NIST SPECIAL PUBLICATION 1800-28C

Data Confidentiality:
Identifying and Protecting Data Against Data Breaches

Volume C:
How-To Guides

William Fisher
National Cybersecurity Center of Excellence
NIST

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

December 2023

DRAFT

This publication is available free of charge from
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, (December 2023), CODEN: NSPUE2

FEEDBACK

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

Comments on this publication may be submitted to: ds-nccoe@nist.gov

Public comment period: December 13, 2023 through January 15, 2024

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

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

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

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

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.

CALL FOR PATENT CLAIMS

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

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

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

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

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

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

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

Such statements should be addressed to: ds-nccoe@nist.gov

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

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. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to 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.

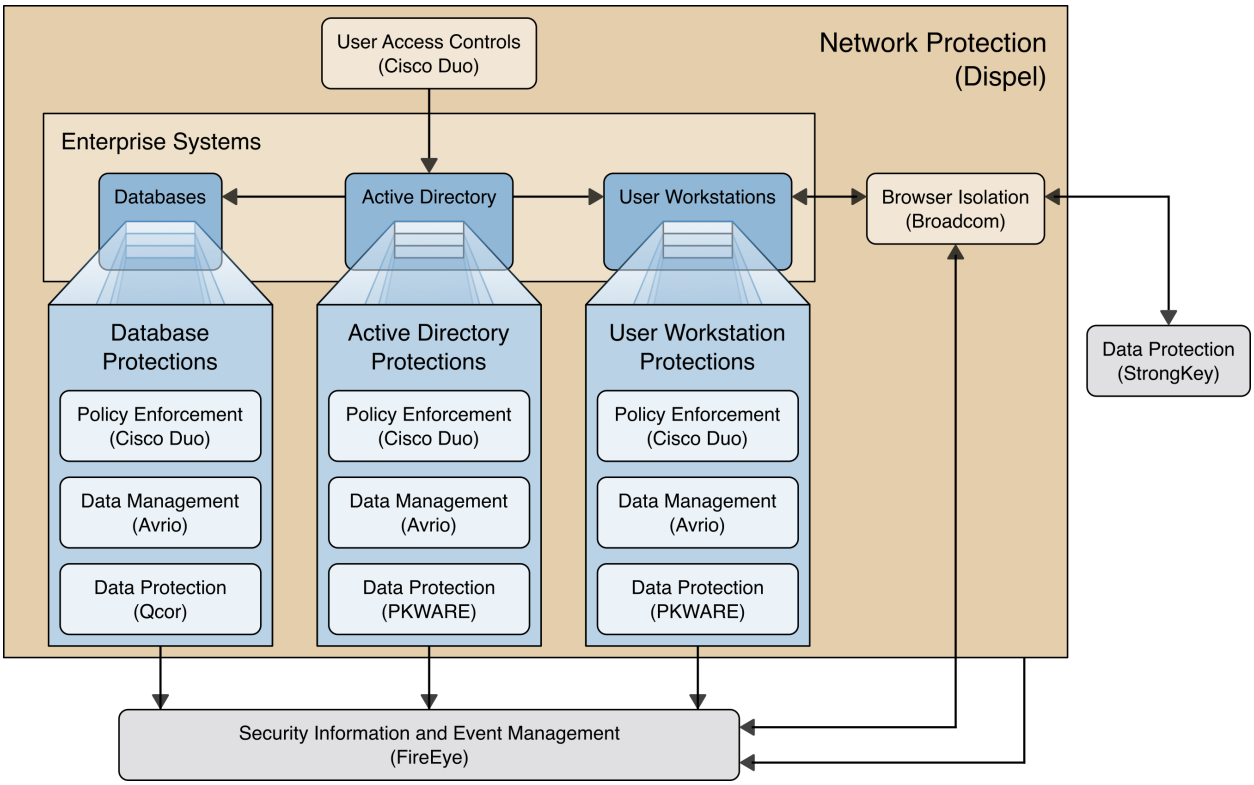
1.3 Typographic Conventions

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.



- **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.

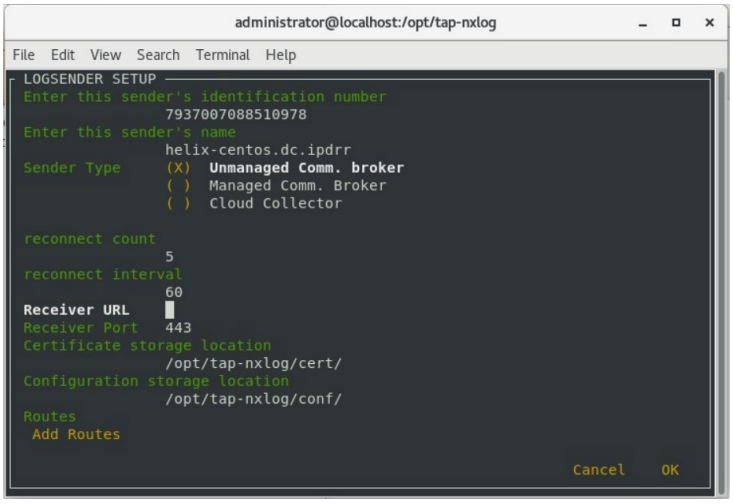
2.1 FireEye Helix

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.

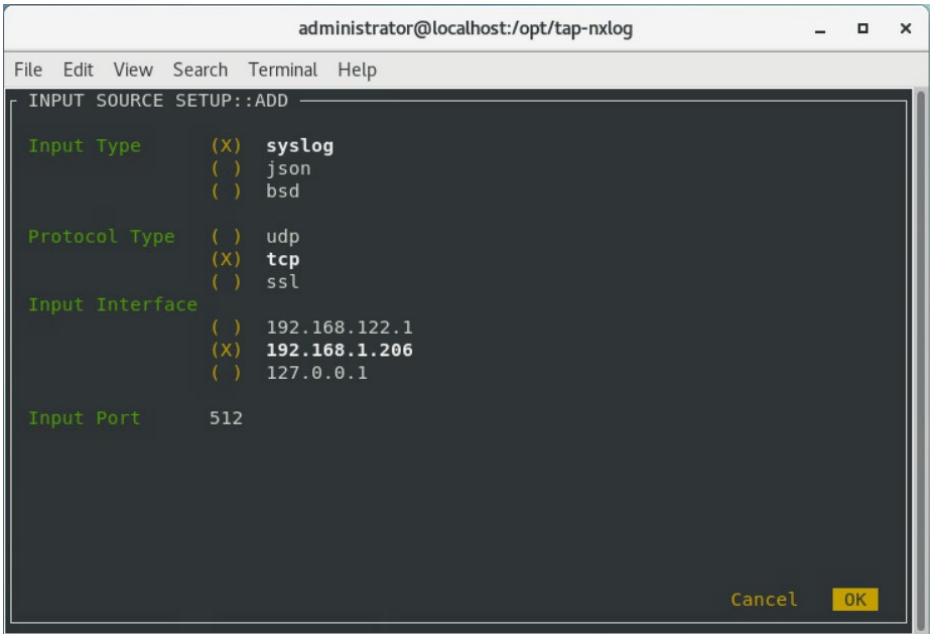
In this setup, we detail the installation of a communications broker which will be used to collect logs from the enterprise and forward them to the cloud deployment. This installation took place on a CentOS 7 Virtual Machine.

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.



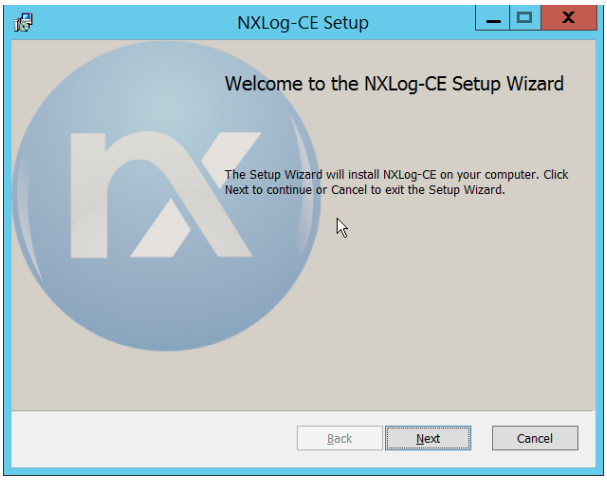
15. Select **Add Routes** and press **Enter**.
16. Select **syslog**.
17. Select **tcp**.
18. Select the IP address of the machine where logs should be sent.
19. Enter 512 for the port number where logs should be sent.



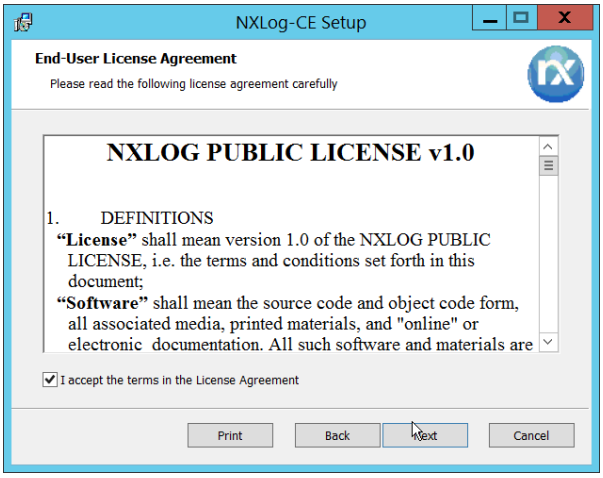
20. Select **OK** and press **Enter**.
21. Review the configuration, then select **OK** and press **Enter**.

Forwarding Event Logs from Windows 2012 R2

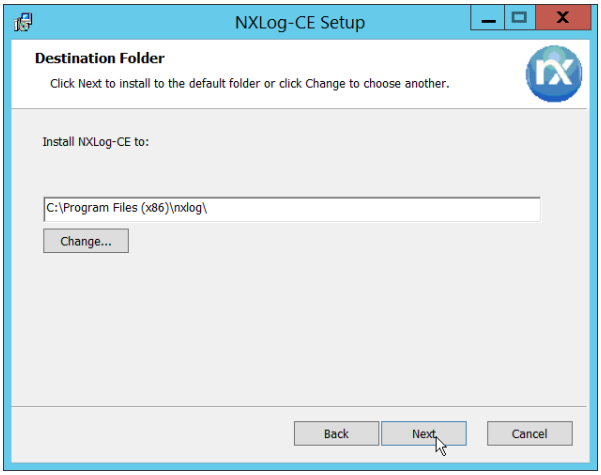
22. Acquire **nxlog-ce-2.10.2150.msi** from http://nxlog.org/products/nxlog-community-edition/download.
23. Run **nxlog-ce-2.10.2150.msi**.



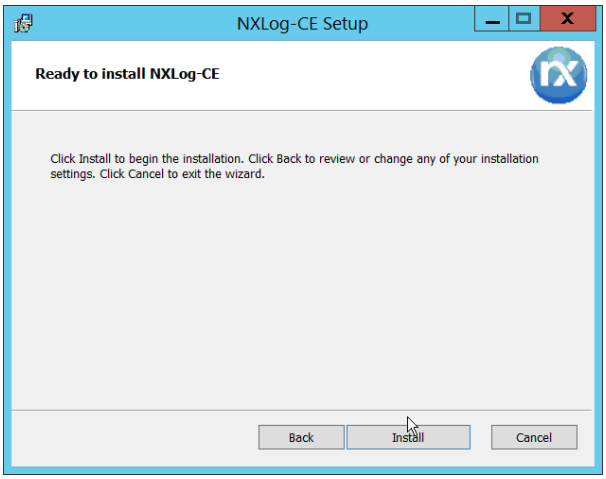
24. Click **Next**.
25. Check the box next to **I accept the terms in the License Agreement**.



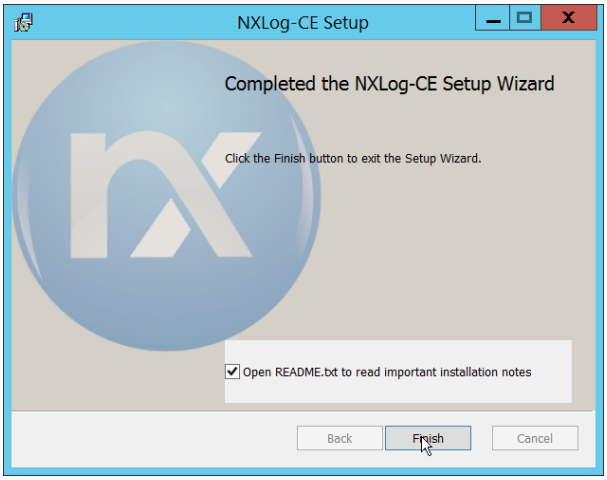
26. Click **Next**.



27. Click **Next**.



299 28. Click **Install**.



300 29. Click **Finish**.

301 30. Navigate to *C:\Program Files (x86)\nxlog\conf* and open **nxlog.conf**.

