NIST SPECIAL PUBLICATION 1800-29

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

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

William Fisher
R. Eugene Craft
Michael Ekstrom
Julian Sexton
John Sweetnam

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-detect-respond-and-recover-data-breaches

NIST SPECIAL PUBLICATION 1800-29

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

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

William Fisher
National Cybersecurity Center of Excellence
NIST

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

FINAL

February 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST SPECIAL PUBLICATION 1800-29A

Data Confidentiality:

Detect, Respond to, and Recover from Data Breaches

Volume A:
Executive Summary

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

Executive Summary

CHALLENGE

An organization must protect its information from unauthorized access and disclosure. Data breaches large and small can have far-reaching operational, financial, and reputational impacts on an organization. In the event of a data breach, data confidentiality can be compromised via unauthorized exfiltration, leaking, or spills of data to unauthorized parties, including the general public.

It is essential for an organization to identify and protect assets to prevent breaches. And in the event a data breach occurs, it is essential that an organization be able to detect the ongoing breach themselves, as well as begin to execute a response and recovery plan that leverages security technology and controls.

BENEFITS

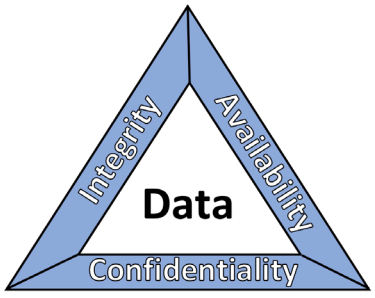
The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) developed this guide to help organizations implement strategies in response to data confidentiality attacks. This NIST Cybersecurity Practice Guide demonstrates how organizations can develop and implement appropriate actions to detect, respond and recover from a data confidentiality cybersecurity event. It includes numerous technology and security recommendations to improve your organization's cybersecurity posture.

This practice guide can help your organization:

- Detect losses of data confidentiality in your organization.
- Respond to data breach events using your organization's security architecture.
- Recover from a data breach in a manner that lessens monetary and reputational damage.

APPROACH

This publication is part of a series of projects that seek to provide guidance to improve an organization's data security in the context of the CIA triad. The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability. This practice guide focuses on data confidentiality: the property that data has not been disclosed in an unauthorized fashion. Data confidentiality concerns data in storage, during processing, and while in transit. (Note: These definitions are from NIST Special Publication (SP) 800-12 Rev 1, An Introduction to Information Security.)



This guide applies data confidentiality principles through the lens of the NIST Cybersecurity Framework version 1.1. Specifically this practice guide focuses on the latter three of those functions, informing organizations on how to **detect**, **respond** to, and **recover** from a data confidentiality attack, and manage data confidentiality risks. A complementary project and accompanying practice guide (SP1800-28) addresses data confidentiality through the lens of the principles of **identify** and **protect**.

The NCCoE developed and implemented an example solution that incorporates multiple systems working in concert to detect, respond to, and recover from data confidentiality cybersecurity events. The solution will demonstrate the ability to detect an ongoing data breach, as well as recommending technical and policy remediations against the same. This document highlights both the security and privacy characteristics of the example solution by considering common data security use cases an organization might seek to address and by enumerating problematic data actions that might impact privacy.

Collaborator	Security Capability or Component
Dispel	Network Protection
Cisco	Event Detection, User Access Control
FireEye	Logging
PKWARE	Data Protection

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. 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.

HOW TO USE THIS GUIDE

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

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-29A: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-29B: Approach, Architecture, and Security*

Characteristics, which describes what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-29C: How-To Guides*, which provide specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/data-security/dc-detect-identify-protect. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at ds-nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

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.

NIST SPECIAL PUBLICATION 1800-29B

Data Confidentiality:

Detect, Respond to, and Recover from Data Breaches

Volume B:
Approach, Architecture, and Security Characteristics

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.

National Institute of Standards and Technology Special Publication 1800-29B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-28B, 58 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 seeks to help organizations detect, respond, and recover from a data confidentiality attack.

KEYWORDS

asset management; cybersecurity framework; data breach; data confidentiality; data protection; detect; 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

Name	Organization
Jim Wyne	PKWARE
Spike Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Brian Johnson	The MITRE Corporation
Lauren Lusty	The MITRE Corproation
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
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

List of Tables

1 Summary

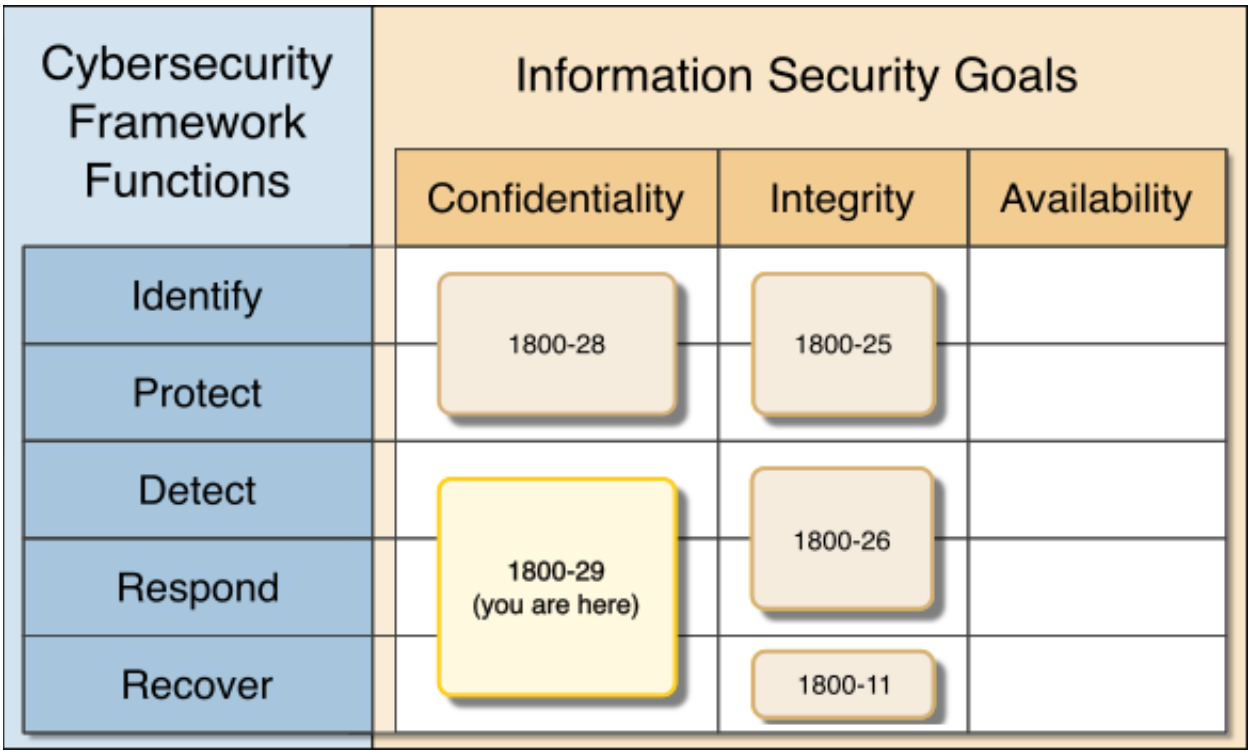
In our data-driven world, organizations must prioritize cybersecurity and privacy as part of their business risk management strategy. Specifically, data confidentiality remains a challenge as attacks against an organization's data can compromise emails, employee records, financial records, and customer information—impacting business operations, revenue, and reputation.

Confidentiality is officially defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[1] Data confidentiality makes sure that only the right users and systems have access to the right data. Ensuring data confidentiality should be a priority for any organization regardless of industry. A loss of data confidentiality can be of great impact to not just the company or organization, but also to the individual who have trusted the organization with their data.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) developed an example solution to address data security and privacy needs. This project fits within a larger series of Data Security projects that are organized by the elements of the Confidentiality, Integrity, Availability (CIA) triad, and the NIST Cybersecurity Framework's (CSF) Core Functions: Identify, Protect, Detect, Respond, and Recover.

Note: This project was initiated before the release of the DRAFT NIST CSF 2.0 and thus does not include the newly added GOVERN function. The DRAFT NIST CSF 2.0 defines Govern as "Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy". The govern function cuts across the other CSF functions. Though this document focuses on technical capabilities, it's intended that those capabilities would support an organizational governance function in managing data confidentiality attack risk.

Figure 1-1 Data Security Project Mapping



The goals of this NIST Cybersecurity Practice Guide are to assist organizations in detecting, responding to, and recovering from data confidentiality events. This guide will help organizations:

- Monitor the enterprise's user and data activity.
- Detect unauthorized data flows, user behavior, and data access.
- Report unauthorized activity with respect to users and data in transit, at rest, or in use to centralized monitoring and reporting software.
- Analyze the impact of unauthorized behavior and malicious behavior on the network or end points. Determine if a loss of data confidentiality is occurring or has occurred.
- Mitigate the impact of such losses of data confidentiality by facilitating an effective response to a data breach scenario.
- Contain the effects of a data breach so that more data is not exposed.
- Facilitate the recovery effort from data breaches by providing detailed information as to the scope and severity of the breach.
- Enumerate data flows and problematic data actions in line with the NIST Privacy Framework

In addition to the guidance provided in these documents, NIST has many resources available to help organizations detect, respond to and recover from data confidentiality attacks:

- NIST Special Publication 1800-25, *Identifying and Protecting Assets from Ransomware and Other Destructive Events* [2]
- NIST Special Publication 1800-26, *Detecting and Responding to Ransomware and Other Destructive Events* [3]
- NIST Special Publication 1800-11, *Recovering from Ransomware and other Destructive Events* [4]

- NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* [5]
- NIST Special Publication 800-46, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* [6]
- NIST Special Publication 1800-184, *Guide for Cybersecurity Event Recovery* [7]
- NIST Privacy Framework [8]
- NIST Cybersecurity Framework [9]
- NIST Interagency Report 8374, *Ransomware Risk Management: A Cybersecurity Framework Profile* [10]

1.1 Challenge

Fundamentally, data confidentiality is a challenge because all data exists to be accessible by some number of authorized people or systems. Data access only becomes a data breach when that access is by an unauthorized person or system. The quantity and diversity of an organization's data, the varying methods of data access (on-site versus remote, computer versus mobile device) and the potential for the compromise of valid user credentials all challenge an organization's ability to maintain the confidentiality of their data. NIST SP 1800-29 focuses on the Detect, Respond, and Recover functions of the NIST Cybersecurity Framework and addresses the challenges related to categorizing authorized and unauthorized data access. Once that ontology is developed, this document helps organizations address detecting, responding to, and recovering from a loss of data confidentiality.

