NIST SPECIAL PUBLICATION 1800-29C

Data Confidentiality:

Detect, Respond to, and Recover from Data Breaches

Volume C:
How-To Guides

William Fisher
National Cybersecurity Center of Excellence
NIST

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

February 2024

FINAL

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

The first draft of this publication is available free of charge from:
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 1800-29C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-29C, 67 pages, (February 2024), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at 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 standards and technologies that are relevant in the detection, response, and recovery phases of a data breach.

KEYWORDS

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

ACKNOWLEDGMENTS

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

Name	Organization
Trey Doré	Cisco
Matthew Hyatt	Cisco
Randy Martin	Cisco
Peter Romness	Cisco
Bryan Rosensteel	Cisco
Micah Wilson	Cisco
Ben Burke	Dispel
Fred Chang	Dispel
Matt Fulk	Dispel
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
Spike Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation

Name	Organization
Brian Johnson	The MITRE Corporation
Lauren Lusty	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Julie Snyder	The MITRE Corporation
Lauren Swan	The MITRE Corporation
Anne Townsend	The MITRE Corporation
Jessica Walton	The MITRE Corporation

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

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

DOCUMENT CONVENTIONS

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

PATENT DISCLOSURE NOTICE

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

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

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

Contents

List of Figures

1 Introduction

The following volumes of this guide show information technology (IT) professionals and security engineers how we implemented this example solution. We cover all of the products employed in this reference design. We do not re-create the product manufacturers' documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our lab environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

1.1 How to Use this Guide

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate ability to detect, respond to, and recover from a loss of data confidentiality. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

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

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-29A*, which describes the following topics:

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

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

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

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

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-29C*, to replicate all or parts of the build

created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

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

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

1.2 Build Overview

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

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

1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

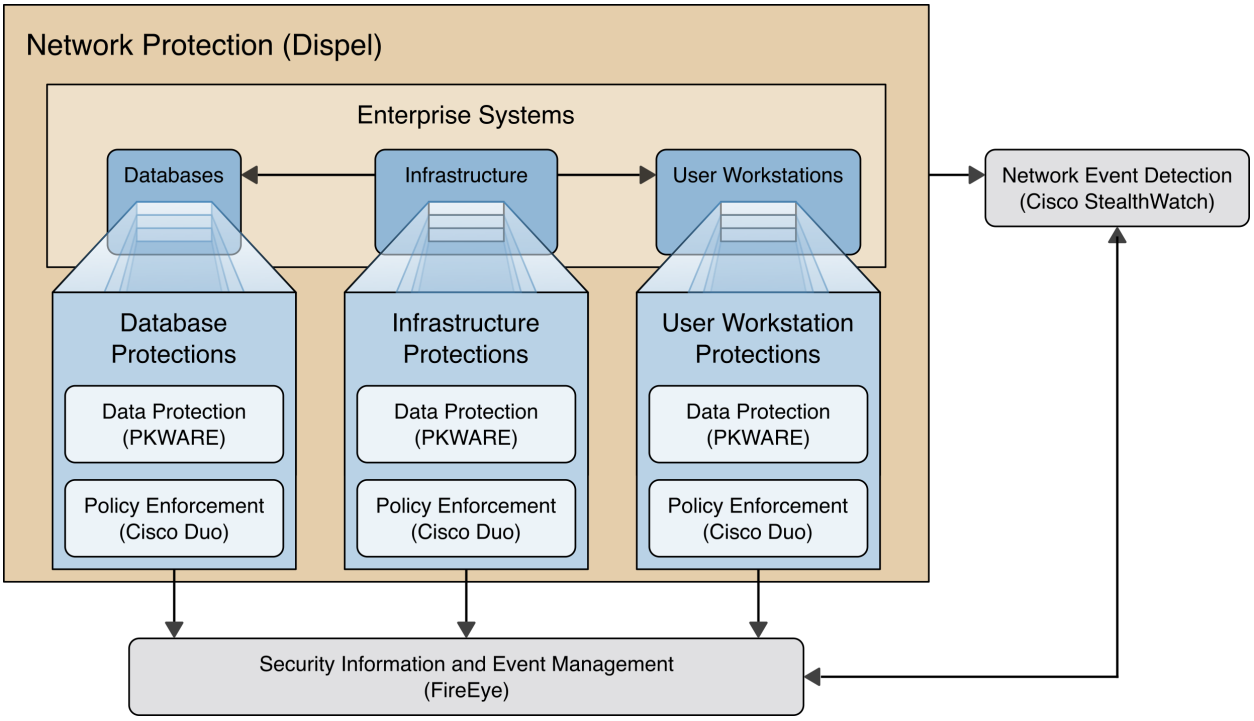
Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the NCCoE Style Guide.
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit.**
`Monospace`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

Typeface/Symbol	Meaning	Example
`Monospace Bold`	command-line user input contrasted with computer output	`service sshd start`
blue text	link to other parts of the document, a web Uniform Resource Locator (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 to technologies in their existing infrastructure. In addition to network management resources, such as a border firewall, the architecture assumes the presence of user workstations, an active directory system, and databases. The diagram below shows the components of the architecture and how they interact with enterprise resources.

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



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

- **User access controls (Cisco Duo)** work to regulate and restrict the level of access different users have, so that they can perform their work without providing unnecessary access that can be turned to more malicious ends.
- **Network Protection (Dispel)** ensures that hosts on the network only communicate in allowed ways, preventing side-channel attacks and attacks that rely on direct communication between hosts. Furthermore, it protects against potentially malicious hosts joining or observing traffic (encrypted or decrypted) traversing the network.

2 Product Installation Guides

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

2.1 FireEye Helix

FireEye Helix is a security incident and event management system used for collecting and managing logs from various sources. In this build, Helix is primarily used to manage events and alerts generated by data collected from across the enterprise. This build implemented a cloud deployment of Helix, and as such, much of the documentation provided will be integrating a cloud deployment with various products and components of the enterprise.

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

2.1.1 Installing the Communications Broker

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

   ```
   > sudo yum localinstall ./cbs-installer_1.4.2-9.x86_64.rpm
   ```

3. Log on to the Helix web console.
4. Navigate to **Dashboards** > **Operational**.
5. Click **Download Certificate**.
6. Click **Download**. This will download a “bootstrap.zip” file.
7. Copy the zip file to the Helix Communications Broker certificate directory.

   ```
   > sudo cp bootstrap.zip /opt/tap-nxlog/cert
   ```

8. Navigate to the certificate directory.

```
> cd /opt/tap-nxlog/cert
```

9. Extract the zip file you just copied.

```
> sudo unzip ./bootstrap.zip
```

10. If prompted, select “Yes” to overwrite any previous certificate files.

11. Navigate to one folder above.

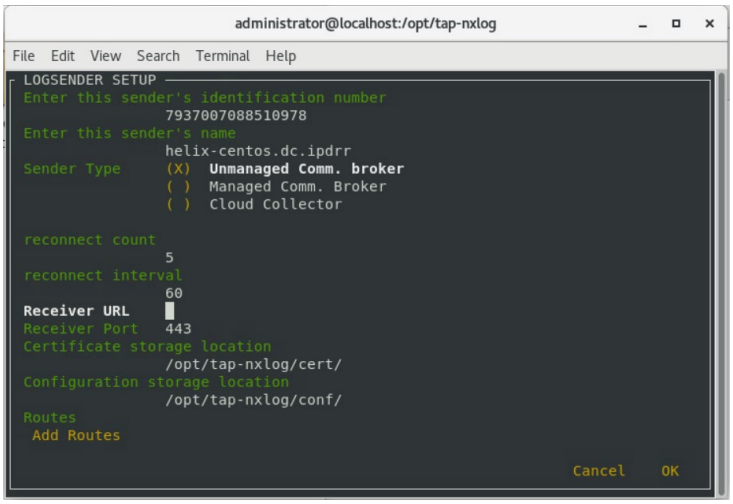
```
> sudo cd ..
```

12. Run the setup script.

```
> sudo ./setup.sh
```

13. Enter the name of the CentOS machine.

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



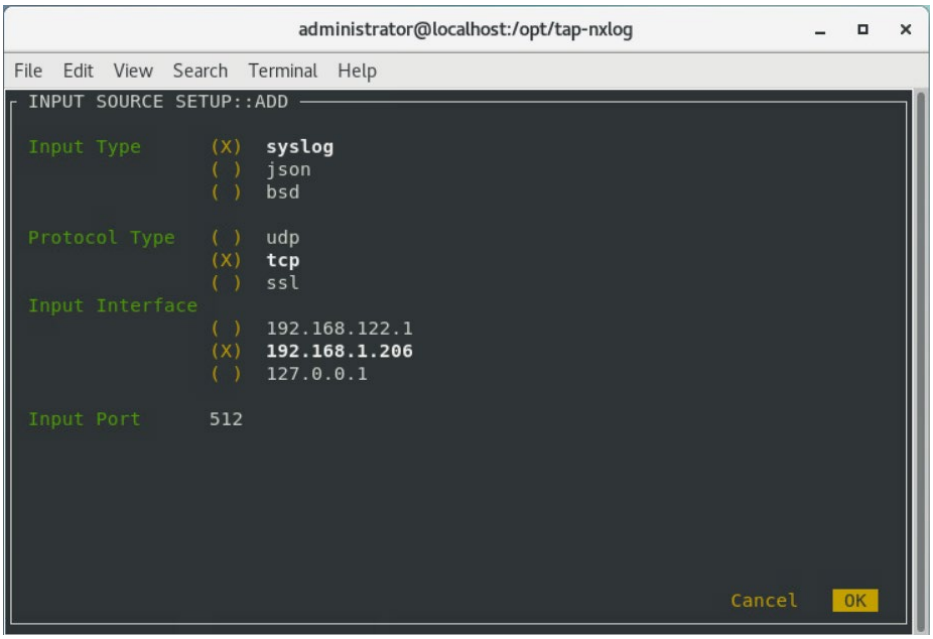
15. Select **Add Routes** and press **Enter**.

16. Select **syslog**.

17. Select **tcp**.

18. Select the Internet Protocol (IP) address of the machine where logs should be sent.

19. Enter 512 for the port number where logs should be sent.



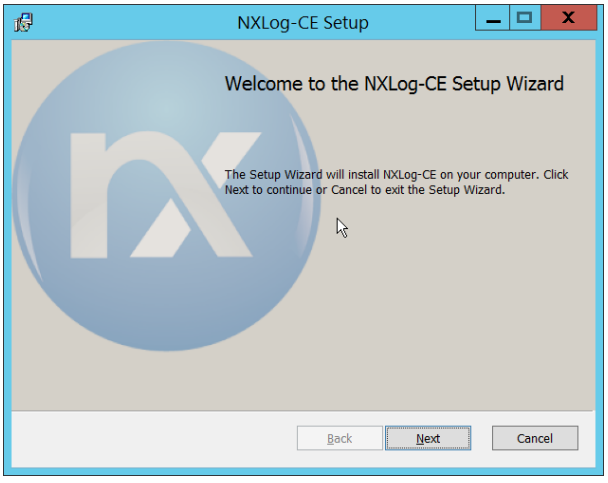
20. Select **OK** and press **Enter**.

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

2.1.2 Forwarding Event Logs from Windows 2012 R2

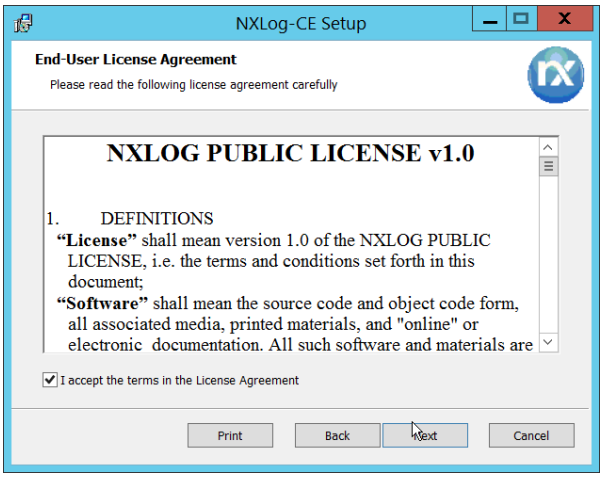
1. Acquire **nxlog-ce-2.10.2150.msi** from http://nxlog.org/products/nxlog-community-edition/download.

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

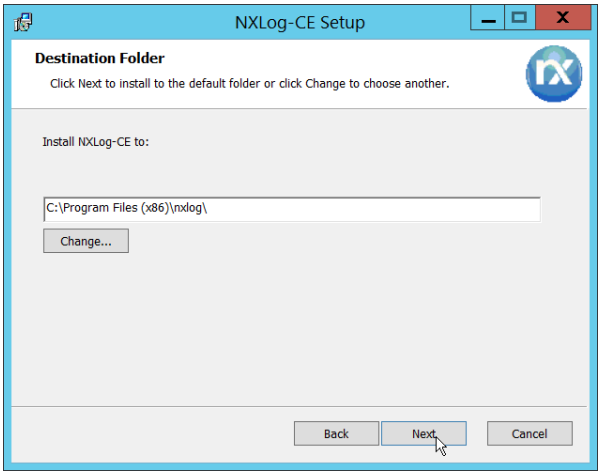


3. Click **Next**.

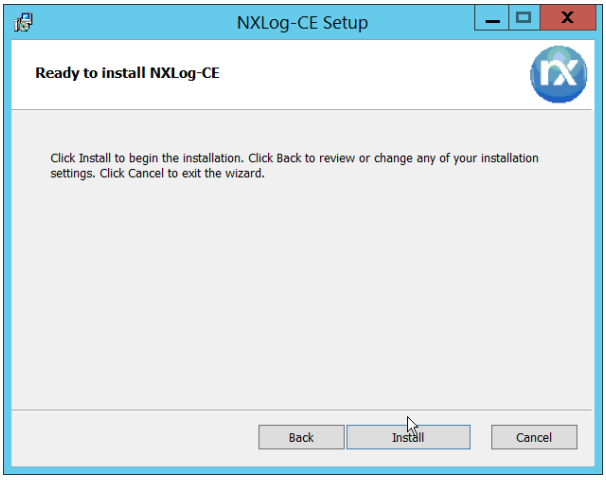
4. Check the box next to **I accept the terms in the License Agreement**.



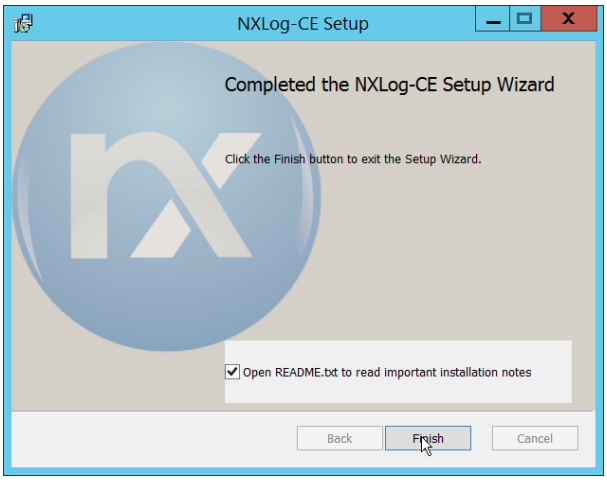
5. Click **Next**.