302 31. Copy the **nxlog.conf** file provided below.

```
Panic Soft
#NoFreeOnExit TRUE

define ROOT     C:\Program Files (x86)\nxlog
define CERTDIR  %ROOT%\cert
define CONFDIR  %ROOT%\conf
define LOGDIR   %ROOT%\data
define LOGFILE  %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir  %ROOT%\data
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir  %ROOT%\data

<Extension _syslog>
    Module      xm_syslog
</Extension>

<Input in>
    Module      im_msvistalog
# For windows 2003 and earlier use the following:
#   Module      im_mseventlog
</Input>

<Output out>
    Module      om_tcp
    Host        192.168.1.206
    Port        512
    Exec        to_syslog_snare();
</Output>

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

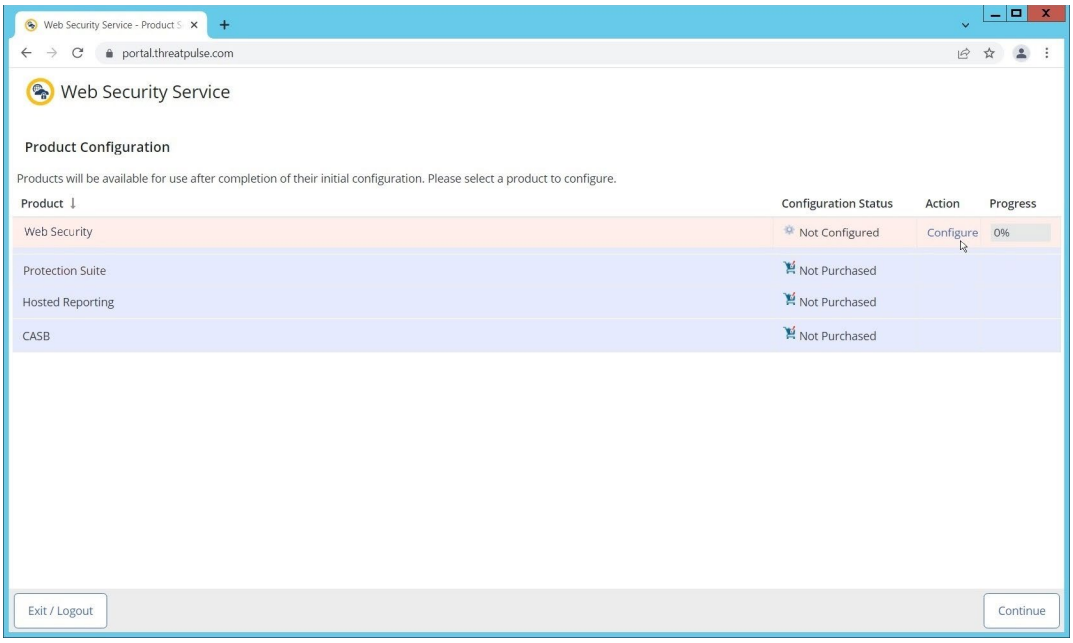
32. Restart the **nxlog** service.
33. You can verify that this connection is working by checking the logs in *data\nxlog.log*, and by noting an increase in events on the Helix Dashboard.

2.2 Symantec Cloud Secure Web Gateway

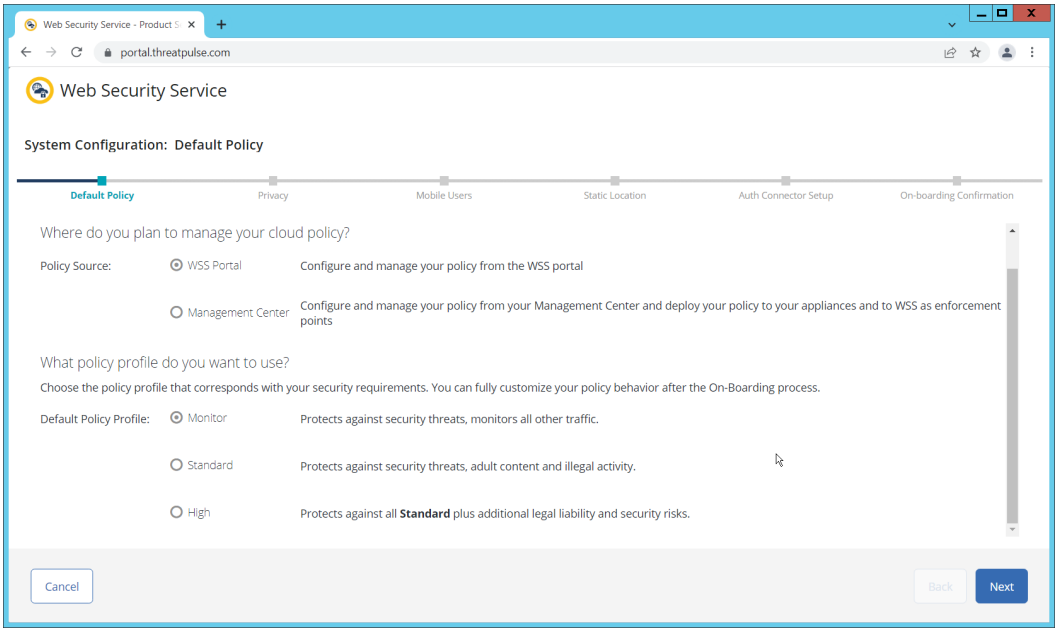
This installation and configuration guide for Symantec SWG uses a cloud instance of Web Isolation. In this guide, Web Isolation is used to isolate threats to the user through the browser. It does this through the use of a web proxy, which captures traffic and assigns a threat level to it, and based on 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.

Configure Web Security Service

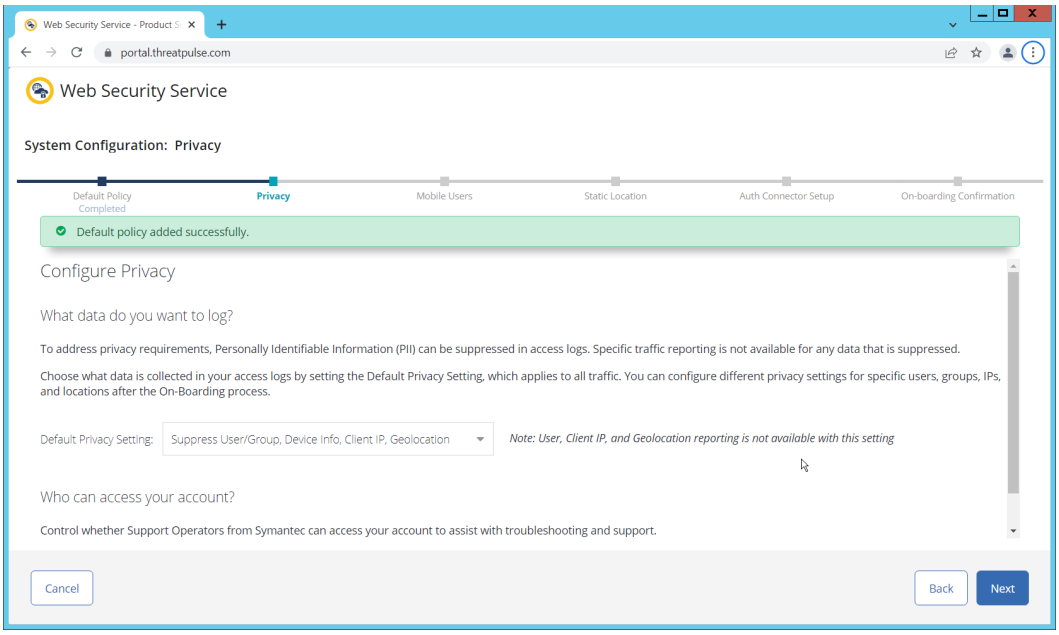
1. Login to the Symantec portal by navigating to https://portal.threatpulse.com/.



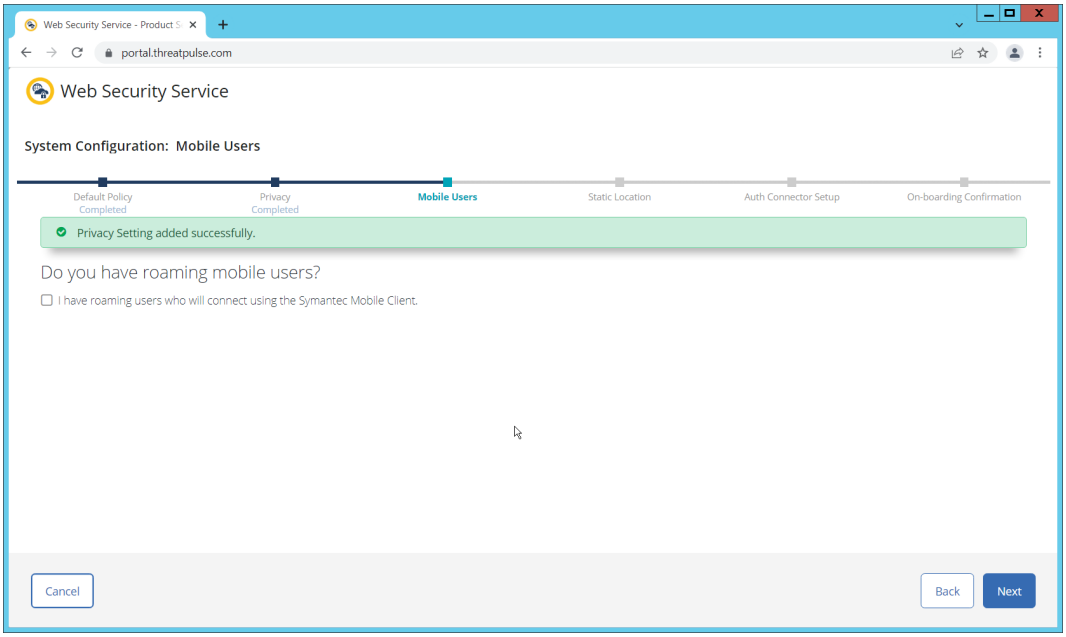
2. Click **Configure** next to Protection Suite.
3. Select **WSS Portal**.
4. Select **Monitor**.



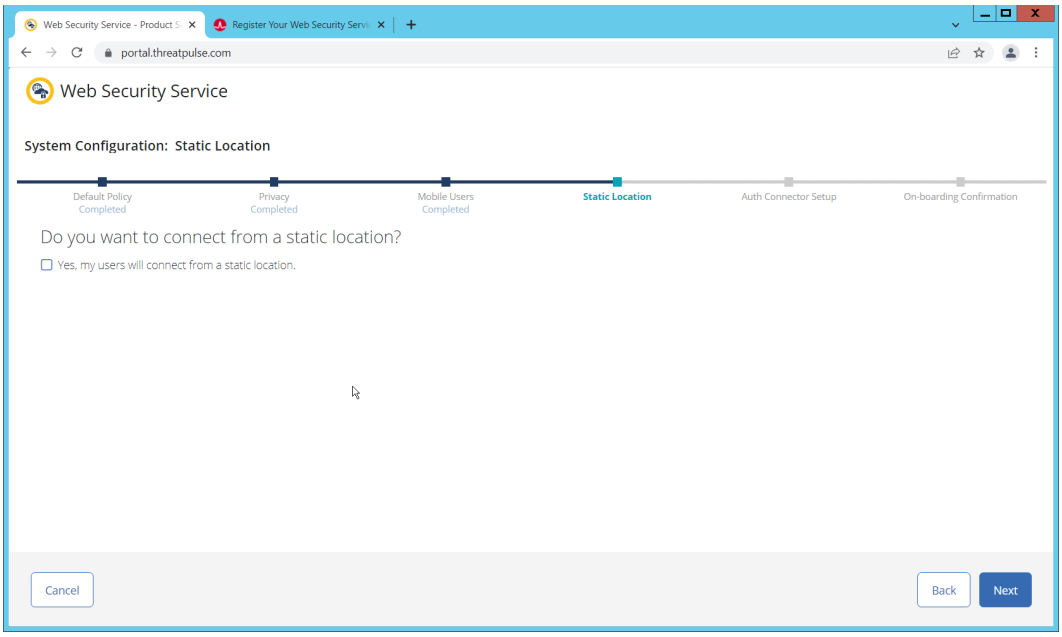
5. Click **Next**.
6. Select **Suppress User/Group, Device Info, Client IP, Geolocation**. (Note: If you are planning to use this tool for network monitoring of organizational users, a less strict privacy policy may be preferable; however, for this build, we are using Web Isolation primarily for external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



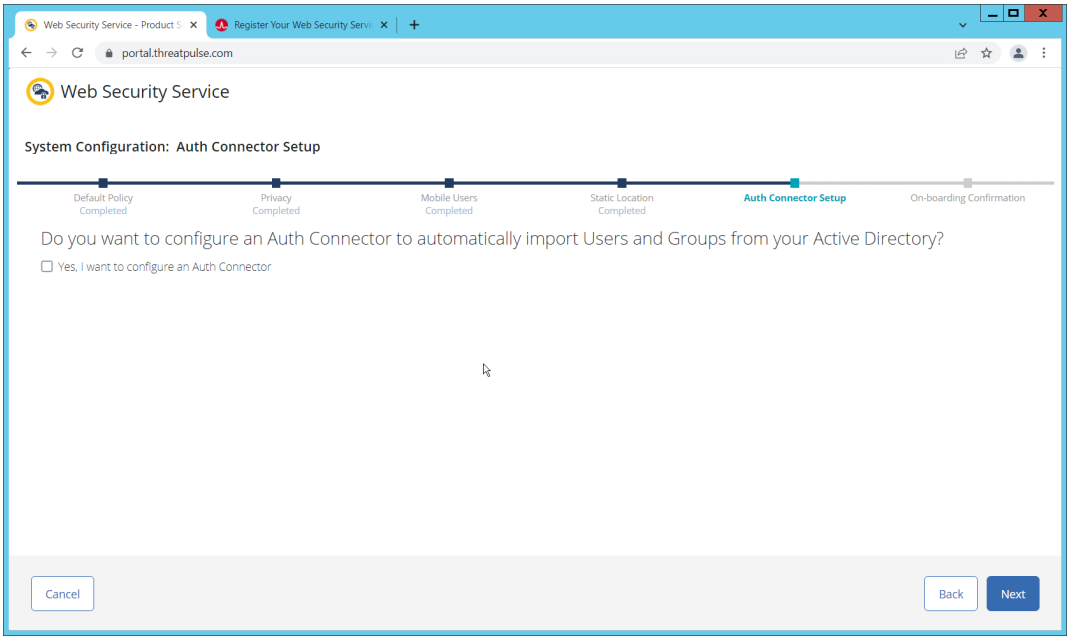
7. Click **Next**.
8. Indicate whether you have mobile users.



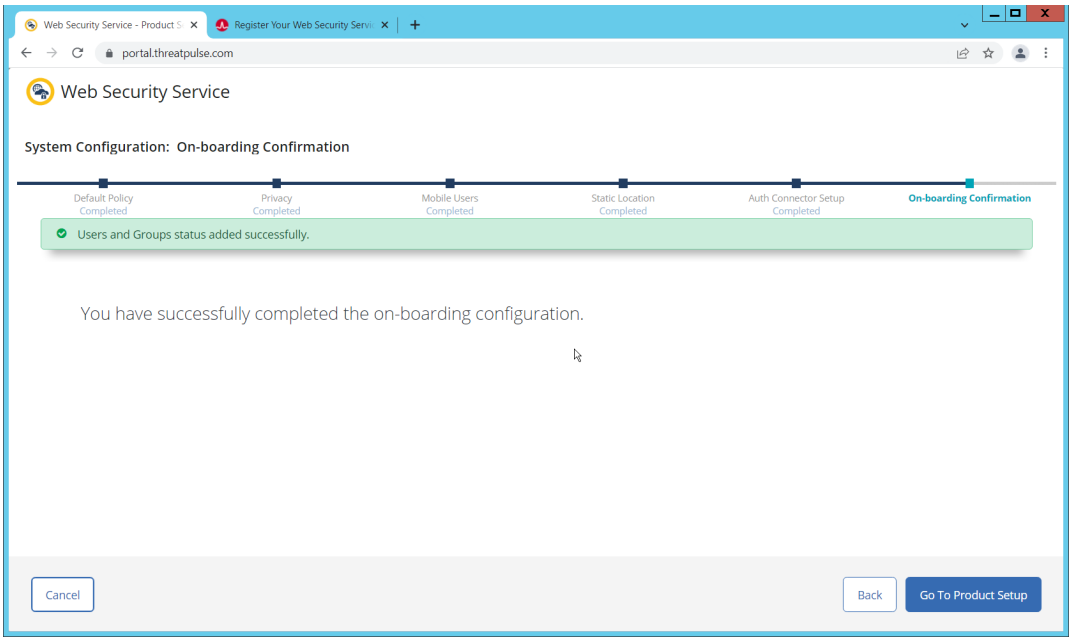
9. Click **Next**. Indicate whether your users connect from a static location.



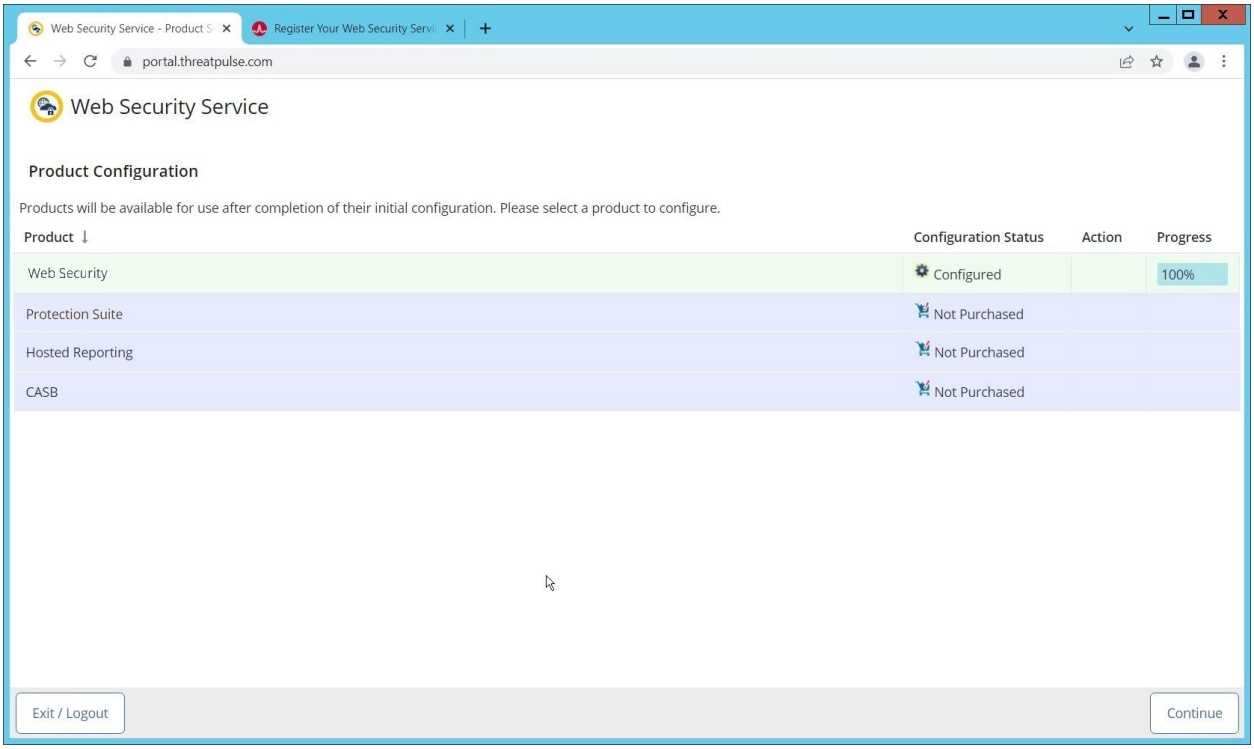
325 10. Click **Next**. Indicate whether you want to configure an Auth Connector.



326 11. Click **Next**.



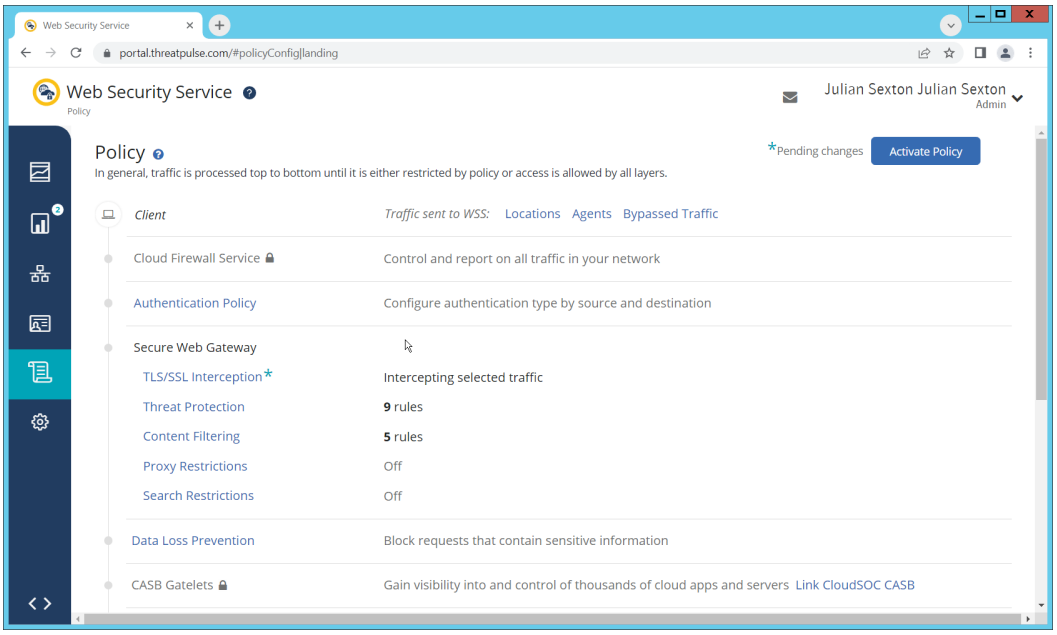
12. Click **Go To Product Setup**.



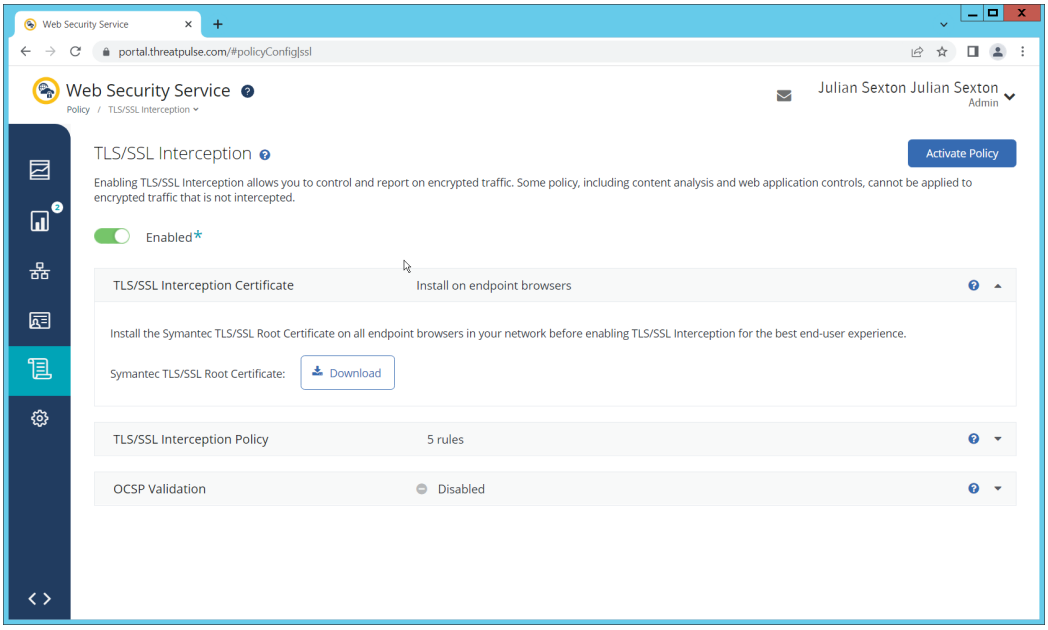
13. Click **Continue**.

Install Proxy Certificates and enabling TLS/SSL Interception

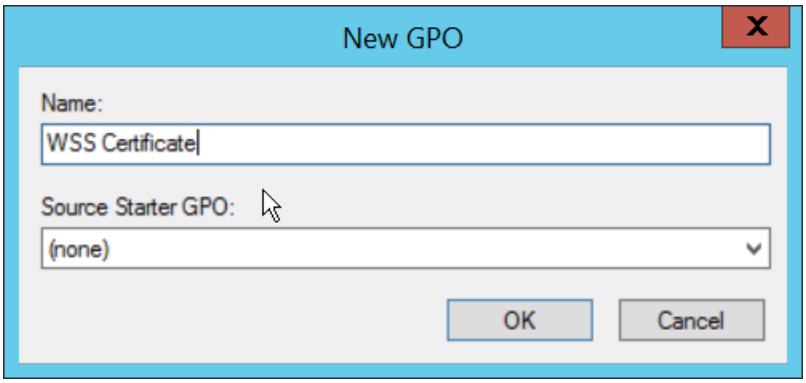
1. Click the **Policy** tab.



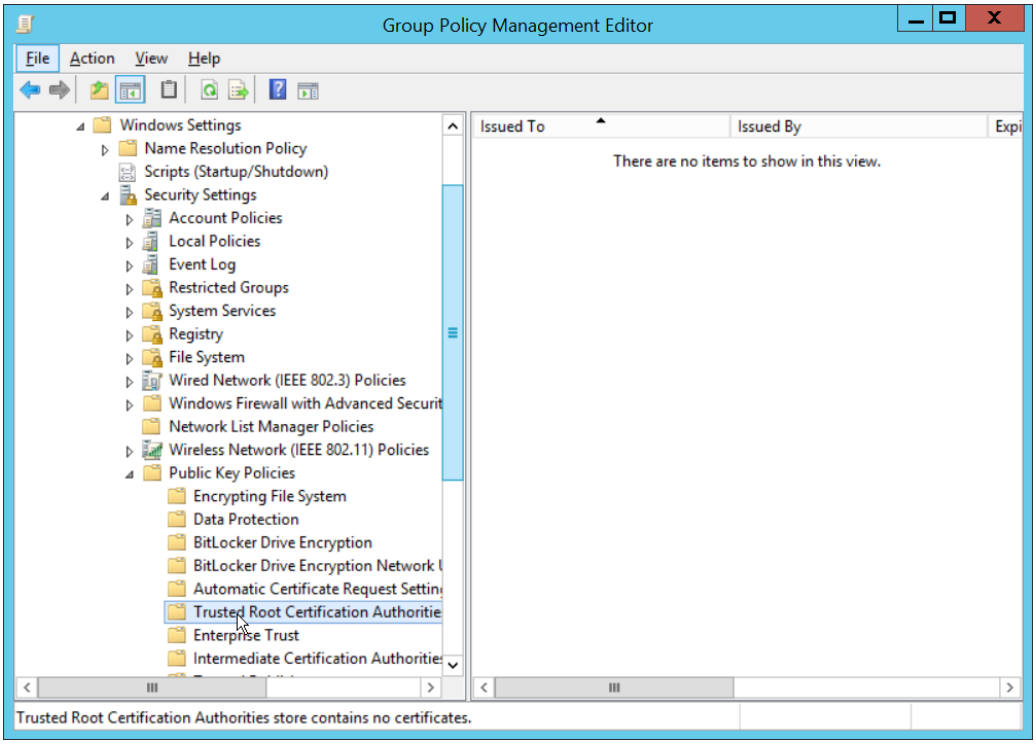
2. Click **TLS/SSL Interception**.
3. Enable TLS/SSL interception by clicking the toggle.



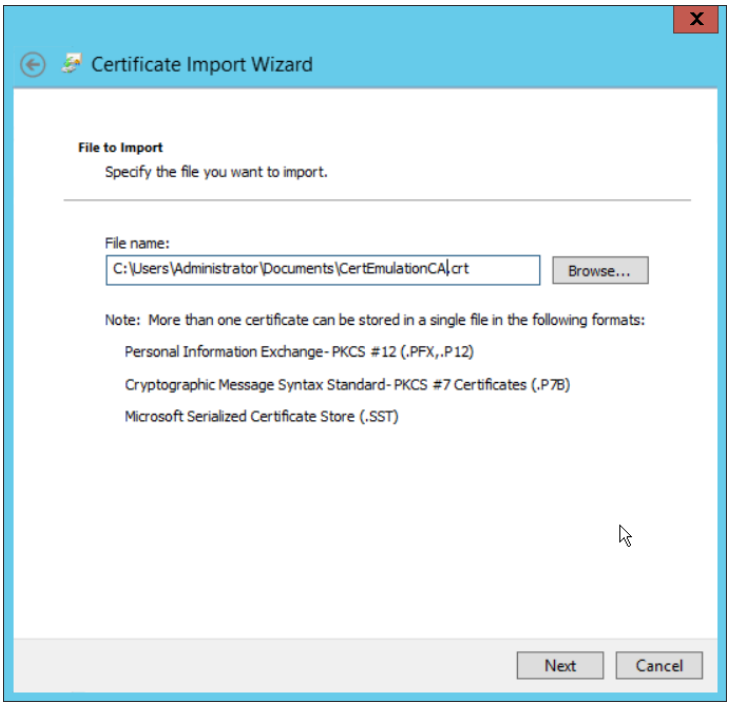
4. Download the certificate here. You can either install this individually in the Trusted Root Certification Authorities store on individual machines or follow the below steps to distribute the certificate via Group Policy.
5. Open the **Group Policy Management Console**.
6. Right click the **Domain**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



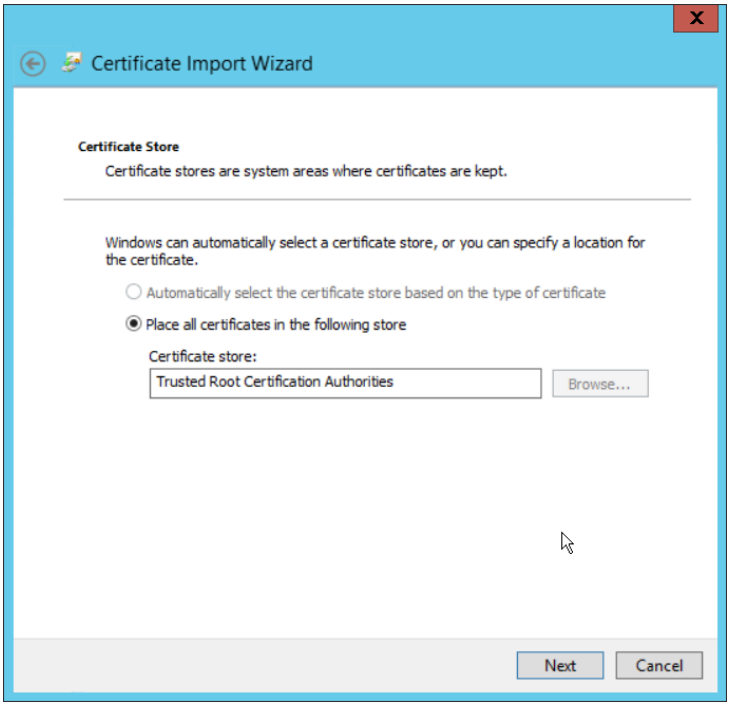
7. Enter a name and click **OK**.
8. Right click the newly created GPO and click **Edit…**.



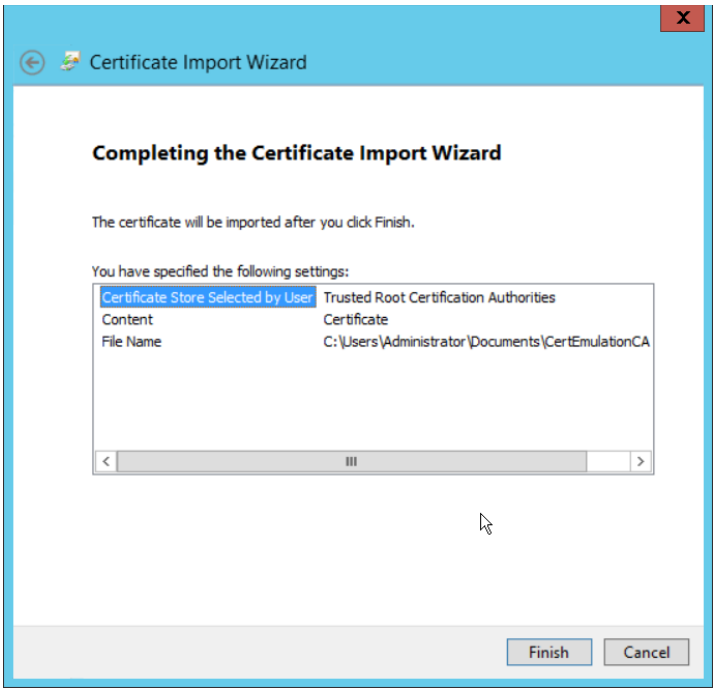
9. Navigate to **Computer Configuration > Policies > Window Settings > Security Settings > Public Key Policies**, and right click **Trusted Root Certification Authorities**.
10. Click **Import**.
11. Click **Next**.
12. Select the certificate you just downloaded.



345 13. Click **Next**.



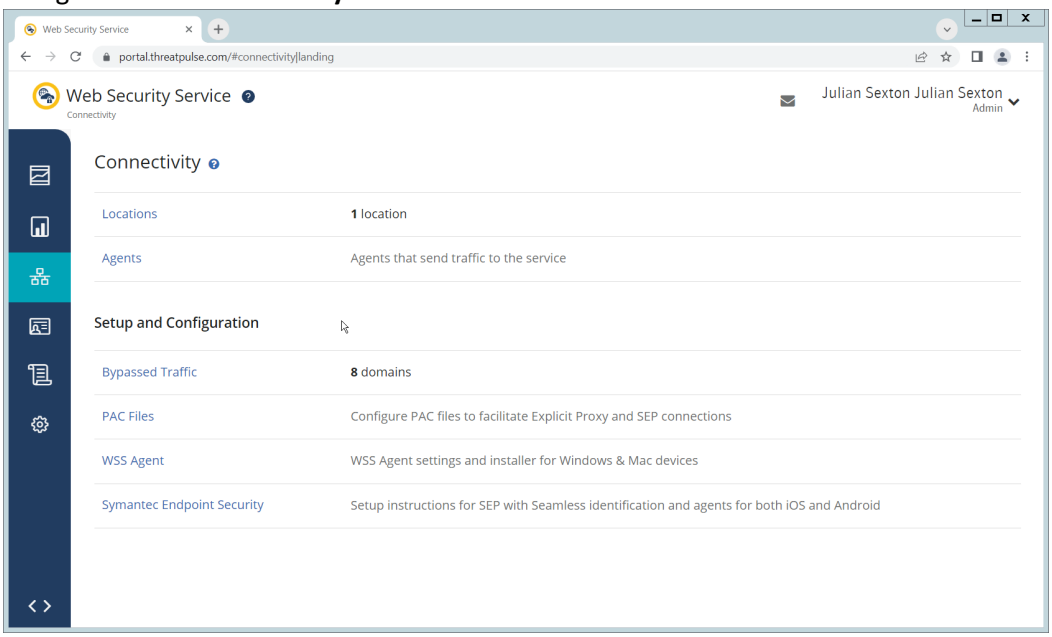
346 14. Click **Next**.



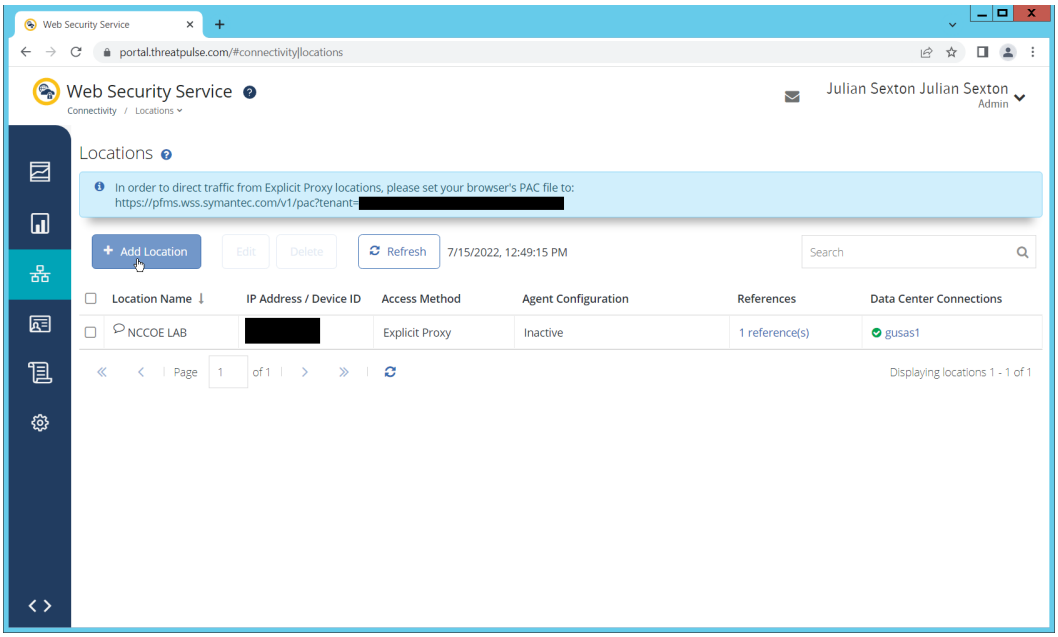
15. Click **Finish**.
16. Click **OK**.

Configure Symantec Web Security Service Proxy

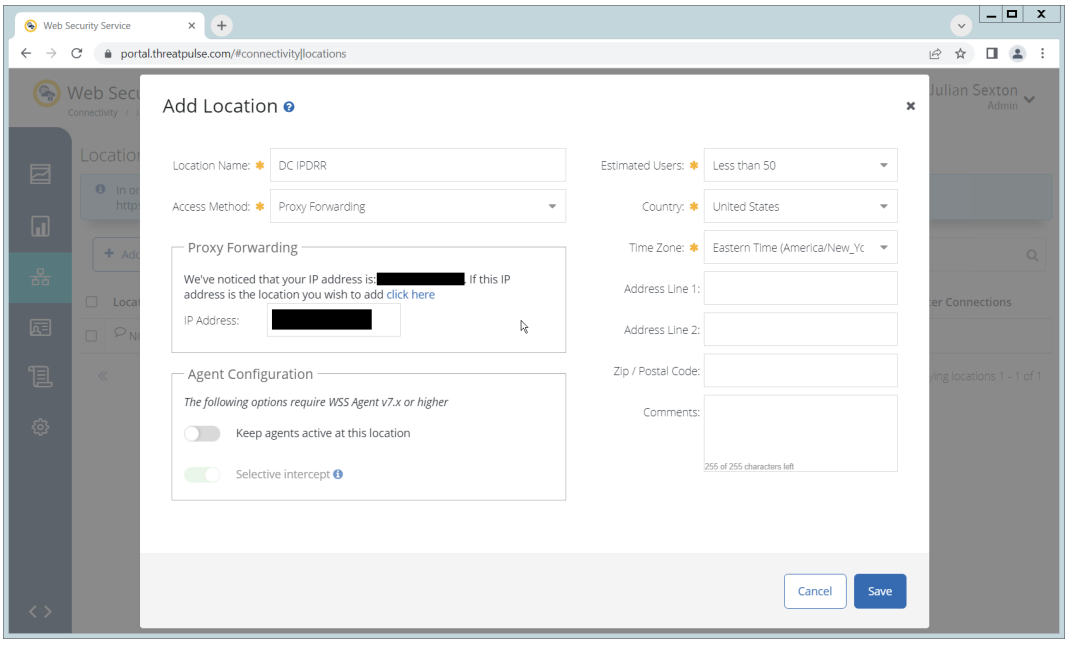
1. Navigate to the **Connectivity** tab.



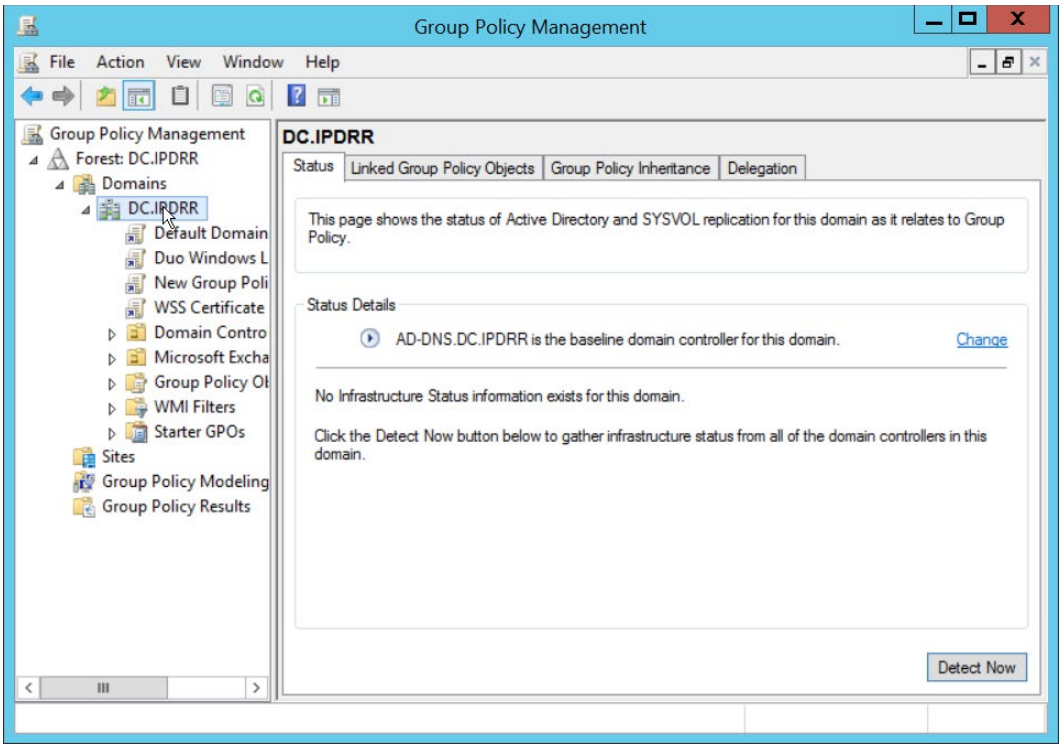
2. Click **Locations**.



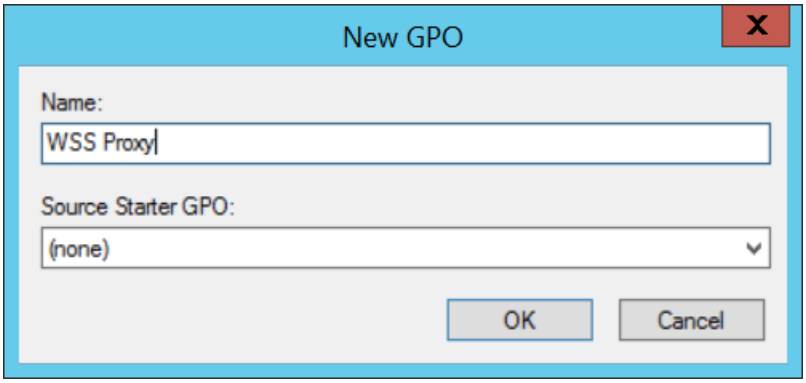
3. Click **Add Location**.
4. Enter a name for the **Location**.
5. Select **Proxy Forwarding** for **Access Method**.
6. Enter any public IP addresses of your organization, to ensure that traffic sent through the WSS proxy is redirected to the proper dashboard.



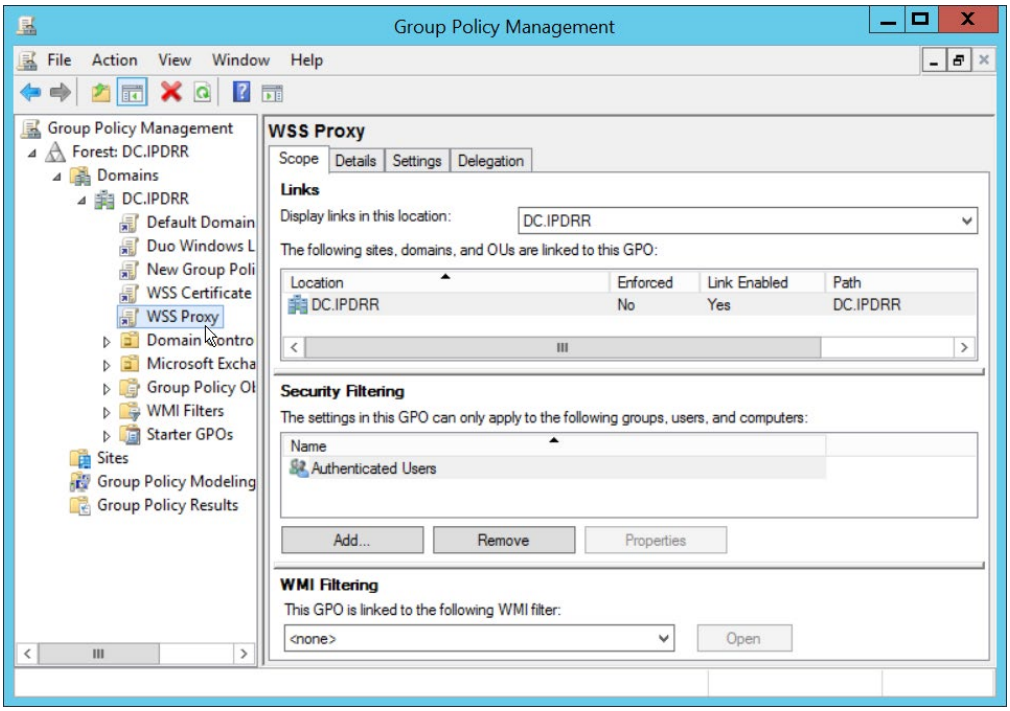
7. Click **Save**.
8. This page will now provide a URL to a PAC file which can be distributed to browsers across the organization via GPO. If you wish to create a custom PAC file, you can navigate to **Connectivity > PAC Files**.
9. Open the **Group Policy Management Console**.



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

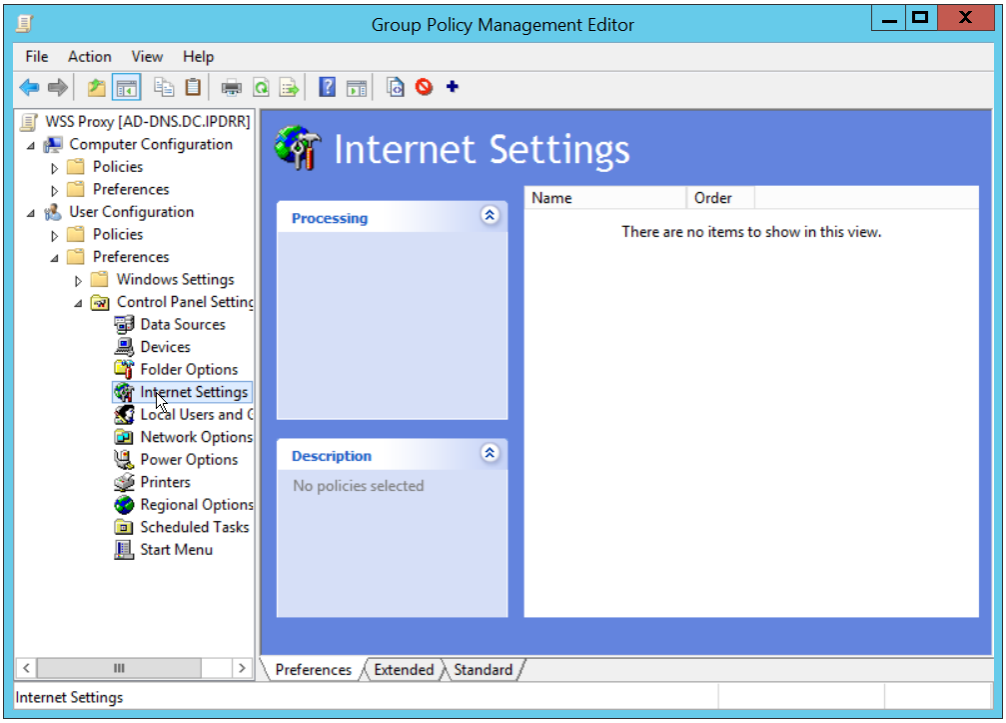


363 11. Enter a name and click **OK**.



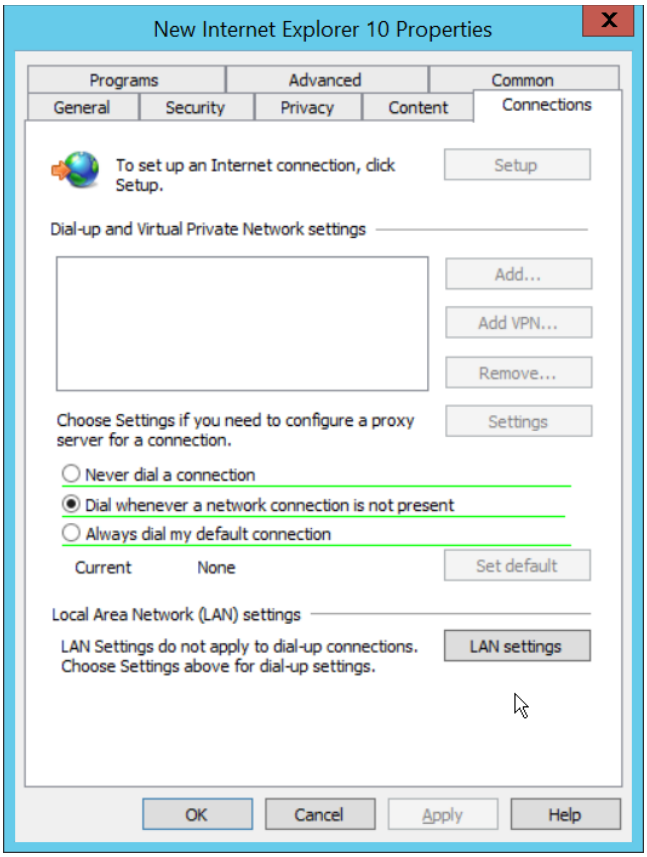
364 12. Right click the newly created GPO and click **Edit…**.

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

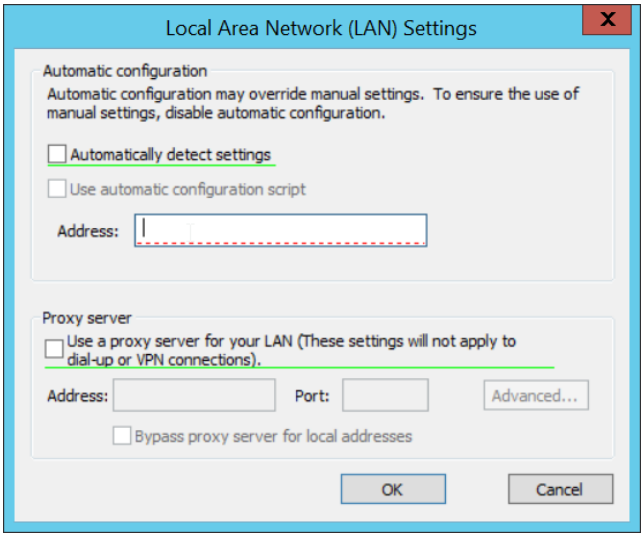


366 14. Right click **Internet Settings** and select **New** > **Internet Explorer 10 Properties**.

367 15. Click the **Connections** Tab.



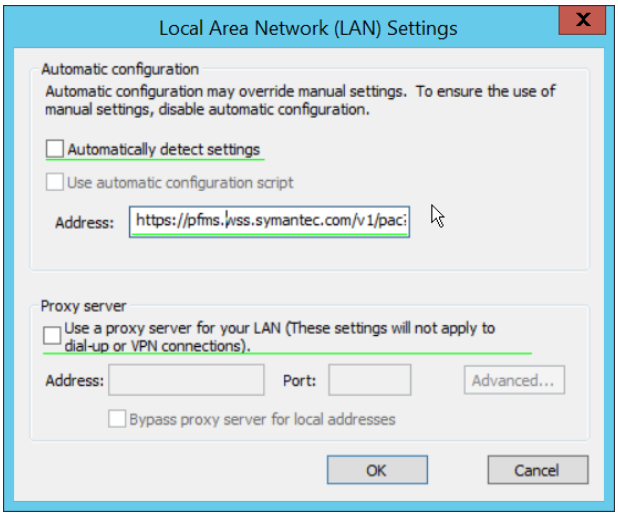
368 16. Click **Local Area Network (LAN Settings)**.



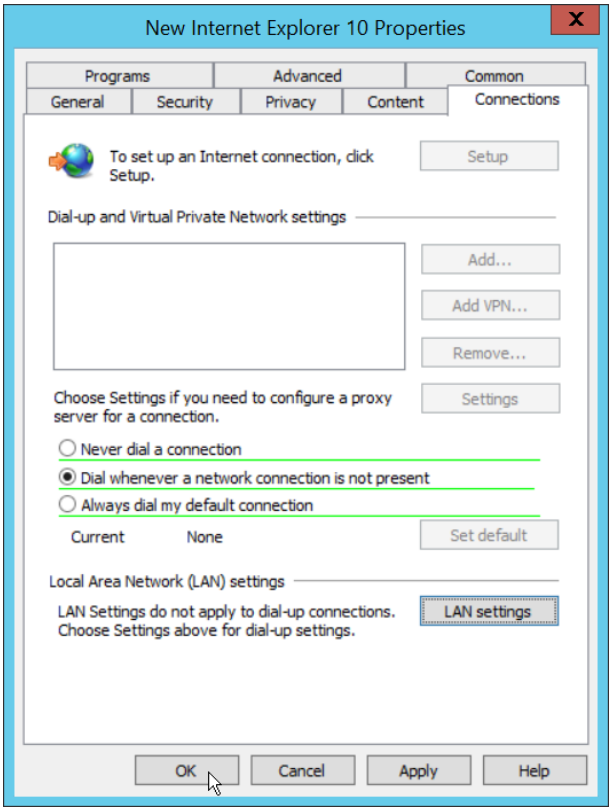
369 17. Select the **Address** field.

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

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

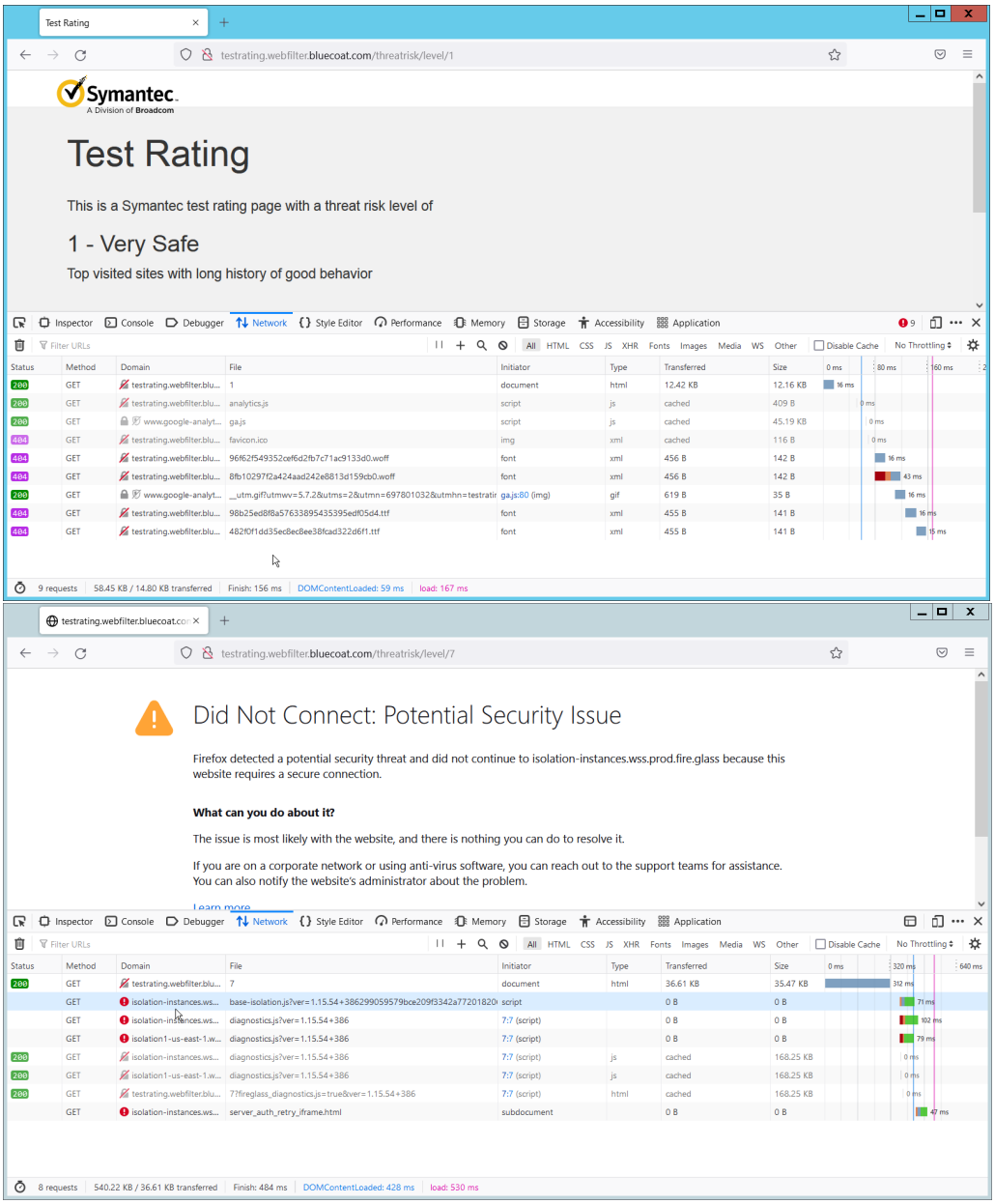


