NIST SPECIAL PUBLICATION 1800-28C

Data Confidentiality:

Identifying and Protecting Data Against Data Breaches

Volume C:
How-To Guides

William Fisher
National Cybersecurity Center of Excellence
NIST

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

February 2024

FINAL

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-28

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

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 1800-28C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-28C, 86 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 ds-nccoe@nist.gov.

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology 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 https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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 risks associated with the loss of data confidentiality, and mitigations to protect against those risks.

KEYWORDS

asset management; cybersecurity framework; data breach; data confidentiality; data protection; identify; malicious actor; malware; protect; ransomware

ACKNOWLEDGMENTS

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

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

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

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
Avrio	Avrio SIFT
Cisco Systems	DUO

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

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 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 the ability to identify threats to and protect 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 1800-28A: *Executive Summary*
- NIST SP 1800-28B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-28C: *How-To Guides* – instructions for building the example solution **(you are here)**

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-28A*, which describes the following topics:

- challenges that enterprises face in identifying vulnerable assets and protecting them from data breaches
- 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 1800-28B*, 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 Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary, NIST SP 1800-28A*, with your leadership team members to help them understand the importance of adopting a standards-based solution to identify threats to and protect 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*-28C, 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 a solution to identify threats to and protect 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 ds-nccoe@nist.gov .

1.2 Build Overview

The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively identify sensitive data and protect against 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.

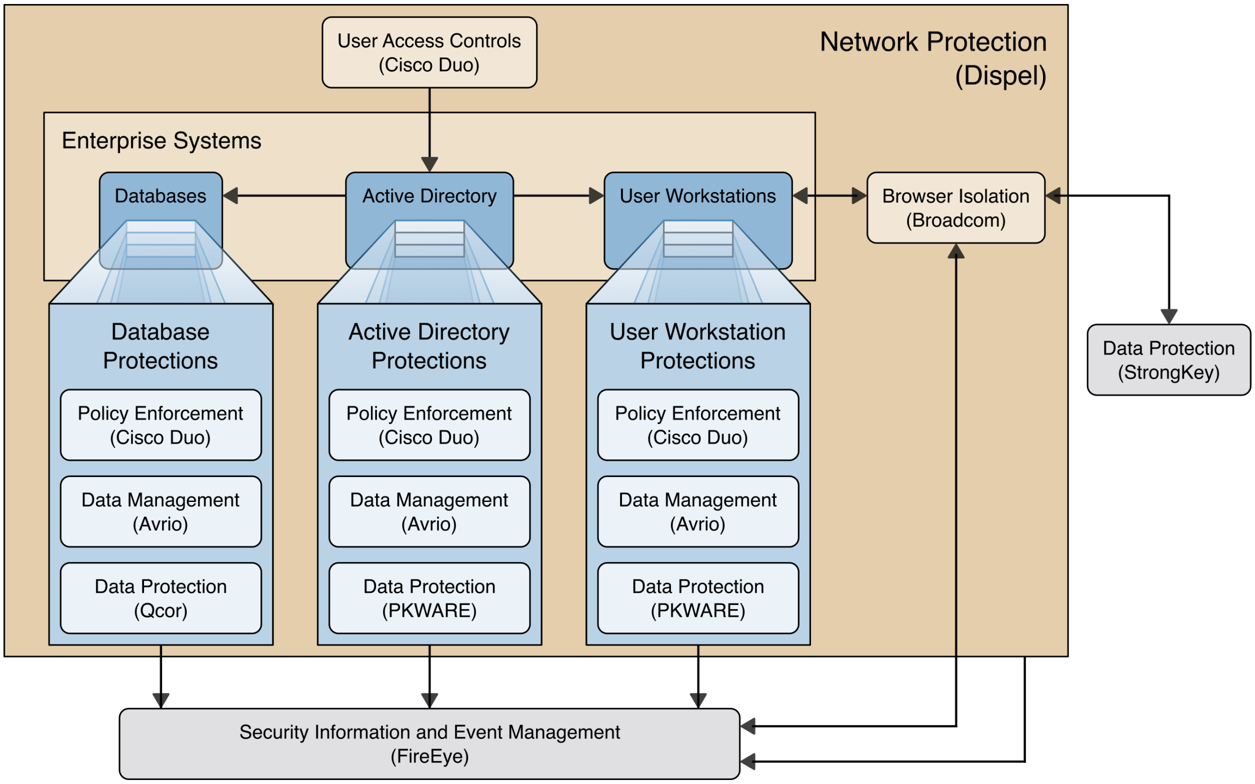
1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

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 technologies 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.


Network Protection (Dispel)
User Access Controls (Cisco Duo)
Enterprise Systems
Databases
Active Directory
User Workstations
Browser Isolation (Broadcom)
Data Protection (StrongKey)
Database Protections
Policy Enforcement (Cisco Duo)
Data Management (Avrio)
Data Protection (Qcor)
Active Directory Protections
Policy Enforcement (Cisco Duo)
Data Management (Avrio)
Data Protection (PKWARE)
User Workstation Protections
Policy Enforcement (Cisco Duo)
Data Management (Avrio)
Data Protection (PKWARE)
Security Information and Event Management (FireEye)

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

For a more detailed description of our architecture, see Volume B, Section 4.

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, which 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- CentOS 7

1. Acquire the Helix Communications Broker for CentOS 7.
2. Navigate to the folder containing the installer, and run

   ```
   > 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.

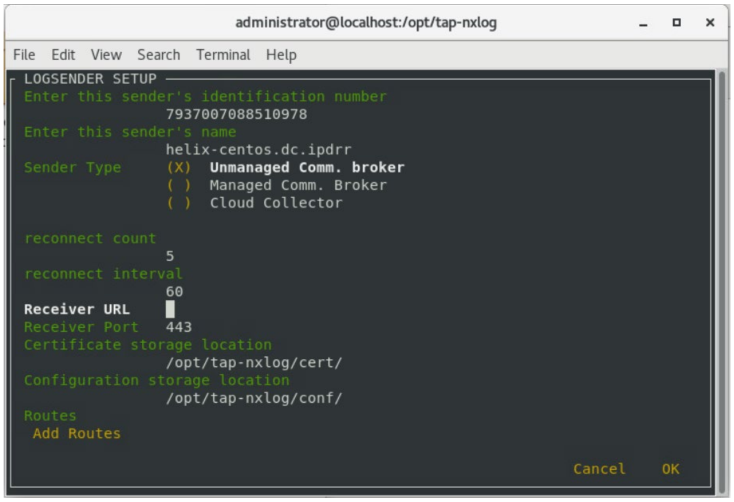
    ```
    > sudo cd ..
    ```

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.


administrator@localhost:/opt/tap-nxlog
File Edit View Search Terminal Help
Cancel
OK

```
LOGSENDER SETUP
Enter this sender's identification number
                7937007088510978
Enter this sender's name
                helix-centos.dc.ipdrr
Sender Type     (X)  Unmanaged Comm. broker
                ( )  Managed Comm. Broker
                ( )  Cloud Collector

reconnect count
                5
reconnect interval
                60
Receiver URL    █
Receiver Port   443
Certificate storage location
                /opt/tap-nxlog/cert/
Configuration storage location
                /opt/tap-nxlog/conf/
Routes
 Add Routes
```

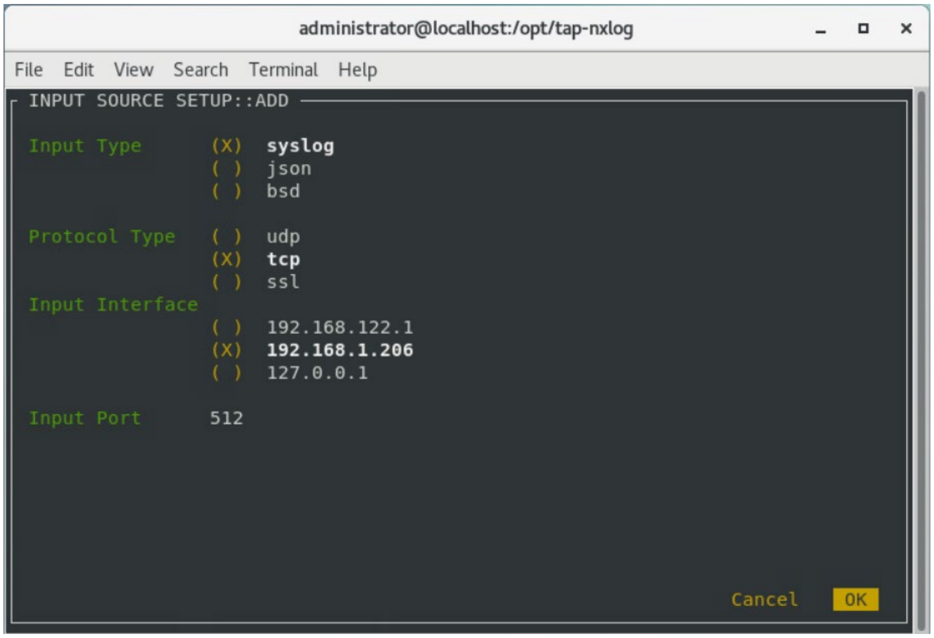
15. Select **Add Routes** and press **Enter**.

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.


administrator@localhost:/opt/tap-nxlog
File Edit View Search Terminal Help
Cancel
OK

```
INPUT SOURCE SETUP::ADD

Input Type        (X)  syslog
                  ( )  json
                  ( )  bsd

Protocol Type     ( )  udp
                  (X)  tcp
                  ( )  ssl
Input Interface
                  ( )  192.168.122.1
                  (X)  192.168.1.206
                  ( )  127.0.0.1

Input Port        512
```

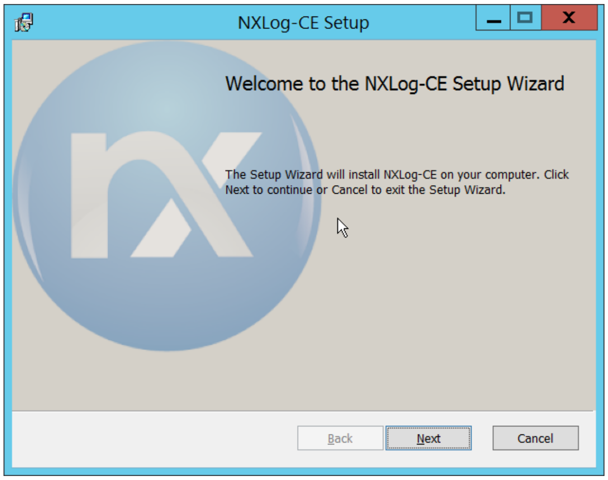
20. Select **OK** and press **Enter**.

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 http://nxlog.org/products/nxlog-community-edition/download.

2. Run **nxlog-ce-2.10.2150.msi**.



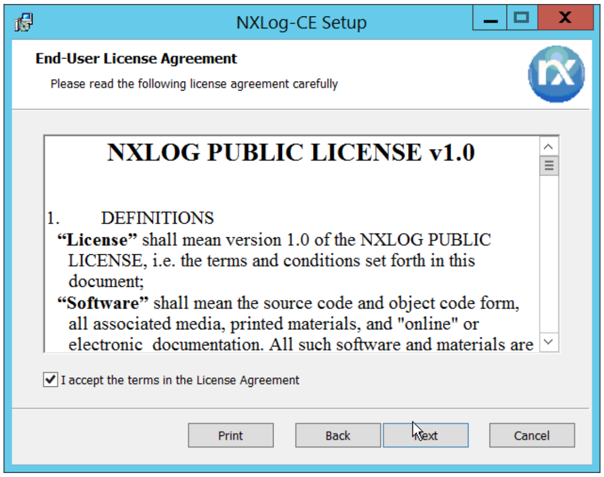
NXLog-CE Setup

Welcome to the NXLog-CE Setup Wizard

The Setup Wizard will install NXLog-CE on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

3. Click **Next**.

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



NXLog-CE Setup

End-User License Agreement

Please read the following license agreement carefully

NXLOG PUBLIC LICENSE v1.0

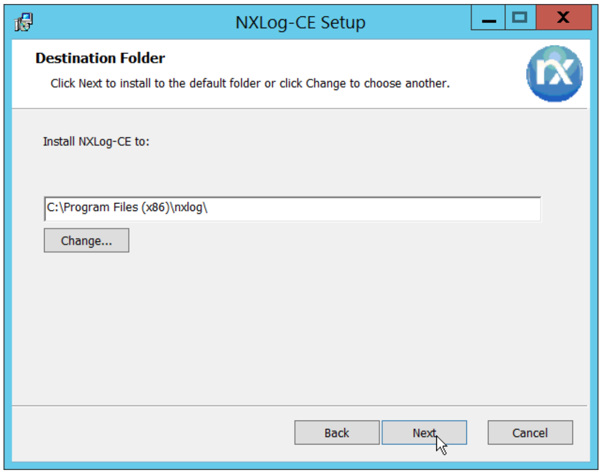
1. DEFINITIONS

"License" shall mean version 1.0 of the NXLOG PUBLIC LICENSE, i.e. the terms and conditions set forth in this document;

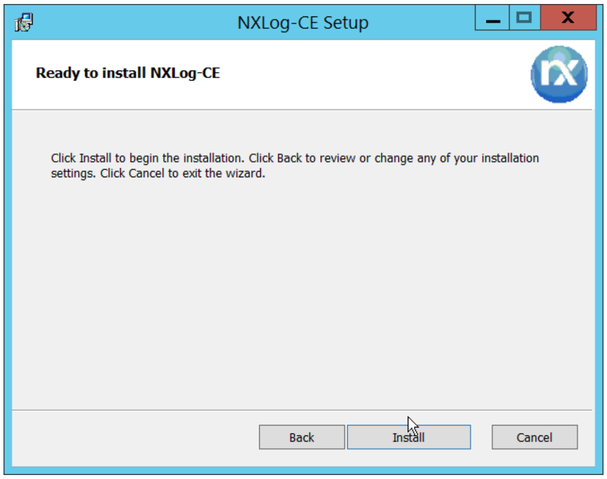
"Software" shall mean the source code and object code form, all associated media, printed materials, and "online" or electronic documentation. All such software and materials are

☑ I accept the terms in the License Agreement

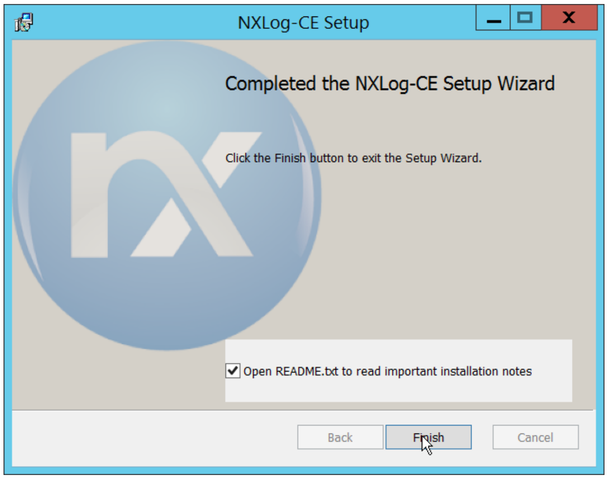
5. Click **Next**.


NXLog-CE Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Install NXLog-CE to:
C:\Program Files (x86)\nxlog\
Change...
Back
Next
Cancel

6. Click **Next**.


NXLog-CE Setup
Ready to install NXLog-CE
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

7. Click **Install**.


NXLog-CE Setup
Completed the NXLog-CE Setup Wizard
Click the Finish button to exit the Setup Wizard.
☑ Open README.txt to read important installation notes
Back
Finish
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
    Host        192.168.1.206
    Port        512
    Exec        to_syslog_snare();
</Output>

<Route 1>
    Path        in => out
</Route>
```

11. Restart the **nxlog** service.

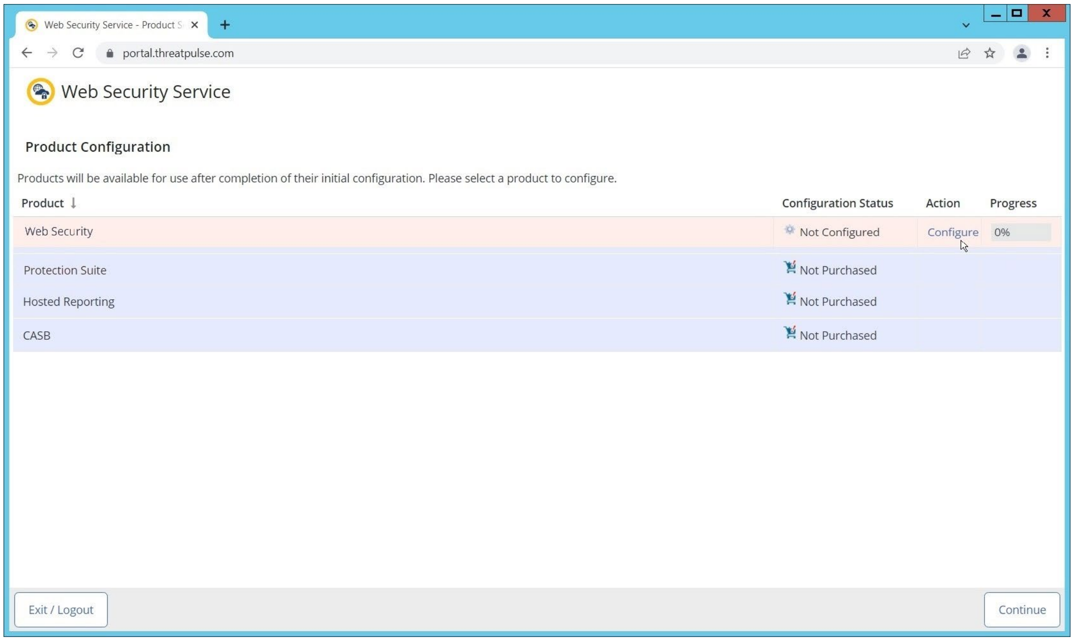
12. You can verify that this connection is working by checking the logs in *data\nxlog.log*, and by noting an increase in events on the Helix Dashboard.

2.2 Symantec Cloud Secure Web Gateway

This installation and configuration guide for Symantec SWG uses a cloud instance of Web Isolation. In this guide, Web Isolation is used to isolate threats to the user through the browser. It does this through the use of a web proxy, which captures traffic and assigns a threat level to it, and based on administrative policy decides whether to serve the page to the user. In doing so, threats from the web can be mitigated through shared intelligence and isolated execution of the page before it reaches the user’s desktop.

2.2.1 Configure Web Security Service (WSS)

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



Product Configuration

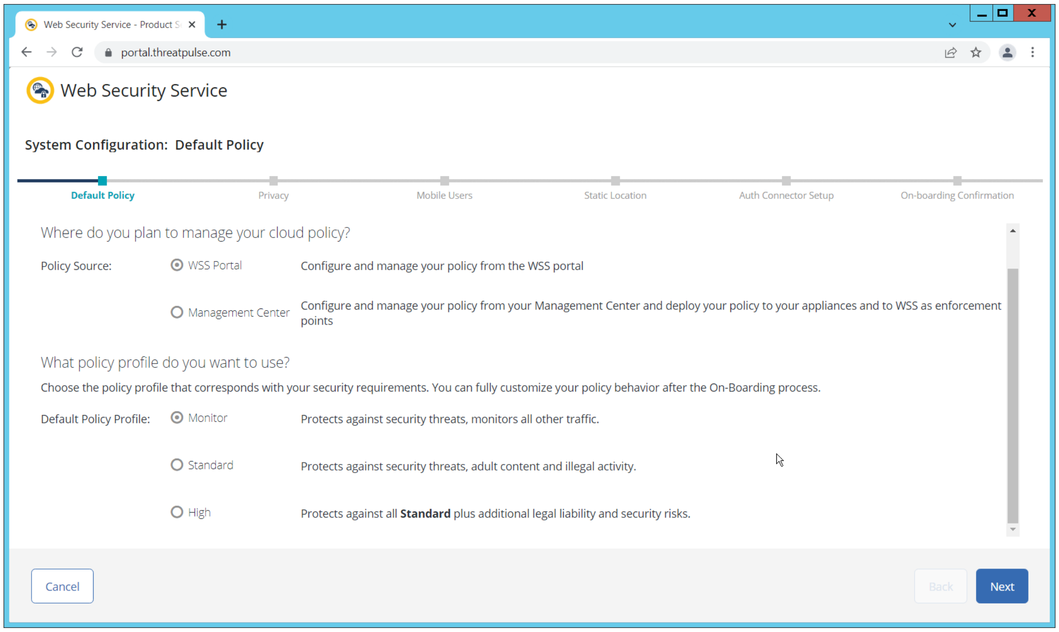
Products will be available for use after completion of their initial configuration. Please select a product to configure.

Product ↓	Configuration Status	Action	Progress
Web Security	Not Configured	Configure	0%
Protection Suite	Not Purchased		
Hosted Reporting	Not Purchased		
CASB	Not Purchased		

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

3. Select **WSS Portal**.

4. Select **Monitor**.



System Configuration: Default Policy

Where do you plan to manage your cloud policy?

Policy Source: ● WSS Portal — Configure and manage your policy from the WSS portal

○ Management Center — Configure and manage your policy from your Management Center and deploy your policy to your appliances and to WSS as enforcement points

What policy profile do you want to use?

Choose the policy profile that corresponds with your security requirements. You can fully customize your policy behavior after the On-Boarding process.

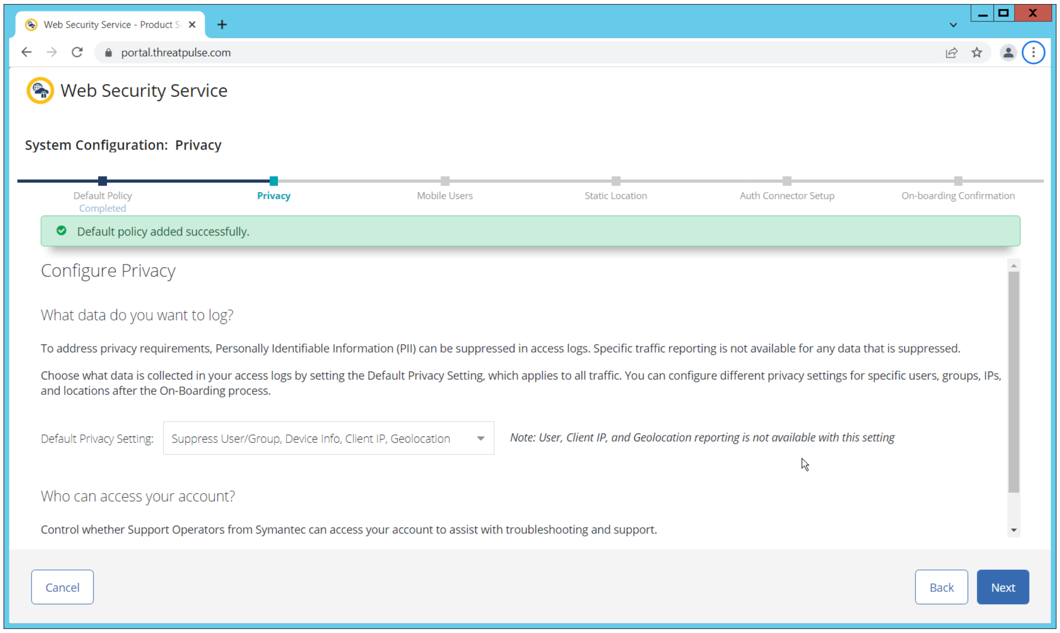
Default Policy Profile: ● Monitor — Protects against security threats, monitors all other traffic.

○ Standard — Protects against security threats, adult content and illegal activity.

○ High — Protects against all **Standard** plus additional legal liability and security risks.

5. Click **Next**.

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



System Configuration: Privacy

Default policy added successfully.

Configure Privacy

What data do you want to log?

To address privacy requirements, Personally Identifiable Information (PII) can be suppressed in access logs. Specific traffic reporting is not available for any data that is suppressed.

Choose what data is collected in your access logs by setting the Default Privacy Setting, which applies to all traffic. You can configure different privacy settings for specific users, groups, IPs, and locations after the On-Boarding process.

Default Privacy Setting: Suppress User/Group, Device Info, Client IP, Geolocation

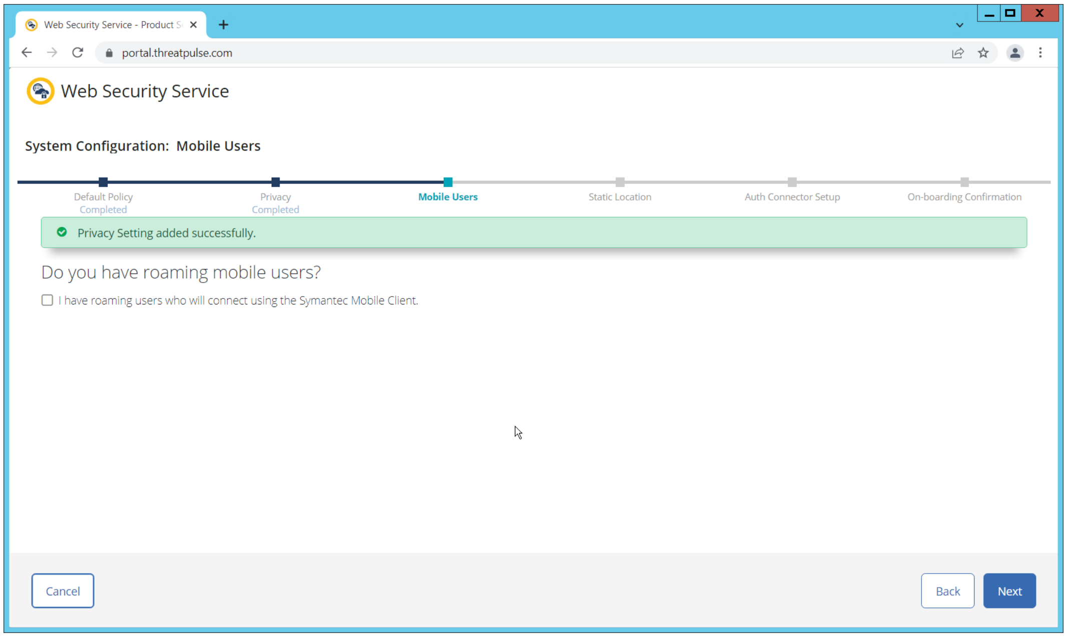
Note: User, Client IP, and Geolocation reporting is not available with this setting

Who can access your account?

Control whether Support Operators from Symantec can access your account to assist with troubleshooting and support.

7. Click Next.

8. Indicate whether you have mobile users.



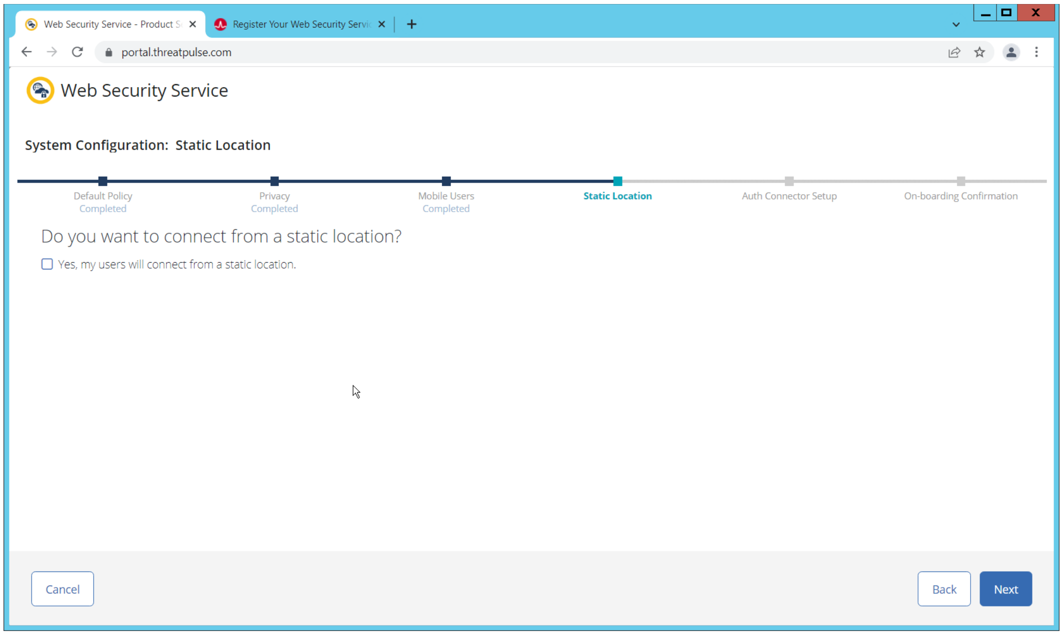
System Configuration: Mobile Users

Privacy Setting added successfully.

Do you have roaming mobile users?

☐ I have roaming users who will connect using the Symantec Mobile Client.

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



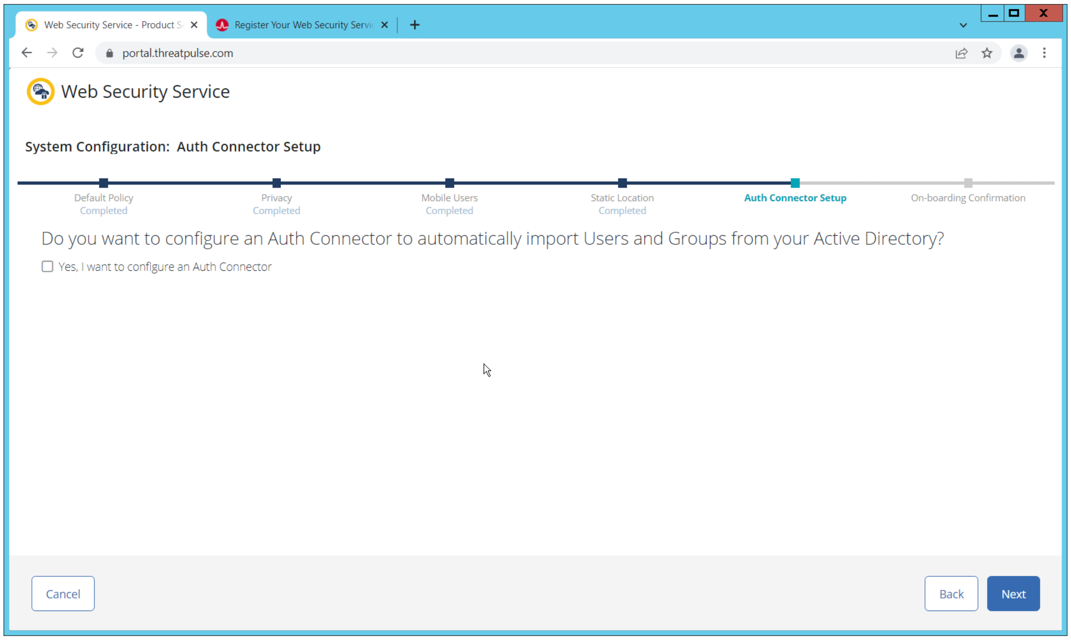
Web Security Service

System Configuration: Static Location

Do you want to connect from a static location?

□ Yes, my users will connect from a static location.

10. Click **Next**. Indicate whether you want to configure an Auth Connector.



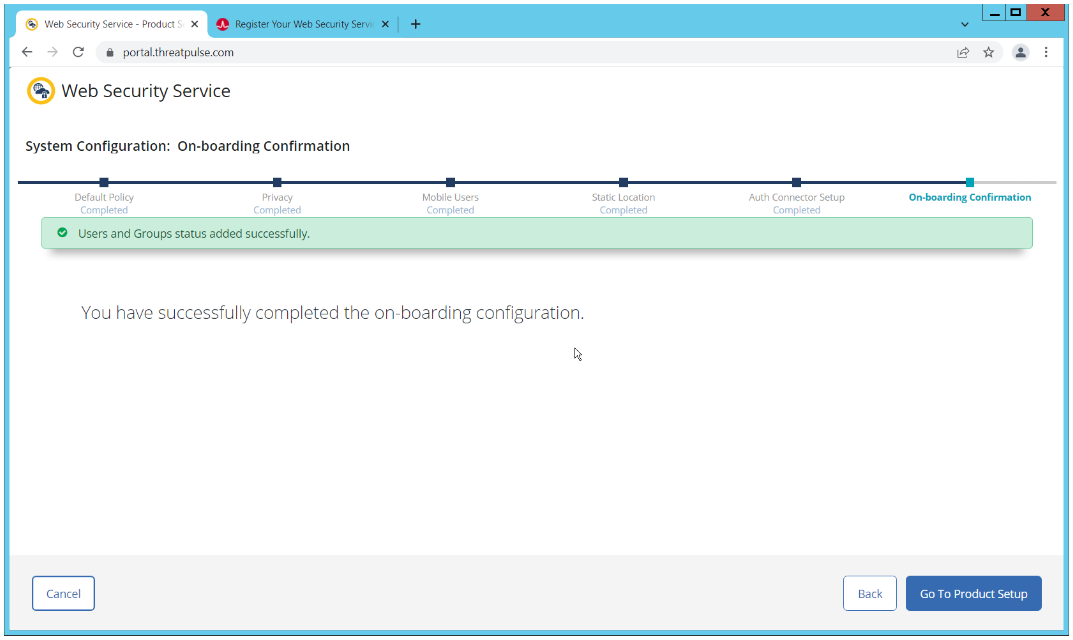
Web Security Service

System Configuration: Auth Connector Setup

Do you want to configure an Auth Connector to automatically import Users and Groups from your Active Directory?

□ Yes, I want to configure an Auth Connector

11. Click **Next**.



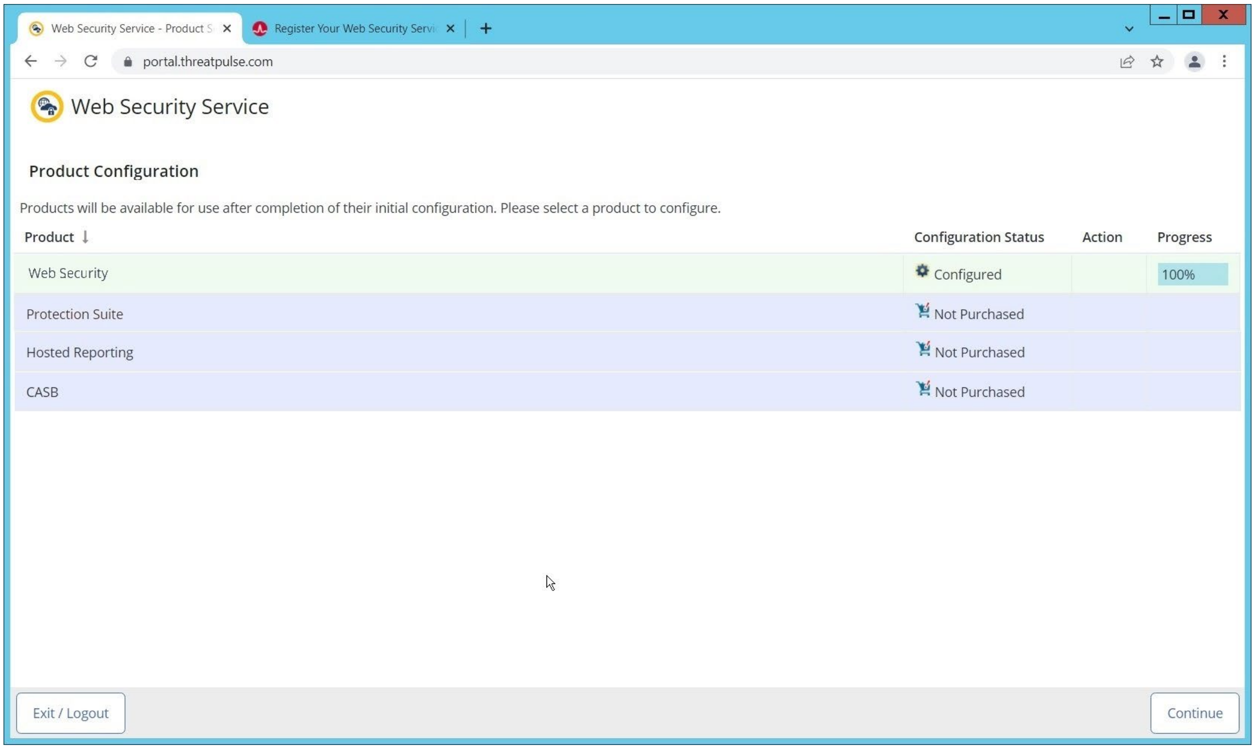
Web Security Service

System Configuration: On-boarding Confirmation

Users and Groups status added successfully.

You have successfully completed the on-boarding configuration.

12. Click Go To Product Setup.



Web Security Service

Product Configuration

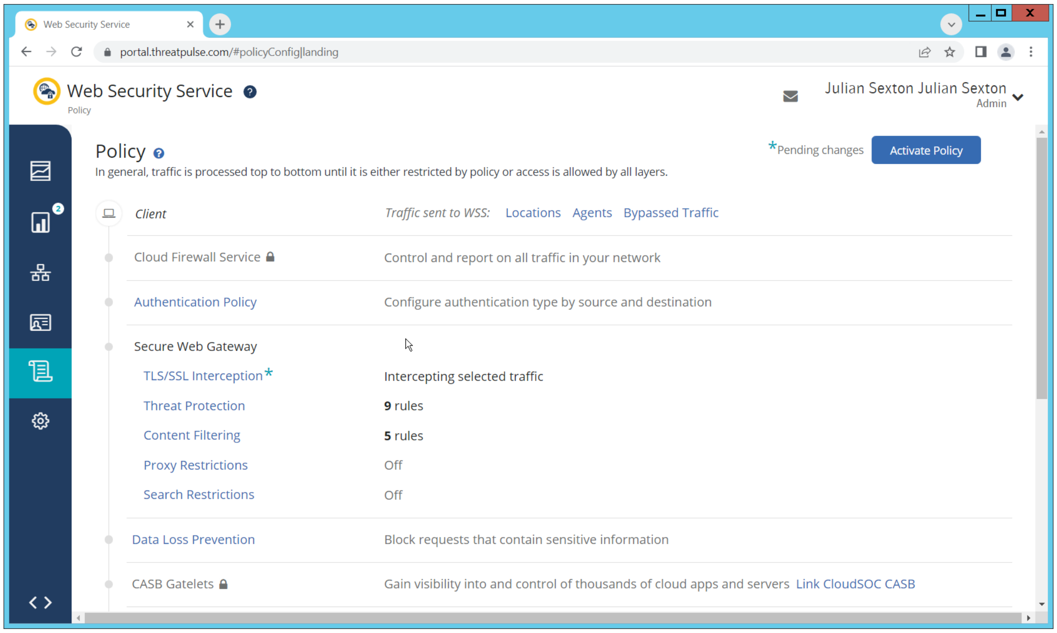
Products will be available for use after completion of their initial configuration. Please select a product to configure.

Product	Configuration Status	Action	Progress
Web Security	Configured		100%
Protection Suite	Not Purchased		
Hosted Reporting	Not Purchased		
CASB	Not Purchased		

13. Click Continue.

2.2.2 Install Proxy Certificates and enabling TLS/SSL Interception

1. Click the **Policy** tab.



Web Security Service

portal.threatpulse.com/#policyConfig|landing

Web Security Service
Policy

Julian Sexton Julian Sexton
Admin

Policy

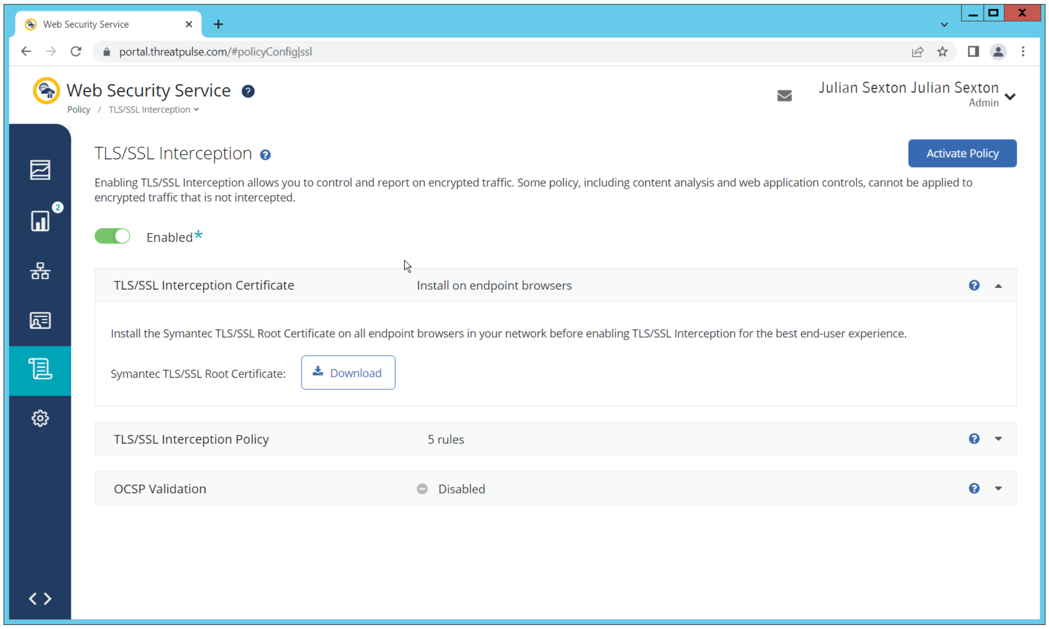
In general, traffic is processed top to bottom until it is either restricted by policy or access is allowed by all layers.