Additional challenges arise when defining what it means to "respond to" or "recover from" a data breach. In the NCCoE's previous work on Data Integrity (1800-25, 1800-26, and 1800-11), it was possible to define recovery as a rollback of the compromised data to a point in time before it was altered. With respect to a loss of data confidentiality, there is no such process by which to "undo" the effects of such a loss—once digital data is in the hands of an unauthorized user, there is no guaranteed method by which to get all copies of the data back. This leaves an organization and the affected individuals with non-technical mitigations for the consequences of the breach (financial, reputational, etc.), as well as the ability of the organization to apply the lessons learned to technical improvements earlier in the timeline to prevent against future breaches.

1.2 Solution

The NCCoE developed this two-part solution to address considerations for both data security and data privacy to help organizations manage the risk of a data confidentiality attack. The work in 1800-28 addressed an organization's needs prior to a loss of data confidentiality (by focusing on the NIST CSF Functions of Identify and Protect) while this guide's focus is on the actions of an organization during and after a loss of data confidentiality (the remaining NIST CSF Functions of Detect, Respond, and Recover). The solution utilizes commercially available tools to provide certain relevant capabilities such as event detection, log correlation, incident response information, and credential management among others.

1.3 Benefits

Organizations can use this guide to help:

- Evaluate their data confidentiality concerns.

- Determine whether their data security needs align with the challenges described in these documents.
- Conduct a gap analysis to determine the distance between the organization's current state and desired state with respect to data confidentiality.
- Perform an assessment of the feasibility of implementing any number of these solutions.
- Determine a business continuity analysis to identify potential impacts on business operations as a result of a loss of data confidentiality.

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the data confidentiality capabilities described in this document. 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 **(you are here)**
- NIST SP 1800-29C: *How-To Guides* – instructions for building the example solution

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 this part of the guide, *NIST SP 1800-29B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.5, Risk Assessment, provides a description of 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 1800-29A*, with your leadership team members to help them understand the importance of adopting standards-based solutions to detect and respond to losses in data confidentiality.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-29C*, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create 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 detecting, responding to, and recovering 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 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.

2.1 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.

3 Approach

The NCCoE is developing a set of data confidentiality projects mapped to the five Functions of the NIST Cybersecurity Framework. This project centers on detecting, responding to, and recovering from potential threats to confidentiality. Our commercial collaboration partners have volunteered to provide the products for the example solution for the problems raised in each of our use cases. Through this

collaboration, our goal is to create actionable recommendations for organizations and individuals trying to solve data confidentiality issues.

3.1 Audience

The architecture of this project and accompanying documentation targets three distinct groups of readers. The first is those personally managing, implementing, installing and configuring IT security solutions for their organization. The walkthroughs of installation and configuration of the chosen commercial products In Volume C of this guide, as well as any of our notes on lessons learned, work to ease the challenge of implementing security best practices. This guide also serves as a starting point for those addressing these security issues for the first time, and a reference for experienced admins who want to do better.

The second group are those tasked with establishing broader security policies for their organizations. Reviewing the threats each organization needs to account for and their potential solutions allows for more robust and efficient security policy to be generated with greater ease.

The final group are those individuals responsible for the legal ramifications of breaches of confidentiality. Many organizations have legal obligations to protect the personal data or personally identifiable information they handle, and the ramifications for failing to at least adequately attempt to protect that data can have severe consequences for the privacy of individuals and follow on consequences for the organizations as a whole.

This guide will allow potential adopters to assess the feasibility of implementing data confidentiality best practices within the IT systems of their own organization.

3.2 Scope

This document provides guidance on detecting, responding to, and recovering from a loss of data confidentiality. Refer to Figure 1-1 to understand how this document fits within the larger set of NCCoE Data Security projects, as organized by the CIA triad and the functions of the NIST Cybersecurity Framework.

3.3 Assumptions

The technical solution developed at the NCCoE and represented in this guide does not incorporate the non-technical aspects of managing the confidentiality of an organization's data. The non-technical components could include (but are not limited to):

- applicable legal requirements based on pertinent jurisdictions
- corporate or other superseding policies relevant to confidentiality and privacy
- standard operating procedures in the event of a loss of data confidentiality
- public relations strategies

This project is guided by the following assumptions:

- The solution was developed in a laboratory environment and is limited in the size and scale of data

- Only a subset of products relevant to data confidentiality are included in this project; therefore, organizations should consider the guiding principles of this document when evaluating their organization's needs against the product landscape at the time of their IT implementation.

3.4 Privacy Considerations

Because privacy risks may arise as a result of a loss of confidentiality of data, this guide includes privacy considerations. This section gives a primer for why privacy is important to protect the relationship between privacy and cybersecurity risk, as well as NIST's approach to privacy risk assessment.

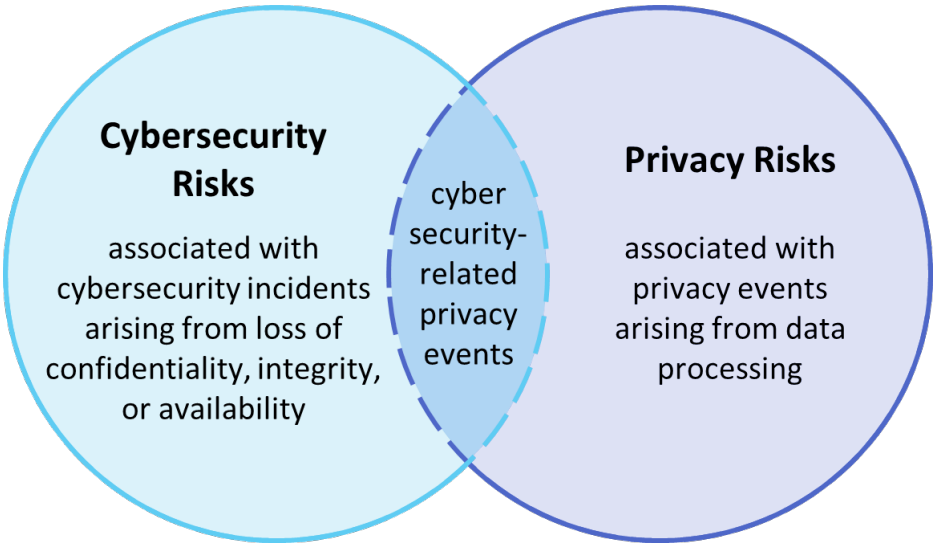
In today's digital landscape, consumers conduct much of their lives on the internet. Data processing, which includes any operations taken with data, including the collection, usage, storage, and sharing of data by organizations, can result in privacy problems for individuals. Privacy risks can evolve with changes in technology and associated data processing. How organizations treat privacy has a direct bearing on their perceived trustworthiness. Recognizing the evolving privacy impacts of technology on individuals, governments across the globe are working to address their concerns through new or updated laws and regulations.

Following an open and transparent development process, NIST published the NIST Privacy Framework, Version 1.0 to help organizations better identify and manage their privacy risks, build trust with customers and partners, and meet their compliance obligations. The Privacy Framework Core provides privacy outcomes that organizations may wish to achieve as part of a privacy risk management program. The Privacy Framework also discusses privacy engineering objectives that can be used to help organizations prioritize their privacy risk management activities. The privacy engineering objectives are:

- Predictability: Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system
- Manageability: Providing the capability for granular administration of data, including collection, alteration, deletion, and selective disclosure
- Disassociability: Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system

It is important for individuals and organizations to understand the relationship between cybersecurity and privacy. As noted in Section 1.2.1 of the *NIST Privacy Framework* [8], having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks. Figure 3-1 illustrates this relationship, showing that some privacy risks arise from cybersecurity risks, and some are unrelated to cybersecurity risks.

Figure 3-1 Cybersecurity and Privacy Risk Relationship



Though a data confidentially breach may lead to privacy problems for individuals, it is important to note that privacy risks can arise without a cybersecurity incident. For example, an organization might process data in ways that violates an individual's privacy without that data having been breached or compromised through a security incident. This type of issue can occur under a variety of scenarios, such as when data is stored for extended periods, beyond the need for which the information was initially collected.

Privacy risks arise from privacy events—the occurrence or potential occurrence of problematic data actions. The NIST Privacy Framework defines problematic data actions as data actions that may cause an adverse effect for individuals. Problematic data actions might arise by data processing simply for mission or business purposes. Privacy risk is the likelihood that individuals will experience problems resulting from data processing, and the impact should they occur [11]. As reflected in the overlap of Figure 3-1, analyzing these risks in parallel with cybersecurity risks can help organizations understand the full consequences of impacts of data confidentiality breaches. Section 5.3 demonstrates scenarios where privacy risks may arise and potential mitigations.