372 20. Click **OK**.



373 21. Click **OK**.

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



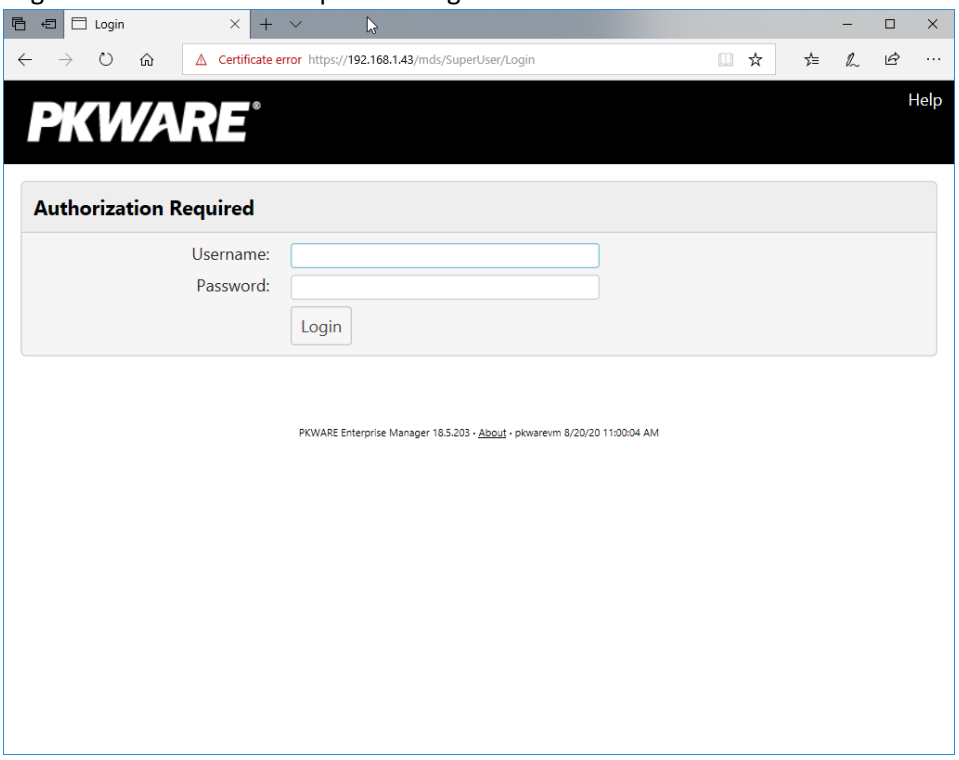
23. On this test URL (tested July 2022), levels 5-7 will go through isolation, and you will be able to see the isolation traffic from the network tab in developer mode (**F12**) on the browser. Levels 8-10 will be blocked by the content filter, and levels 1-4 will not go through isolation or content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

2.3 PKWARE PKProtect

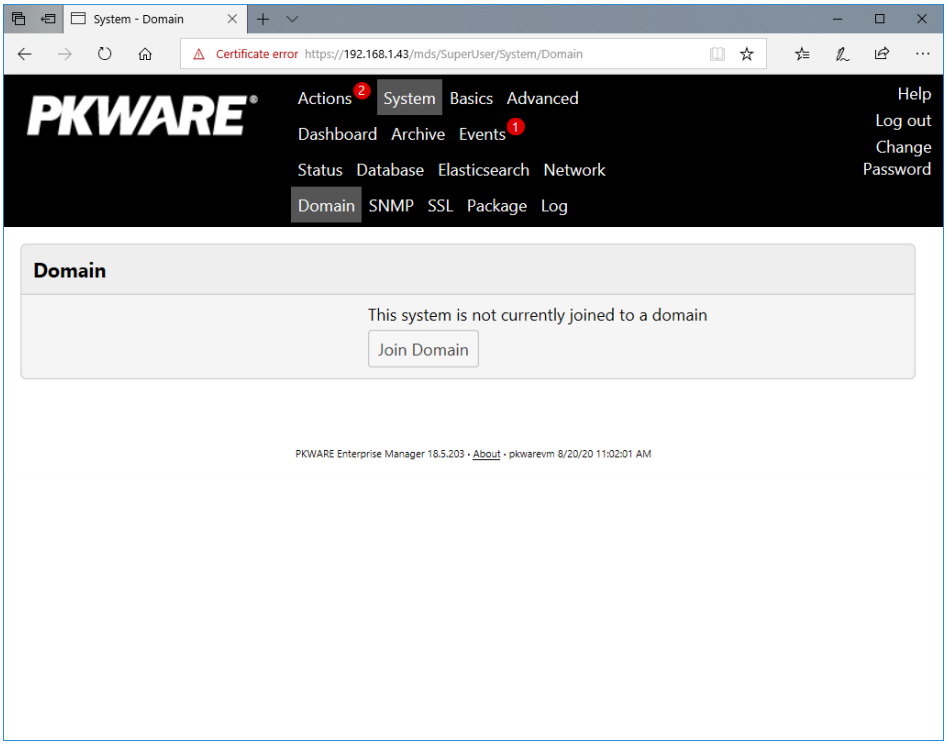
This installation and configuration guide for PKWARE PKProtect uses a physical PKWARE server, and as such will not delve into the installation of server components. In this guide, PKWARE is used to automatically perform data inventory and data protection functions. PKWARE provides users with the ability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

Configure PKWARE with Active Directory

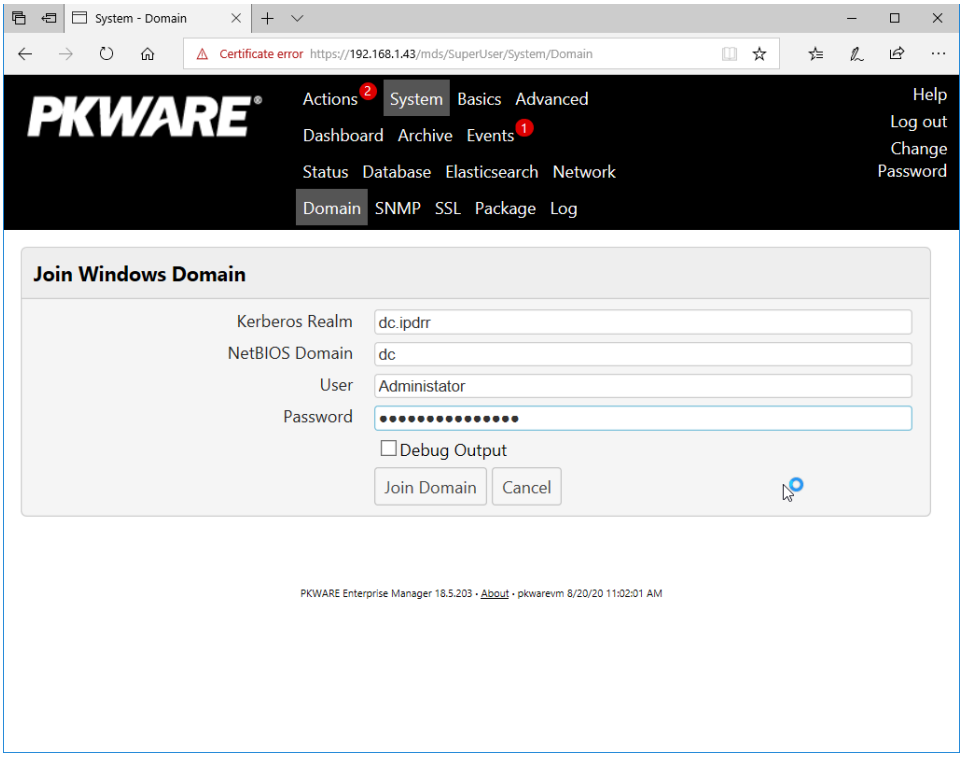
1. Login to the PKWARE web portal using the administrative credentials.



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.**



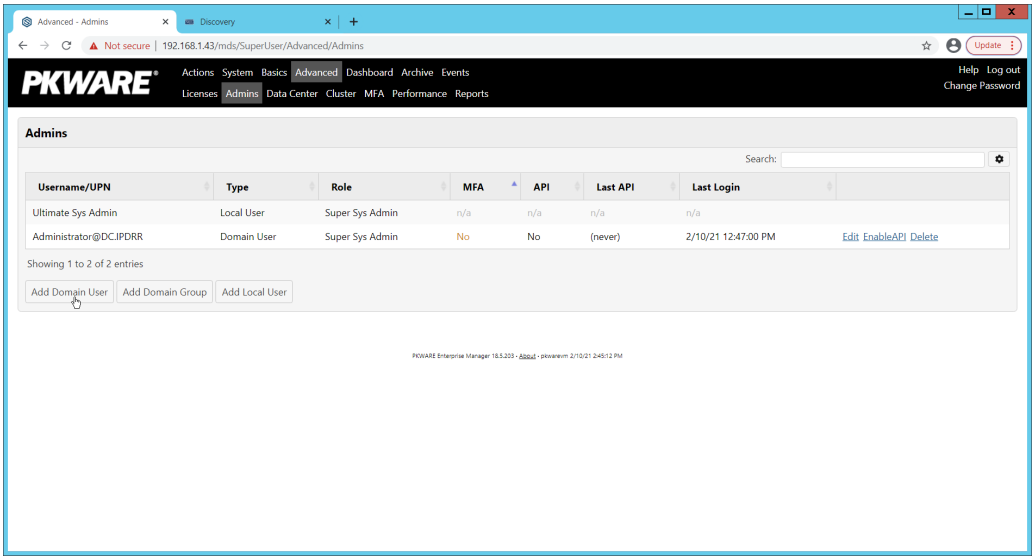
4. Click **Join Domain.**
5. Enter the **Kerberos Realm, NetBIOS Domain,** as well as the **username** and **password** of an administrative user on the domain.



6. Click **Join Domain.**

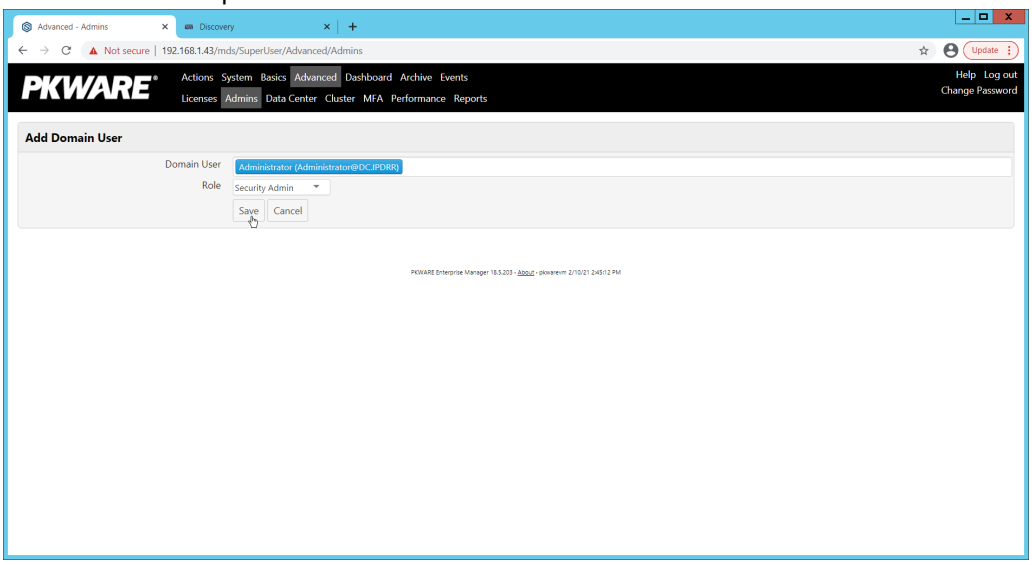
Create a New Administrative User

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



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).

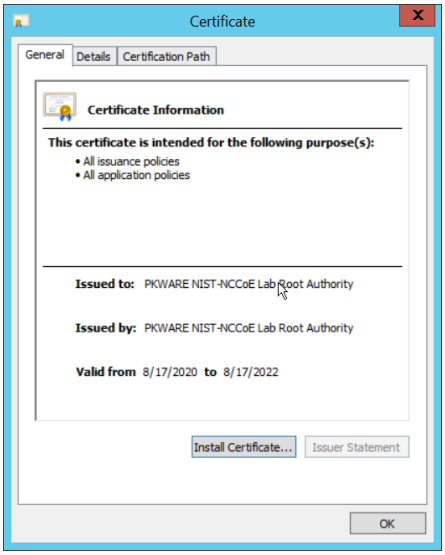
4. Select the level of permissions the user should have.



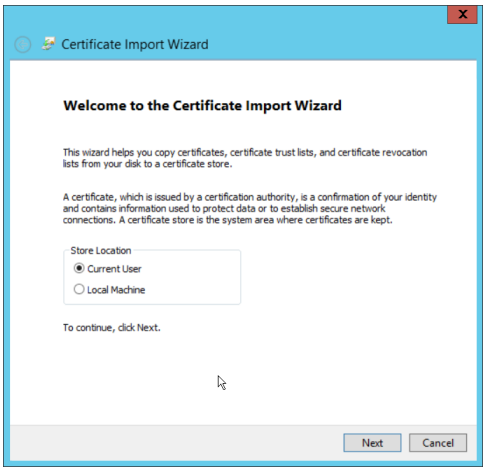
5. Click **Save.**

Install Prerequisites

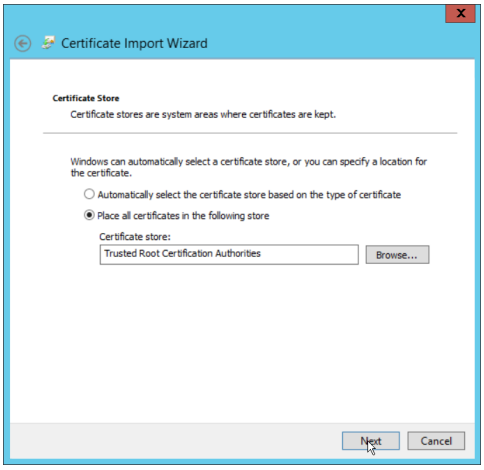
1. If needed for your environment, you may need to install certificates locally before agents can connect to PKProtect - ask your PKWARE representative if this is necessary for your environment.
2. Double click the certificate you wish to install.



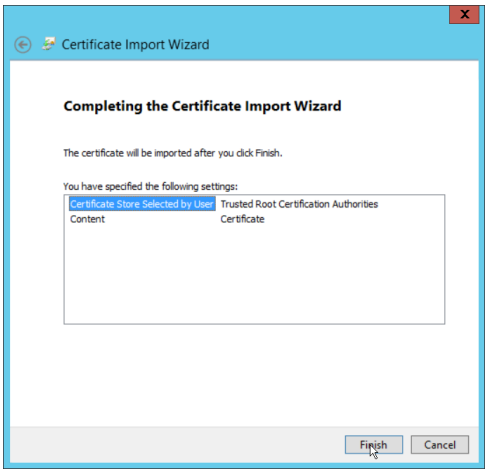
3. Click **Install Certificate….**
4. Select **Current User.**



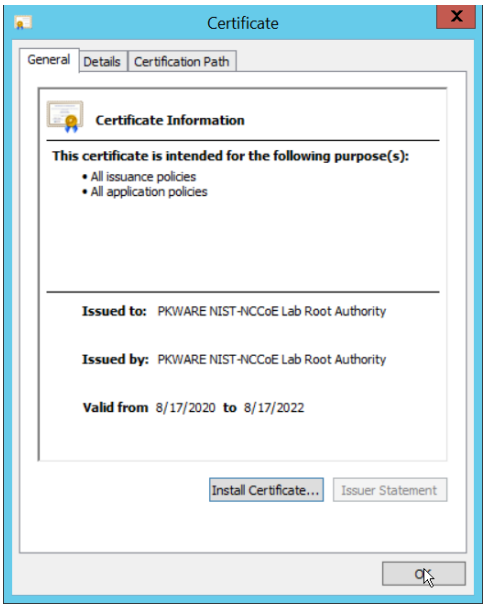
5. Click **Next.**
6. Click **Browse.**
7. Select **Trusted Root Certification Authorities.**



8. Click **Next.**



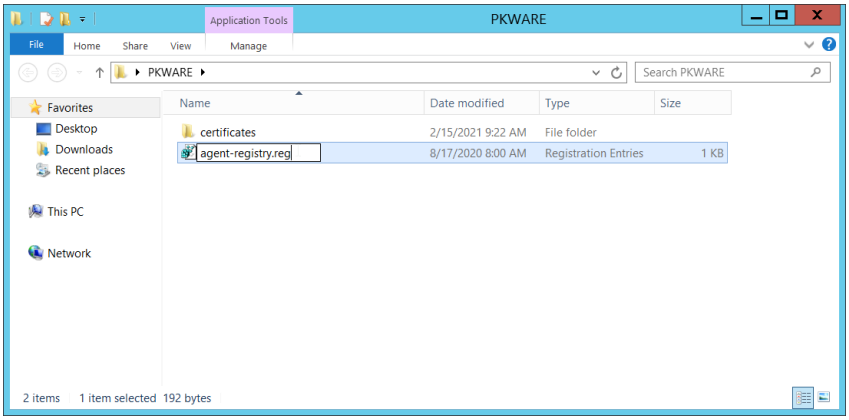
9. Click **Finish.**



413 10. Click **OK.**

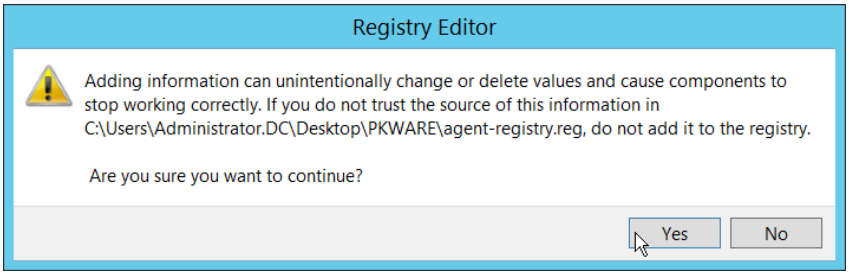
414 11. Repeat steps 1 through 10 but select **Personal** instead of **Trusted Root Certification Authorities.**

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

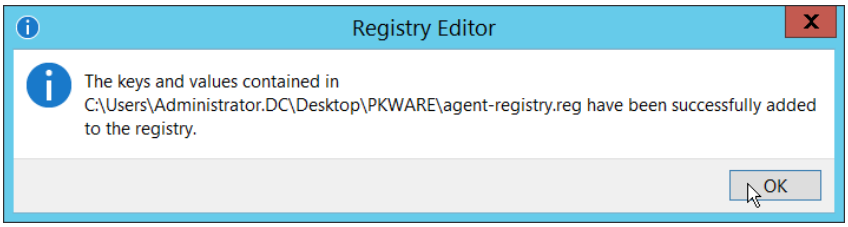


416 13. Rename agent-registry.txt to agent-registry.reg.

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



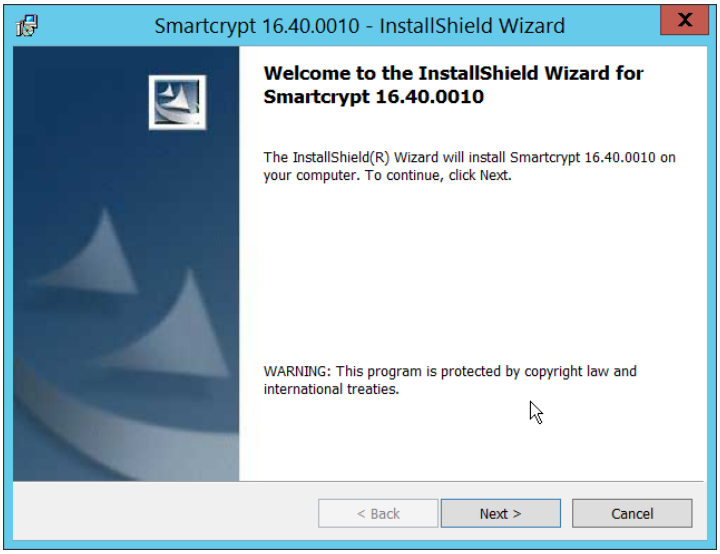
418 15. Click **Yes.**



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

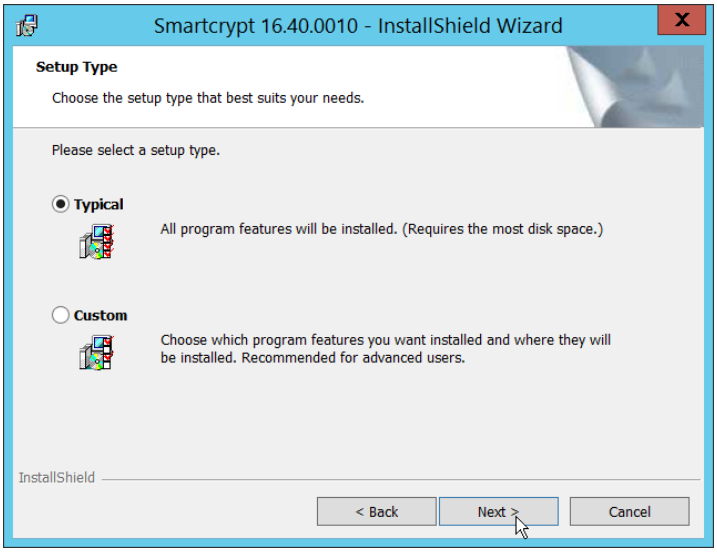
Install the PKProtect Agent

1. Run the PKProtect Installation executable.

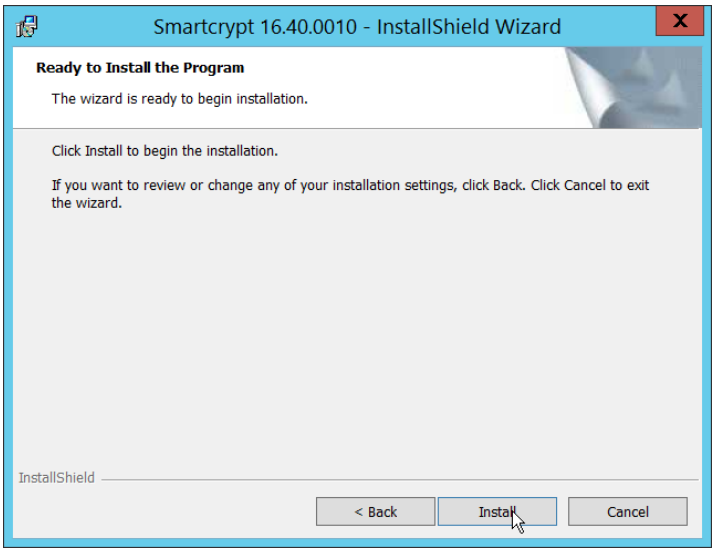


2. Click **Next.**
3. Select **I accept the terms in the license agreement.**

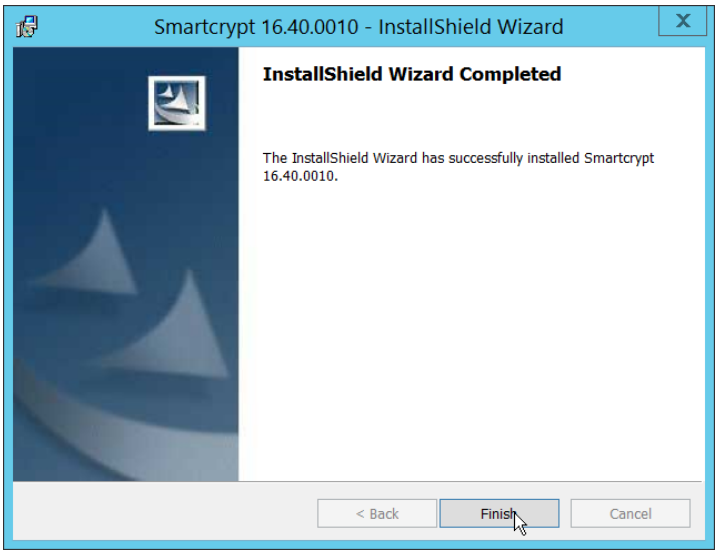
4. Click **Next.**
5. Select **Typical.**



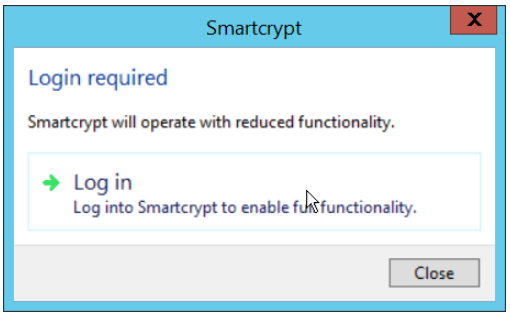
427 6. Click **Next.**



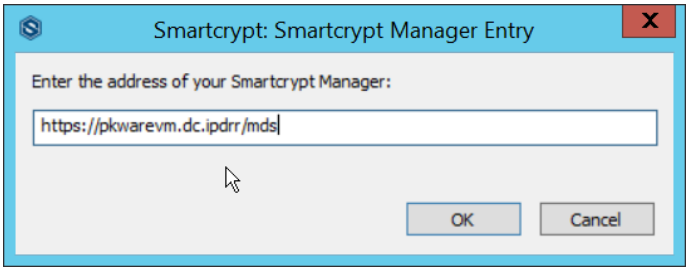
428 7. Click **Install.**



8. Click **Finish.**



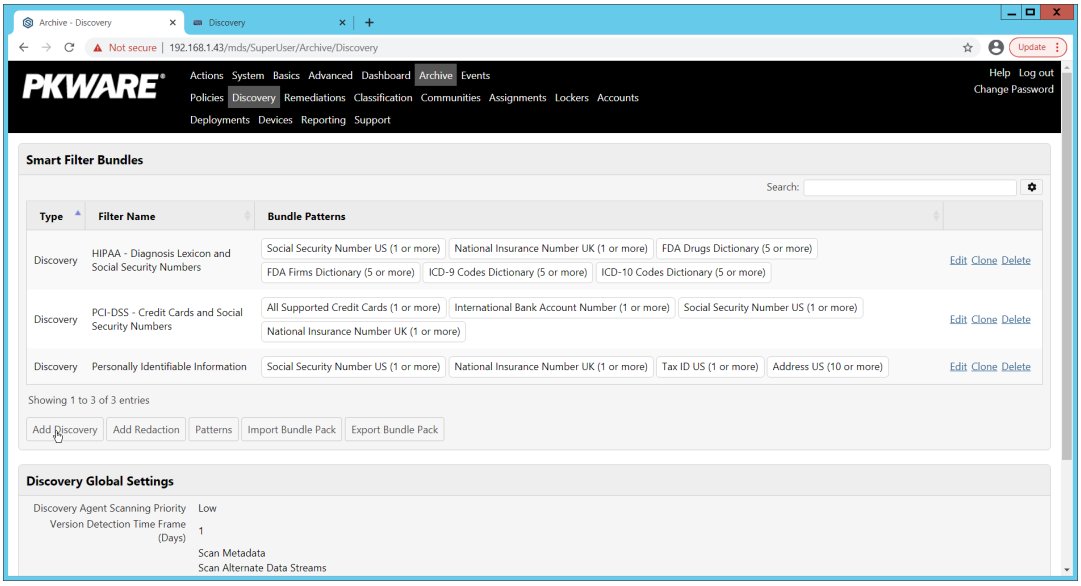
9. If a window to login is not automatically shown, you can right click the PKProtect icon in the Windows taskbar and click **Login….** If a window is automatically shown, click **Log in.**
10. Login using the username of the account in the domain, in email format (such as administrator@domain.id).



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

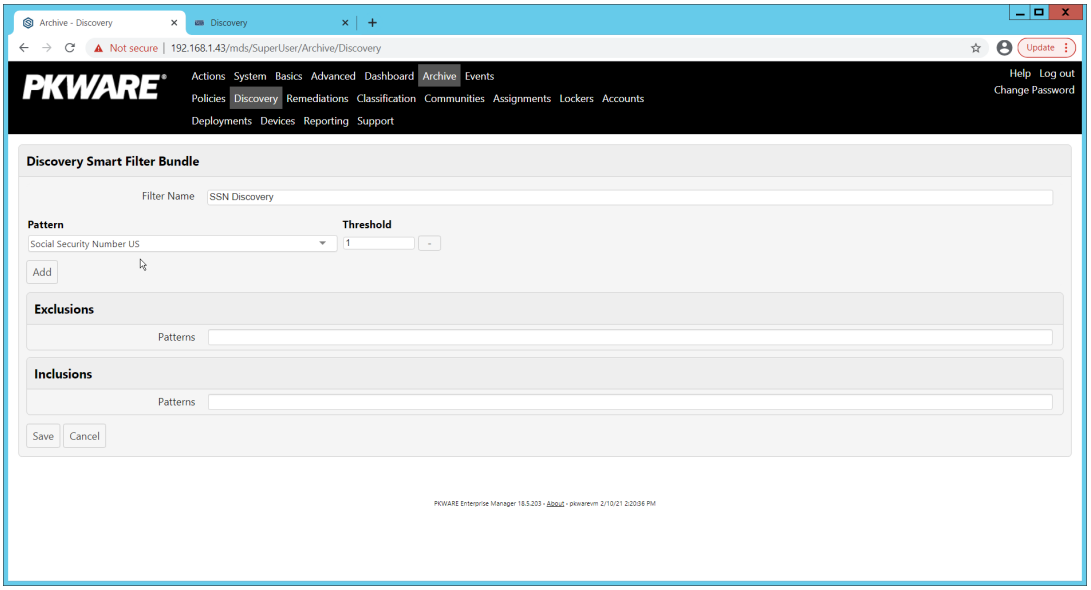
Configure Discovery and Reporting

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

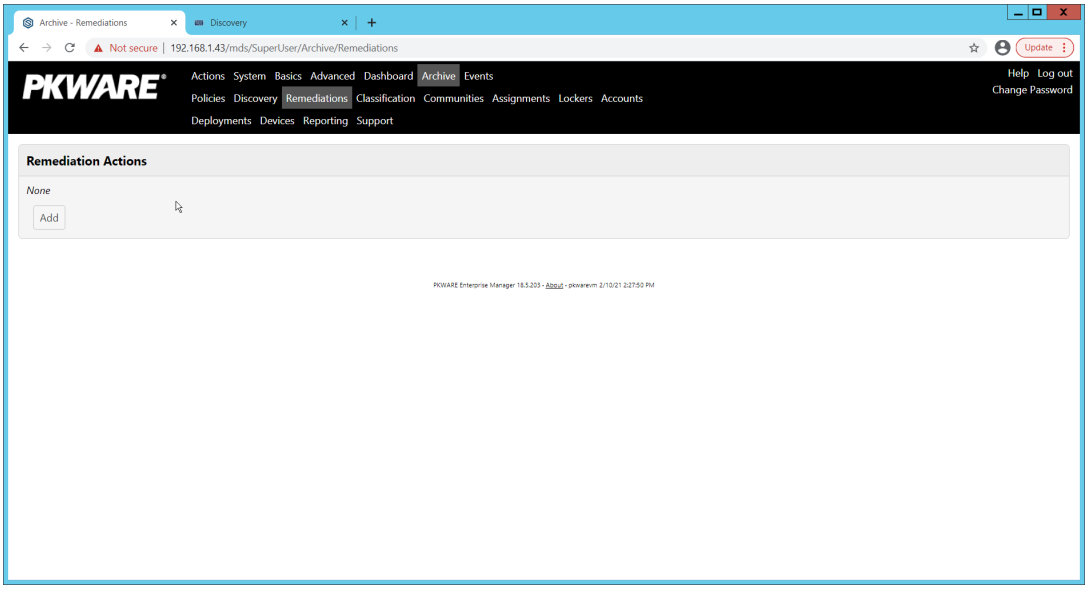


2. Click **Add Discovery.**
3. Enter a **name** for the discovery rule.

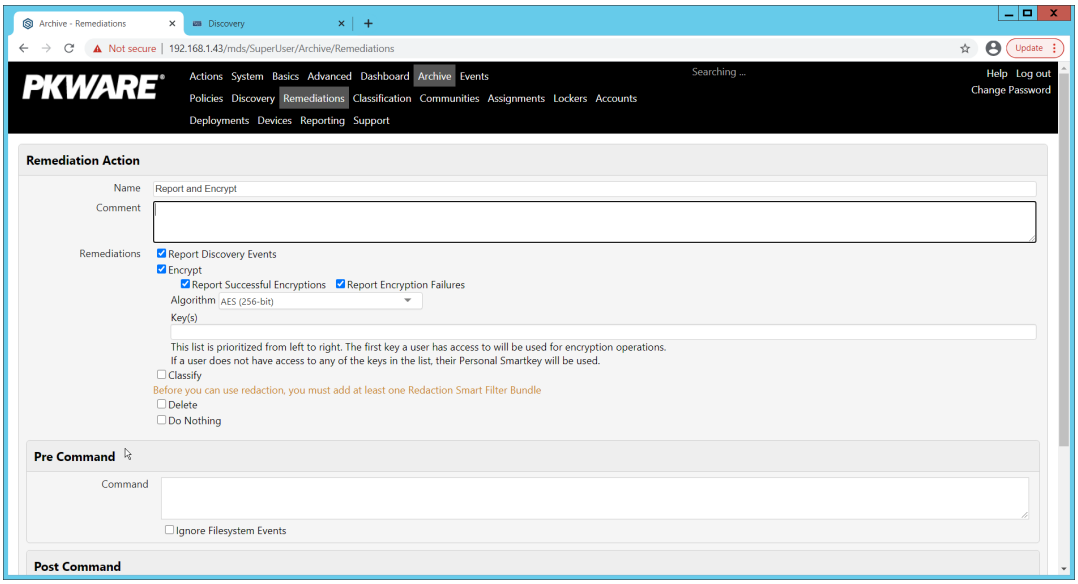
4. Select a **pattern** for the rule to discover. In this case, we are setting up a rule to detect social security numbers in files for reporting/remediation.
5. The **Threshold** field refers to how many of those patterns must be present in a document for the rule to be applied.



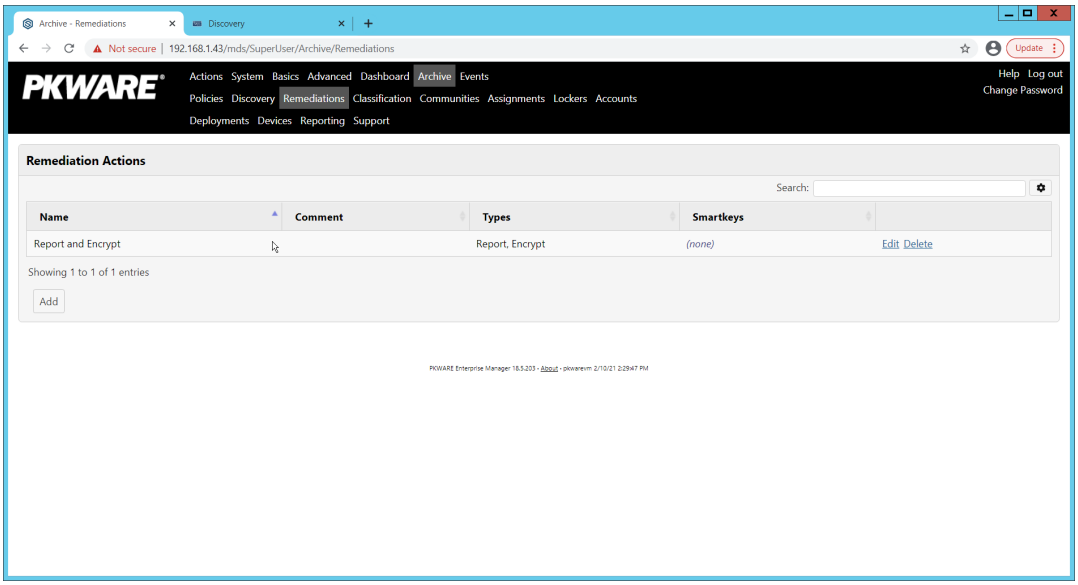
6. Click **Save.**
7. Navigate to **Archive > Remediations.**



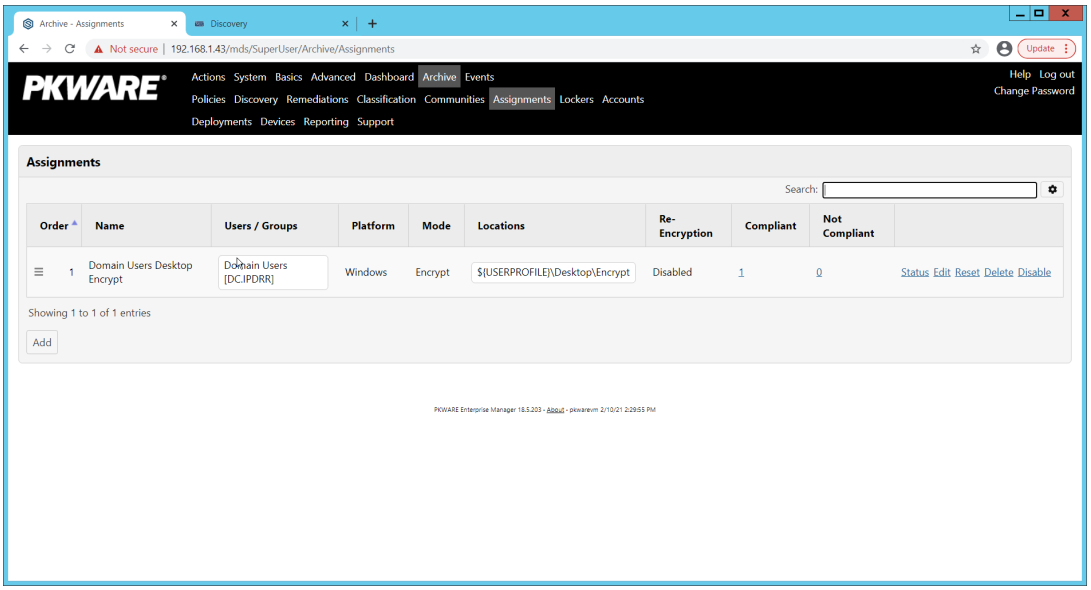
8. Click **Add.**
9. Enter a name for the remediation.



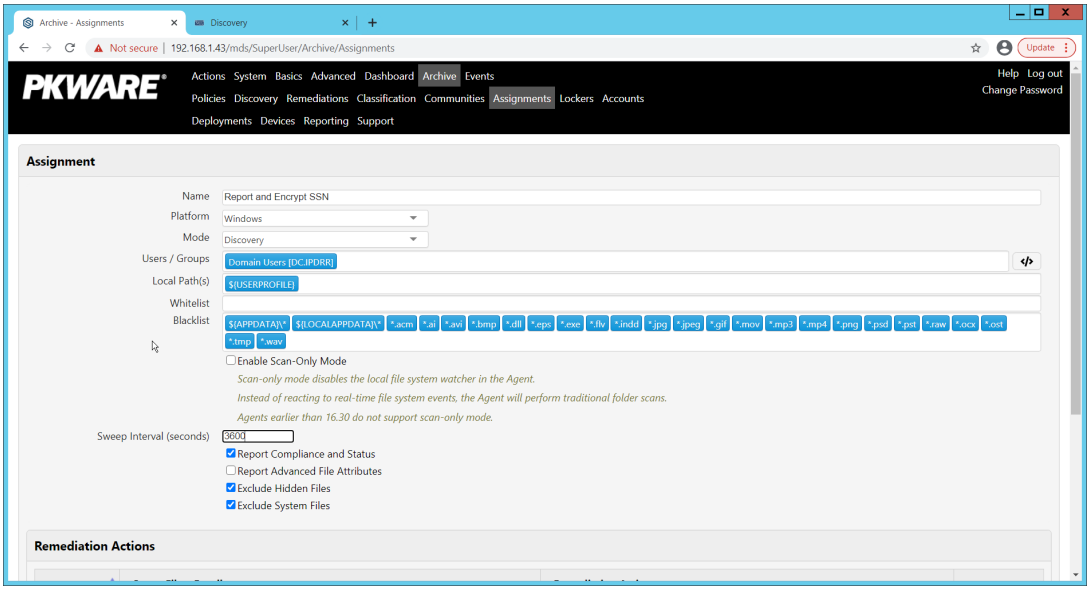
10. Check the box next to **Report Discovery Events.**
11. Check the box next to **Encrypt.**
12. Ensure that **AES (256-bit)** is selected.
13. Click **Save.**



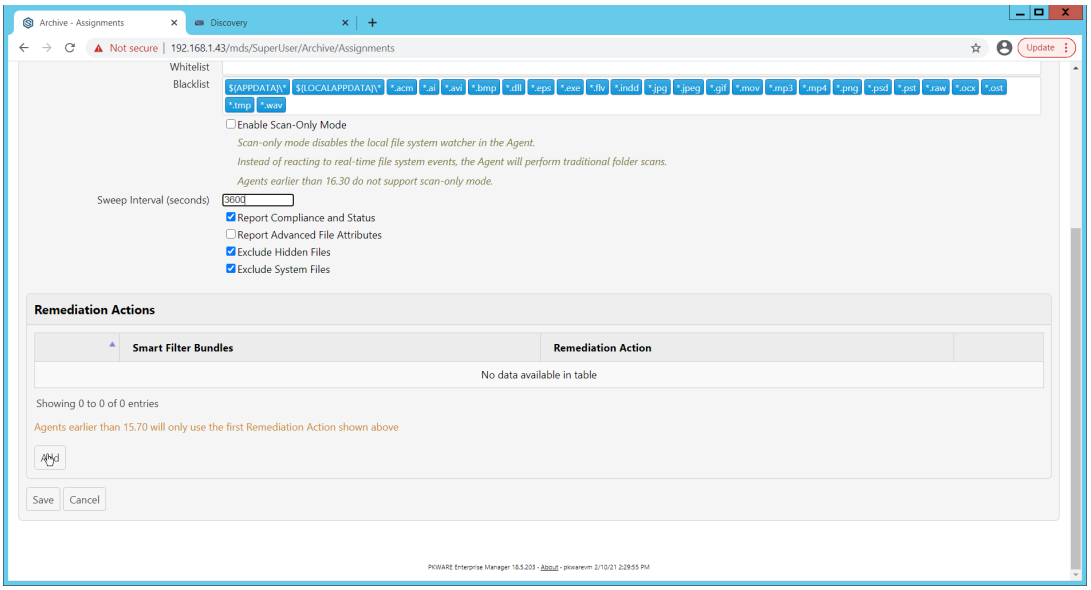
14. Navigate to **Archive > Assignments.**



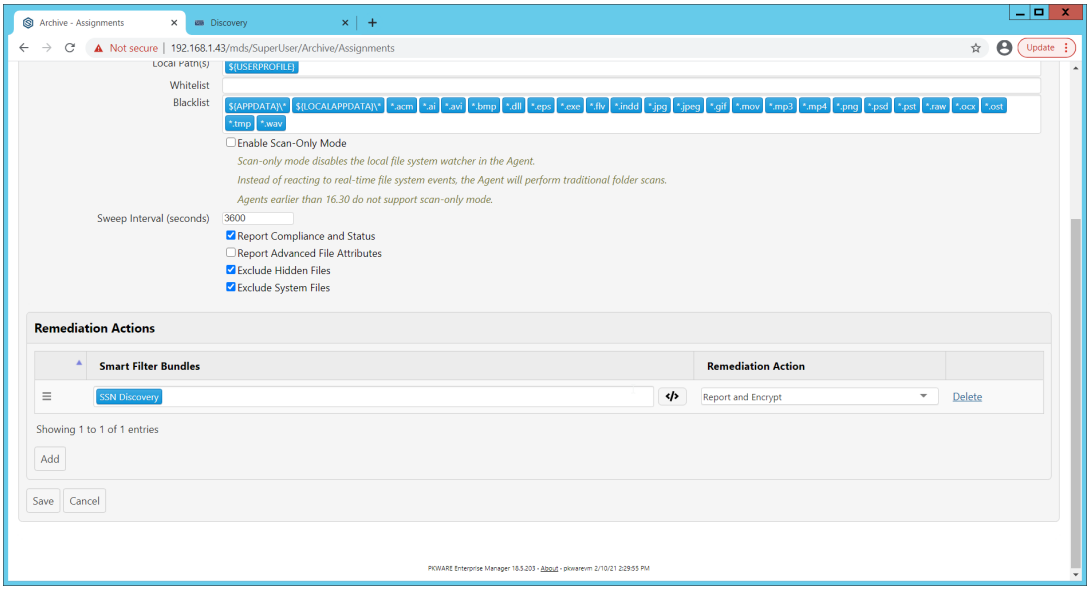
454 15. Click **Add.**



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



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.**



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

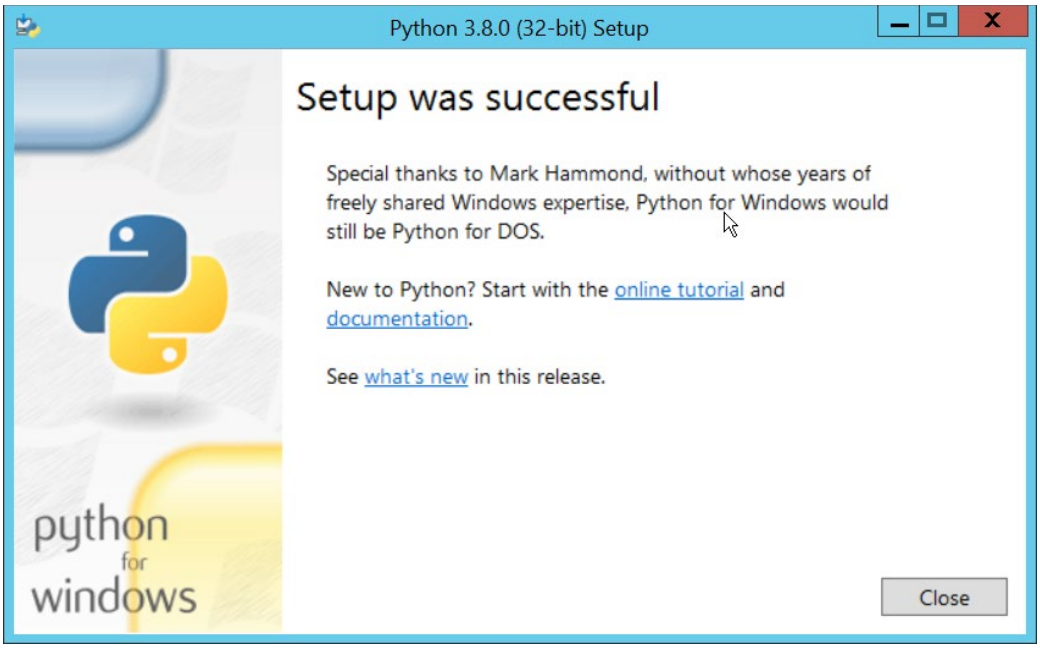
2.4 StrongKey Tellaro

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

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.**

6. Click **Install Now.**



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=us-
ers,ou=v2,ou=SKCE,ou=StrongAuth,ou=Applications,dc=strongauth,dc=com",
        "authgroups": "cn=EncryptionAuthor-
ized,did="+skdid+",ou=groups,ou=v2,ou=SKCE,ou=StrongAuth,ou=Applica-
tions,dc=strongauth,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"])