*Pending changes Activate Policy

Client	*Traffic sent to WSS:* Locations Agents Bypassed Traffic
Cloud Firewall Service	Control and report on all traffic in your network
Authentication Policy	Configure authentication type by source and destination
Secure Web Gateway	
TLS/SSL Interception*	Intercepting selected traffic
Threat Protection	**9** rules
Content Filtering	**5** rules
Proxy Restrictions	Off
Search Restrictions	Off
Data Loss Prevention	Block requests that contain sensitive information
CASB Gatelets	Gain visibility into and control of thousands of cloud apps and servers Link CloudSOC CASB

2. Click TLS/SSL Interception.

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



Web Security Service

portal.threatpulse.com/#policyConfig|ssl

Web Security Service
Policy / TLS/SSL Interception

Julian Sexton Julian Sexton
Admin

TLS/SSL Interception

Activate Policy

Enabling TLS/SSL Interception allows you to control and report on encrypted traffic. Some policy, including content analysis and web application controls, cannot be applied to encrypted traffic that is not intercepted.

Enabled*

TLS/SSL Interception Certificate	Install on endpoint browsers

Install the Symantec TLS/SSL Root Certificate on all endpoint browsers in your network before enabling TLS/SSL Interception for the best end-user experience.

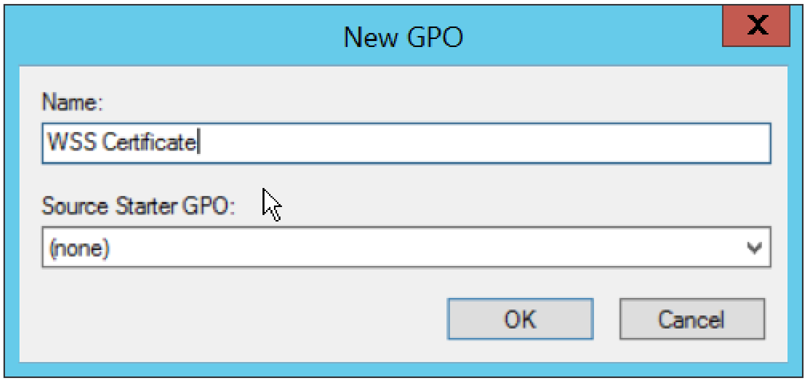
Symantec TLS/SSL Root Certificate: Download

TLS/SSL Interception Policy	5 rules
OCSP Validation	Disabled

4. Download the certificate here. You can either install this individually in the Trusted Root Certification Authorities store on individual machines or follow the below steps to distribute the certificate via Group Policy.

5. Open the Group Policy Management Console.

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

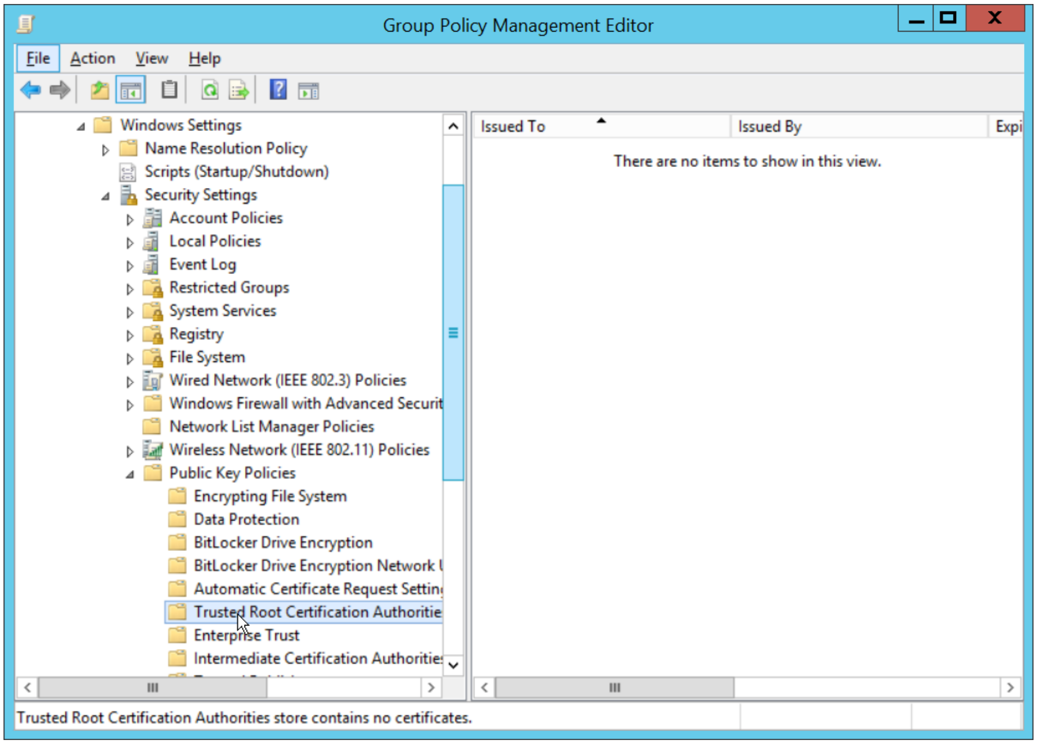


Name: WSS Certificate

Source Starter GPO: (none)

7. Enter a name and click OK.

8. Right click the newly created GPO and click **Edit…**.


Group Policy Management Editor
File
Action
View
Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Securit
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network U
Automatic Certificate Request Settin
Trusted Root Certification Authoritie
Enterprise Trust
Intermediate Certification Authoritie
Issued To
Issued By
Expi

There are no items to show in this view.

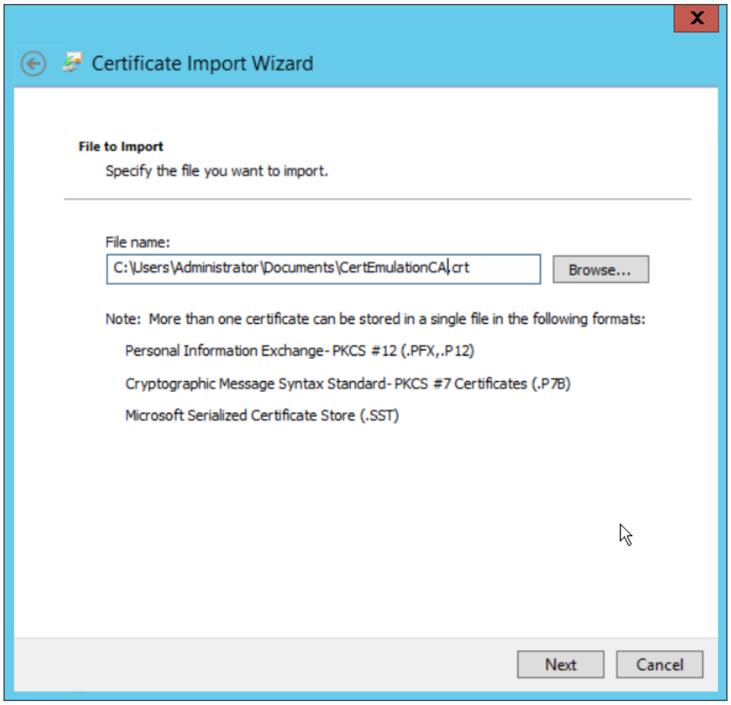
Trusted Root Certification Authorities store contains no certificates.

9. Navigate to Computer Configuration > Policies > Window Settings > Security Settings > Public Key Policies, and right click Trusted Root Certification Authorities.

10. Click Import.

11. Click Next.

12. Select the certificate you just downloaded.



File to Import

Specify the file you want to import.

File name:

C:\Users\Administrator\Documents\CertEmulationCA.crt

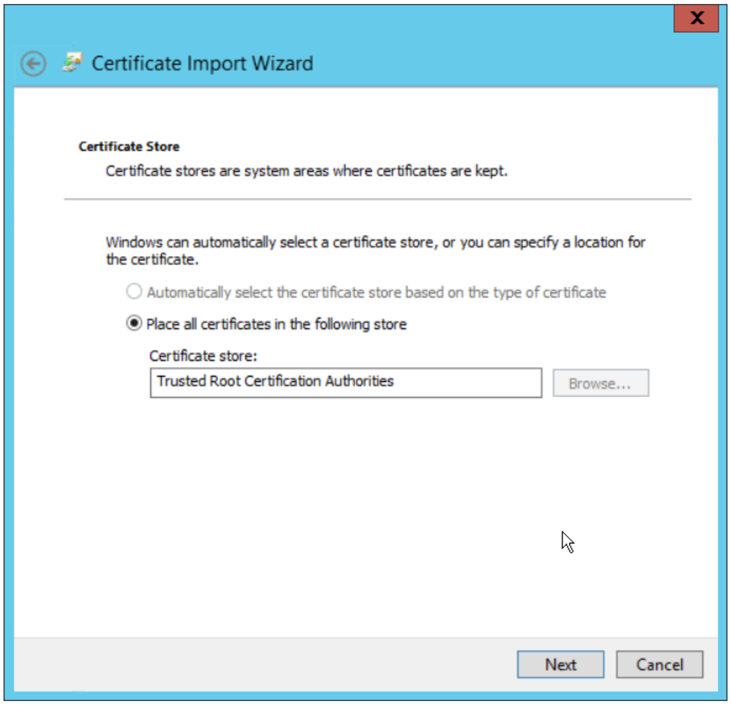
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

13. Click **Next**.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

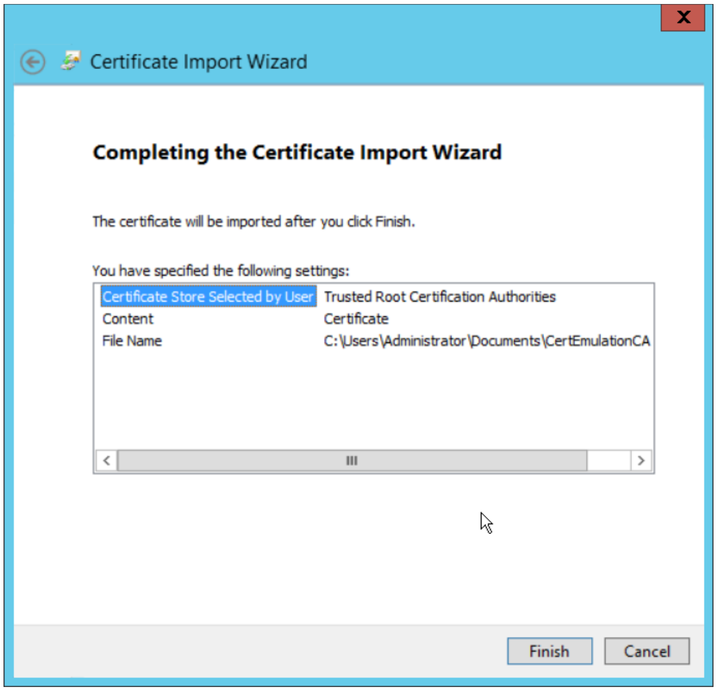
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

14. Click **Next**.



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

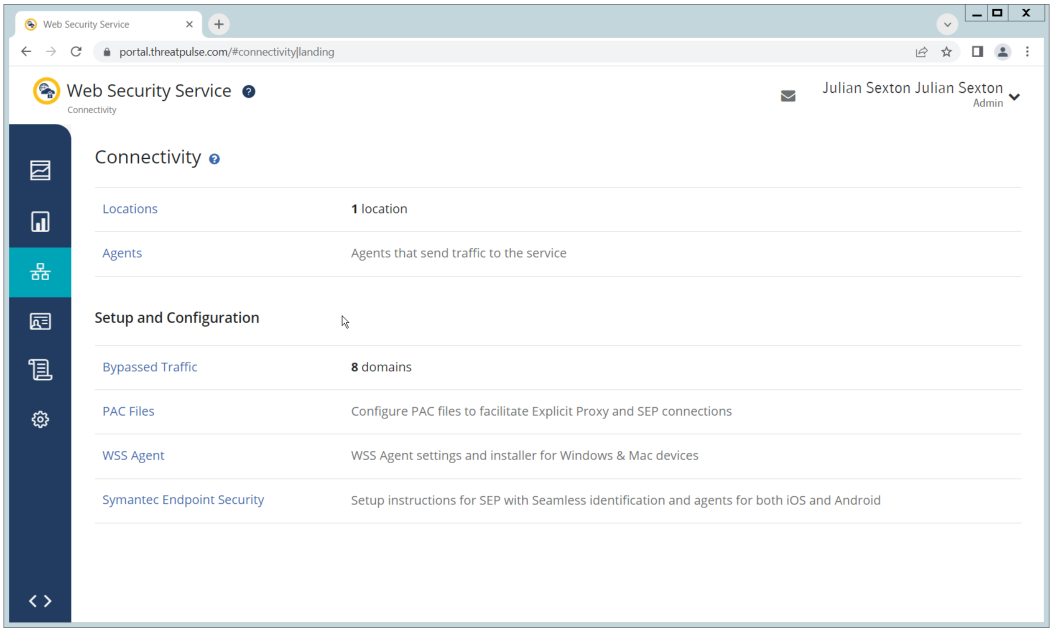
Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\Administrator\Documents\CertEmulationCA

15. Click Finish.

16. Click OK.

2.2.3 Configure Symantec Web Security Service Proxy

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



Web Security Service
portal.threatpulse.com/#connectivity|landing
Web Security Service
Connectivity
Julian Sexton Julian Sexton
Admin

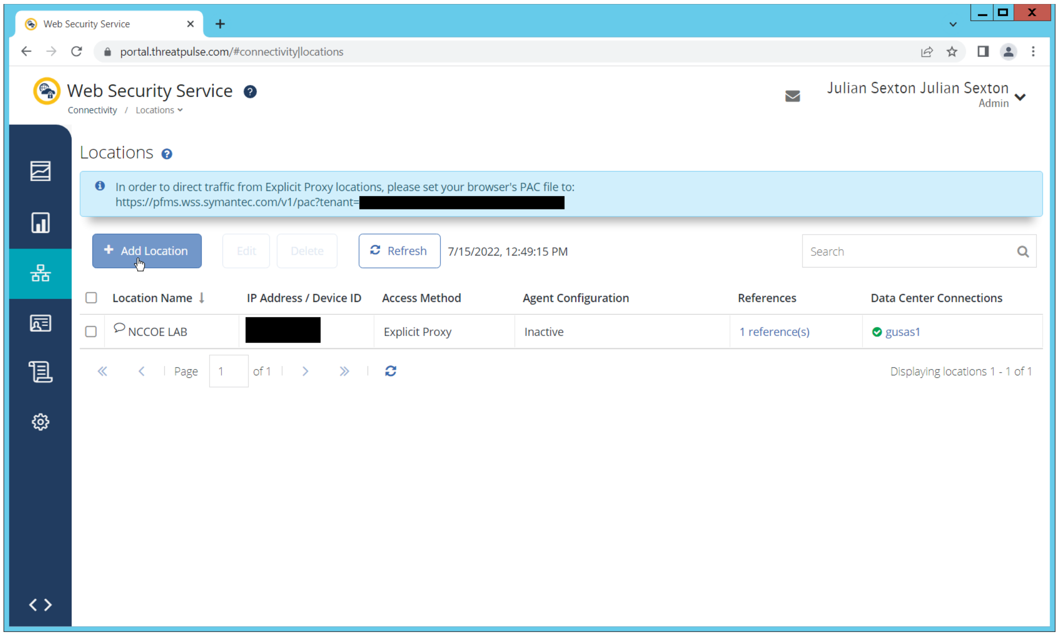
Connectivity

Locations	1 location
Agents	Agents that send traffic to the service

Setup and Configuration

Bypassed Traffic	8 domains
PAC Files	Configure PAC files to facilitate Explicit Proxy and SEP connections
WSS Agent	WSS Agent settings and installer for Windows & Mac devices
Symantec Endpoint Security	Setup instructions for SEP with Seamless identification and agents for both iOS and Android

2. Click Locations.


Web Security Service
portal.threatpulse.com/#connectivity|locations
Web Security Service
Connectivity / Locations
Julian Sexton Julian Sexton
Admin

Locations

In order to direct traffic from Explicit Proxy locations, please set your browser's PAC file to: https://pfms.wss.symantec.com/v1/pac?tenant=[redacted]

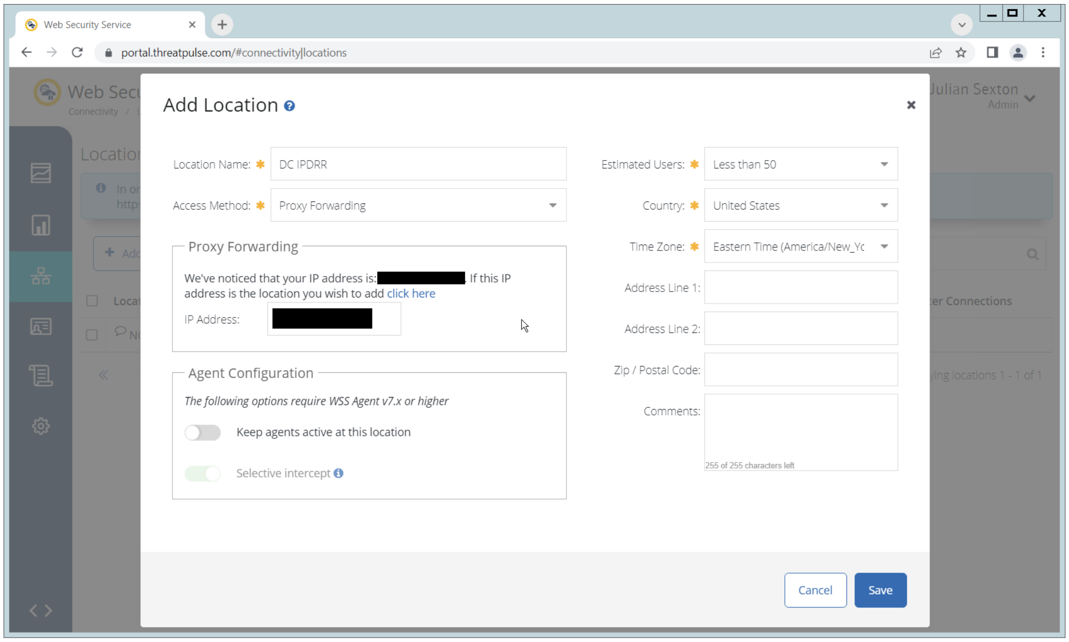
□	Location Name	IP Address / Device ID	Access Method	Agent Configuration	References	Data Center Connections
□	NCCOE LAB	[redacted]	Explicit Proxy	Inactive	1 reference(s)	✓ gusas1

3. Click Add Location.

4. Enter a name for the Location.

5. Select Proxy Forwarding for Access Method.

6. Enter any public IP addresses of your organization, to ensure that traffic sent through the WSS (Web Security Service) proxy is redirected to the proper dashboard.



Add Location

Location Name: *	DC IPDRR
Access Method: *	Proxy Forwarding

Proxy Forwarding

We've noticed that your IP address is:[redacted] If this IP address is the location you wish to add click here

IP Address: [redacted]

Agent Configuration

The following options require WSS Agent v7.x or higher

○ Keep agents active at this location

○ Selective intercept

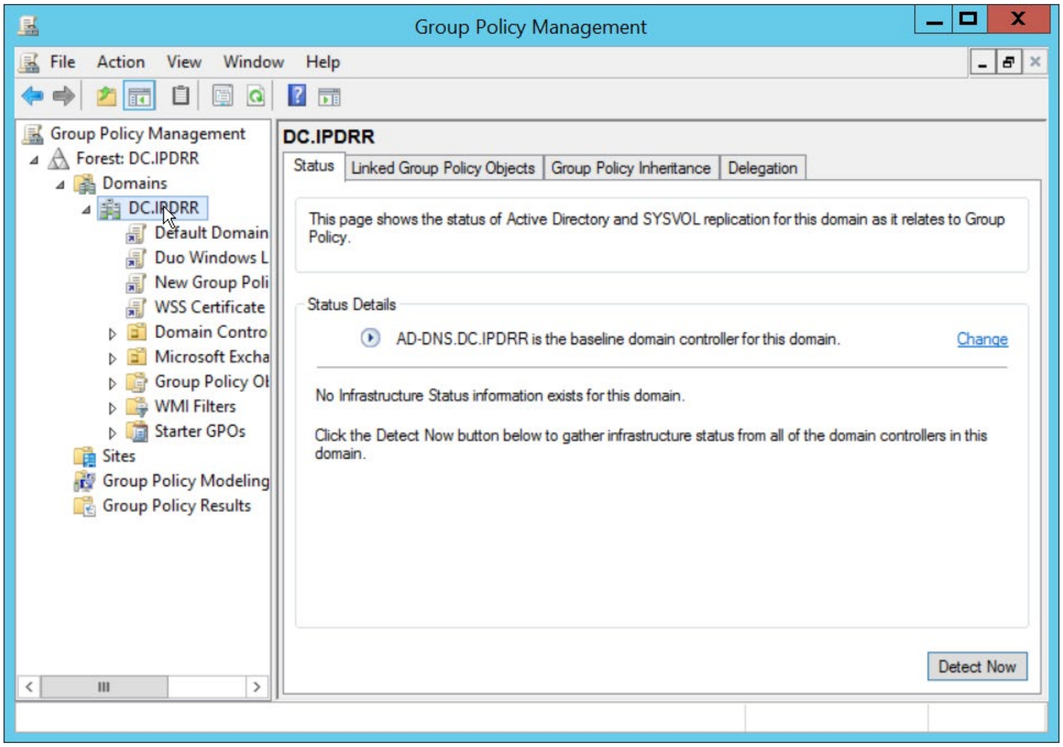
Estimated Users: *	Less than 50
Country: *	United States
Time Zone: *	Eastern Time (America/New_Yo
Address Line 1:	
Address Line 2:	
Zip / Postal Code:	
Comments:	

255 of 255 characters left

7. Click **Save**.

8. This page will now provide a URL to a PAC file that can be distributed to browsers across the organization via GPO. If you wish to create a custom PAC file, you can navigate to **Connectivity > PAC Files**.

9. Open the Group Policy Management Console.



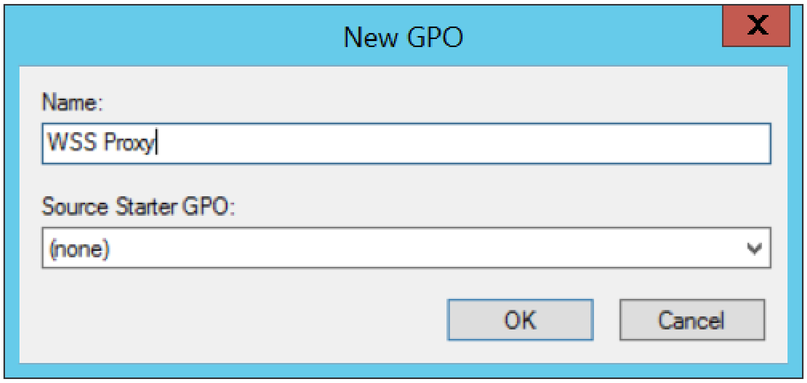
This page shows the status of Active Directory and SYSVOL replication for this domain as it relates to Group Policy.

AD-DNS.DC.IPDRR is the baseline domain controller for this domain.

No Infrastructure Status information exists for this domain.

Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.

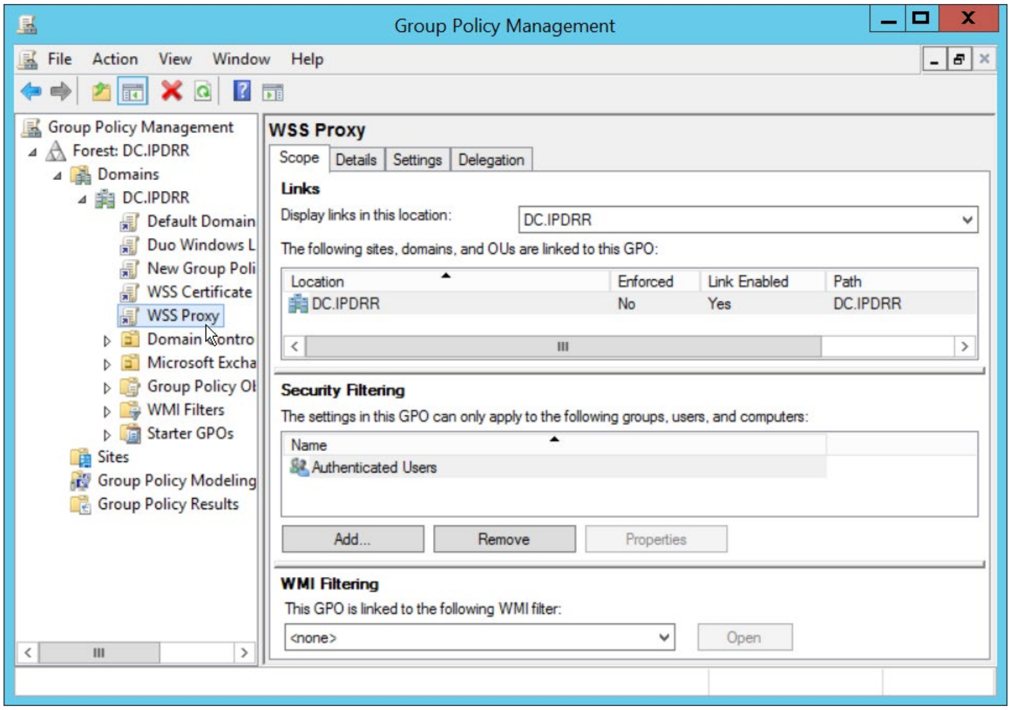
10. Right click the Domain and select Create a GPO in this domain, and Link it here….



Name: WSS Proxy

Source Starter GPO: (none)

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



WSS Proxy

Links

Display links in this location: DC.IPDRR

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
DC.IPDRR	No	Yes	DC.IPDRR

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

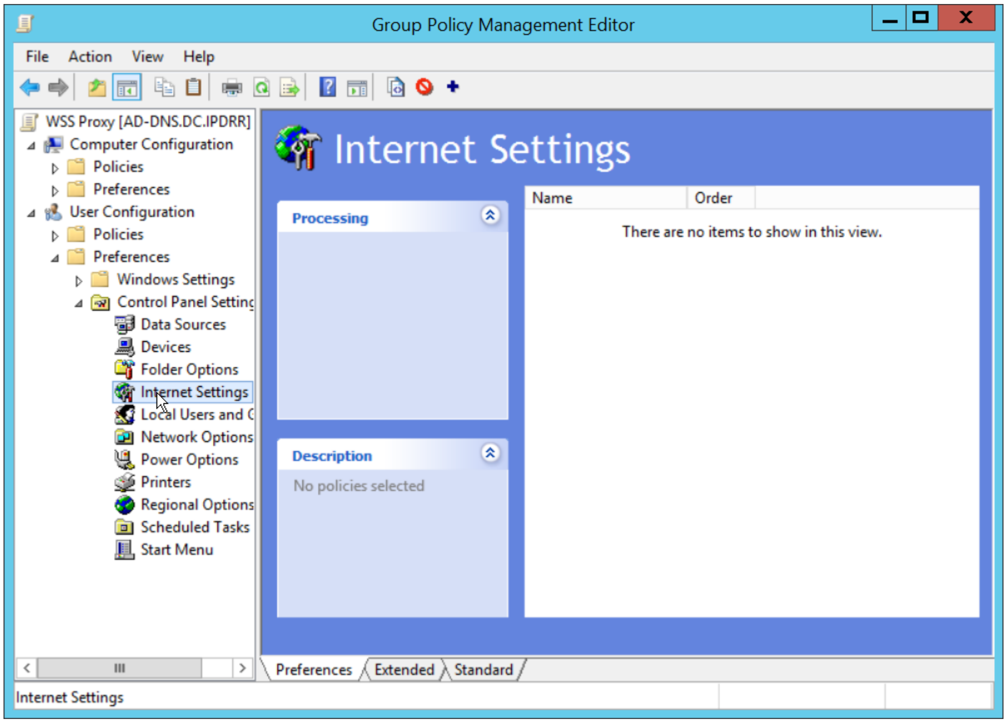
WMI Filtering

This GPO is linked to the following WMI filter:

<none>

12. Right click the newly created GPO and click **Edit…**.

13. Navigate to **User Configuration > Preferences > Control Panel Settings**.



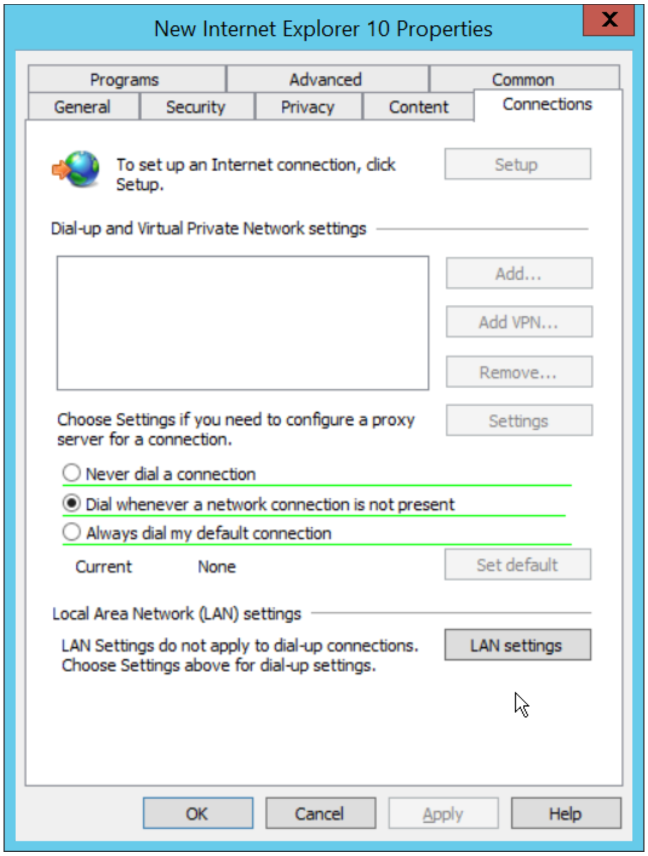
Internet Settings

Name	Order
There are no items to show in this view.	

No policies selected

14. Right click Internet Settings and select New > Internet Explorer 10 Properties.

15. Click the Connections Tab.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

○ Never dial a connection

● Dial whenever a network connection is not present

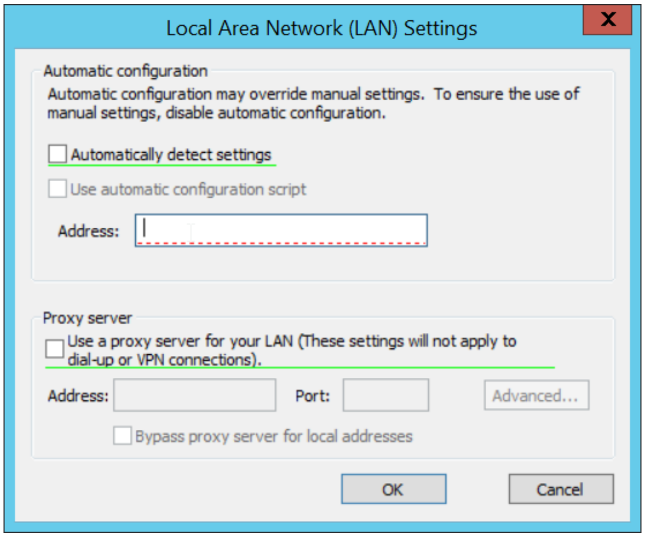
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

16. Click Local Area Network (LAN Settings).



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address:

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

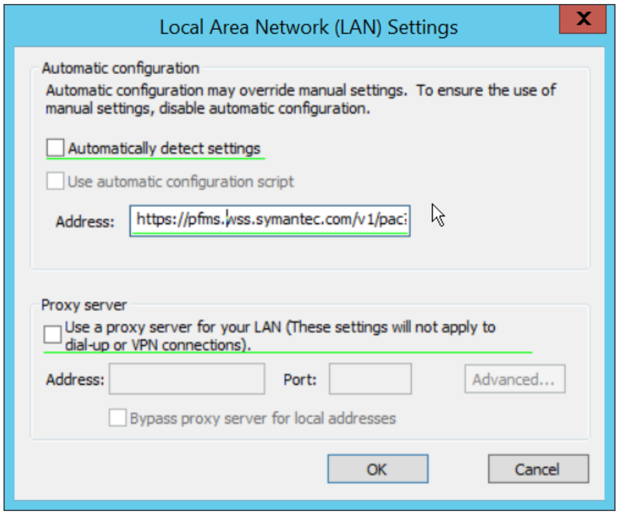
Address: Port:

□ Bypass proxy server for local addresses

17. Select the **Address** field.

18. Press **F6** to enable it (it is enabled if the box has a solid green underline.

19. Enter the PAC file URL from earlier in the **Address** field.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address: https://pfms.wss.symantec.com/v1/pac:

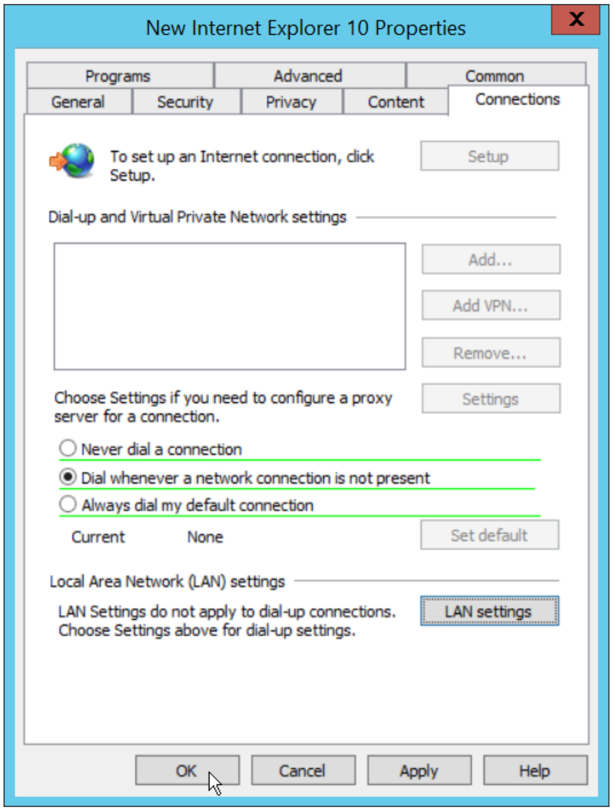
Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

□ Bypass proxy server for local addresses

20. Click **OK**.



New Internet Explorer 10 Properties

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

○ Never dial a connection

● Dial whenever a network connection is not present

○ Always dial my default connection

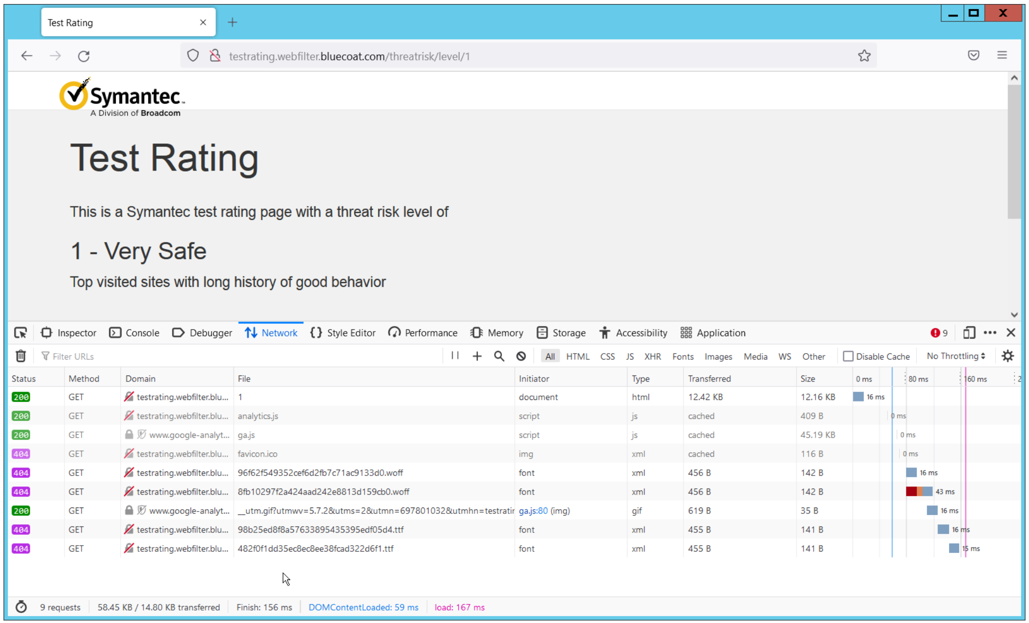
Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

21. Click OK.

22. To verify that traffic is going through Isolation, you can visit the following test website, and substitute 1-10 for the threat level: http://testrating.webfilter.bluecoat.com/threatrisk/level/7.