6. Click **Next**.



7. Click **Install**.



8. Click **Finish**.

9. Navigate to C:\Program Files (x86)\nxlog\conf and open nxlog.conf.

10. Copy the nxlog.conf file provided below.

```
Panic Soft
#NoFreeOnExit TRUE

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

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

<Extension _syslog>
    Module      xm_syslog
</Extension>

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

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

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

11. Restart the **nxlog** service.

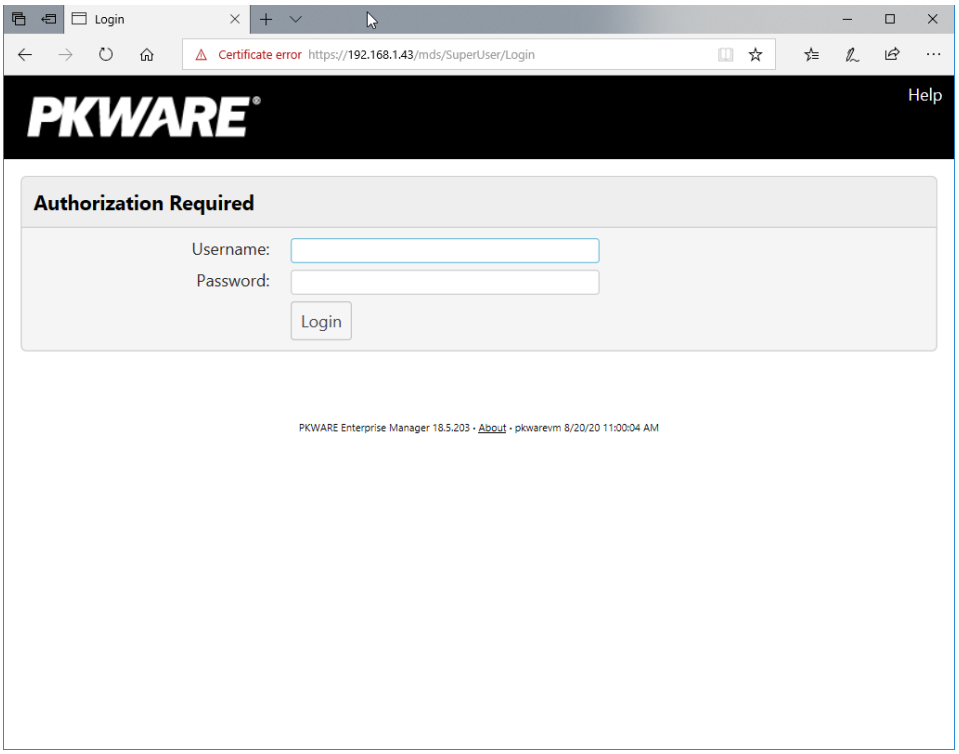
12. You can verify that this connection is working by checking the logs in data\nxlog.log, and by noting an increase in events on the Helix Dashboard.

2.2 PKWARE PKProtect

This installation and configuration guide for PKWARE PKProtect uses a physical PKWARE server, and as such will not delve into the installation of server components. In this guide, PKWARE is used to automatically perform data inventory and data protection functions.

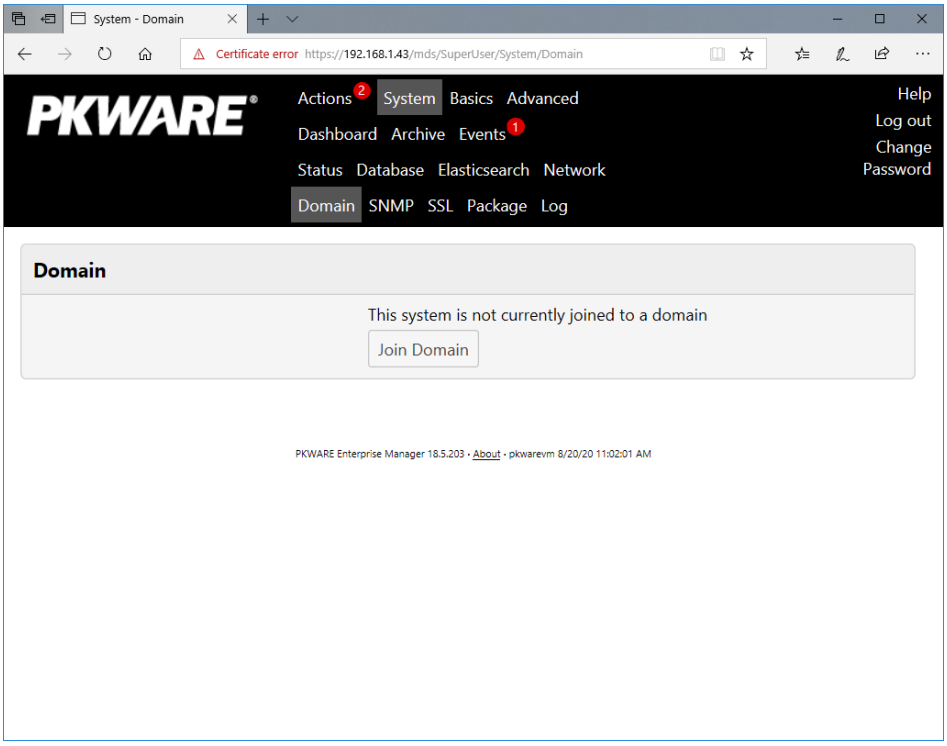
2.2.1 Configure PKWARE with Active Directory

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



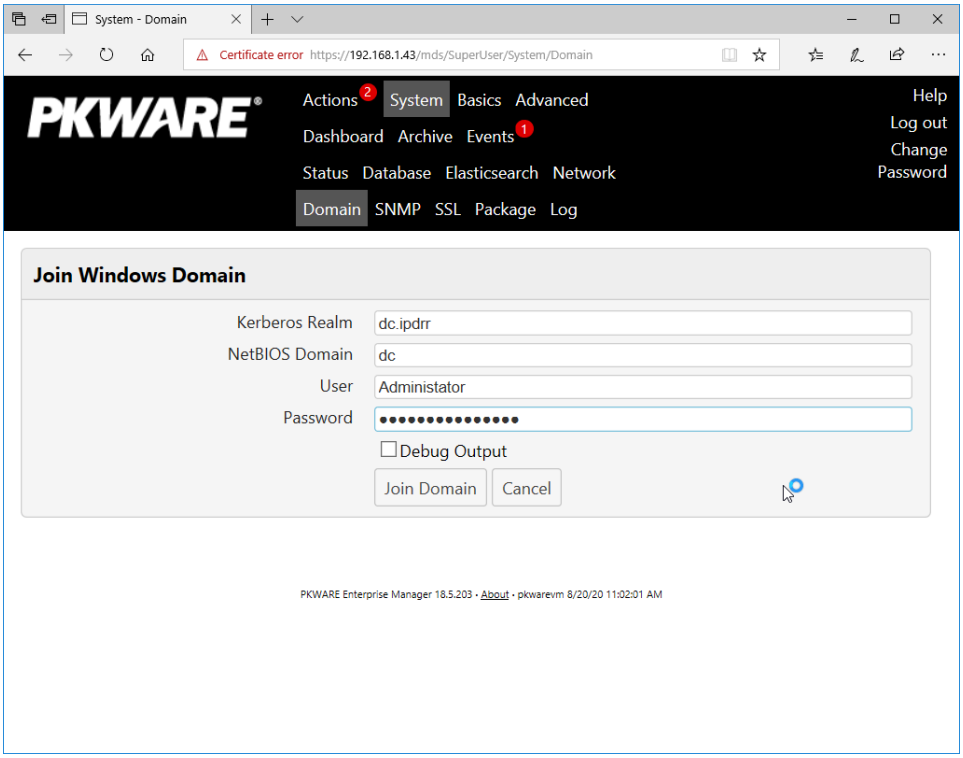
2. Once logged in, you can and should change the password to this administrative account by clicking **Change Password** in the top right corner.

3. Navigate to **System > Domain**.



4. Click **Join Domain**.

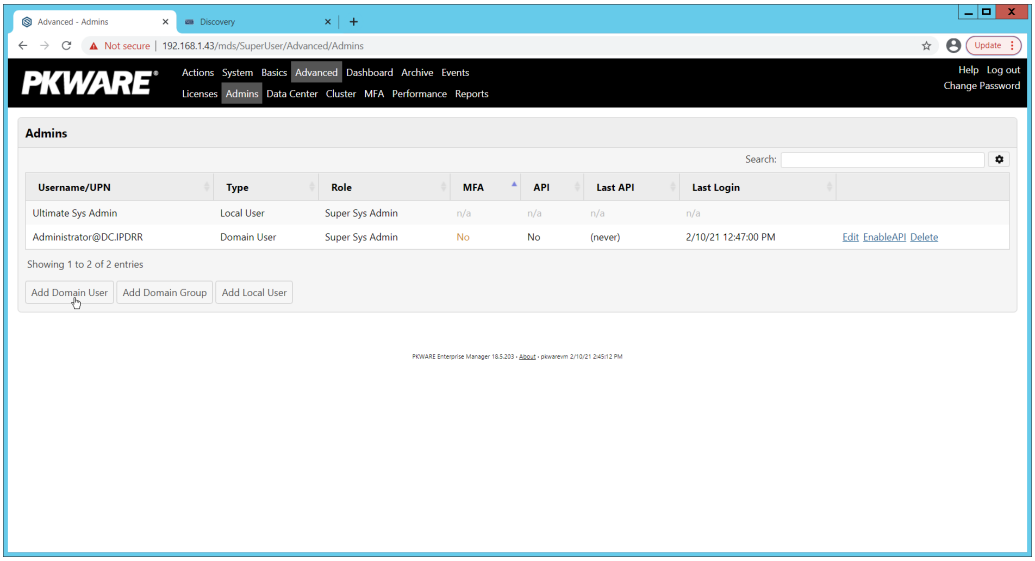
5. Enter the **Kerberos Realm, NetBIOS Domain**, as well as the **username** and **password** of an administrative user on the domain.



6. Click **Join Domain**.

2.2.2 Create a New Administrative User

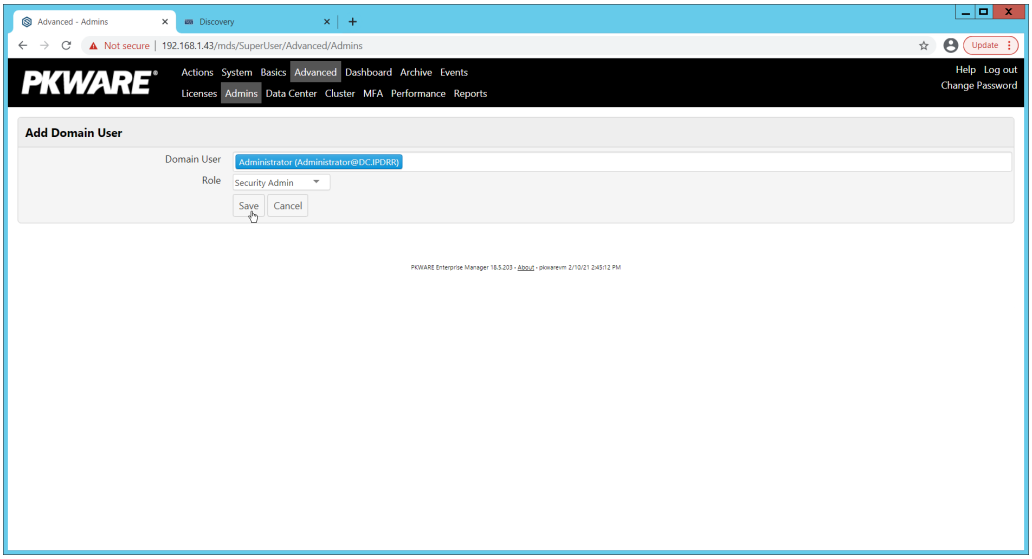
1. Navigate to **Advanced > Admins**.



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.

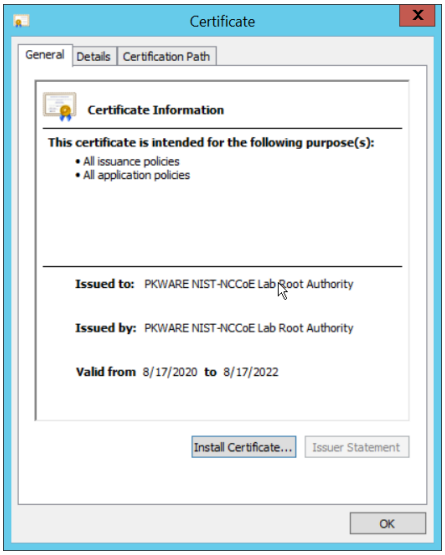


5. Click **Save**.

2.2.3 Install Prerequisites

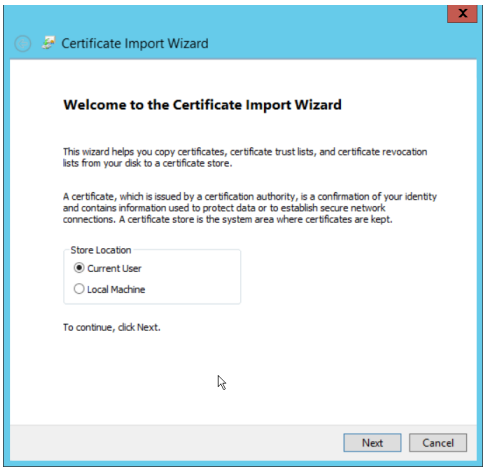
1. If needed for your environment, you may need to install certificates locally before agents can connect to PKProtect - ask your PKProtect representative if this is necessary for your environment.

2. Double click the certificate you wish to install.



3. Click **Install Certificate**.

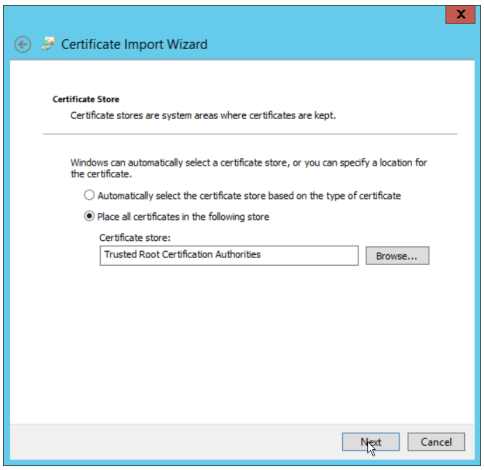
4. Select **Current User**.



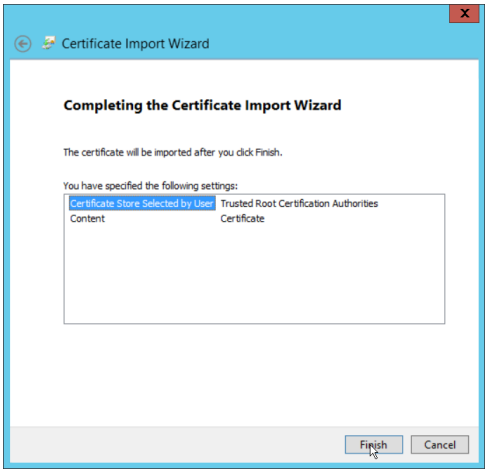
5. Click **Next**.

6. Click **Browse**.

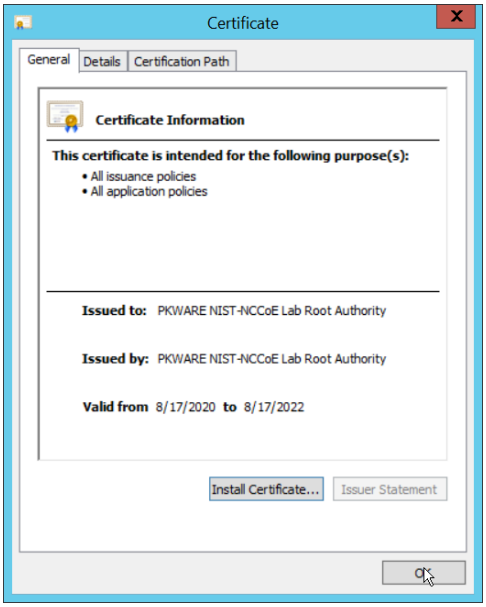
7. Select **Trusted Root Certification Authorities**.



8. Click **Next**.



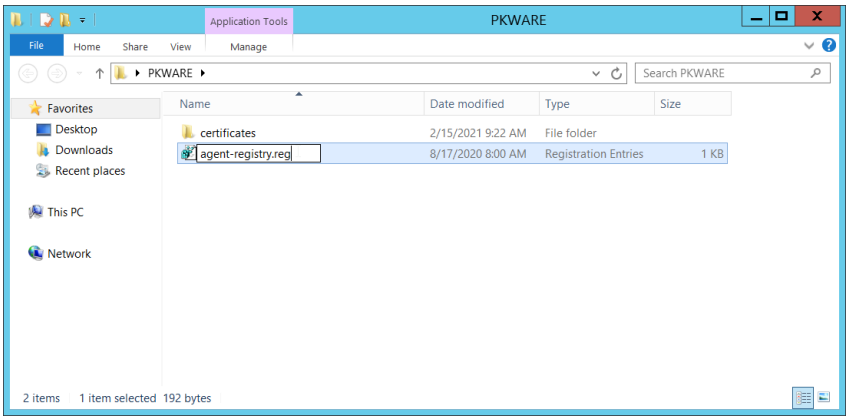
9. Click **Finish**.



10. Click **OK.**