```

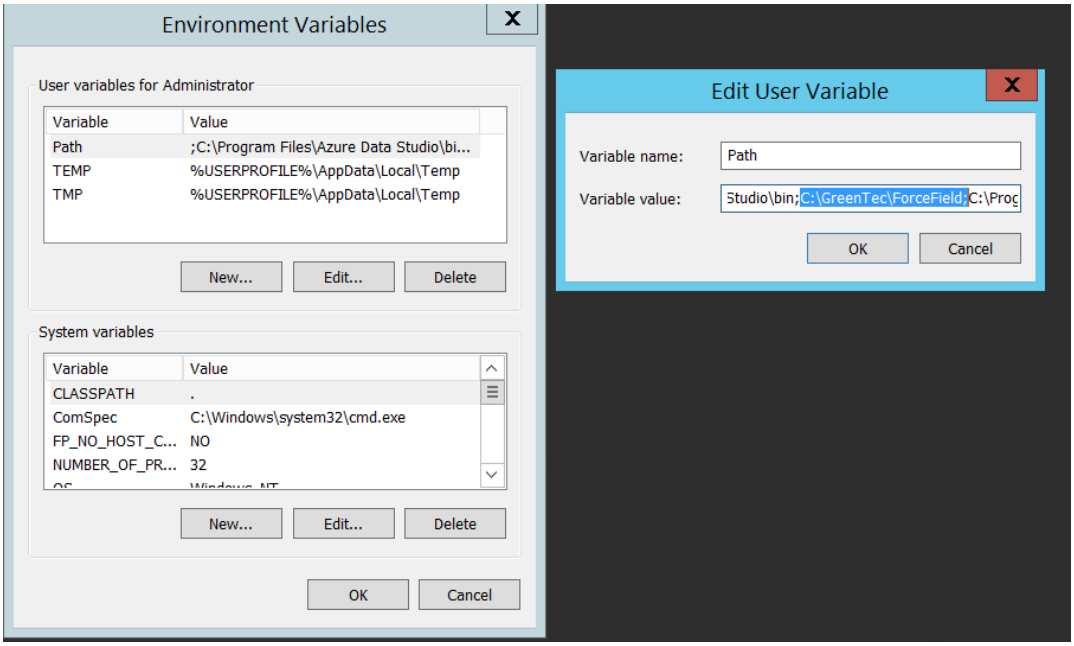
```
    return req

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

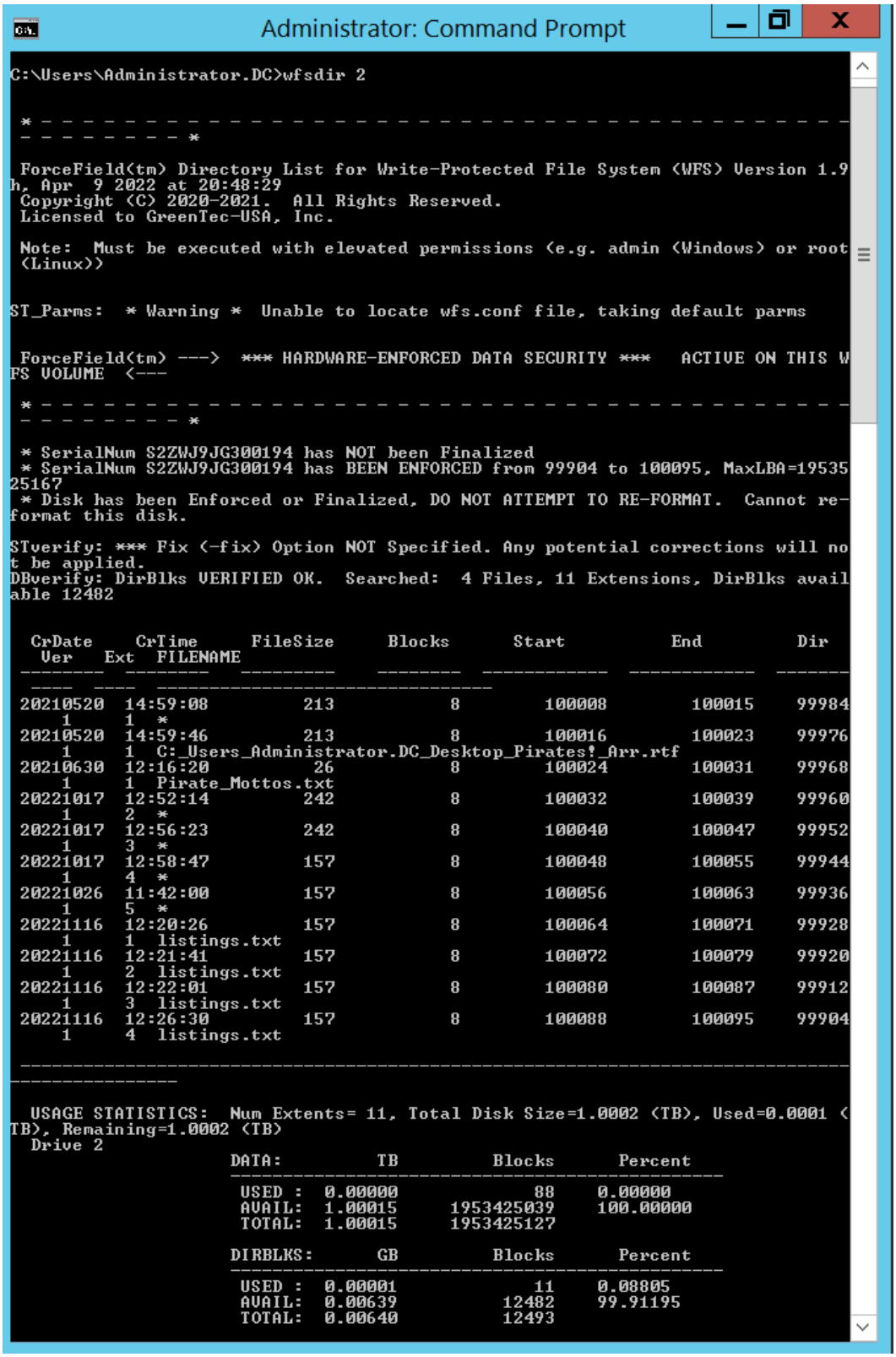
ForceField is a Write-Protected File System (WFS) combining hardware device security and encryption. In this build, ForceField is primarily used to backup data while maintaining confidentiality through encryption. In this build, we used ForceField is for the protection of a transactional database which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

Installation and Usage of ForceField

1. Either a 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**.



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



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 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:
```