Test Rating

testrating.webfilter.bluecoat.com/threatrisk/level/1

Symantec.
A Division of Broadcom

Test Rating

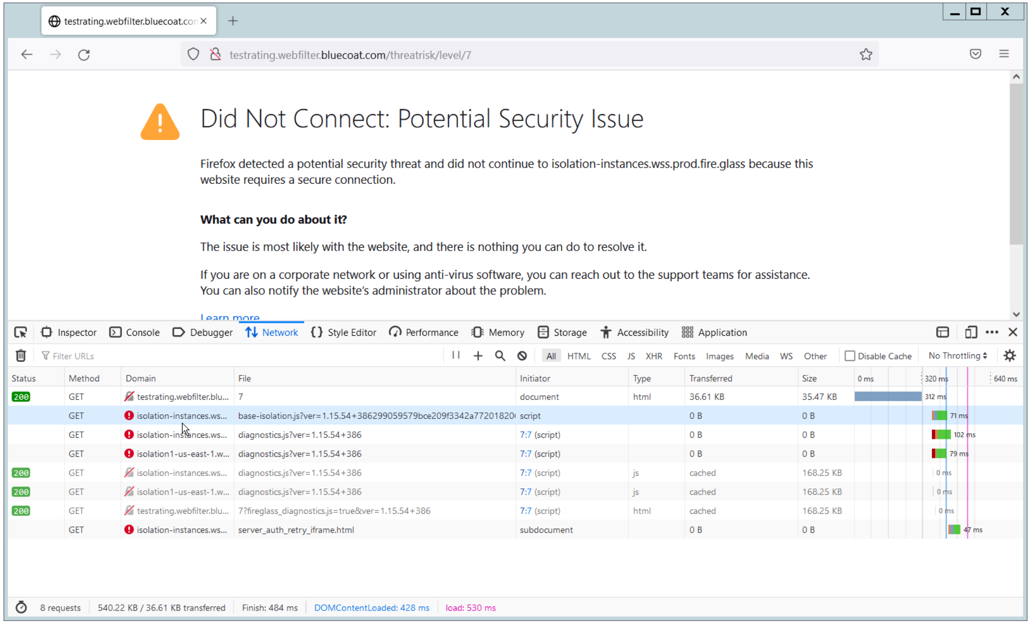
This is a Symantec test rating page with a threat risk level of

1 - Very Safe

Top visited sites with long history of good behavior

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms 80 ms 160 ms
200	GET	testrating.webfilter.blu...	1	document	html	12.42 KB	12.16 KB	16 ms
200	GET	testrating.webfilter.blu...	analytics.js	script	js	cached	409 B	0 ms
200	GET	www.google-analyt...	ga.js	script	js	cached	45.19 KB	0 ms
404	GET	testrating.webfilter.blu...	favicon.ico	img	xml	cached	116 B	0 ms
404	GET	testrating.webfilter.blu...	96f62f549352cef6d2fb7c71ac9133d0.woff	font	xml	456 B	142 B	16 ms
404	GET	testrating.webfilter.blu...	8fb10297f2a424aad242e8813d159cb0.woff	font	xml	456 B	142 B	43 ms
200	GET	www.google-analyt...	__utm.gif?utmwv=5.7.2&utms=2&utmn=697801032&utmhn=testratir	ga.js:80 (img)	gif	619 B	35 B	16 ms
404	GET	testrating.webfilter.blu...	98b25ed8f8a57633895435395edf05d4.ttf	font	xml	455 B	141 B	16 ms
404	GET	testrating.webfilter.blu...	482f0f1dd35ec8ec8ee38fcad322d6f1.ttf	font	xml	455 B	141 B	15 ms

9 requests | 58.45 KB / 14.80 KB transferred | Finish: 156 ms | DOMContentLoaded: 59 ms | load: 167 ms



testrating.webfilter.bluecoat.con

testrating.webfilter.bluecoat.com/threatrisk/level/7

Did Not Connect: Potential Security Issue

Firefox detected a potential security threat and did not continue to isolation-instances.wss.prod.fire.glass because this website requires a secure connection.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms 320 ms 640 ms
200	GET	testrating.webfilter.blu...	7	document	html	36.61 KB	35.47 KB	312 ms
	GET	isolation-instances.ws...	base-isolation.js?ver=1.15.54+386299059579bce209f3342a77201820	script		0 B	0 B	71 ms
	GET	isolation-instances.ws...	diagnostics.js?ver=1.15.54+386	7:7 (script)		0 B	0 B	102 ms
	GET	isolation1-us-east-1.w...	diagnostics.js?ver=1.15.54+386	7:7 (script)		0 B	0 B	79 ms
200	GET	isolation-instances.ws...	diagnostics.js?ver=1.15.54+386	7:7 (script)	js	cached	168.25 KB	0 ms
200	GET	isolation1-us-east-1.w...	diagnostics.js?ver=1.15.54+386	7:7 (script)	js	cached	168.25 KB	0 ms
200	GET	testrating.webfilter.blu...	7?fireglass_diagnostics.js=true&ver=1.15.54+386	7:7 (script)	html	cached	168.25 KB	0 ms
	GET	isolation-instances.ws...	server_auth_retry_iframe.html	subdocument		0 B	0 B	47 ms

8 requests | 540.22 KB / 36.61 KB transferred | Finish: 484 ms | DOMContentLoaded: 428 ms | load: 530 ms

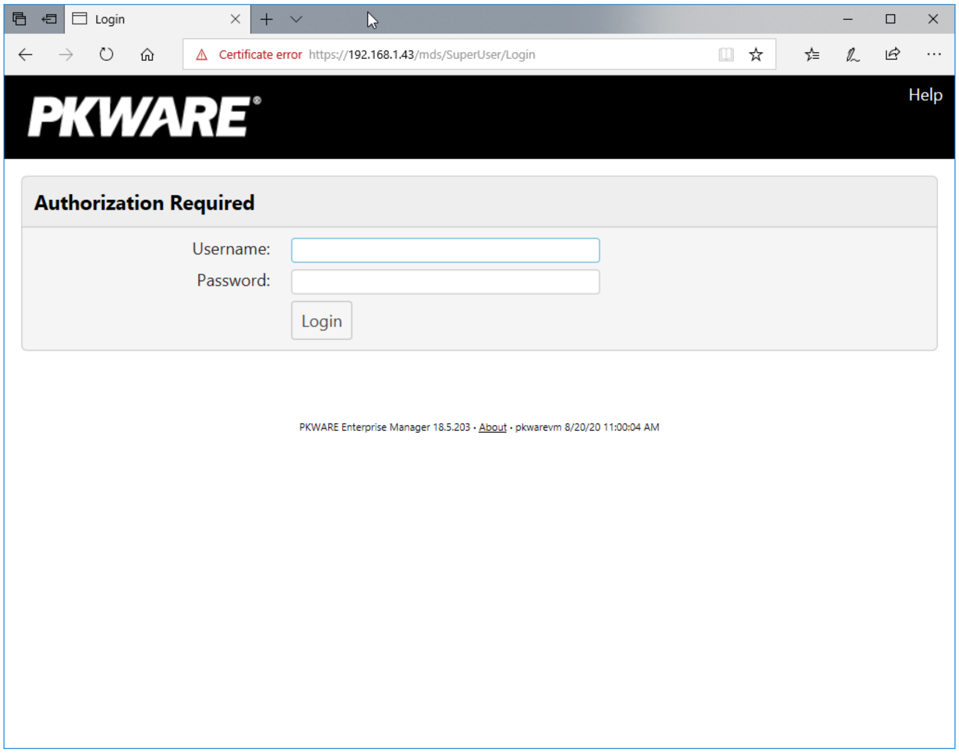
23. On this test URL (tested July 2022), levels 5-7 will go through isolation, and you will be able to see the isolation traffic from the network tab in developer mode (**F12**) on the browser. Levels 8-10 will be blocked by the content filter, and levels 1-4 will not go through isolation or content filtering.

2.3 PKWARE PKProtect

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

2.3.1 Configure PKWARE with Active Directory

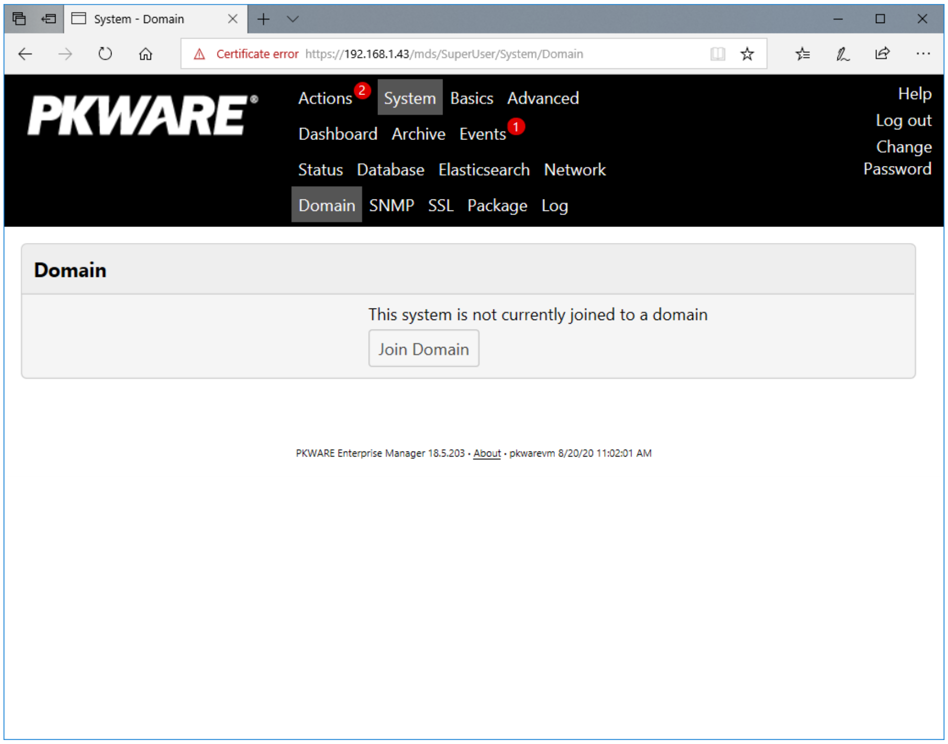
1. Login to the PKWARE web portal using the administrative credentials.



PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 8/20/20 11:00:04 AM

2. Once logged in, you can and should change the password to this administrative account by clicking Change Password in the top right corner.

3. Navigate to System > Domain.



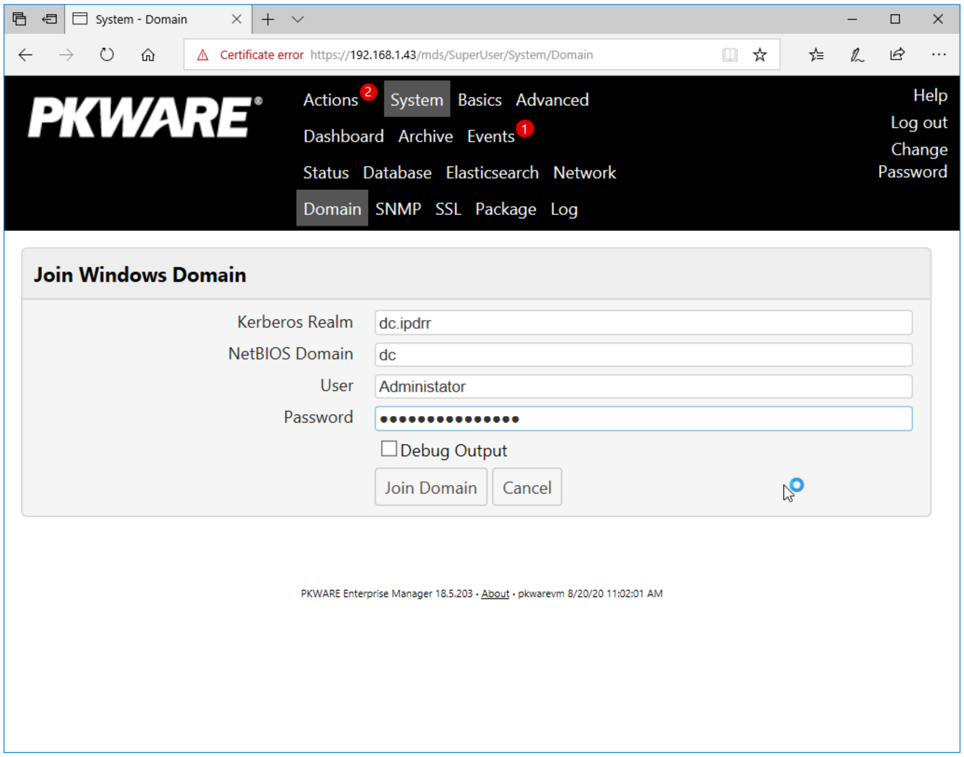
Domain

This system is not currently joined to a domain

PKWARE Enterprise Manager 18.5.203 · About · 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.



Join Windows Domain

Kerberos Realm: dc.ipdrr

NetBIOS Domain: dc

User: Administator

Password: ●●●●●●●●●●●●●●●

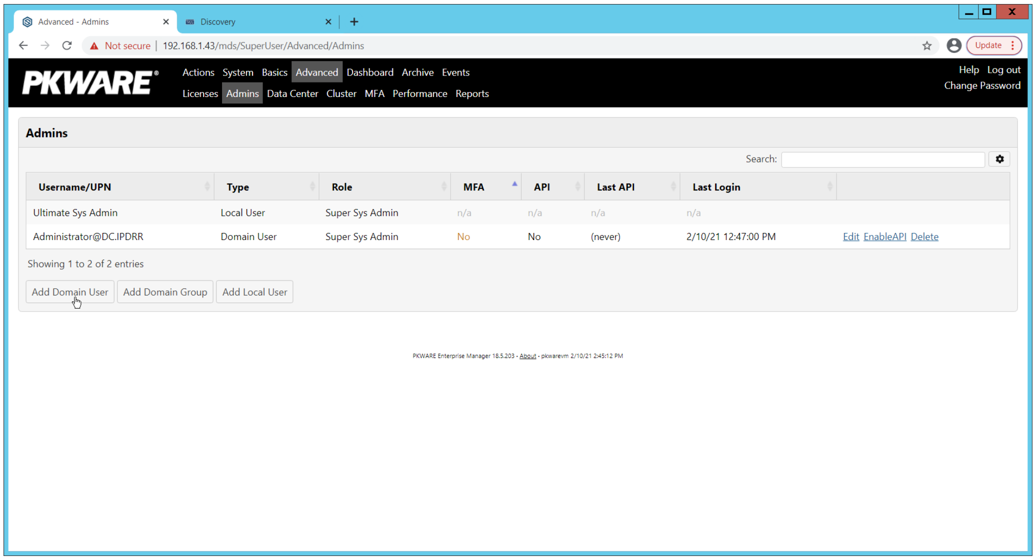
☐ Debug Output

PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 8/20/20 11:02:01 AM

6. Click Join Domain.

2.3.2 Create a New Administrative User

1. Navigate to Advanced > Admins.



Advanced - Admins
Discovery
Not secure | 192.168.1.43/mds/SuperUser/Advanced/Admins
Update
PKWARE
Actions System Basics Advanced Dashboard Archive Events
Licenses Admins Data Center Cluster MFA Performance Reports
Help Log out
Change Password

Admins

Search:

Username/UPN	Type	Role	MFA	API	Last API	Last Login	
Ultimate Sys Admin	Local User	Super Sys Admin	n/a	n/a	n/a	n/a	
Administrator@DC.IPDRR	Domain User	Super Sys Admin	No	No	(never)	2/10/21 12:47:00 PM	Edit EnableAPI Delete

Showing 1 to 2 of 2 entries

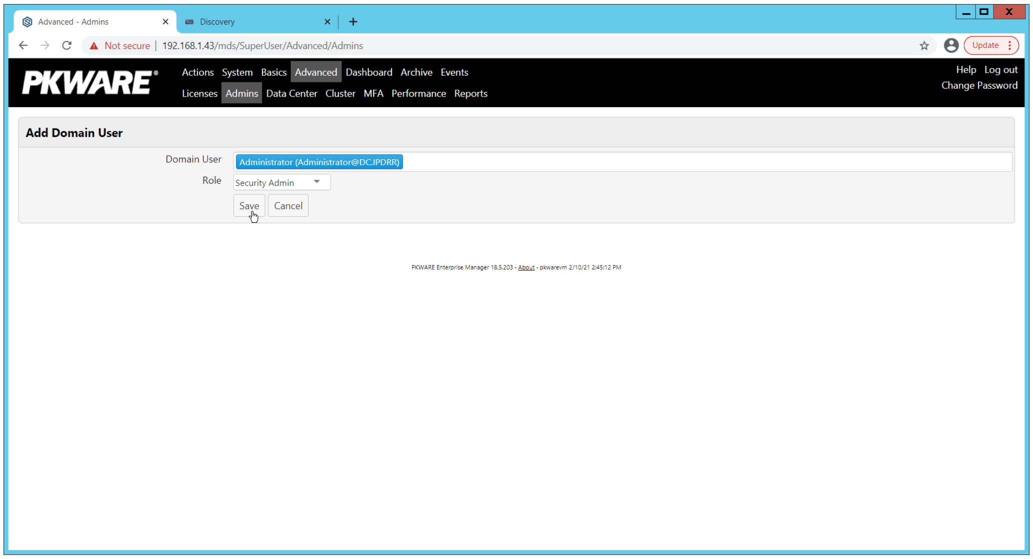
Add Domain User
Add Domain Group
Add Local User

PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 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.



Advanced - Admins
Discovery
Not secure | 192.168.1.43/mds/SuperUser/Advanced/Admins
Update
PKWARE
Actions System Basics Advanced Dashboard Archive Events
Licenses Admins Data Center Cluster MFA Performance Reports
Help Log out
Change Password

Add Domain User

Domain User: Administrator (Administrator@DC.IPDRR)

Role: Security Admin

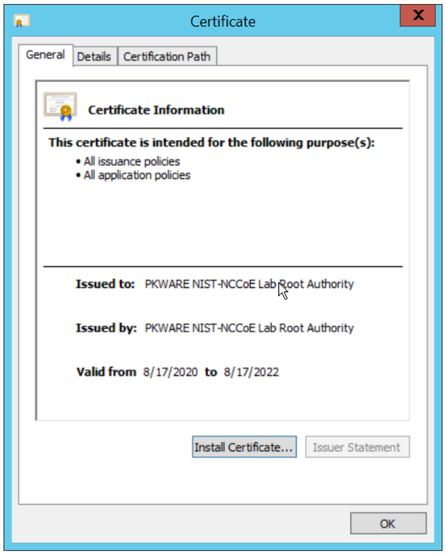
PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 2/10/21 2:45:12 PM

5. Click **Save.**

2.3.3 Install Prerequisites

1. If needed for your environment, you may need to install certificates locally before agents can connect to PKProtect - ask your PKWARE representative if this is necessary for your environment.

2. Double click the certificate you wish to install.



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

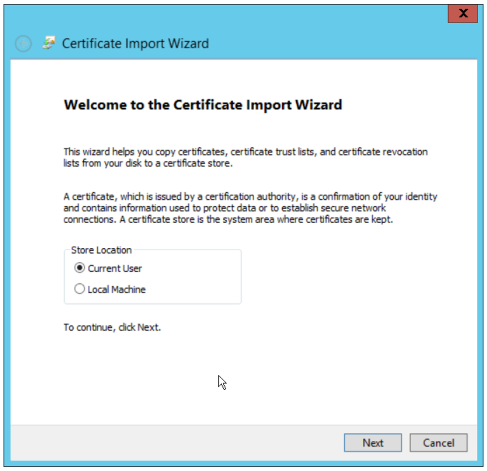
Issued to: PKWARE NIST-NCCoE Lab Root Authority

Issued by: PKWARE NIST-NCCoE Lab Root Authority

Valid from 8/17/2020 **to** 8/17/2022

3. Click Install Certificate…

4. Select Current User.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

● Current User

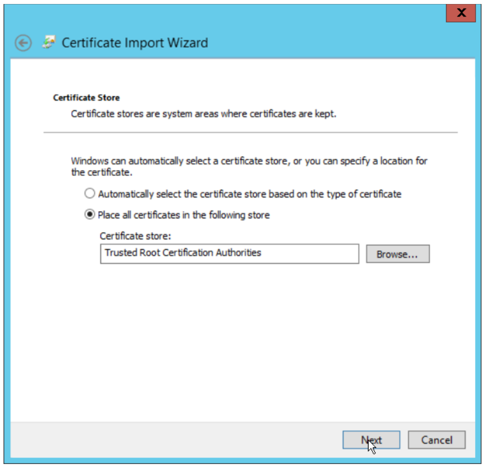
○ Local Machine

To continue, click Next.

5. Click **Next.**

6. Click **Browse.**

7. Select **Trusted Root Certification Authorities.**



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

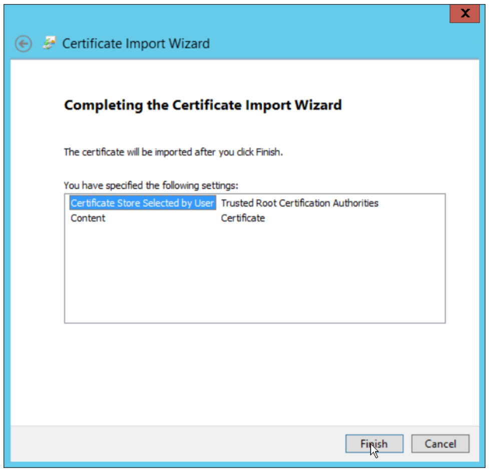
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

8. Click **Next.**



Certificate Import Wizard

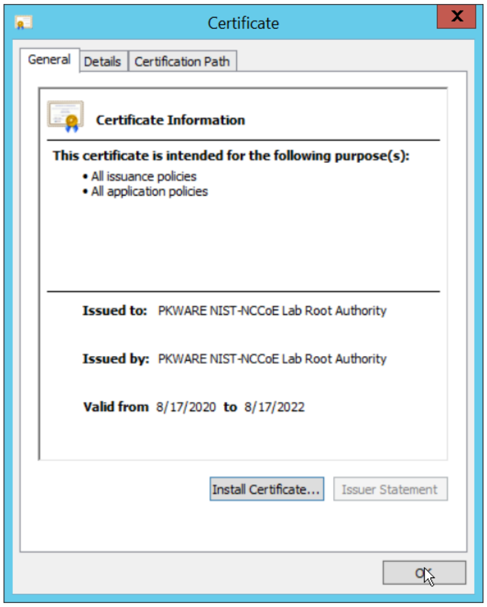
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

9. Click Finish.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: PKWARE NIST-NCCoE Lab Root Authority

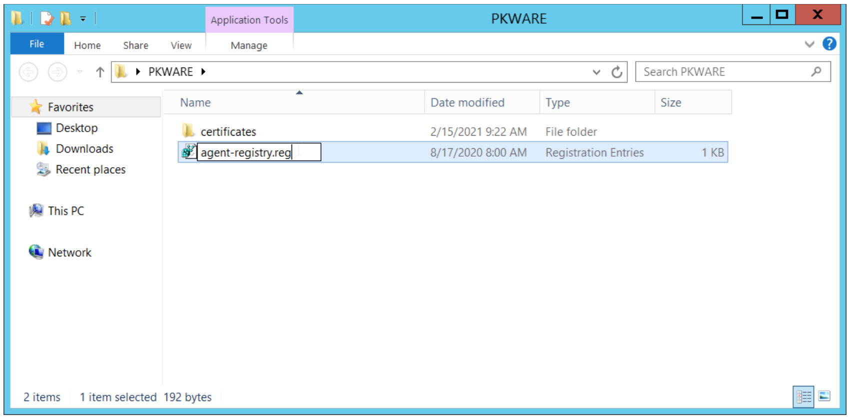
Issued by: PKWARE NIST-NCCoE Lab Root Authority

Valid from 8/17/2020 **to** 8/17/2022

10. Click **OK.**

11. Repeat steps 1 through 10 but select **Personal** instead of **Trusted Root Certification Authorities.**

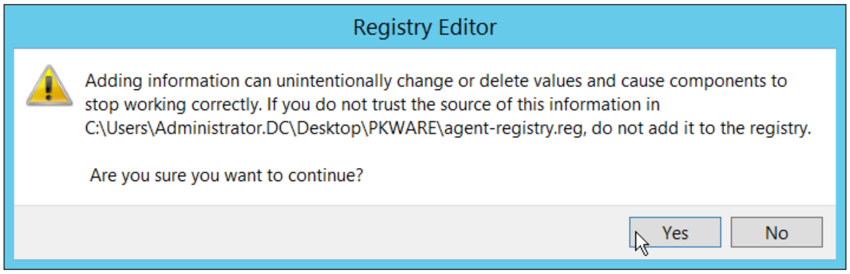
12. Repeat steps 1 through 11 for each certificate that needs to be installed.



Name	Date modified	Type	Size
certificates	2/15/2021 9:22 AM	File folder	
agent-registry.reg	8/17/2020 8:00 AM	Registration Entries	1 KB

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

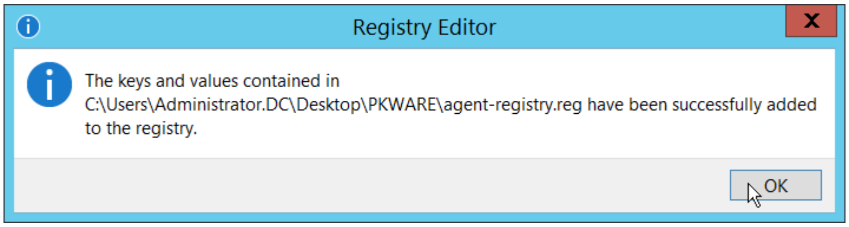
14. Double click the file (must have administrator privileges).


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?

15. Click **Yes.**


Registry Editor

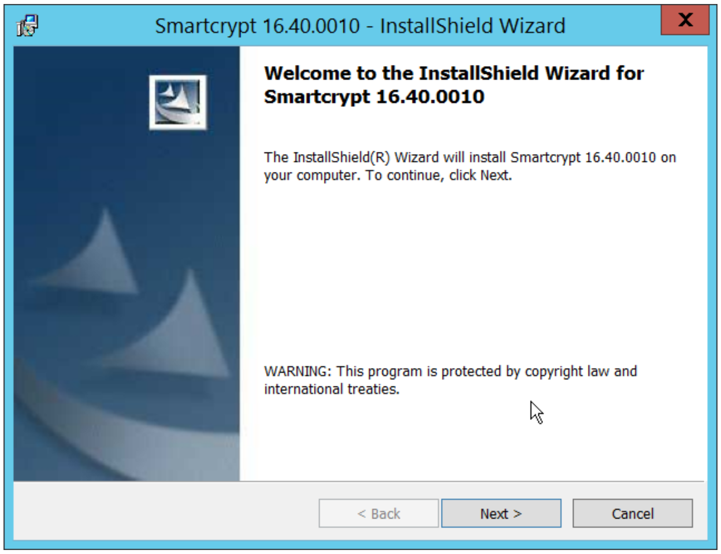
The keys and values contained in C:\Users\Administrator.DC\Desktop\PKWARE\agent-registry.reg have been successfully added to the registry.

16. Click OK.

17. Restart the machine to apply these changes.

2.3.4 Install the PKProtect Agent

1. Run the PKProtect Installation executable.



Smartcrypt 16.40.0010 - InstallShield Wizard

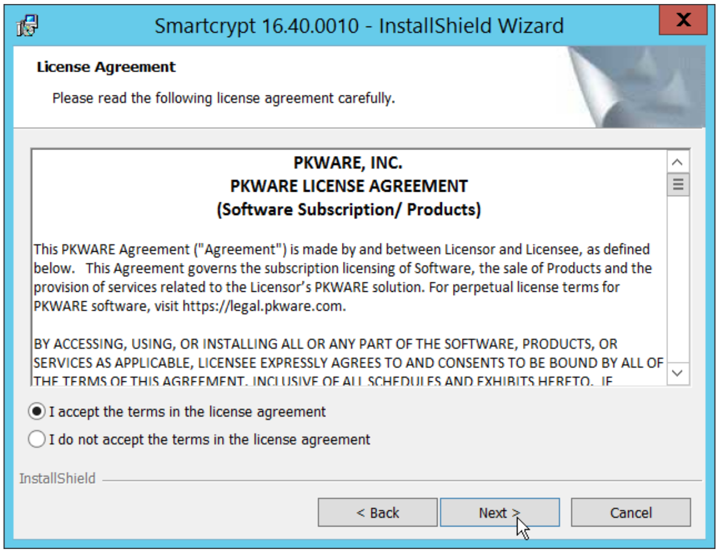
Welcome to the InstallShield Wizard for Smartcrypt 16.40.0010

The InstallShield(R) Wizard will install Smartcrypt 16.40.0010 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

2. Click Next.

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



Smartcrypt 16.40.0010 - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

PKWARE, INC.
PKWARE LICENSE AGREEMENT
(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.

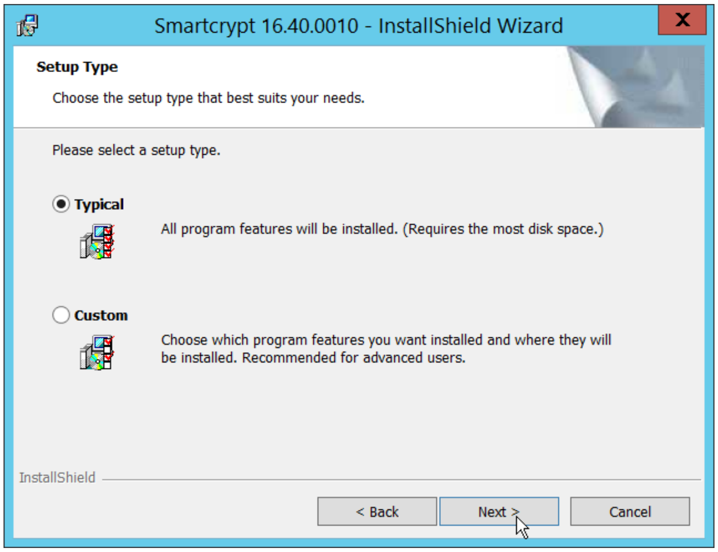
BY ACCESSING, USING, OR INSTALLING ALL OR ANY PART OF THE SOFTWARE, PRODUCTS, OR SERVICES AS APPLICABLE, LICENSEE EXPRESSLY AGREES TO AND CONSENTS TO BE BOUND BY ALL OF THE TERMS OF THIS AGREEMENT, INCLUSIVE OF ALL SCHEDULES AND EXHIBITS HERETO. IF

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

4. Click Next.

5. Select Typical.


Smartcrypt 16.40.0010 - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

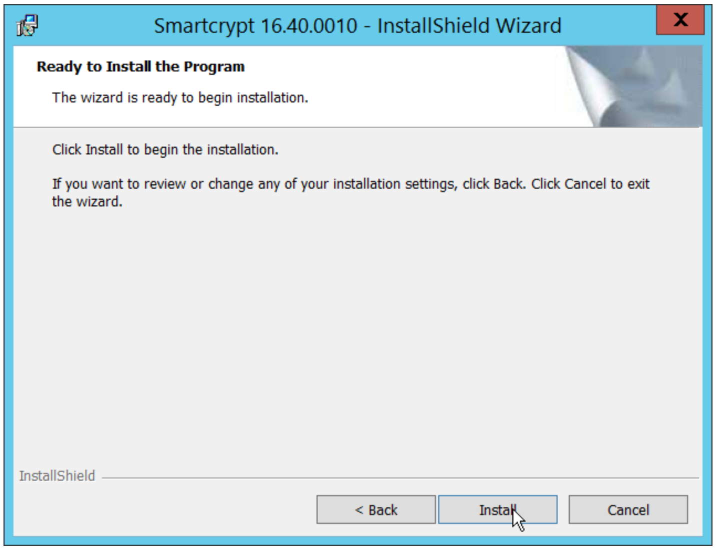
● **Typical**

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.

6. Click **Next.**


Smartcrypt 16.40.0010 - InstallShield Wizard

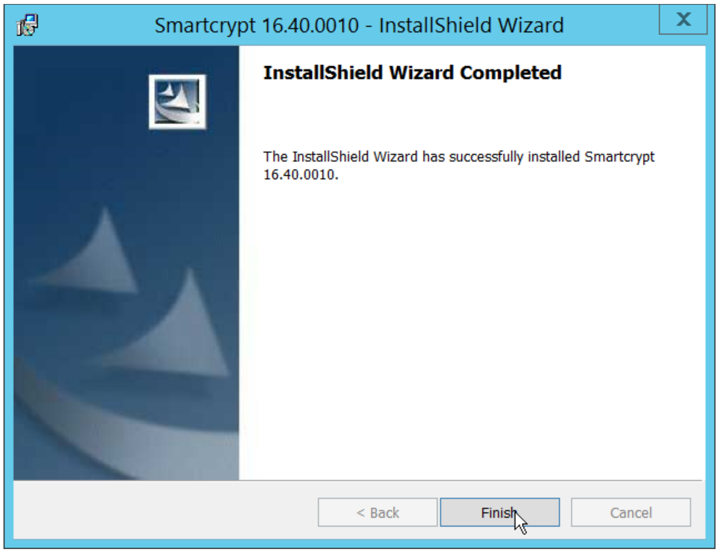
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

7. Click Install.

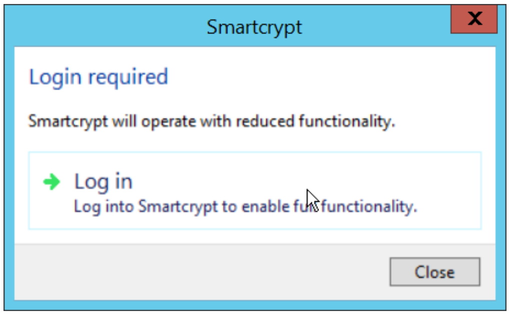


Smartcrypt 16.40.0010 - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Smartcrypt 16.40.0010.

8. Click Finish.



Smartcrypt

Login required

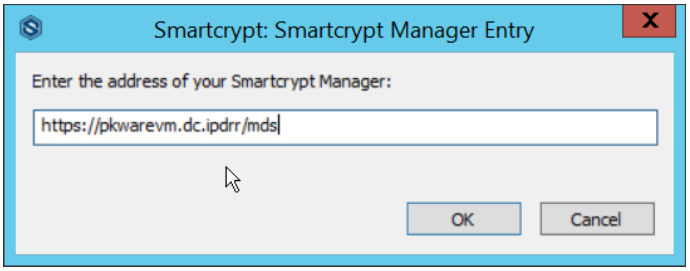
Smartcrypt will operate with reduced functionality.

Log in

Log into Smartcrypt to enable full functionality.

9. If a window to login is not automatically shown, you can right click the PKProtect icon in the Windows taskbar and click Login…. 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).



Smartcrypt: Smartcrypt Manager Entry

Enter the address of your Smartcrypt Manager:

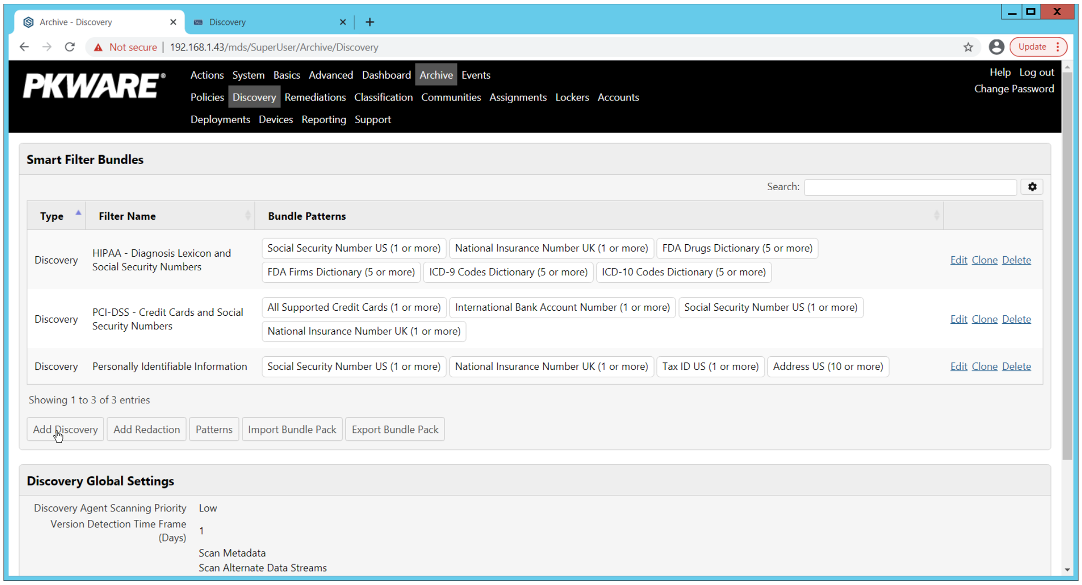
https://pkwarevm.dc.ipdrr/mds

11. Enter the address of the PKWARE server.

12. The PKWARE agent will now run in the background.

2.3.5 Configure Discovery and Reporting

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


Archive - Discovery
Discovery
Not secure | 192.168.1.43/mds/SuperUser/Archive/Discovery
Update
PKWARE
Actions System Basics Advanced Dashboard Archive Events
Policies Discovery Remediations Classification Communities Assignments Lockers Accounts
Deployments Devices Reporting Support
Help Log out
Change Password

Smart Filter Bundles

Search:

Type	Filter Name	Bundle Patterns	
Discovery	HIPAA - Diagnosis Lexicon and Social Security Numbers	Social Security Number US (1 or more) National Insurance Number UK (1 or more) FDA Drugs Dictionary (5 or more) FDA Firms Dictionary (5 or more) ICD-9 Codes Dictionary (5 or more) ICD-10 Codes Dictionary (5 or more)	Edit Clone Delete
Discovery	PCI-DSS - Credit Cards and Social Security Numbers	All Supported Credit Cards (1 or more) International Bank Account Number (1 or more) Social Security Number US (1 or more) National Insurance Number UK (1 or more)	Edit Clone Delete
Discovery	Personally Identifiable Information	Social Security Number US (1 or more) National Insurance Number UK (1 or more) Tax ID US (1 or more) Address US (10 or more)	Edit Clone Delete

Showing 1 to 3 of 3 entries

Discovery Global Settings

Discovery Agent Scanning Priority: Low

Version Detection Time Frame (Days): 1

Scan Metadata

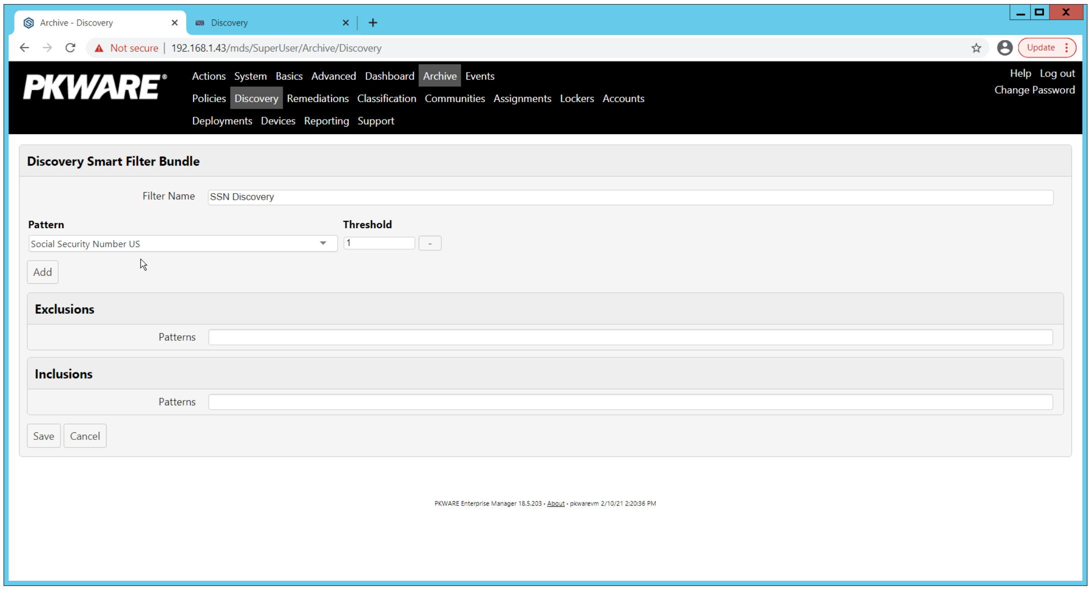
Scan Alternate Data Streams

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.


Archive - Discovery
Discovery
Not secure | 192.168.1.43/mds/SuperUser/Archive/Discovery
Update
PKWARE
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	1

Exclusions

Patterns

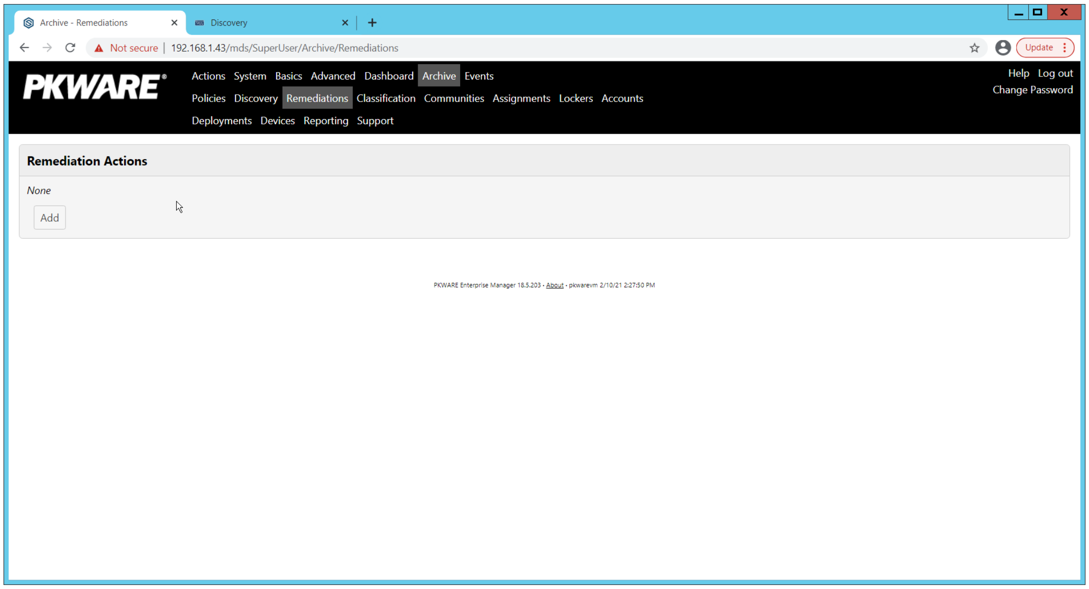
Inclusions

Patterns

PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 2/10/21 2:20:36 PM

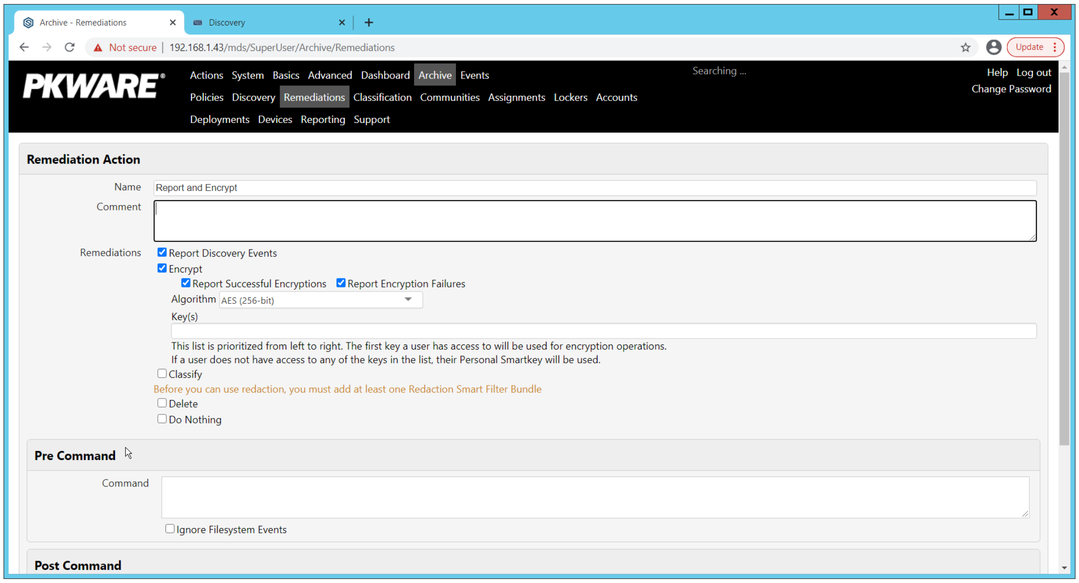
6. Click Save.