Based on the reference architecture, this build considered the data actions that potentially cause problematic data actions.

3.5 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* [12]—material that is available to the public. The Risk Management Framework (RMF) [13] guidance proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

3.5.1 Security Risk Assessment

Security risk assessments often discuss the consideration of threats to an information system. NIST SP 800-30 Revision 1 defines a threat as "[a]ny circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service". Threats are actions that may compromise a system's confidentiality, integrity, or availability [14]. Threats evolve, and an organization needs to perform its own analysis when evaluating threats and risks that the organization faces.

The following threats were considered during the development of the data confidentiality solution:

- exfiltration by malicious outsider actor
- exfiltration by malicious internal actor (privilege misuse)
- ransomware with threat to leak data
- non-malicious insider actor (accidental email)
- misplaced hardware

For a threat to be realized, a system, process or person must be vulnerable to a threat action. A vulnerability is a deficiency or weakness that a threat source may exploit, resulting in a threat event. Vulnerabilities may exist in a broader context. That is, they may be found in organizational governance structures, external relationships, and mission/business processes.

Organizations should consider the impact in the event that a data confidentiality breach occurs including potential decline in organizational trust and credibility affecting employees, customers, partners, stakeholders as well as financial impacts due to loss of proprietary or other sensitive information.

3.5.2 Privacy Risk Assessment

This build also incorporates privacy as part of the build risk assessment. It is important for organizations to address privacy risk as part of a comprehensive risk management process. The build utilized the NIST Privacy Framework [8] and Privacy Risk Assessment Methodology (PRAM) [15] to identify and address privacy risks.

As part of identifying privacy risks in this build, problematic data actions were correlated to observed privacy risks. In many cases, the security capabilities in this build will help mitigate privacy risks, but organizations should use caution to implement these capabilities in a way that does not introduce new privacy risks.

Section 5.3 discusses problematic data actions and privacy considerations for this build.

3.6 Technologies

Table 3-1 lists the technologies used in this project, and provides a mapping among the generic application term, the specific product used, and the security control(s) that the product provides. Refer to Table 6-1 for an explanation of the NIST Cybersecurity Framework Subcategory identifiers. Table 3-1 also provides the Privacy Framework Subcategory identifiers, which are explained in Appendix E.

Table 3-1 Products and Technologies

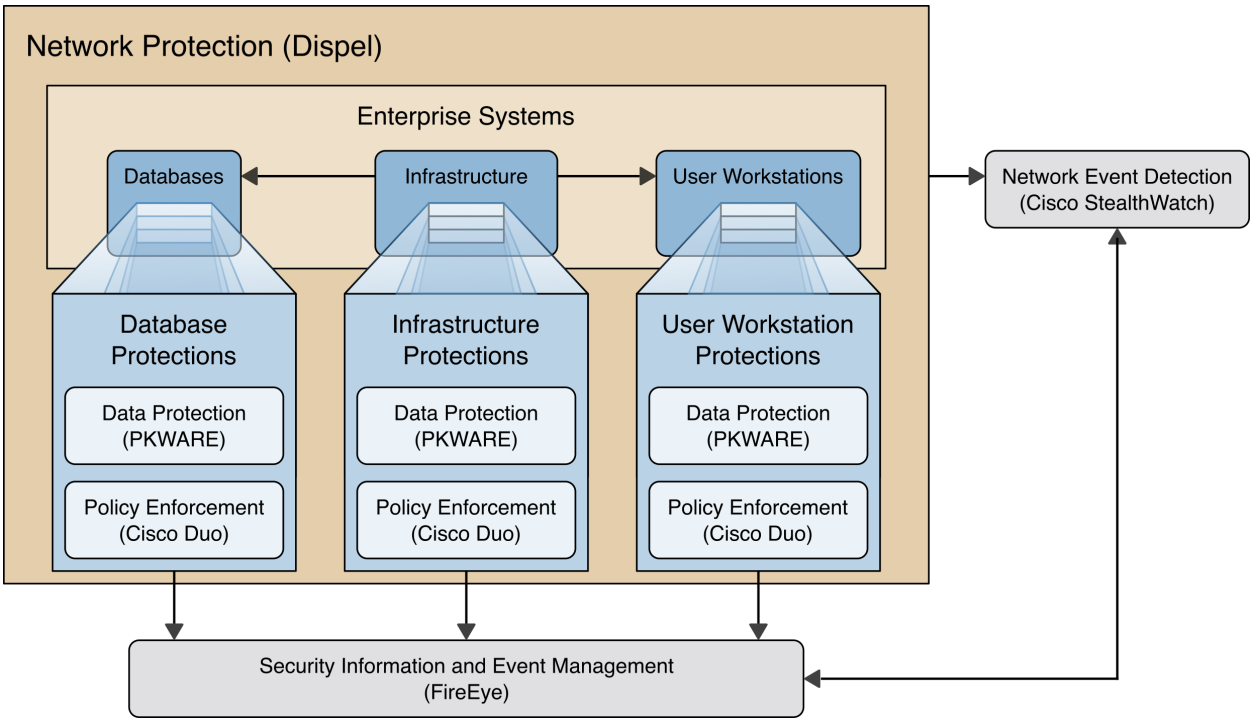
Component	Product	Capability	NIST Cybersecurity Framework Subcategories	NIST Privacy Framework Subcategories
File Detection and Monitoring	PKWARE PKProtect	• Logs data protection and access activity • Revokes and rotates breach-affected access and encryptions keys	RS.MI-2	CT.DM-P8, PR.AC-P1
Network Detection and Monitoring	Cisco Stealthwatch	• Detects threats and determine affected user, device, location, and other relevant information • Analyzes network traffic	DE.CM-1, DE.CM-3, DE.CM-4, DE.CM-7	PR.AC-P5, PR.PT-P3
Logging	FireEye Helix	• Provides aggregate view of entire environment • Enables incident response	DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, RS.RP-1, RS.CO-2, RS.AN-3	CT.DM-P8
User Access Control	Cisco DUO	• Revokes compromised credentials	RC.RP-1	PR.AC-P1, PR.AC-P6
Network Protection	Dispel	• Provides remote access to network	DE.AE-3, DE.CM-3, DE.CM-7, RS.MI-2	PR.AC-P3

4 Architecture

This section presents the high-level architecture and a set of capabilities used in our data confidentiality reference design to detect, respond, and recover from data confidentiality events.

4.1 Architecture Description

Figure 4-1 Data Confidentiality Detect, Respond, and Recover High-Level Architecture



Each of the capabilities implemented plays a role in mitigating data confidentiality attacks:

- **Data Protection** involves maintaining the confidentiality and integrity of proprietary data, even in the event of a security breach or outright theft.
- **Event Detection and Monitoring** 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** 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** 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** provides protection for security architecture and enterprise components, as well as providing additional network and authentication logging data for analysis.

These capabilities work together to detect malicious activity, respond appropriately, and aid in recovering both the system's security and any corrupted data. The data protection capability works to encrypt and manage encryption keys for the data. This data protection is critical as a line of defense against breaches; encryption ensures that data captured in a breach is effectively unusable by the

adversary. The monitoring capability analyzes network traffic to detect abnormal or malicious network activity and the user accounts affected by it. The event detection capability similarly detects unauthorized data access and other software related events which may be related to data breaches, such as the usage of USBs, printers, and email to transfer sensitive files. The anomalies detected by the event detection and monitoring capabilities can provide warnings of a potential breach, triggering responses which the organization has set in place.

The log collection, collation, and correlation capability collect data from other capabilities to provide administrators with an overview of organizational health and knowledge about potential and actual data breaches. This larger view of the entire network enables administrators to determine the extent of the damage to the organization, the status of the containment of the security breach, and whether the remnants of the security breach have been successfully removed. In combination with the access control capability, these can be used to revoke compromised user credentials, and restrict the access of uncompromised accounts related to the breach.

5 Security & Privacy Characteristic Analysis

The following section is intended to help organization understand the extent to which the project meets its objective of demonstrating technologies and capabilities to mitigate data confidentiality risk. To support this, we developed several scenarios which organizations may consider when conducting their security and privacy risk analysis. For each scenario we discuss how our architecture might help mitigate or limit security and privacy risks.

5.1 Assumptions and Limitations

The following analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses or risks
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

5.2 Security Scenarios

Our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. Each scenario lays out a potential cybersecurity event and discusses the responsibilities of an organization with respect to each event, and how the security capabilities of our architecture would help an organization address the Cybersecurity Framework functions of **Detecting, Responding** and **Recovering** to each proposed scenario.

NOTE: The below scenarios map to the DRAFT NIST CSF 2.0. For a mapping to the NIST CSF 1.1 please see Security Control Map in Appendix D.

5.2.1 Exfiltration of Encrypted Data

Table 5-1 Exfiltration of Encrypted Data Security Scenario

Description	An organization has unknowingly acquired a compromised machine from an outside source and has attached the machine to its trusted network. This machine periodically scans a certain part of the filesystem, which it has deemed to be potentially sensitive, and encrypts and uploads the contents to a malicious web host. Because the machine was assumed to be trusted due to human error, the delivery of this malware into the system is difficult to detect; it must be detected and stopped after it has already started running.
Associated DRAFT CSF 2.0 Subcategories	DE.AE-02, DE.AE-03, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, RS.MA-02, RS.AN-03, RS.CO-02, RS.CO-03, RS.MI-02
Organizational Response	In this scenario, the organization accepts an infected machine onto its network. As an example, this could be hardware ordered from a third-party vendor, potentially having been refurbished or modified before delivery to the organization. Because the organization connects the machine directly to the network, the acquisition of the malware happens immediately and without warning. It falls to the organization to detect any changes in the network caused by the malware. It must also understand the extent of the damage, to properly scale the response and recovery efforts.
Detect	The **Monitoring** capability is used to watch the network for anomalous traffic which may indicate a breach of data confidentiality. The tools being employed monitor all data transfers and distinguish between the unauthorized and authorized. The data gathered feeds into the **Logging** and **Reporting** capabilities, which enable response and recovery.
Respond	The **Reporting** capability is used to set events into motion once the **Monitoring** capability has alerted it to malicious activity. This will alert administrators to the issue while also triggering automated responses to prevent further damage to proprietary data.
Recover	The **Logging** capability provides a history of what data was access and exfiltrated, as knowledge of what precisely was taken will determine exactly what liability the organization holds and which affected parties will need to be notified.