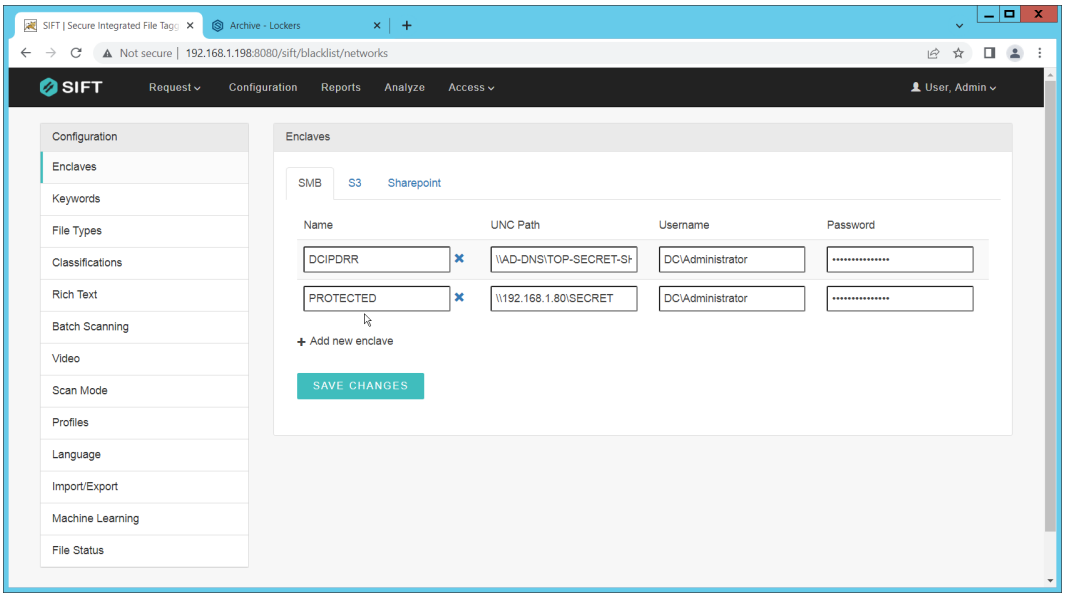
The above command will display the contents of the WFS file myfile.txt from disk 4 onto the console. This is similar to using the type command in the Windows command line.

2.6 Avrio SIFT

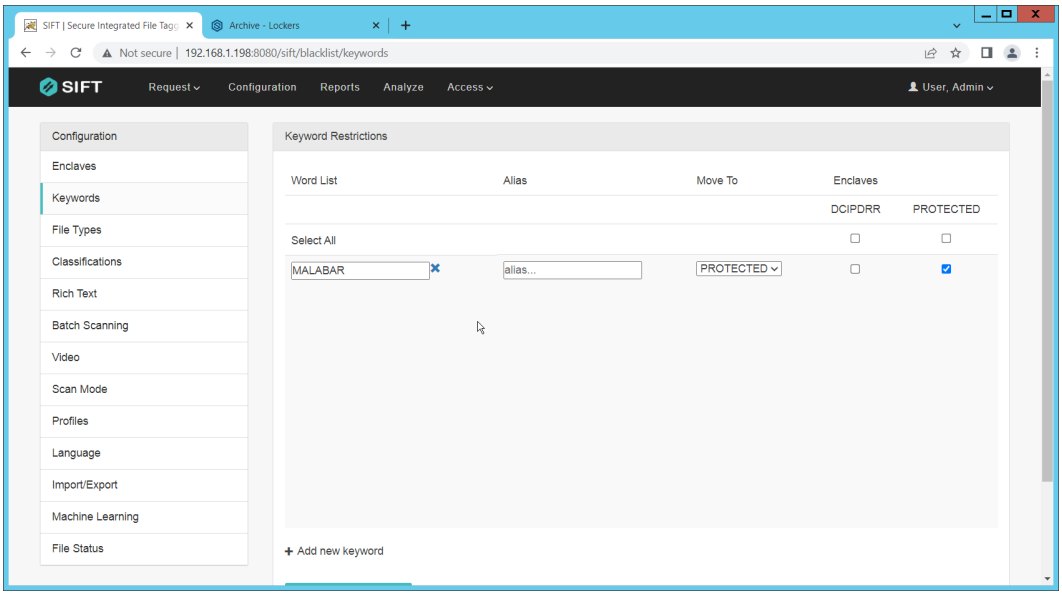
Avrio SIFT is a data inventory and management capability designed to enforce data policies. The installation of Avrio SIFT is typically done in a managed fashion by the vendor, and the deployment seen in the NCCoE lab may not resemble other deployments. In the case of a Docker deployment, configuration 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.

Configuring Avrio SIFT

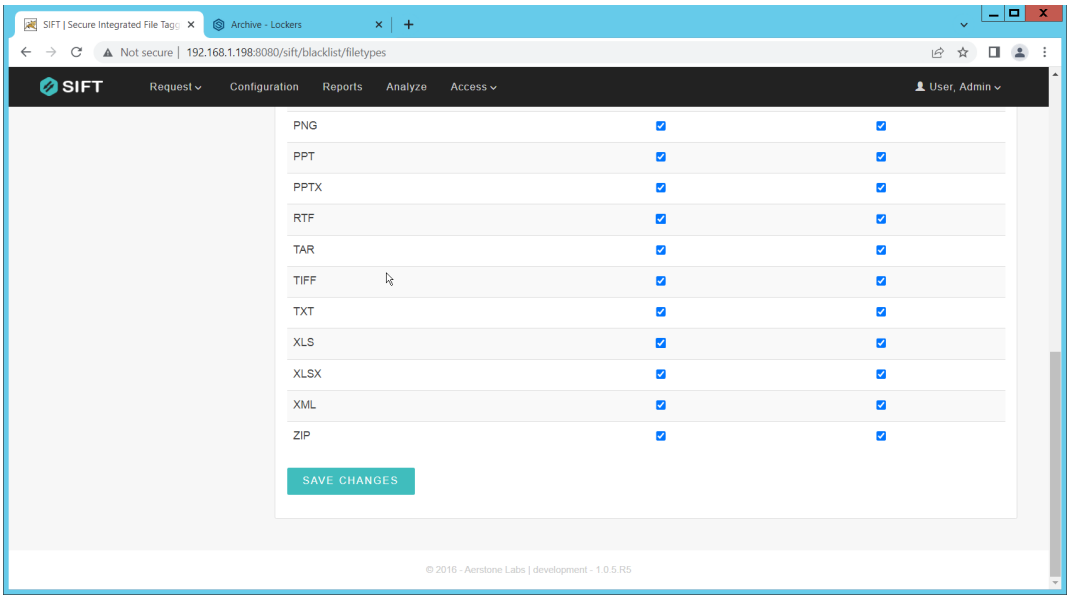
1. Navigate to the SIFT dashboard (default address: http://IP-address:8080/sift/) and login.
2. Click **Configuration**.
3. Under **Enclaves**, enter two locations. First, the path to the public Windows share, and second, the path to the one protected by PKProtect. We will use this second path later 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.



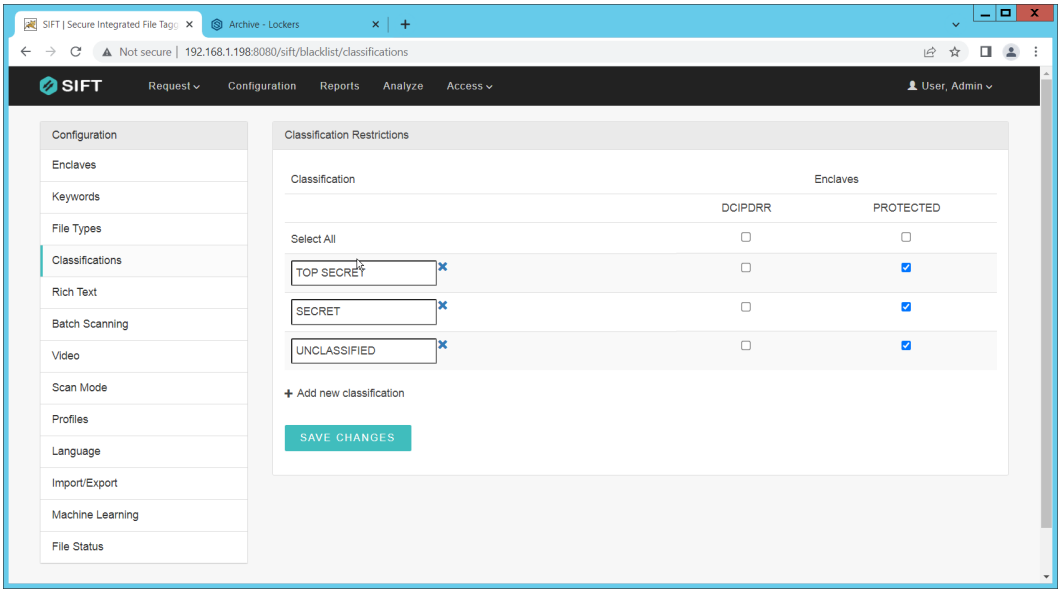
4. Click **Save Changes**.
5. Click **Keywords** on the left menu.
6. Click **Add new keyword**.
7. Enter the keyword under **Name**, and an **Alias** (if desired). Check the box next to any enclaves which are allowed to have this keyword – SIFT will be able to move files matching it to the enclaves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



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

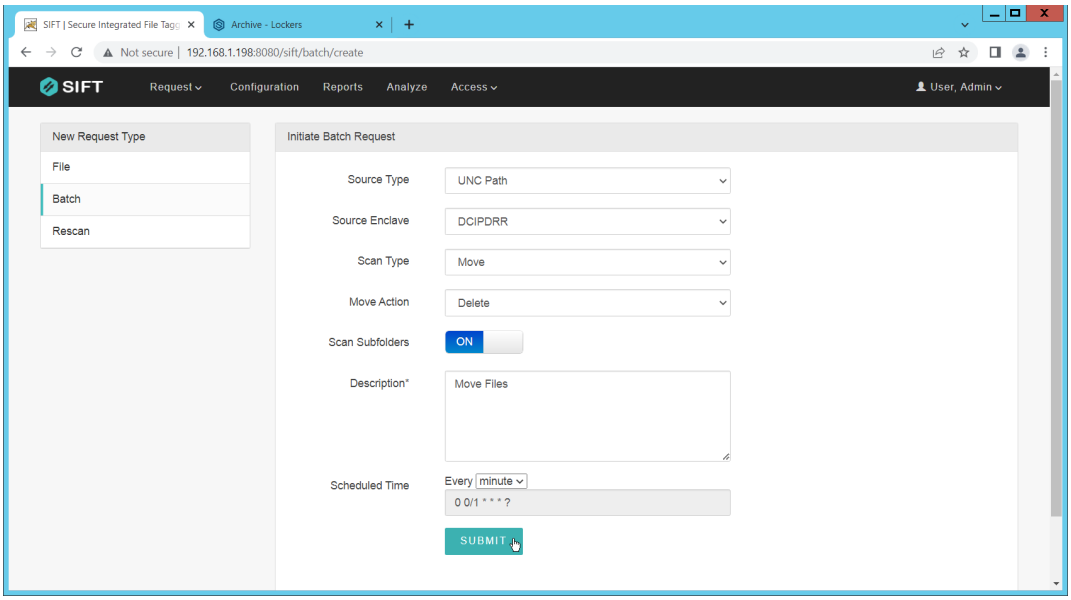


707 12. Click **Save Changes**.
708 13. Click **Classifications**.
709 14. Designate the classifications which are allowed to exist under each enclave.



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

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.



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

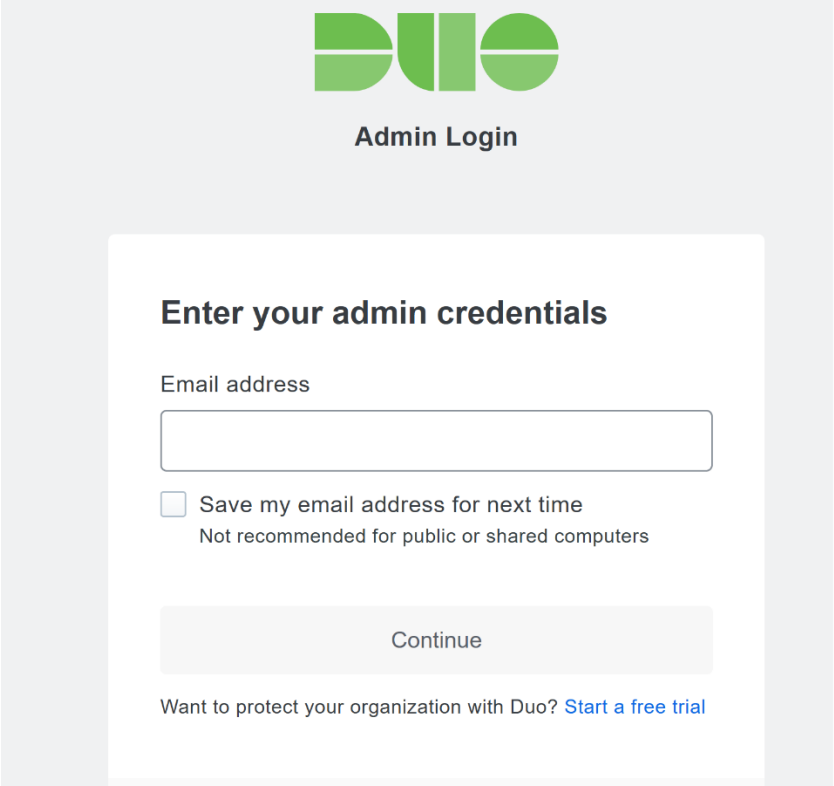
2.7 Cisco Duo

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.

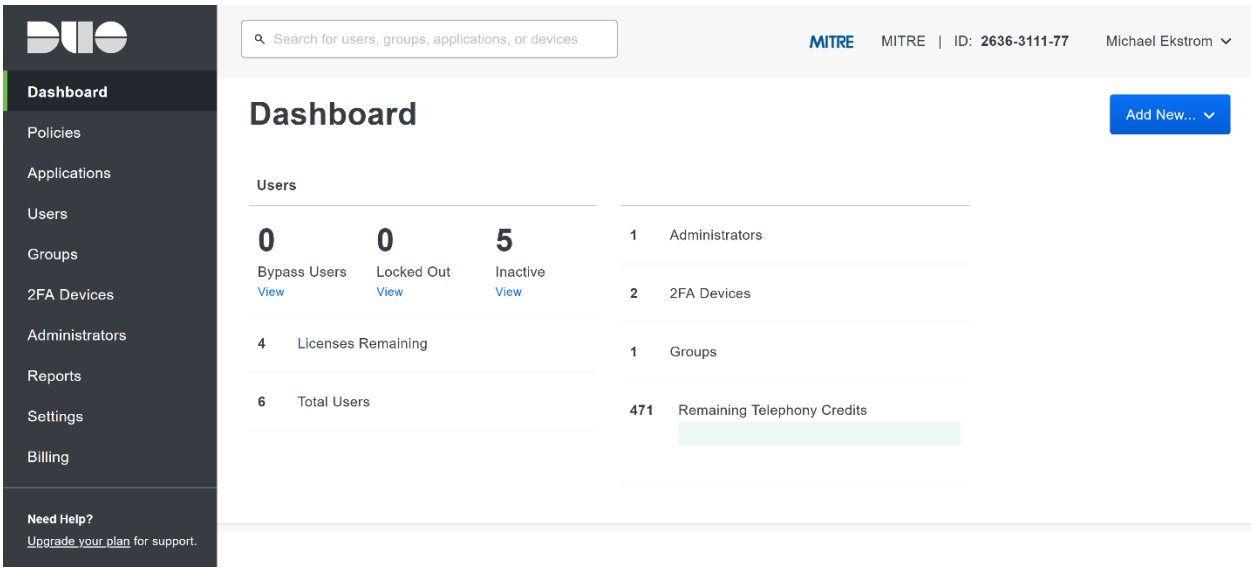
In the following section, we demonstrate the installation of Cisco Duo on an internal system in such a way that RDP and local login to that system is protected by multifactor authentication.

Installing Cisco Duo

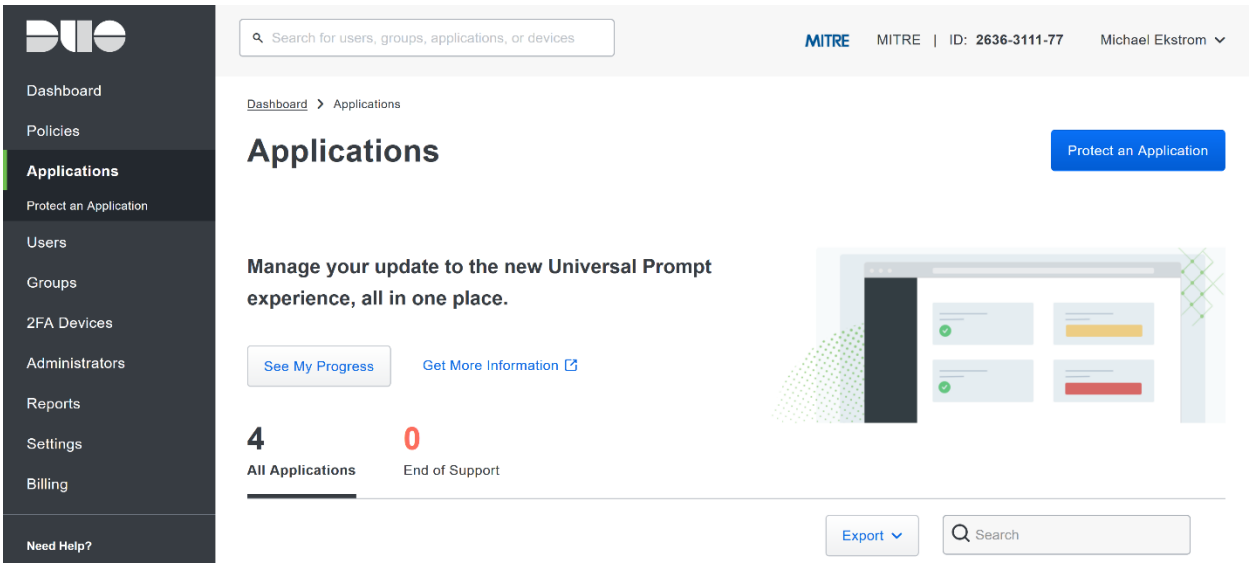
1. Begin by logging into the system you wish to protect with Duo.
2. Then connect to the internet, if not connected already, and go to the Duo Admin login page at https://admin.duosecurity.com/.



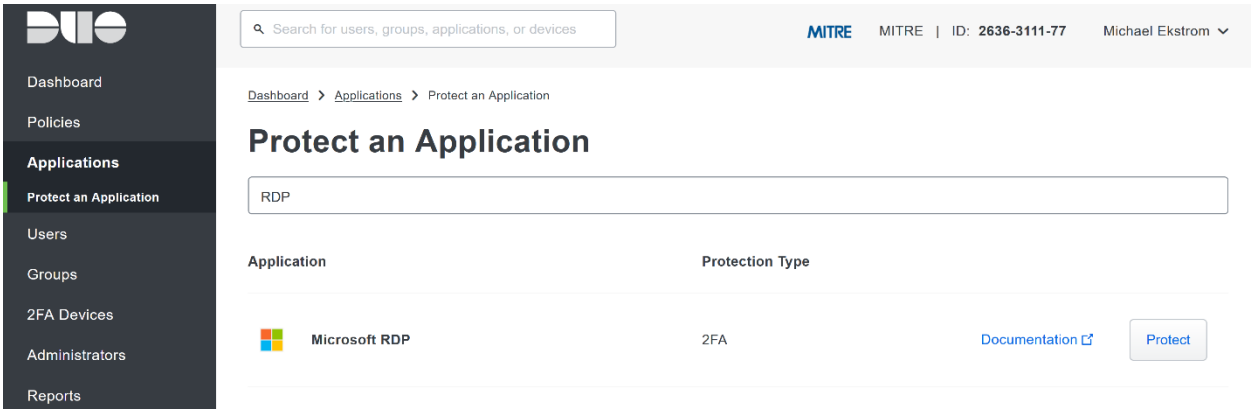
3. Login with your admin credentials and dual factor authentication until the admin dashboard is reached.



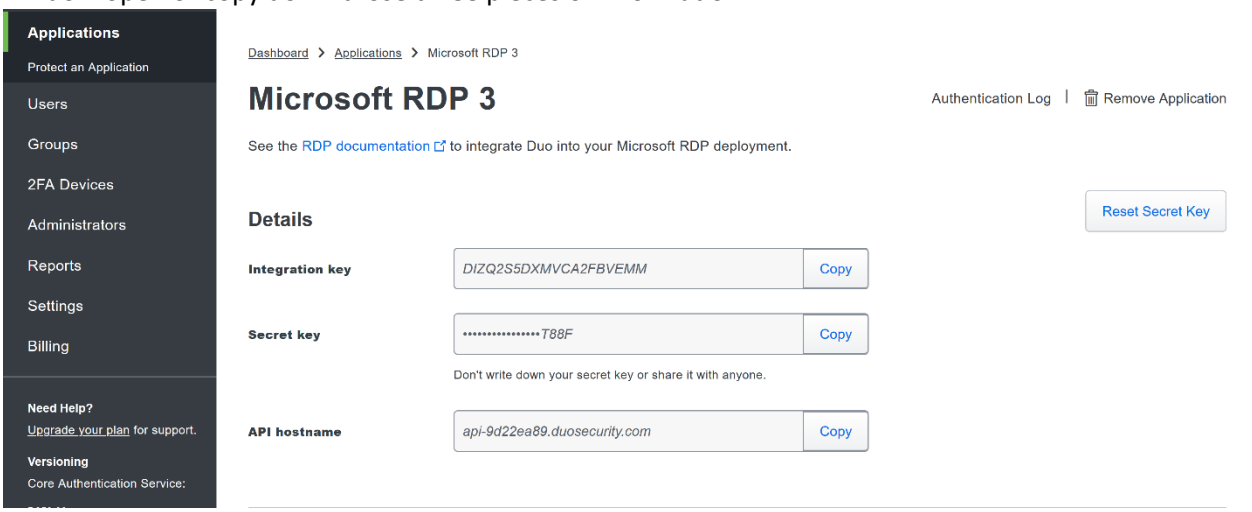
4. Click **Applications** in the sidebar.
5. Click **Protect an Application**.



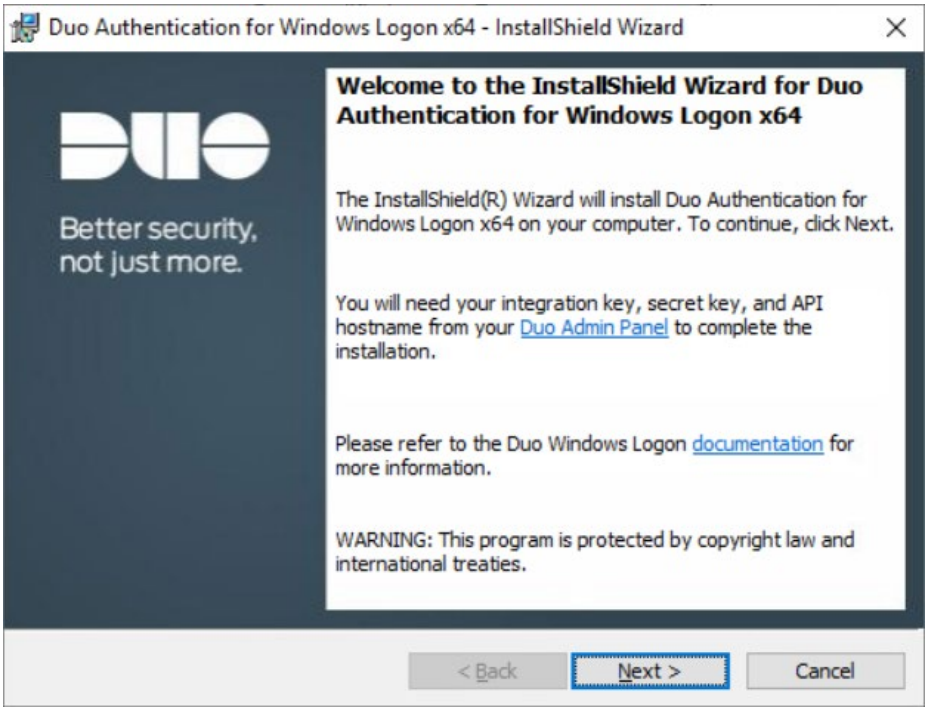
745 6. Search for, or scroll down to, **Microsoft RDP**.
746 7. Click **Protect**.



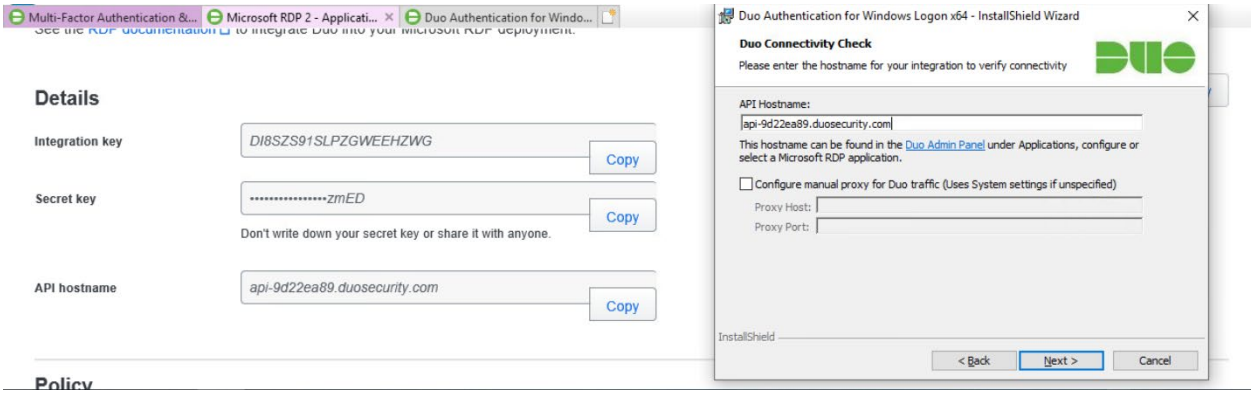
747 8. The next screen will provide policy configuration options, as well as the **Integration Key**, **Secret**
748 **Key**, and **API hostname**, which are required information for the next step. Either keep this
749 window open or copy down those three pieces of information.