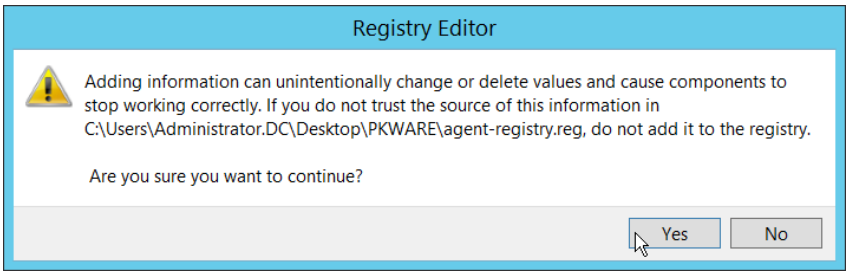
11. Repeat steps 1 through 10 but select **Personal** instead of **Trusted Root Certification Authorities.**

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

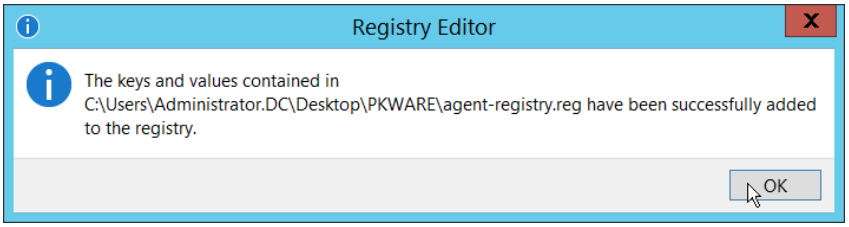


13. Rename *agent-registry.txt* to *agent-registry.reg*.

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



15. Click **Yes.**

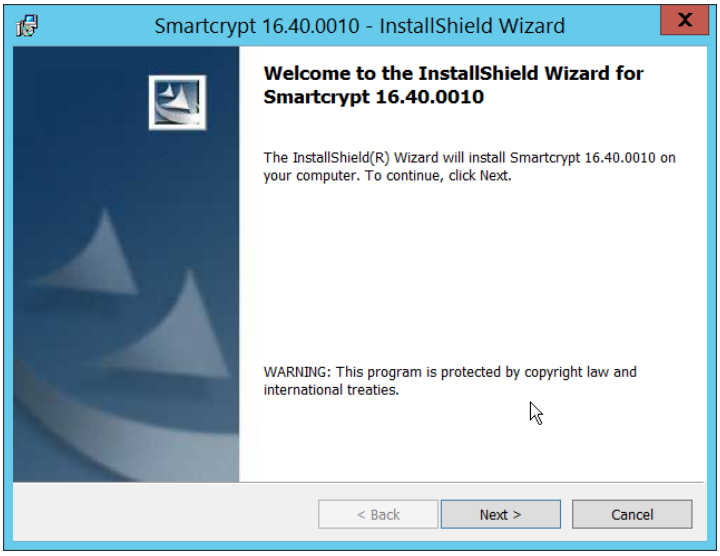


16. Click **OK**.

17. Restart the machine to apply these changes.

2.2.4 Install the PKProtect Agent

1. Run the PKProtect Installation executable.

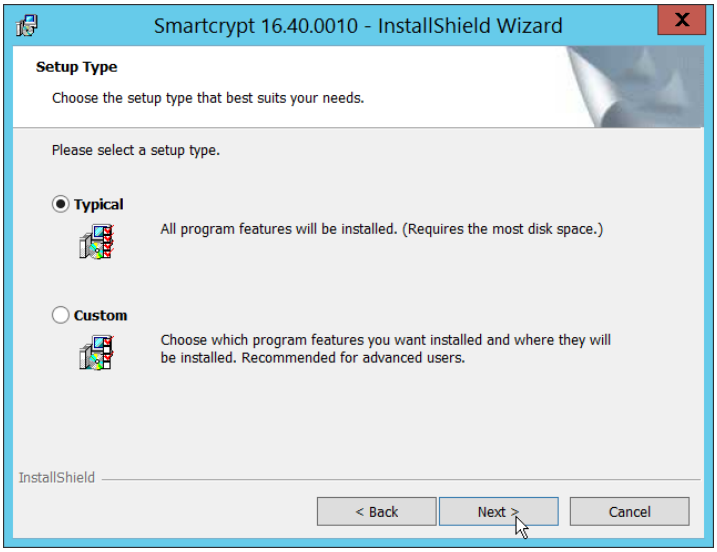


2. Click **Next**.

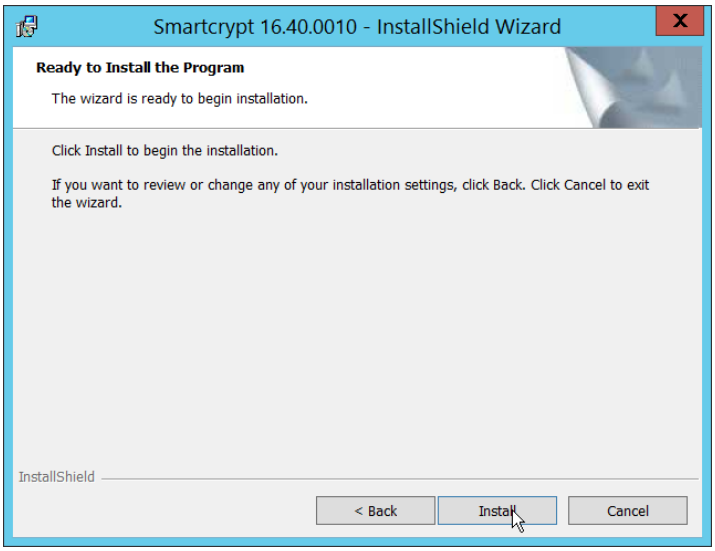
3. Select **I accept the terms in the license agreement**.

4. Click **Next**.

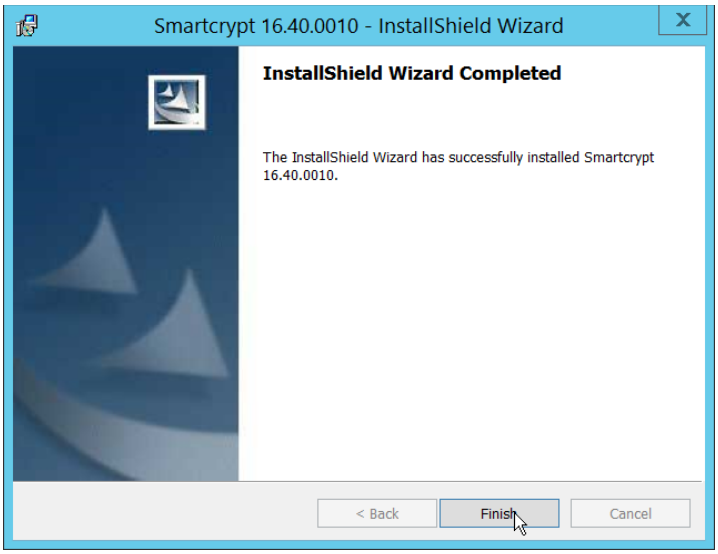
5. Select **Typical**.



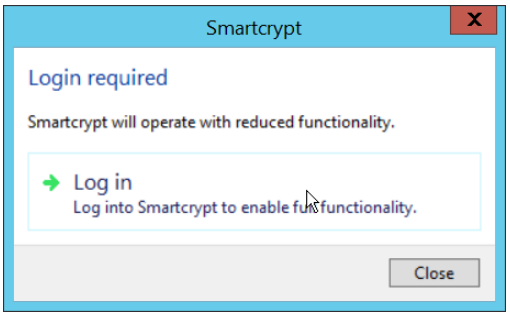
6. Click **Next**.



7. Click **Install**.

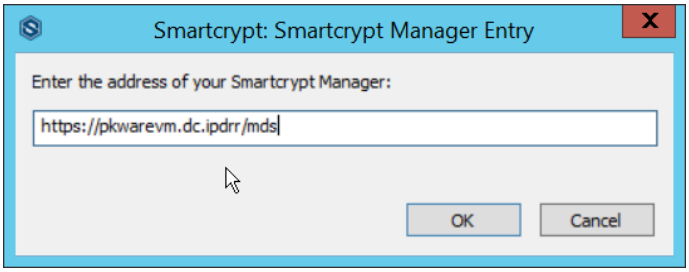


8. Click **Finish**.



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

10. Login using the username of the account in the domain, in email format (such as administrator@domain.id).

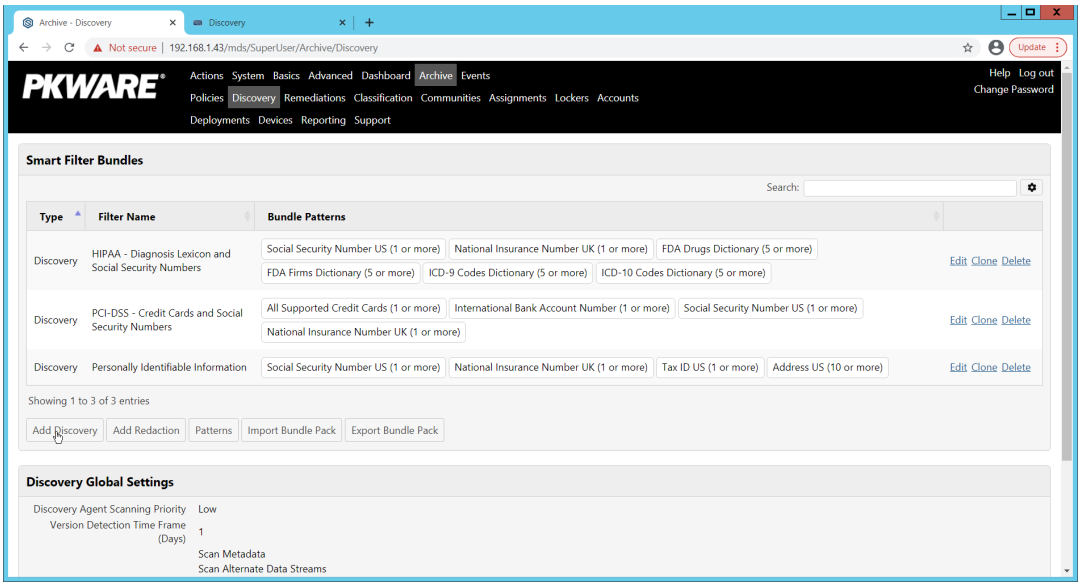


11. Enter the address of the PKWARE server.

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

2.2.5 Configure Discovery and Reporting

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

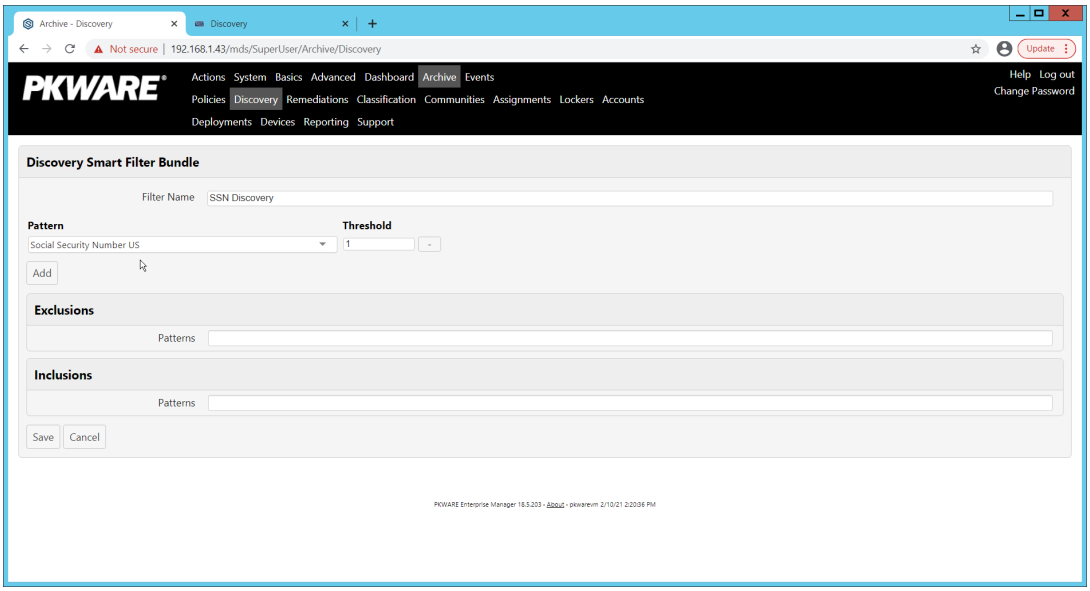


2. Click **Add Discovery**.

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

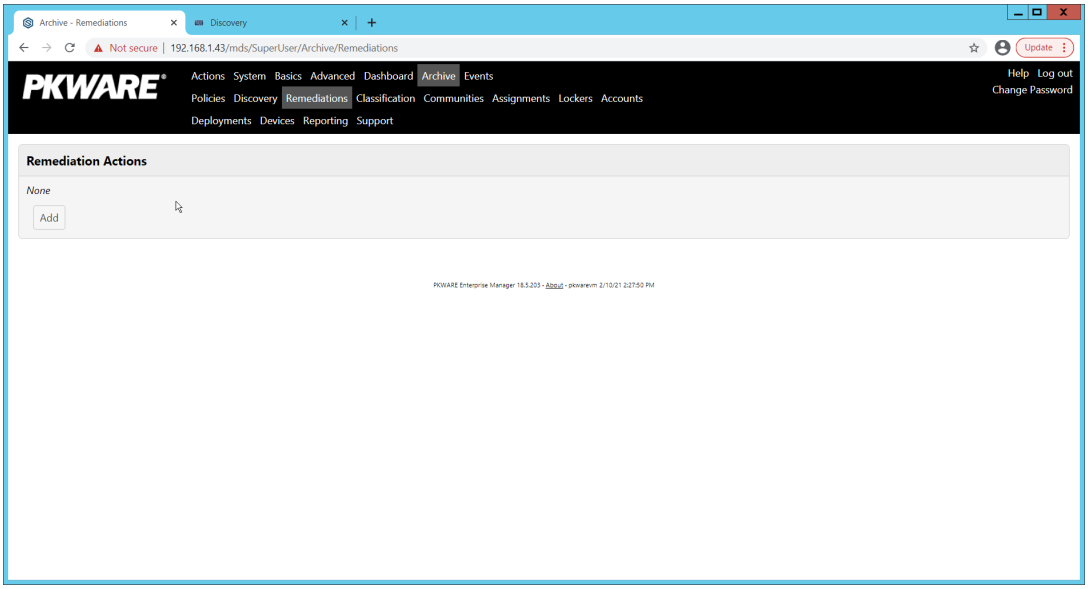
4. Select a **pattern** for the rule to discover. In this case, we are setting up a rule to detect social security numbers in files for reporting/remediation.

5. The **Threshold** field refers to how many of those patterns must be present in a document for the rule to be applied.



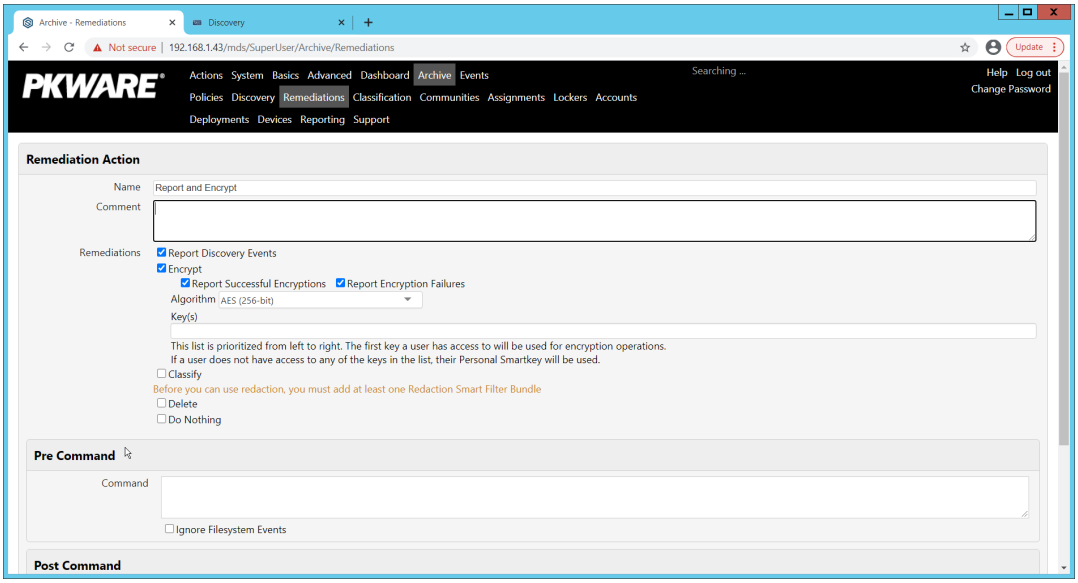
6. Click **Save**.

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



8. Click **Add**.

9. Enter a name for the remediation.

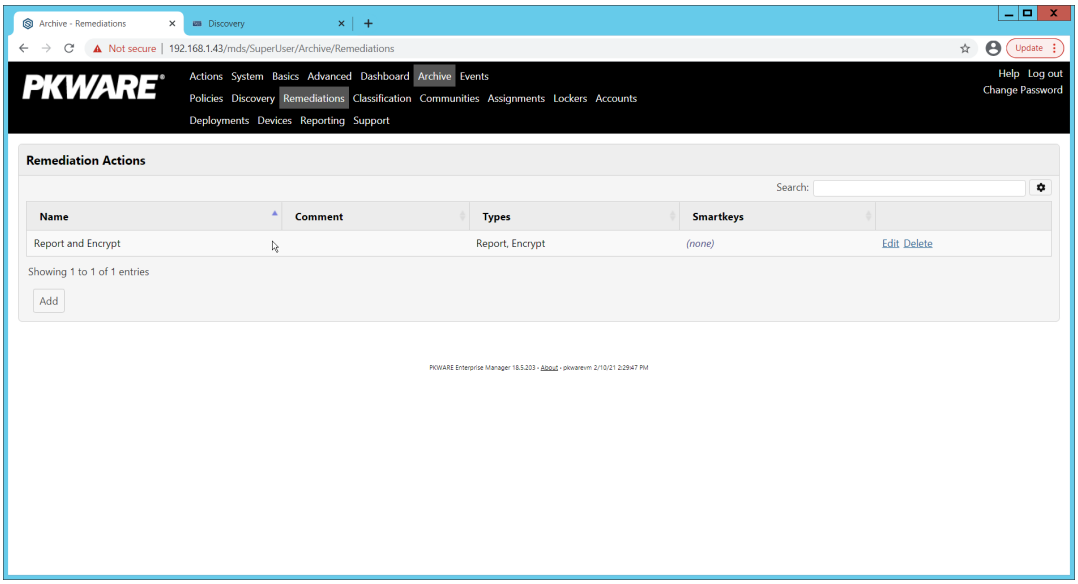


10. Check the box next to **Report Discovery Events**.

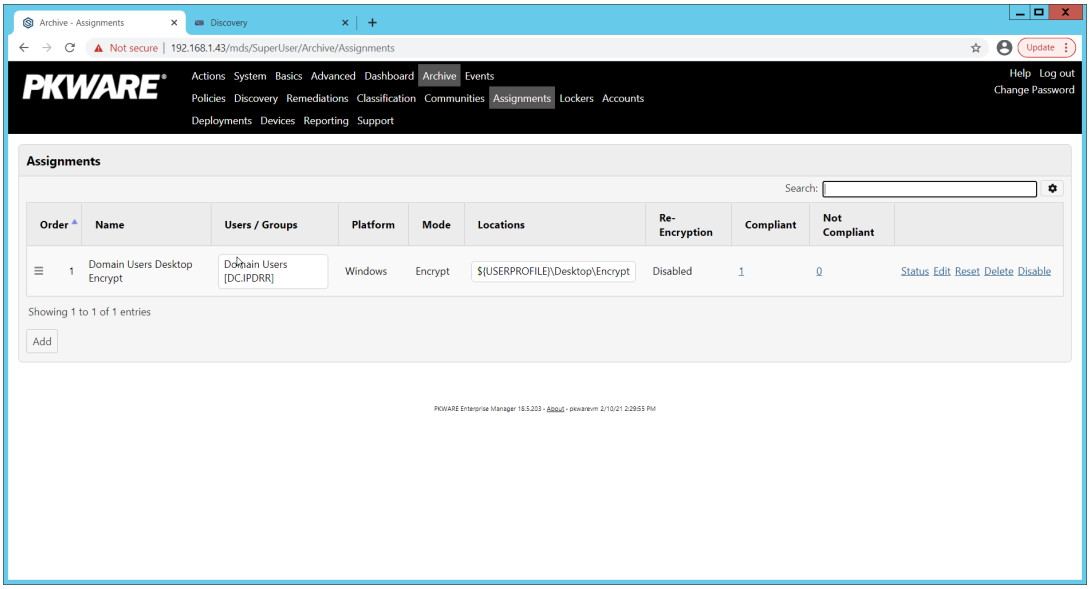
11. Check the box next to **Encrypt**.

12. Ensure that **AES (256-bit)** is selected.

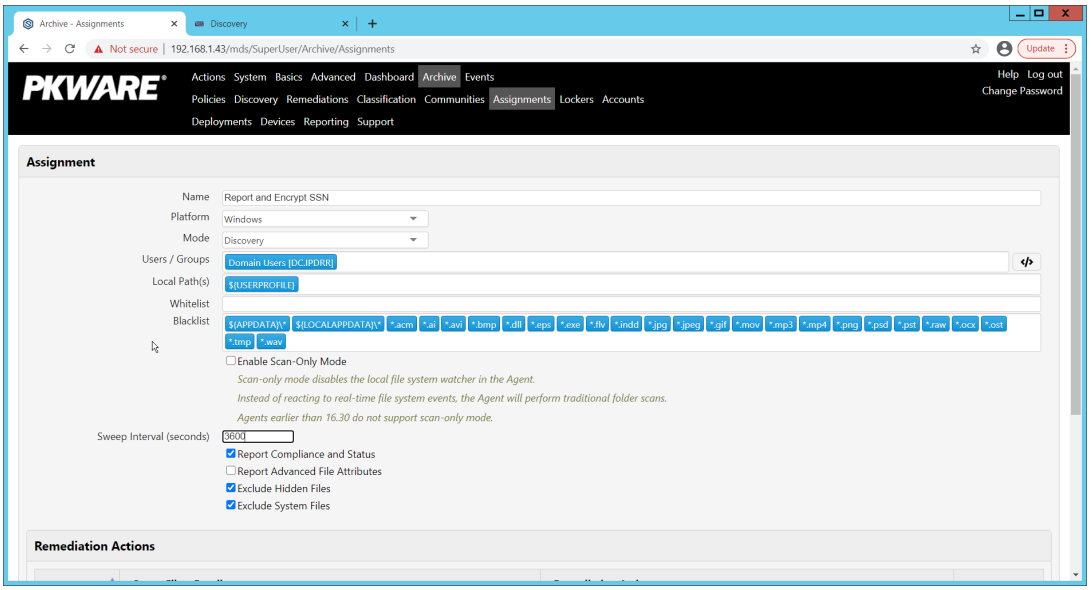
13. Click **Save**.



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



15. Click **Add**.



16. Enter a **Name** for the Assignment.

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

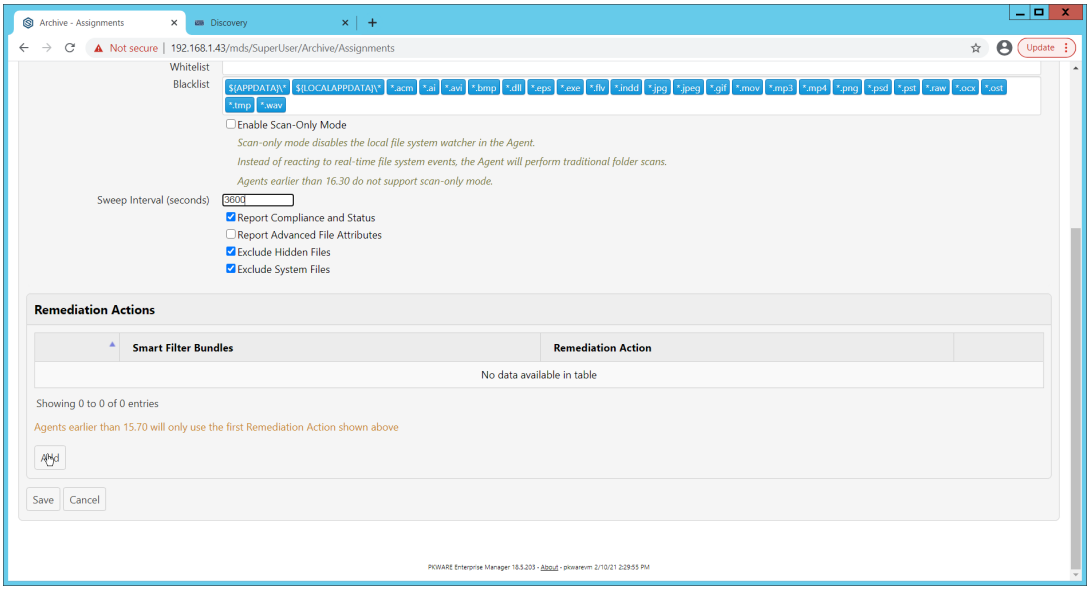
18. Select **Discovery** for the **Mode**.

19. Enter the names of the Active Directory users or groups this rule should apply to.