5.2.2 Spear Phishing Campaign

Table 5-2 Spear Phishing Campaign Security Scenario

Description	An unknown user has successfully launched a spear phishing attack, and in the process retrieved an authorized user's login and password. This user has access to several of the organization's databases, allowing them to both view and manipulate the data contained within. This exposes proprietary data to theft and manipulation or deletion.

Associated DRAFT CSF 2.0 Subcategories	DE.AE-02, DE.AE-03, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, RS.MA-02, RS.AN-03, RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02
Organizational Response	This scenario illustrates the compromise of valid, privileged credentials through a spear phishing email. The user may report this themselves if they retroactively realize it was a phishing attack, or they may not. The organization will need to detect the compromised account and assess any unauthorized access or data exfiltration.
Detect	The **Network Monitoring** and **Logging** capabilities are used to watch for those anomalous behaviors most often associated with compromised accounts.
Respond	The **Mitigation** capability demonstrated in this project allows for rapid disabling of account privileges in the event of compromised credentials, preventing further access to additional sensitive data.
Recover	The **Logging** and **Reporting** capabilities provided a detailed picture of all sensitive data accessed by the compromised account, which will allow the organization to determine what liability it holds and what affected parties will need to be notified.

5.2.3 Ransomware

Table 5-3 Ransomware Security Scenario

Description	An employee of the company makes a mistake while entering the URL of their company's email provider. This mistake takes them to an identical login page, but it is hosted by a malicious actor. When they enter their credentials on the login page, the page records their credentials, and forwards them to the actual login page, as if the credentials were mistyped. The malicious actor later uses these credentials to login as the employee. They download and run a malicious ransomware executable as the user. The ransomware executable encrypts the files and notifies the company they must pay a ransom to access their data.
Associated DRAFT CSF 2.0 Subcategories	DE.AE-02, DE.AE-03, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, RS.MA-02, RS.AN-03, RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02
Organizational Response	In this scenario, an account at the organization has downloaded malware onto the system, which has begun encrypting sensitive data. The user may or may not report the attack, though there may be clues as to its existence - a user with account troubles and traffic going to a domain name very similar to the organization's domain might be enough to send up red flags if noticed. Regardless, the organization will need to deal with a privileged user account being used to download malware and hold the confidentiality of sensitive files ransom.
Detect	The **Monitoring** capability for this scenario includes network monitoring, which can detect unauthorized data exfiltration out of the network and any irregular access or changes to existing data. Any exfiltration or data encryption actions would also be included in logs forwarded to the tools used for **Reporting** and **Logging** capabilities.

Respond	The **Mitigation** capability for this scenario will allow for rapid disabling and secure re-enabling of compromised accounts once the relevant member accounts are detected. The **Reporting** capability is designed to quickly notify security teams of necessary actions, such as isolating the system from the network and securing any data not yet attacked by the ransomware.
Recover	The scenario build doesn't possess any technical capabilities for literal recovery of the stolen data, as the scenario predicates the data has already been successfully stolen, but the **Logging** capabilities should allow a detailed review of what was taken. This will allow for post-incident review of security flaws and notification of anyone inside or outside the organization affected by the security breach.

5.2.4 Accidental Email

Table 5-4 Accidental Email Security Scenario

Description	A user of the organization accidentally cc's an individual on an email. This email has an attachment containing proprietary information which the cc'd individual is not cleared for. The individual copied on the email is considered a disgruntled employee, and when he sees this email, immediately downloads and saves these files.
Associated DRAFT CSF 2.0 Subcategories	DE.AE-02, DE.AE-03, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, RS.MA-02, RS.AN-03, RS.CO-02, RS.MI-02
Organizational Response	In the event of an accidental information leak via email, it is not unlikely that the event will be reported. Since there are multiple parties involved who are not malicious, it is possible that one of them will report the incident. Regardless of whether it is reported, however, the organization should be able to track the transfer of sensitive data to the unauthorized employee's system, and also prevent that employee from reading it.
Detect	The **Monitoring** and **Event Detection** capability watches over network traffic, which includes scanning emails for sensitive content and its intended recipients.
Respond	The **Mitigation** capability of the scenario may block any uncleared individuals from seeing sensitive information in the accidentally sent emails, or even remove it automatically from uncleared systems on the network. The **Reporting** capability is designed to quickly notify security teams so they can attempt to contain the data exposed through the email.
Recover	As the scenario build should prevent any information from being leaked due to an uncleared email receiving sensitive information, there are no significant capabilities being used for recovery of proprietary data. However, the **Logging** and **Reporting** capabilities should allow for all organization members involved in the incident to be notified of their roles, and the aggregation of data regarding the incident should alert the organization if additional training on the distribution of proprietary data is necessary.

5.2.5 Lost Laptop

Table 5-5 Lost Laptop Security Scenario

Description	A user has lost their work laptop, which contains proprietary information. It is unknown if the laptop was targeted for its data and access credentials by a malicious actor, or if the incident was an unfortunate accident. For the purposes of this scenario, we assume the user of the laptop has reported the missing system on their own.
Associated DRAFT CSF 2.0 Subcategories	DE.CM-03, DE.CM-09, DE.AE-06, RS.MA-01, RS.AN-03, RS.AN-08, RS.CO-2
Organizational Response	In the event of a lost laptop, it is likely that the loss will be reported by the user, as the user will directly lose their ability to work. The organization must determine the data that was on the laptop, the security posture of the laptop, and the access the laptop provided to the organization's network, so that the loss can be accurately assessed, and further data loss can be prevented.
Detect	In many cases, the user will need to report their own laptop lost or stolen. While the **Logging** and **Monitoring** components can identify if the laptop is a security risk by verifying if the laptop attempts to connect to the network, it may be impossible to detect whether the data on the laptop has been accessed once network connectivity is lost. The **Logging** and **Reporting** capabilities create a record that can detect if data has been inappropriately accessed from laptops that are reported missing, based on user logins and activity.
Respond	The **Mitigation** capability of this scenario should allow for remote wiping of proprietary data from laptops, should they attempt to reconnect to the organization's network. The **Reporting** capability is designed to quickly notify security teams so they can flag the laptop as missing and assess from backups what data is exposed.
Recover	This scenario build does not contain the capability for physical recovery of lost laptops. However, **Logging** and **Reporting** capabilities can determine what data was on the lost laptop, and the individuals who might be affected by the potential exposure of the laptop's contents.

5.2.6 Privilege Misuse

Table 5-6 Privilege Misuse Security Scenario

Description	A malicious insider navigates to one of the organization's shared drives, and finds sensitive information stored there. Looking to sell this information to competitors, the insider copies the information to his personal USB drive. The insider also prints these files.
Associated DRAFT CSF 2.0 Subcategories	DE.CM-01, DE.CM-03, DE.CM-09, DE.AE-02, DE.AE-03, DE.AE-04, RS.MA-01, RS,MA-05, RS.AN-03, RS.CO-2, RS.CO-3, RS.MI-01, RC.CO-3, RC.CO-4

Organizational Response	It is unlikely that a malicious insider will advertise their misdoings - it falls to the organization to discover the insider behavior and protect assets from them. Through proper access control and encryption of sensitive files, organizations can hinder the insider's attempt to exfiltrate useful data. It is unlikely that an organization will be able to completely stop a determined insider through technical means, however; organizations should use the technical capabilities they have to limit the exfiltration, while also gathering information about the extent of the loss to aid in the pursuit of legal resolutions to the incident.
Detect	The **Event Detection** capability of the scenario is designed to watch for users accessing data they are not authorized for, the insertion of USB drives, and even the activation of printers.
Respond	The **Reporting** capability, combined with **Event Detection**, allows for security administrators to be quickly notified of potentially malicious actions. They can then respond by utilizing the **Mitigation** capability to restrict **User Access Controls** for any suspected insider accounts. **Mitigation** capabilities also exist to restrict copying and printing functionality.
Recover	The **Logging** capability in this scenario tracks user access to sensitive data, allowing for a full accounting of potentially compromised proprietary data.

5.2.7 Eavesdropping

Table 5-7 Eavesdropping Security Scenario

Description	A malicious outsider has gained access to the network traffic of the organization. They possess the capability to intercept and hijack internal communications via a man-in-the-middle attack. A user begins uploading a sensitive proposal for a new project. The malicious outsider can intercept and view these files.
Associated DRAFT CSF 2.0 Subcategories	DE.CM-01, DE.CM-03, DE.CM-09, DE.AE-02, DE.AE-03, DE.AE-04, RS.MA-01, RS,MA-05, RS.AN-03, RS.CO-2, RS.CO-3, RS.MI-01, RS.MI-02, RC.RP-01, RC.CO-3, RC.CO-4
Organizational Response	In this scenario, an organization will likely be able to see the introduction of a new device on the network. In this example, a user's sensitive upload is stolen while it is in transit. The user may see warnings about HTTPS or invalid certificates due to the nature of the attack, and the organization may notice anomalous traffic going through the new device on the network. The organization is responsible for identifying the new device as malicious, protecting data intercepted by it through encryption, and mitigating its ability to communicate with trusted enterprise machines.
Detect	The **Event Detection** and **Monitoring** capabilities of this scenario provide the means to detect and track anomalous network activity, specifically if the flow of communication is following anomalous patterns or routing through unnecessary systems. The **Logging** capability would also assist in identifying the source of the leak.