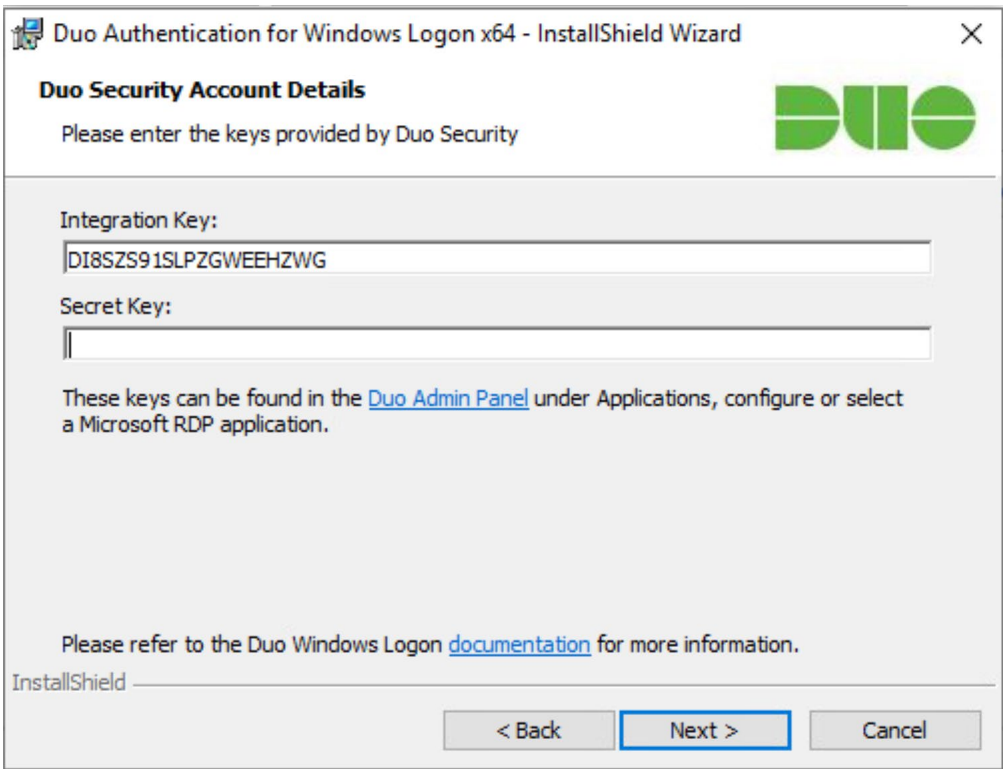
9. Download the **Duo Authentication for Windows Logon** installer package, located at https://dl.duosecurity.com/duo-win-login-latest.exe.
10. Run the downloaded EXE file.



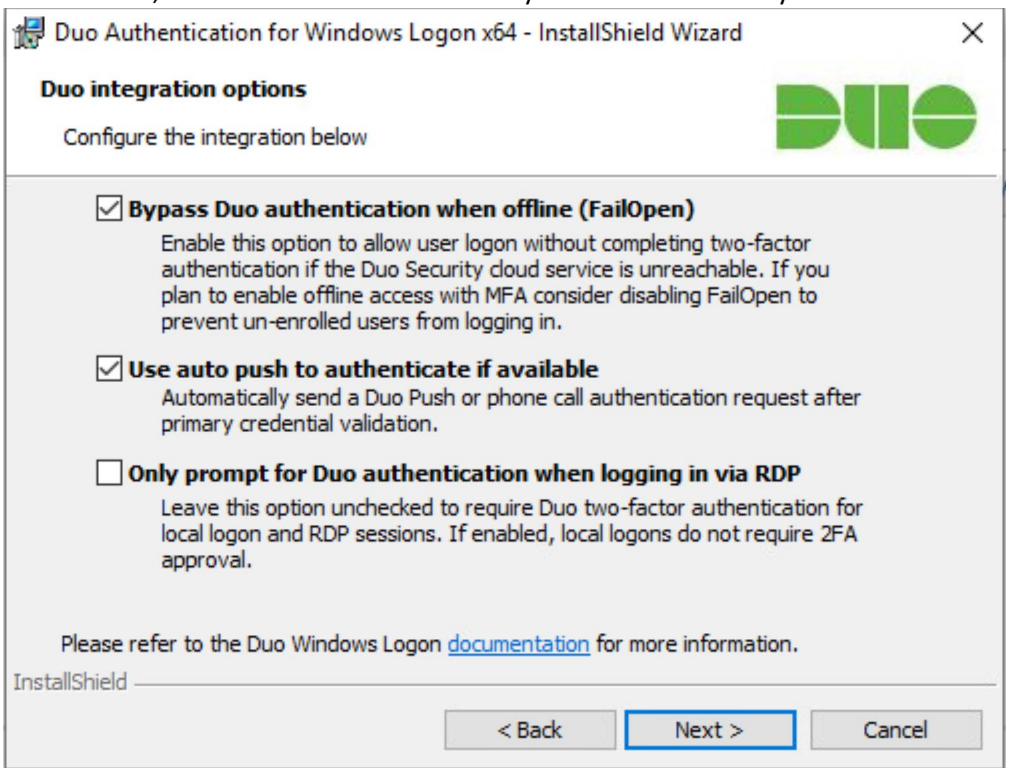
11. Click **Next**.
12. Copy the **API Hostname** into the labeled field.



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

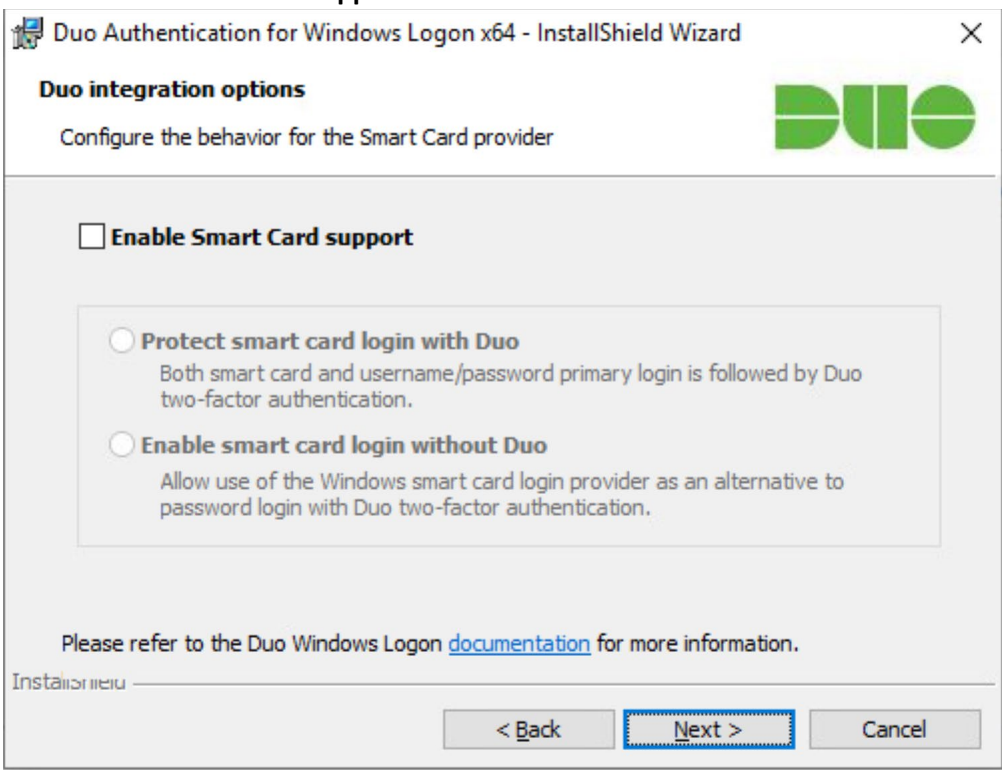


15. Click **Next**.
16. Configure Duo's integration options according to the needs of your organization. Note that **Bypass Duo authentication when offline** will allow users to skip the two-factor authentication when offline, which increases the availability of their files but may increase risk.



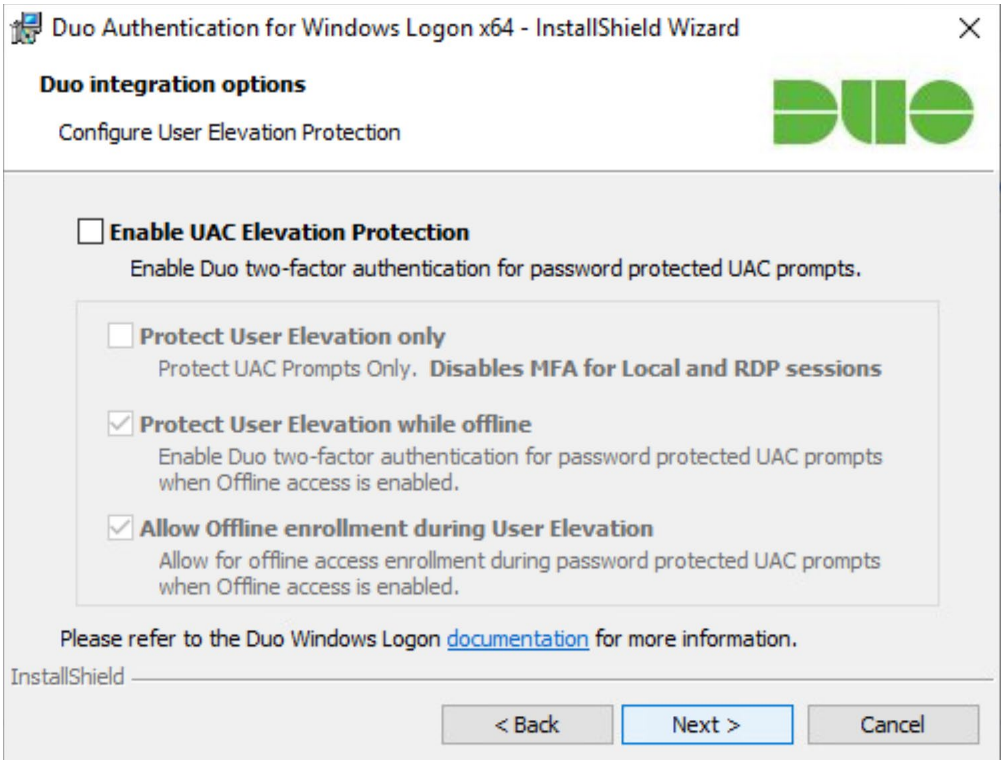
17. Click **Next**.

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

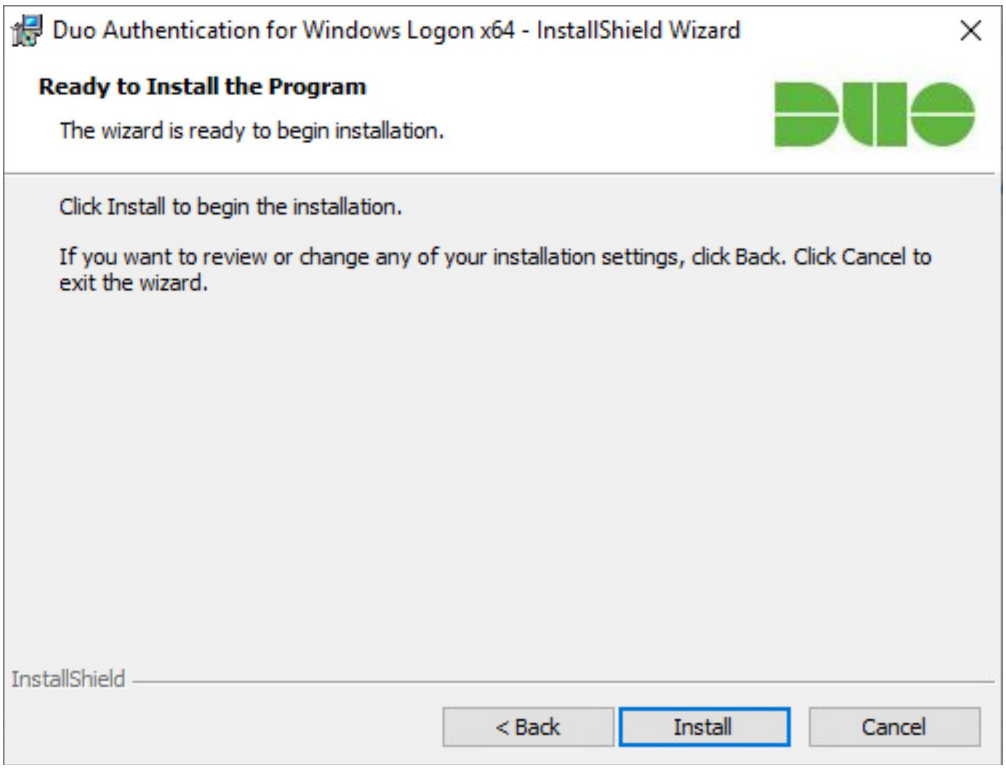


19. Click **Next**.

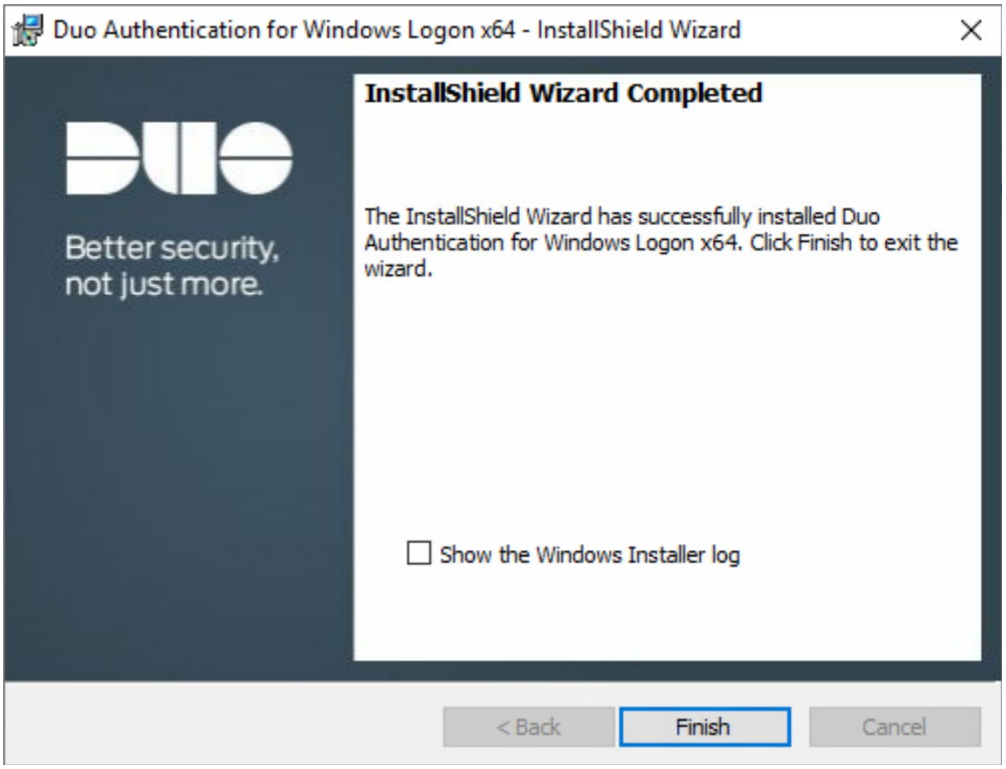
20. Leave **Enable UAC Elevation Protection** unchecked.



21. Click **Next**.



765 22. Click **Install**.

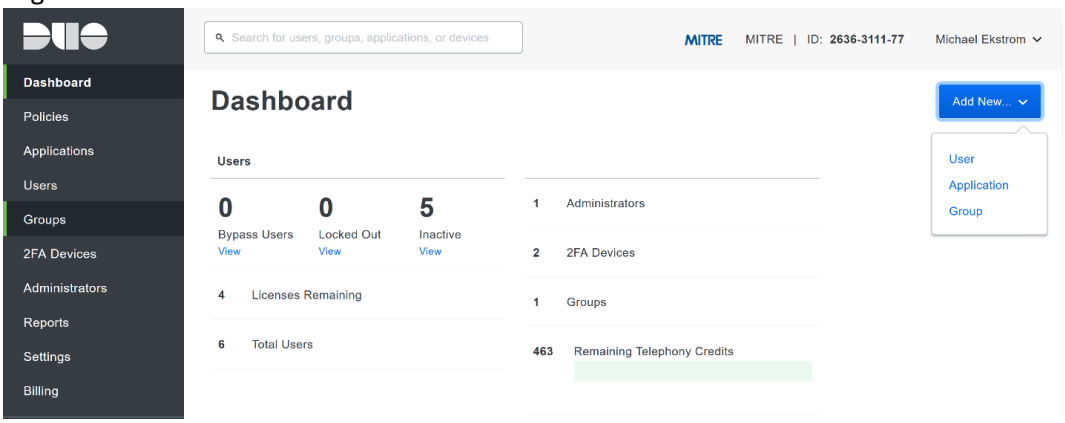


766 23. Click **Finish**.

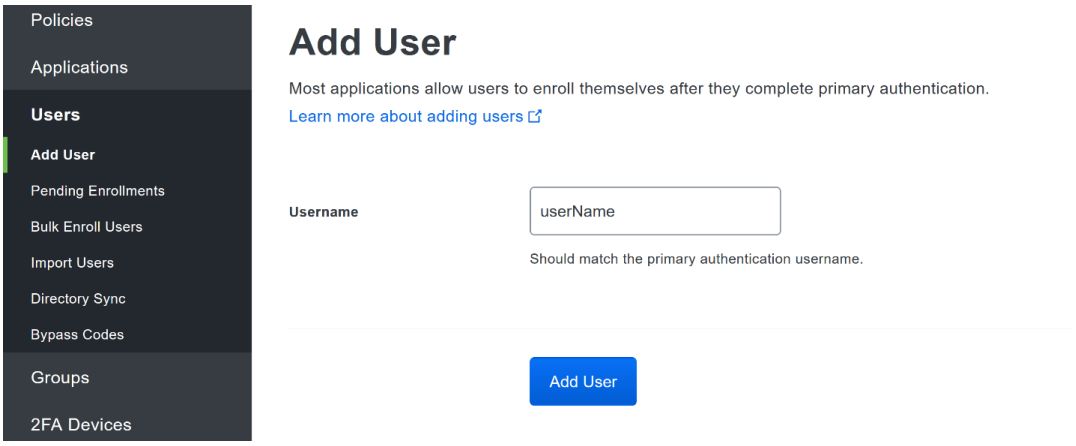
767 24. Installation should now be complete. Users registered on the Duo Dashboard with a linked
768 phone will be allowed access to the system.

Registering a Duo User

1. Login to the Duo Admin Dashboard.



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



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, 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 WAN and LAN interfaces, placing the device in-line between the enterprise systems and the external network.

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. Being 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':
```

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

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


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

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

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

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

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

798 10. Log in with the user “dispel” and the new password set in step 9.

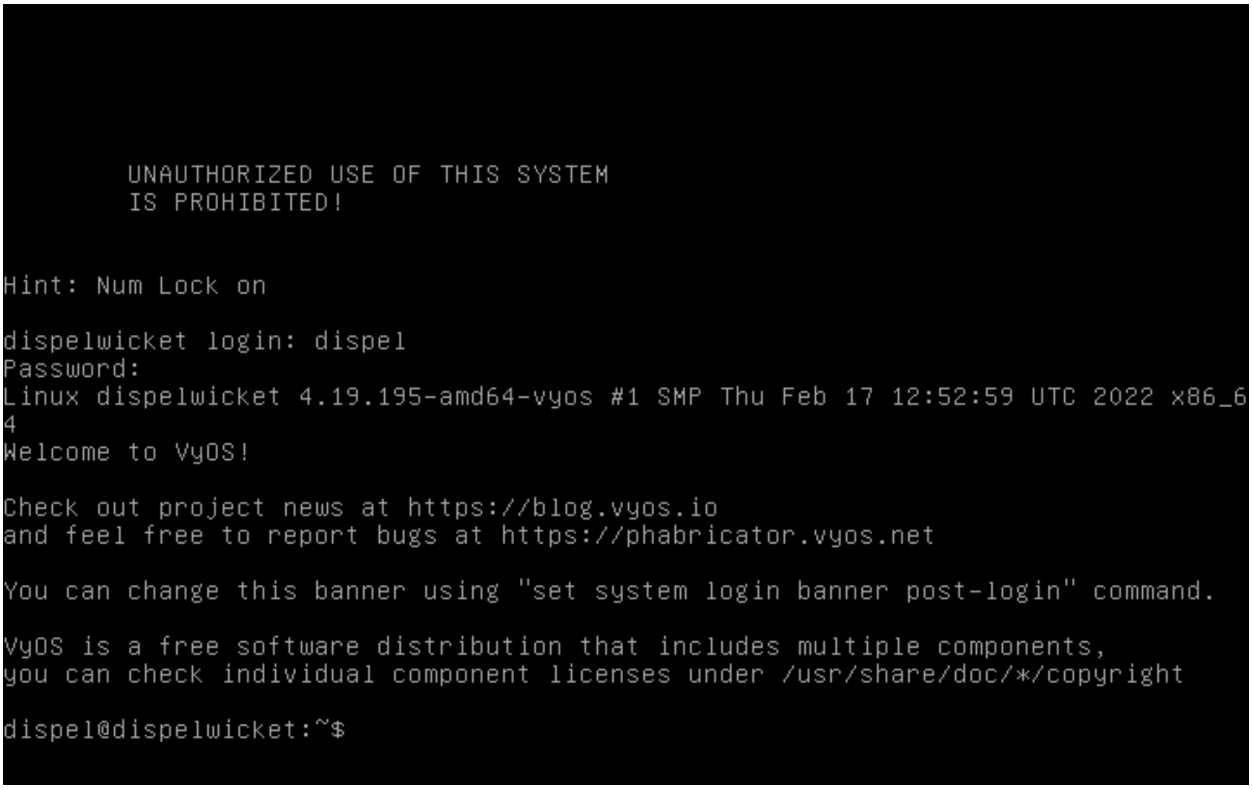
```
        UNAUTHORIZED USE OF THIS SYSTEM
        IS PROHIBITED!


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:~$ _
```

799 11. Type in the command > `ifconfig | grep inet`. Verify the output to make sure it matches
800 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:~$
```

Configuring IP Addresses

1. Login to the device with the user “dispel”.



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:~$
```

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# _
```

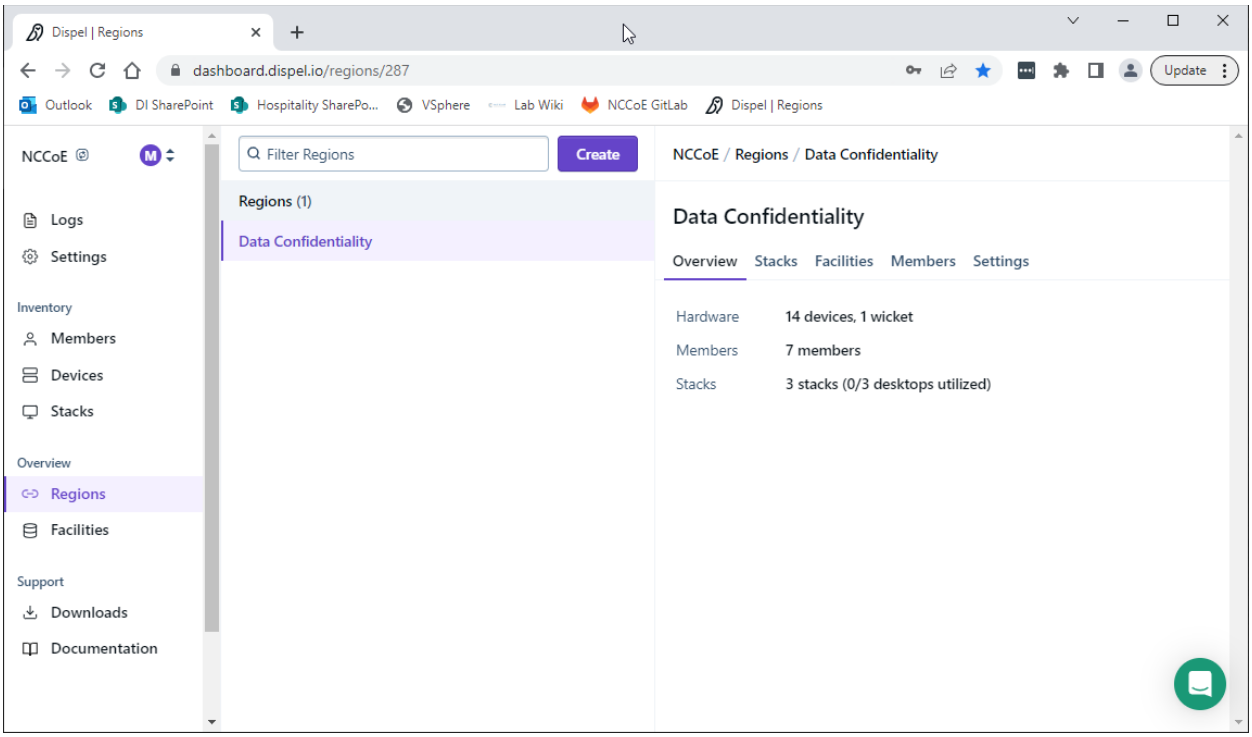
5. Type in the command > `exit`.

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

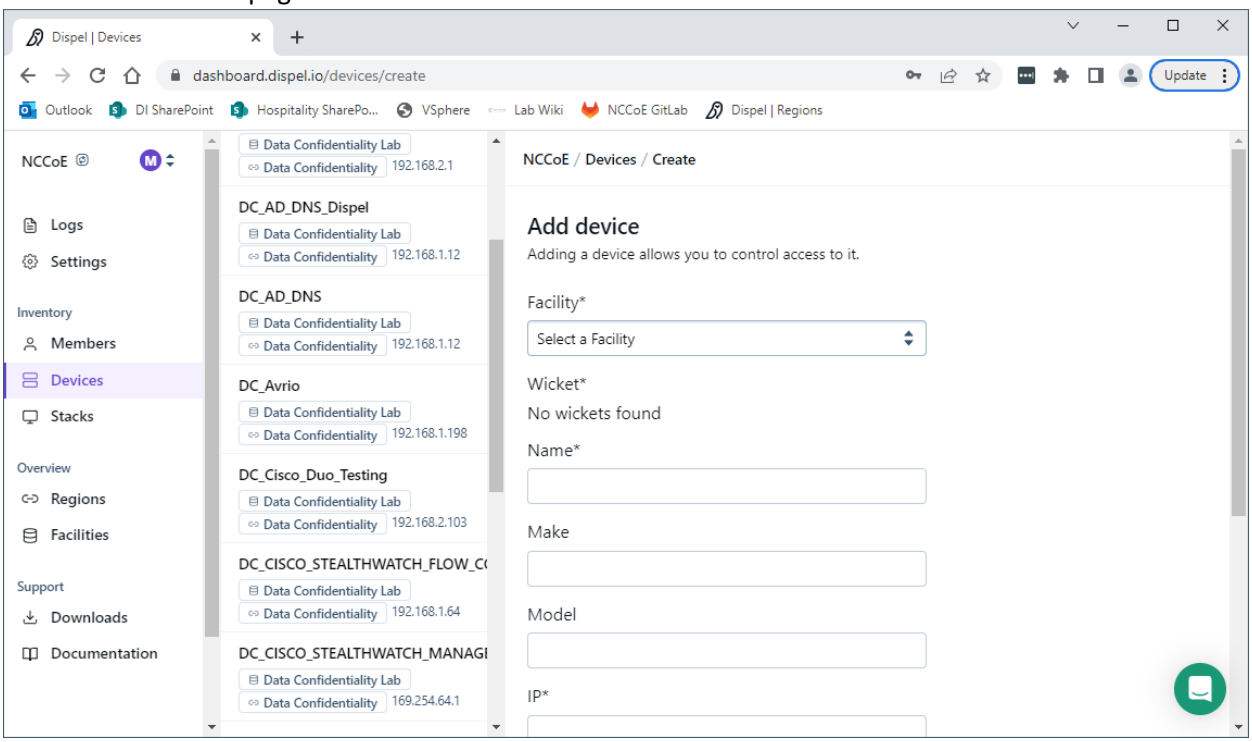
6. On the designated router or firewall, ensure UDP is allowed from the Dispel device on the provided port. For the NCCoE deployment, port 1194 was utilized. A target destination for the traffic will be provided by Dispel.
7. Modify the IP addresses of the south-side network interface to properly align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

Adding a Device

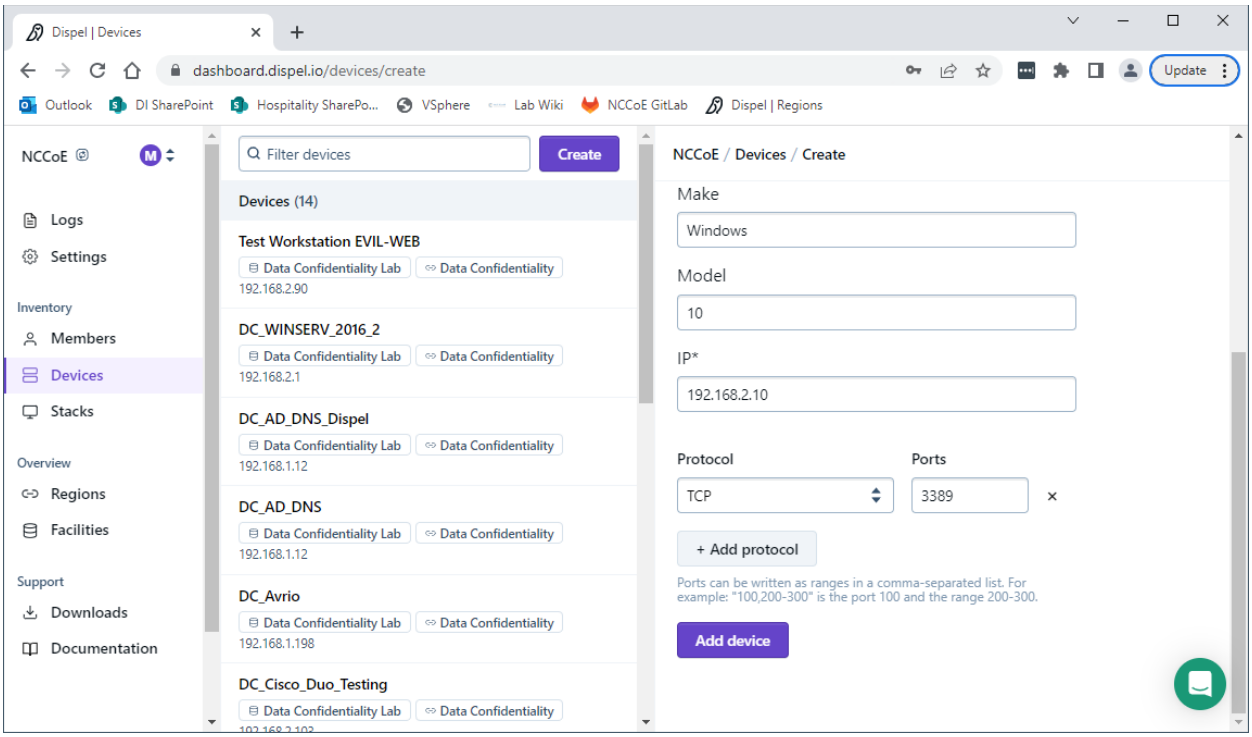
1. On the workstation in question, ensure that ping and RDP are accessible, including allowing such connections through a local firewall.
2. Authenticate to the Dispel webpage with the provided credentials.