20. Enter the folders for this rule to search in **Local Paths**.

21. Use **Whitelist** and **Blacklist** to specify file types that should or should not be considered.

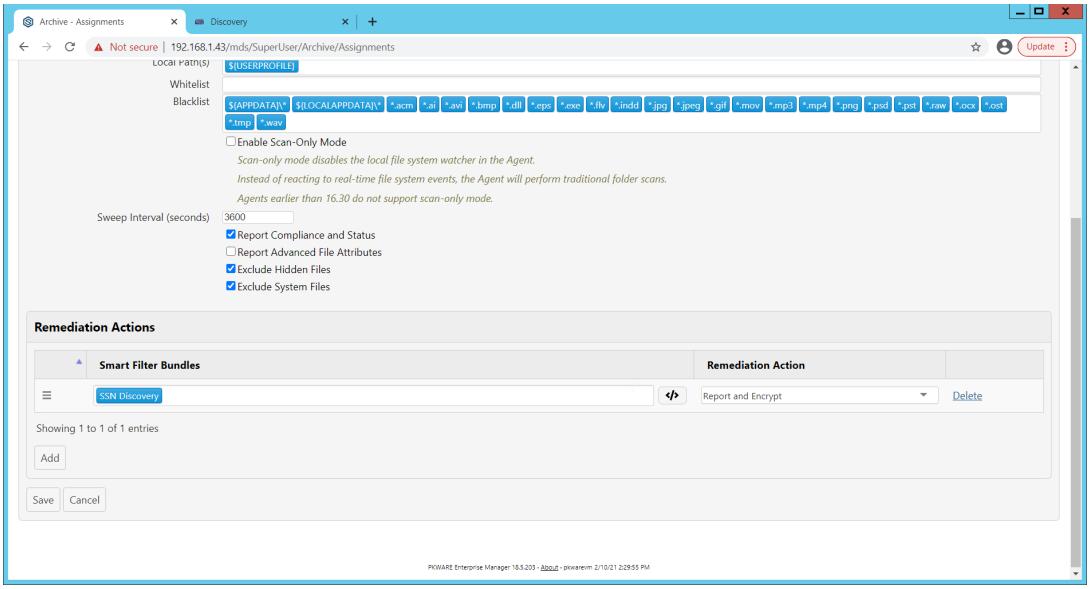
22. Enter the interval for this rule to run in **Sweep Interval**.



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 that match its discovery conditions.

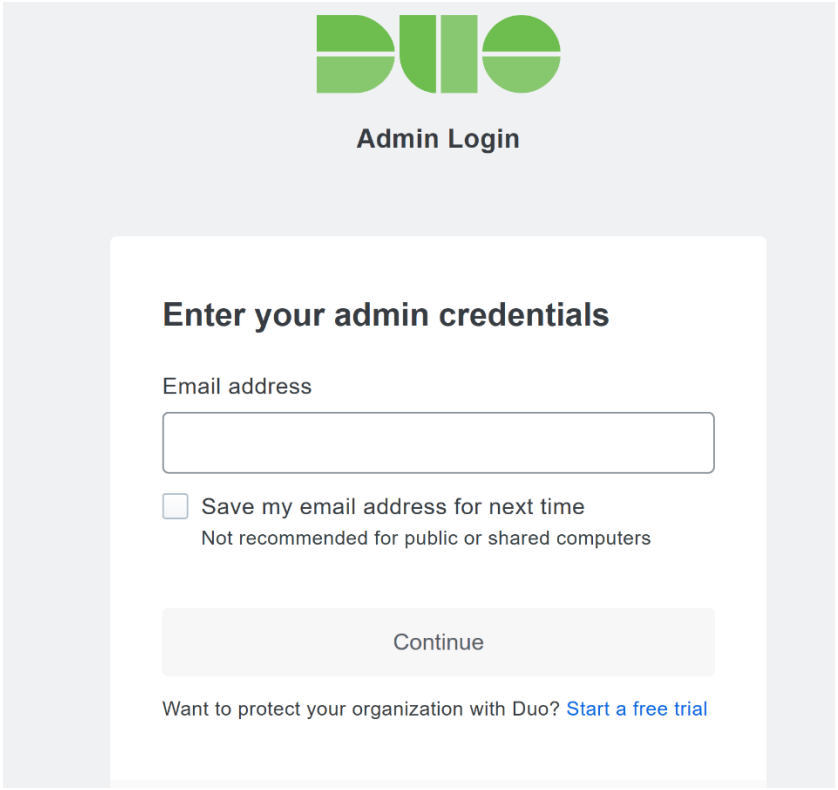
2.3 Cisco Duo

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

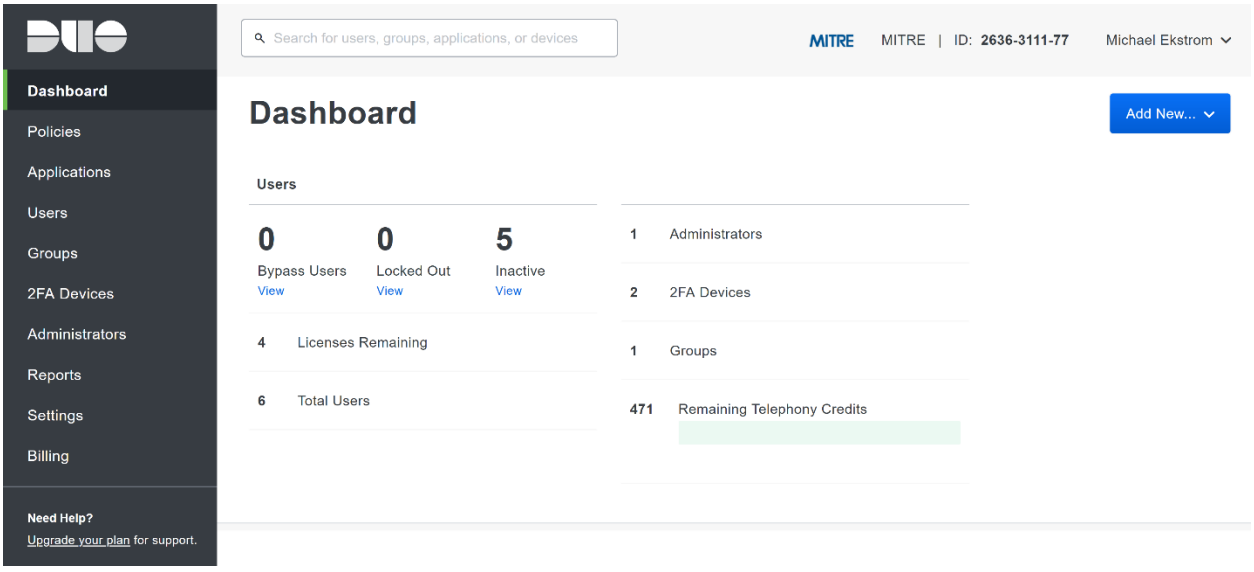
In the following section, we demonstrate the installation of Cisco Duo on an internal system in such a way that Remote Desktop Protocol (RDP) and local login to that system are protected by multifactor authentication.

2.3.1 Installing Cisco Duo

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

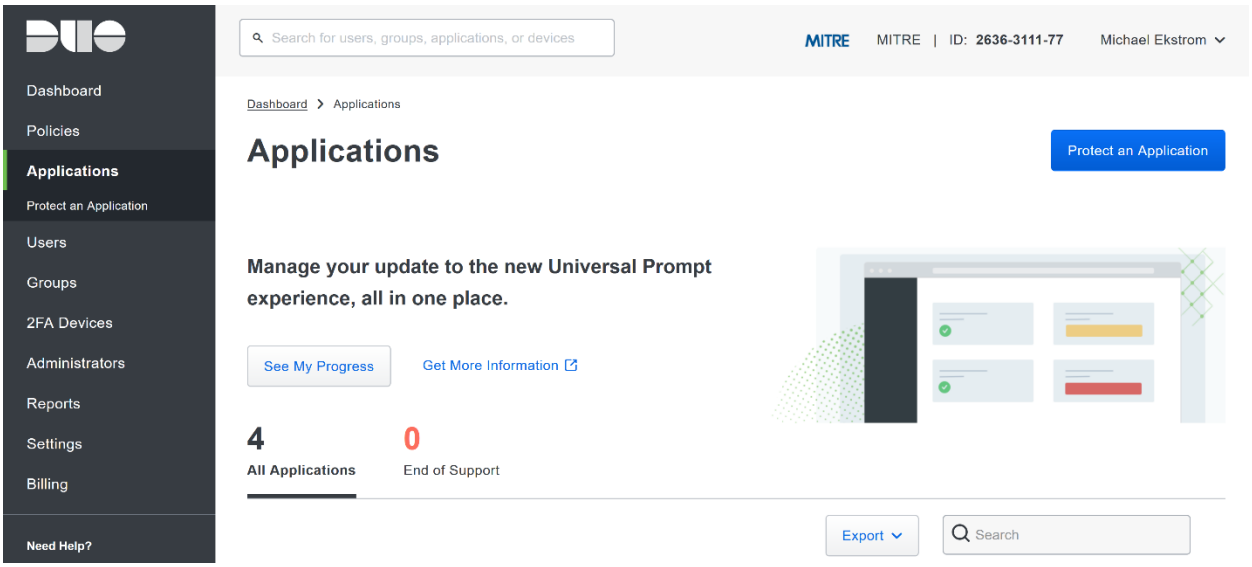


3. Login with your admin credentials and dual factor authentication to reach the administrator dashboard.



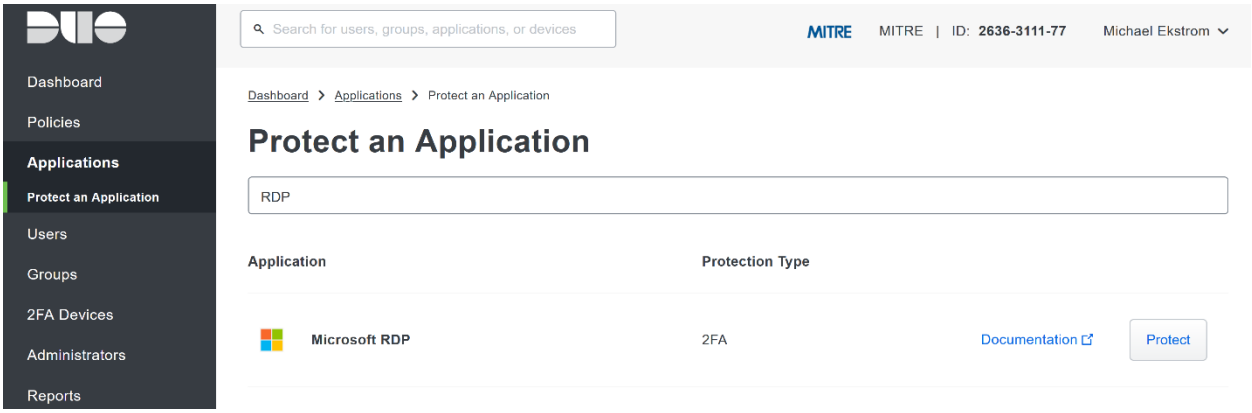
4. Click **Applications** in the sidebar.

5. Click **Protect an Application**.

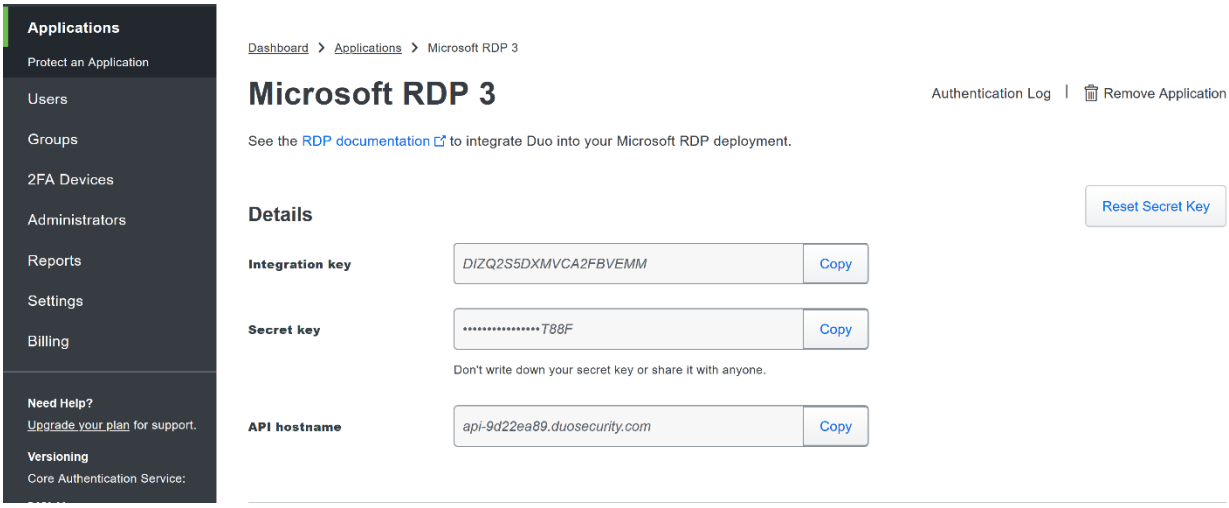


6. Search for, or scroll down to, **Microsoft RDP**.

7. Click **Protect**.

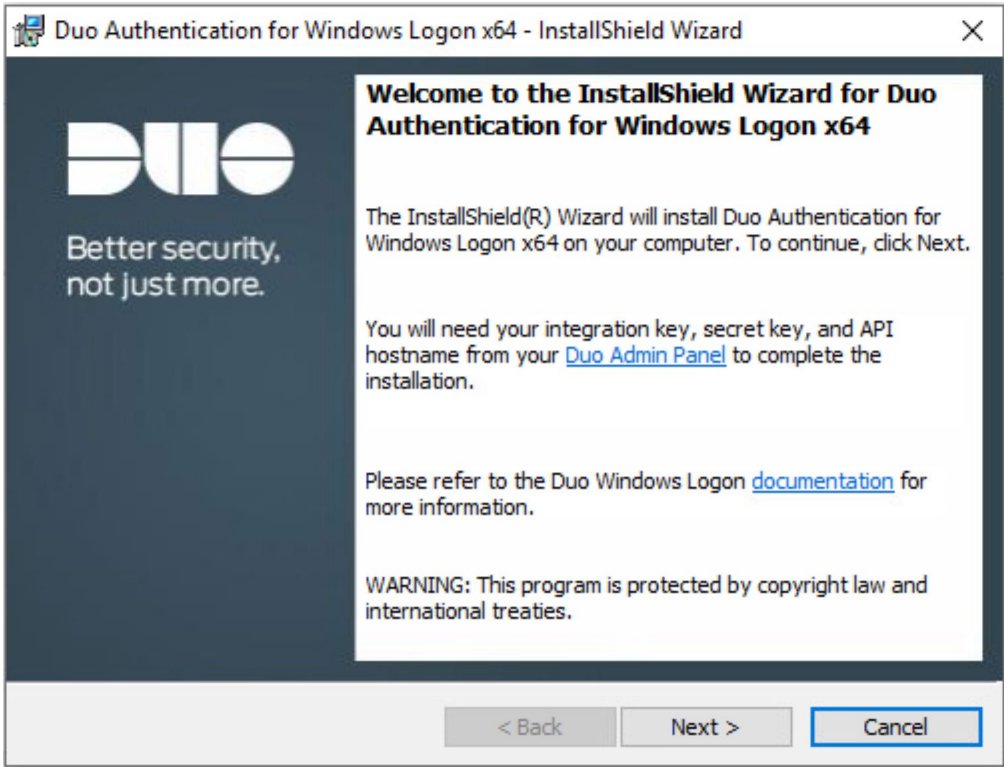


8. The next screen will provide policy configuration options, as well as the **Integration Key**, **Secret Key**, and **API hostname**, which are required information for the next step. Either keep this window open or copy down those three pieces of information.



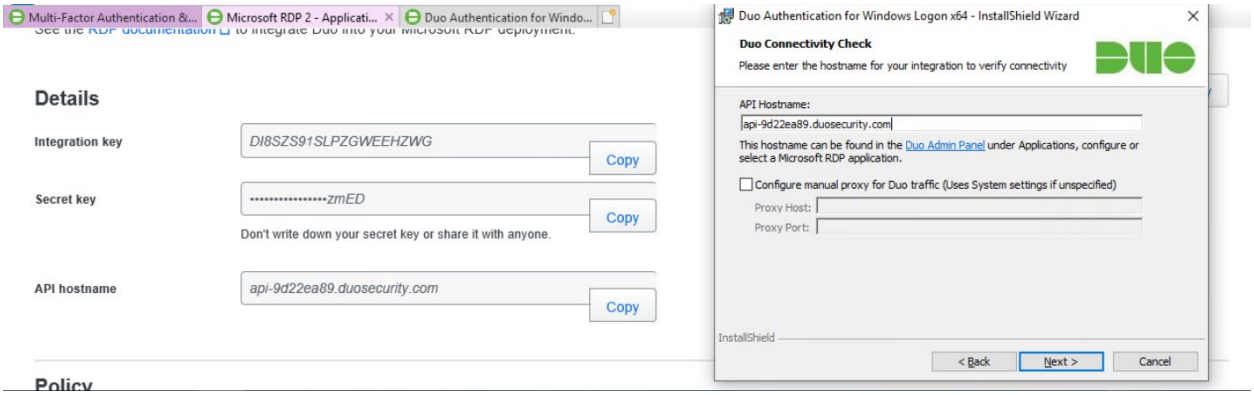
9. Download the **Duo Authentication for Windows Logon** installer package, located at https://dl.duosecurity.com/duo-win-login-latest.exe.

10. Run the downloaded EXE file.



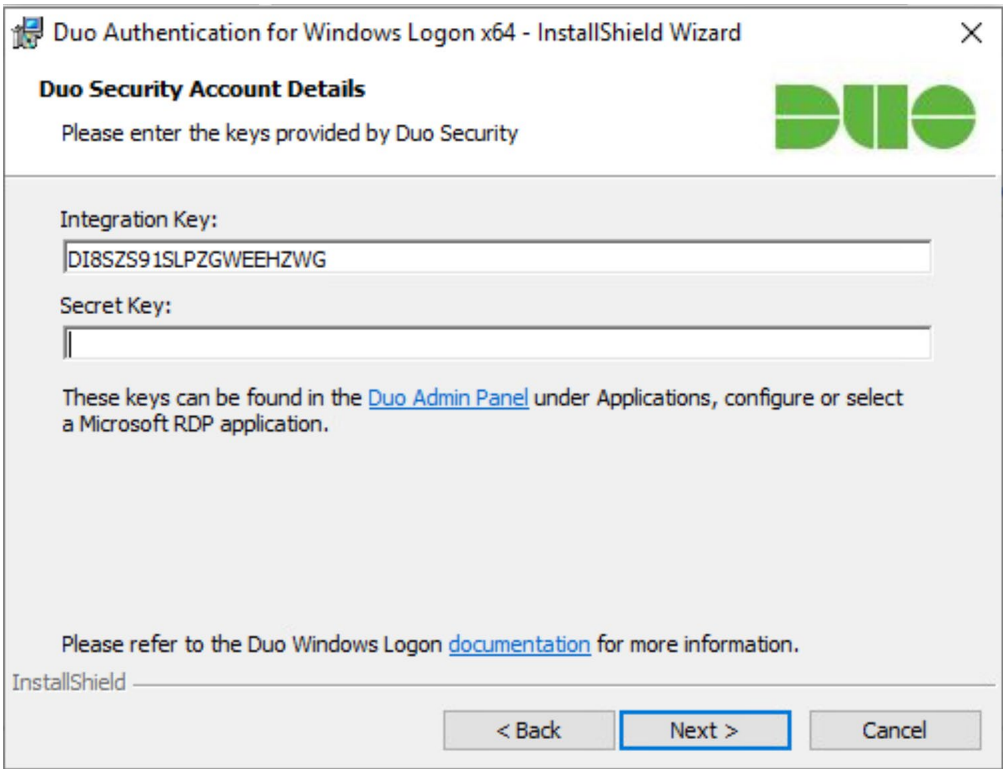
11. Click **Next**.

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



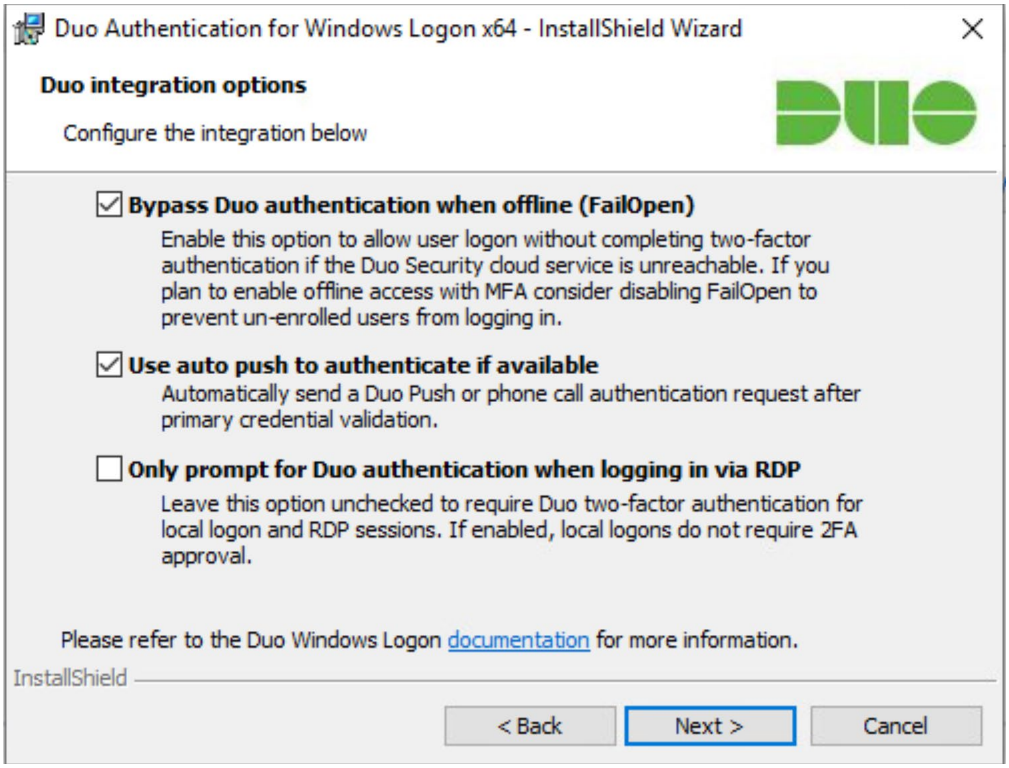
13. Click **Next**.

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



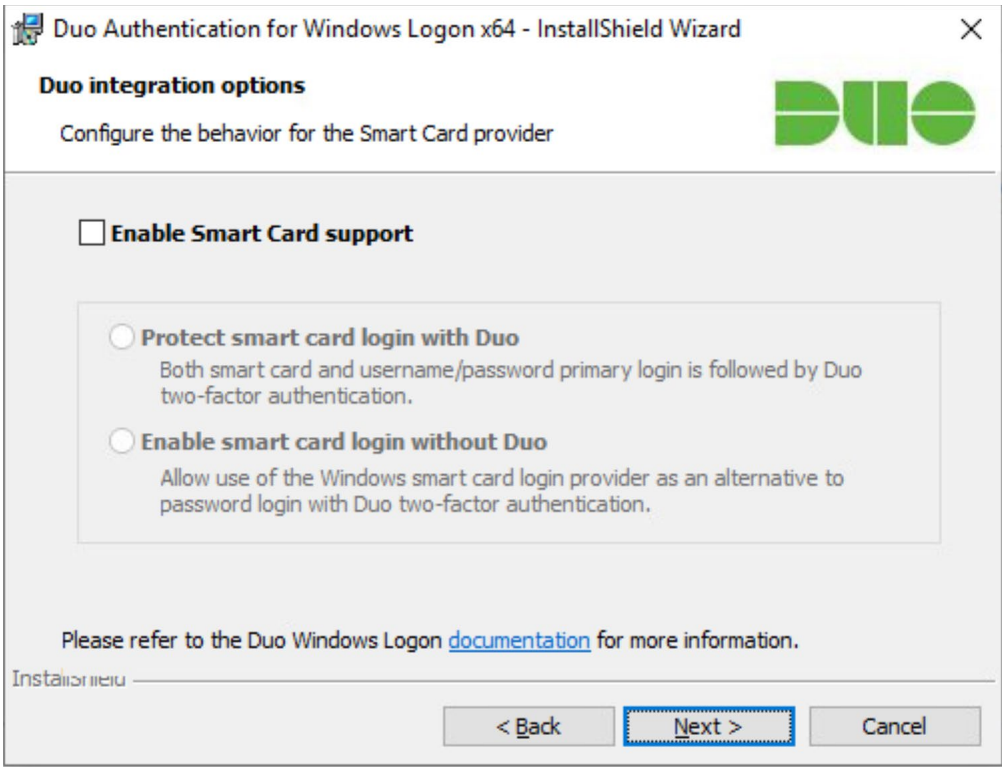
15. Click **Next**.

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.



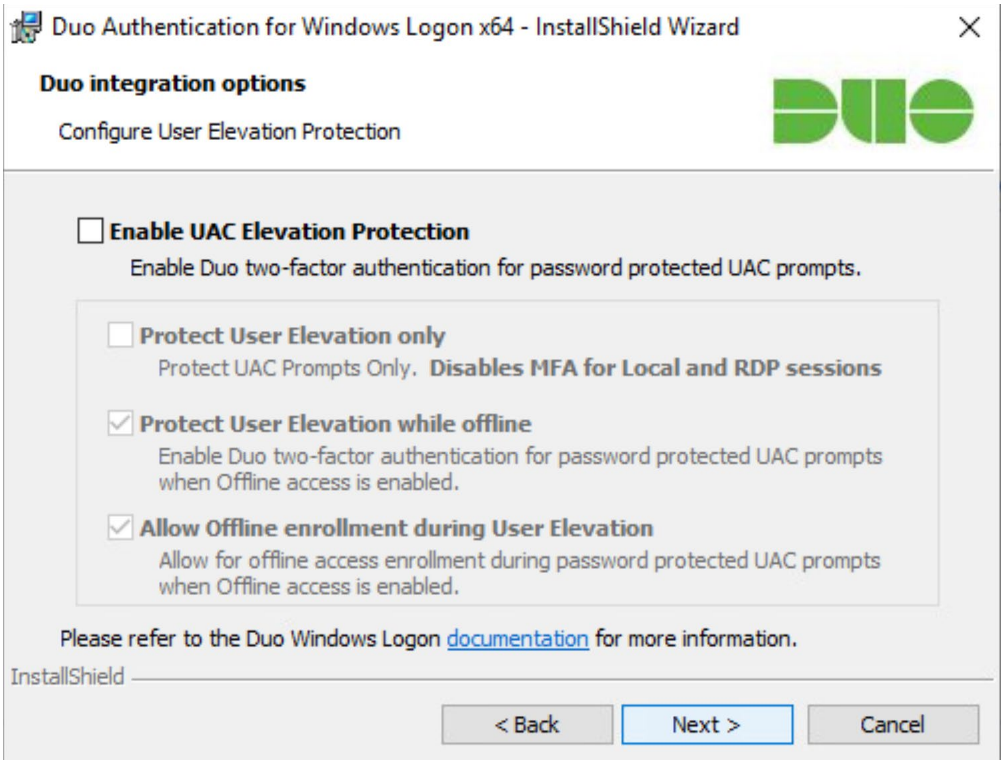
17. Click **Next**.

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

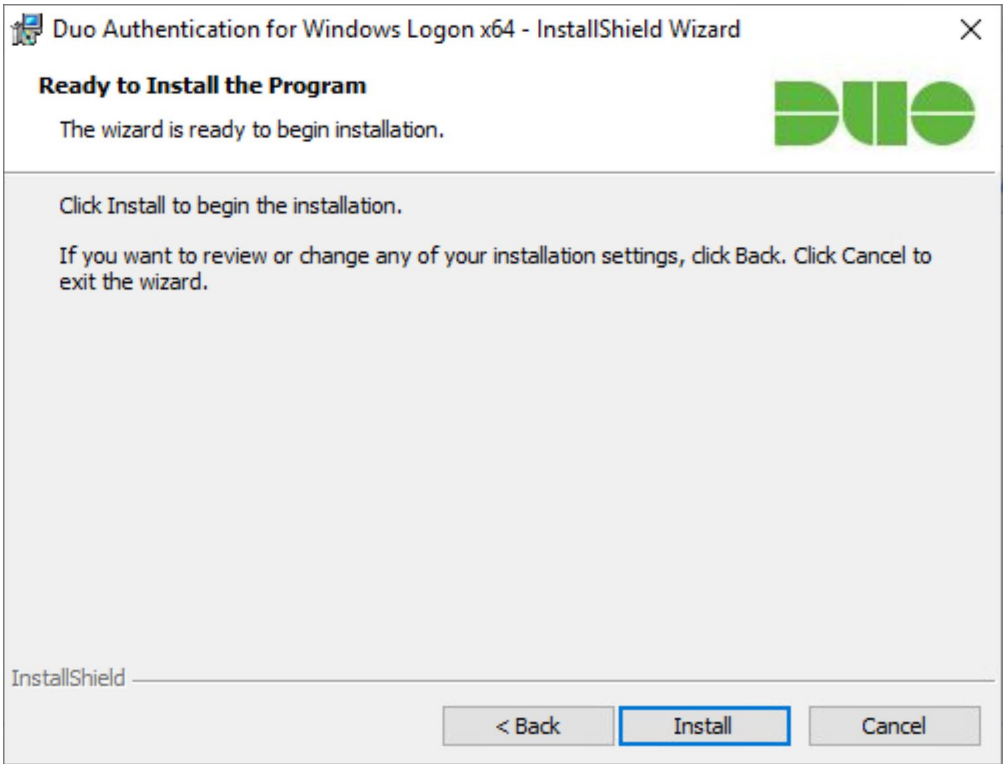


19. Click **Next**.

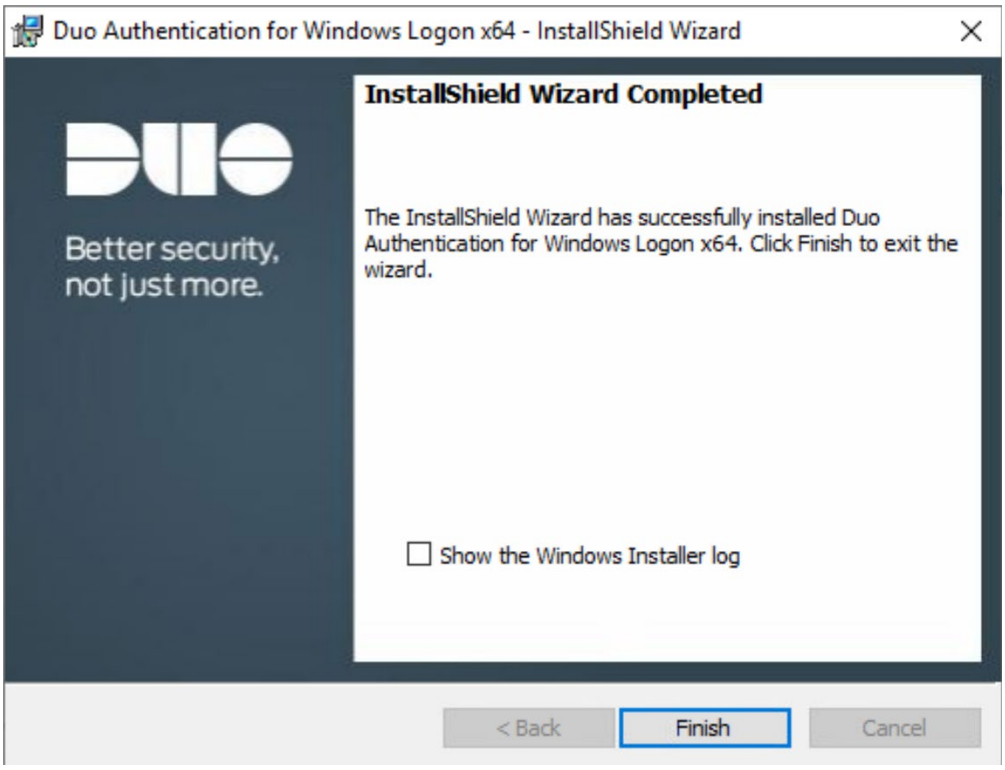
20. Leave **Enable UAC Elevation Protection** unchecked.



21. Click **Next**.



22. Click **Install**.

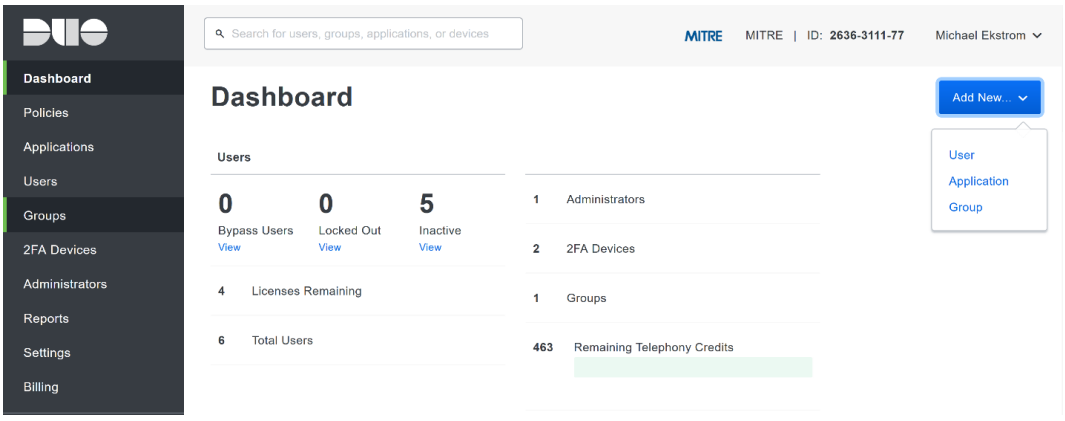


23. Click **Finish**.

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

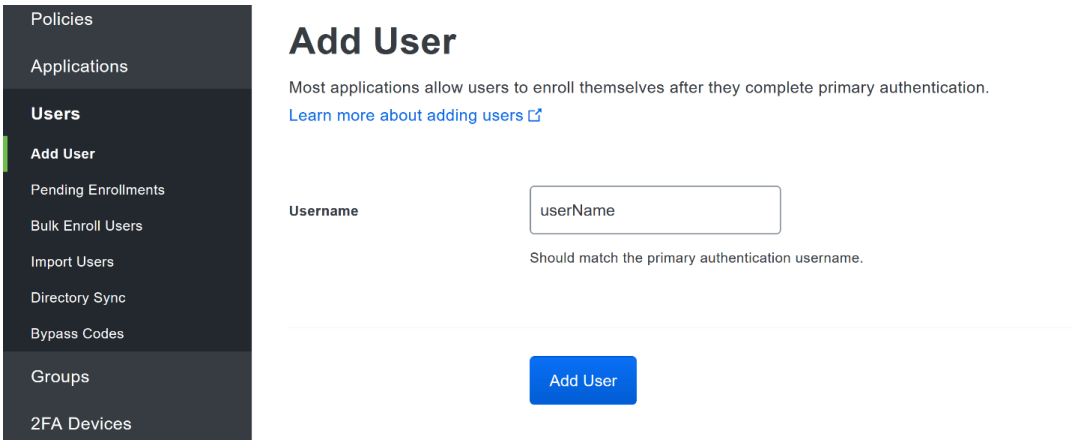