Respond	If the activities of the malicious host are allowed to continue, further loss of data can occur. Because of this, it is important to stop the interception of data quickly. In the event that the attacker is in the building, or even reading the data themselves as they intercept it, swift mitigation of the leak is necessary. Through the **Mitigation** component, we can contain or disconnect the malicious host from the network, to learn more information about it and prevent the leak. This can happen automatically or manually, depending on the reliability of the anomaly detection software.
Recover	The **Logging** and **Reporting** capabilities allow for the full accounting of the traffic and data the man-in-the-middle system touched before its detection and removal from the network, allowing for the notification of all affected parties.

5.3 Privacy Scenarios

The following section describes scenarios an organization may consider when conducting their privacy risk assessment. Based on the reference architecture used in this project each scenario is examined for data actions that give rise to potential privacy problems for individuals. Each table documents problematic data actions taken from the NIST Catalogue of Problematic Data Actions and Problems [16], and lists privacy mitigations mapped to the NIST Privacy Framework [8]. For the privacy risks analyzed, consideration was given to how the data is processed. The specific privacy risks found within the scenarios are derived from the architecture components and the data flows used in this build, but to the extent possible, generalized for organizations using similar components and capabilities.

Organizations may collect information affecting privacy when implementing cybersecurity or privacy-based controls. For example, an organization might implement multi-factor authentication (MFA) using information such as a mobile phone number. Even though collecting this information helps to protect systems and data by supporting capabilities like non-repudiation and system auditing, it may also generate privacy risks.

When implementing cybersecurity or privacy-based controls, organizations should consider the benefit a user realizes, both from the use of a service and the securing of that service before processing information affecting privacy. This benefit can be weighed against the risk posed to both individuals and the organization should a privacy event occur.

For example, using the MFA example mentioned above, users may feel compelled to provide information affecting privacy, such as their personal phone number for SMS (short messaging service) authentication, to gain access to systems or services. However, if the user is accessing publicly-available information, the risk of the misuse of information from collecting personal phone numbers may be greater than the security benefit for protecting the low-sensitivity information. Additionally, if given the option, users may elect to use alternative authentication methods that are less privacy-invasive, such as using a work phone number over a personal number or a hardware MFA authenticator over SMS authentication. The NIST Privacy Risk Assessment Methodology (PRAM)refers to this problematic data action, where the user is compelled to provide information disproportionate to the purpose or outcome of the transaction, as induced disclosure.

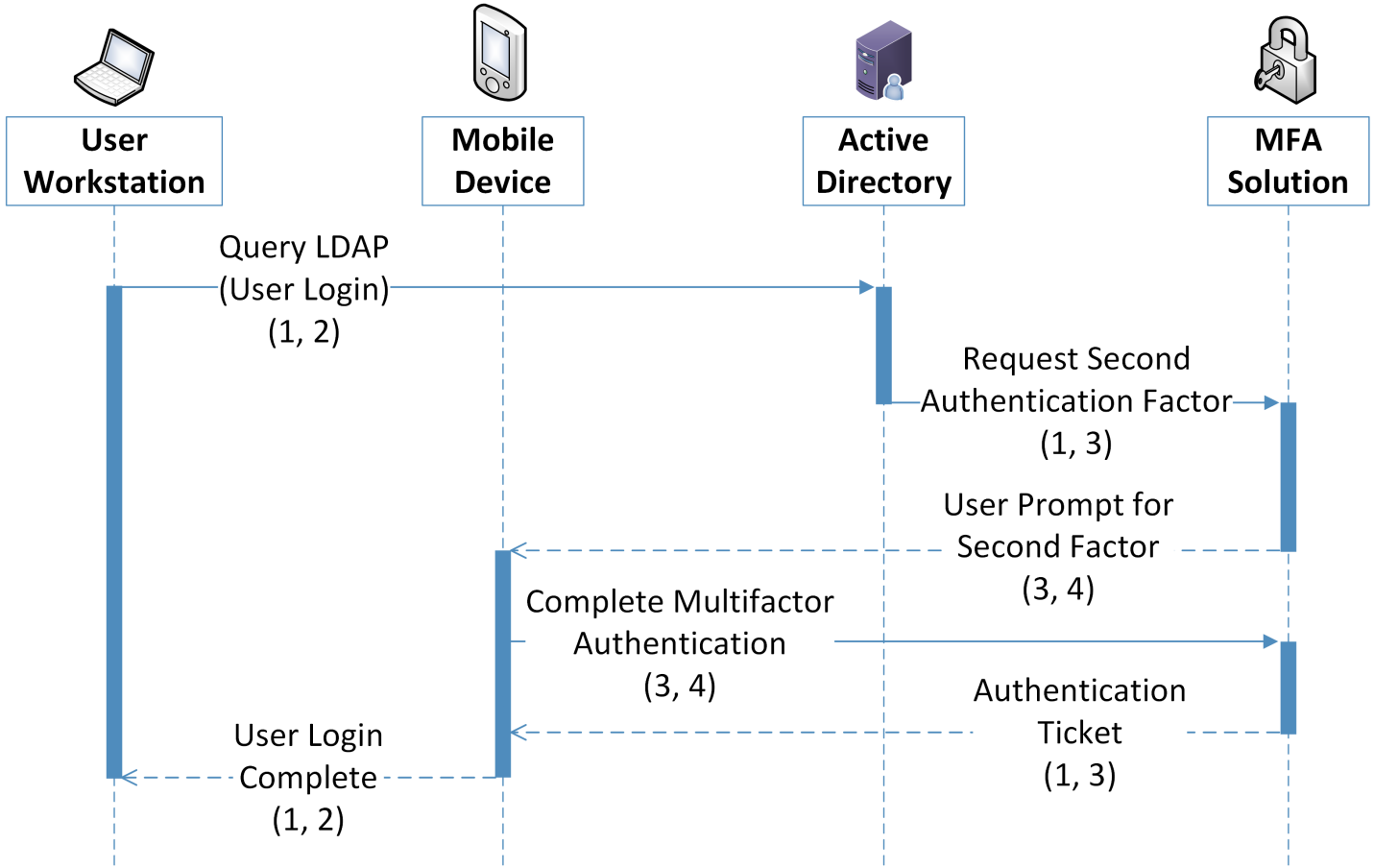
Organizations should consider these types of risks as they design and implement systems. As demonstrated in the scenarios below, risk mitigations should be implemented within the design to limit privacy risks. These privacy risk mitigations might include the following, among others:

- Understand where and how information is processed, including collection practices and system components that store and transmit this information (data flows and mapping)
- Understand the risks and benefits of collecting different data elements to determine if it should not be collected
- Keep data only as long as needed for its function and destroy or de-identify it otherwise using proper data lifecycle management practices and in accordance with applicable laws and policies
- Keep personal data segregated in a different repository, when practicable
- Encrypt data at rest, in transit, and in use
- Use role-based access controls
- Consider what measures should be taken to address predictability and manageability before deciding whether data can be used beyond its initial expected and agreed upon use
- Implement privacy-enhancing technologies to increase disassociability while retaining confidentiality and the capability to process data for mission or business purposes

5.3.1 User Login with Multifactor Authentication

Phishing-resistant multifactor MFA is a security best practice. The architecture recommends the use of a password, pin or biometric with an asymmetric cryptographic key for authentication. However, it is common practice for organizations to offer a variety of MFA solutions. Some MFA solutions, such as biometrics or authenticating with user-owned mobile devices, might introduce privacy risks.

Figure 5-1 Multifactor Authentication Data Flow Diagram



Data Key

1. Username
2. Client IP Address
3. Transaction Identifier
4. Mobile device information (Cellular number)

Table 5-8 User Login With Multifactor Authentication Data Actions

Data Type	Data Action	Examples of Privacy Considerations
Username	Username is stored by the user workstation, and transferred across the authentication process to help identify the transaction.	Usernames are unique to an individual and potentially contain identifiable information such as user's first and last names
Client IP (internet protocol) Address	The client IP address is stored by the user workstation, and transferred as part of communications where it is an endpoint.	IP addresses can be easily linkable to an individual or their device, allow tracking activities across multiple systems or services, or used to derive other information such as user's general location
Transaction Identifier	The transaction identifier is generated by active directory and transferred to the MFA solution and the mobile device.	Cross-device identifiers for a transaction can be used to re-identify information that was otherwise de-identified, such as connections between a user's name and their cellular phone number.
Mobile device information	The mobile device information is stored by the MFA solution and the mobile device and transferred as a part of the communication between the mobile device and MFA solution.	Mobile device information used in certain MFA transactions, such as phone numbers, identify individuals and their device. Furthermore, information about a user's mobile device, such as device type and version, can be used to infer privacy-impacting information such as spending habits and other behaviors.