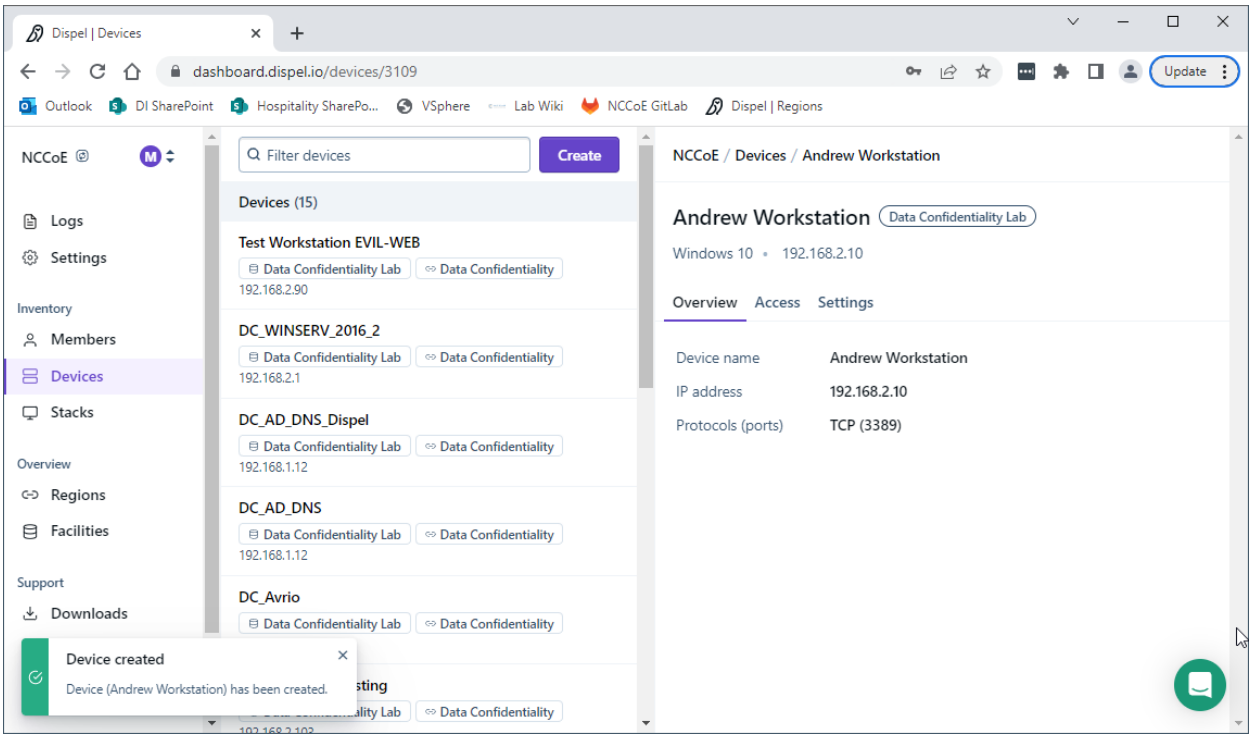
3. Click on the **Devices** page on the sidebar and click **Create**.



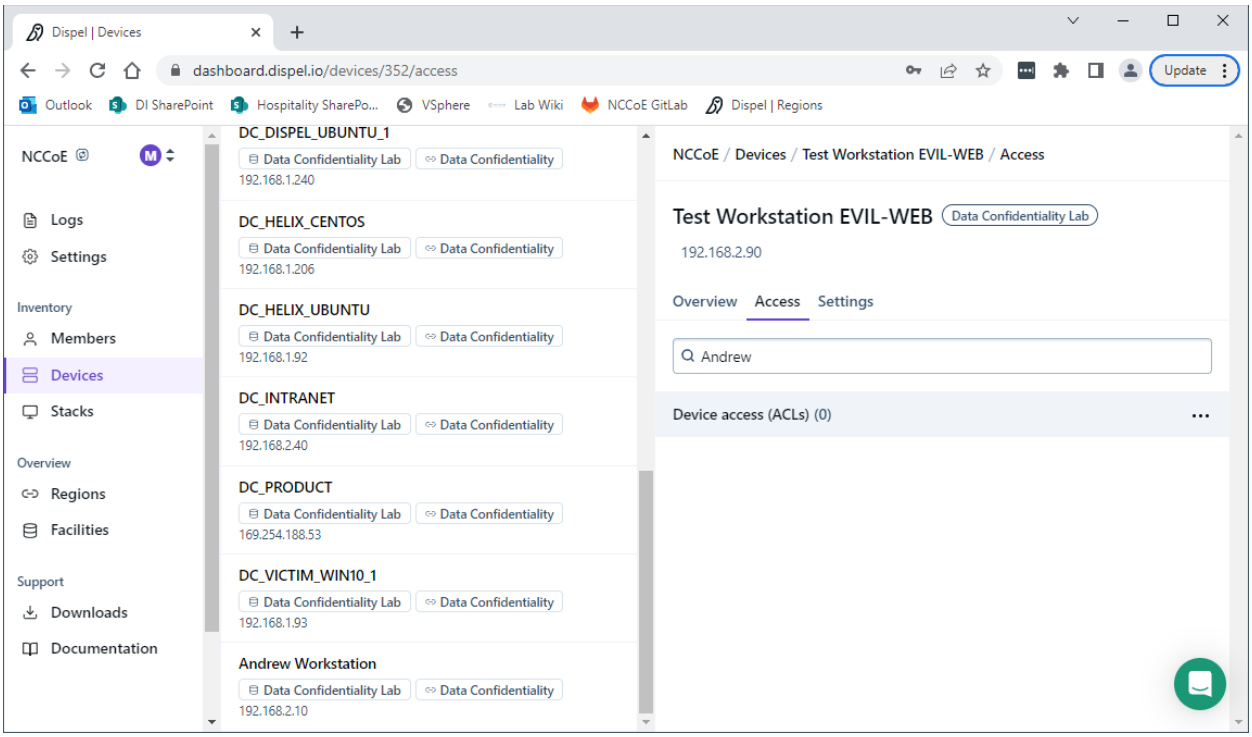
4. Under the **Add Device** window, fill out all fields, including **Facility**, **Wicket**, **Name**, **Make**, **Model**, **IP**, and **Protocol**.



833 5. Click **Add Device**.



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



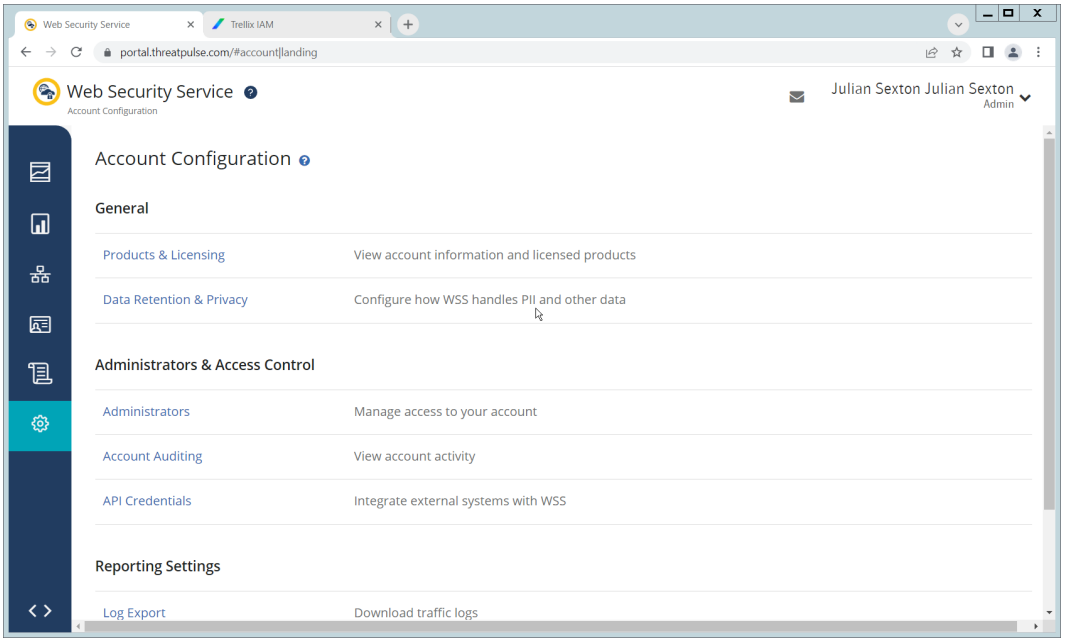
7. If a user is not already a member of the region, click **Members** in the sidebar and click **Invite.** Fill out relevant information for this individual and click **Invite this Member.**

2.9 Integration: FireEye Helix and Symantec SWG

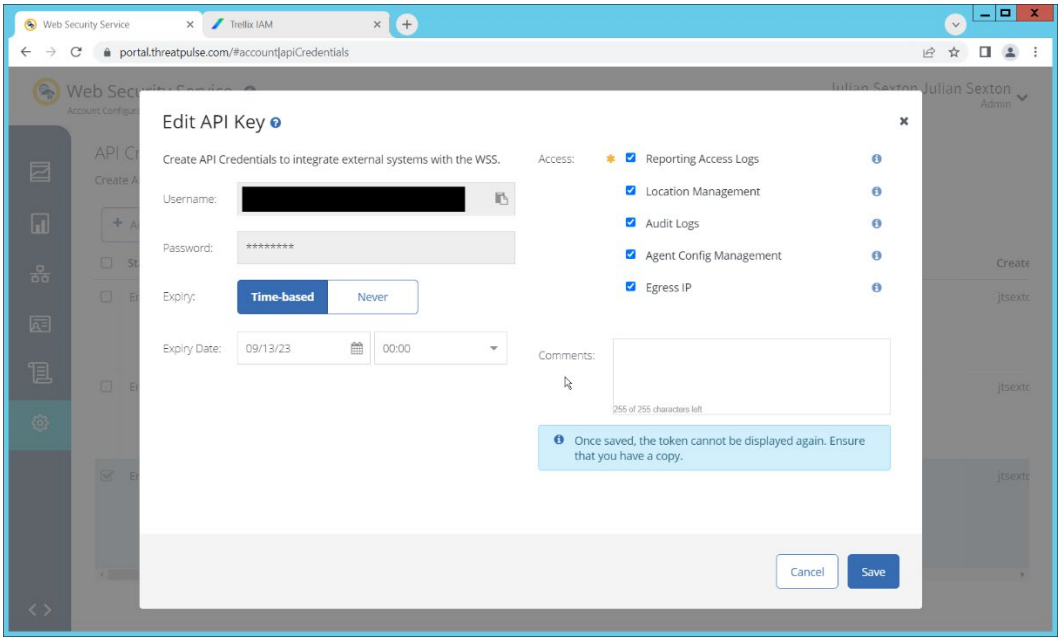
In this integration the output of the web isolation tool, Symantec SWG, will be forwarded to our SIEM, FireEye Helix. In this guide, we will aim to forward most logs to our SIEM, which can collect, analyze, and report on these logs to better maintain awareness of our systems and provide a single interface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

Configure Fireye Helix to Collect Logs from Symantec SWG

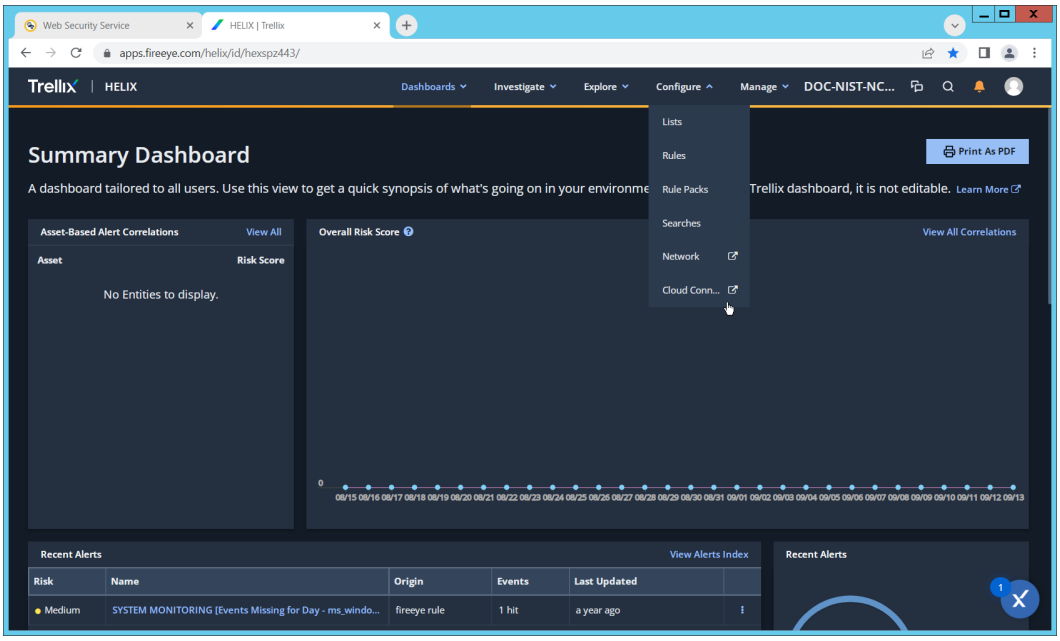
1. Navigate to the Symantec dashboard, and login.
2. Navigate to **Account Configuration** by clicking the gear icon on the left sidebar.



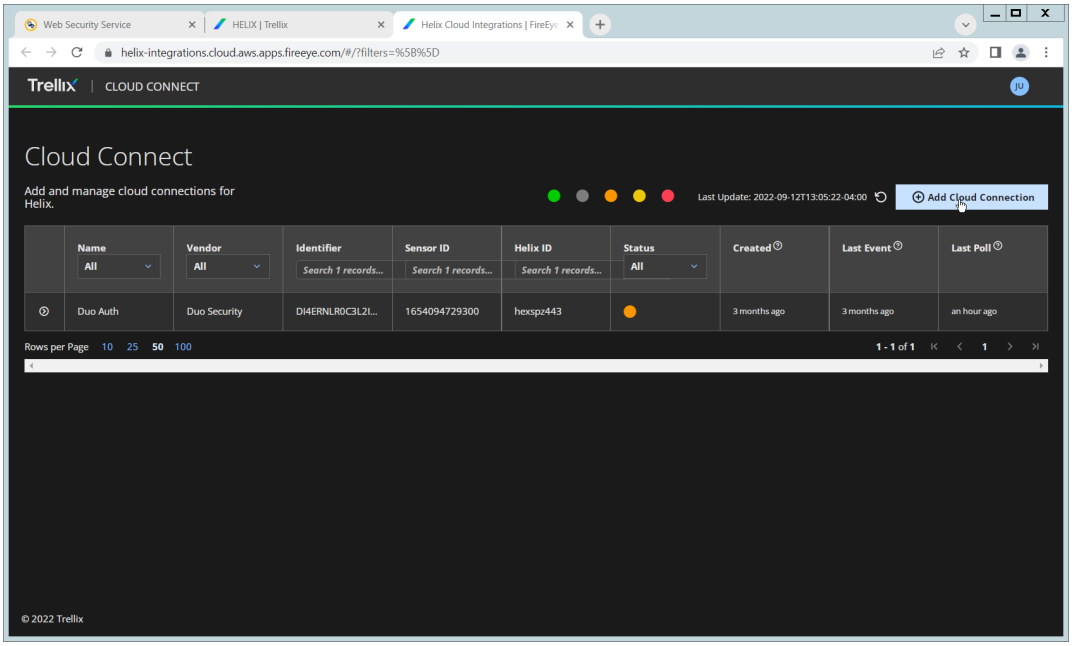
3. Click **API Credentials**.
4. Click **Add**.
5. Check the boxes next to **Reporting Access Logs**, **Location Management**, **Audit Logs**, **Agent Config Management**, and **Egress IP**.
6. Set an **Expiration Date** for the credential (1 year recommended).
7. Copy the **Username** and **Password**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



8. Click **Save**.

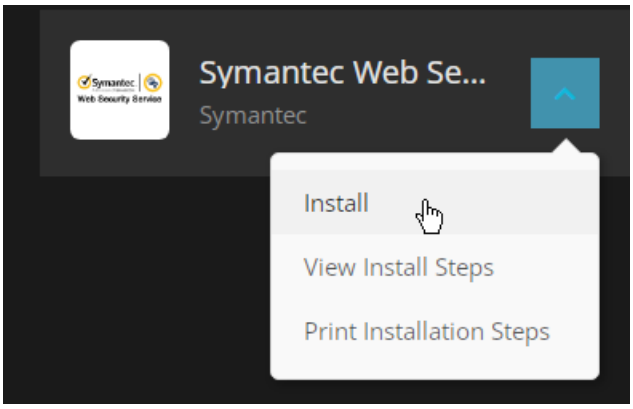


855 9. On the Helix Dashboard, click **Configure > Cloud Connect**.

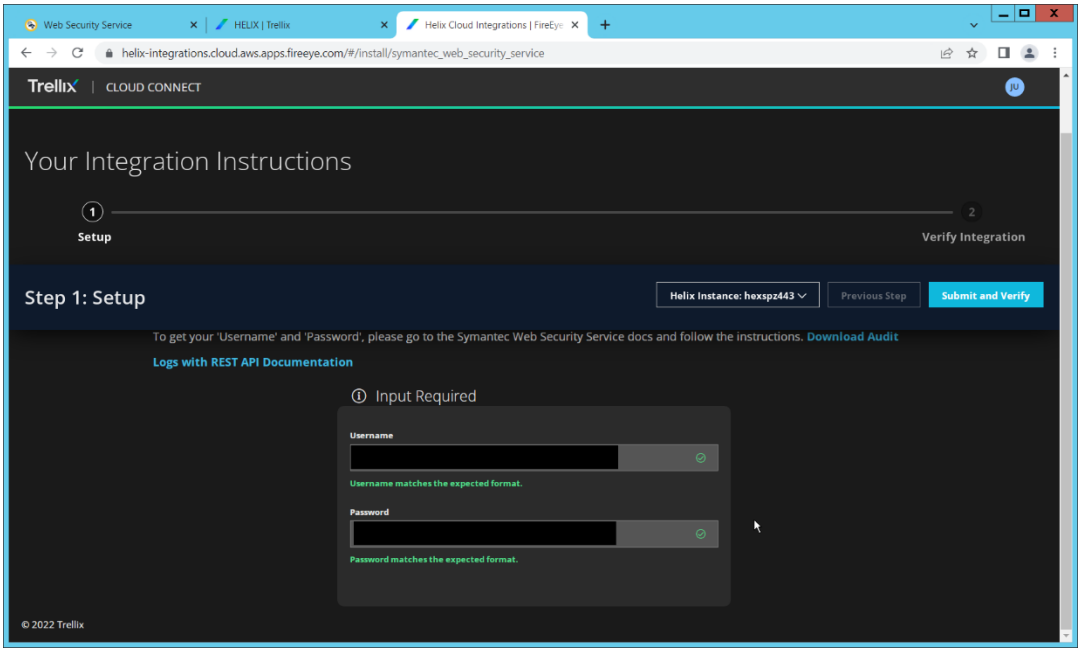


856 10. Click **Add Cloud Connection**.

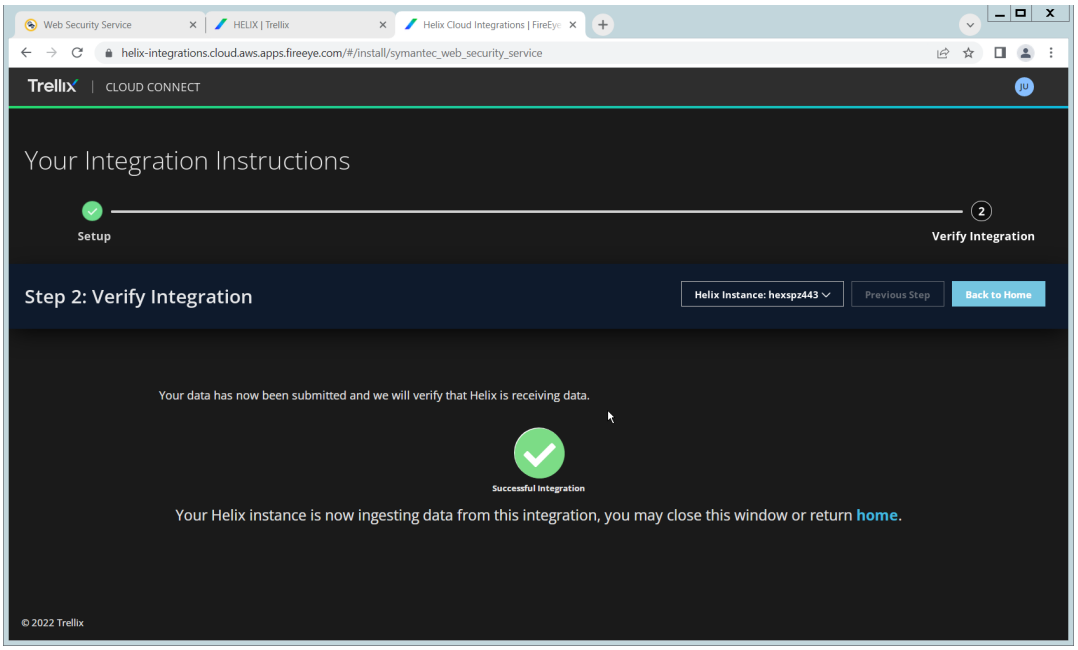
857 11. Click the arrow next to Symantec Web Security Service.



858 12. Click **Install**.



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



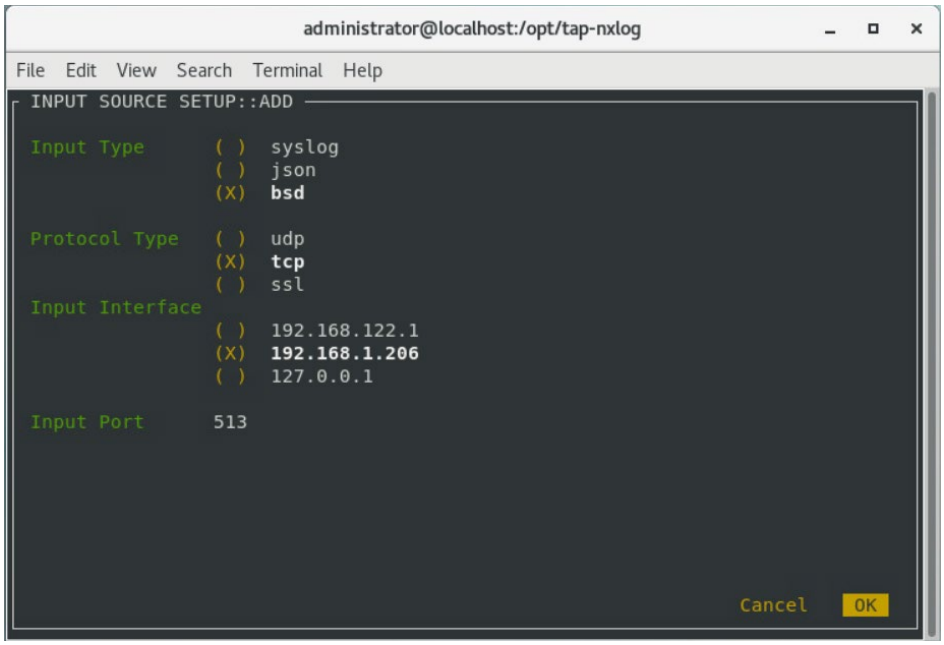
14. Click **Submit and Verify**.
15. Click **Back to Home**. You will now be able to see events from Symantec WSS in Helix.

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 which may indicate a breach. This section assumes the Helix Communications Broker has already been installed.

Configure the Helix Communications Broker

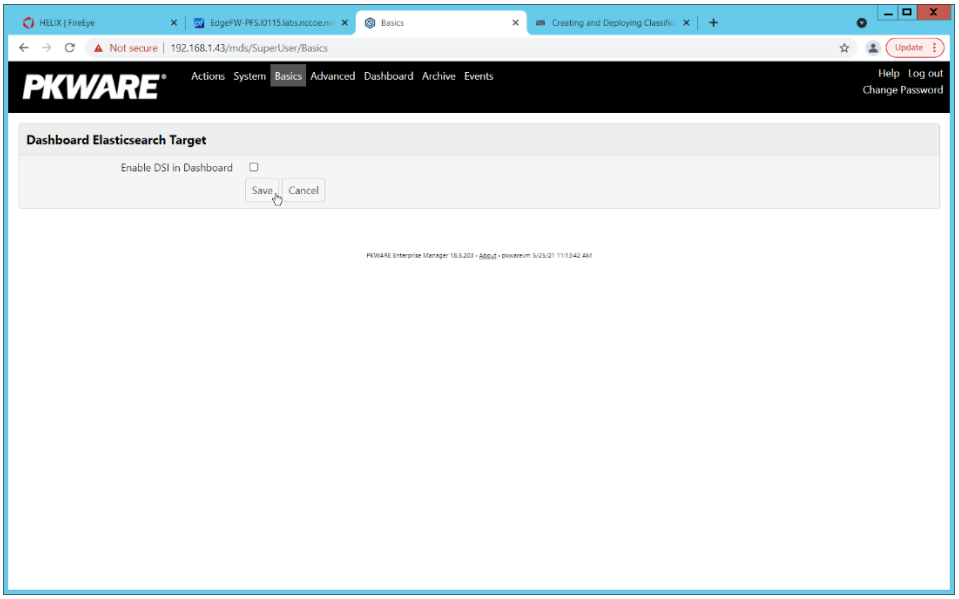
1. On the CentOS system with the Helix Communications Broker installed, run the following commands:
   ```
   > cd /opt/tap-nxlog
   > sudo ./setup.sh
   ```
2. Select **Add Routes** and press **Enter**.
3. Select **bsd**.
4. Select **tcp**.
5. Select the IP address of the network interface which should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



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

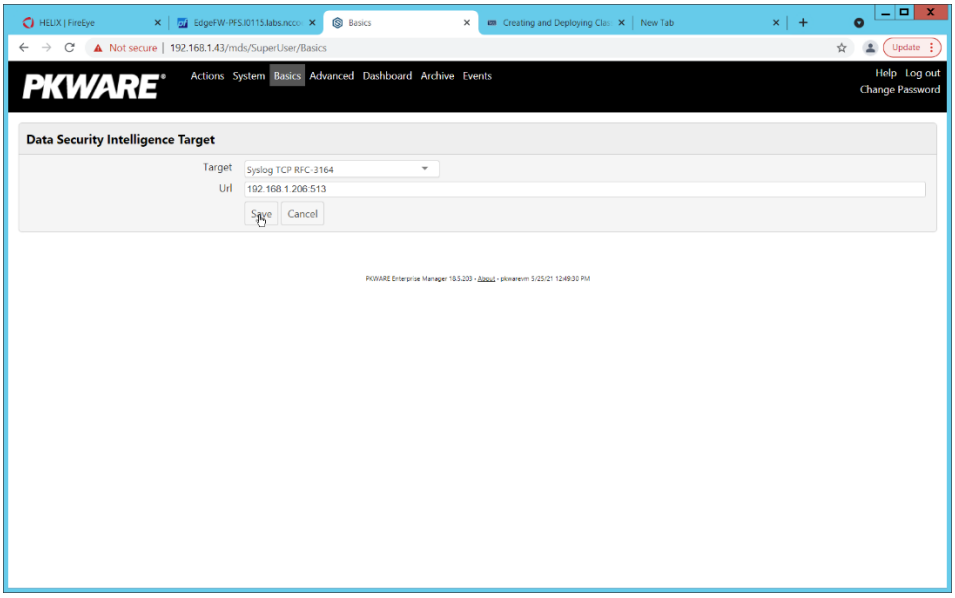
880 ## Configure PKWARE PKProtect to Forward Events

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



887 7. Click **Save**.
888 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.



