabled**.
- 14. Click the **plus sign** under "Rule is triggered if". You can select conditions for the rule to trigger, based on severity, processing time, and type.

- C A NOUSECURE Https://192.16	o. 1.05/sw-response-mgmt/		F	γ H L
Associated Astions				
Associated Actions				
Execute the following actions when the ala	arm becomes active :			
Name †	Туре	Description	Used By Rules	Assigned
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	
Execute the following actions when the ala	arm becomes inactive :			
Name †	Туре	Description	Used By Rules	Assigned
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	

- 15. Enable **Send to Syslog** in the **Associated Actions** section. You can enable syslog messages for when the alarm becomes active and inactive.
- 16. You can also configure email alerts through this interface to improve the response time for incidents (this is a separate **Action** that needs to be edited on the **Actions** tab).

Response Management Stealth: × +		✓ - □ ×
← → C ▲ Not secure https://192.168.1.63/sw-response-mgmt/		ie 🖈 🛛 😩 :
Rules Actions Syslog Formats		
Rules FlowCollector System Alarm		Cancel
Name	Description	
Flow Collector Alarm. C Enabled Disabled rules are not triggered even when associated conditions are met.		Å
Rule is triggered if:		
ANY • of the following is true:	G.	+ ->)
Severity v is Minor v or higher	×	—
Associated Actions		
Funanta the following estimate when the slarm becames asthmy		

17. Click Save.

2.7 Integration: FireEye Helix and PKWARE PKProtect

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. In this build, PKProtect provides a data management capability that allows organizations to track data across an enterprise. As it is also providing encryption for this data, it provides important insight into sensitive data that is vulnerable to attack, as well as the ability to review, post-breach, which data may have been compromised in an

attack. An integration with the logging capability is useful for contextualizing information provided by other tools, generating alerts, and providing historical archives for reporting and compliance purposes. This section assumes the Helix Communications Broker has already been installed.

2.7.1 Configure the Helix Communications Broker

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

	administrator@localhost:/opt/tap-nxlog	-	•	×
File Edit View Search	Terminal Help			
INPUT SOURCE SETUP:	: ADD			٦
Input Type () () (X)	syslog json bsd			
Protocol Type () (X) () Toput Interface	udp tcp ssl			
() (X) ()	192.168.122.1 192.168.1.206 127.0.0.1			
Input Port 513				
	Cancel		ок	

- 7 . Select OK and press Enter.
- 8. Select OK and press Enter.

2.7.2 Configure PKWARE PKProtect to Forward Events

- 1. Navigate to the PKWARE PKProtect web portal.
- 2 . Click the \mbox{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	× 🗾 EdgeFW-PFS.ID115.Ja	bs.nccoe.nis 🗙 🕲 Basics	× Creating and Deploying Classific: × +	• - • ×
$\leftarrow \rightarrow C$ A Not secure	192.168.1.43/mds/SuperUs	er/Basics		🖈 🚨 Update 🔅
PKWARE	 Actions System Base 	ics Advanced Dashboard Archive	Events	Help Log out Change Password
Dashboard Elasticsearc	h Target			
Enable D	SI in Dashboard Save	Cancel		
		DVWARE Enterning Manager 16.5	001 - About - environme 1/21/21 11/21/2 AM	
		The second processing of the second processing of the second	and a Canada a boundar put standar put standar beat	

- 7. Click Save.
- 8. In the **Data Security Intelligence** section, click **Internal** next to **Target**.
- 9. Select Syslog TCP RFC-3164 for Target.
- 10. Enter the URL and port of the Helix Communications Broker that was just configured.

HEUX FireEye × EdgeFW-PF	SJ0115.labs.nccor × 🕲 Basics	× Creating and Deploying Clas: × New Tab	× +	0 X
← → C ▲ Not secure 192.168.1.43/mi	ds/SuperUser/Basics			🖈 😩 Update 🔅
PKWARE" Actions 5	Basics Advanced Dashboard	Archive Events		Help Log out Change Password
Data Security Intelligence Target				
Target	Syslog TCP RFC-3164	Ŧ		
нU	192.168.1.206:513			
	Save Cancel			
	PODAE 61814	na Menger 18320 - <u>Jouri</u> - Janaseon 30207 124930 PA		

11. Click Save.

12. Verify that PKWARE logs now show up in Helix.

2.8 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. This was a bespoke integration performed by Dispel. Organizations should ensure that this integration is performed, and discussed with their Security Information and Event Management (SIEM) and Virtual Desktop Interface (VDI) vendors.

- This integration has two primary components. The first, configuring the route, is done locally on the Dispel wicket. This can be done using the following commands. Ensure that you replace the <subnet> and the <gateway> such that the Dispel wicket can accurately route to the Helix Communications Broker.
 - > config
 > set protocols static route <subnet> next-hop <gateway>
 - > commit && save && exit
- 2. The second component is configured server-side and involves informing the Dispel wicket via config file the actual port and location of the Helix Communications Broker. Instructions are not included for this, as in this integration, it was necessary to perform this integration remotely via the Dispel team.

2.9 Integration: Dispel and Cisco DUO

In this build, Dispel acts as an intermediary between the user and the enterprise systems, by providing temporary remote desktops with access to the enterprise systems. In this integration, we primarily installed Cisco Duo on the enterprise systems, to require multifactor authentication over RDP between Dispel's temporary remote desktops and the enterprise systems.

In this particular integration, no extra work was required other than installing Cisco Duo (see <u>Section</u> 2.3) on systems to control remote desktop access between Dispel machines and the other machines. However, it is important for organizations to check that this integration works and is present to ensure that multifactor authentication is being applied to users who are logging in remotely.
Appendix A List of Acronyms

SIEM	Security Information and Event Management
RDP	Remote Desktop Protocol
IP	Internet Protocol
ТСР	Transmission Control Protocol
SMC	Stealthwatch Management Console
DNS	Domain Name Service
NTP	Network Time Protocol
2FA	Two Factor Authentication
SFC	Stealthwatch Flow Collector
UDP	User Datagram Protocol