7. Navigate to **Archive > Remediations.**


Archive - Remediations
Discovery
Not secure | 192.168.1.43/mds/SuperUser/Archive/Remediations
Update
PKWARE
Actions System Basics Advanced Dashboard Archive Events
Policies Discovery Remediations Classification Communities Assignments Lockers Accounts
Deployments Devices Reporting Support
Help Log out
Change Password
Remediation Actions
None
Add
PKWARE Enterprise Manager 18.5.203 - About - pkwarevm 2/10/21 2:27:50 PM

8. Click Add.

9. Enter a name for the remediation.


Archive - Remediations
Discovery
Not secure | 192.168.1.43/mds/SuperUser/Archive/Remediations
Update
PKWARE
Actions System Basics Advanced Dashboard Archive Events
Policies Discovery Remediations Classification Communities Assignments Lockers Accounts
Deployments Devices Reporting Support
Searching ...
Help Log out
Change Password

Remediation Action

Name: Report and Encrypt

Comment:

Remediations:
☑ Report Discovery Events
☑ Encrypt
☑ 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 Smartkey 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

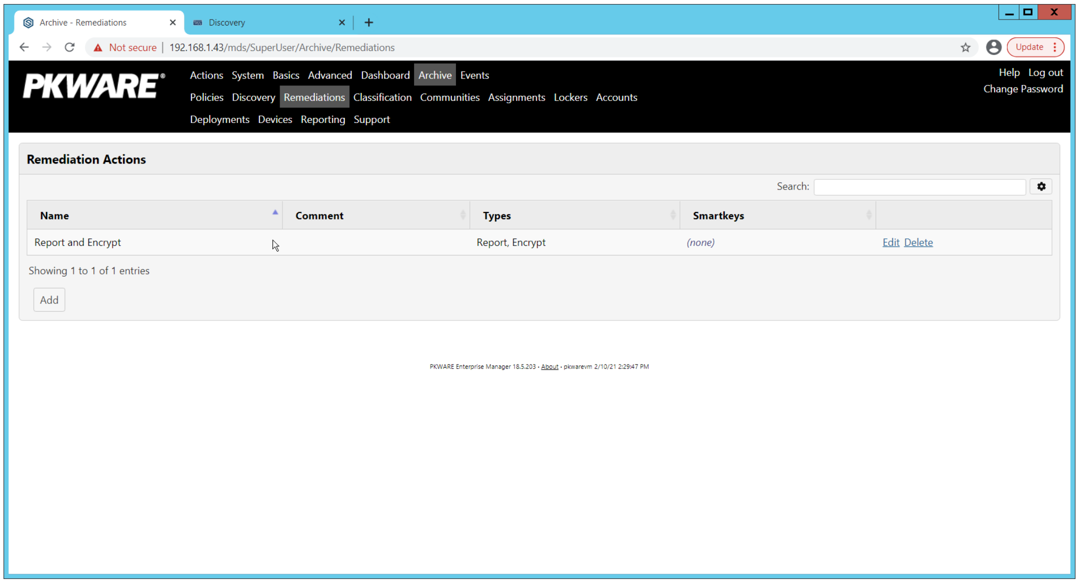
Post Command

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
Not secure | 192.168.1.43/mds/SuperUser/Archive/Remediations
Update
PKWARE
Actions System Basics Advanced Dashboard Archive Events
Policies Discovery Remediations Classification Communities Assignments Lockers Accounts
Deployments Devices Reporting Support
Help Log out
Change Password

Remediation Actions

Search:

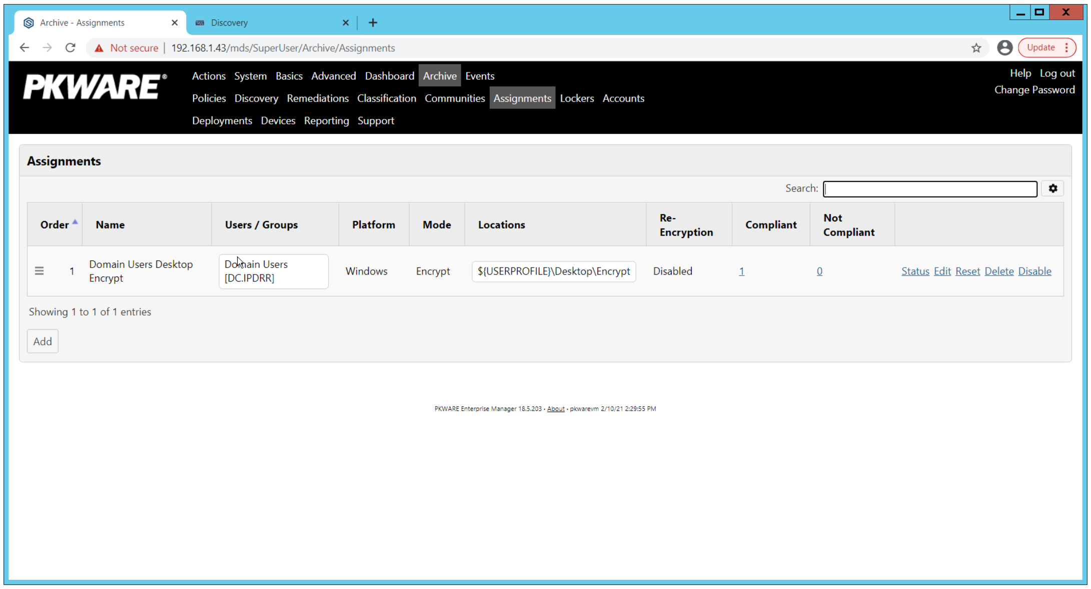
Name	Comment	Types	Smartkeys	
Report and Encrypt		Report, Encrypt	*(none)*	Edit Delete

Showing 1 to 1 of 1 entries

Add

PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 2/10/21 2:29:47 PM

14. Navigate to Archive > Assignments.


Archive - Assignments
Discovery
Not secure | 192.168.1.43/mds/SuperUser/Archive/Assignments
Update
PKWARE
Actions System Basics Advanced Dashboard Archive Events
Policies Discovery Remediations Classification Communities Assignments Lockers Accounts
Deployments Devices Reporting Support
Help Log out
Change Password

Assignments

Search:

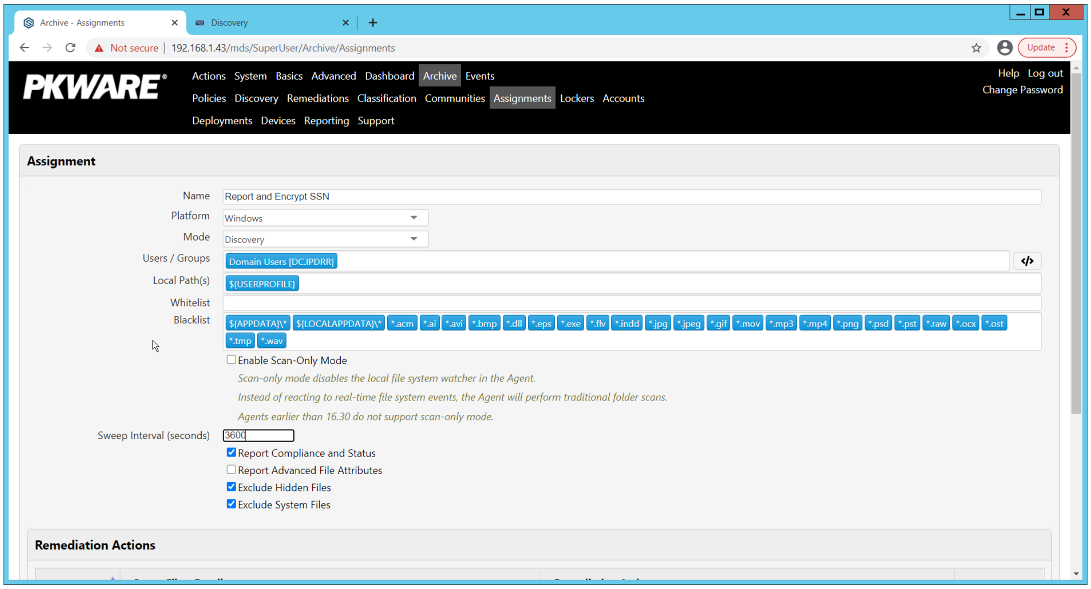
	Order	Name	Users / Groups	Platform	Mode	Locations	Re-Encryption	Compliant	Not Compliant	
≡	1	Domain Users Desktop Encrypt	Domain Users [DC.IPDRR]	Windows	Encrypt	$(USERPROFILE)\Desktop\Encrypt	Disabled	1	0	Status Edit Reset Delete Disable

Showing 1 to 1 of 1 entries

Add

PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 2/10/21 2:29:55 PM

15. Click **Add.**


Archive - Assignments
Discovery
Not secure | 192.168.1.43/mds/SuperUser/Archive/Assignments
Update
PKWARE
Actions System Basics Advanced Dashboard Archive Events
Policies Discovery Remediations Classification Communities Assignments Lockers Accounts
Deployments Devices Reporting Support
Help Log out
Change Password

Assignment

Name: Report and Encrypt SSN

Platform: Windows

Mode: Discovery

Users / Groups: Domain Users [DC.IPDRR]

Local Path(s): ${USERPROFILE}

Whitelist:

Blacklist: ${APPDATA}* ${LOCALAPPDATA}* *.acm *.ai *.avi *.bmp *.dll *.eps *.exe *.flv *.indd *.jpg *.jpeg *.gif *.mov *.mp3 *.mp4 *.png *.psd *.pst *.raw *.ocx *.ost *.tmp *.wav

☐ Enable Scan-Only Mode

Scan-only mode disables the local file system watcher in the Agent.

Instead of reacting to real-time file system events, the Agent will perform traditional folder scans.

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

☑ Exclude System Files

Remediation Actions

16. Enter a name for the Assignment.

17. Select the Platform for this assignment to run on.

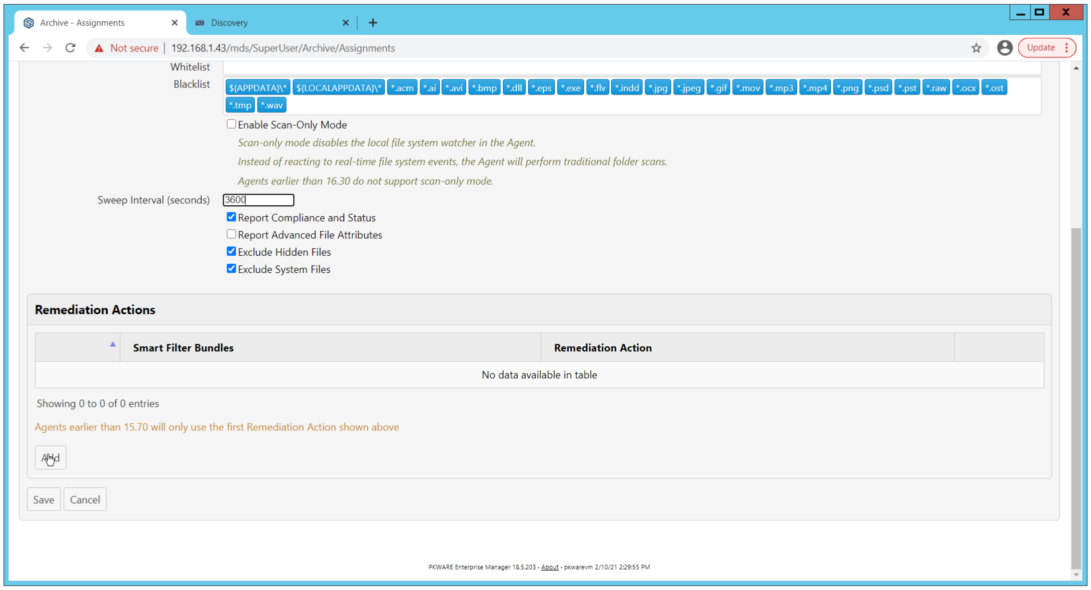
18. Select Discovery for the Mode.

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.



Whitelist:

Blacklist: ${APPDATA}* ${LOCALAPPDATA}* *.acm *.ai *.avi *.bmp *.dll *.eps *.exe *.flv *.indd *.jpg *.jpeg *.gif *.mov *.mp3 *.mp4 *.png *.psd *.pst *.raw *.ocx *.ost *.tmp *.wav

☐ Enable Scan-Only Mode

Scan-only mode disables the local file system watcher in the Agent.

Instead of reacting to real-time file system events, the Agent will perform traditional folder scans.

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

☑ Exclude System Files

Remediation Actions

	Smart Filter Bundles	Remediation Action	
	No data available in table		

Showing 0 to 0 of 0 entries

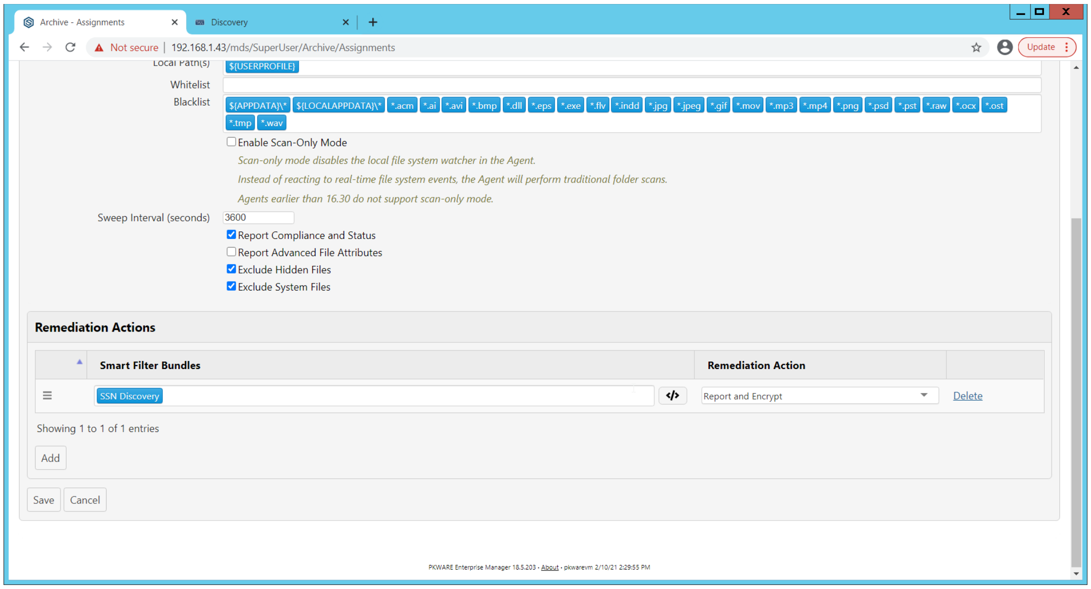
Agents earlier than 15.70 will only use the first Remediation Action shown above

Add
Save
Cancel
PKWARE Enterprise Manager 18.5.203 - About - pkwarevm 2/10/21 2:29:55 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.



Local Path(s): ${USERPROFILE}

Whitelist:

Blacklist: ${APPDATA}* ${LOCALAPPDATA}* *.acm *.ai *.avi *.bmp *.dll *.eps *.exe *.flv *.indd *.jpg *.jpeg *.gif *.mov *.mp3 *.mp4 *.png *.psd *.pst *.raw *.ocx *.ost *.tmp *.wav

☐ Enable Scan-Only Mode

Scan-only mode disables the local file system watcher in the Agent.

Instead of reacting to real-time file system events, the Agent will perform traditional folder scans.

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
☑ Exclude System Files

Remediation Actions

	Smart Filter Bundles	Remediation Action	
≡	SSN Discovery	Report and Encrypt	Delete

Showing 1 to 1 of 1 entries

Add
Save
Cancel
PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 2/10/21 2:29:55 PM

26. Click **Save.**

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

2.4 StrongKey Tellaro

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

2.4.1 Python Client for StrongKey – Windows Executable Creation and Use

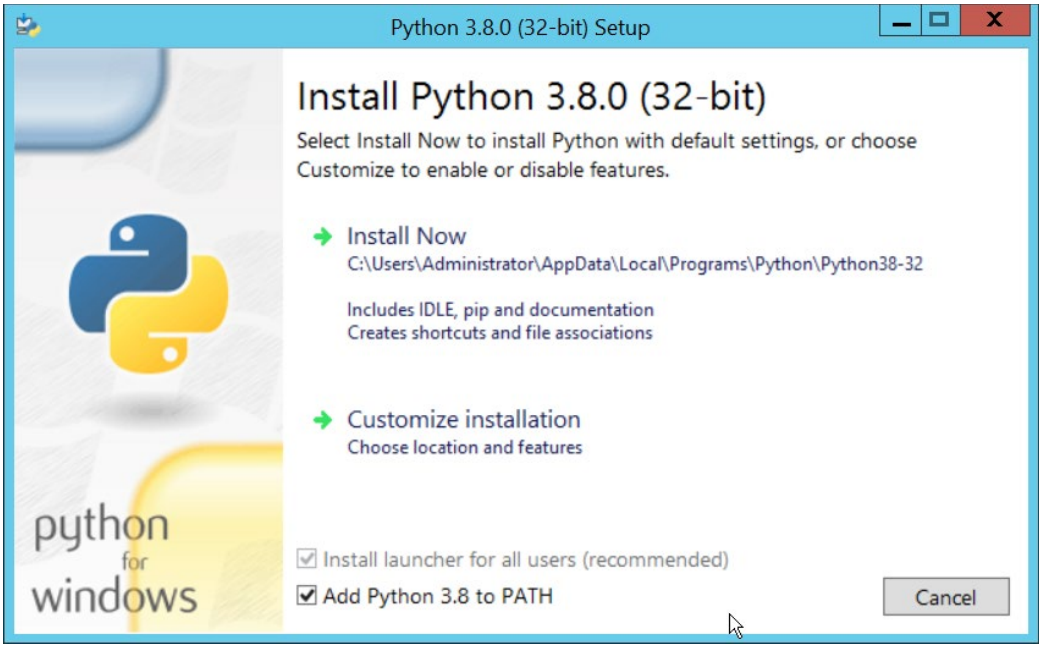
1. Ensure that the following script (see end of section) is filled out with information specific to your enterprise, including the variables skdid, skuser, and skpass.

2. Save the file as strongkey-client.py.

3. This example will demonstrate how to create an executable from the script below. Download Python 3.8.0 from the Python website: https://www.python.org/downloads/release/python-380/. Specifically, download the Windows x86 executable installer. The 32-bit version will provide better access to Active Directory packages and interfaces.

4. Run the installer.

5. Check the box next to **Add Python 3.8 to PATH.**



Python 3.8.0 (32-bit) Setup

Install Python 3.8.0 (32-bit)

Select Install Now to install Python with default settings, or choose Customize to enable or disable features.

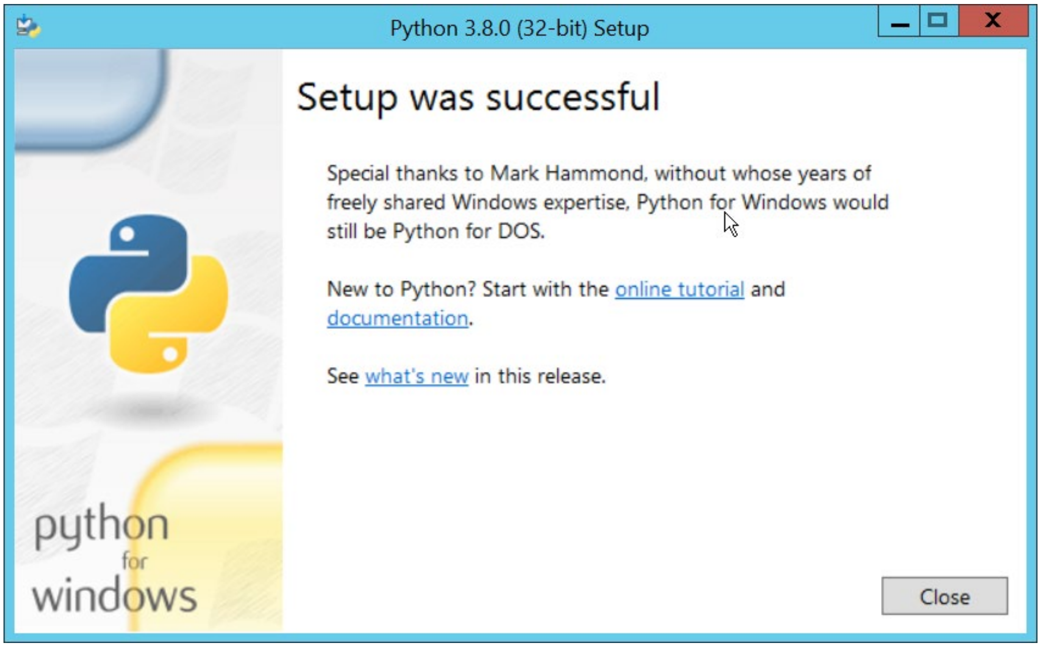
Install Now
C:\Users\Administrator\AppData\Local\Programs\Python\Python38-32

Includes IDLE, pip and documentation
Creates shortcuts and file associations

Customize installation
Choose location and features

☑ Install launcher for all users (recommended)
☑ Add Python 3.8 to PATH

6. Click Install Now.



Python 3.8.0 (32-bit) Setup

Setup was successful

Special thanks to Mark Hammond, without whose years of freely shared Windows expertise, Python for Windows would still be Python for DOS.

New to Python? Start with the online tutorial and documentation.

See what's new in this release.

7. Click Close.
8. Open a PowerShell window.
9. Run the following command to install pyinstaller.

```
> pip install pyinstaller
```

10. Run the following command to install requests.

```
> pip install requests
```

11. From the PowerShell window, navigate to where you saved strongkey-client.py.
12. Run the following command to build the client into an executable.

    ```
    > pyinstaller --onefile .\strongkey-client.py
    ```

13. A folder called **dist** will be created. In this folder will be an executable named strongkey-client.exe.
14. To encrypt a file in place (i.e., overwrite the file with encrypted contents), run the following command:

    ```
    > ./strongkey-client.exe  -encrypt -overwrite --infile sensitive.txt
    ```

15. To encrypt a file and save it to a new location, run the following command:

    ```
    > ./strongkey-client.exe -encrypt --outfile encrypted.txt --infile sensitive.txt
    ```

16. To decrypt a file in place (i.e., overwrite the encrypted file with plaintext contents), run the following command:

    ```
    > ./strongkey-client.exe -decrypt -overwrite --infile sensitive.txt
    ```

17. To decrypt a file and save it to a new location, run the following command:

    ```
    > ./strongkey-client.exe -decrypt --outfile decrypted.txt --infile encrypted.txt
    ```

18. This client can be configured to run on a schedule, or be iterated over a directory of files, depending on the needs of the organization. Because the client is Python and StrongKey is REST API based, the script is adaptable to various architectures and can be deployed widely across the enterprises, to fill in gaps that the enterprise may have in its data protection capabilities.

```
import requests
import json
import argparse

skdid = # Note: Users should reference a separate file for this ID
skuser = # Note: Users should reference a separate file for the username
skpass = # Note: Users should reference a separate file for the password
encurl = "https://demo4.strongkey.com/skee/rest/encrypt"
decurl = "https://demo4.strongkey.com/skee/rest/decrypt"

def buildrequest(fname, encrypt):
   req = {}
   req["svcinfo"] = {
      "did": skdid,
      "svcusername":skuser,
      "svcpassword":skpass
   }

   if (encrypt):
      req["encinfo"] = {
         "algorithm": "AES",
         "keysize":256,
         "uniquekey":True
      }
```

```
    req["fileinfo"] = {
       "filename": name
    }

    req["authzinfo"] = {
       "username": "encryptdecrypt",
       #"userdn": "cn=encryptdecrypt,did="+skdid+",ou=users,ou=v2,ou=SKCE,ou=Stron-
gAuth,ou=Applications,dc=strongauth,dc=com",
       "authgroups": "cn=EncryptionAuthor-
ized,did="+skdid+",ou=groups,ou=v2,ou=SKCE,ou=StrongAuth,ou=Applications,dc=stron-
gauth,dc=com",
       "requiredauthorization": 0
    }

    req["svcinfo"] = json.dumps(req["svcinfo"])
    req["fileinfo"] = json.dumps(req["fileinfo"])
    if (encrypt):
       req["encinfo"] = json.dumps(req["encinfo"])
    req["authzinfo"] = json.dumps(req["authzinfo"])

    return req

 def encrypt(filename,output,overwrite):
    req = buildrequest(filename, True)
    with open(filename, mode='rb') as f:
       files = [('filedata', f)]
       p = requests.request("POST", encurl, headers={}, data=req, files=files)
    print(p)
    p.raise_for_status()
    if (p.status_code == 200):
       output = filename if overwrite else output
       with open(output, mode='wb') as o:
          o.write(p.content)

 def decrypt(filename,out,overwrite):
    req = buildrequest(filename, False)
    with open(filename, mode='rb') as f:
       files = [('filedata', f)]
       p = requests.request("POST", decurl, headers={}, data=req, files=files)
    p.raise_for_status()
    if (p.status_code == 200):
       output = filename if overwrite else out
       with open(output, mode='wb') as o:
          o.write(p.content)


 parser = argparse.ArgumentParser(description='Encrypt or decrypt a file using
Strongkey.')

 group = parser.add_mutually_exclusive_group(required=True)
 group.add_argument("-encrypt", action='store_true')
 group.add_argument("-decrypt", action='store_true')

 group = parser.add_mutually_exclusive_group(required=True)
 group.add_argument("-overwrite", action='store_true')
 group.add_argument("--outfile", type=str)

 parser.add_argument("--infile", type=str, required=True)

 a = parser.parse_args()

 if (a.overwrite is True):
    overwrite = True
    out = ""
elif (a.outfile is not None):
    out = a.outfile
    overwrite = False

if (a.encrypt is True):
    encrypt(a.infile, out, overwrite)
elif (a.decrypt is True):
   decrypt(a.infile, out, overwrite)
```

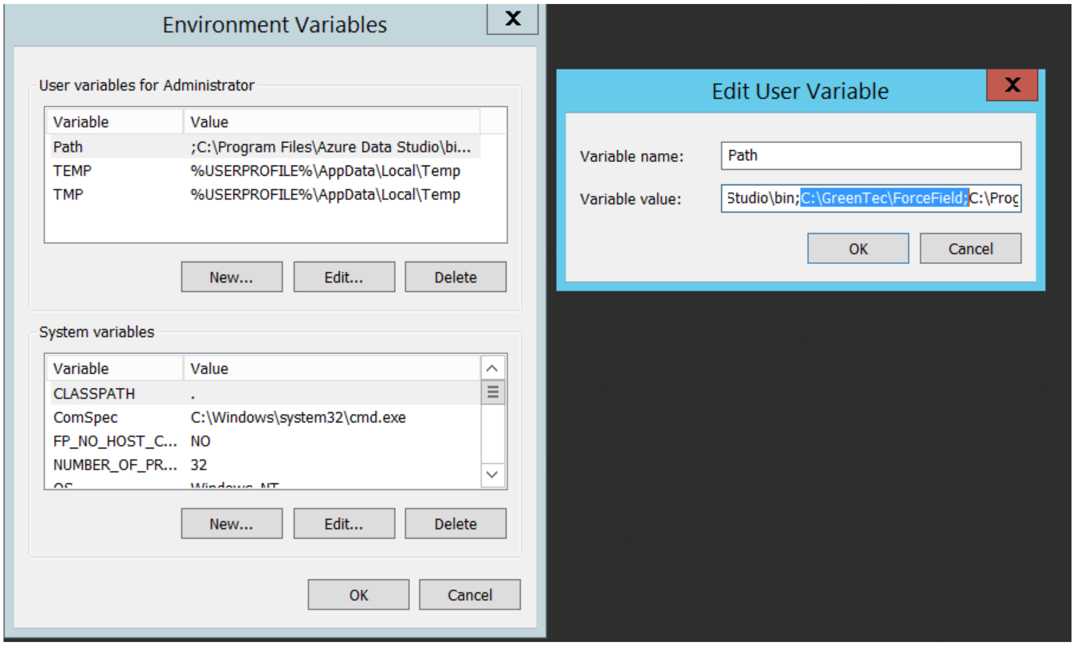
2.5 Qcor ForceField

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

2.5.1 Installation and Usage of ForceField

1. Either a Compact Disk (CD) or zip file will be provided by Qcor containing the WFS API and associate utilities. Copy the contents of *GreenTec*\Release onto the C: drive of the Qcor ForceField server.

2. Add the destination folder to the command line PATH variable if necessary. To do this, from the start menu search for **Environment Variables**.



Environment Variables

User variables for Administrator

Variable	Value
Path	;C:\Program Files\Azure Data Studio\bi...
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

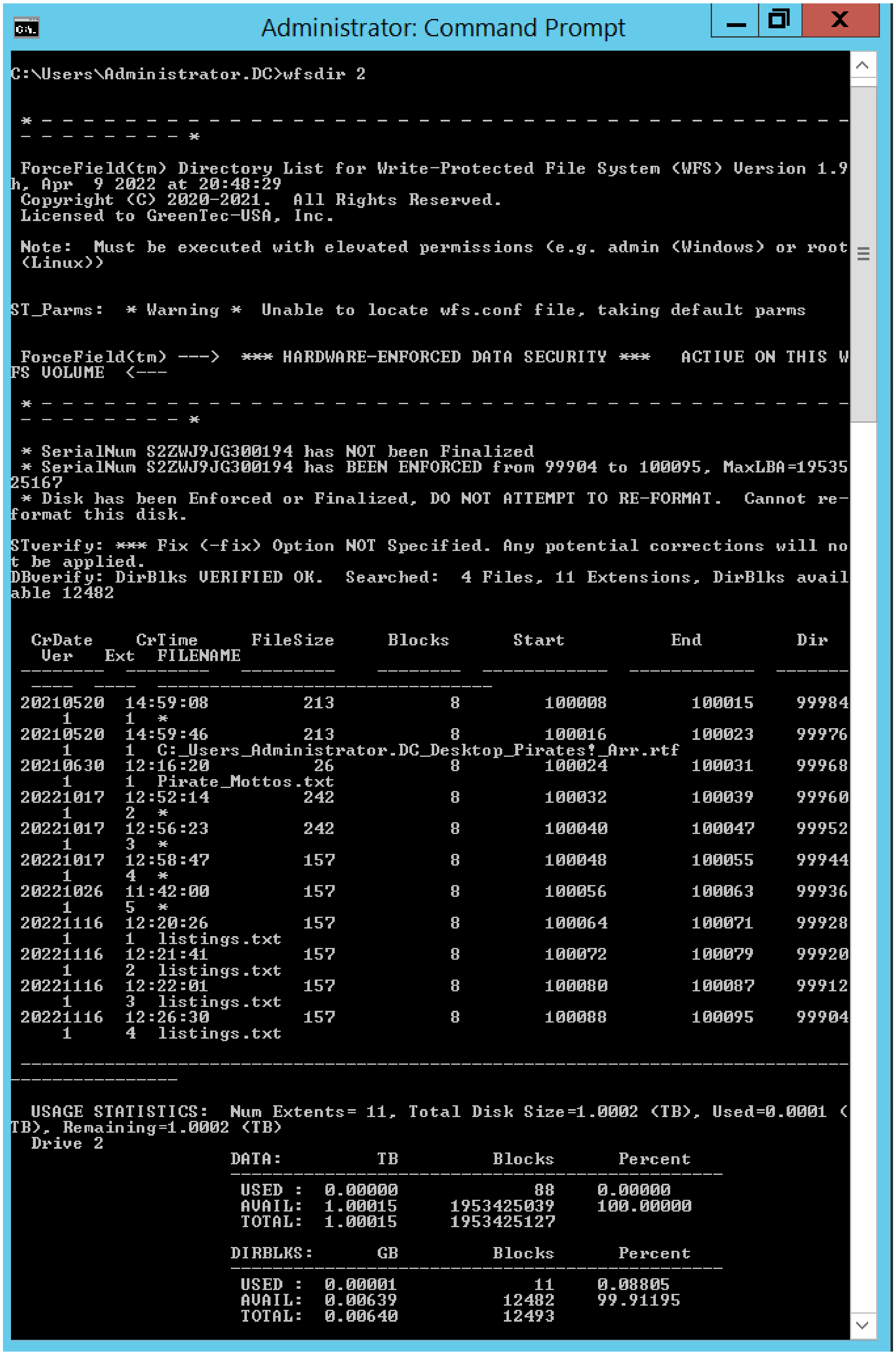
Variable	Value
CLASSPATH	.
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_C...	NO
NUMBER_OF_PR...	32

Edit User Variable

Variable name: Path

Variable value: Studio\bin;C:\GreenTec\ForceField;C:\Proc

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



```
C:\Users\Administrator.DC>wfsdir 2


 * - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
 - - - - - - - - - *

 ForceField(tm) Directory List for Write-Protected File System (WFS) Version 1.9
h, Apr  9 2022 at 20:48:29
 Copyright (C) 2020-2021.  All Rights Reserved.
 Licensed to GreenTec-USA, Inc.

 Note:  Must be executed with elevated permissions (e.g. admin (Windows) or root
 (Linux))


ST_Parms:  * Warning *  Unable to locate wfs.conf file, taking default parms


 ForceField(tm) --->  *** HARDWARE-ENFORCED DATA SECURITY ***   ACTIVE ON THIS W
FS VOLUME  <---

 * - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
 - - - - - - - - - *

 * SerialNum S2ZWJ9JG300194 has NOT been Finalized
 * SerialNum S2ZWJ9JG300194 has BEEN ENFORCED from 99904 to 100095, MaxLBA=19535
25167
 * Disk has been Enforced or Finalized, DO NOT ATTEMPT TO RE-FORMAT.  Cannot re-
format this disk.

STverify: *** Fix (-fix) Option NOT Specified. Any potential corrections will no
t be applied.
DBverify: DirBlks VERIFIED OK.  Searched:  4 Files, 11 Extensions, DirBlks avail
able 12482


  CrDate     CrTime      FileSize      Blocks       Start          End          Dir
   Ver    Ext  FILENAME
 --------  --------  ----------    ---------   ------------   ------------   -------
  ----  ----  --------------------------------
 20210520  14:59:08         213            8        100008        100015     99984
     1      1  *
 20210520  14:59:46         213            8        100016        100023     99976
     1      1  C:_Users_Administrator.DC_Desktop_Pirates!_Arr.rtf
 20210630  12:16:20          26            8        100024        100031     99968
     1      1  Pirate_Mottos.txt
 20221017  12:52:14         242            8        100032        100039     99960
     1      2  *
 20221017  12:56:23         242            8        100040        100047     99952
     1      3  *
 20221017  12:58:47         157            8        100048        100055     99944
     1      4  *
 20221026  11:42:00         157            8        100056        100063     99936
     1      5  *
 20221116  12:20:26         157            8        100064        100071     99928
     1      1  listings.txt
 20221116  12:21:41         157            8        100072        100079     99920
     1      2  listings.txt
 20221116  12:22:01         157            8        100080        100087     99912
     1      3  listings.txt
 20221116  12:26:30         157            8        100088        100095     99904
     1      4  listings.txt

 --------------------------------------------------------------------------------
----------------

  USAGE STATISTICS:  Num Extents= 11, Total Disk Size=1.0002 (TB), Used=0.0001 (
TB), Remaining=1.0002 (TB)
  Drive 2
                     DATA:          TB          Blocks       Percent
                     -----------------------------------------------
                      USED :  0.00000               88     0.00000
                      AVAIL:  1.00015       1953425039     100.00000
                      TOTAL:  1.00015       1953425127

                     DIRBLKS:       GB          Blocks       Percent
                     -----------------------------------------------
                      USED :  0.00001               11     0.08805
                      AVAIL:  0.00639            12482     99.91195
                      TOTAL:  0.00640            12493
```

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

following command to determine whether a drive is formatted. In place of "N", enter the number of the drive to check.

```
> wfsdir N
```

5. *If the hard drive(s) have not been formatted*, use the wfsx command line tool to format your drive. **Note:** Once performed, the formatting cannot be undone. The following instructions are copied from the WFS User Guide.

   ```
   > wfsfx <devicename> <options>
   ```

   `devicename` is the device identifier of the disk to be formatted. For Windows, this is the Windows disk number that may be found via the Windows Disk Manager (e.g. 1, 2, etc.). For Linux, this is the physical device name (e.g. /dev/sdb/).

   `options` may be:

   `-DirX` or `-x <power of 10>` (optional power of 10 for max number of files, default is 10) 1 will format for 1,243 files, 10 will allow 12,489 files, 100 allows 124,993 files, 1000 allows 1,249,930 files

   `-vuser <username>` specifies a volume user name, DO NOT FORGET THIS USE NAME IF USED!

   `-vpass <password>` specifies a volume password, DO NOT FORGET THIS PASSWORD IF USED!

   `-cache ON|OFF` will turn on or off the disk drive internal cache (default is ON).

   `-verifywrite ON|OFF` will turn write verify on or off for the WFS volume (default is OFF). The write verify status may be toggled ON or OFF using the WFScache utility. NOTE: turning write verify ON may significantly degradeI/O performance.

6. Files can then be copied into or out of the designated drives using the wfscopy command line tool. The following instructions are copied from the WFS User Guide.

   ```
   > wfscopy <source-file> <destination-file> <count>
   ```

One of the files must be a native Operating System (OS) file system file, and the other file must be a WFS file. **source-file** is the name of the input file and may be a native OS filename, or a WFS filename. **destination-file** is the name of the input file and may be a native OS filename, or a WFS filename. **count** is the optional number of bytes to copied. count defaults to all records.