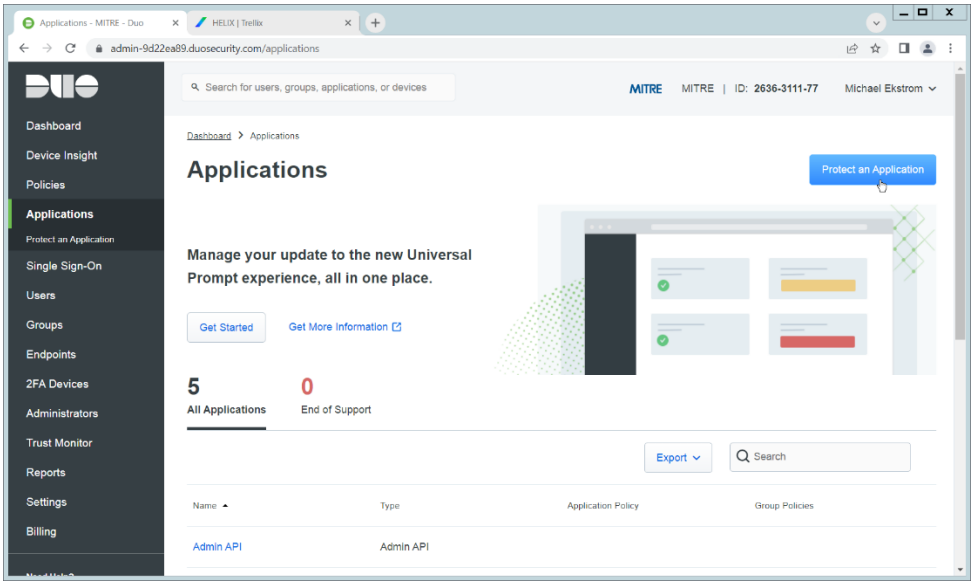
11. Click **Save**.
12. Verify that PKWARE logs now show up in Helix.

2.11 Integration: FireEye Helix and Cisco Duo

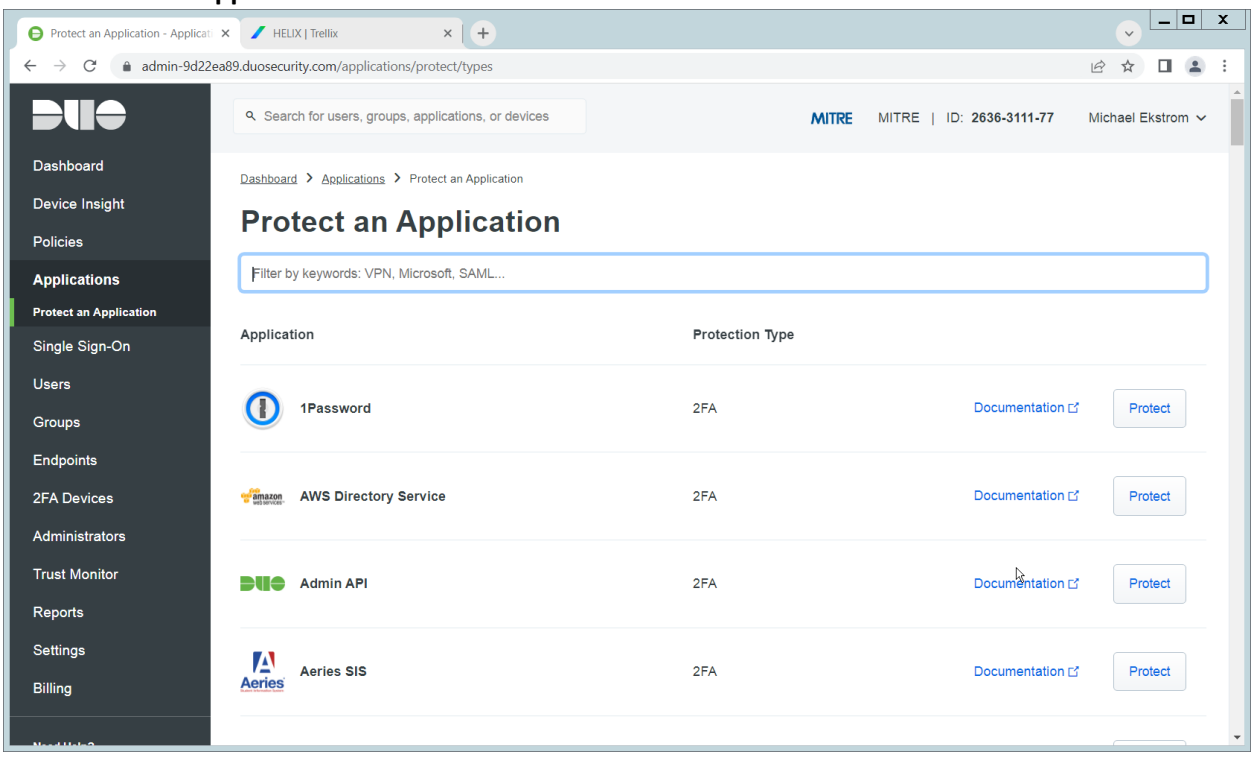
In this integration, FireEye Helix will be configured to collect logs from Cisco Duo. Cisco Duo is our multi-factor authentication mechanism and acts as source of information both for detecting breaches and for detecting insider threats. Information about a login, such as the username, time, location, 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.

Configure Fireye Helix to Collect Logs from Cisco Duo

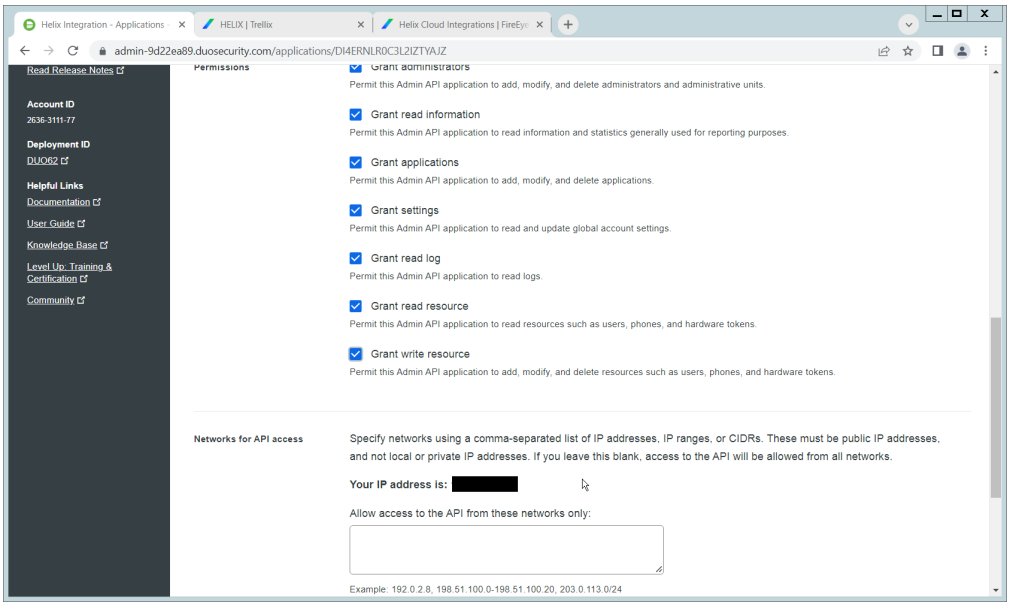
1. On the Cisco Duo dashboard navigate to **Applications**.



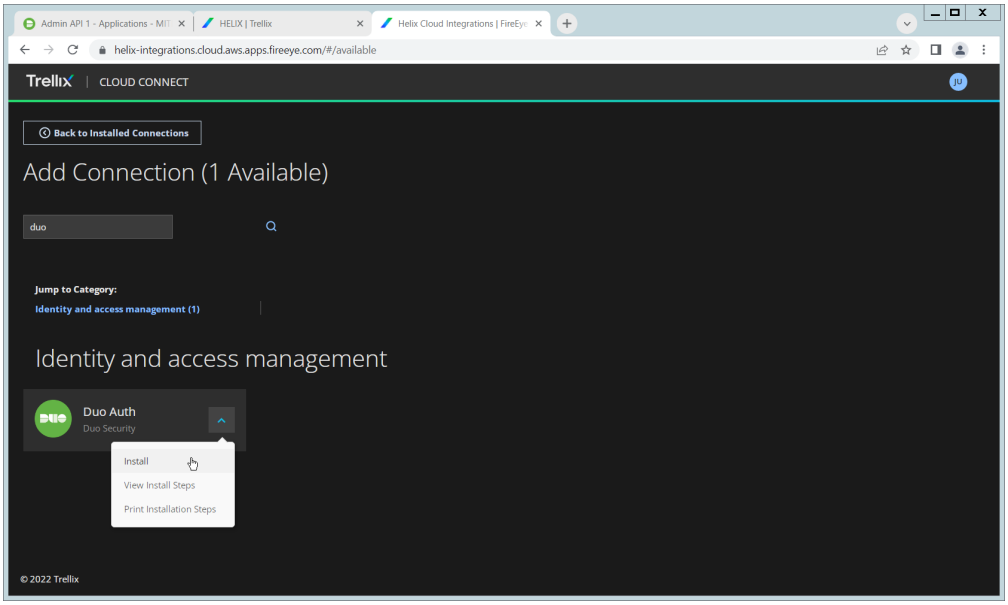
901 2. Click **Protect an Application**.



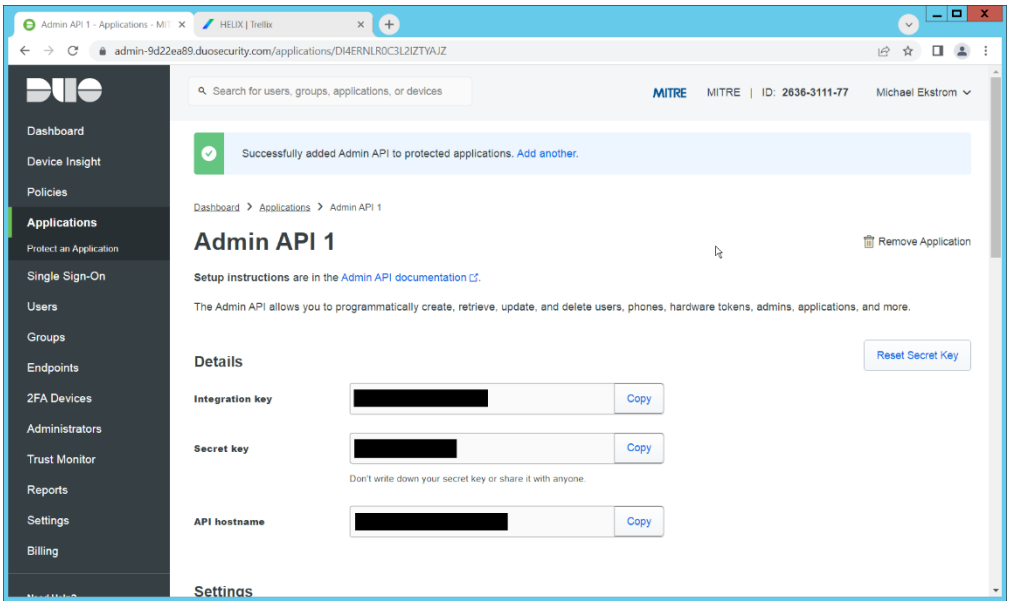
902 3. Click **Admin API**.



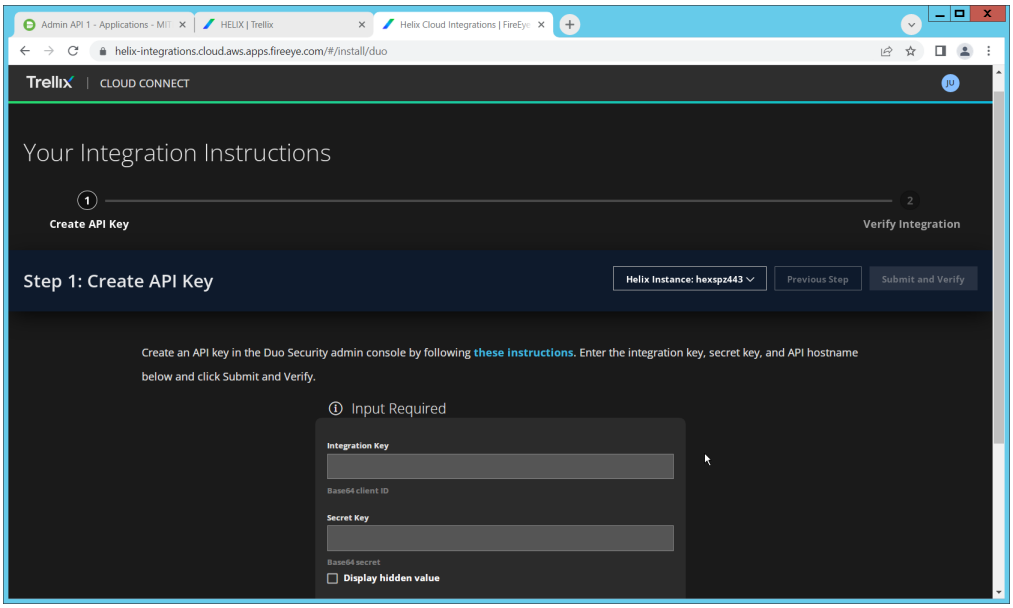
4. Scroll down and check the boxes next to **Grant administrators**, **Grant read information**, **Grant applications**, **Grant settings**, **Grant read log**, **Grant read resource**, and **Grant write resource**
5. Click **Save**.
6. Login to the Helix dashboard.
7. Navigate to **Configure** > **Cloud Connect**.
8. Click **See Available Connections**.
9. Type “Duo” in the Search box.



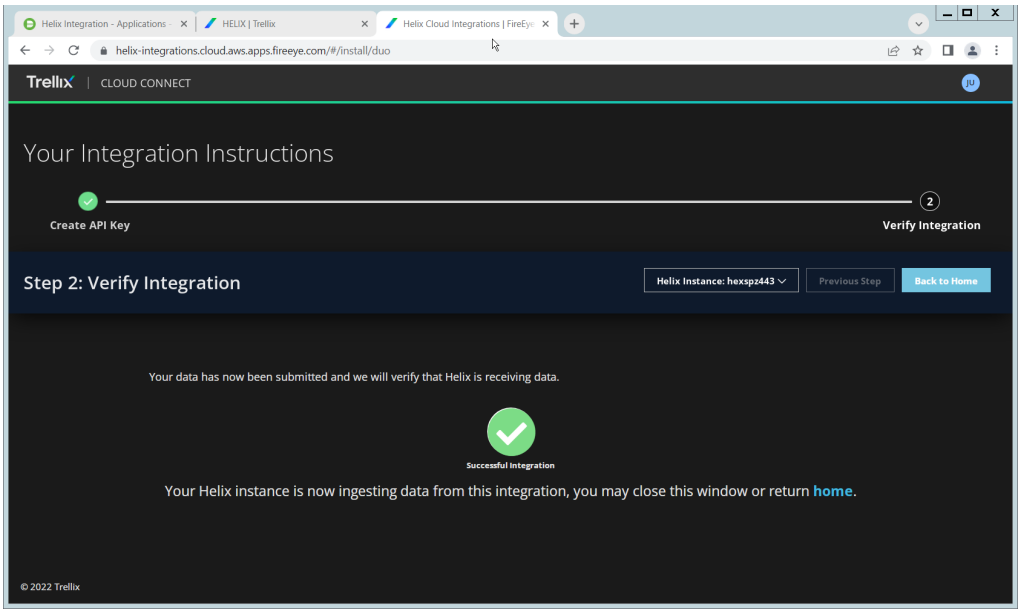
10. Click the **Arrow** next to the Cisco Duo integration and click **Install**.



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



12. Click **Submit and Verify**.



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.

Configure an 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 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 FTPS would at some point require a plaintext password, while SFTP can default to the system's SSH capabilities.

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

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.

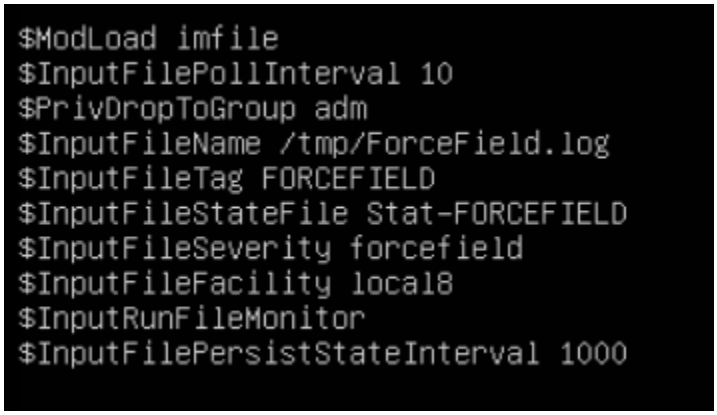
```
0 * * * * sftp
administrator@forcefield.dc.ipdrr:/ForceField.log
/tmp/ForceField.log
```

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
```



25. Restart rsyslog.

```
sudo service rsyslog restart
```

2.13 Integration: FireEye Helix and Dispel

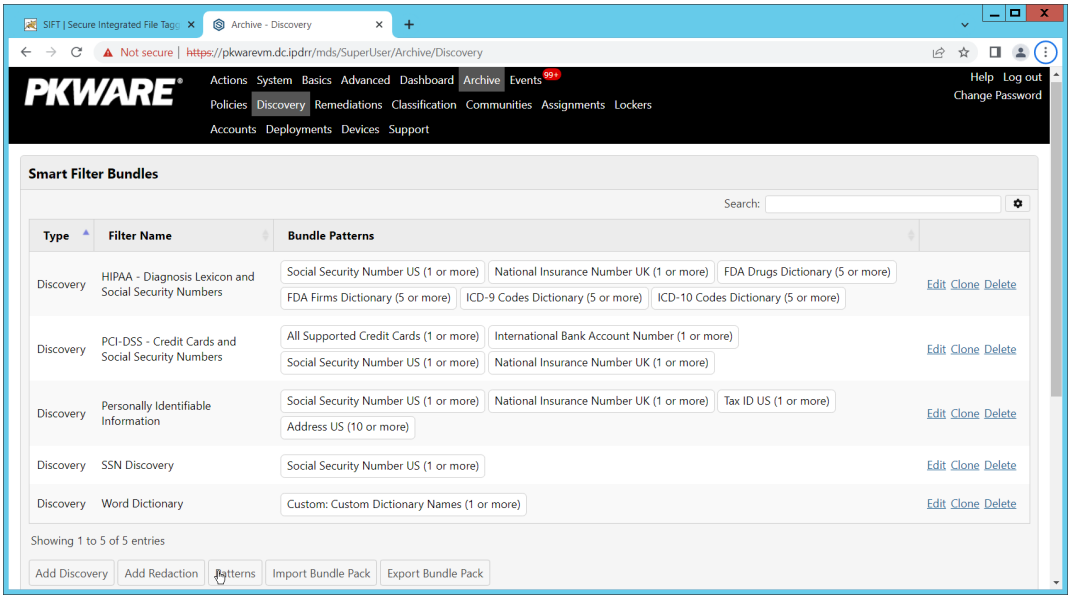
In this integration, we configure the collection of logs from Dispel, our network protection solution. Because Dispel controls access from users to enterprise systems it is important to have an overview of its actions through log collection and reporting. Dispel personnel can perform this integration 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

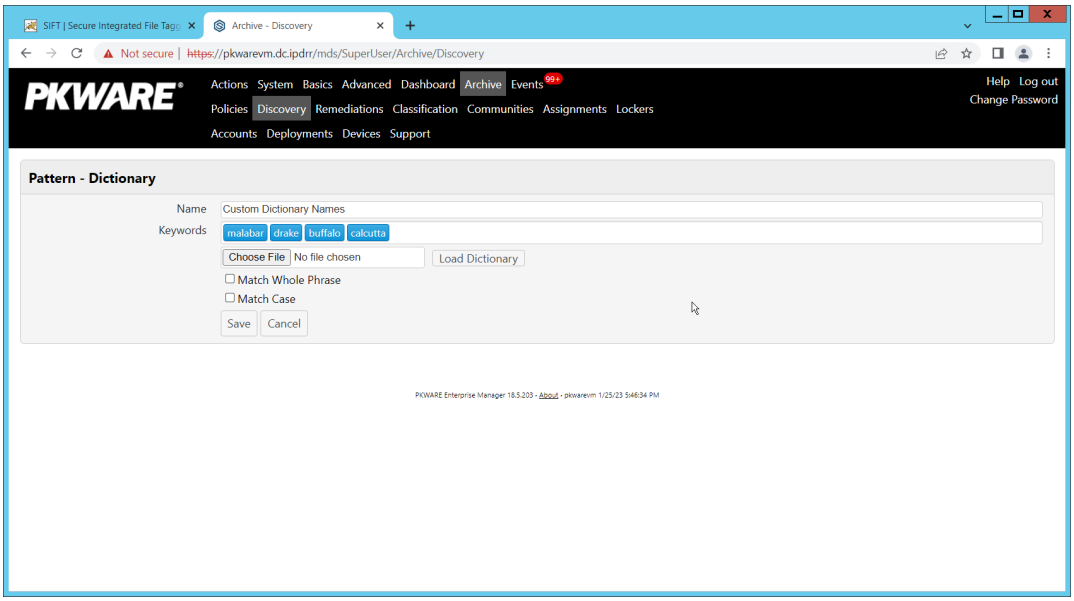
When used together, SIFT and PKProtect can protect sensitive data accidentally dropped into public shares on the enterprise. In Section 2.6, we detail how to configure SIFT to detect sensitive data in a Windows Share and move it to a location designated for sensitive information. Now, we will demonstrate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

Configuring PKWARE PKProtect

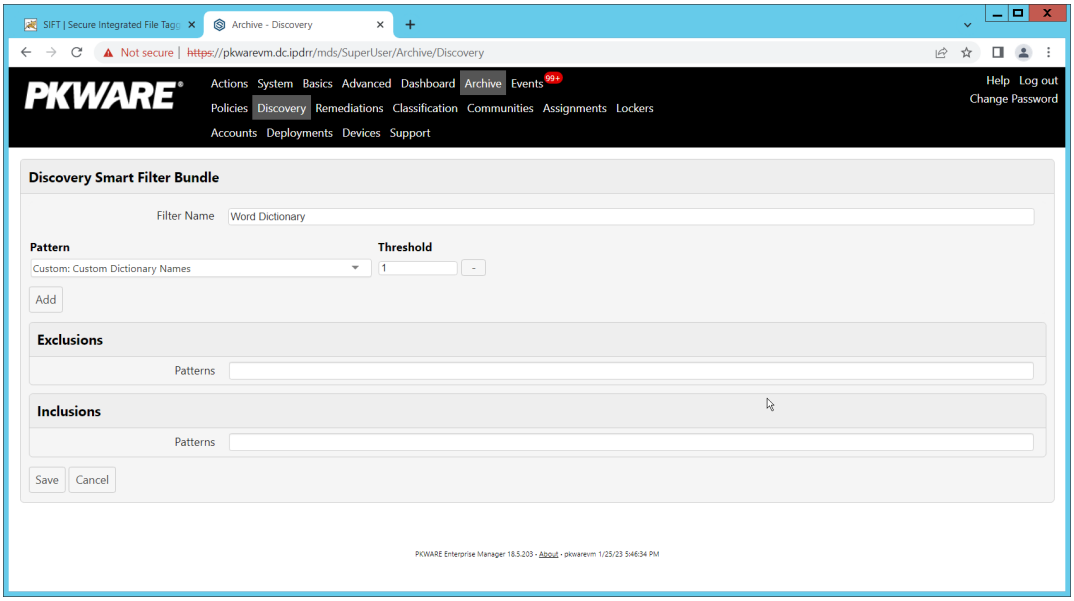
1. Navigate to the PKProtect dashboard and login.
2. Navigate to **Archive > Discovery**.



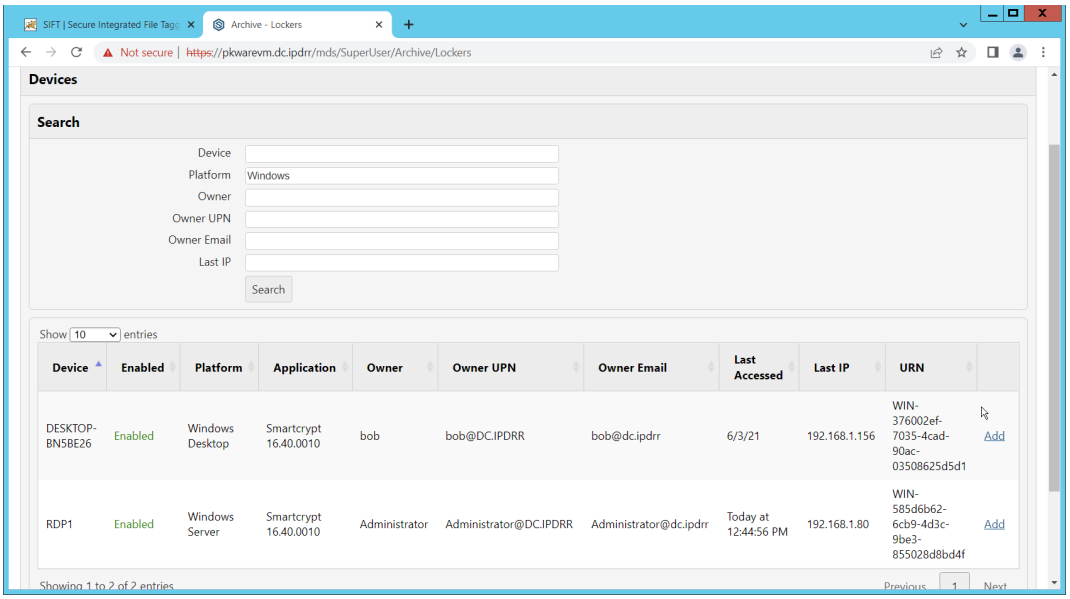
3. Click **Pattern – Dictionary.**
4. Enter a name for these patterns in the **Name** field.
5. Enter keywords to match in the **Keywords** field.



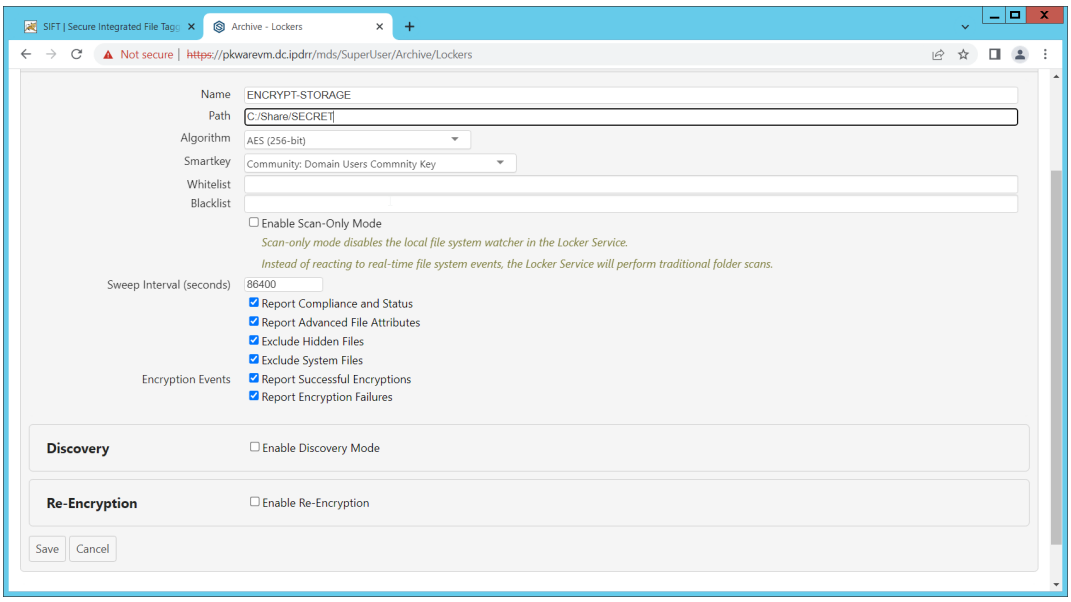
6. Click **Save**.
7. Click **Add Discovery**.
8. Under **Pattern**, select the name of the **Pattern** you just created.
9. For **Threshold**, enter the number of matches of this pattern needed to consider the file sensitive.



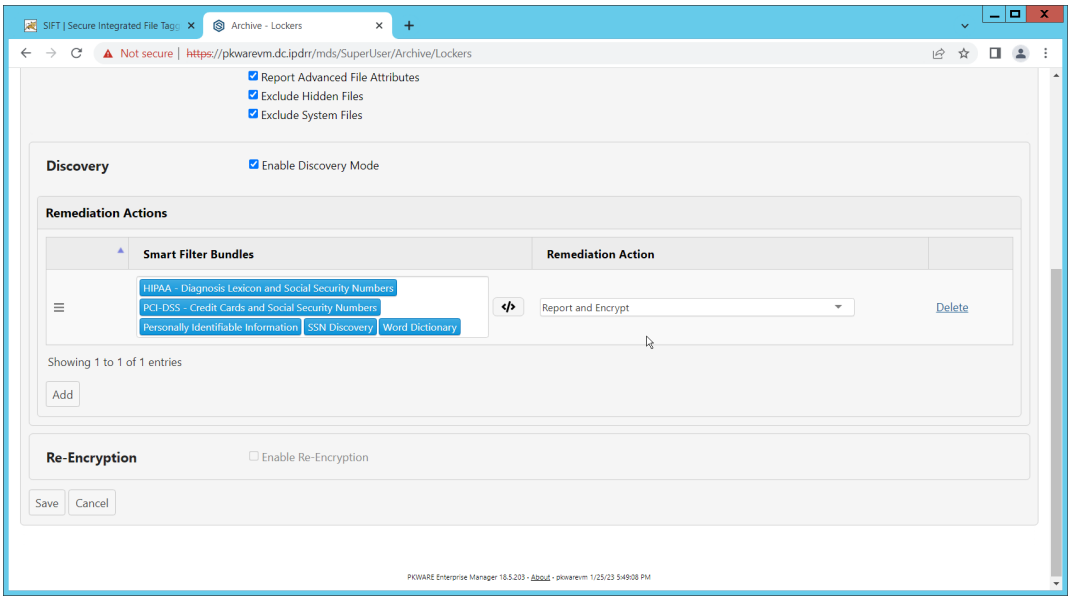
10. Click **Save**.
11. Navigate to **Archive > Lockers**.
12. Ensure that a PKWARE client is installed on the device which will be monitored for encryption. The device should show up in the list. If it doesn't you can search for the device and select it from the list.



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**.



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**.



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