2.3.2 Registering a Duo User

1. Login to the Duo Admin Dashboard.



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, Two-Factor Authentication (2FA) hardware tokens, WebAuthn, etc.) can be associated with that username. *Note: A user will not be able to log into a Duo protected system unless the user is registered and has an authentication device associated with their username.*

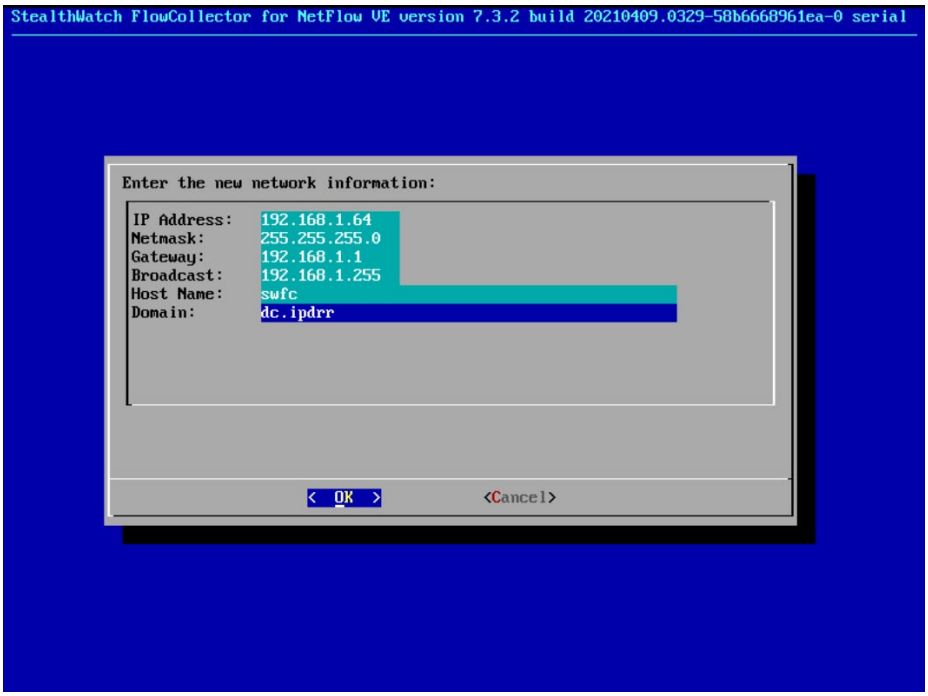
2.4 Cisco Stealthwatch

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

2.4.1 Configure Stealthwatch Flow Collector

1. Log in to the console of the Stealthwatch Flow Collector.

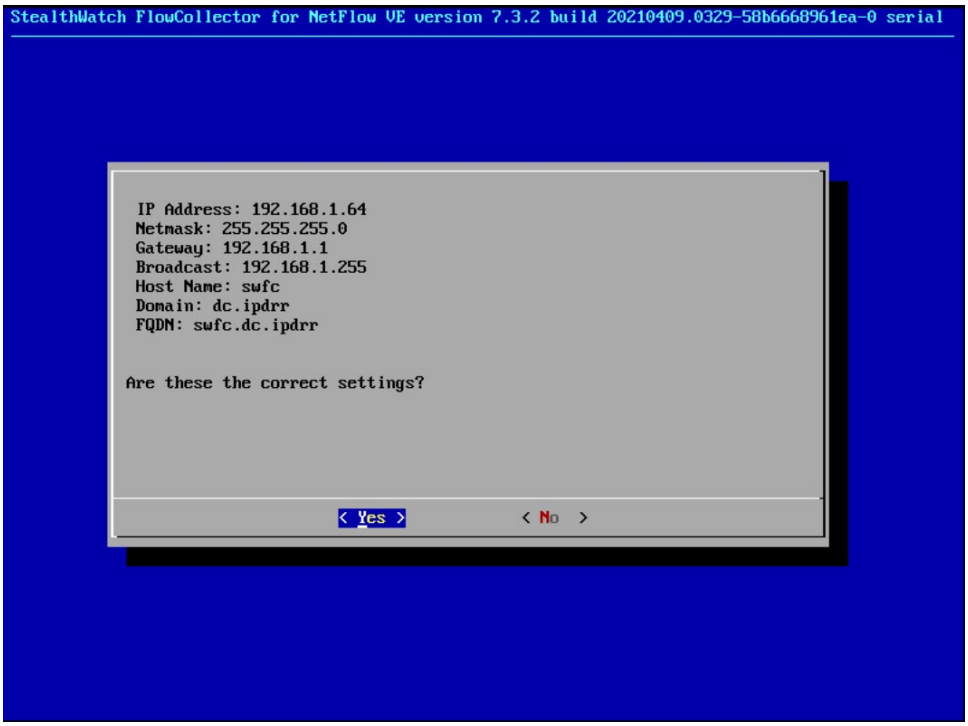
2. Enter the networking information for the machine.



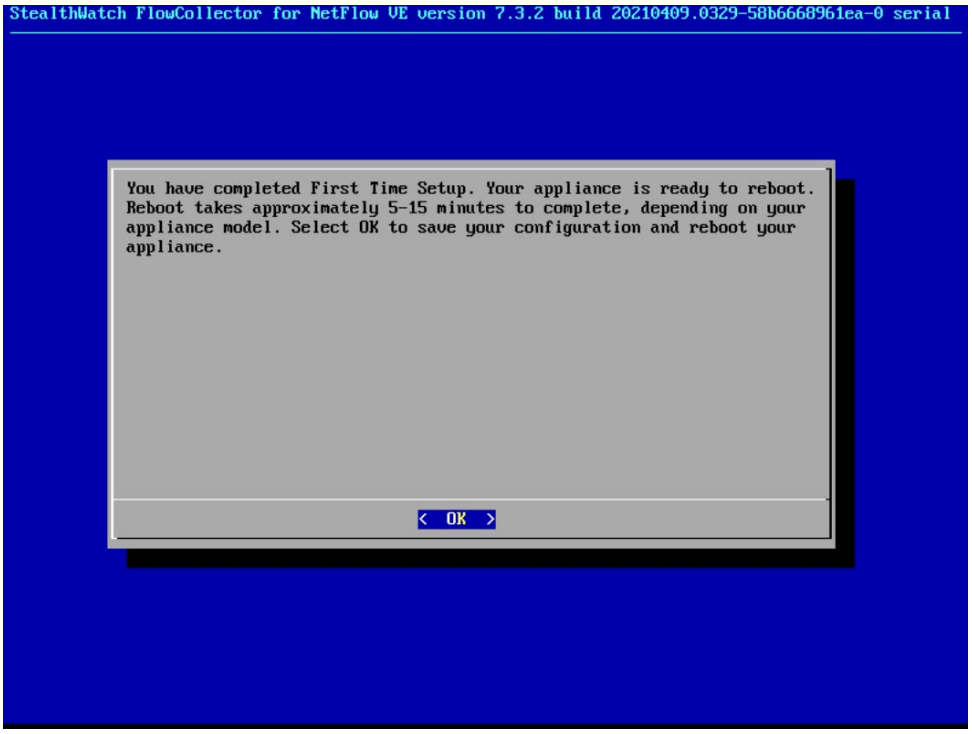
3. Select **OK** and press **Enter**.

4. Navigate the menu to highlight **Management** and **Select**.

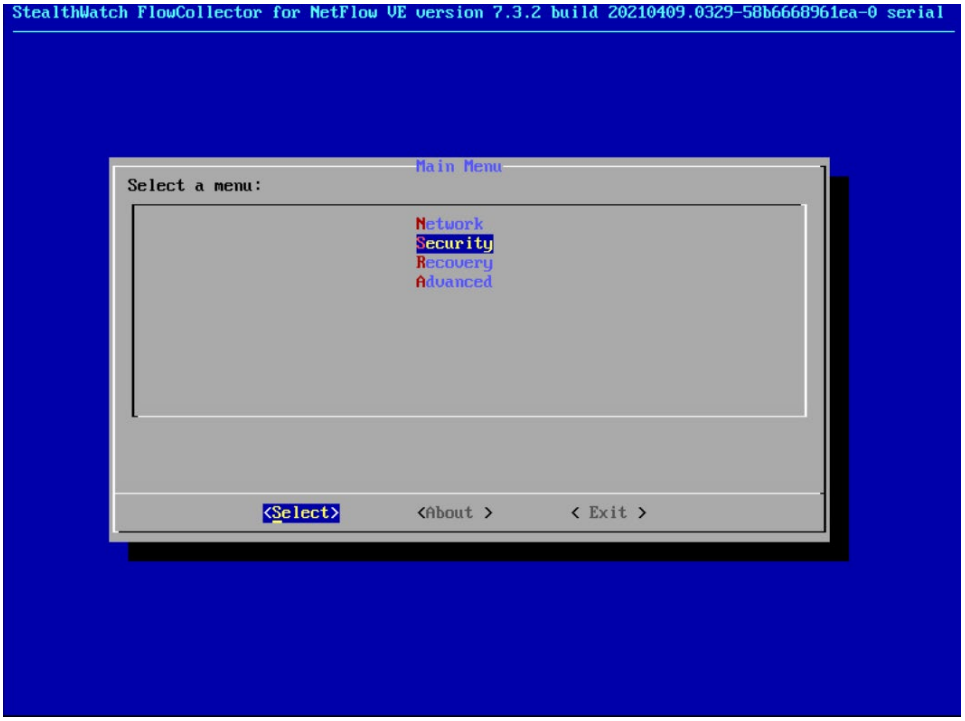
5. Confirm the settings.



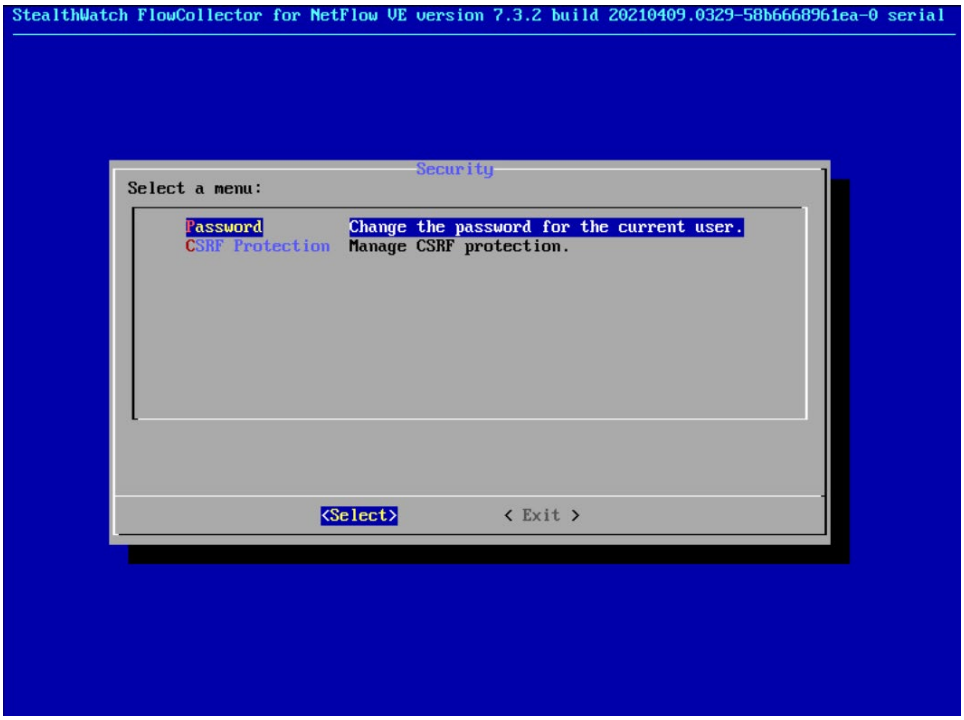
6. Select **Yes** and press **Enter**.



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



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



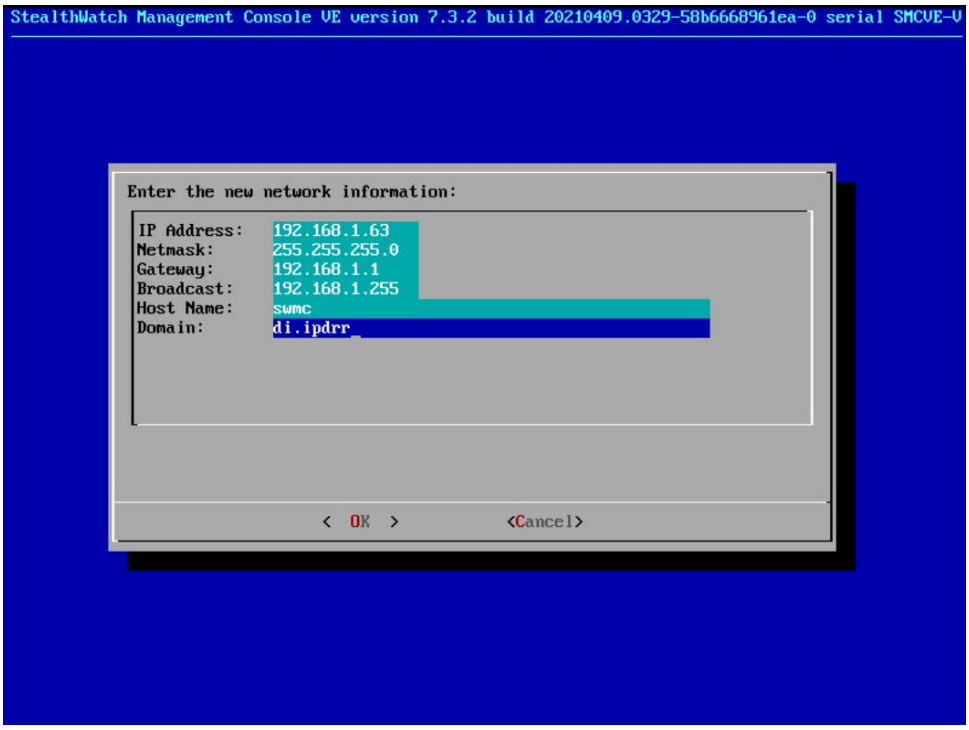
9. Select **Password** and press **Enter**.

10. Change the password from the default password to a secure password.

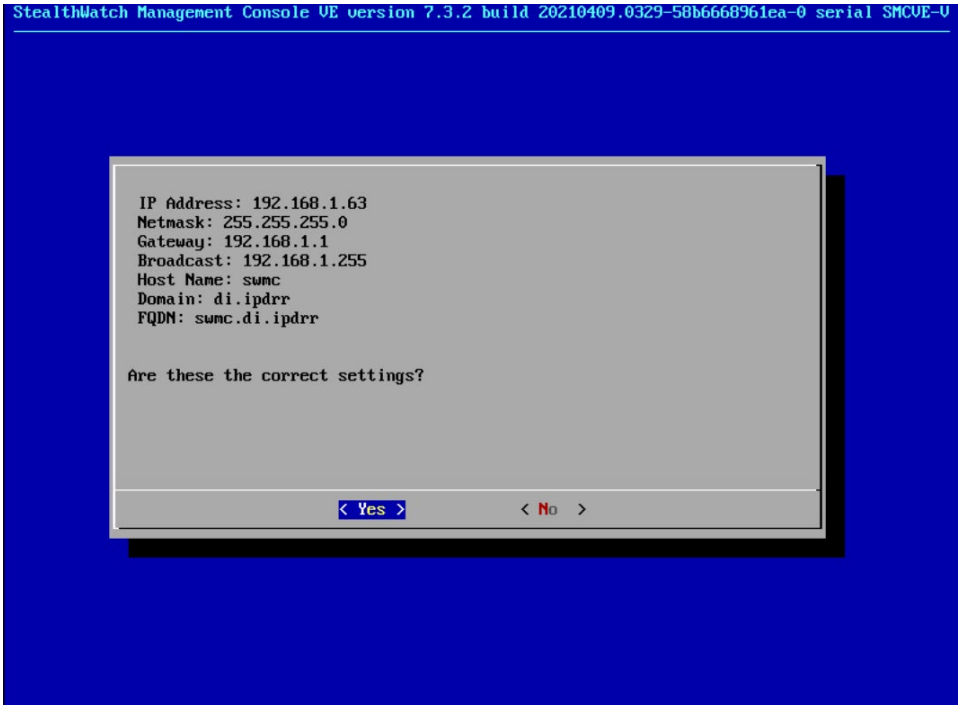
2.4.2 Configure Stealthwatch Management Console

1. Log in to the console of the Stealthwatch Management Console.

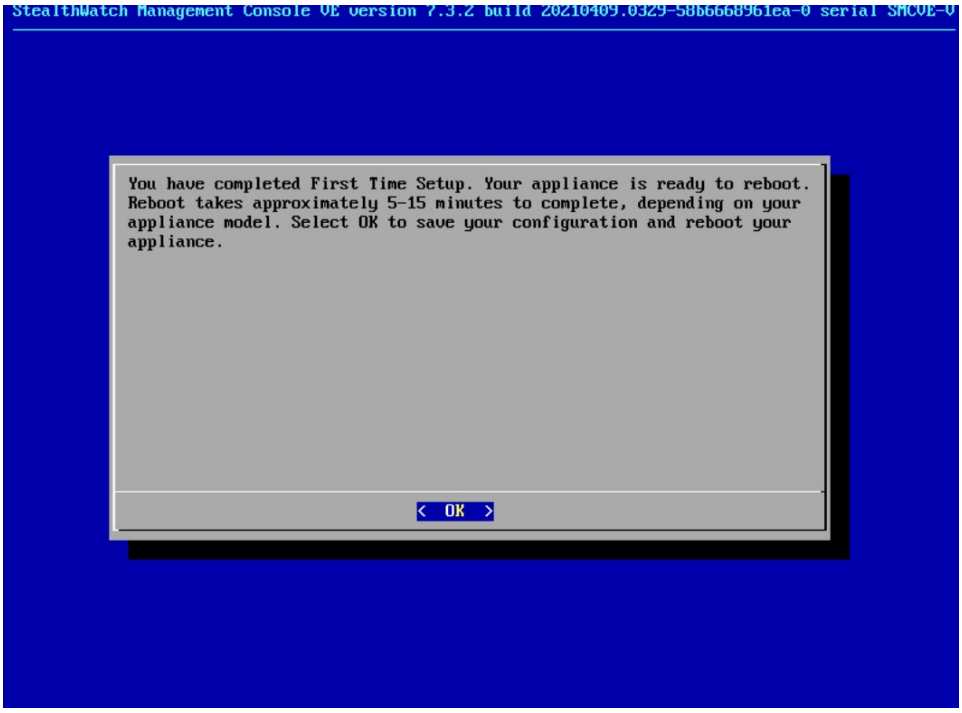
2. Enter the networking information for the machine.



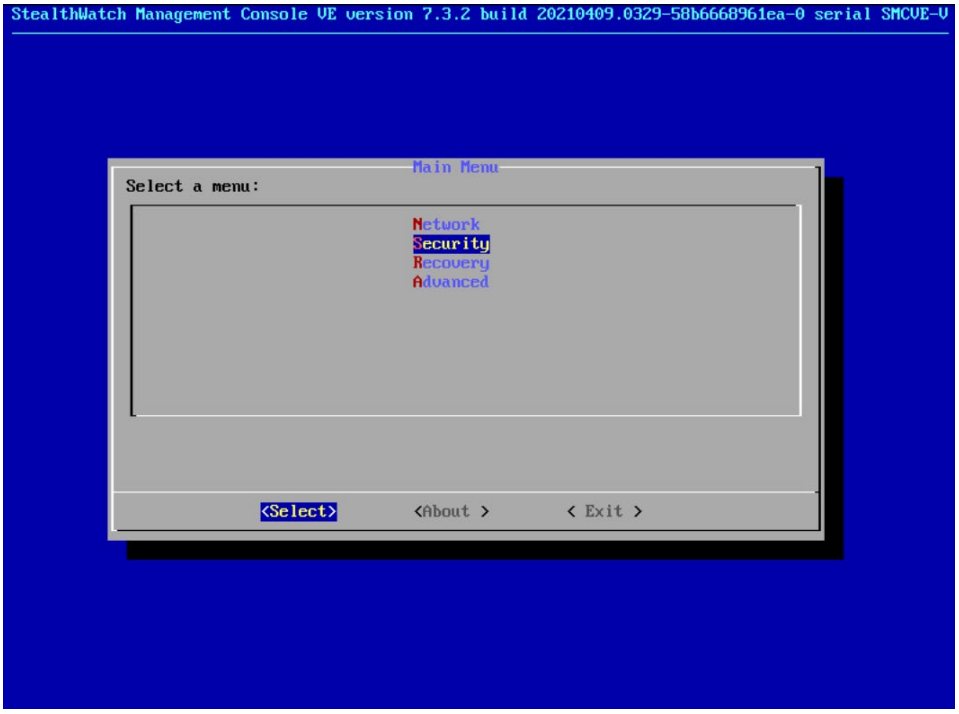
3. Select **OK** and press **Enter**.



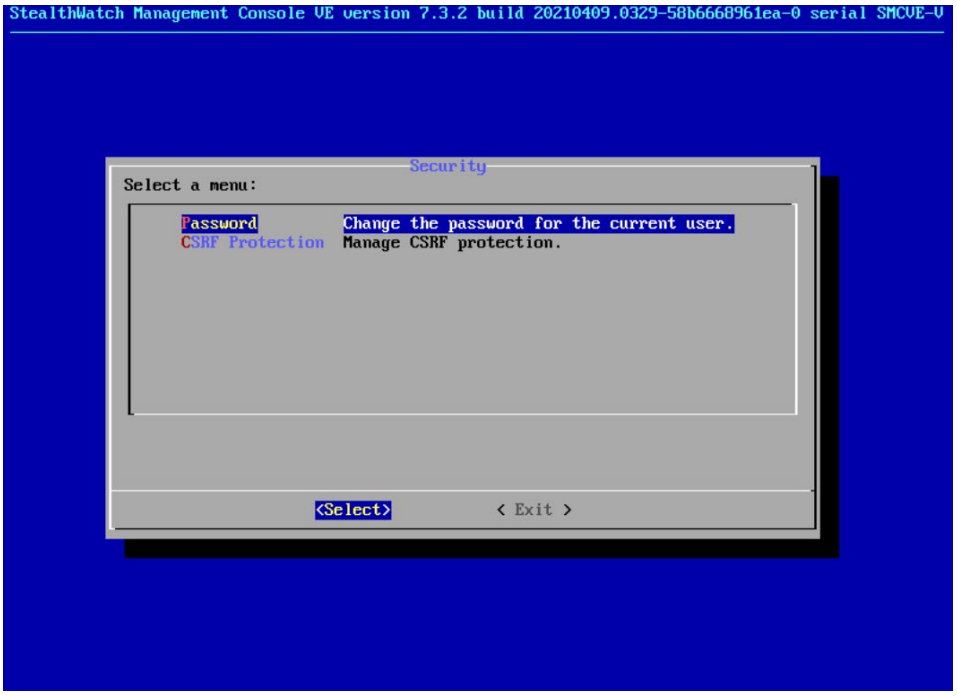
4. Select **Yes** and press **Enter**.



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



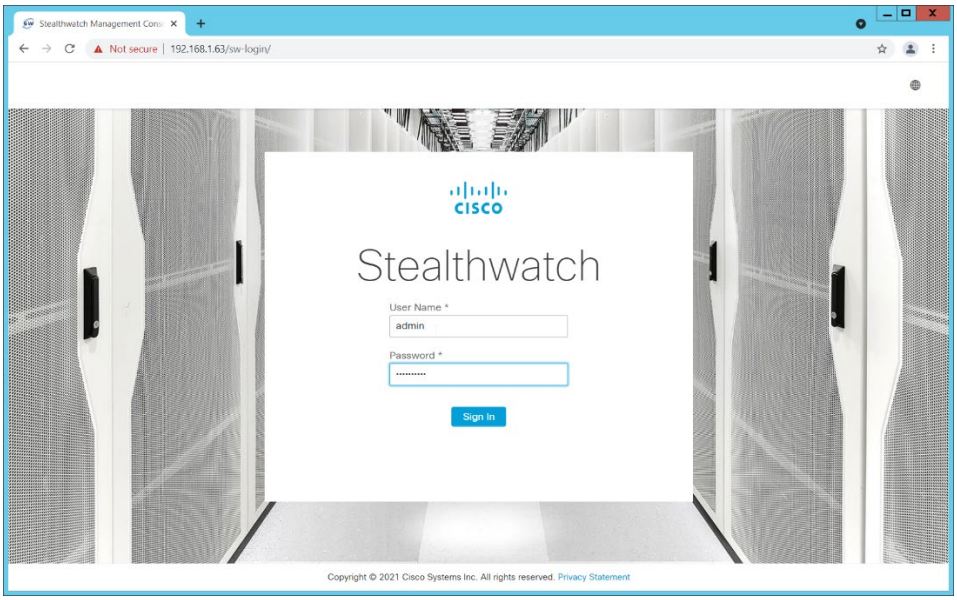
6. Once the machine restarts, navigate to **Security**, and press **Enter**.



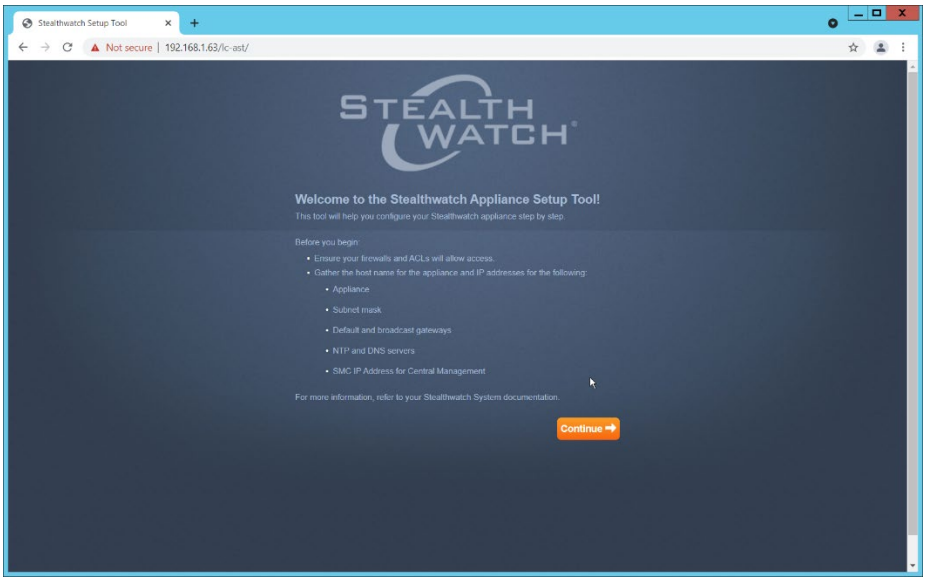
7. Select **Password** and press **Enter**.

8. Change the password from the default password to a secure password.

9. Navigate to the Stealthwatch Management Console from a web browser. The URL will be https://<<*address of Stealthwatch MC*>>.

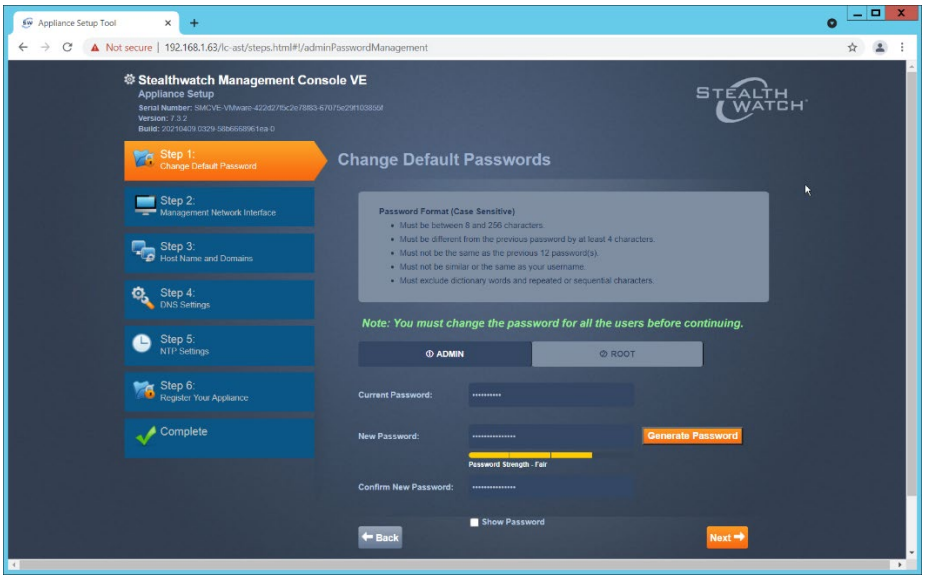


10. Login using the default username and password (should be provided by product vendor).



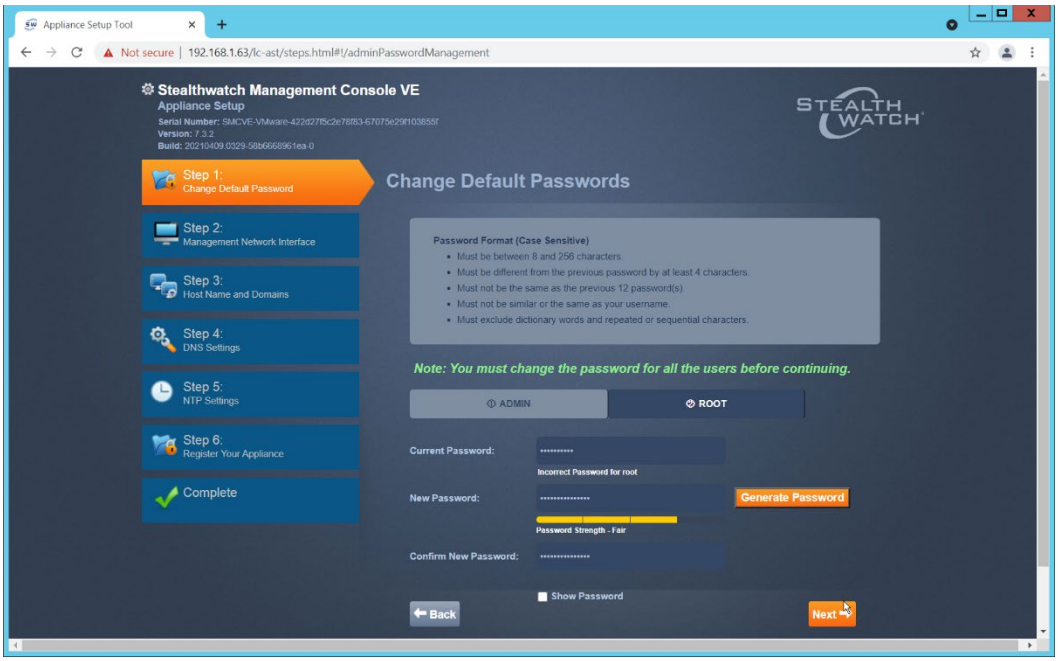
11. Click **Continue**.

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



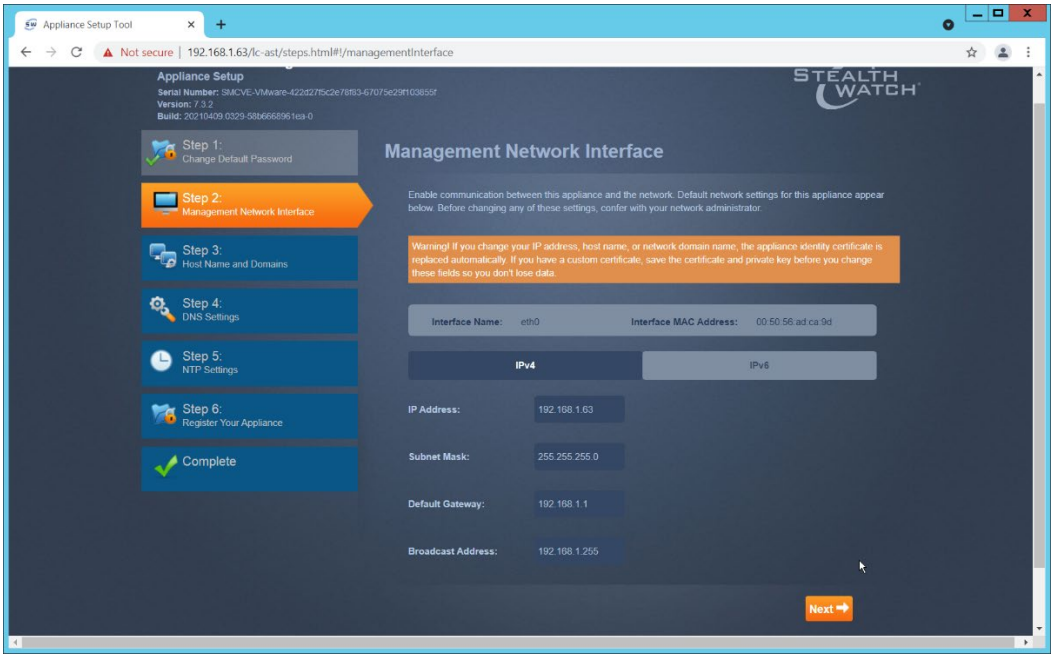
13. Click **Next**.

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

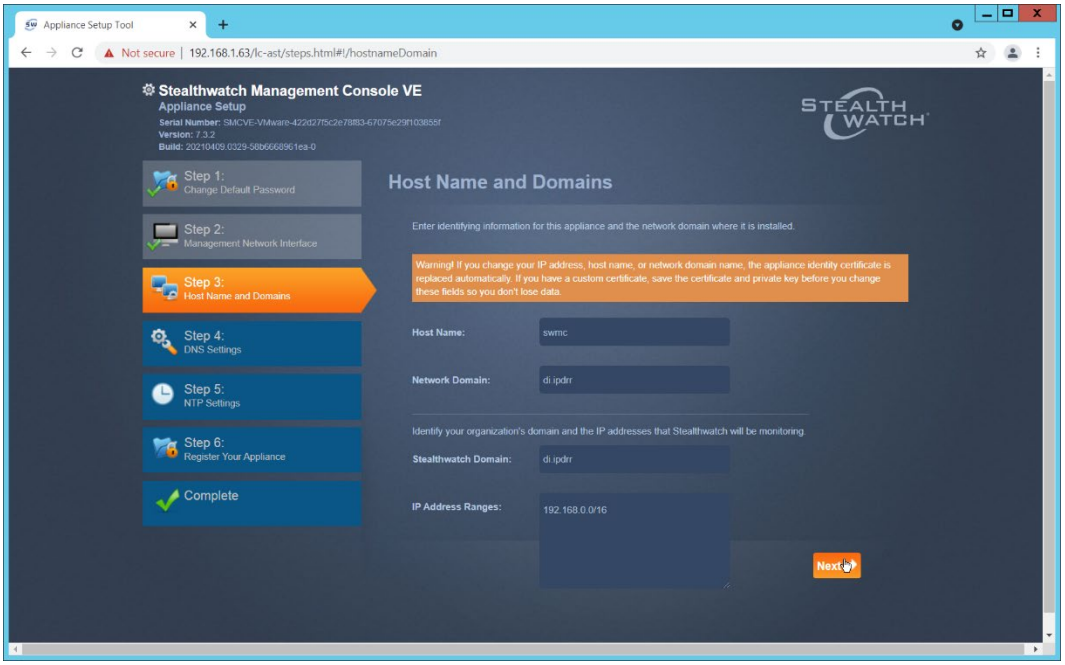


15. Click **Next**.

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