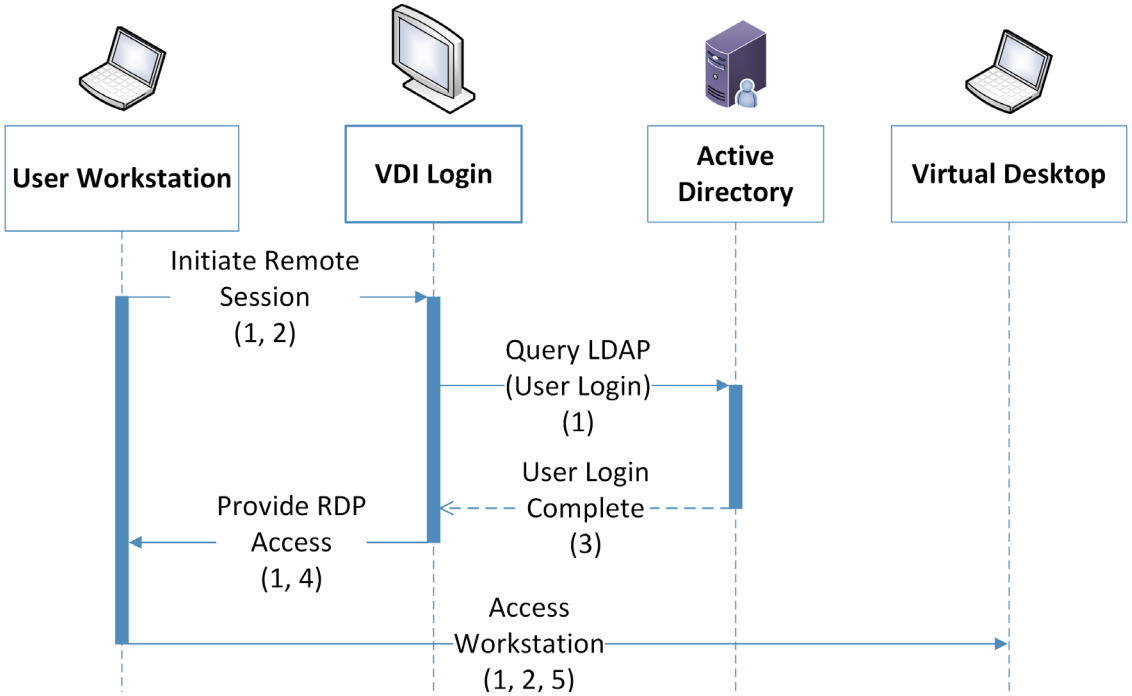
Table 5-9 User Login with Multifactor Authentication Problematic Data Action

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
User authentication may use a personally or organizationally owned mobile device as an authenticator.	Users non-work activity may be tracked by an organization.	**Context:** Users may not want to provide personal information, including phone number and location information, but may feel compelled to meet organizational security requirements. Tracking within the work environment or even outside the work environment could be disproportionate to the security needs leading to unanticipated revelations about user activities or degradation of the dignity or autonomy of users. **Problematic Data Action:** Surveillance, Unanticipated Revelation, Induced Disclosure **Problem:** Loss of Autonomy: Users have no control over what information is shared in this scheme. Users may not feel comfortable using their own personal information as a security feature for an organizational service. Loss of Trust: Users may not feel comfortable with their personal phone numbers and device information being shared with third-party applications and Software as a Service providers.	**Predictability: Organizations should inform** users of information that processed by login tools and viewed by administrators, such as through privacy notices when devices are enrolled. System administrators should have limited access to user authentication information. **Manageability**: Organizations that leverage user's personal devices for user login processes should consider tools that give the users options for registering different types of authenticators, including those that do not use personal devices and information. In this build, DUO offers a variety of authentication options, such as a hardware-based authenticator. Organizations should be auditing tools to determine what information they are using and collecting as well as who is accessing and using it. **Disassociability:** Organizations should explore capabilities and configurations that allow for the de-identification of phone numbers and other personal information, such as the capability to replace a phone-number with placeholder text or privacy-enhancing cryptographic techniques to limit the tracking of users.

5.3.2 Authentication to Virtual Desktop Interface Solution

The reference architecture in this document demonstrates a Virtual Desktop Interface (VDI) solution to facilitate secure access to organizational resources and data. Organizations may allow users' personal devices to access corporate resources using the VDI solution. Organizations should consider the privacy risk of installing VDI software on personally owned devices, information revealed by the VDI protocol, and monitoring of user activity while in the virtual environment.

Figure 5-2 Virtual Desktop Interface Data Flow Diagram



Data Key
1. Username
2. Client IP address
3. Token identifier
4. One-time password
5. Client time zone, computer name

Table 5-10 Virtual Desktop Interface Data Actions

Data Type	Data Action	Examples of Privacy Considerations
Username	The username is stored by the user workstation and active directory. It is transferred as part of the authentication process.	Usernames potentially contain inferable PII such as user's first and last names
Client IP Address	The Client IP Address is stored on the user workstation, and transferred as part of transactions and connections it generates.	IP addresses can be used to derive PII such as user's general location
Token Identifier	A Token Identifier is generated by Active Directory in support of the authentication process, and transferred to the VDI.	Token identifiers can be used to re-identify other information affecting privacy that occur as part of transactions.
Client Time Zone	The Client Time Zone is stored by the user workstation and transferred as part of an RDP (remote desktop protocol) connection to the virtual desktop.	When combined with IP addresses, Client Time Zones provide greater certainty about a user's location.
Client Computer Name	The Client Computer Name is stored by the user workstation and transferred as part of an RDP connection to the virtual desktop.	Client Computer Name can be easily linkable to an individual, allow tracking activities across multiple systems and services, or used to derive other information, such as names and device locations

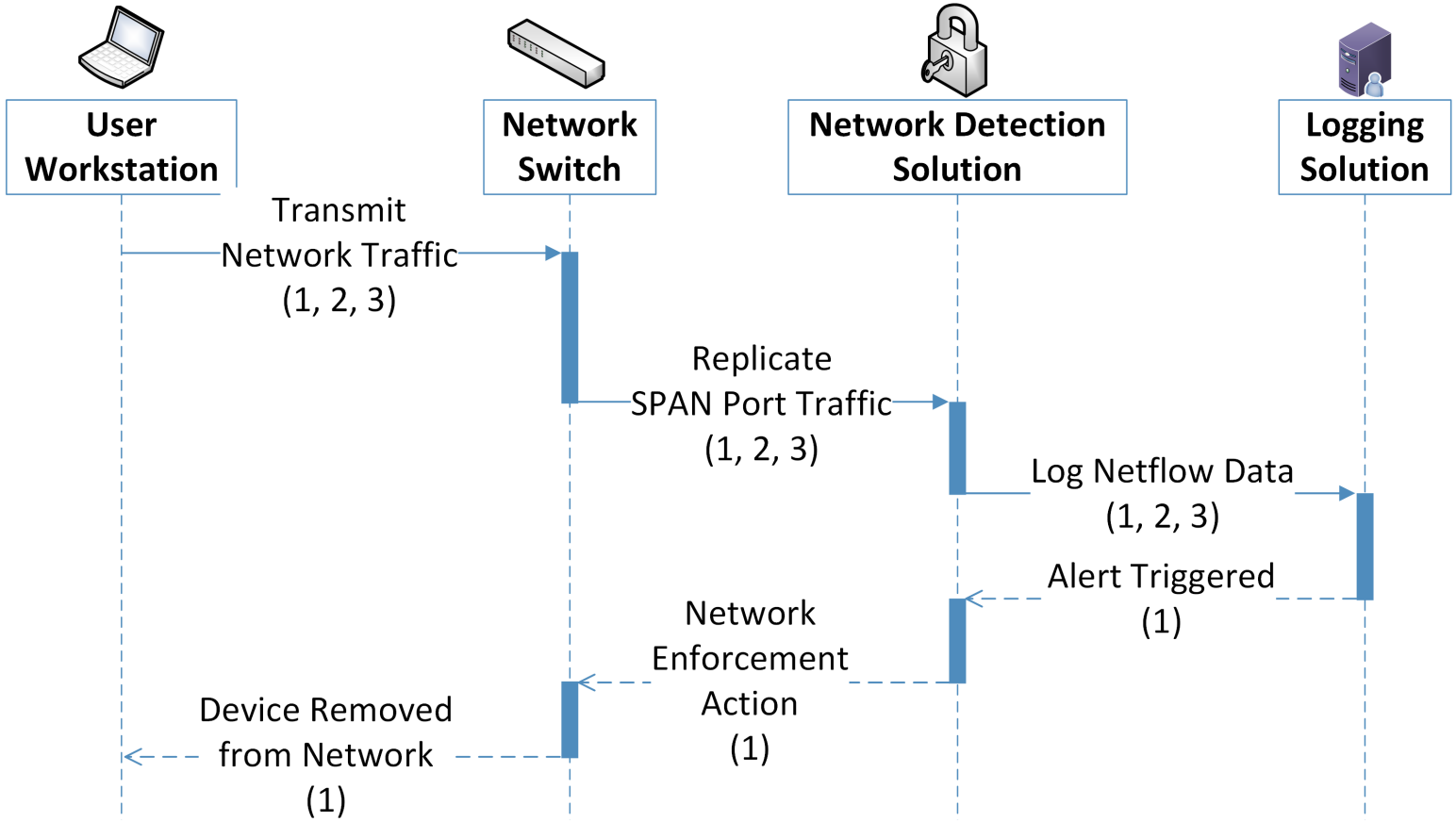
Table 5-11 Virtual Desktop Interface Problematic Data Actions

Scenarios	Examples of Privacy Risk	Problematic Data Actions	Privacy Mitigations
User logs into a Virtual Desktop Interface solution from a personally or organizationally owned device.	Information that can be associated with the user, such as their device information or location, may be transmitted to security tools as part of the authentication process. This information could result in tracking a user's non-work activity or exposing a user's non-work related information.	**Context:** Users may use a variety of devices to connect to central login platforms, including personally owned devices. Users operating under a BYOD or remote work scheme may not expect that certain data from their personal devices is shared with the organization. This can include their location and operating hours. Organizations can choose to use less identifiable information for a Client Computer Name (e.g., an asset tag number), but do not have control over how users name the personal devices they may use to authenticate. **Problematic Data Action:** Surveillance, Unanticipated Revelation **Problem:** Loss of Trust. Users may not feel comfortable with this information being shared with their employer or third-party applications. Dignity Loss. Users may have information, such as their physical location and work hours, revealed to organizations in an undesired or unexpected fashion.	**Predictability**: Users should be informed of information that is viewed and collected by login tools such as Dispel, such as through a login banner. Use privacy enhancing technologies and techniques like data minimization, encryption, obfuscation, anonymization, data minimization, and pseudonymization, among others. **Manageability:** Organizations that include user's personal devices in day-to-day operation should audit tools to determine what information they are using and collecting. **Confidentiality**: Organizations should mandate strict access control for the management and configuration of user login services, such as with MFA. **Availability:** Organizations that utilize central login platforms as their entry should consider the robustness of their platforms and systems. A loss of access to these systems can lead to an inability for users to access their data.