Examples of wfscopy using Windows:

```
> wfscopy testfile.txt 1:*
```

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

```
> wfscopy 2:Contracts.pdf c:\myfolder\Contracts.pdf
```

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

```
> wfscopy 4:myfile.txt con:
```

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

2.6 Avrio SIFT

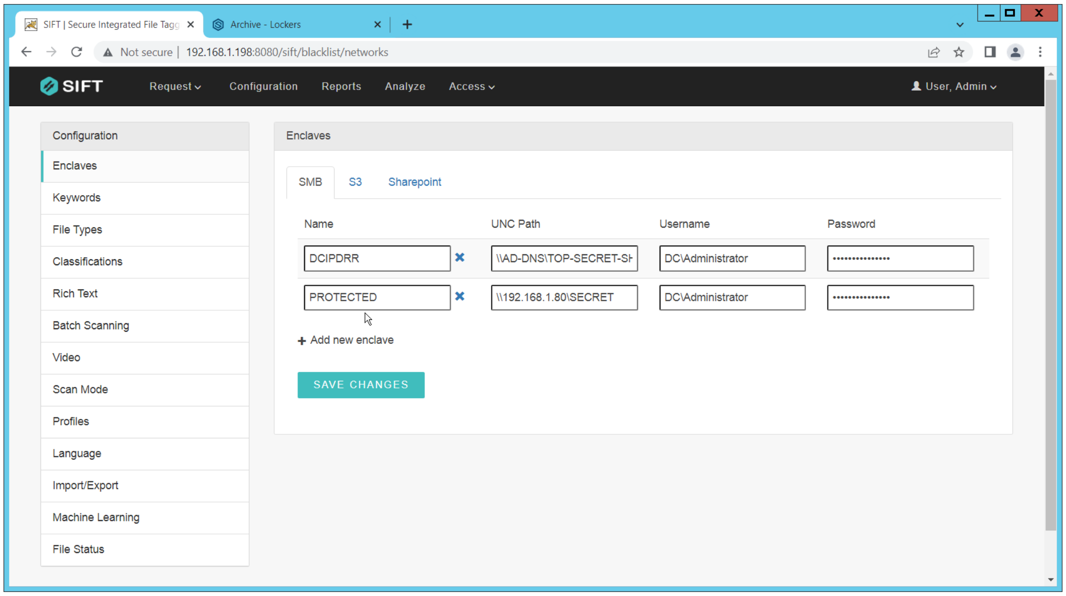
Avrio SIFT is a data inventory and management capability designed to enforce data policies. The installation of Avrio SIFT is typically done in a managed fashion by the vendor, and the deployment seen in the NCCoE lab may not resemble other deployments. In the case of a Docker deployment, configuration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

2.6.1 Configuring Avrio SIFT

1. Navigate to the SIFT dashboard (default address: http://IP-address:8080/sift/) and login.

2. Click **Configuration**.

3. Under **Enclaves**, enter two locations. First, the path to the public Windows share, and second, the path to the one protected by PKProtect. We will use this second path later in the integration between PKProtect and SIFT. In this example, DCIPDRR is the path to the public share, and PROTECTED is the path to the one protected by PKProtect. Enter user accounts that can access each share. In production, it is recommended to create a separate user account for SIFT to use to access these shares.



Name	UNC Path	Username	Password
DCIPDRR	\\AD-DNS\TOP-SECRET-SH	DC\Administrator	•••••••••••••••
PROTECTED	\\192.168.1.80\SECRET	DC\Administrator	•••••••••••••••

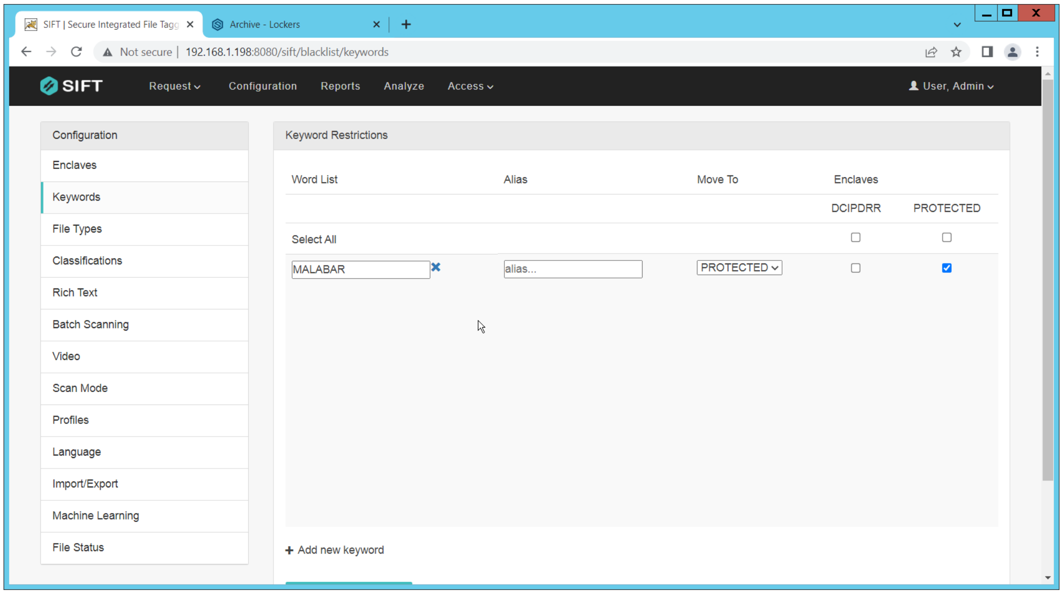
4. Click **Save Changes**.

5. Click **Keywords** on the left menu.

6. Click **Add new keyword**.

7. Enter the keyword under **Name**, and an **Alias** (if desired). Check the box next to any enclaves that are allowed to have this keyword – SIFT will be able to move files matching it to the enclaves you check the box for.

8. Select the PROTECTED enclave under **Move To**.



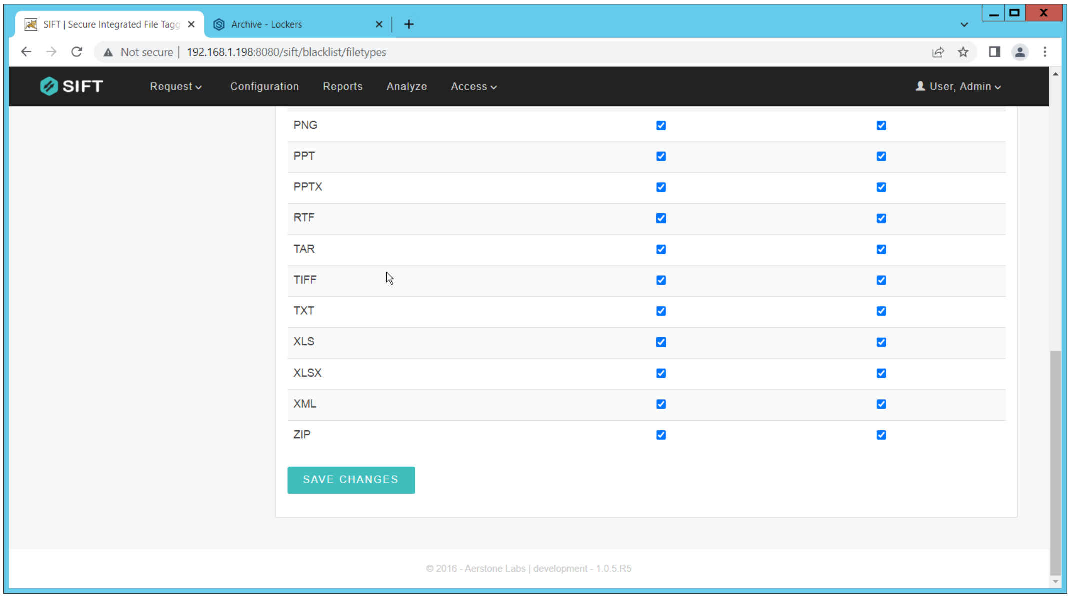
Keyword Restrictions

Word List	Alias	Move To	Enclaves	
			DCIPDRR	PROTECTED
Select All			☐	☐
MALABAR	alias...	PROTECTED	☐	☑

9. Click **Save Changes**.

10. Click **File Types**.

11. Designate file types that are allowed to exist under each enclave.

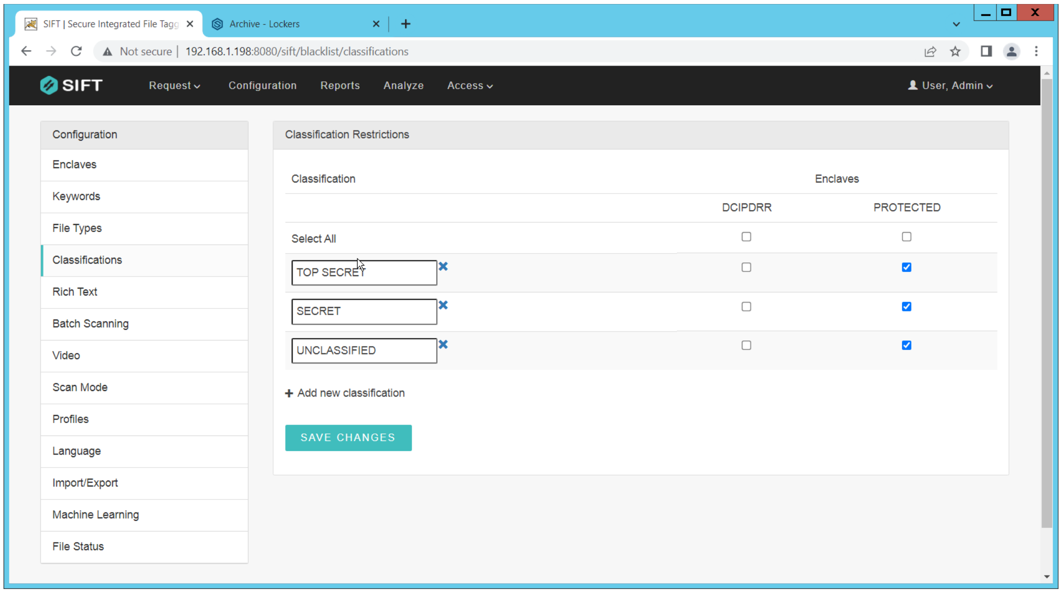

SIFT | Secure Integrated File Tagg
Archive - Lockers
Not secure | 192.168.1.198:8080/sift/blacklist/filetypes
SIFT
Request
Configuration
Reports
Analyze
Access
User, Admin
SAVE CHANGES
© 2016 - Aerstone Labs | development - 1.0.5.R5

PNG	☑	☑
PPT	☑	☑
PPTX	☑	☑
RTF	☑	☑
TAR	☑	☑
TIFF	☑	☑
TXT	☑	☑
XLS	☑	☑
XLSX	☑	☑
XML	☑	☑
ZIP	☑	☑

12. Click **Save Changes**.

13. Click **Classifications**.

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



Classification	Enclaves	
	DCIPDRR	PROTECTED
Select All	□	□
TOP SECRET	□	☑
SECRET	□	☑
UNCLASSIFIED	□	☑

15. Click **Save Changes**.

16. On the top click **Request** > **New Request**.

17. Click **Batch**.

18. Select **UNC Path** for **Source Type**.

19. Select the enclave to scan for sensitive files.

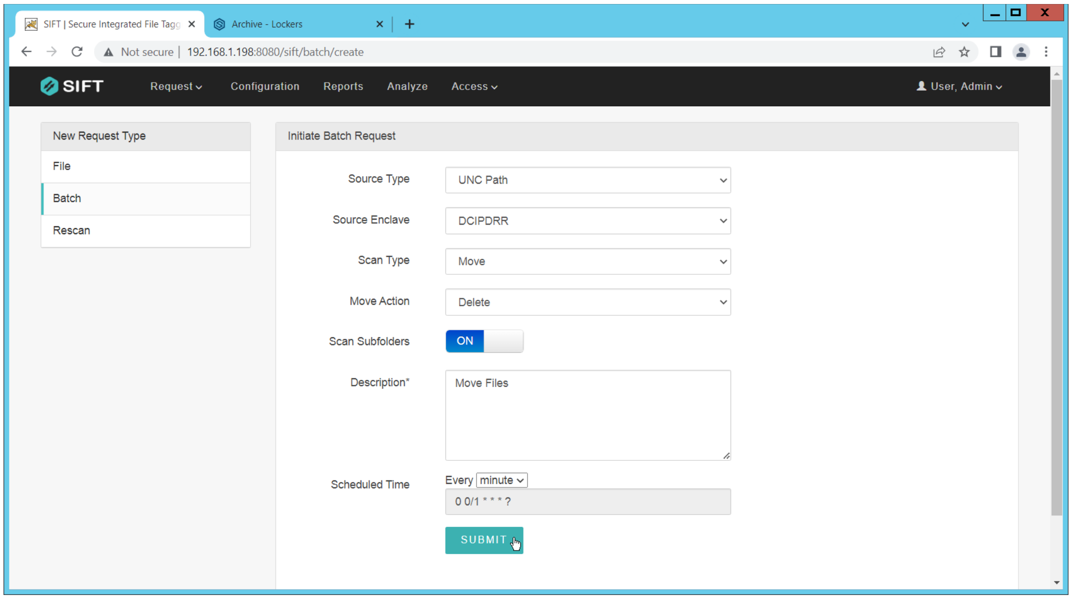
20. Select **Move** for **Scan Type**. (Note that if you select **Scan** for **Scan Type**, it will scan files and tell you they are sensitive and whether they can be moved but will not attempt to move them. This is useful for debugging.)

21. Select **Delete** for **Move Action**, or another action depending on the needs of your organization. Selecting Delete will remove the sensitive file from the public share and move it to the protected one.

22. Set **Scan Subfolders** to **ON**.

23. Enter a description for the scan.

24. Set the frequency of the scan. Note that the efficiency of the scan will likely depend on the size of the organization, and it may be more desirable to scan once an hour rather than once a minute.



Initiate Batch Request

Source Type: UNC Path

Source Enclave: DCIPDRR

Scan Type: Move

Move Action: Delete

Scan Subfolders: ON

Description*: Move Files

Scheduled Time: Every minute

0 0/1 * * * ?

25. Click **Submit**.

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

2.7 Cisco Duo

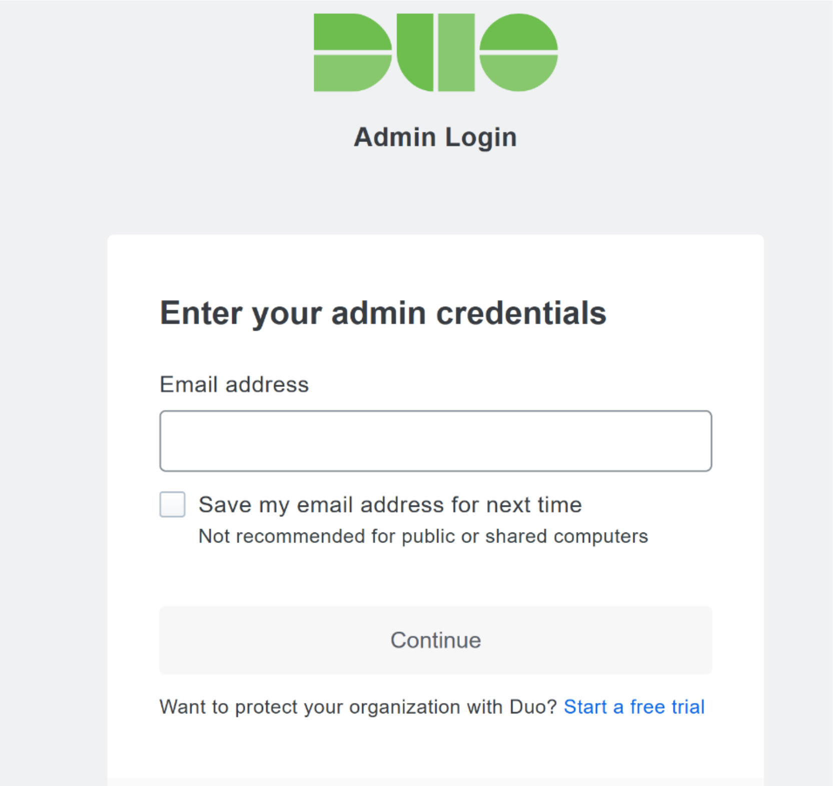
Cisco Duo is a Multi-Factor Authentication and Single Sign-On tool. In this project, Dispel is used to control access to internal systems through virtualization, and Duo is used as a multifactor authentication solution between Dispel and those internal systems. This ensures that even if a Dispel virtual 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.

2.7.1 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

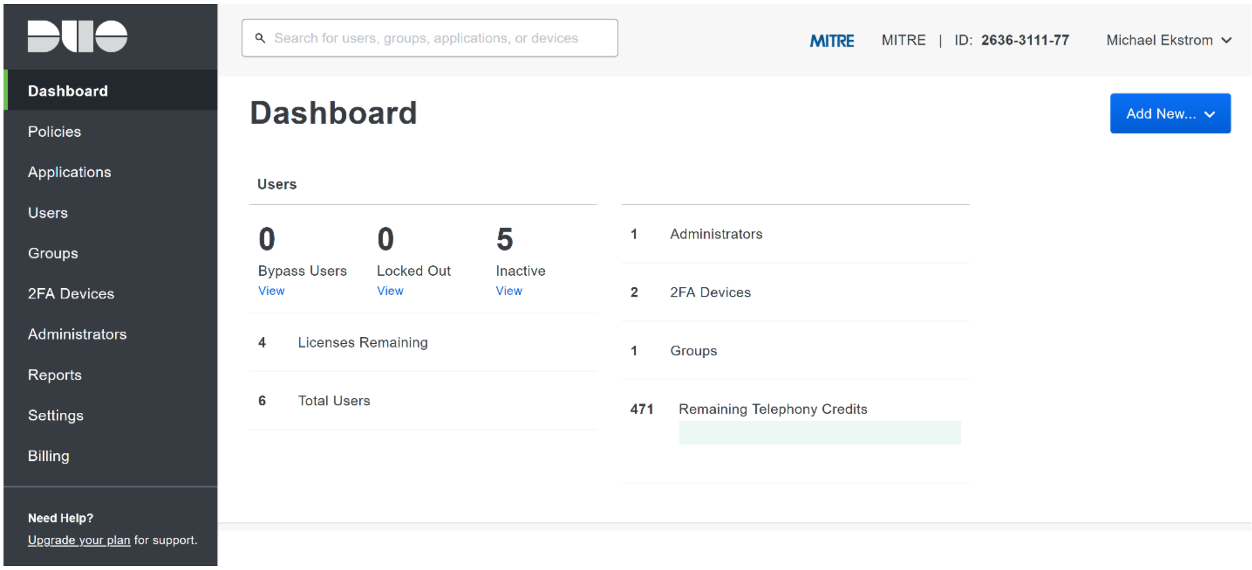
Enter your admin credentials

Email address

☐ Save my email address for next time
Not recommended for public or shared computers

Want to protect your organization with Duo? Start a free trial

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



Dashboard

Users

0 Bypass Users View
0 Locked Out View
5 Inactive View

4 Licenses Remaining

6 Total Users

1 Administrators

2 2FA Devices

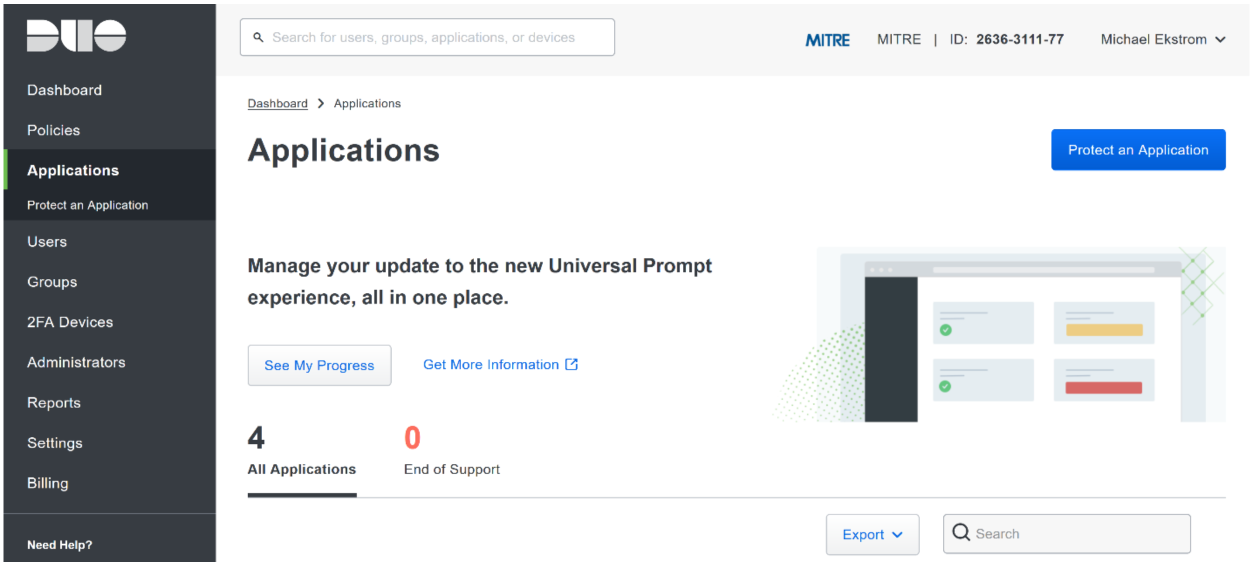
1 Groups

471 Remaining Telephony Credits

Need Help?
Upgrade your plan for support.

4. Click **Applications** in the sidebar.

5. Click **Protect an Application**.

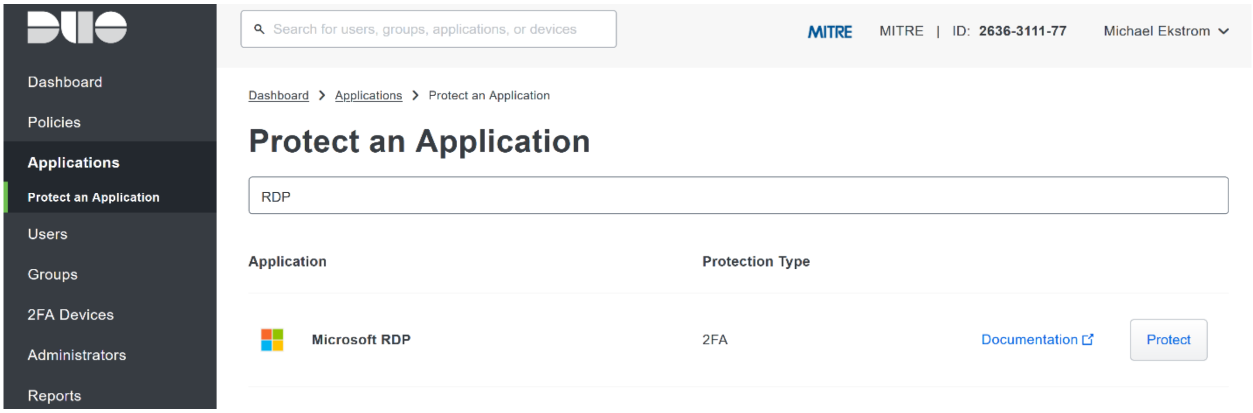


Applications

Manage your update to the new Universal Prompt experience, all in one place.

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

7. Click **Protect**.

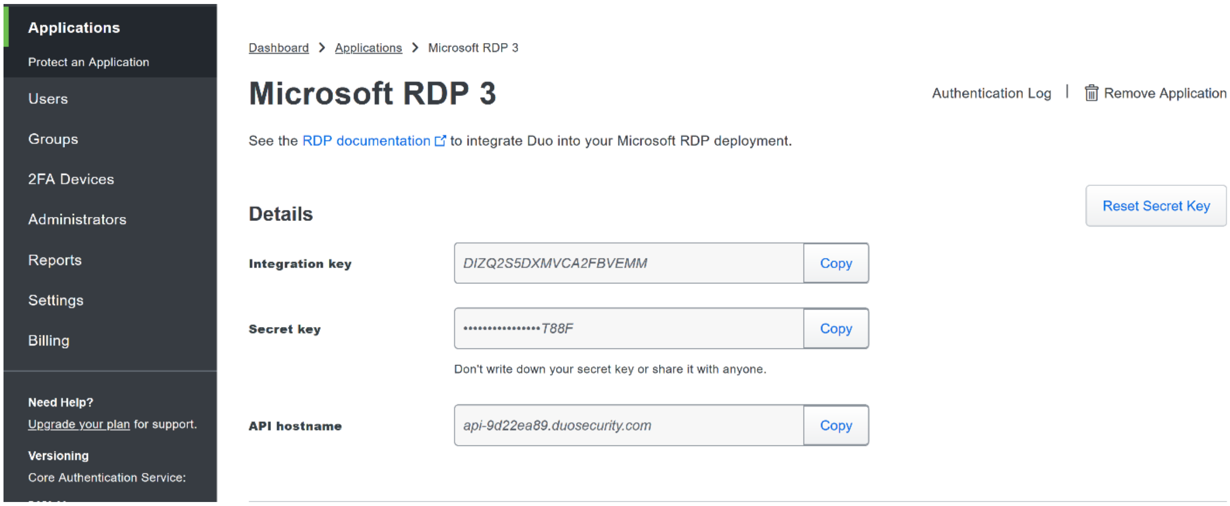


Protect an Application

RDP

Application	Protection Type
Microsoft RDP	2FA

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.



Dashboard > Applications > Microsoft RDP 3

Microsoft RDP 3

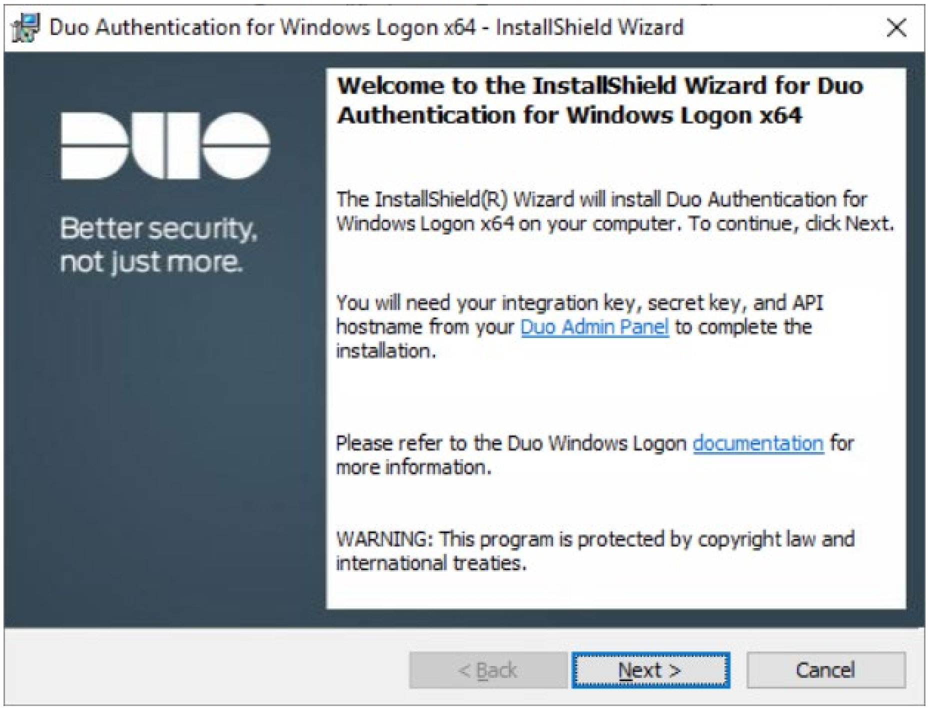
See the RDP documentation to integrate Duo into your Microsoft RDP deployment.

Details

Integration key	DIZQ2S5DXMVCA2FBVEMM	Copy
Secret key	••••••••••••••••T88F	Copy
	Don't write down your secret key or share it with anyone.	
API hostname	api-9d22ea89.duosecurity.com	Copy

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

10. Run the downloaded EXE file.


Duo Authentication for Windows Logon x64 - InstallShield Wizard
Better security, not just more.
< Back
Next >
Cancel

Welcome to the InstallShield Wizard for Duo Authentication for Windows Logon x64

The InstallShield(R) Wizard will install Duo Authentication for Windows Logon x64 on your computer. To continue, click Next.

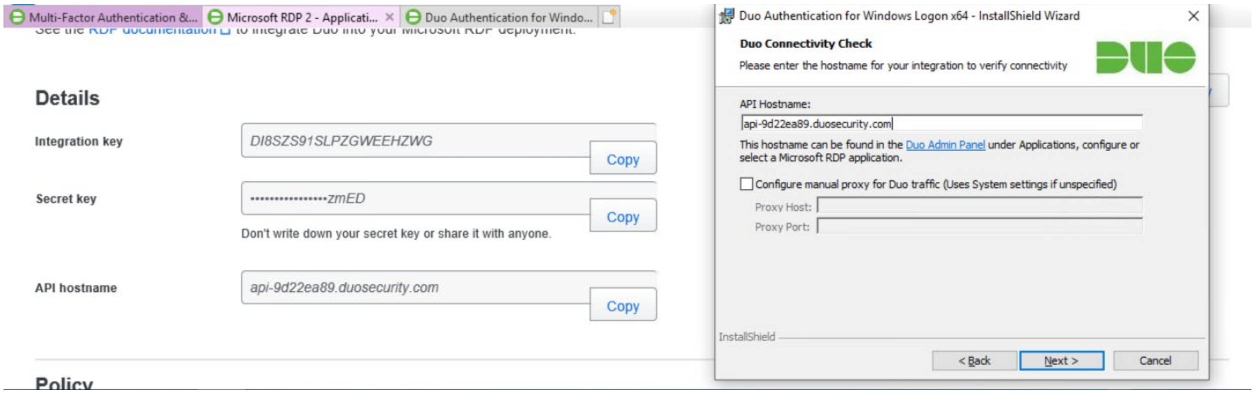
You will need your integration key, secret key, and API hostname from your Duo Admin Panel to complete the installation.

Please refer to the Duo Windows Logon documentation for more information.

WARNING: This program is protected by copyright law and international treaties.

11. Click **Next**.

12. Copy the **API Hostname** into the labeled field.


Multi-Factor Authentication &...
Microsoft RDP 2 - Applicati...
Duo Authentication for Windo...
See the RDP documentation to integrate Duo into your Microsoft RDP deployment.

Details

Integration key: DI8SZS91SLPZGWEEHZWG

Secret key: ••••••••••••••••zmED

Don't write down your secret key or share it with anyone.

API hostname: api-9d22ea89.duosecurity.com

Duo Authentication for Windows Logon x64 - InstallShield Wizard

Duo Connectivity Check

Please enter the hostname for your integration to verify connectivity

API Hostname: api-9d22ea89.duosecurity.com

This hostname can be found in the Duo Admin Panel under Applications, configure or select a Microsoft RDP application.

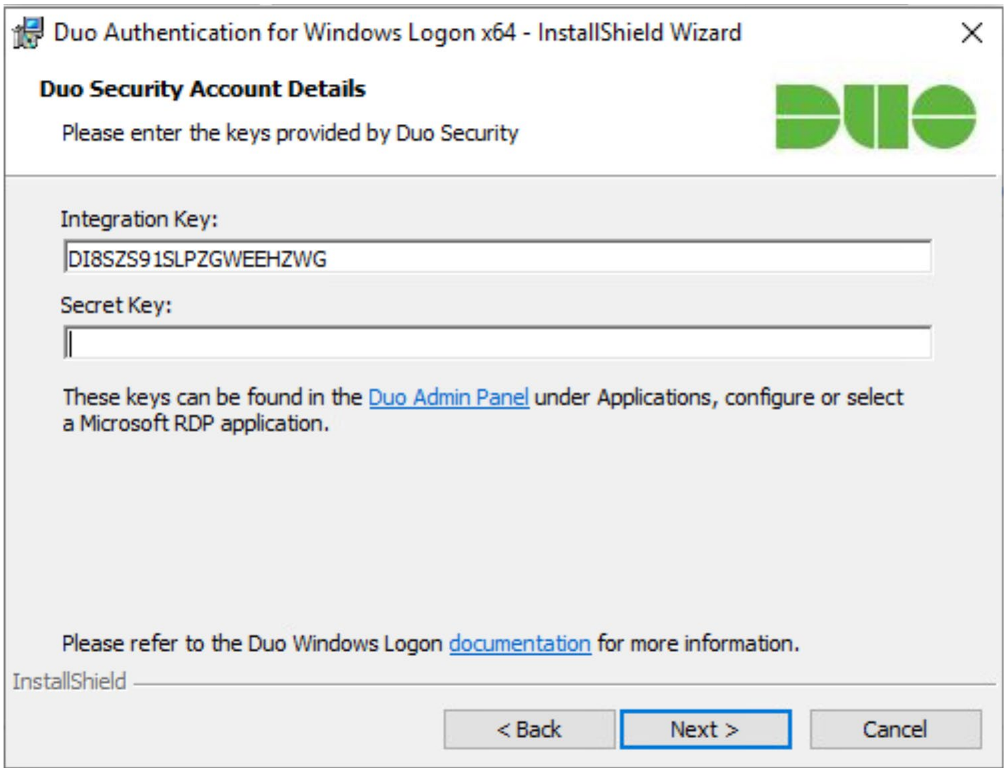
□ Configure manual proxy for Duo traffic (Uses System settings if unspecified)

Proxy Host:

Proxy Port:

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

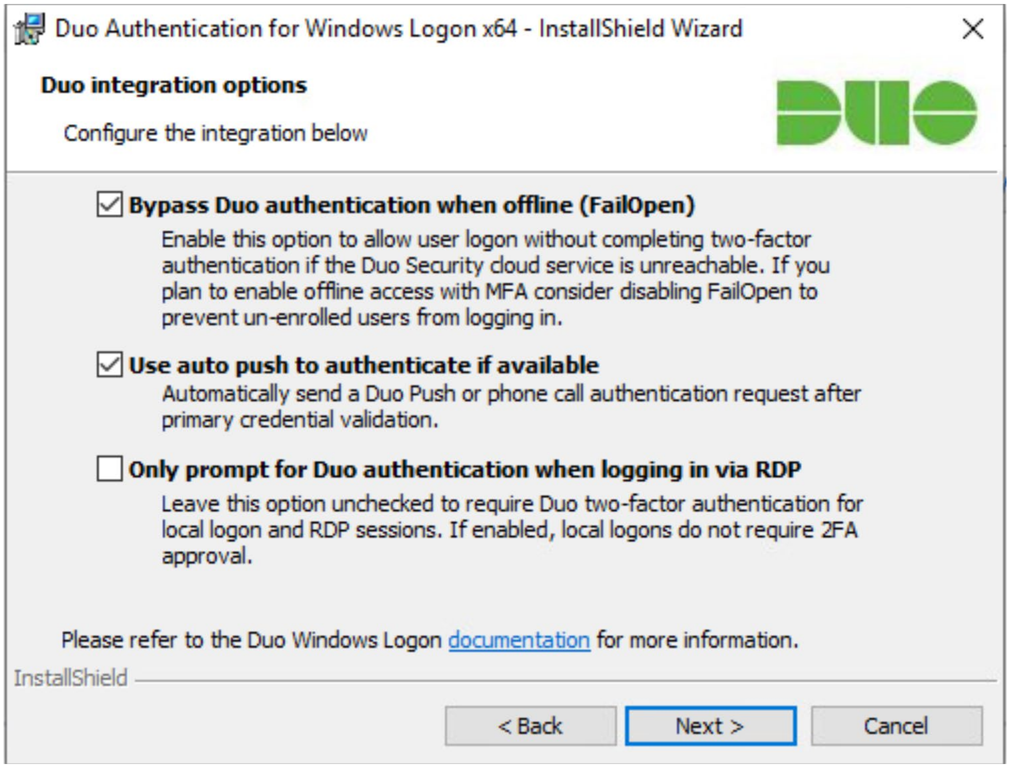
Secret Key:

These keys can be found in the Duo Admin Panel under Applications, configure or select a Microsoft RDP application.

Please refer to the Duo Windows Logon documentation for more information.

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

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.

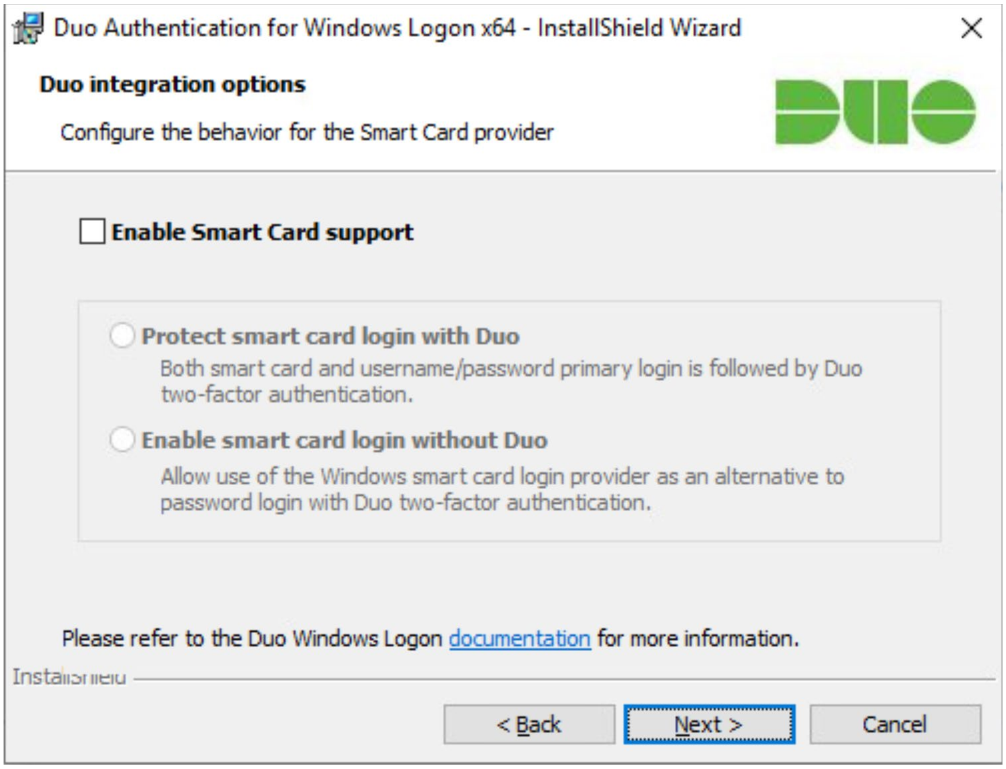
□ **Only prompt for Duo authentication when logging in via RDP**

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 documentation for more information.

17. Click **Next**.

18. Leave **Enable Smart Card support** unchecked.



Duo Authentication for Windows Logon x64 - InstallShield Wizard

Duo integration options

Configure the behavior for the Smart Card provider

□ **Enable Smart Card support**

○ **Protect smart card login with Duo**

Both smart card and username/password primary login is followed by Duo two-factor authentication.

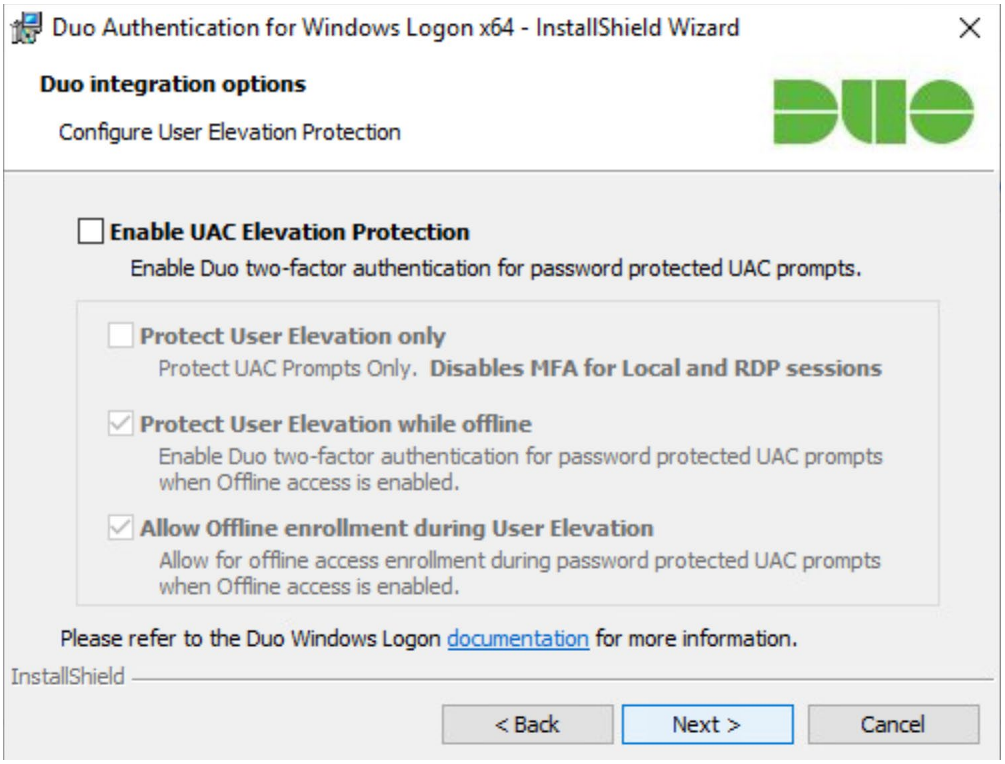
○ **Enable smart card login without Duo**

Allow use of the Windows smart card login provider as an alternative to password login with Duo two-factor authentication.