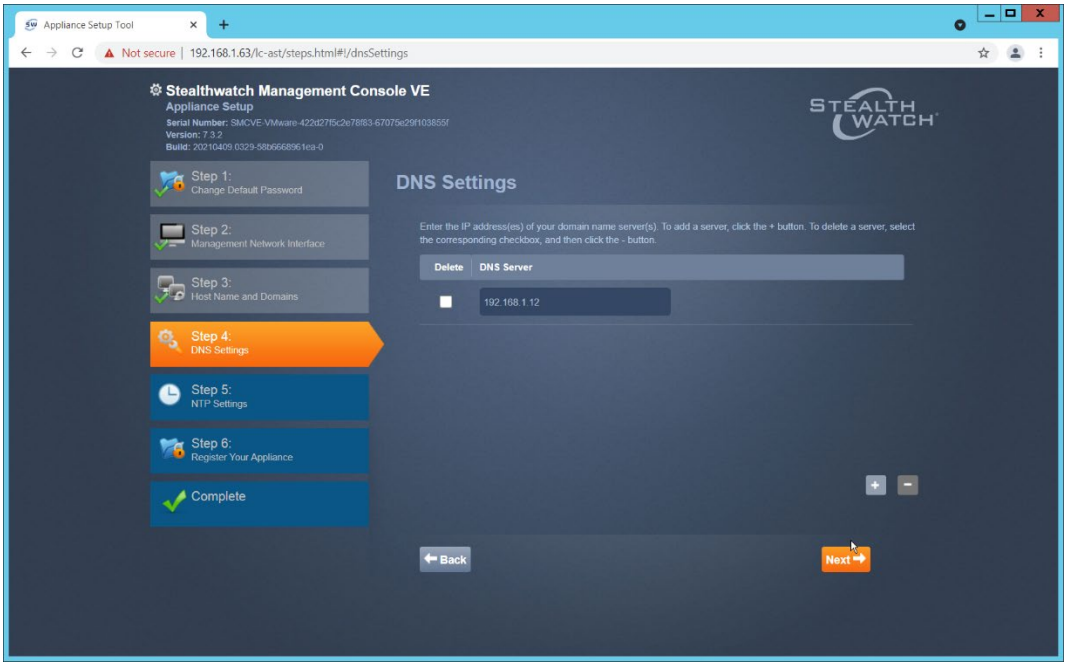


17. Enter the domain for Stealthwatch, and the IP addresses Stealthwatch will be monitoring.



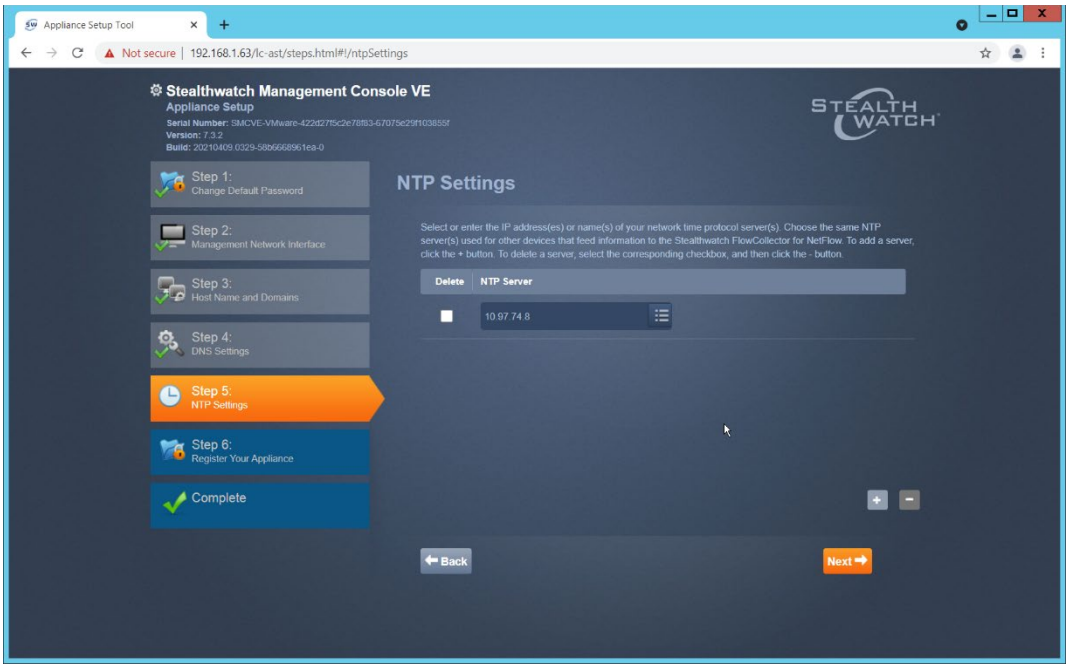
18. Click **Next**.

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

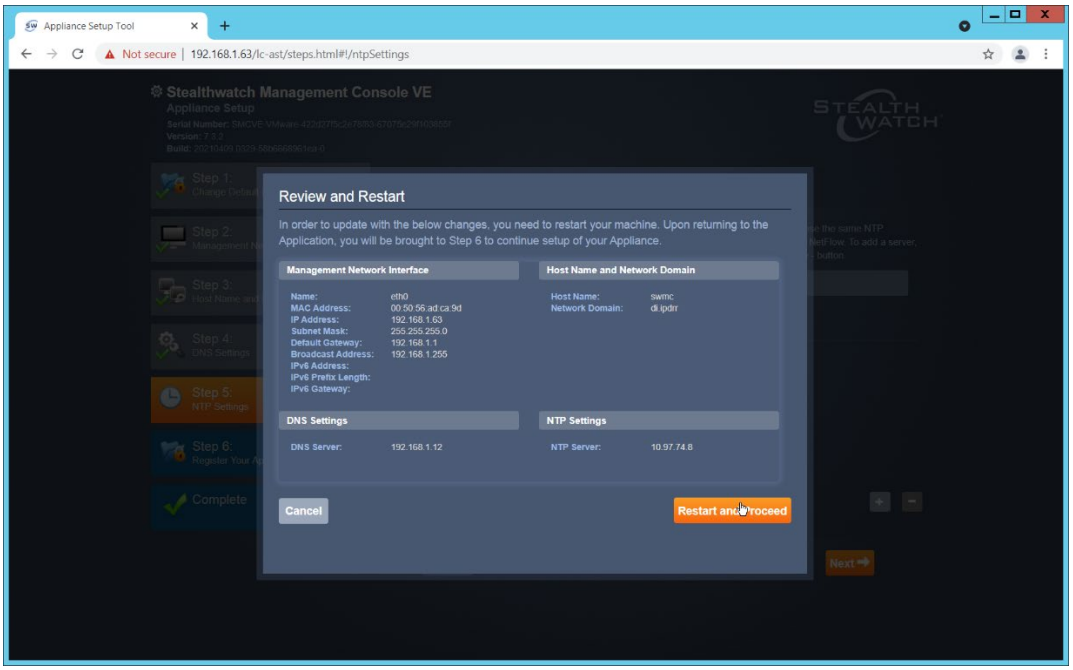


20. Click **Next**.

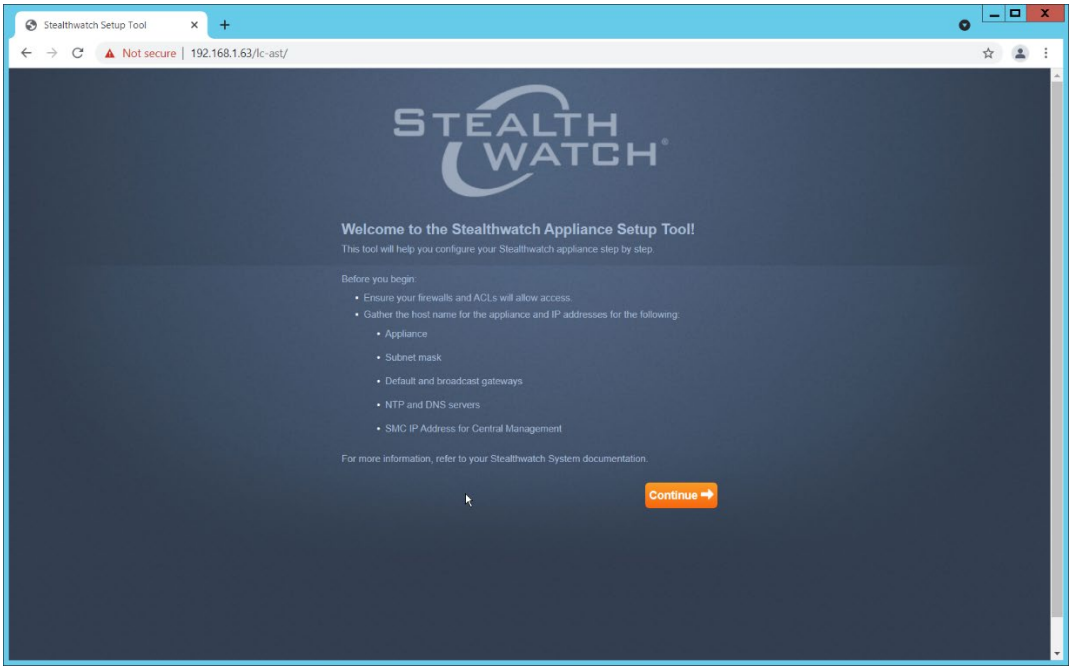
21. Enter the Network Time Protocol (NTP) server(s) Stealthwatch should use.



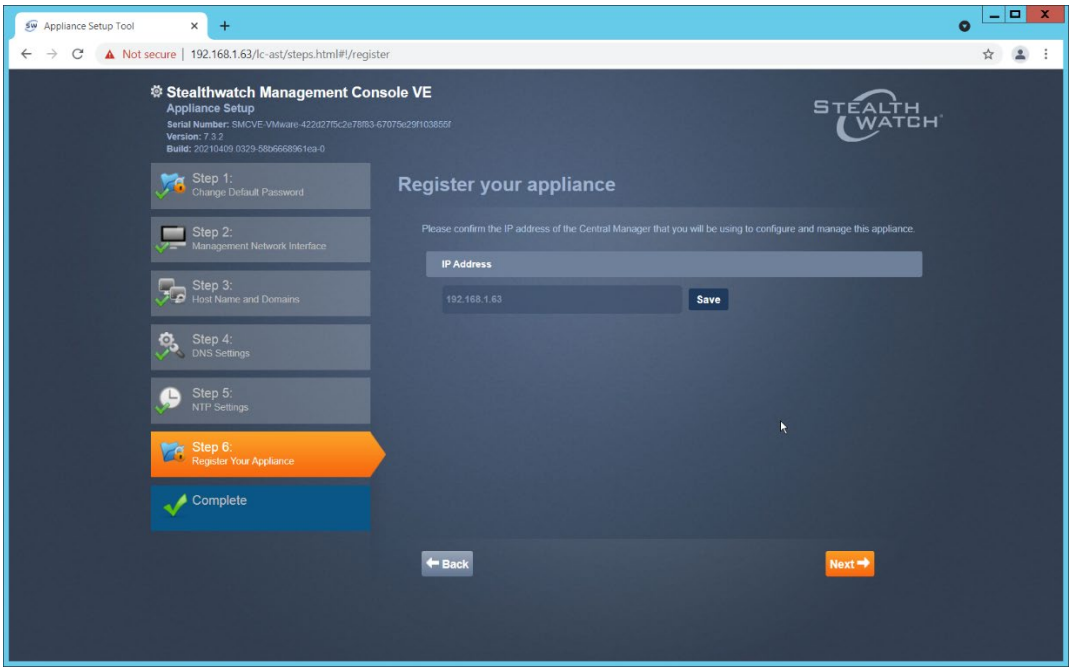
22. Click **Next**.



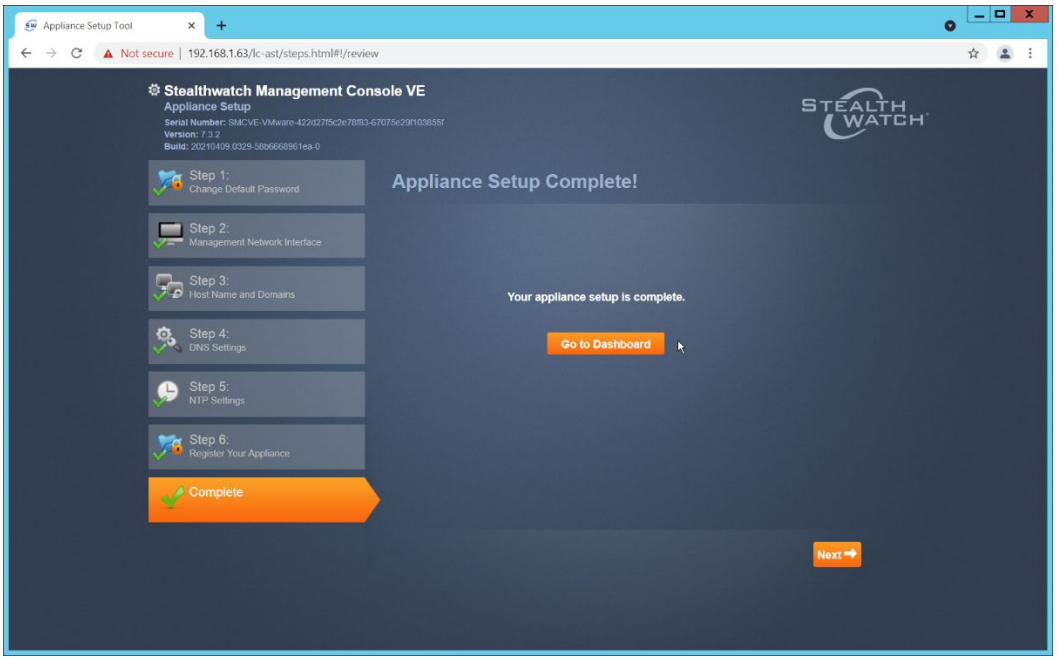
23. Click **Restart and Proceed**.



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



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

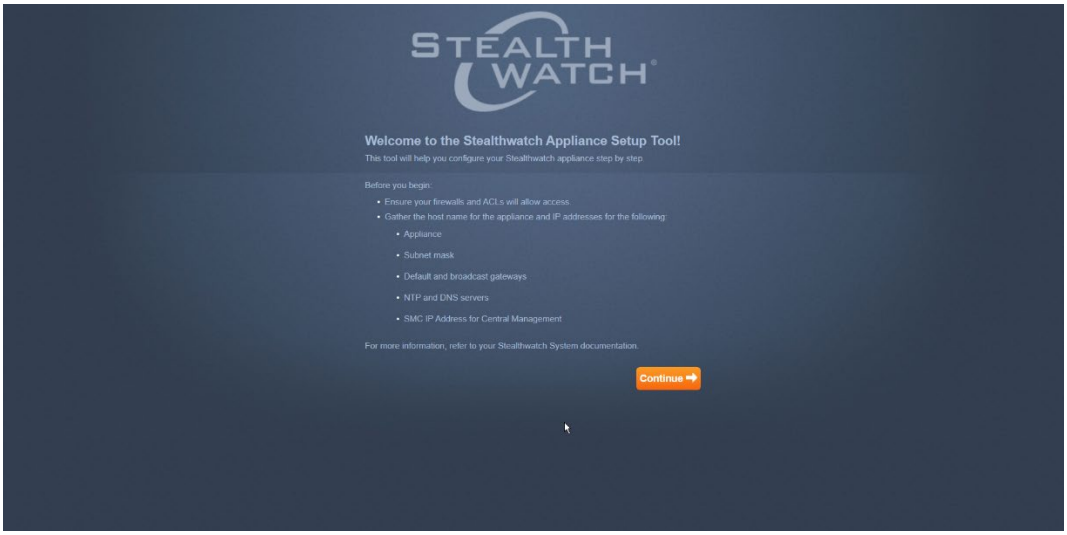


26. Click **Go to Dashboard**.

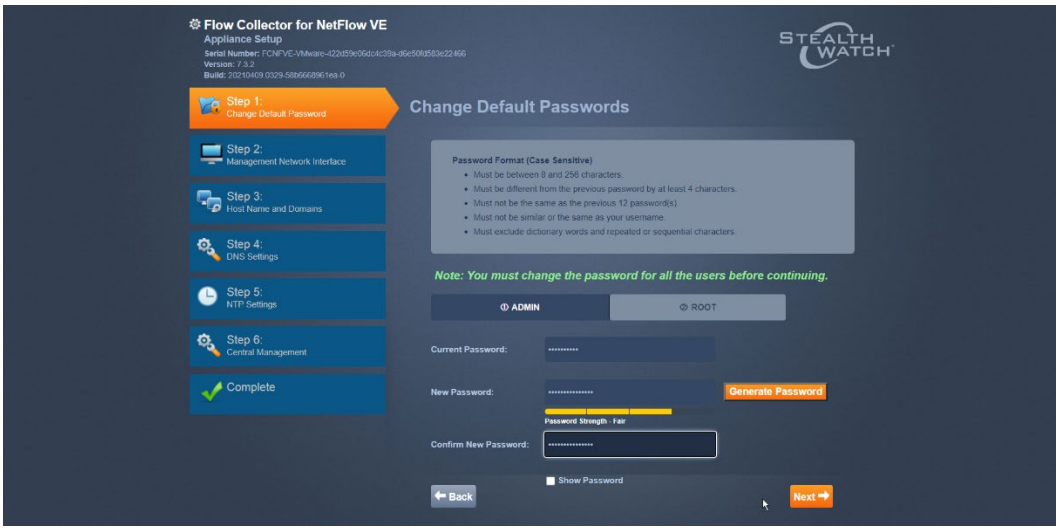
2.4.3 Add Stealthwatch Flow Collector to the Management Console

1. Navigate to the Stealthwatch Flow Collector Console from a web browser. The URL will be https://<<*address of Stealthwatch FC*>>.

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

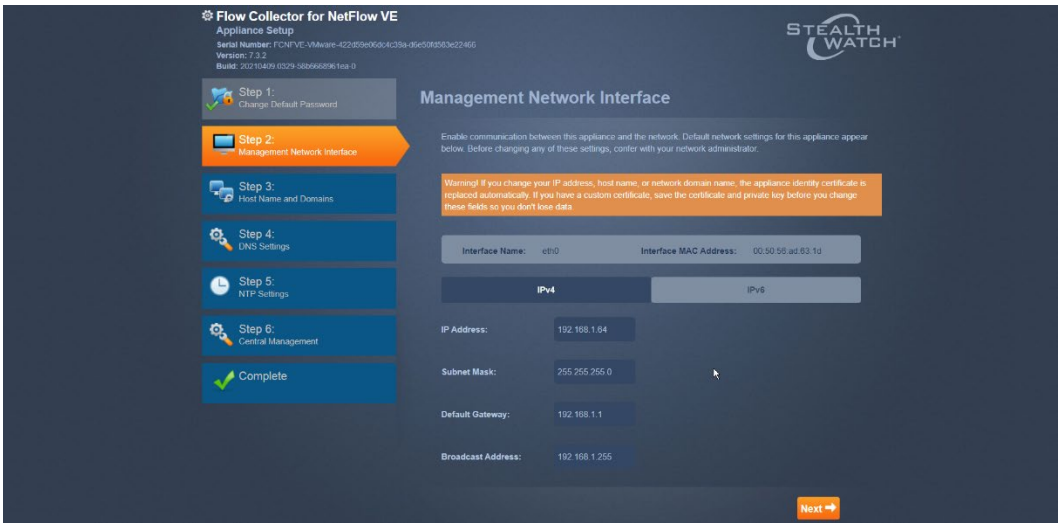


3. Click **Continue**.



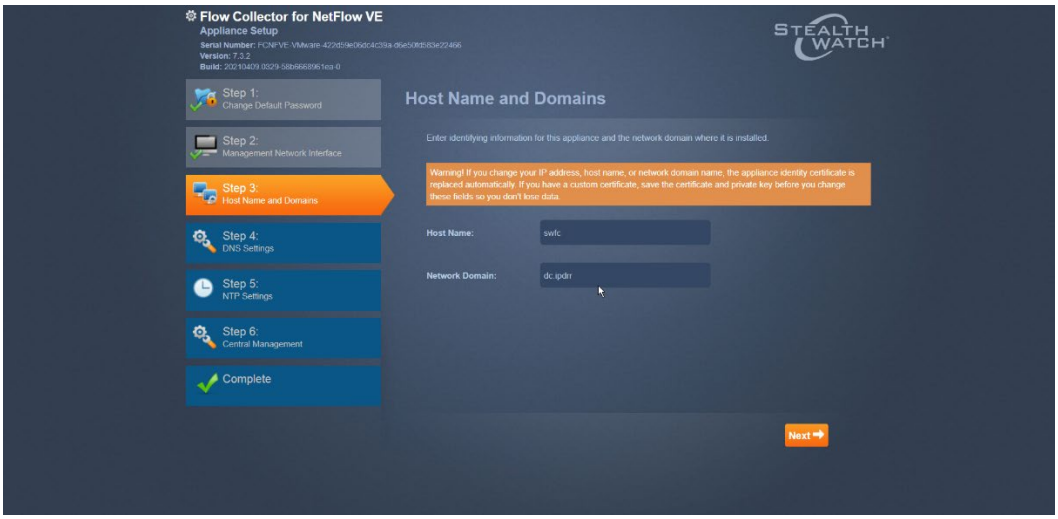
4. Change the passwords for the admin and root accounts.

5. Click **Next**.



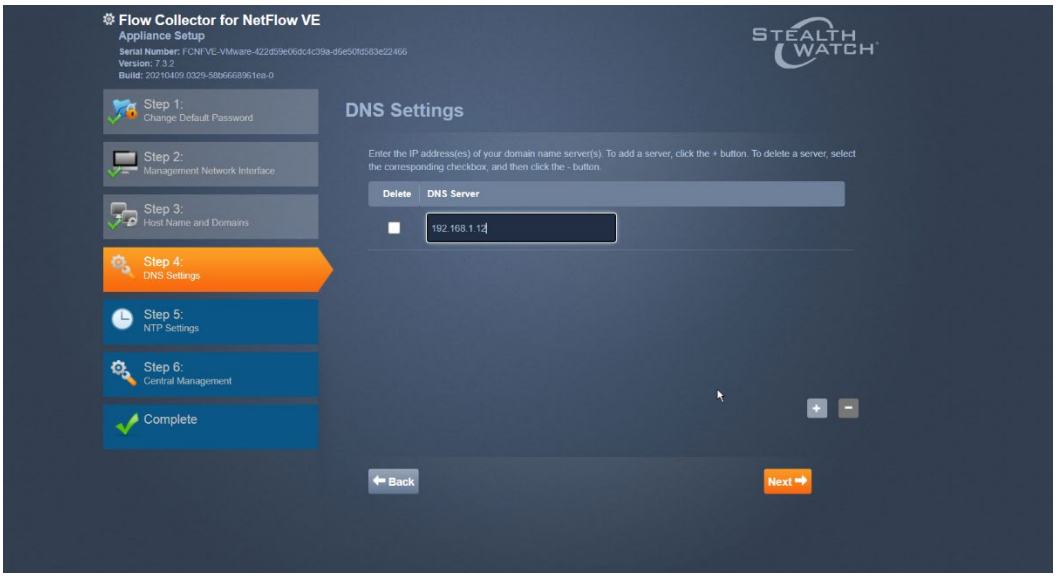
6. Confirm the networking information is correct and click **Next**.

7. Confirm the domain name for Flow Collector is correct.



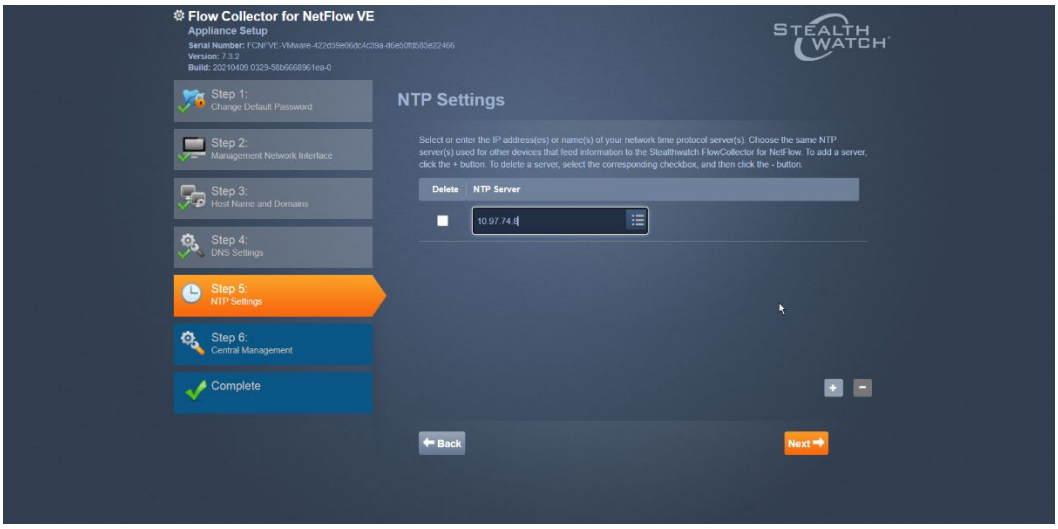
8. Click **Next**.

9. Add the DNS server(s) Stealthwatch should be using.

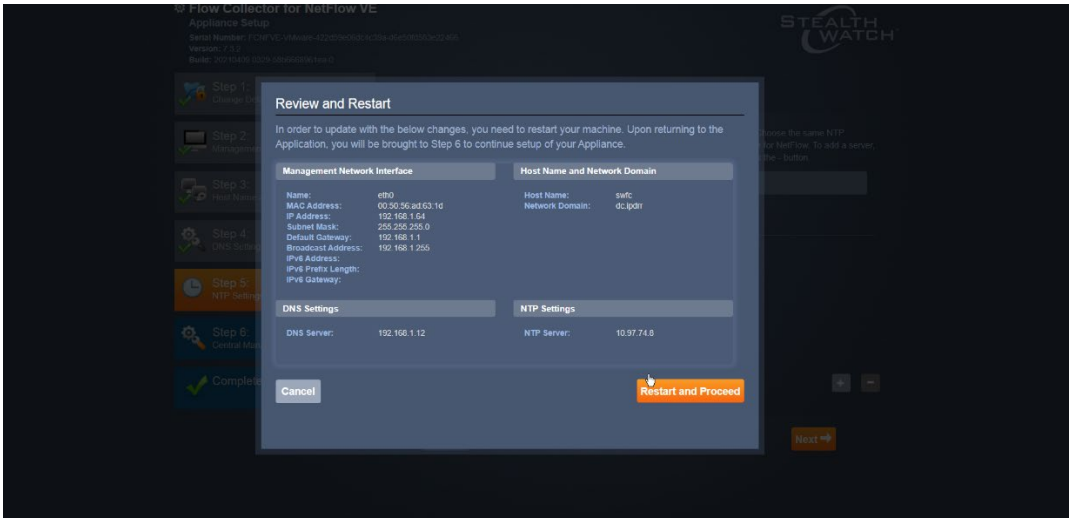


10. Click **Next**.

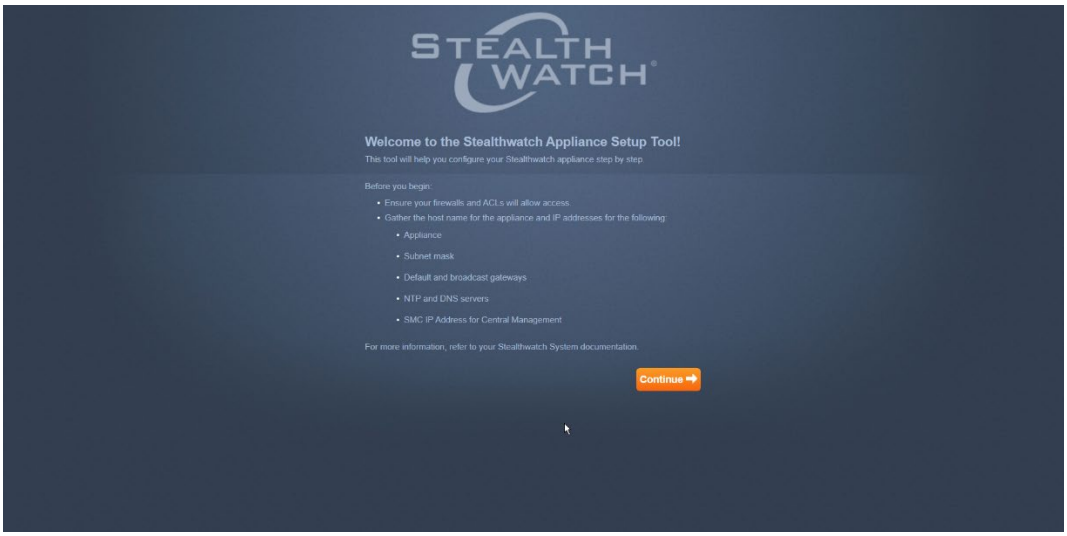
11. Enter the NTP server(s) Stealthwatch should use.



12. Click **Next**.

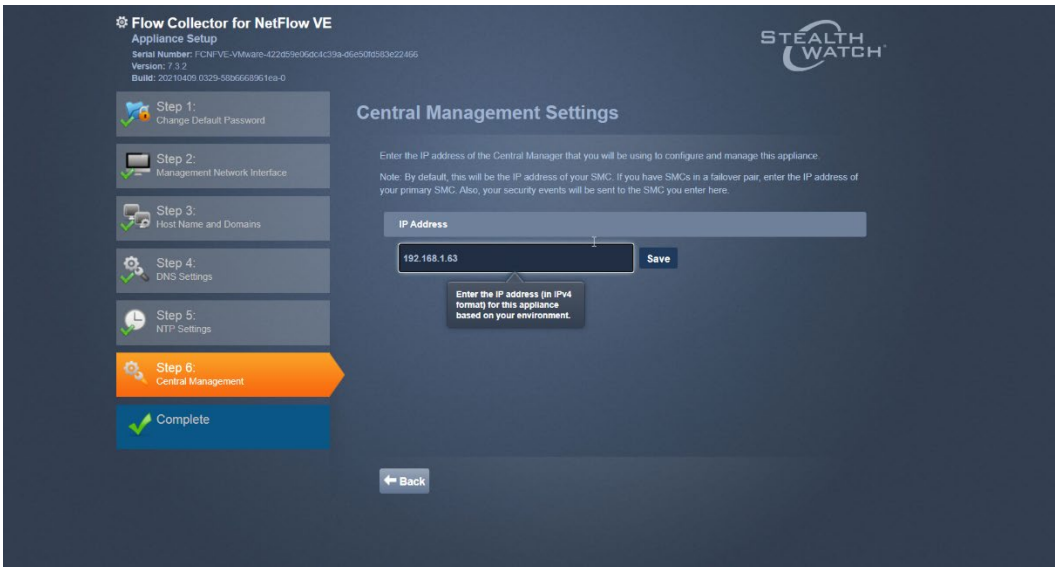


13. Click **Restart and Proceed**.

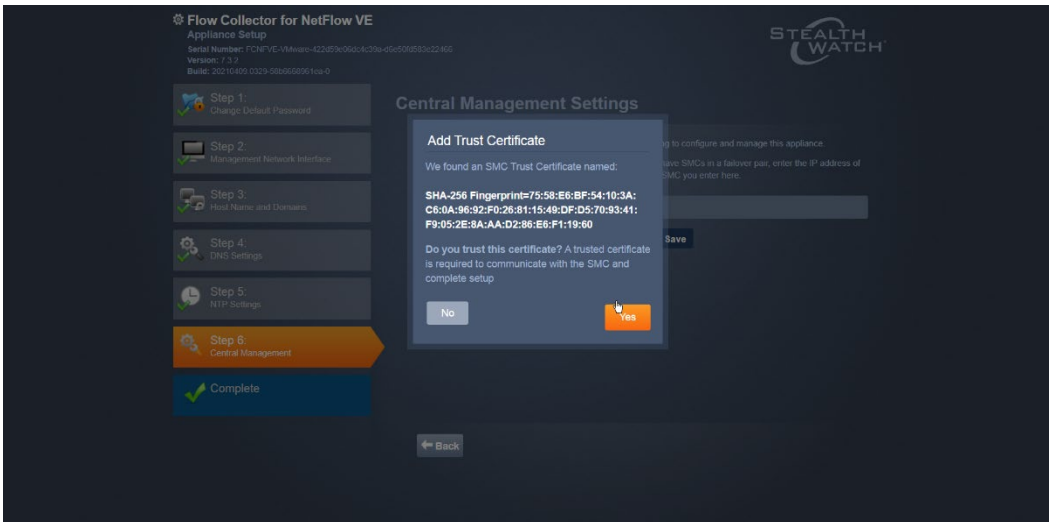


14. After it restarts, log in again, and click **Continue**.

15. Enter the IP of the Stealthwatch Management Console.

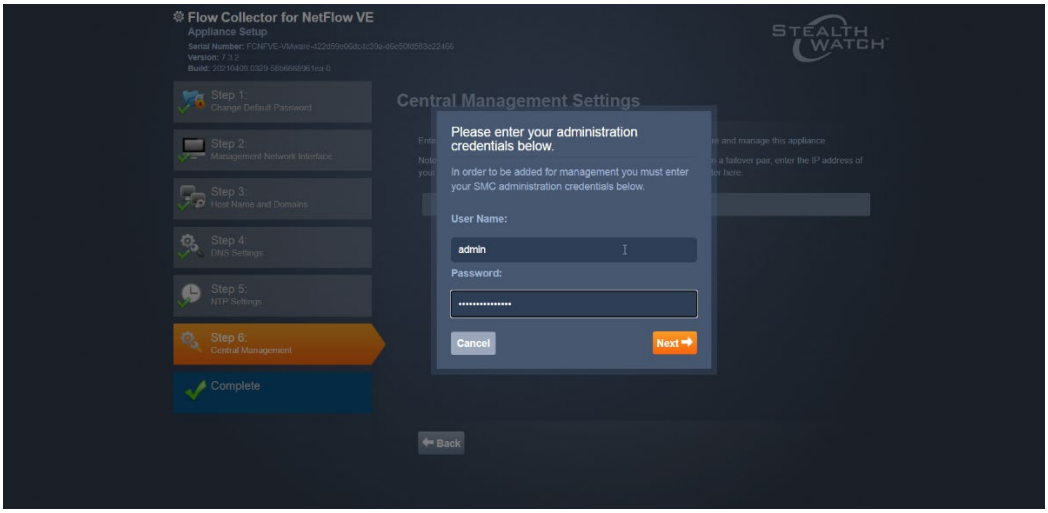


16. Click **Save**.



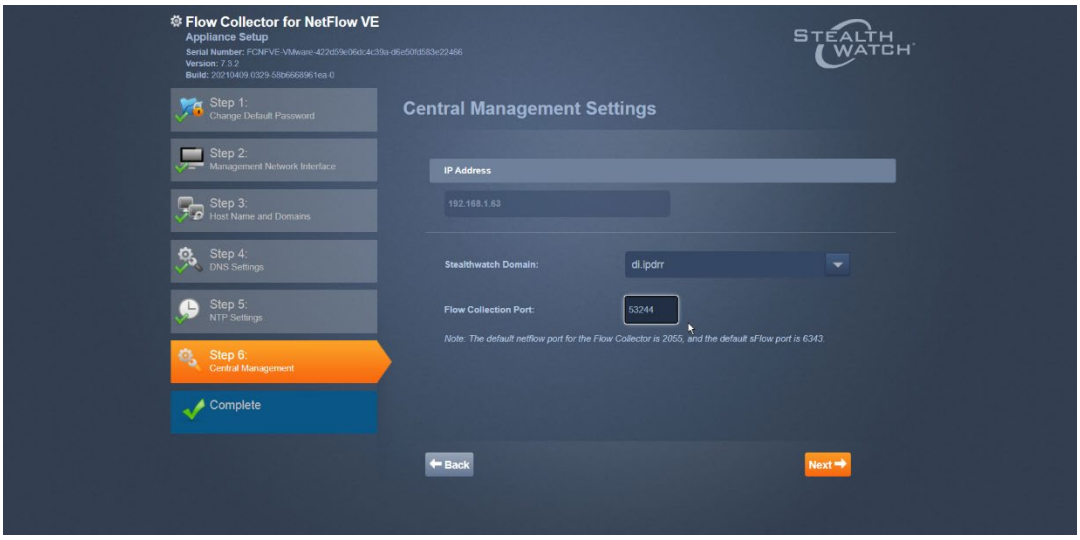
17. Accept the certificate by clicking **Yes**.

18. Enter the username and password for the Stealthwatch Management Console.

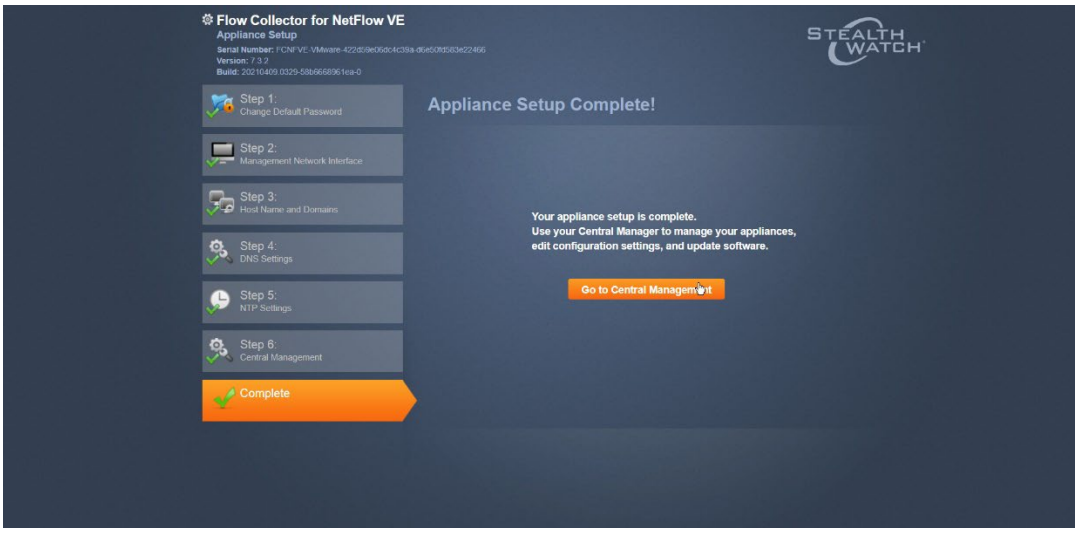


19. Click **Next**.

20. Enter the **Domain** and **Flow Collection Port**.



21. Click **Next**.



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

2.5 Dispel

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

2.5.1 Installation

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

2. Login with username “dispel” and the password provided.