5.3.3 Monitoring by Network Detection Solution

Network detection solutions monitor network traffic to identify network patterns that may indicate malicious or harmful activity on a system or network. As part of this monitoring, network data may be duplicated, sent to third party applications or centralized. The transmission and use of this data for network monitoring may reveal more about users than necessary for security purposes, which raises privacy risk.

Figure 5-3 Network Detection Data Flow Diagram



Data Key

1. Client IP Address
2. User network metadata (Target IP address, Session information)
3. User network traffic content

Table 5-12 Network Detection Data Actions

Data Type	Data Action	Examples of Privacy Considerations
Client IP Address	IP Addresses are stored on the User Workstation and Logging Solution, and transferred between the User Workstation, network infrastructure, Network Detection Solution, and the Logging Solution.	IP addresses can be used to derive a user's location.
Network metadata	Network metadata is generated on the User Workstation and is transferred to the network infrastructure, the Network Detection Solution, and the Logging Solution. It is stored by the Logging Solution.	Network metadata can contain information that can be used to derive location or as a common identifier to re-identify previously de-identified information.
Network traffic content	Network traffic content is generated on the User Workstation and is transferred to the network infrastructure, the Network Detection Solution, and the Logging Solution. It is stored by the Logging Solution.	Network traffic content can contain a variety of information or inferences about the individual, such as health or financial data.

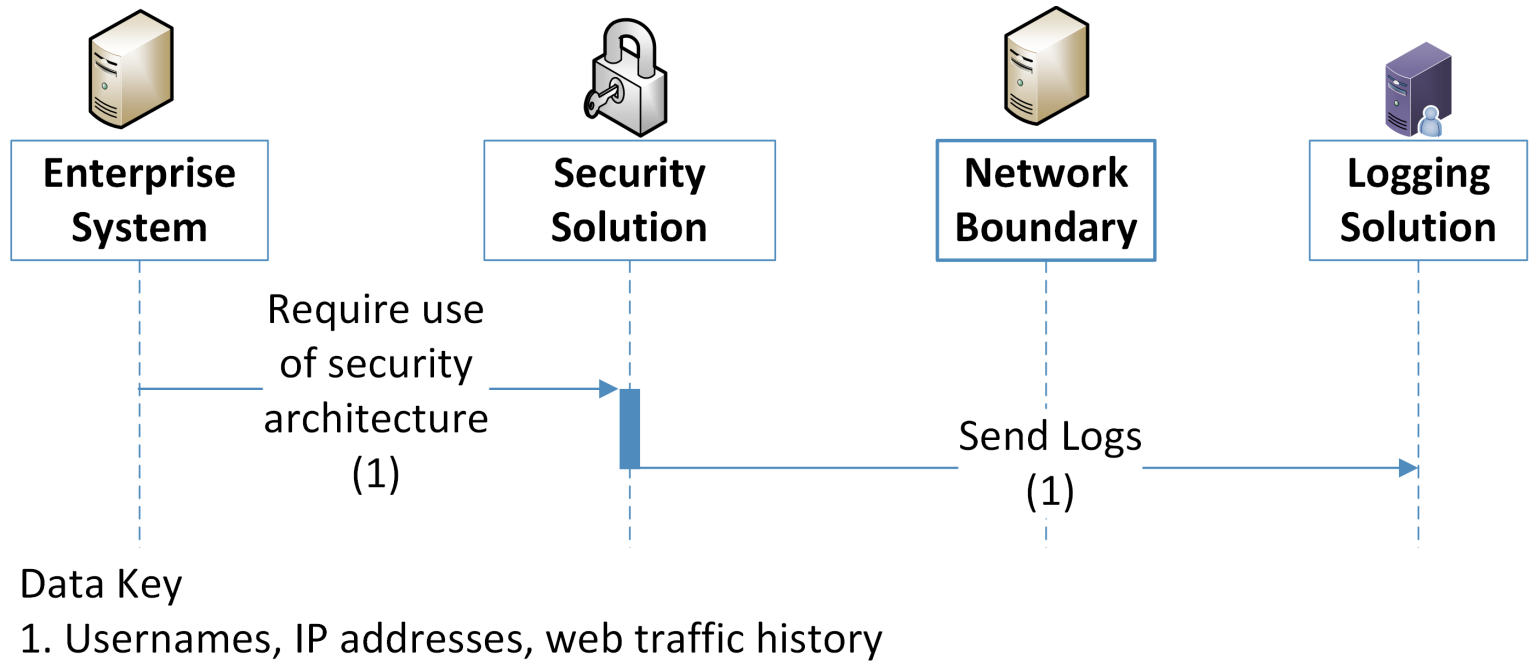
Table 5-13 Network Detection Problematic Data Actions

Scenarios	Examples of Privacy Risk	Problematic Data Actions	Privacy Mitigations
Netflow data is replicated to a network monitoring solution for analysis.	User data and metadata that is transmitted across the network through a network monitoring solution increases the chance of exposure of information to organizational administrators and third-party tools. Further, user network traffic may be used to profile user behavior.	Context: Network monitoring tools commonly duplicate and centralize network traffic activity. This may expose information affecting privacy to third party software or to network administrators. Additionally, such monitoring capabilities can prevent or undo the effects of de-identification capabilities used by other security tools. Finally, this additional viewing and analysis might be used to profile a user, and conflict with their expectations regarding the level of scrutiny to which their data is exposed. Problematic Data Action: Surveillance, Unanticipated Revelation, Re-Identification Problem: Loss of Trust. Users may find the scrutiny of their network traffic unexpected or unwarranted. Furthermore, violation of other advertised anonymization capabilities can strongly affect trust in the security architecture.	Predictability: Users should be informed of monitoring capabilities of Cisco Stealthwatch and related tools, such as through a login banner. Use privacy enhancing technologies and techniques to de-identify user ID and IP address like obfuscation, communication anonymization, data minimization, and pseudonymization, among others. Manageability: Organizations seeking to secure these sorts of tools should make sure that they are configurable, and consider the requirements for them to operate effectively. This can include de-identification options within such monitoring devices. Disassociability: Organizations should employ de-identification options for data when appropriate. Furthermore, tools that rely on unaltered network traffic should consider what privacy mitigations applied to other tools may be compromised by their use. Confidentiality: Organizations should mandate strict access controls for security tools that can impact user privacy, including the use of MFA.

5.3.4 Monitoring by Logging Solution

This reference architecture generates logs used to aid in response and recovery activities. These logs are essential for proper data management and incident response. However, organizations should consider the privacy implications of data processing activities related to logging and montioring.

Figure 5-4 Logging Data Flow Diagram



Data processing throughout the security architecture, and the logs generated by user activities, can interact with and create information that affects the privacy of users. The use of a logging solution requires that data and metadata about user's activity be generated and stored in an additional location. Depending on the details and scope of the logging tool, this can extend the effective domain of information that affects privacy used by those tools. Some examples of information affecting privacy utilized in such transactions is given below:

Table 5-14 Logging Data Actions

Data Type	Data Action	Examples of Privacy Considerations
IP Addresses	IP Addresses are stored and transferred by enterprise systems as well as the Logging Solution. They are transferred by and through the Security Solutions.	IP addresses can be used to determine rough locations for user-owned machines. Additionally, IP Addresses can be common across logs from many security tools, allowing for anonymized data to be re-identified and can enable tracking or surveillance in unintended ways.
Device Identifiers	Device Identifiers are stored and transferred by enterprise systems as well as the Logging Solution. They are transferred by and through the Security Solutions.	Under certain circumstances, Device Identifiers, such as MAC (media access control) addresses, can be used to identify individuals from data that has been de-identified, or allow for privacy-impacting correlations to be made between data logs.

Table 5-15 Logging Problematic Data Actions

Scenarios	Examples of Privacy Risk	Problematic Data Actions	Privacy Mitigations
Security tools generate metadata that is transferred to a logging solution, either directly or via an on-site forwarder.	The security system passively creates data about users, their data, and their activities and may provide insights into users or their activity that they do not anticipate. This information is transmitted across the network, stored remotely, and may be combined with other information in ways that reveal additional information about users beyond what can be gleaned from any one particular system.	Context: Logging systems contain data history of user activities. These logs are transmitted off the device or system in which they were created to other systems where log information is aggregated. The privacy impact of each log and the aggregation of logs must be considered. Furthermore, this information is exposed to administrators who have access to either the individual or aggregated logs. Problematic Data Action: Unanticipated Revelation, Re-identification, Surveillance Problem: Loss of trust. Users may not expect the scope of information created and tracked by logs, even if they understand the scope of the security infrastructure. Dignity Loss. Embarrassing or undesired privacy information may be inferred about individuals whose actions generate logging information.	Predictability: The existence of monitoring systems should be disclosed to users upon their access to organizational systems, such as through a login banner. Use privacy enhancing technologies and techniques to de-identify user ID and IP address like obfuscation, communication anonymization, data minimization, and pseudonymization, among others. Manageability: Organizations should evaluate how logs can be configured to collect the least amount of information necessary in order to meet security needs, especially when security tools are aggregating log information across multiple systems. Disassociability: Organizations should consider de-identification functions for log creation, transmission, storage and aggregation. For example, privacy-relevant information such as the user's name can be disassociated from their IP address or device identifier when collecting log information. Confidentiality: Tools that generate or store logs should have strict access control applied to them such as MFA.