Please refer to the Duo Windows Logon documentation for more information.

19. Click **Next**.

20. Leave **Enable UAC Elevation Protection** unchecked.



Duo Authentication for Windows Logon x64 - InstallShield Wizard

Duo integration options

Configure User Elevation Protection

□ **Enable UAC Elevation Protection**
Enable Duo two-factor authentication for password protected UAC prompts.

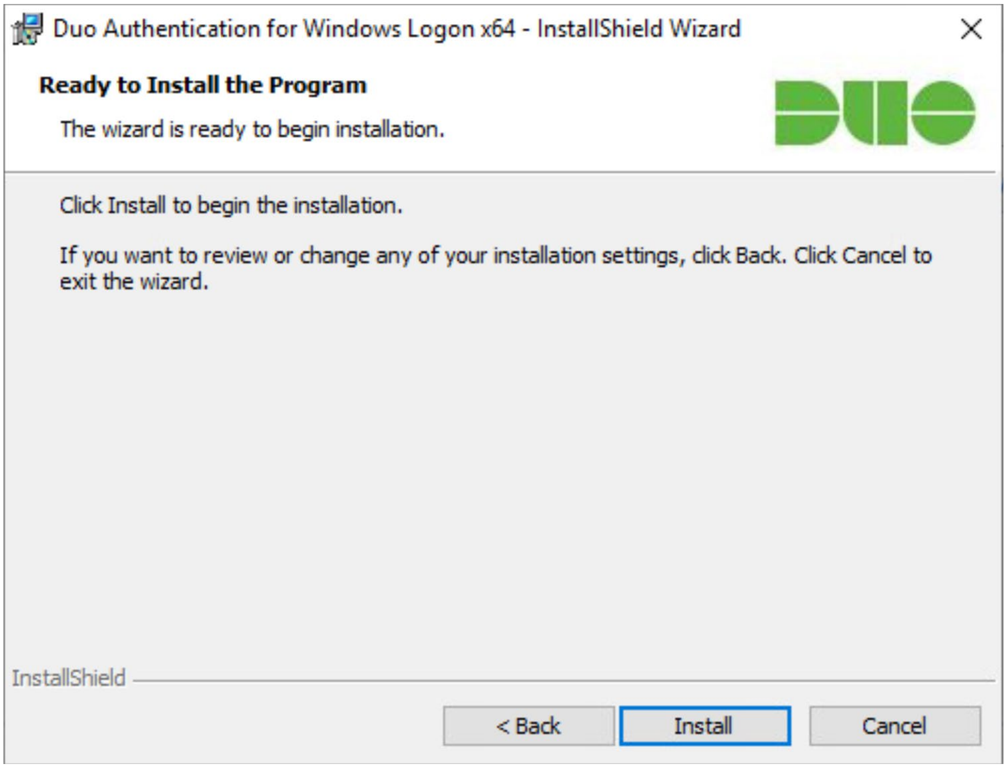
□ **Protect User Elevation only**
Protect UAC Prompts Only. **Disables MFA for Local and RDP sessions**

☑ **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.

21. Click **Next**.



Duo Authentication for Windows Logon x64 - InstallShield Wizard

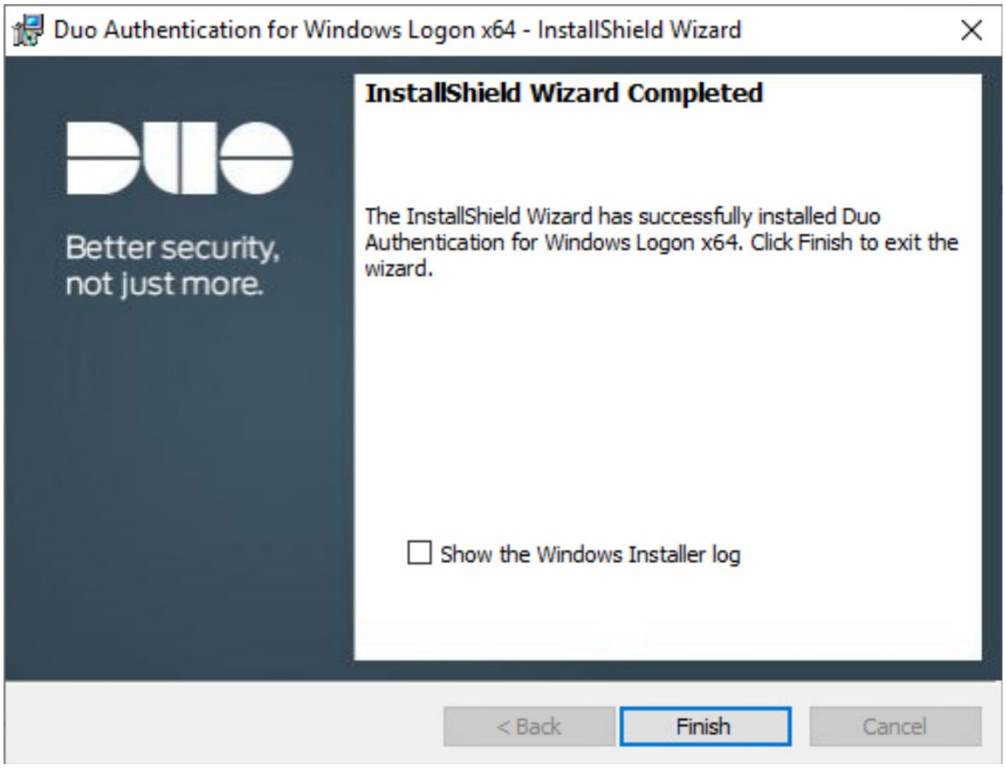
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

22. Click **Install**.


Duo Authentication for Windows Logon x64 - InstallShield Wizard
Better security, not just more.
□ Show the Windows Installer log
< Back
Finish
Cancel

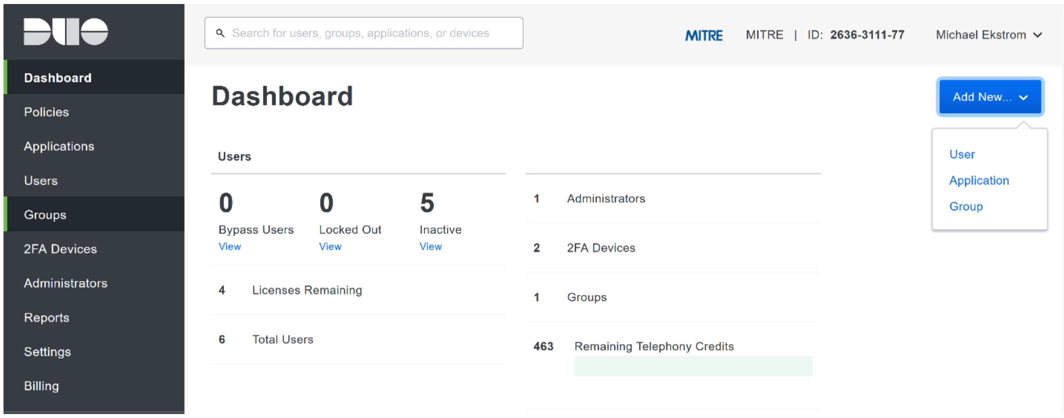
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Duo Authentication for Windows Logon x64. Click Finish to exit the wizard.

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.

2.7.2 Registering a Duo User

1. Login to the Duo Admin Dashboard.



Dashboard

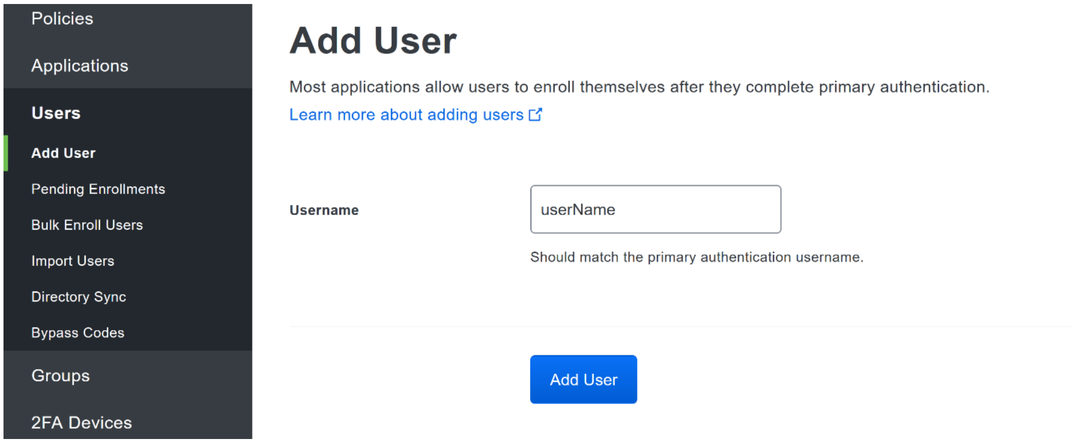
Users

0 Bypass Users View	0 Locked Out View	5 Inactive View

4	Licenses Remaining
6	Total Users

1	Administrators
2	2FA Devices
1	Groups
463	Remaining Telephony Credits

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



Add User

Most applications allow users to enroll themselves after they complete primary authentication.
Learn more about adding users

Username: userName

Should match the primary authentication username.

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, 2 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.

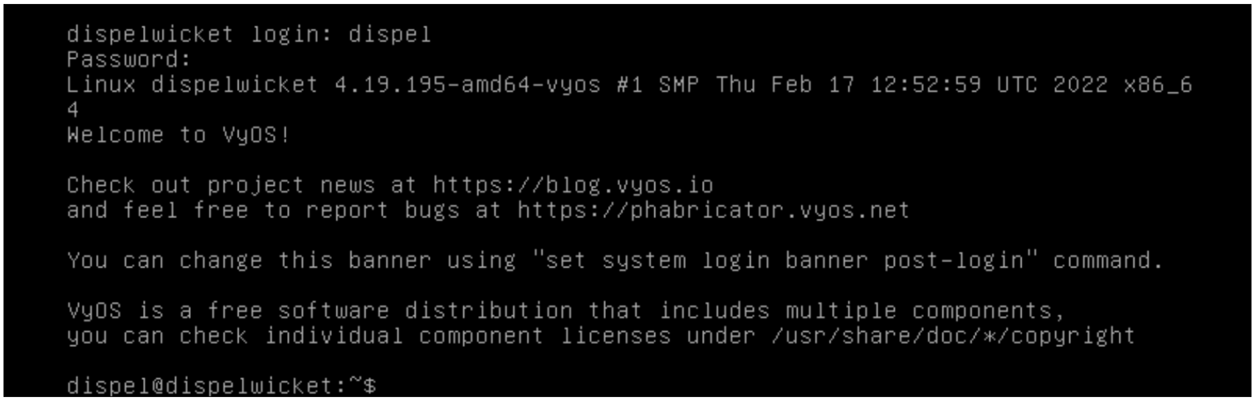
2.8 Dispel

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 Wide-Area Network (WAN) and Local-Area Network (LAN) interfaces, placing the device in-line between the enterprise systems and the external network.

2.8.1 Installation

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

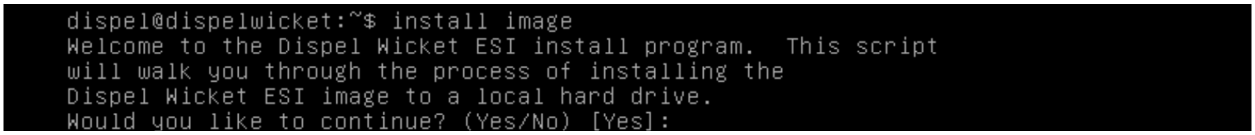
2. Login with username "dispel" and the password provided.



```
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 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:~$
```

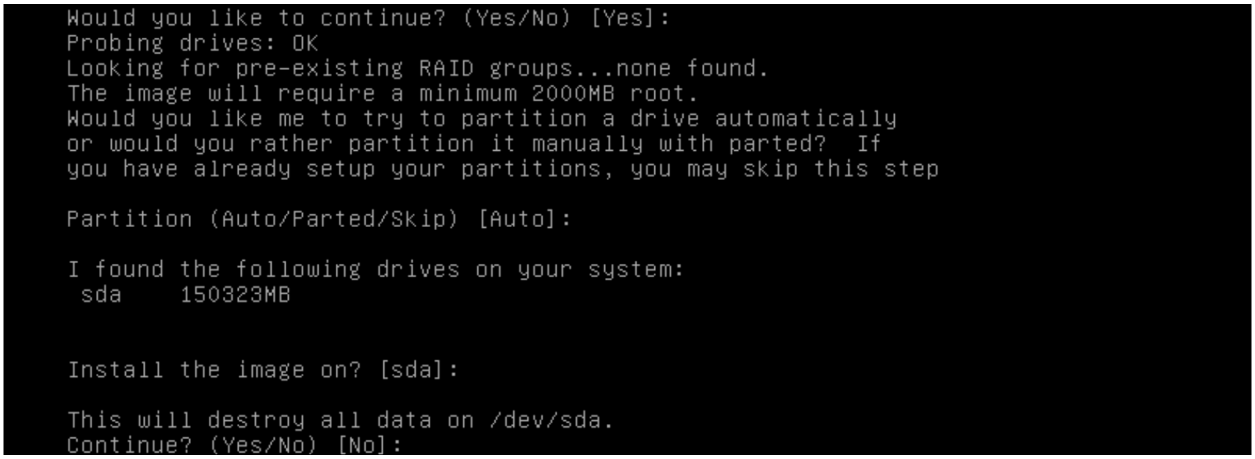
3. Begin the installation process

```
> install image
```



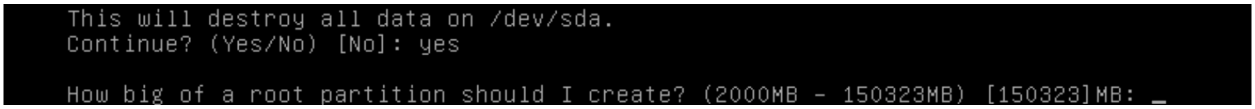
```
dispel@dispelwicket:~$ install image
Welcome to the Dispel Wicket ESI install program.  This script
will walk you through the process of installing the
Dispel Wicket ESI image to a local hard drive.
Would you like to continue? (Yes/No) [Yes]:
```

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



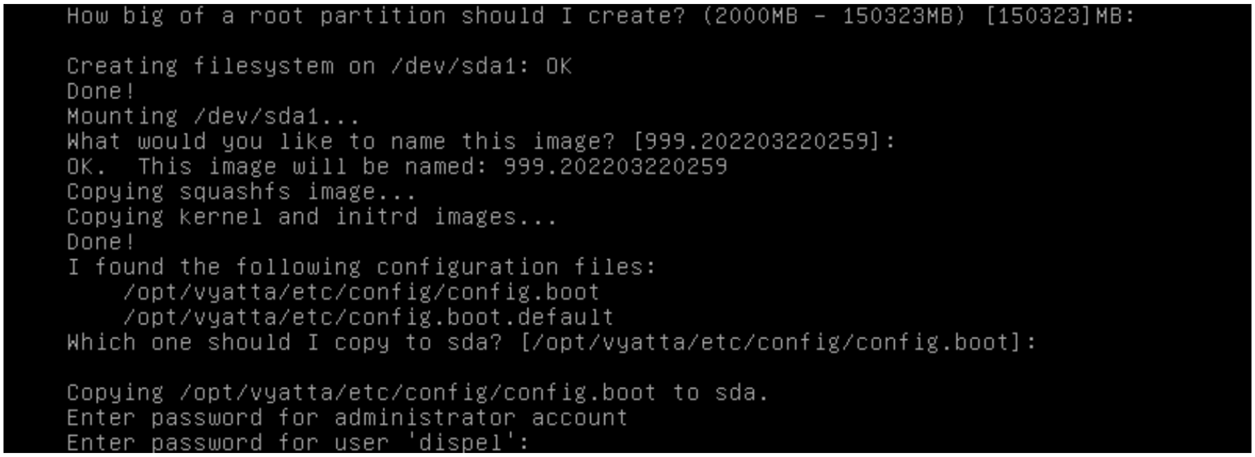
```
Would you like to continue? (Yes/No) [Yes]:
Probing drives: OK
Looking for pre-existing RAID groups...none found.
The image will require a minimum 2000MB root.
Would you like me to try to partition a drive automatically
or would you rather partition it manually with parted?  If
you have already setup 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.



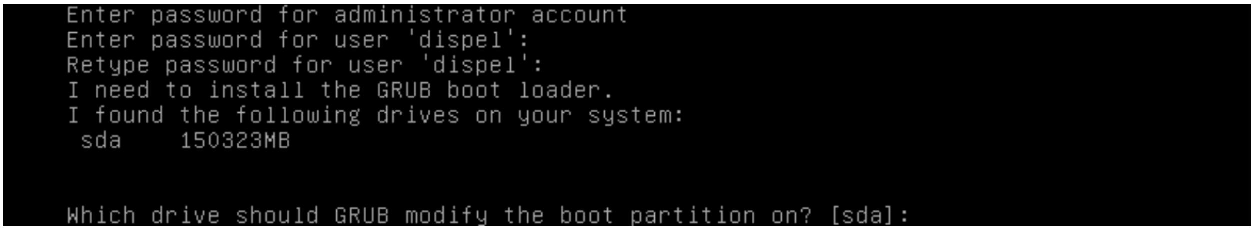
```
This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]: yes

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.



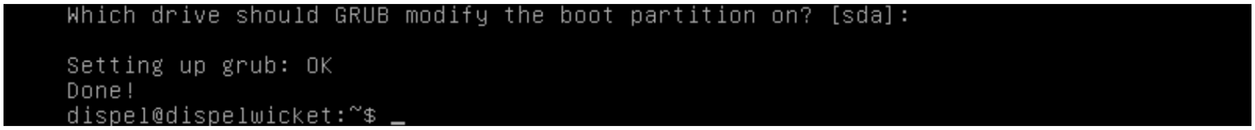
```
How big of a root partition should I create? (2000MB - 150323MB) [150323]MB:

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/config.boot.default
Which one should I copy to sda? [/opt/vyatta/etc/config/config.boot]:

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

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



```
Enter password for administrator account
Enter password for user 'dispel':
Retype password for user 'dispel':
I need to install the GRUB boot loader.
I found the following drives on your system:
 sda    150323MB


Which drive should GRUB modify the boot partition on? [sda]:
```

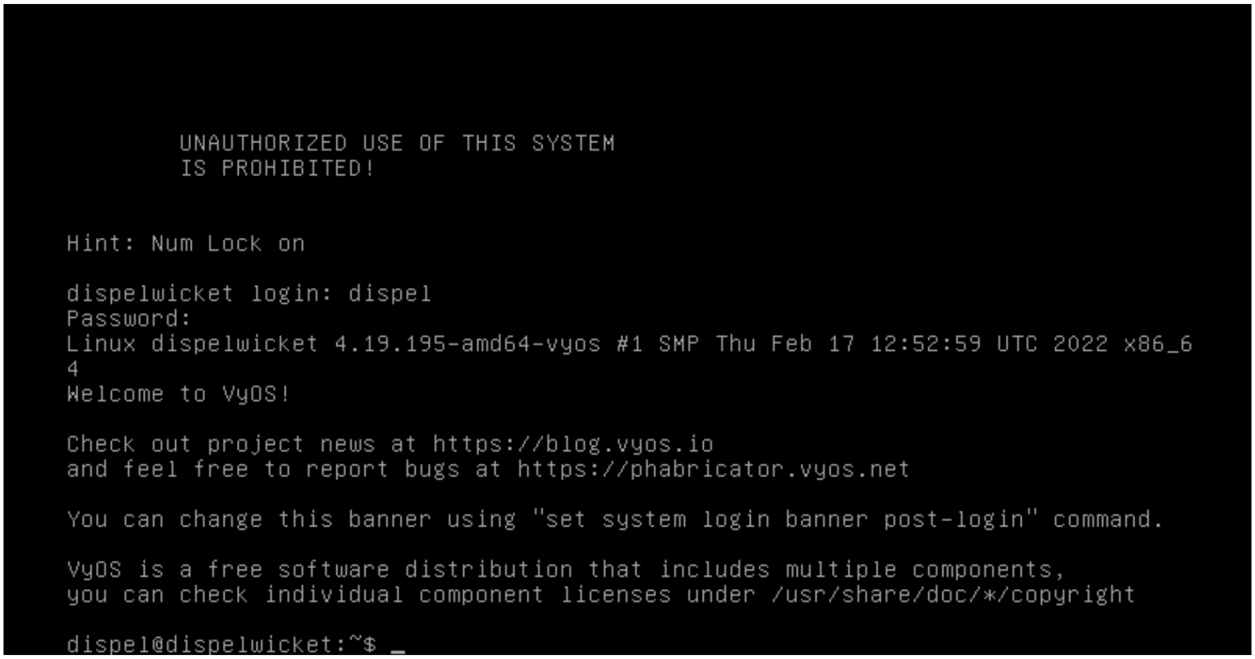
8. Press enter one final time to finish the installation



```
Which drive should GRUB modify the boot partition on? [sda]:

Setting up grub: OK
Done!
dispel@dispelwicket:~$ _
```

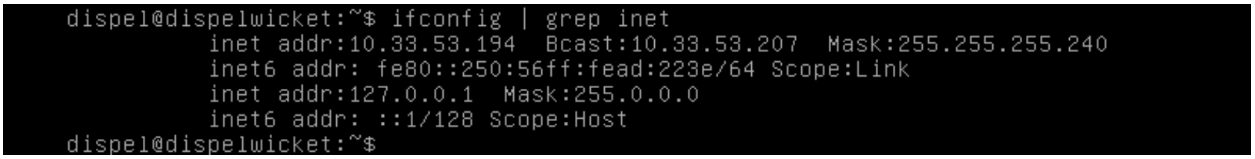
9. Power off the machine, remove the provided ISO, and power it back on.

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:~$ _
```

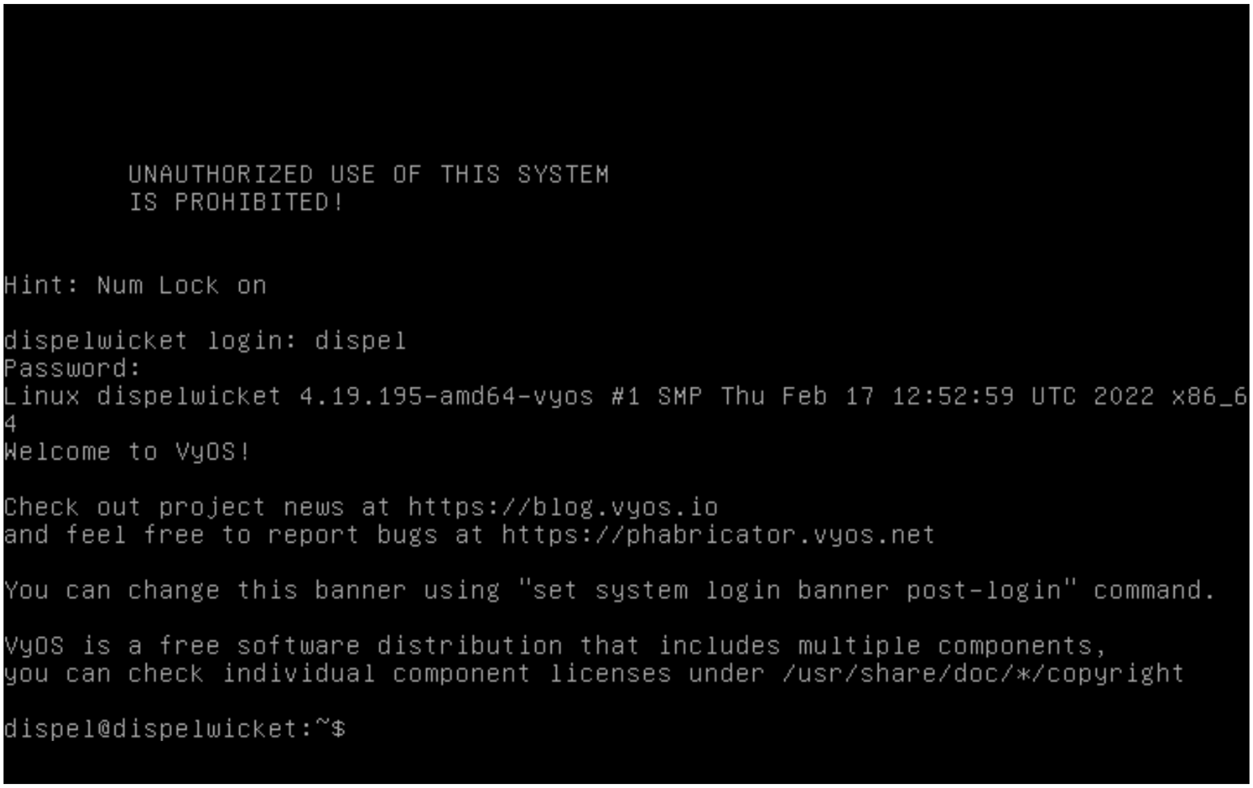
11. Type in the command > `ifconfig | grep inet`. Verify the output to make sure it matches the desired network configuration. If not, see the next section.



```
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:~$
```

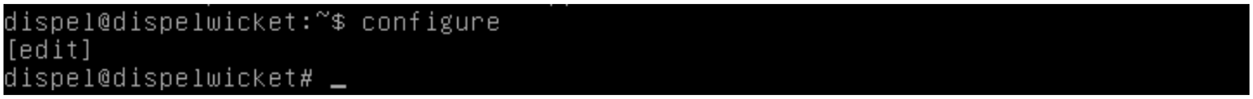
2.8.2 Configuring IP Addresses

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



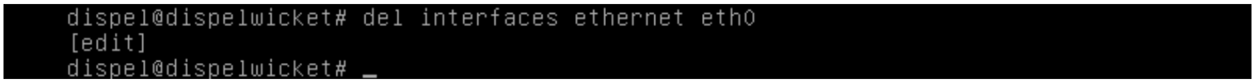
```
        UNAUTHORIZED USE OF THIS SYSTEM
        IS PROHIBITED!


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`.



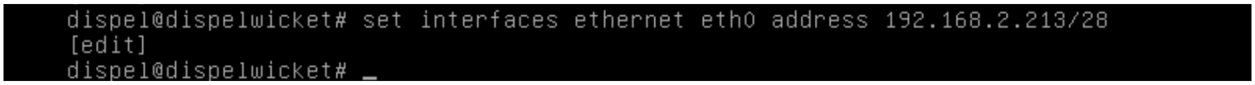
```
dispel@dispelwicket:~$ configure
[edit]
dispel@dispelwicket# _
```

3. Type in the command > `del interfaces ethernet eth0`, or whichever interface you are currently modifying.



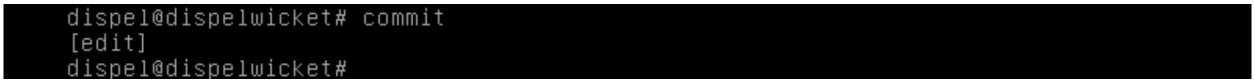
```
    dispel@dispelwicket# del interfaces ethernet eth0
    [edit]
    dispel@dispelwicket# _
```

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.



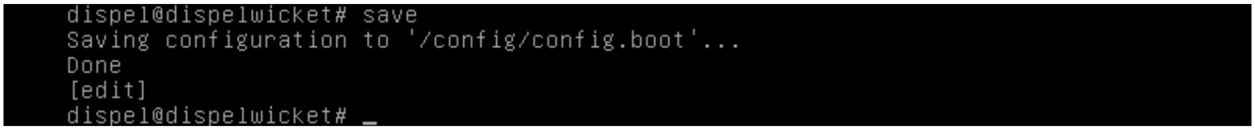
```
    dispel@dispelwicket# set interfaces ethernet eth0 address 192.168.2.213/28
    [edit]
    dispel@dispelwicket# _
```

5. Type in the command > `commit`.



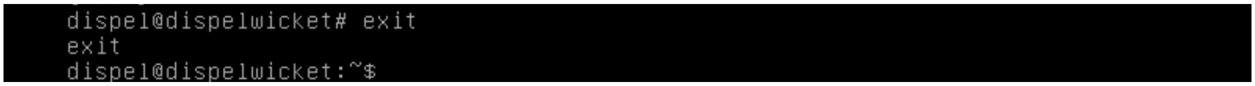
```
    dispel@dispelwicket# commit
    [edit]
    dispel@dispelwicket#
```

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`.

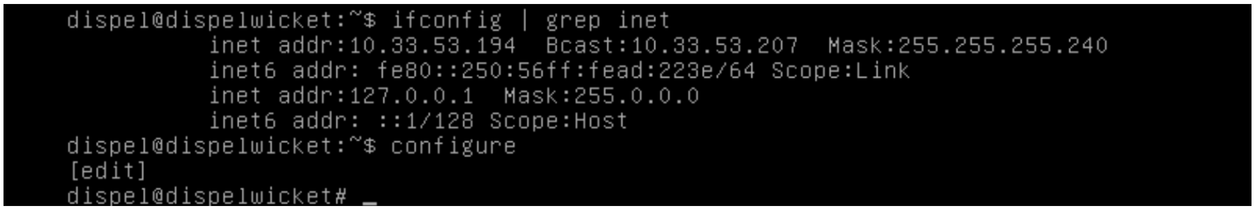


```
dispel@dispelwicket# exit
exit
dispel@dispelwicket:~$
```

2.8.3 Configuring Network

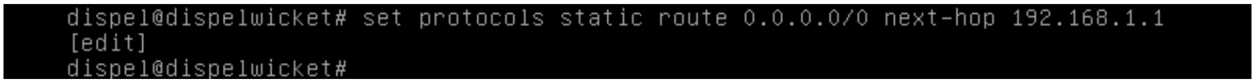
The following instructions are to modify a Dispel wicket device to forward traffic to a different routing device. This may be desirable for some network setups.

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



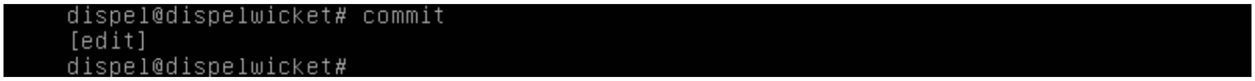
```
dispel@dispelwicket:~$ ifconfig | grep inet
          inet addr:10.33.53.194  Bcast:10.33.53.207  Mask:255.255.255.240
          inet6 addr: fe80::250:56ff:fead:223e/64 Scope:Link
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
dispel@dispelwicket:~$ configure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

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.



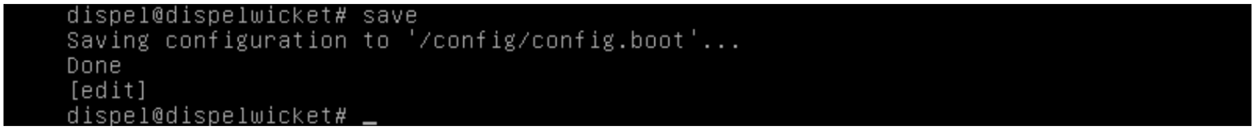
```
dispel@dispelwicket# set protocols static route 0.0.0.0/0 next-hop 192.168.1.1
[edit]
dispel@dispelwicket#
```

3. Type in the command > `commit`.



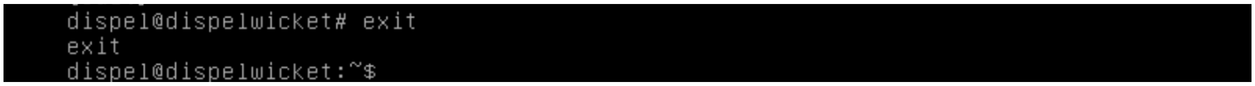
```
dispel@dispelwicket# commit
[edit]
dispel@dispelwicket#
```