```
dispelwicket login: dispel
Password:
Linux dispelwicket 4.19.195-amd64-vyos #1 SMP Thu Feb 17 12:52:59 UTC 2022 x86_6
4
Welcome to VyOS!

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

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

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

dispel@dispelwicket:~$
```

3. Begin the installation process.

> install image

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

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

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

Partition (Auto/Parted/Skip) [Auto]:

I found the following drives on your system:
 sda    150323MB


Install the image on? [sda]:

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

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

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

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

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

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

Creating filesystem on /dev/sda1: OK
Done!
Mounting /dev/sda1...
What would you like to name this image? [999.202203220259]:
OK.  This image will be named: 999.202203220259
Copying squashfs image...
Copying kernel and initrd images...
Done!
I found the following configuration files:
    /opt/vyatta/etc/config/config.boot
    /opt/vyatta/etc/config.boot.default
Which one should I copy to sda? [/opt/vyatta/etc/config/config.boot]:

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

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

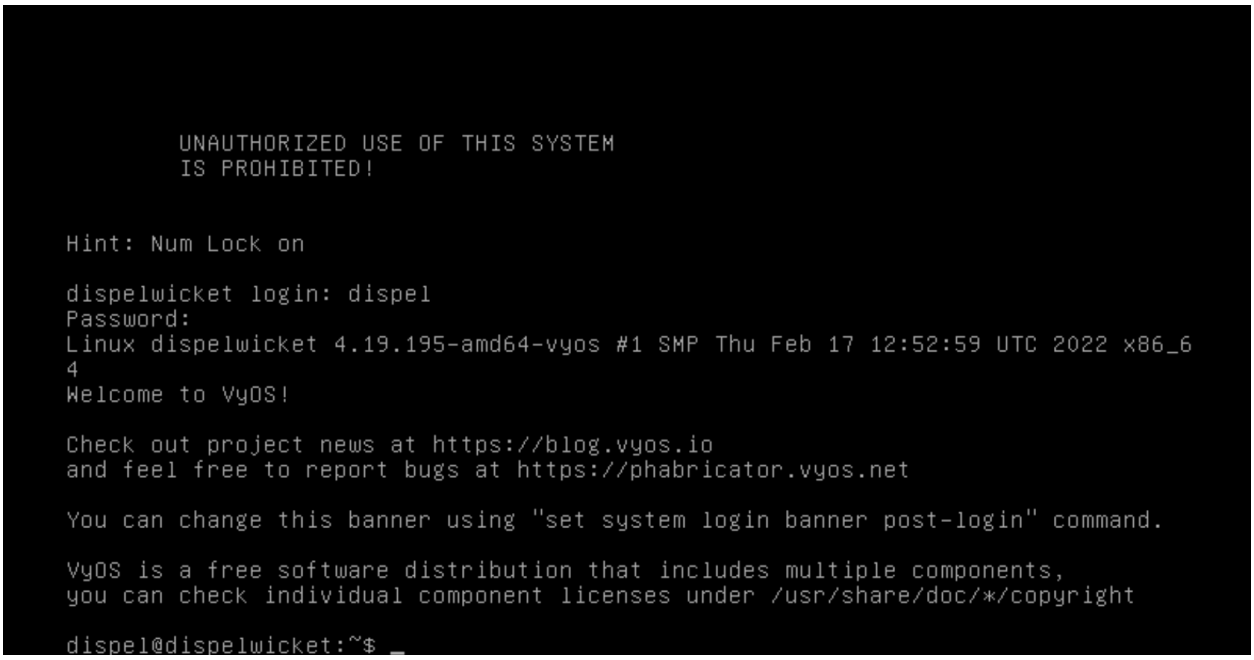
```
Enter password for administrator account
Enter password for user 'dispel':
Retype password for user 'dispel':
I need to install the GRUB boot loader.
I found the following drives on your system:
 sda    150323MB


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

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

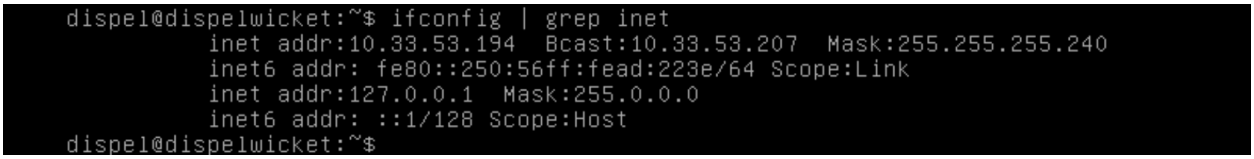
```
Which drive should GRUB modify the boot partition on? [sda]:

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

9. Power off the machine, remove the provided optical disk image, and power it back on.

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



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



2.5.2 Configuring IP Addresses

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

```
        UNAUTHORIZED USE OF THIS SYSTEM
        IS PROHIBITED!


Hint: Num Lock on

dispelwicket login: dispel
Password:
Linux dispelwicket 4.19.195-amd64-vyos #1 SMP Thu Feb 17 12:52:59 UTC 2022 x86_6
4
Welcome to VyOS!

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

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

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

dispel@dispelwicket:~$
```

2. Type in the command > `configure`.

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

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

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

4. Type in the command > `set interfaces ethernet eth0 address` followed by the desired IP address in CIDR notation, modifying for the desired interface as appropriate.

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

5. Type in the command > `commit`.

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

6. Type in the command > `save`.

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

7. Type in the command **> exit**.

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

2.5.3 Configuring Network

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

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

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

2. Type in the command `> set protocols static route 0.0.0/0 next-hop` followed by the IP address of the router you wish to forward to.

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

3. Type in the command `> commit`.

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

4. Type in the command `> save`.

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

5. Type in the command `> exit`.

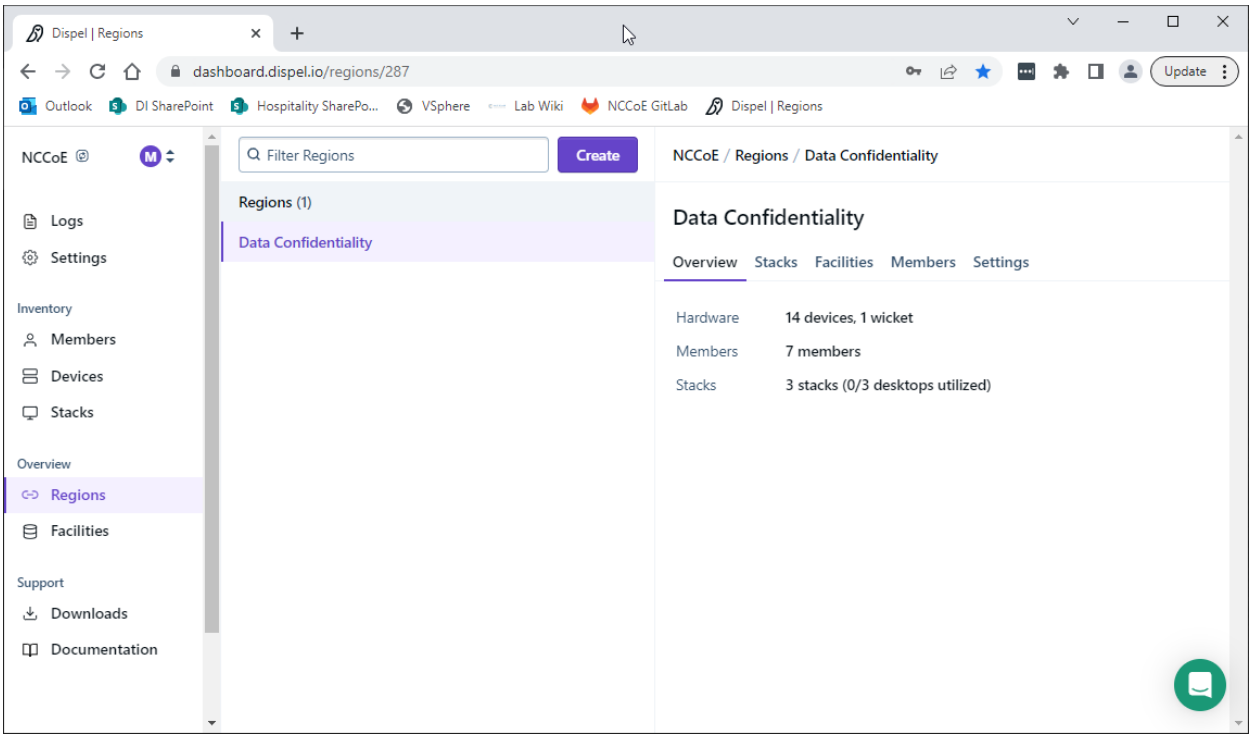
```
dispel@dispelwicket# exit
exit
dispel@dispelwicket:~$
```

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

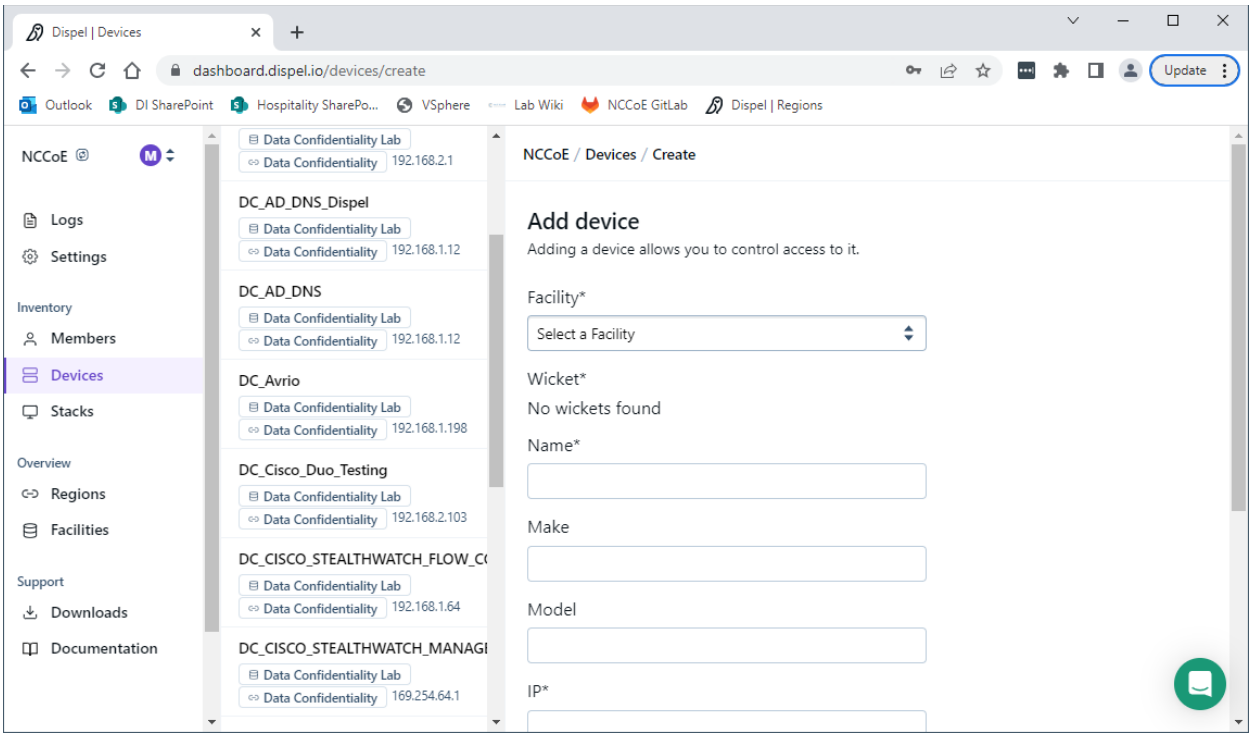
7. Modify the IP addresses of the south-side network interface to properly align with your network. See the “Configuring IP Addresses” section above.

2.5.4 Adding a Device

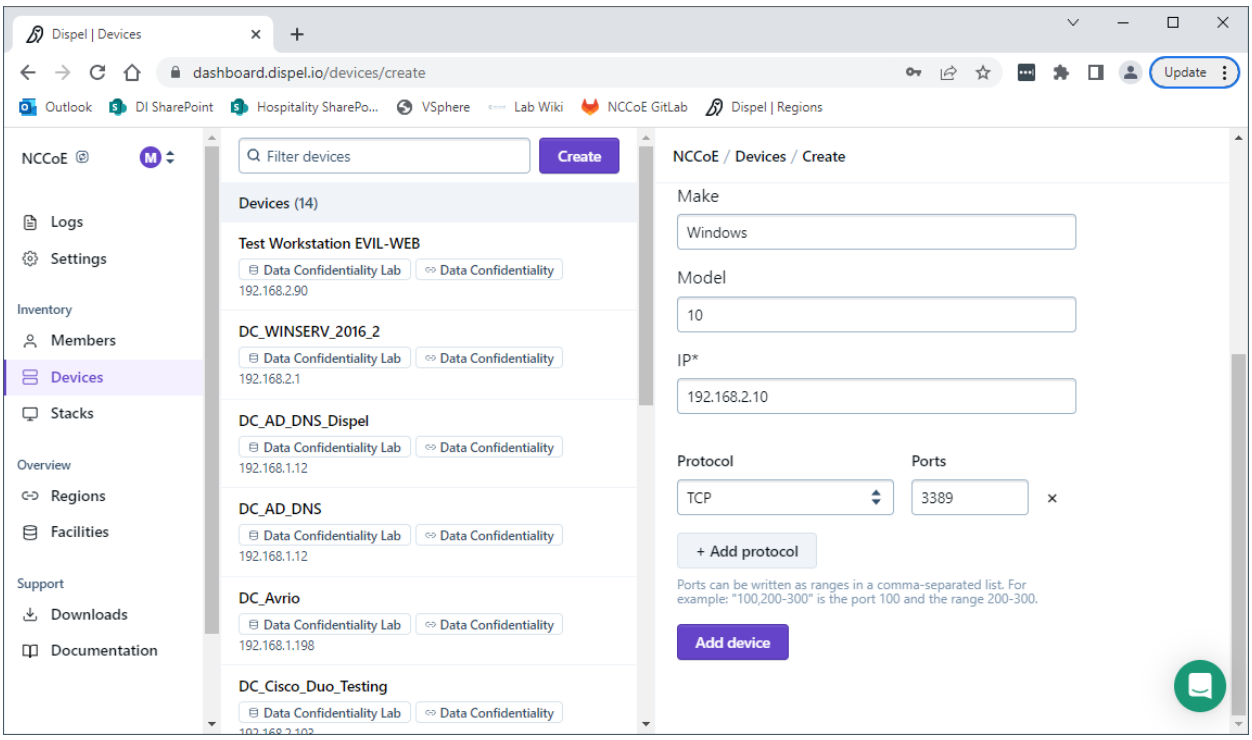
1. On the workstation in question, ensure that ping and RDP are accessible, including allowing such connections through a local firewall.
2. Authenticate to the Dispel webpage with the provided credentials.



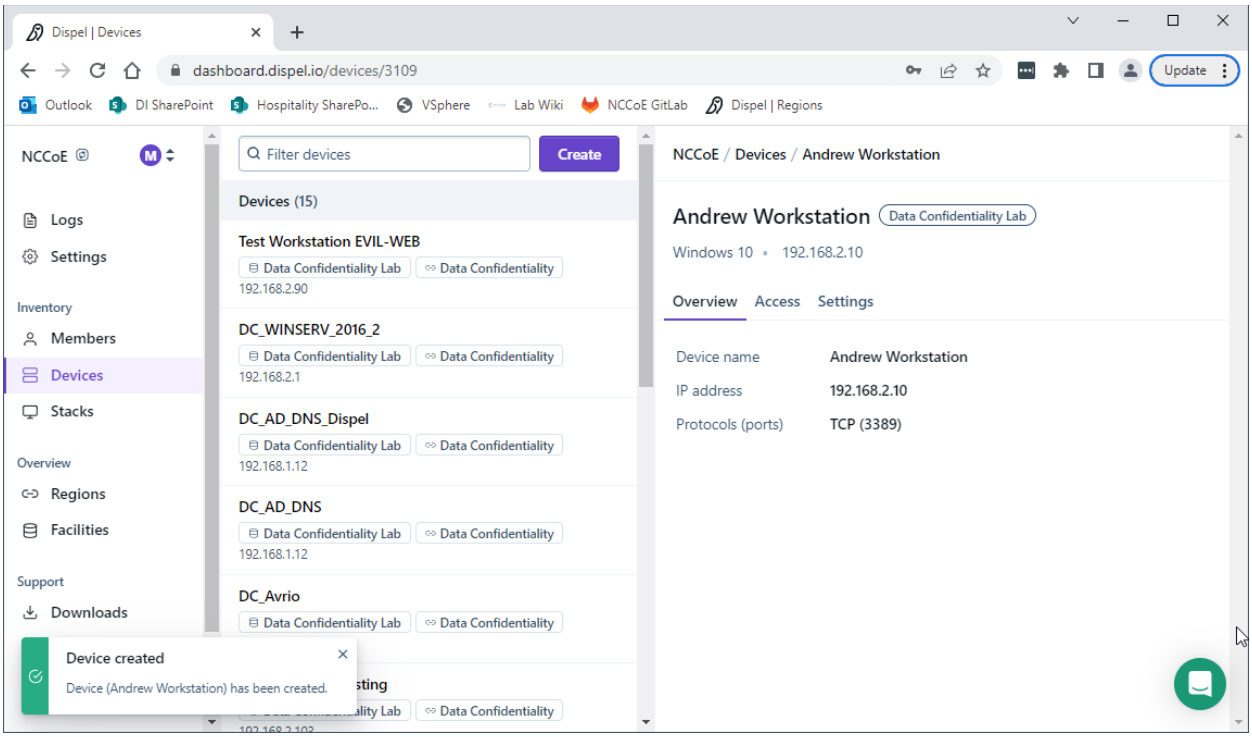
3. Click on the **Devices** page on the sidebar and click **Create**.



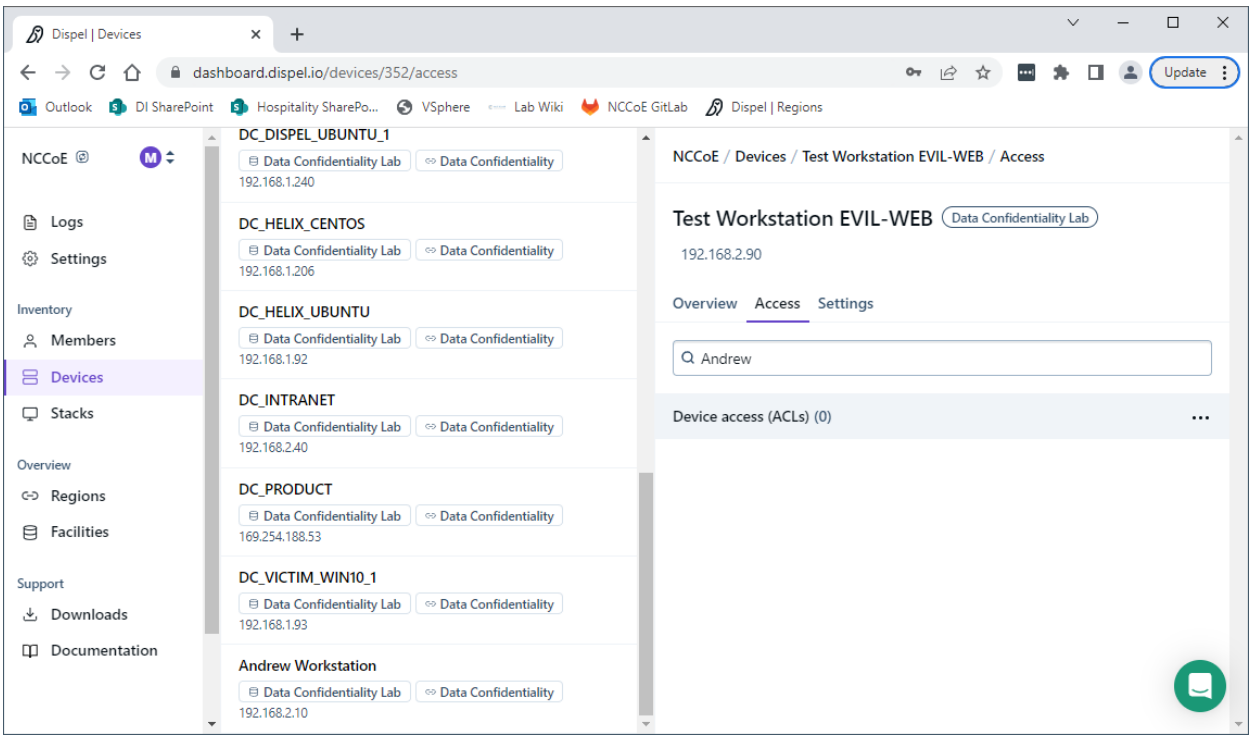
4. Under the **Add Device** window, fill out all fields, including **Facility**, **Wicket**, **Name**, **Make**, **Model**, **IP**, and **Protocol**.



5. Click **Add Device**.



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



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

2.6 Integration: FireEye Helix and Cisco Stealthwatch

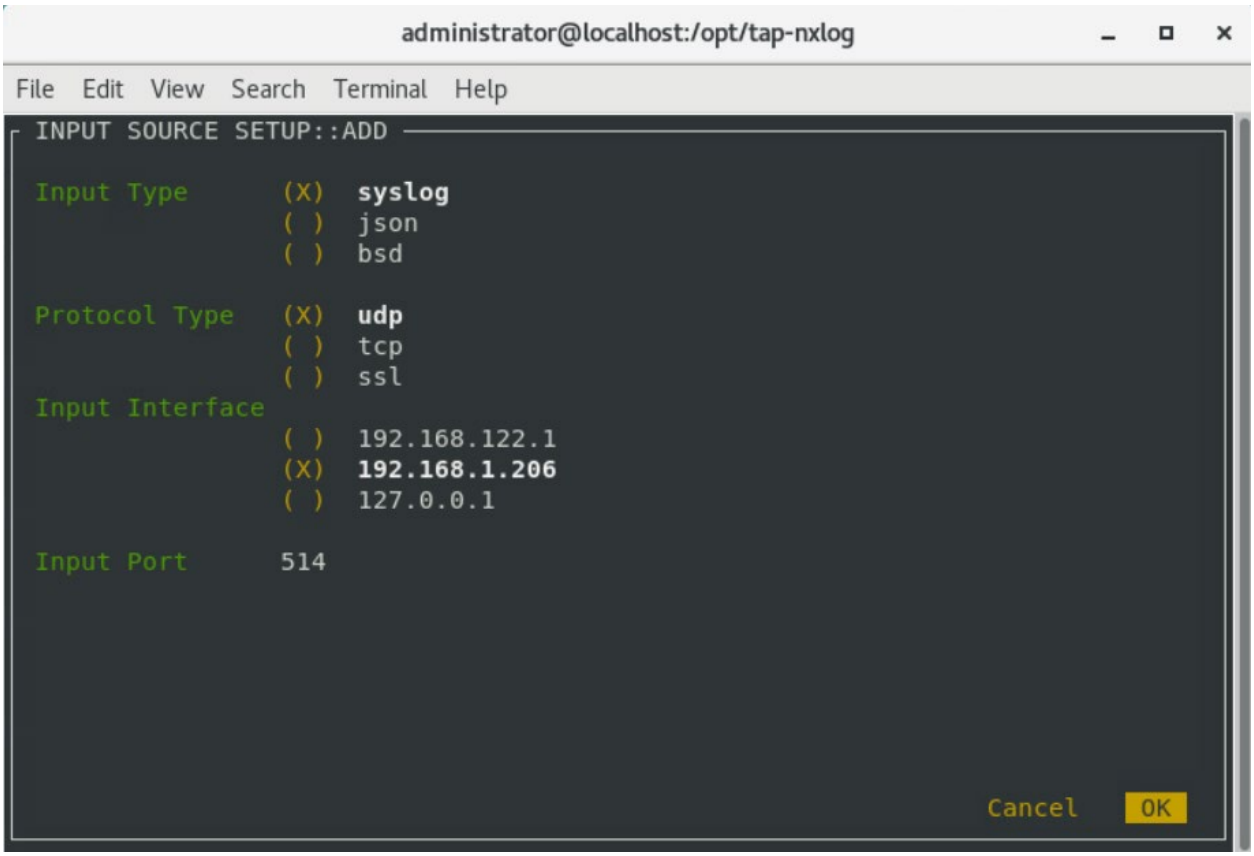
In the following section, Cisco Stealthwatch will be configured to forward logs to an on-premise Helix Communications Broker. Cisco Stealthwatch, as a network monitoring solution, can provide logs relevant to malicious network activity, potential data egress, as well as contextual information that can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

2.6.1 Configure the Helix Communications Broker

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

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

2. Select **Add Routes** and press **Enter**.
3. Select **syslog**.
4. Select **udp**.
5. Select the IP address of the network interface that should receive logs.
6. Enter 514 for the port.



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

8. Select **OK** and press **Enter**.

2.6.2 Configure Stealthwatch to Forward Events

1. Log on to the Stealthwatch Management Console web interface.

2. Navigate to **Configure** > **Response Management**.

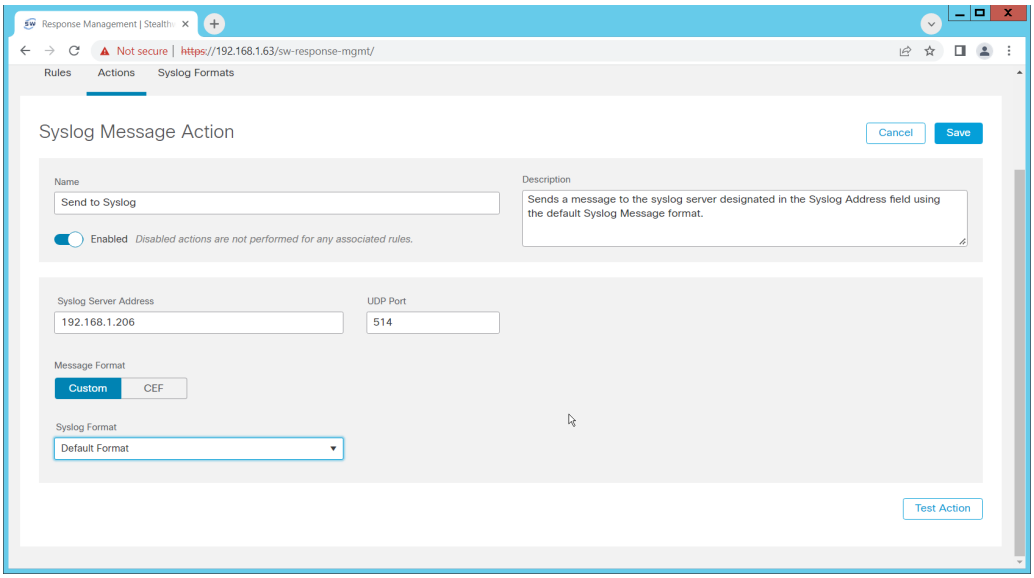
3. Click the **Actions** tab.

4. Click the **three dots** next to **Send to Syslog** and click **Edit**.

5. Set the action to **Enabled**.

6. Enter the address of the Helix Communications Broker.

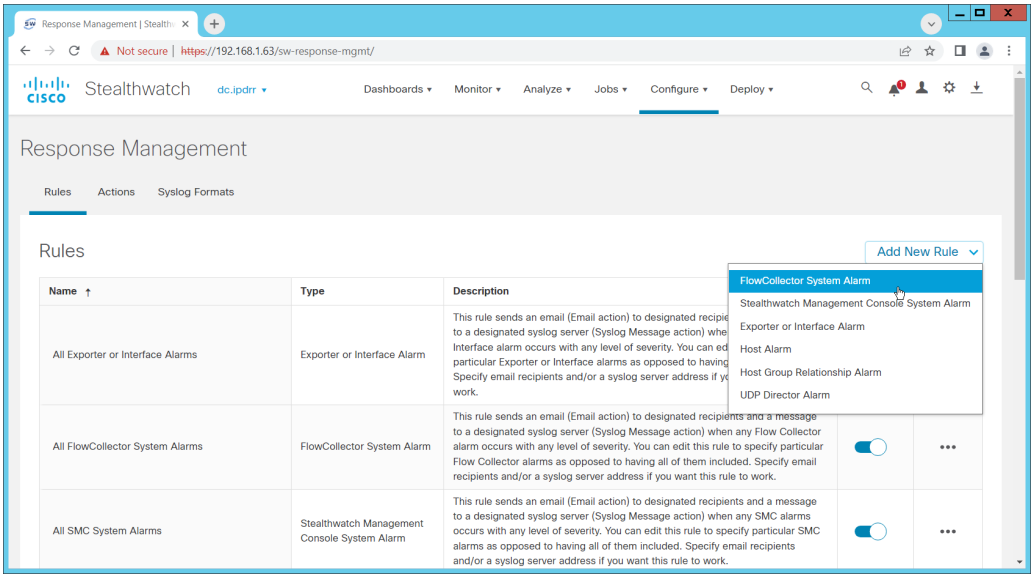
7. Enter the port that you selected earlier.



8. Click **Save**.

9. Click the **Rules** tab.

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

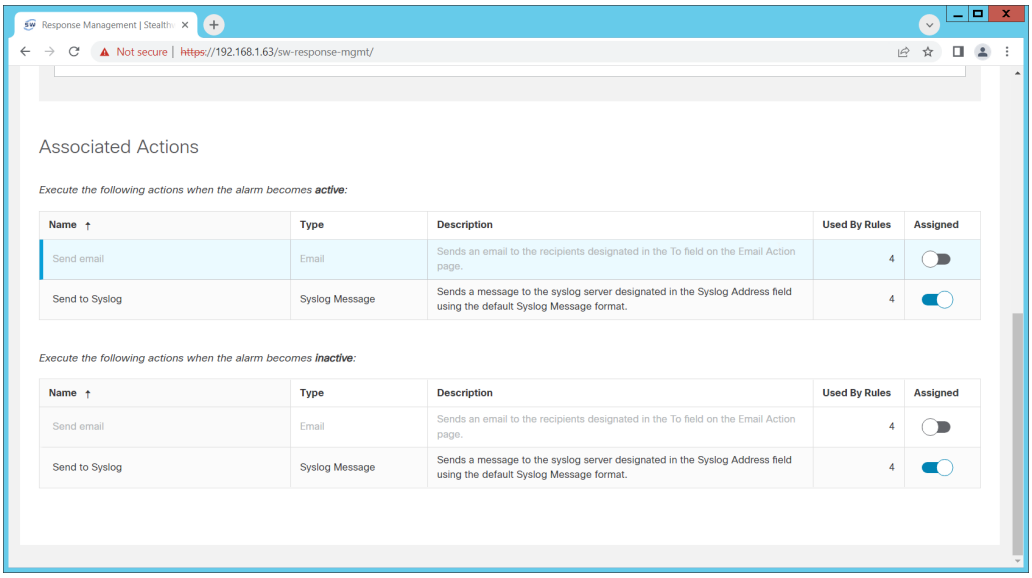


11. To create your own, click **Add New Rule**. For the purposes of this example, we select **FlowCollector System Alarm**.

12. Enter a name for the rule.

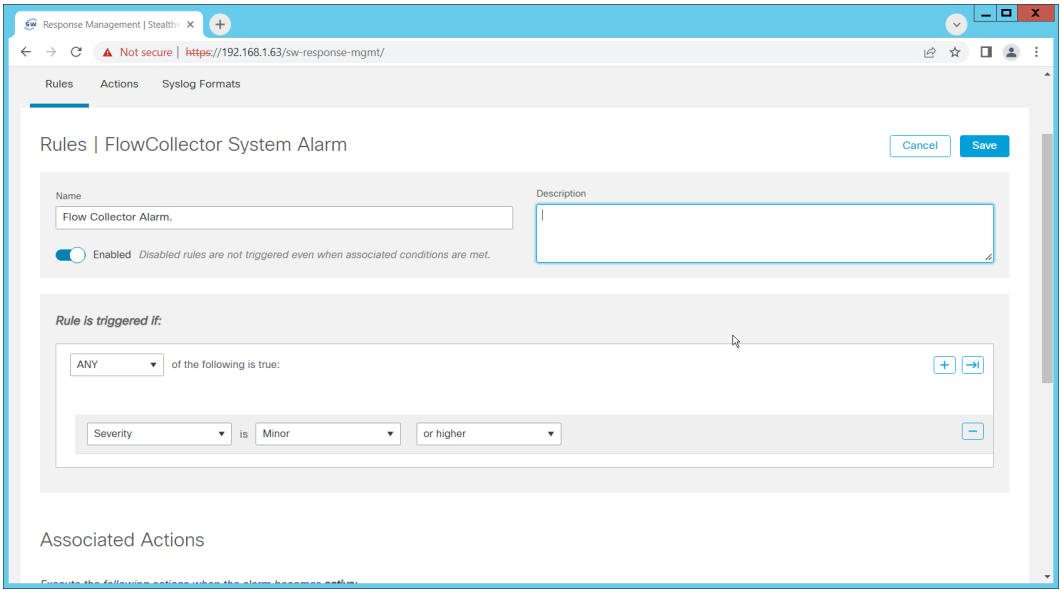
13. Ensure the rule is **Enabled**.

14. Click the **plus sign** under “Rule is triggered if”. You can select conditions for the rule to trigger, based on severity, processing time, and type.



15. Enable **Send to Syslog** in the **Associated Actions** section. You can enable syslog messages for when the alarm becomes active and inactive.

16. You can also configure email alerts through this interface to improve the response time for incidents (this is a separate **Action** that needs to be edited on the **Actions** tab).



17. Click **Save**.

2.7 Integration: FireEye Helix and PKWARE PKProtect

In the following section, PKWARE PKProtect, which has been configured to identify and encrypt sensitive data, will be configured to forward these events to FireEye Helix. In this build, PKProtect provides a data management capability that allows organizations to track data across an enterprise. As it is also providing encryption for this data, it provides important insight into sensitive data that is vulnerable to attack, as well as the ability to review, post-breach, which data may have been compromised in an

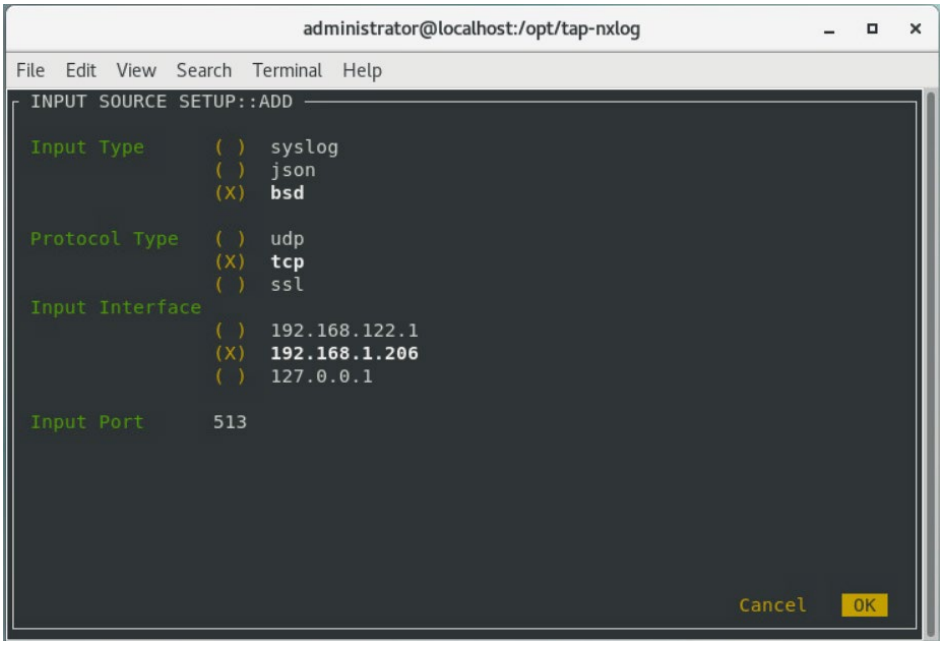
attack. An integration with the logging capability is useful for contextualizing information provided by other tools, generating alerts, and providing historical archives for reporting and compliance purposes. This section assumes the Helix Communications Broker has already been installed.

2.7.1 Configure the Helix Communications Broker

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

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

2. Select **Add Routes** and press **Enter**.
3. Select **bsd**.
4. Select **tcp**.
5. Select the IP address of the network interface that should receive logs.
6. Enter 513 for the port.



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

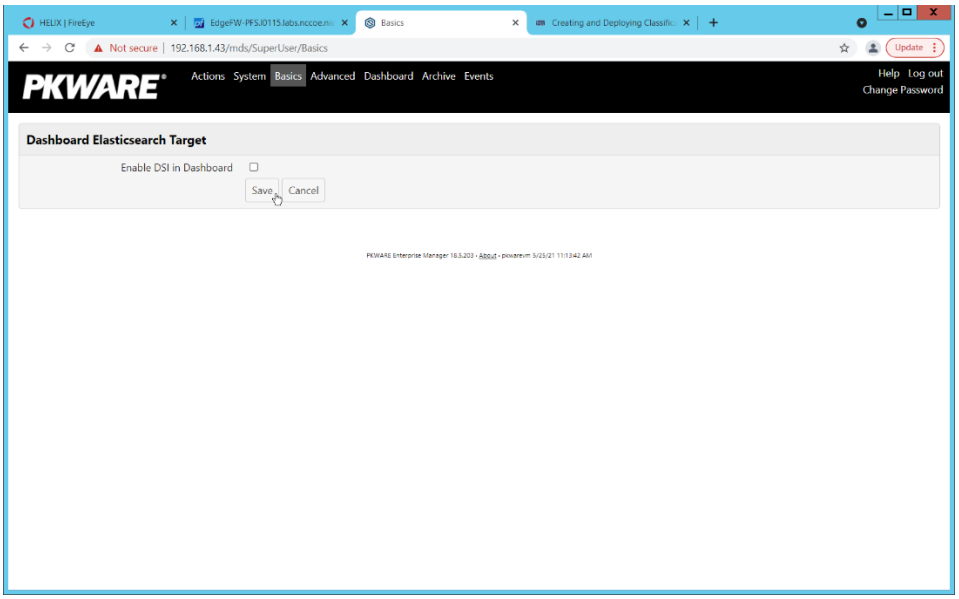
2.7.2 Configure PKWARE PKProtect to Forward Events

1. Navigate to the PKWARE PKProtect web portal.
2. Click the **Basics** link at the top of the page.
3. Scroll down to the **Data Security Intelligence** section.

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

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

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

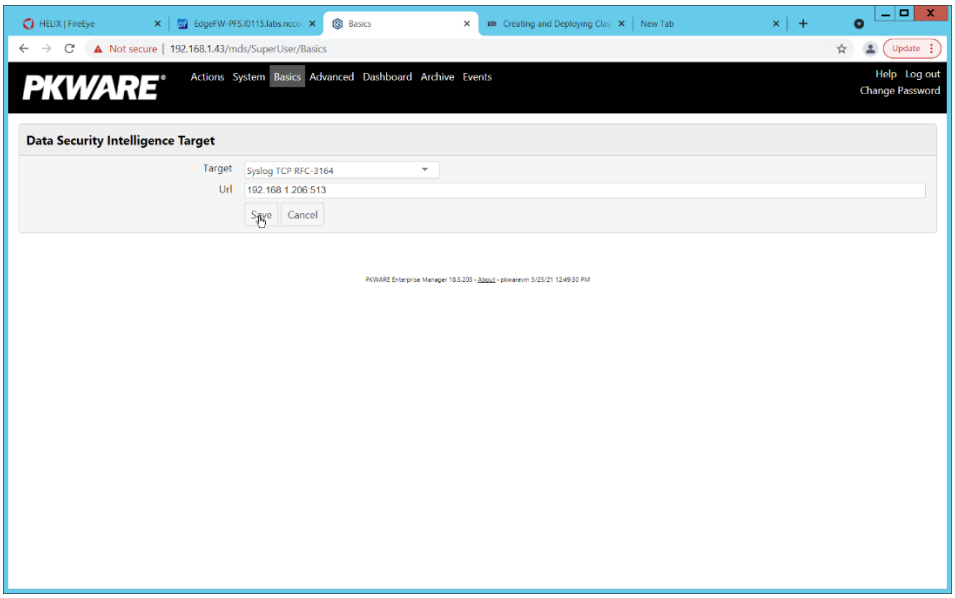


7. Click **Save**.

8. In the **Data Security Intelligence** section, click **Internal** next to **Target**.

9. Select **Syslog TCP RFC-3164** for **Target**.

10. Enter the URL and port of the Helix Communications Broker that was just configured.



11. Click **Save**.

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

2.8 Integration: FireEye Helix and Dispel

In this integration, we configure the collection of logs from Dispel, our network protection solution. Because Dispel controls access from users to enterprise systems it is important to have an overview of its actions through log collection and reporting. This was a bespoke integration performed by Dispel. Organizations should ensure that this integration is performed, and discussed with their Security Information and Event Management (SIEM) and Virtual Desktop Interface (VDI) vendors.

1. This integration has two primary components. The first, configuring the route, is done locally on the Dispel wicket. This can be done using the following commands. Ensure that you replace the <subnet> and the <gateway> such that the Dispel wicket can accurately route to the Helix Communications Broker.

   ```
   > config

   > set protocols static route <subnet> next-hop <gateway>

   > commit && save && exit
   ```

2. The second component is configured server-side and involves informing the Dispel wicket via config file the actual port and location of the Helix Communications Broker. Instructions are not included for this, as in this integration, it was necessary to perform this integration remotely via the Dispel team.

2.9 Integration: Dispel and Cisco DUO

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

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

Appendix A List of Acronyms

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