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:~$
```

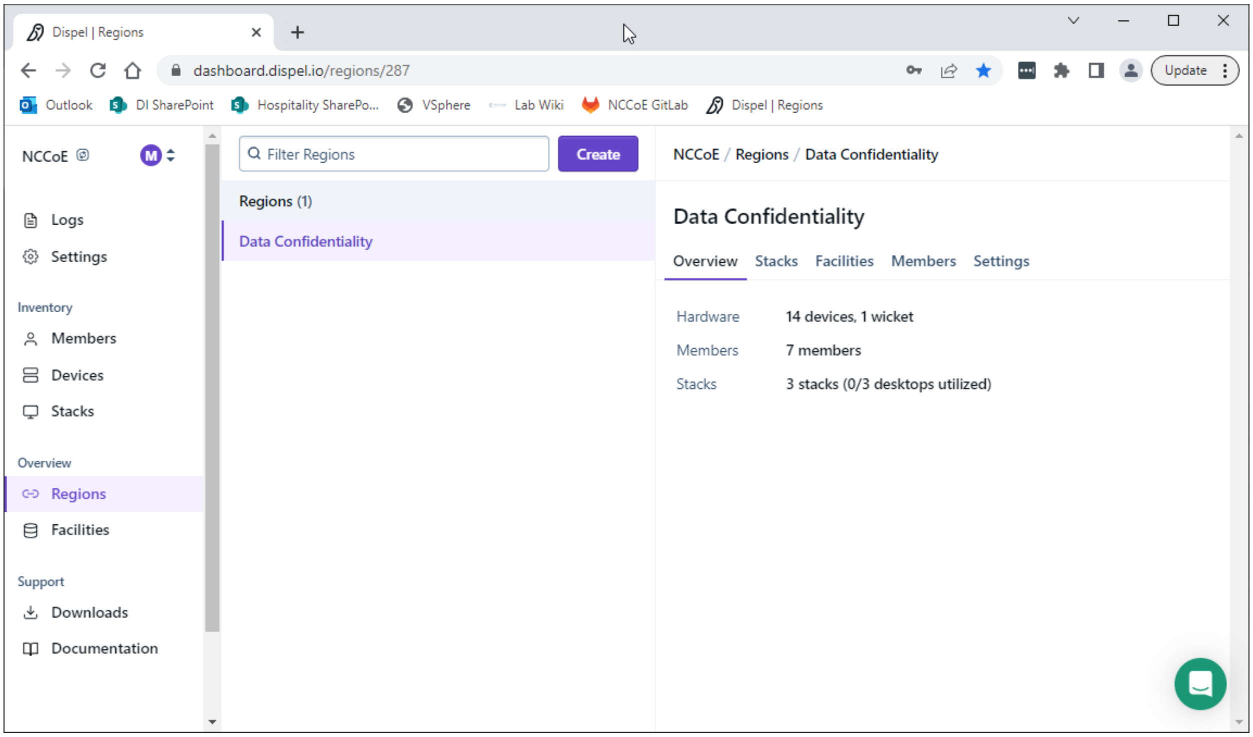
6. On the designated router or firewall, ensure User Datagram Protocol (UDP) is allowed from the Dispel device on the provided port. For the NCCoE deployment, port 1194 was utilized. A target destination for the traffic will be provided by Dispel.

7. Modify the IP addresses of the south-side network interface to properly align with your network. See the “Configuring IP Addresses” section above.

2.8.4 Adding a Device

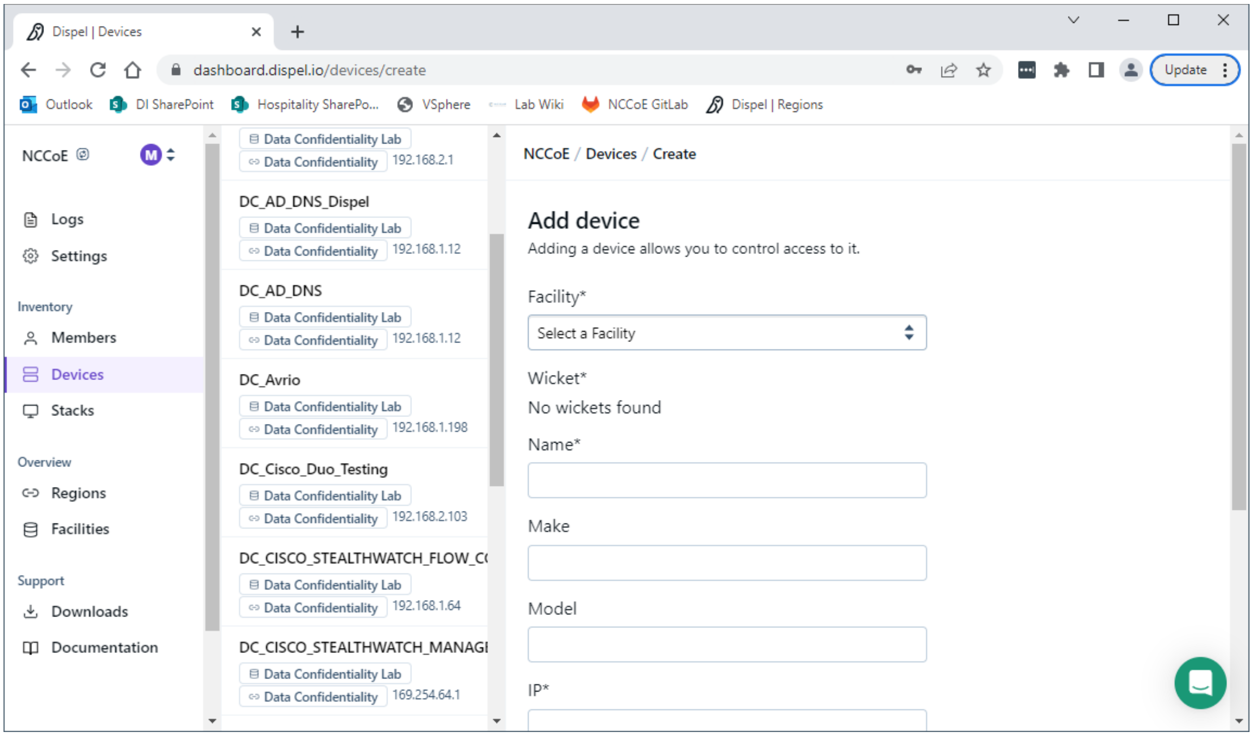
1. On the workstation in question, ensure that ping and RDP are accessible, including allowing such connections through a local firewall.

2. Authenticate to the Dispel webpage with the provided credentials.



Hardware	14 devices, 1 wicket
Members	7 members
Stacks	3 stacks (0/3 desktops utilized)

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



Add device

Adding a device allows you to control access to it.

Facility*

Select a Facility

Wicket*

No wickets found

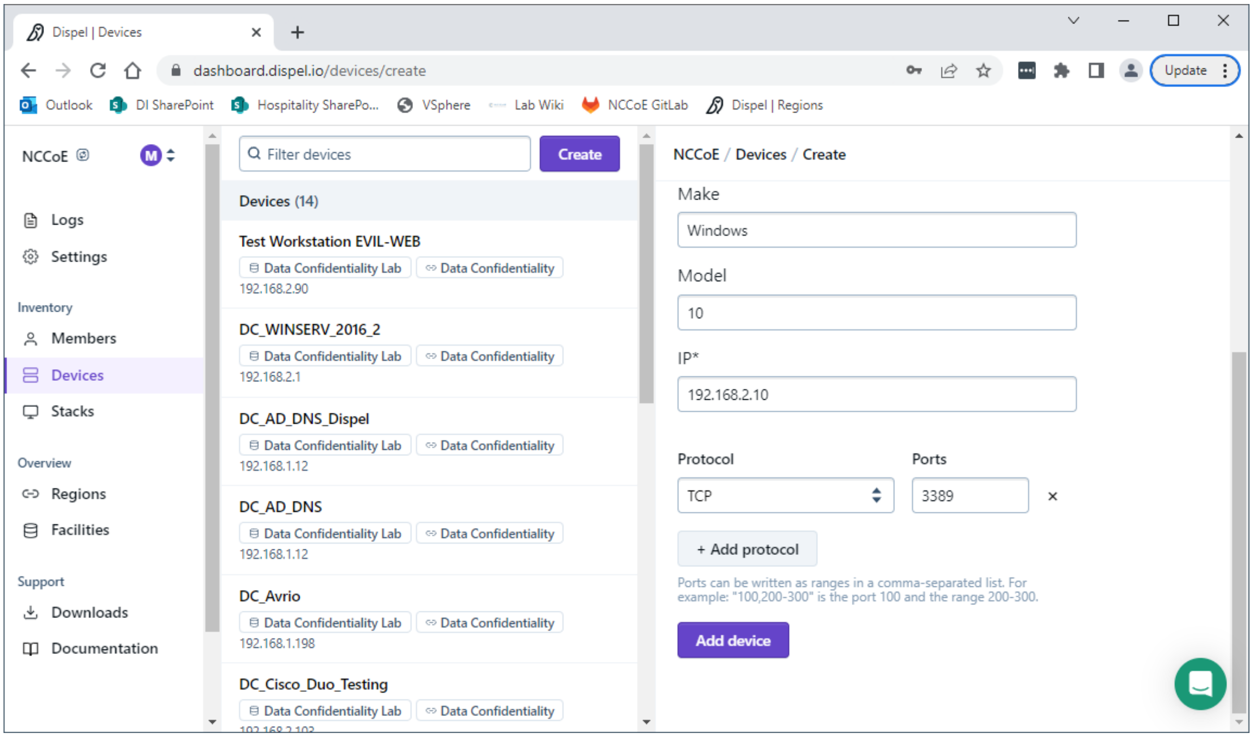
Name*

Make

Model

IP*

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



Make: Windows

Model: 10

IP*: 192.168.2.10

Protocol: TCP

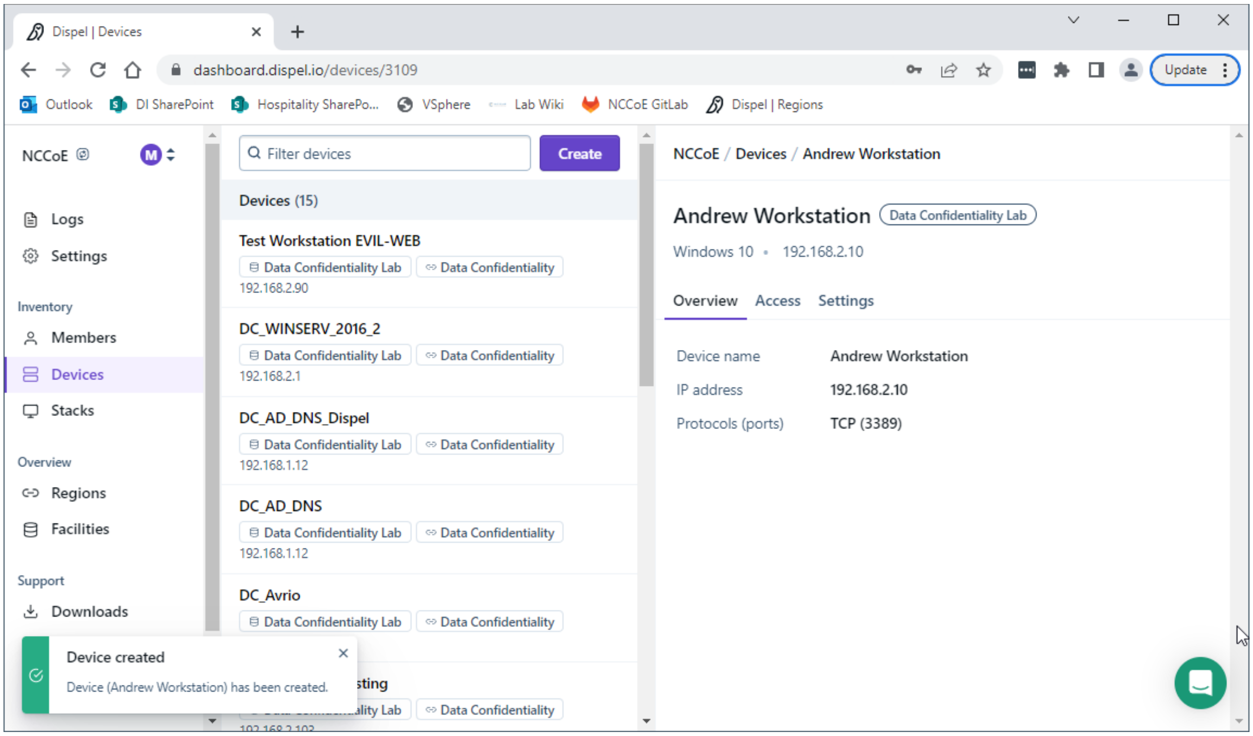
Ports: 3389

+ Add protocol

Ports can be written as ranges in a comma-separated list. For example: "100,200-300" is the port 100 and the range 200-300.

Add device

5. Click Add Device.



Devices (15)

Device	Facility	Region	IP
Test Workstation EVIL-WEB	Data Confidentiality Lab	Data Confidentiality	192.168.2.90
DC_WINSERV_2016_2	Data Confidentiality Lab	Data Confidentiality	192.168.2.1
DC_AD_DNS_Dispel	Data Confidentiality Lab	Data Confidentiality	192.168.1.12
DC_AD_DNS	Data Confidentiality Lab	Data Confidentiality	192.168.1.12
DC_Avrio	Data Confidentiality Lab	Data Confidentiality	

Device created

Device (Andrew Workstation) has been created.

NCCoE / Devices / Andrew Workstation

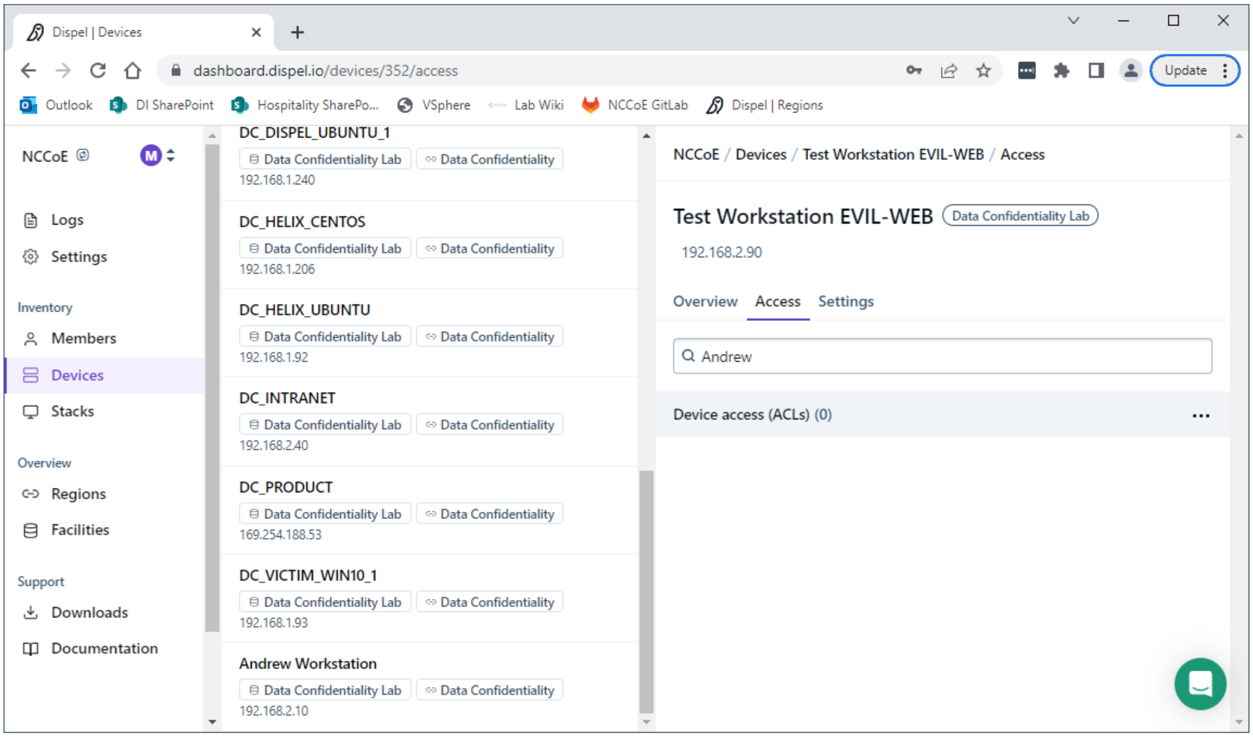
Andrew Workstation (Data Confidentiality Lab)

Windows 10 • 192.168.2.10

Overview Access Settings

Device name	Andrew Workstation
IP address	192.168.2.10
Protocols (ports)	TCP (3389)

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.



Device	Facility	Region	IP
DC_DISPEL_UBUNTU_1	Data Confidentiality Lab	Data Confidentiality	192.168.1.240
DC_HELIX_CENTOS	Data Confidentiality Lab	Data Confidentiality	192.168.1.206
DC_HELIX_UBUNTU	Data Confidentiality Lab	Data Confidentiality	192.168.1.92
DC_INTRANET	Data Confidentiality Lab	Data Confidentiality	192.168.2.40
DC_PRODUCT	Data Confidentiality Lab	Data Confidentiality	169.254.188.53
DC_VICTIM_WIN10_1	Data Confidentiality Lab	Data Confidentiality	192.168.1.93
Andrew Workstation	Data Confidentiality Lab	Data Confidentiality	192.168.2.10

NCCoE / Devices / Test Workstation EVIL-WEB / Access

Test Workstation EVIL-WEB (Data Confidentiality Lab)

192.168.2.90

Overview Access Settings

Andrew

Device access (ACLs) (0)

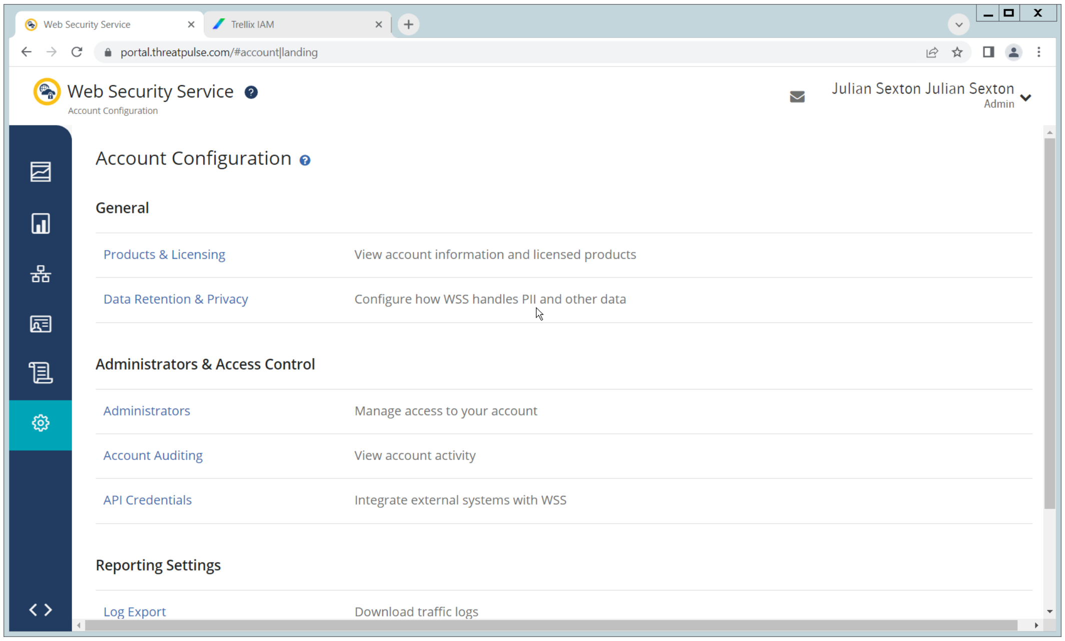
7. If a user is not already a member of the region, click **Members** in the sidebar and click **Invite.** Fill out relevant information for this individual and click **Invite this Member.**

2.9 Integration: FireEye Helix and Symantec SWG

In this integration the output of the web isolation tool, Symantec SWG, will be forwarded to our Security Information and Event Management (SIEM), FireEye Helix. In this guide, we will aim to forward most logs to our SIEM, which can collect, analyze, and report on these logs to better maintain awareness of our systems and provide a single interface for analyzing the health of the system. Logs from SWG will allow us to see statistics on the number of threats that have been blocked, as well as any administrative changes made to the SWG product.

2.9.1 Configure Fireye Helix to Collect Logs from Symantec SWG

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



Account Configuration

General

Products & Licensing	View account information and licensed products
Data Retention & Privacy	Configure how WSS handles PII and other data

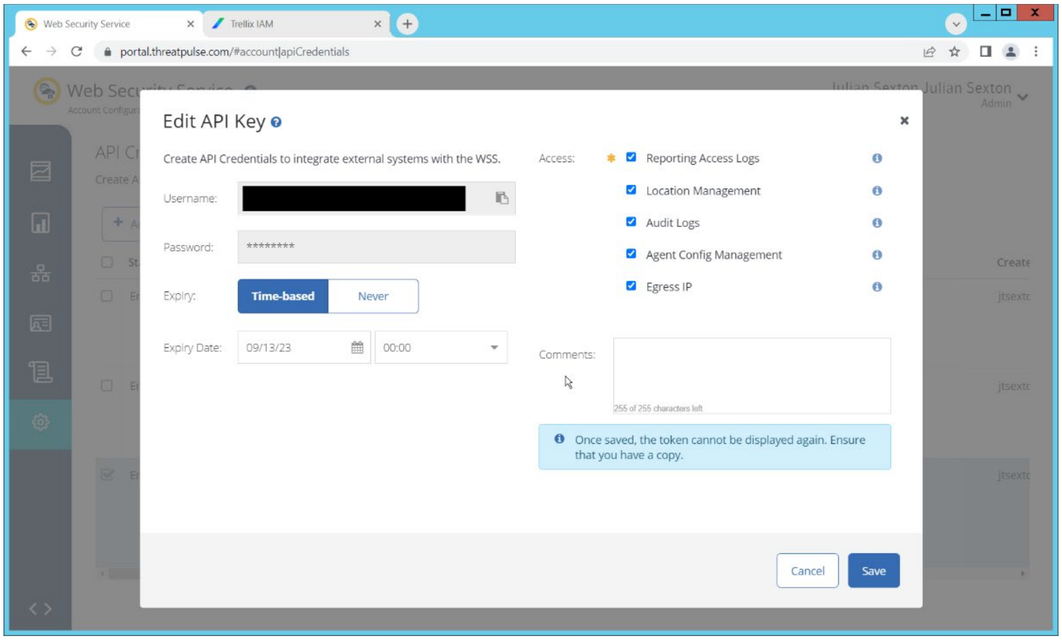
Administrators & Access Control

Administrators	Manage access to your account
Account Auditing	View account activity
API Credentials	Integrate external systems with WSS

Reporting Settings

Log Export	Download traffic logs

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



Edit API Key

Create API Credentials to integrate external systems with the WSS.

Username: [redacted]

Password: ********

Expiry: Time-based | Never

Expiry Date: 09/13/23 00:00

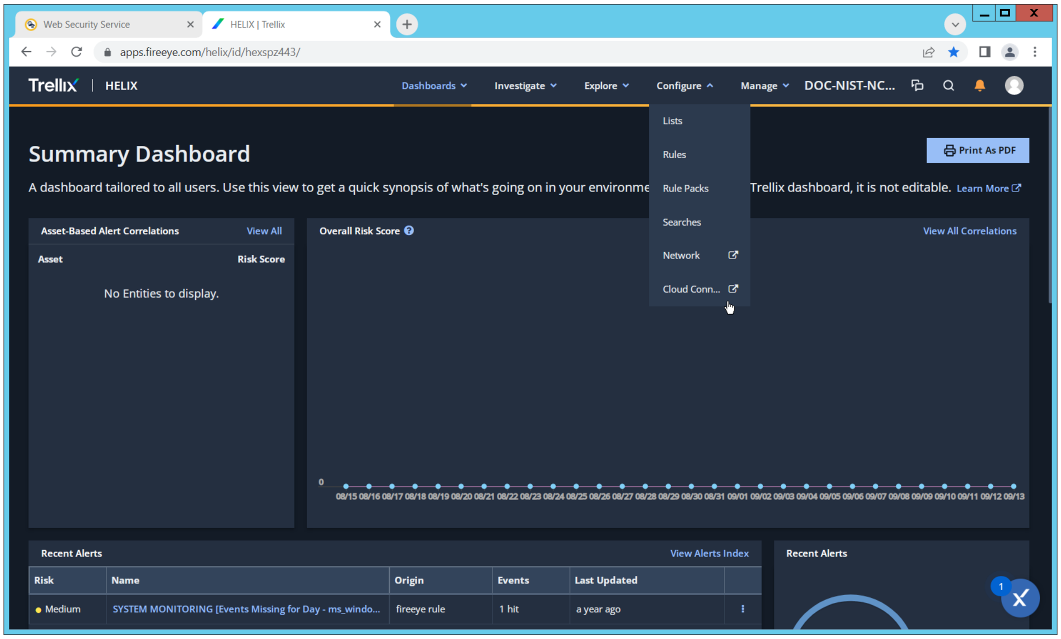
Access:
- ☑ Reporting Access Logs
- ☑ Location Management
- ☑ Audit Logs
- ☑ Agent Config Management
- ☑ Egress IP

Comments:

255 of 255 characters left

Once saved, the token cannot be displayed again. Ensure that you have a copy.

8. Click **Save**.



Summary Dashboard

A dashboard tailored to all users. Use this view to get a quick synopsis of what's going on in your environme Trellix dashboard, it is not editable. Learn More

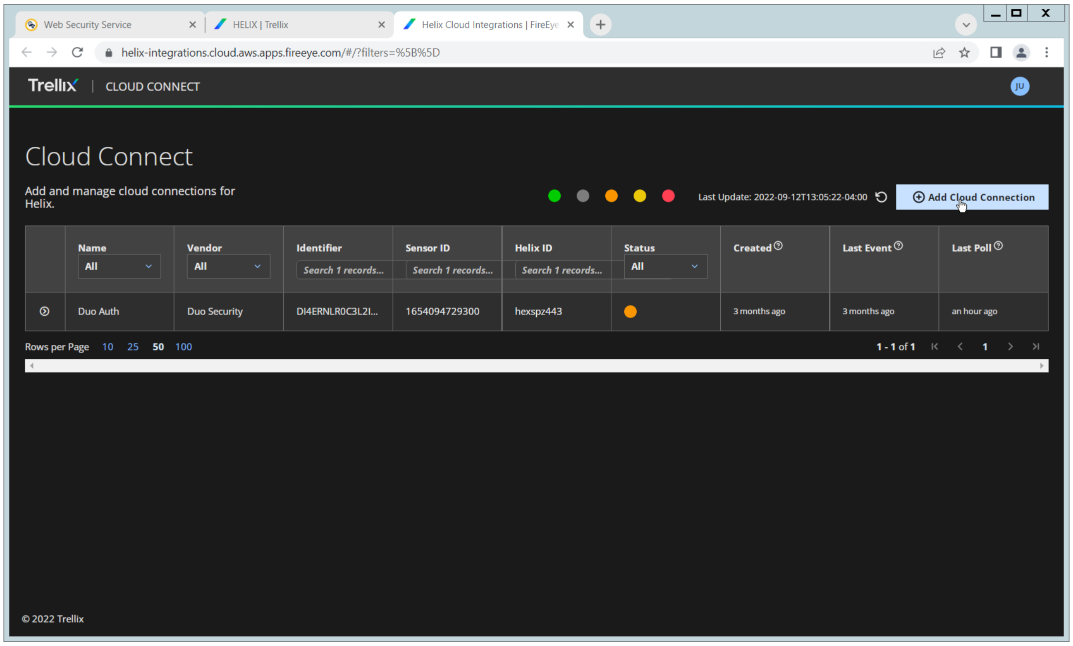
Asset-Based Alert Correlations

Asset	Risk Score
No Entities to display.	

Recent Alerts

Risk	Name	Origin	Events	Last Updated
● Medium	SYSTEM MONITORING [Events Missing for Day - ms_windo...	fireeye rule	1 hit	a year ago

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



Web Security Service
HELIX | Trellix
Helix Cloud Integrations | FireEye
helix-integrations.cloud.aws.apps.fireeye.com/#/?filters=%5B%5D
Trellix
CLOUD CONNECT
JU

Cloud Connect

Add and manage cloud connections for Helix.

Last Update: 2022-09-12T13:05:22-04:00

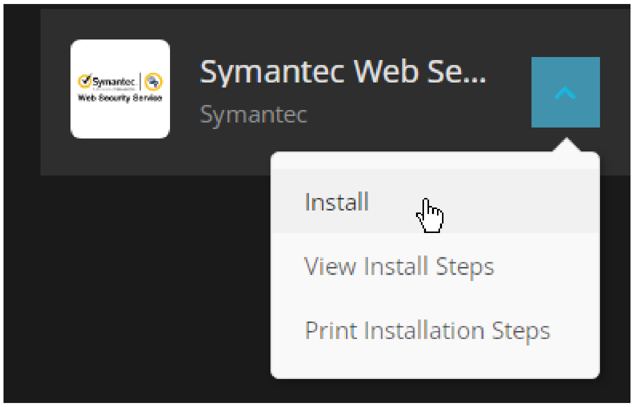
	Name	Vendor	Identifier	Sensor ID	Helix ID	Status	Created	Last Event	Last Poll
	All	All	Search 1 records...	Search 1 records...	Search 1 records...	All			
⦿	Duo Auth	Duo Security	DI4ERNLR0C3L2I...	1654094729300	hexspz443	●	3 months ago	3 months ago	an hour ago

Rows per Page 10 25 50 100 1 - 1 of 1 1

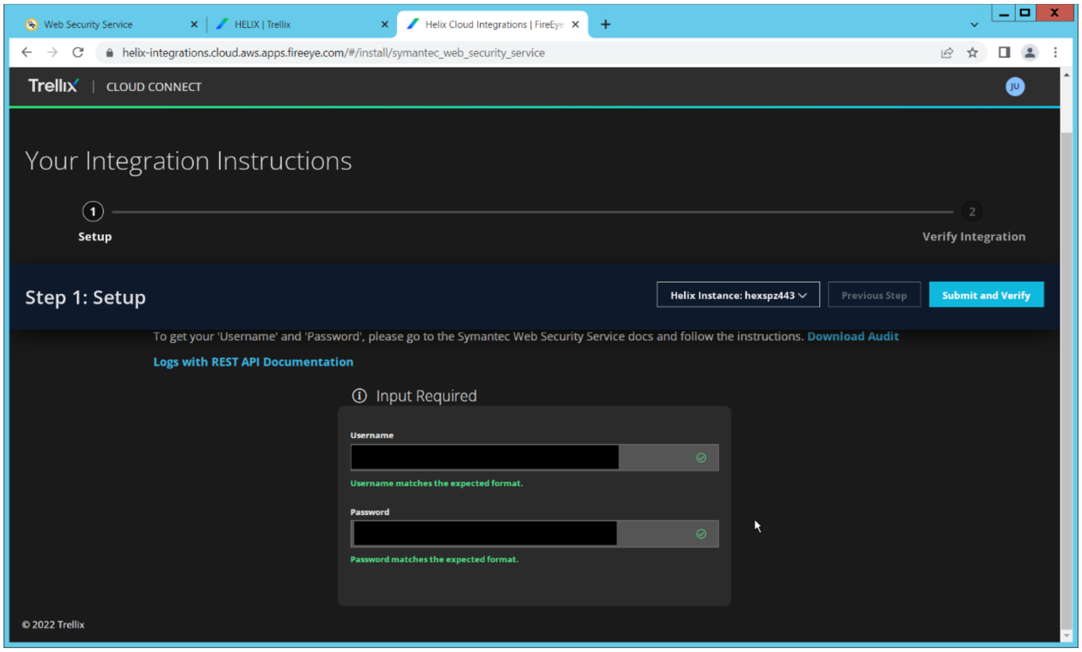
© 2022 Trellix

10. Click Add Cloud Connection.

11. Click the arrow next to Symantec Web Security Service.



12. Click **Install**.


Web Security Service
HELIX | Trellix
Helix Cloud Integrations | FireEye
helix-integrations.cloud.aws.apps.fireeye.com/#/install/symantec_web_security_service
Trellix | CLOUD CONNECT
JU
1
Setup
2
Verify Integration
Helix Instance: hexspz443
Previous Step
Submit and Verify

Your Integration Instructions

Step 1: Setup

To get your 'Username' and 'Password', please go to the Symantec Web Security Service docs and follow the instructions. Download Audit Logs with REST API Documentation

Input Required

Username [redacted]

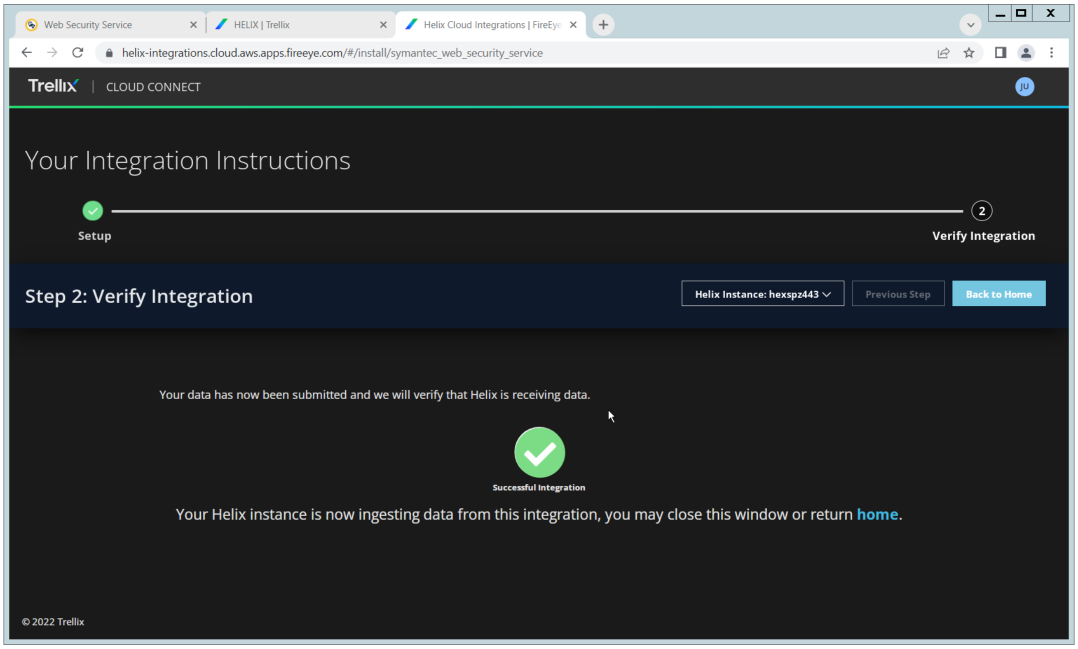
Username matches the expected format.

Password [redacted]

Password matches the expected format.

© 2022 Trellix

13. Enter the username and password from the credential created earlier.


Web Security Service
HELIX | Trellix
Helix Cloud Integrations | FireEye
helix-integrations.cloud.aws.apps.fireeye.com/#/install/symantec_web_security_service
Trellix | CLOUD CONNECT
JU
Setup
2
Verify Integration
Helix Instance: hexspz443
Previous Step
Back to Home

Your Integration Instructions

Step 2: Verify Integration

Your data has now been submitted and we will verify that Helix is receiving data.

Successful Integration

Your Helix instance is now ingesting data from this integration, you may close this window or return home.

© 2022 Trellix

14. Click Submit and Verify.

15. Click **Back to Home**. You will now be able to see events from Symantec SWG in Helix.

2.10 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. Logs from PKWARE PKProtect will allow us to monitor the use of encryption throughout the enterprise, and catch any suspicious decryptions that may indicate a breach. This section assumes the Helix Communications Broker has already been installed.

2.10.1 Configure the Helix Communications Broker

16. On the CentOS system with the Helix Communications Broker installed, run the following commands:

```
> cd /opt/tap-nxlog
> sudo ./setup.sh
```

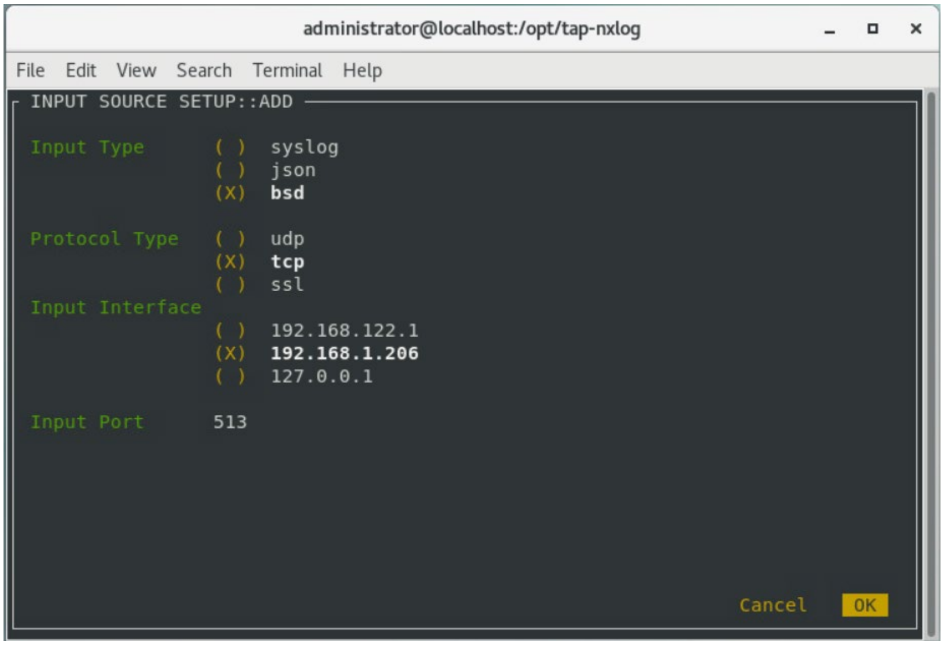
17. Select **Add Routes** and press **Enter**.

18. Select **bsd**.

19. Select **tcp**.

20. Select the IP address of the network interface which should receive logs.

21. Enter 513 for the port.


administrator@localhost:/opt/tap-nxlog
File Edit View Search Terminal Help
Cancel
OK

```
INPUT SOURCE SETUP::ADD

Input Type        ( )  syslog
                  ( )  json
                  (X)  bsd

Protocol Type     ( )  udp
                  (X)  tcp
                  ( )  ssl
Input Interface
                  ( )  192.168.122.1
                  (X)  192.168.1.206
                  ( )  127.0.0.1

Input Port        513
```

22. Select **OK** and press **Enter**.

23. Select **OK** and press **Enter**.

2.10.2 Configure PKWARE PKProtect to Forward Events

1. Navigate to the PKWARE PKProtect web portal.

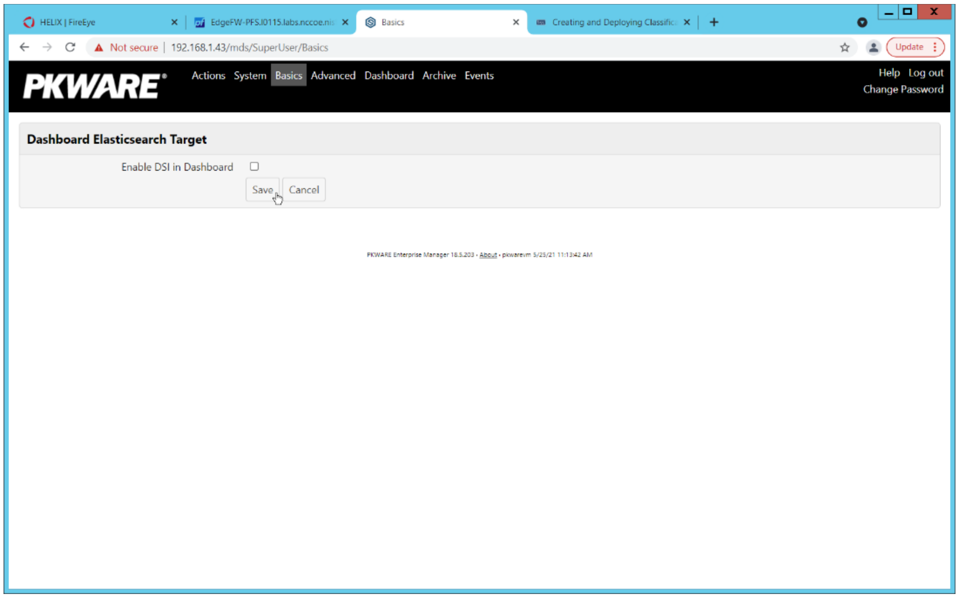
2. Click the **Basics** link at the top of the page.

3. Scroll down to the **Data Security Intelligence** section.

4. Next to **Dashboard Elasticsearch Target**, click **Internal**.

5. Uncheck the box next to **Use Internal Elasticsearch**.

6. Uncheck the box next to **Enable DSI in Dashboard**.


HELIX | FireEye
EdgeFW-PFS.I0115.labs.nccoe.ni
Basics
Creating and Deploying Classific
Not secure | 192.168.1.43/mds/SuperUser/Basics
Update
PKWARE
Actions System Basics Advanced Dashboard Archive Events
Help Log out
Change Password

Dashboard Elasticsearch Target

Enable DSI in Dashboard ☐

Save Cancel

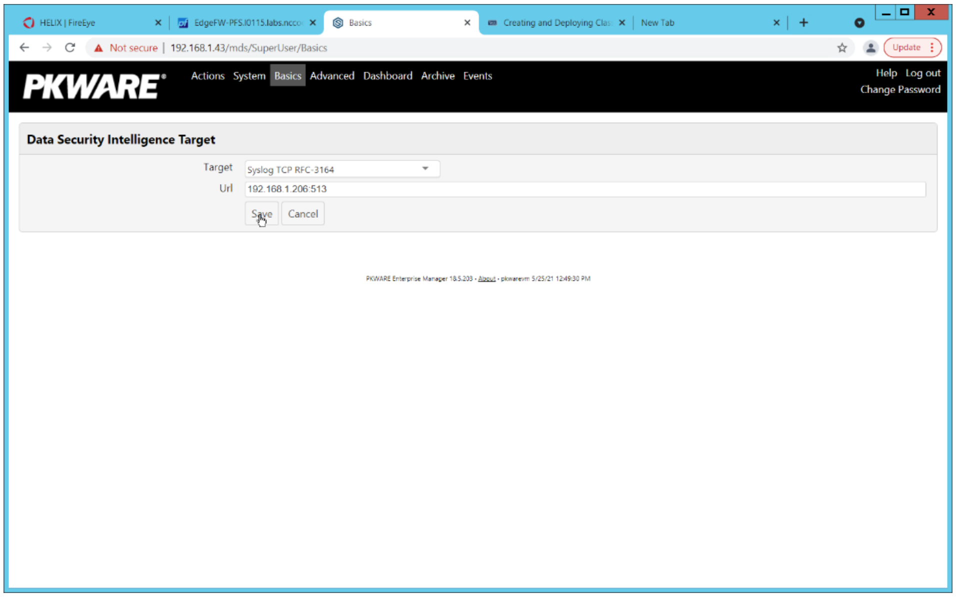
PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 5/25/21 11:13:42 AM

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.


HELIX | FireEye
EdgeFW-PFS.I0115.labs.nccoe
Basics
Creating and Deploying Clas
New Tab
Not secure | 192.168.1.43/mds/SuperUser/Basics
Update
PKWARE
Actions System Basics Advanced Dashboard Archive Events
Help Log out
Change Password

Data Security Intelligence Target

Target: Syslog TCP RFC-3164

Url: 192.168.1.206:513

Save Cancel

PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 5/25/21 12:49:30 PM

11. Click **Save**.

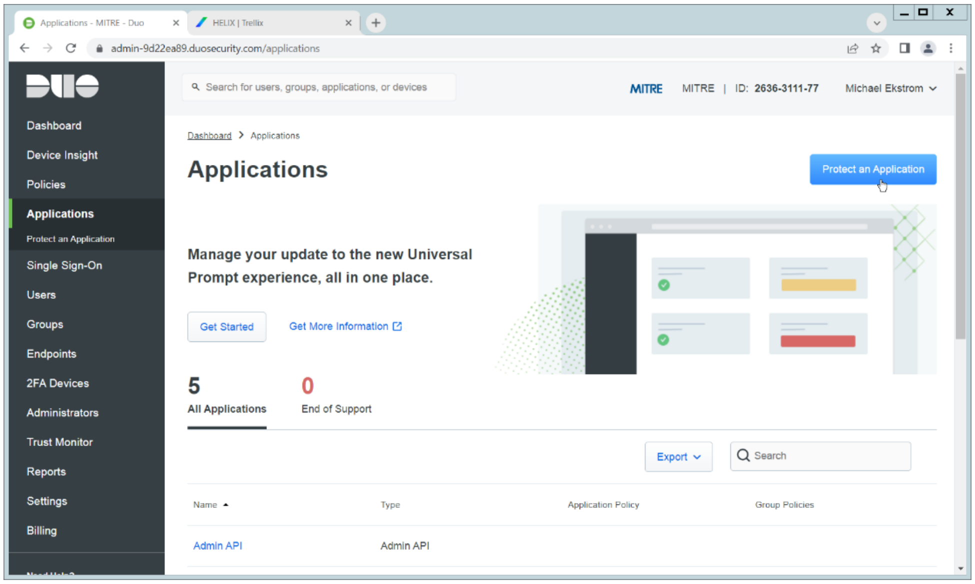
12. Verify that PKWARE logs now show up in Helix.

2.11 Integration: FireEye Helix and Cisco Duo

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

2.11.1 Configure Fireeye Helix to Collect Logs from Cisco Duo

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



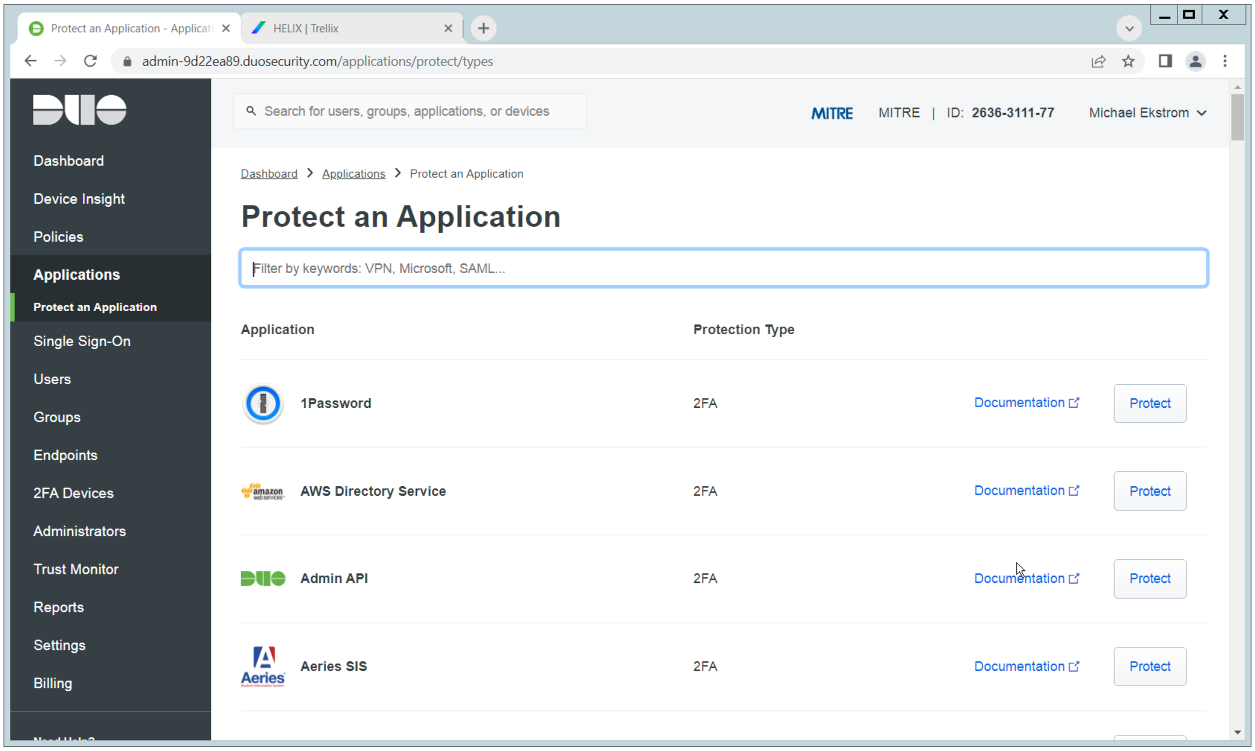
Manage your update to the new Universal Prompt experience, all in one place.

5 All Applications

0 End of Support

Name	Type	Application Policy	Group Policies
Admin API	Admin API		

2. Click Protect an Application.

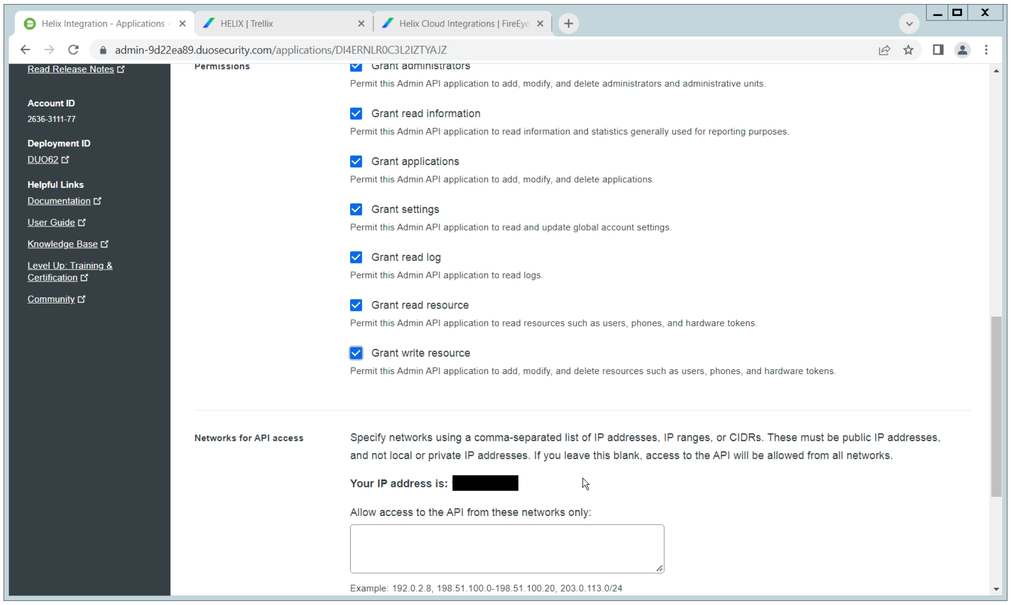


Protect an Application

Filter by keywords: VPN, Microsoft, SAML...

Application	Protection Type		
1Password	2FA	Documentation	Protect
AWS Directory Service	2FA	Documentation	Protect
Admin API	2FA	Documentation	Protect
Aeries SIS	2FA	Documentation	Protect

3. Click Admin API.


Helix Integration - Applications -
HELIX | Trellix
Helix Cloud Integrations | FireEye
admin-9d22ea89.duosecurity.com/applications/DI4ERNLR0C3L2IZTYAJZ
Read Release Notes
Account ID
2636-3111-77
Deployment ID
DUO62
Helpful Links
Documentation
User Guide
Knowledge Base
Level Up: Training & Certification
Community

Permissions

☑ Grant administrators
Permit this Admin API application to add, modify, and delete administrators and administrative units.

☑ Grant read information
Permit this Admin API application to read information and statistics generally used for reporting purposes.

☑ Grant applications
Permit this Admin API application to add, modify, and delete applications.

☑ Grant settings
Permit this Admin API application to read and update global account settings.

☑ Grant read log
Permit this Admin API application to read logs.

☑ Grant read resource
Permit this Admin API application to read resources such as users, phones, and hardware tokens.

☑ Grant write resource
Permit this Admin API application to add, modify, and delete resources such as users, phones, and hardware tokens.

Networks for API access

Specify networks using a comma-separated list of IP addresses, IP ranges, or CIDRs. These must be public IP addresses, and not local or private IP addresses. If you leave this blank, access to the API will be allowed from all networks.

Your IP address is: [redacted]

Allow access to the API from these networks only:

Example: 192.0.2.8, 198.51.100.0-198.51.100.20, 203.0.113.0/24

4. Scroll down and check the boxes next to **Grant administrators**, **Grant read information**, **Grant applications**, **Grant settings**, **Grant read log**, **Grant read resource**, and **Grant write resource**

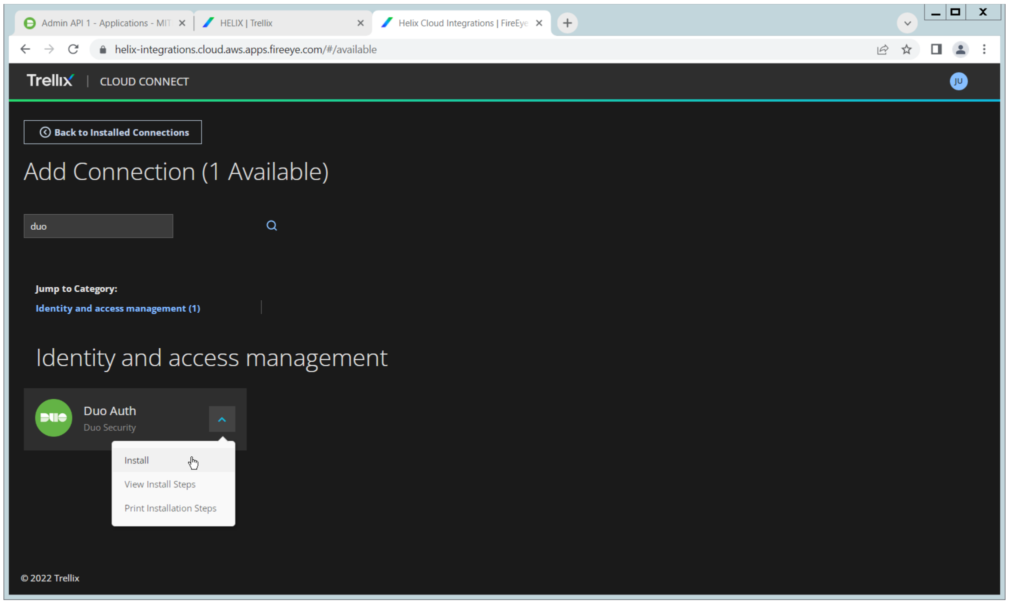
5. Click **Save**.

6. Login to the Helix dashboard.

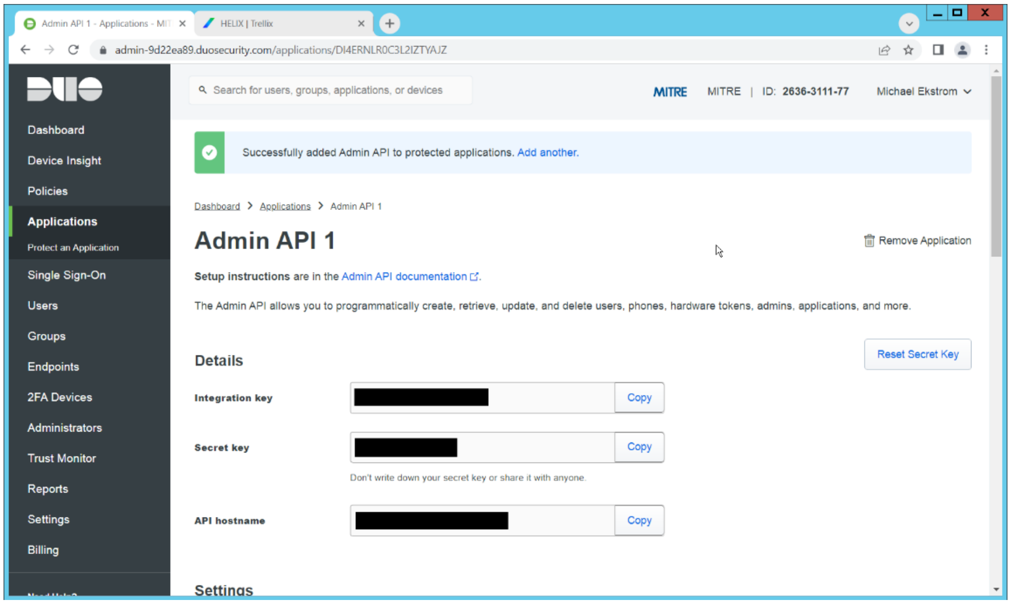
7. Navigate to **Configure** > **Cloud Connect**.

8. Click **See Available Connections**.

9. Type “Duo” in the Search box.


Admin API 1 - Applications - MIT
HELIX | Trellix
Helix Cloud Integrations | FireEye
helix-integrations.cloud.aws.apps.fireeye.com/#/available
Trellix | CLOUD CONNECT
Back to Installed Connections
Add Connection (1 Available)
duo
Jump to Category:
Identity and access management (1)
Identity and access management
Duo Auth
Duo Security
Install
View Install Steps
Print Installation Steps
© 2022 Trellix

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



Successfully added Admin API to protected applications. Add another.

Admin API 1

Setup instructions are in the Admin API documentation.

The Admin API allows you to programmatically create, retrieve, update, and delete users, phones, hardware tokens, admins, applications, and more.

Details

Integration key [redacted]

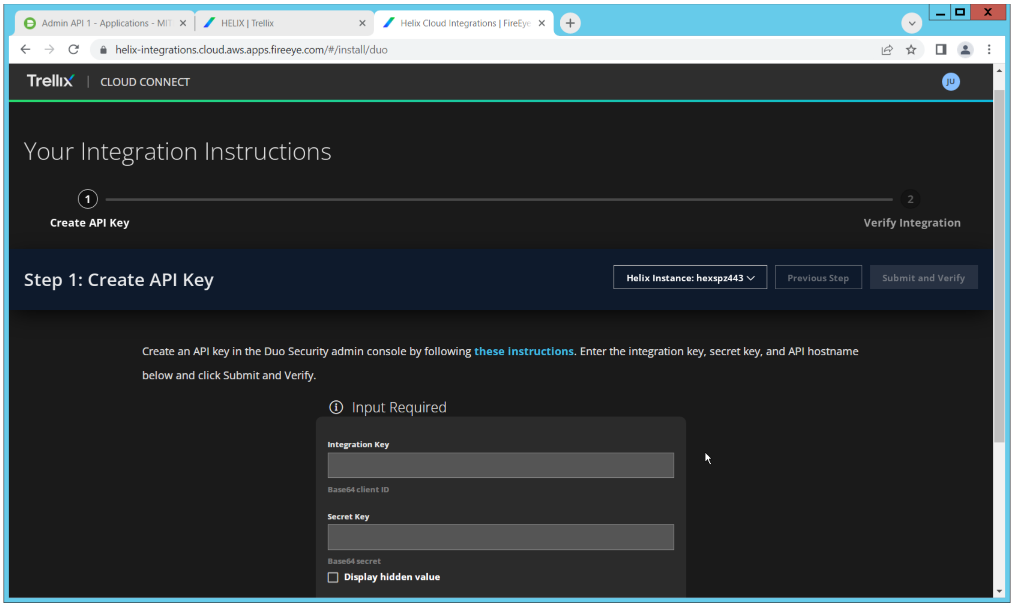
Secret key [redacted]

Don't write down your secret key or share it with anyone.

API hostname [redacted]

Settings

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



helix-integrations.cloud.aws.apps.fireeye.com/#/install/duo

Your Integration Instructions

1 Create API Key — 2 Verify Integration

Step 1: Create API Key

Helix Instance: hexspz443 | Previous Step | Submit and Verify

Create an API key in the Duo Security admin console by following **these instructions**. Enter the integration key, secret key, and API hostname below and click Submit and Verify.

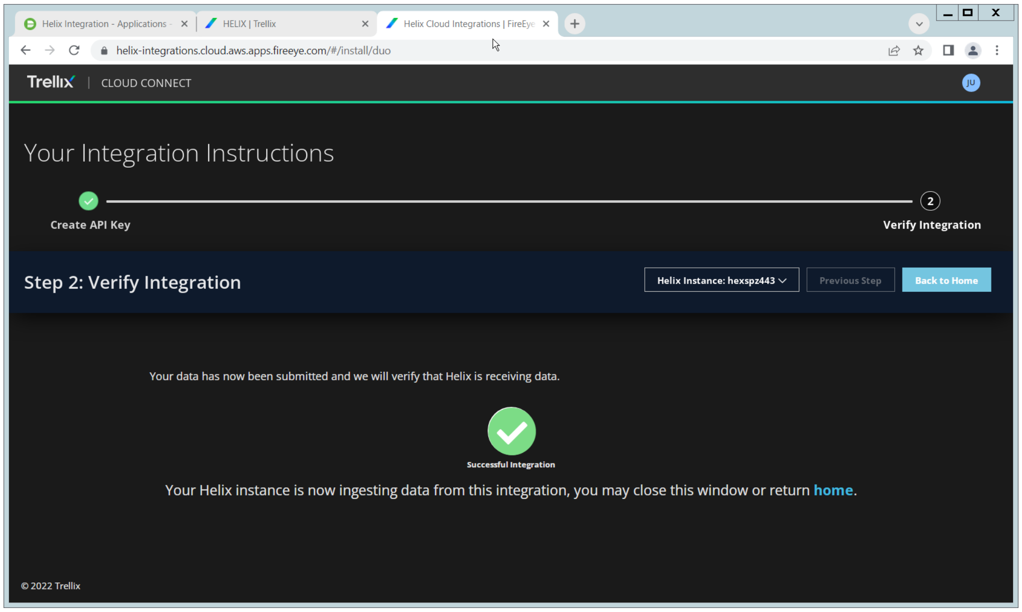
Input Required

Integration Key: Base64 client ID

Secret Key: Base64 secret

□ Display hidden value

12. Click Submit and Verify.



helix-integrations.cloud.aws.apps.fireeye.com/#/install/duo

Your Integration Instructions

Create API Key — 2 Verify Integration

Step 2: Verify Integration

Helix Instance: hexspz443 | Previous Step | Back to Home

Your data has now been submitted and we will verify that Helix is receiving data.

Successful Integration

Your Helix instance is now ingesting data from this integration, you may close this window or return **home**.

© 2022 Trellix

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

2.12 Integration: FireEye Helix and QCOR ForceField

In this integration, we will configure the collection of logs from ForceField, our database encryption solution, into FireEye Helix. Detailed logs describing encryption and decryption are useful for determining how much of an enterprise is encrypted, and statistics and records in this area can prepare the organization for the event of a breach. For the purposes of this guide, we will assume ForceField is running on a Windows Server, and we would like to transfer files from this server to a Linux server. If you are using a Linux server for ForceField, you can skip to the configuration of rsyslog to forward logs directly to the Helix Comm Broker.

2.12.1Configure an Secure File Transfer Protocol (SFTP) server on Windows

In this section, we will configure an SFTP server on the Windows system to allow for encrypted, automated download of Forcefield's logs onto a Linux server. We have specifically elected not to use Windows Server Message Block (SMB) for this scenario because we would like to demonstrate an encrypted transfer of logs from Windows to Linux. We chose SFTP over FTPS because automation of File Transfer Protocol Secure (FTPS) would at some point require a plaintext password, while SFTP can default to the system's Secure Shell (SSH) capabilities.

Once on Linux, rsyslog can be configured to use TLS for encrypted transfer according to the needs of the organization.

1. Download OpenSSH from here (https://github.com/PowerShell/Win32-OpenSSH/releases). During the creation of this guide, version V8.9.1.0p1-Beta was used.

2. Extract to `C:\Program Files\OpenSSH`.

3. In a Powershell window, navigate to the folder you extracted it to, and run the following command to install the server.

   ```
   powershell.exe -ExecutionPolicy Bypass -File ./install-sshd.ps1
   ```

4. Run the following command to open the firewall port for OpenSSH.

   ```
   Run New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH SSH Server' -Enabled
   True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22 -Program
   "C:\Windows\System32\OpenSSH\sshd.exe"
   ```

5. Open **services.msc** and start the **OpenSSH SSH server**.

6. Create a file called **authorized_keys** in **C:\Users\<Your Username>\.ssh**. If needed, create the **.ssh** folder (Windows will not allow you to create it by default – naming the folder **.ssh.** will allow you to bypass this restriction.)

7. Generate a key using **./ssh-keygen**. Copy the contents of the generated public key (.pub file) into the **authorized_keys** file created earlier. The private key should be placed in the **~/.ssh** folder on the Linux machine.

8. Right click the **authorized_keys** file and click **Properties**.

9. Click **Disable Inheritance**.

10. Select **Convert inherited permissions into explicit permissions on this object**.

11. Using the remove button, remove all accounts other than SYSTEM from the list. Ensure that the SYSTEM account has full control.

12. Under **C:\ProgramData\ssh**, open **sshd_config**.

13. Comment out these lines by adding '#' characters before each line, like so:

    ```
    #Match Group administrators

    #      AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
    ```

14. Add the following lines to the **sshd_config** file to ensure that RSA public key authentication is allowed.

```
PubkeyAuthentication yes

PubkeyAcceptedKeyTypes=+ssh-rsa
```

15. Add the directory **C:\Program Files\OpenSSH** to the system path – this is necessary so that the server can find the sftp-server.exe file.

16. Add the following lines to **sshd_config** file to configure the SFTP server.

```
ForceCommand internal-sftp

ChrootDirectory C:\GreenTec\ForceField\log
```

17. Alternatively, if it's preferable to set the root directory somewhere else and move the log file, you can also do that. To edit the log file location, simply open **C:\GreenTec\Forcefield\wfs.conf** and change **Logpath** to a different directory, and update **ChrootDirectory** to point to that.

18. After doing this, you should be able to authenticate over SSH to the server. If the authentication fails, you can check the logs in Event Viewer on the server, under **Applications and Services Logs > OpenSSH > Operational** to see the reason for the failure.

2.12.2 Configure the Linux Machine to Download and Send Logs to the Helix Communications Broker

19. On the Linux server, we can use sftp to download the file. Ensure that you replace the username and hostname with the username and hostname of your actual SSH server.

```
sftp administrator@forcefield.dc.ipdrr:/ForceField.log /tmp/ForceField.log
```

20. For automation purposes, we can use cron jobs to automatically download this file at regular intervals. Use crontab to edit the list of cron jobs.

```
Crontab -e
```

21. Enter the interval and command for sftp in the crontab file. The following line will download the log file once an hour. Ensure that you replace the username and hostname with the username and hostname of your actual SSH server.

```
0 * * * * sftp administrator@forcefield.dc.ipdrr:/ForceField.log
/tmp/ForceField.log
```

22. Next, we will use **rsyslog** to forward this log file to the Helix Comm Broker.

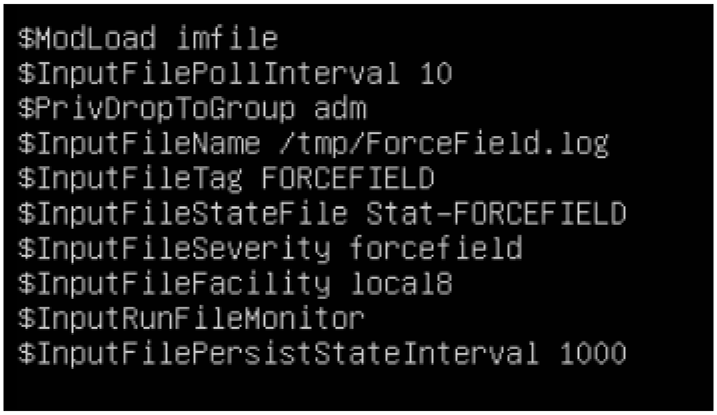
23. Open **/etc/rsyslog.conf**, and add the following line, using the IP and port of the Helix Comm Broker. (Note that putting a single '@' symbol here indicates UDP. Use two, such as '@@' for TCP.)

```
*.* @192.168.1.206:514
```

24. Create a file **/etc/rsyslog.d/forcefield.conf** and enter the following lines in it.

```
sudo nano /etc/rsyslog.d/forcefield.conf
$ModLoad imfile
$InputFilePollInterval 10
```

```
$PrivDropToGroup adm
$InputFileName /tmp/ForceField.log
$InputFileTag FORCEFIELD
$InputFileStateFile Stat-FORCEFIELD
$InputFileFacility local8
$InputRunFileMonitor
$InputFilePersistStateInterval 1000
```



```
$ModLoad imfile
$InputFilePollInterval 10
$PrivDropToGroup adm
$InputFileName /tmp/ForceField.log
$InputFileTag FORCEFIELD
$InputFileStateFile Stat-FORCEFIELD
$InputFileSeverity forcefield
$InputFileFacility local8
$InputRunFileMonitor
$InputFilePersistStateInterval 1000
```

25. Restart rsyslog.

```
sudo service rsyslog restart
```

2.13 Integration: FireEye Helix and Dispel

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

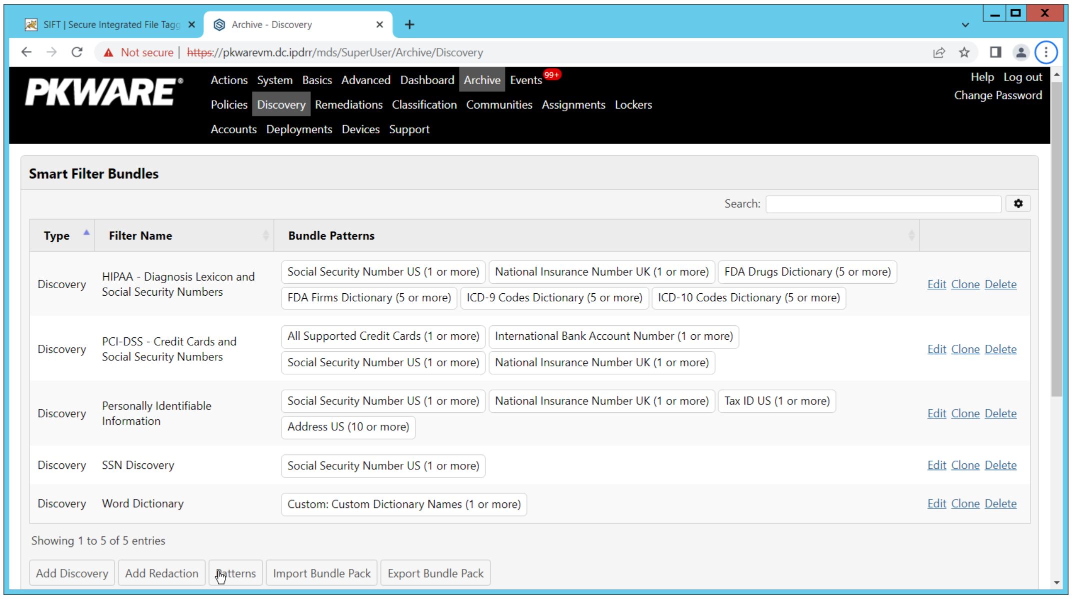
2.14 Integration: Avrio SIFT and PKWARE PKProtect

When used together, SIFT and PKProtect can protect sensitive data accidentally dropped into public shares on the enterprise. In Section 2.6, we detail how to configure SIFT to detect sensitive data in a Windows Share and move it to a location designated for sensitive information. Now, we will demonstrate how to ensure that location is protected by PKProtect, which will automatically encrypt the data.

2.14.1 Configuring PKWARE PKProtect

1. Navigate to the PKProtect dashboard and login.

2. Navigate to **Archive > Discovery**.


SIFT | Secure Integrated File Tagg
Archive - Discovery
Not secure | https://pkwarevm.dc.ipdrr/mds/SuperUser/Archive/Discovery
PKWARE
Actions System Basics Advanced Dashboard Archive Events 99+
Policies Discovery Remediations Classification Communities Assignments Lockers
Accounts Deployments Devices Support
Help Log out
Change Password

Smart Filter Bundles

Search:

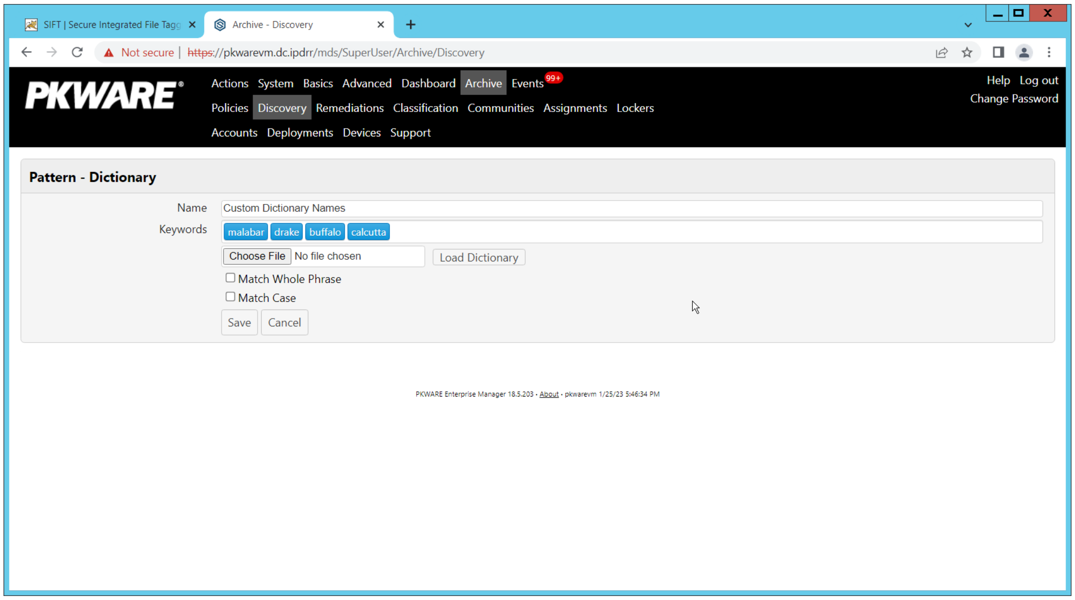
Type	Filter Name	Bundle Patterns	
Discovery	HIPAA - Diagnosis Lexicon and Social Security Numbers	Social Security Number US (1 or more) National Insurance Number UK (1 or more) FDA Drugs Dictionary (5 or more) FDA Firms Dictionary (5 or more) ICD-9 Codes Dictionary (5 or more) ICD-10 Codes Dictionary (5 or more)	Edit Clone Delete
Discovery	PCI-DSS - Credit Cards and Social Security Numbers	All Supported Credit Cards (1 or more) International Bank Account Number (1 or more) Social Security Number US (1 or more) National Insurance Number UK (1 or more)	Edit Clone Delete
Discovery	Personally Identifiable Information	Social Security Number US (1 or more) National Insurance Number UK (1 or more) Tax ID US (1 or more) Address US (10 or more)	Edit Clone Delete
Discovery	SSN Discovery	Social Security Number US (1 or more)	Edit Clone Delete
Discovery	Word Dictionary	Custom: Custom Dictionary Names (1 or more)	Edit Clone Delete

Showing 1 to 5 of 5 entries

3. Click **Pattern – Dictionary**.

4. Enter a name for these patterns in the **Name** field.

5. Enter keywords to match in the **Keywords** field.


SIFT | Secure Integrated File Tagg
Archive - Discovery
Not secure | https://pkwarevm.dc.ipdrr/mds/SuperUser/Archive/Discovery
PKWARE
Actions System Basics Advanced Dashboard Archive Events 99+
Policies Discovery Remediations Classification Communities Assignments Lockers
Accounts Deployments Devices Support
Help Log out
Change Password

Pattern - Dictionary

Name: Custom Dictionary Names

Keywords: malabar drake buffalo calcutta

Choose File No file chosen
Load Dictionary

□ Match Whole Phrase

□ Match Case

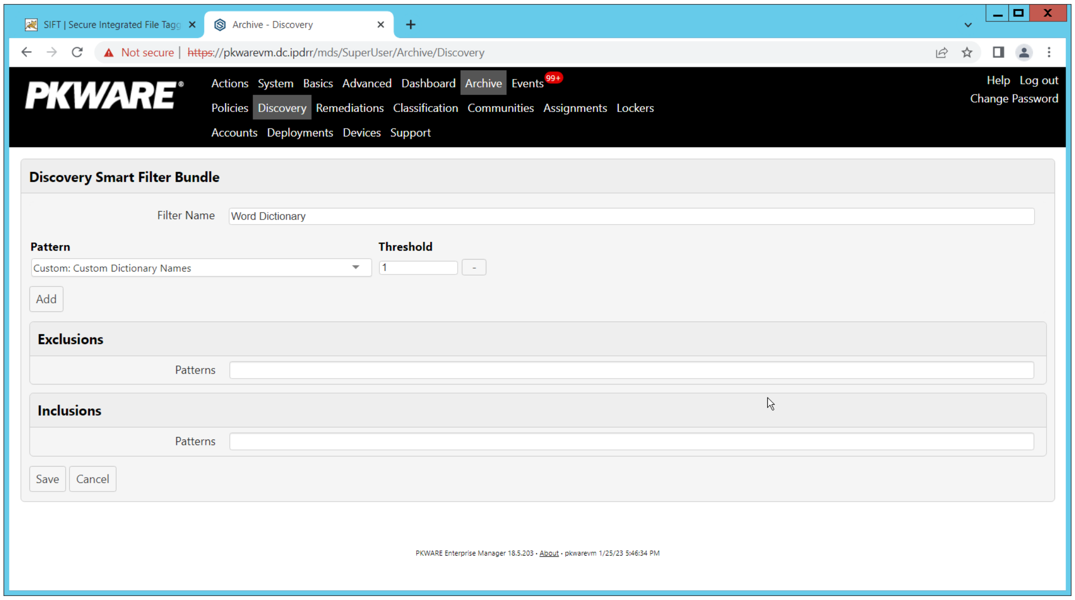
Save
Cancel
PKWARE Enterprise Manager 18.5.203 - About - pkwarevm 1/25/23 5:46:34 PM

6. Click **Save**.

7. Click **Add Discovery**.

8. Under **Pattern**, select the name of the **Pattern** you just created.

9. For **Threshold**, enter the number of matches of this pattern needed to consider the file sensitive.


SIFT | Secure Integrated File Tagg
Archive - Discovery
Not secure | https://pkwarevm.dc.ipdrr/mds/SuperUser/Archive/Discovery
PKWARE
Actions System Basics Advanced Dashboard Archive Events 99+
Policies Discovery Remediations Classification Communities Assignments Lockers
Accounts Deployments Devices Support
Help Log out
Change Password
Add
Save Cancel
PKWARE Enterprise Manager 18.5.203 - About - pkwarevm 1/25/23 5:46:34 PM

Discovery Smart Filter Bundle

Filter Name: Word Dictionary

Pattern: Custom: Custom Dictionary Names

Threshold: 1

Exclusions

Patterns:

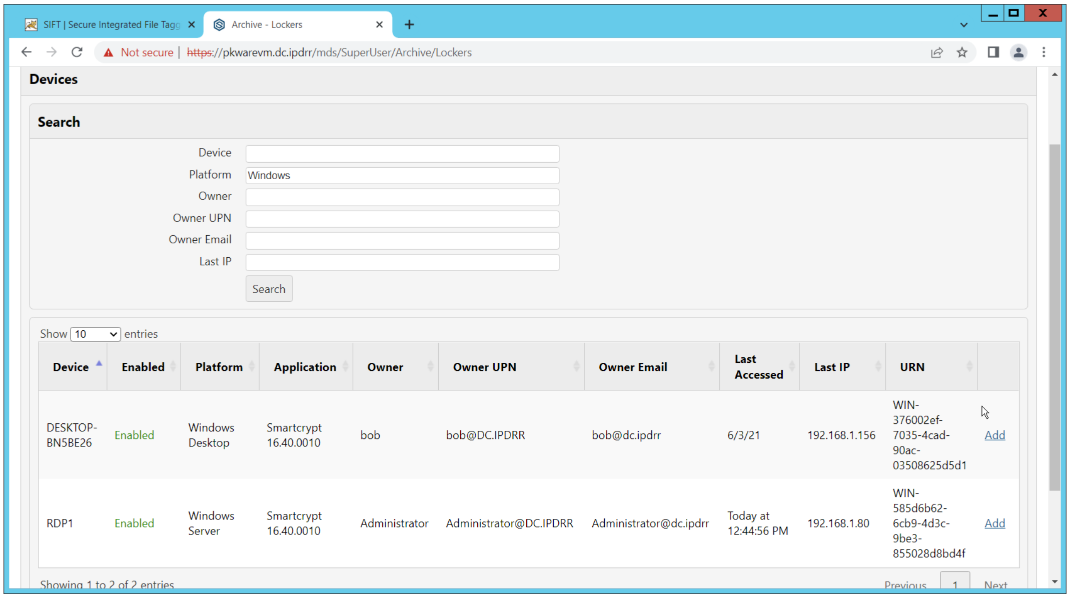
Inclusions

Patterns:

10. Click **Save**.

11. Navigate to **Archive** > **Lockers**.

12. Ensure that a PKWARE client is installed on the device which will be monitored for encryption. The device should show up in the list. If it doesn't you can search for the device and select it from the list.


SIFT | Secure Integrated File Tagg
Archive - Lockers
Not secure | https://pkwarevm.dc.ipdrr/mds/SuperUser/Archive/Lockers
Search
Show 10 entries
Showing 1 to 2 of 2 entries
Previous 1 Next

Devices

Search

Device:
Platform: Windows
Owner:
Owner UPN:
Owner Email:
Last IP:

Device	Enabled	Platform	Application	Owner	Owner UPN	Owner Email	Last Accessed	Last IP	URN	
DESKTOP-BN5BE26	Enabled	Windows Desktop	Smartcrypt 16.40.0010	bob	bob@DC.IPDRR	bob@dc.ipdrr	6/3/21	192.168.1.156	WIN-376002ef-7035-4cad-90ac-03508625d5d1	Add
RDP1	Enabled	Windows Server	Smartcrypt 16.40.0010	Administrator	Administrator@DC.IPDRR	Administrator@dc.ipdrr	Today at 12:44:56 PM	192.168.1.80	WIN-585d6b62-6cb9-4d3c-9be3-855028d8bd4f	Add

13. Click **Add** on the device you wish to add a locker for.

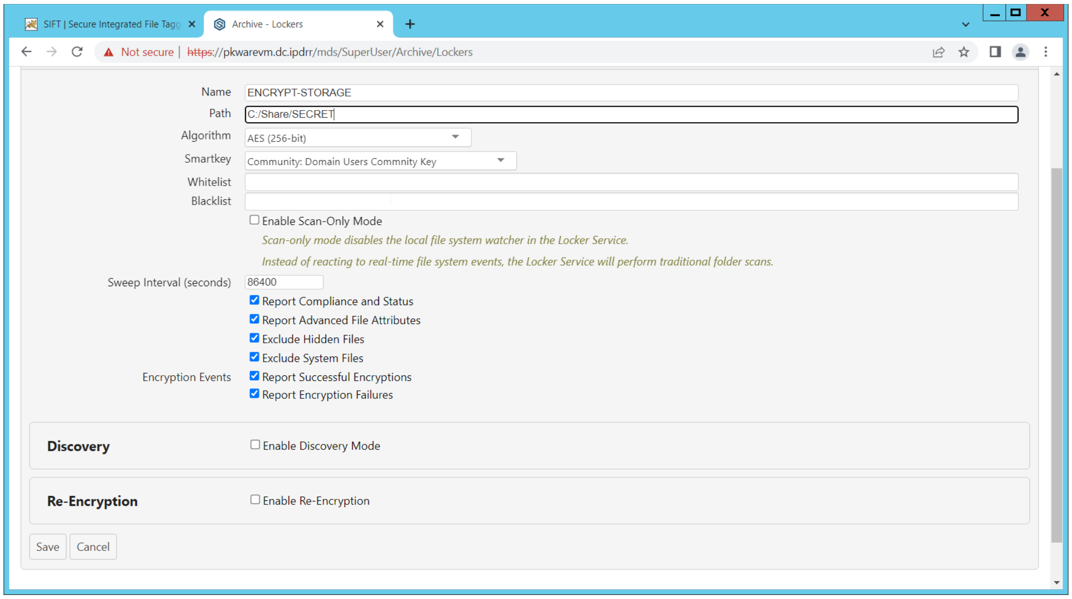
14. Enter a **Name** for the locker.

15. Enter the **path** to the protected folder.

16. Select **AES 256** for the **Algorithm**.

17. Select the PKWARE Smartkey to use.

18. Check all the boxes next to **Encryption Events**.


SIFT | Secure Integrated File Tagg
Archive - Lockers
Not secure | https://pkwarevm.dc.ipdrr/mds/SuperUser/Archive/Lockers

Name: ENCRYPT-STORAGE
Path: C:/Share/SECRET
Algorithm: AES (256-bit)
Smartkey: Community: Domain Users Commnity Key
Whitelist:
Blacklist:
☐ Enable Scan-Only Mode
Scan-only mode disables the local file system watcher in the Locker Service.
Instead of reacting to real-time file system events, the Locker Service will perform traditional folder scans.
Sweep Interval (seconds): 86400
☑ Report Compliance and Status
☑ Report Advanced File Attributes
☑ Exclude Hidden Files
☑ Exclude System Files
Encryption Events: ☑ Report Successful Encryptions
☑ Report Encryption Failures

Discovery ☐ Enable Discovery Mode

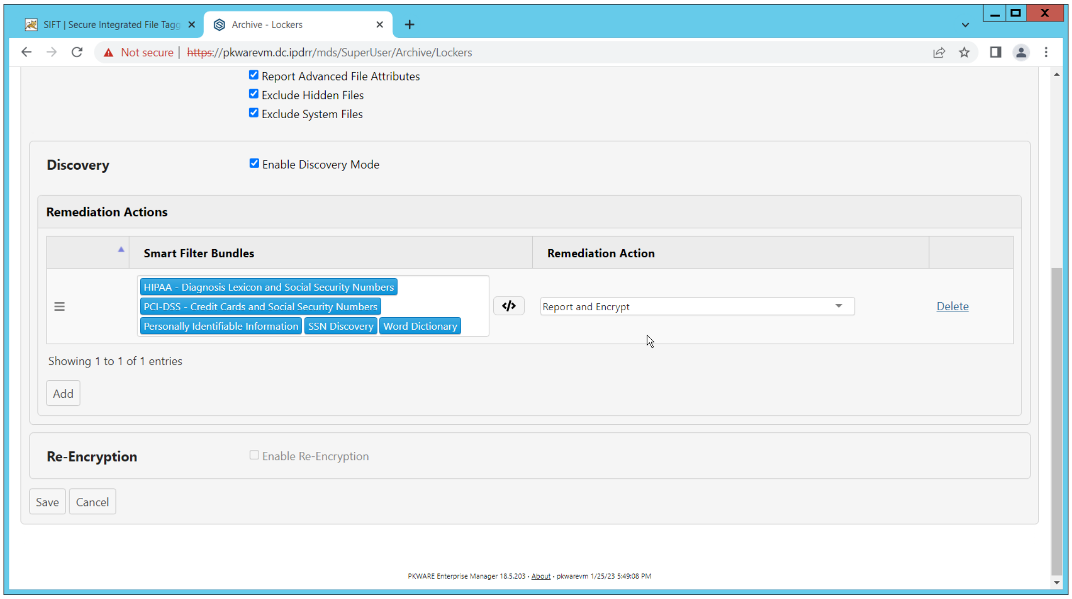
Re-Encryption ☐ Enable Re-Encryption

Save | Cancel

19. Check the box next to **Enable Discovery Mode**.

20. Add the relevant rules to the **Smart Filter Bundles** box.

21. Select **Report and Encrypt** for **Remediation Action**.


SIFT | Secure Integrated File Tagg
Archive - Lockers
Not secure | https://pkwarevm.dc.ipdrr/mds/SuperUser/Archive/Lockers

☑ Report Advanced File Attributes
☑ Exclude Hidden Files
☑ Exclude System Files

Discovery ☑ Enable Discovery Mode

Remediation Actions

	Smart Filter Bundles		Remediation Action	
≡	HIPAA - Diagnosis Lexicon and Social Security Numbers PCI-DSS - Credit Cards and Social Security Numbers Personally Identifiable Information SSN Discovery Word Dictionary	</>	Report and Encrypt	Delete

Showing 1 to 1 of 1 entries

Add

Re-Encryption ☐ Enable Re-Encryption

Save | Cancel

PKWARE Enterprise Manager 18.5.203 · About · pkwarevm 1/25/23 5:49:08 PM

22. Click **Save**.

23. Now the folder on the device you selected will be monitored, and files which match the selected rules will be encrypted automatically.

2.15 Integration: Dispel and Cisco Duo

In this build, Dispel acts as an intermediary between the user and enterprise systems, by providing temporary remote desktops with access to 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 Section 2.7) 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

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

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