6 Future Build Considerations

As shown in Figure 1-1, the NCCoE Data Security work that remains to be addressed within the framework of the CIA triad is that of Data Availability. The Data Security team plans to evaluate the current landscape of Data Availability challenges that organizations face and determine future relevant projects to address those needs.

Appendix A List of Acronyms

BYOD	Bring Your Own Device
COBIT	Control Objectives for Information and Related Technologies
CIA	Confidentiality Integrity Availability
CIS	Center for Internet Security
CNSSI	Committee on National Security Systems Instruction
CRADA	Cooperative Research And Development Agreement
CSC	Critical Security Controls
CSF	Cybersecurity Framework
FIPS	Federal Information Processing Standard
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
MAC	Media Access Control
MFA	Multi Factor Authentication
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NIST IR	NIST Interagency or Internal Report
PII	Personally Identifiable Information
PRAM	Privacy Risk Assessment Methodology
RDP	Remote Desktop Protocol
RMF	Risk Management Framework
SMS	Short Messaging Service
SP	Special Publication
URL	Uniform Resource Location

USB	Universal Series Bus
VDI	Virtual Desktop Interface

Appendix B Glossary

Access Control	The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances). SOURCE: Federal Information Processing Standard (FIPS) 201-3
Adversary	Person, group, organization, or government that conducts or has the intent to conduct detrimental activities. SOURCE: CNSSI 4009-2015
Asset	A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. SOURCE: Committee on National Security Systems Instruction (CNSSI) 4009-2015
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: FIPS 200
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges. SOURCE: CNSSI 4009-2015
Backup	A copy of files and programs made to facilitate recovery if necessary. SOURCE: NIST SP 800-34 Rev. 1
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose. SOURCE: NIST SP 800-53 Rev. 5

Control	The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature. SOURCE: NIST SP 800-160 Vol. 2 Rev. 1
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. SOURCE: FIPS 200
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted. SOURCE: CNSSI 4008-2015
Data Action	A system/product/service data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal. SOURCE: NIST Privacy Framework Version 1.
Disassociability	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system. SOURCE: NISTIR 8062
Encrypt	Cryptographically transform data to produce cipher text. SOURCE: CNSSI 4009-2015
Enterprise	An entity of any size, complexity, or positioning within an organizational structure. SOURCE: NIST SP 800-72
Event	Any observable occurrence in a network or system. SOURCE: CNSSI 4009-2015
Exfiltration	The unauthorized transfer of information from an information system. SOURCE: CNSSI 4009-2015

Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. SOURCE: FIPS 200
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. SOURCE: FIPS 200
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. SOURCE: CNSSI 4009-2015
Manageability	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure. SOURCE: NISTIR 8062
Mitigation	A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities. SOURCE: NIST SP 1800-160 Vol. 2 Rev. 1
Phishing	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. SOURCE: CNSSI 4009-2015
Predictability	Enabling reliable assumptions by individuals, owners, and operators about PII and its processing by a system. SOURCE: NISTIR 8062
Privacy	A condition that safeguards human dignity and autonomy by means of methods that achieve predictability, manageability, and disassociability

Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. SOURCE: FIPS 200
Security Control	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: NIST SP 800-53
Security Policy	A set of rules that governs all aspects of security-relevant system and system component behavior. SOURCE: NIST SP 800-53 Rev. 5
Spear Phishing	A colloquial term that can be used to describe any highly targeted phishing attack. SOURCE: CNSSI 4009-2015
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. SOURCE: NIST SP 800-53 Rev. 5
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. SOURCE: FIPS 200

Appendix C References

[1] W. Barker, *Guideline for Identifying an Information System as a National Security System*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59, Gaithersburg, Md., Aug. 2003, 17 pp. Available: https://doi.org/10.6028/NIST.SP.800-59.

[2] T. McBride *et. al*, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-25, Gaithersburg, Md., Dec. 2020, 488 pp. Available: https://doi.org/10.6028/NIST.SP.1800-25.

[3] T. McBride *et. al*, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*, National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-26, Gaithersburg, Md., Dec. 2020, 441 pp. Available: https://doi.org/10.6028/NIST.SP.1800-26.

[4] T. McBride *et. al*, *Data Integrity: Recovering from Ransomware and Other Destructive Events*, National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-11, Gaithersburg, Md., Sep. 2020, 377 pp. Available: https://doi.org/10.6028/NIST.SP.1800-11.

[5] M. Souppaya and K. Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-83 Revision 1, Gaithersburg, Md., July 2013, 36 pp. Available: https://doi.org/10.6028/NIST.SP.800-83r1.

[6] M. Souppaya and K. Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Devise (BYOD) Security*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 2, Gaithersburg, Md., July 2016, 43 pp. Available: https://doi.org/10.6028/NIST.SP.800-46r2.

[7] M. Bartok *et. al*, *Guide for Cybersecurity Event Recovery*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-184, Gaithersburg, Md., Dec. 2016, 45 pp. Available: https://doi.org/10.6028/NIST.SP.800-184.

[8] NIST. *Privacy Framework*. Available: https://www.nist.gov/privacy-framework.

[9] NIST. *Cybersecurity Framework*. Available: http://www.nist.gov/cyberframework.

[10] W. Barker *et. al*, *Ransomware Risk Management: A Cybersecurity Framework Profile*, NIST Interagency Report 8374, Gaithersburg, Md., Feb. 2022, 23 pp. Available: https://doi.org/10.6028/NIST.IR.8374.

[11] S. Brooks *et. al*, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, NIST Interagency Report 8062, Gaithersburg, Md., Jan. 2017, 41 pp. Available: https://doi.org/10.6028/NIST.IR.8062.

[12] Joint Task Force, *Risk Management Framework for Information Systems and Organizations*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 2, Gaithersburg, Md., Dec. 2018, 164 pp. Available: https://doi.org/10.6028/NIST.SP.800-37r2.

[13] NIST. *Risk Management Framework*. Available: https://csrc.nist.gov/projects/risk-management/about-rmf.

[14] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1, Gaithersburg, Md., Sep. 2012, 83 pp. Available: https://doi.org/10.6028/NIST.SP.800-30r1.

[15] NIST. *Privacy Risk Assessment Methodology*. Available: https://www.nist.gov/privacy-framework/nist-pram.

[16] NIST. *Catalog of Problematic Data Actions and Problems*. Available: https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md.

[17] NIST. *Privacy Framework Resource Repository*. Available: https://www.nist.gov/privacy-framework/resource-repository.

Appendix D Security Control Map

The following table lists the NIST Cybersecurity Framework Functions, Categories, and Subcategories addressed by this project and maps them to relevant NIST standards, industry standards, and controls and best practices.

Table 6-1 Security Control Map

Cybersecurity Framework v1.1			Standards & Best Practices
Function	**Category**	**Subcategory**	**Informative References**
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **ISO/IEC 27001:**2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 ISA 62443-3-3:2013 SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4

Cybersecurity Framework v1.1			Standards & Best Practices
Function	**Category**	**Subcategory**	**Informative References**
	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM3, SC-5, SC-7, SI-4
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
RESPOND (RS)	Communications (RS.CO)	RS.CO-2: Incidents are reported consistent with established criteria	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
	Analysis (RS.AN)	RS.AN-3: Forensics are performed	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
	Mitigation (RS.MI)	RS.MI-2: Incidents are mitigated	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10

Cybersecurity Framework v1.1			Standards & Best Practices
Function	**Category**	**Subcategory**	**Informative References**
			ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
RECOVER (RC)	Recover (RC.RP)	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8

Appendix E Privacy Control Map

The following table lists the NIST Privacy Framework Functions, Categories and Subcategories addressed by this project and maps them to relevant NIST standards, industry standards, and controls and best practices.

NOTE: The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standard 27701 references were not mapped by NIST, but by an external organization. They are available at the NIST Privacy Framework Repository [17] and provided here for convenience. The Fair Information Privacy Principles (FIPPS) references are provided to aid understanding of the Privacy Control Map.

Table 6-2 Privacy Control Map

Privacy Framework 1.0				Standards and Best Practices
	Function	**Category**	**Subcategory**	**Informative Refences**
	CONTROL-P (CT-P Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	**Data Processing Management (CT.DM-P):** Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P8:** Audit/log records are determined, documented, and reviewed in accordance with policy and incorporating the principle of data minimization.	**FIPPS 4**: Minimization **NIST SP 800-53 Rev. 5:** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16 **NIST IR 8062** **ISO/IEC 27701:2019** 6.9.4.1, 6.9.4.2, 6.15.1.3
	PROTECT-P (PR-P): Develop and Implement appropriate data processing safeguards.	**Identity Management, Authentication, and Access Control (PR.AC-P):** Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes,	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12 **NIST SP 800-63-3** **ISO/IEC 27701:2019** 6.6.2.1, 6.6.2.2, 6.6.4.2

Privacy Framework 1.0				Standards and Best Practices
	Function	Category	Subcategory	Informative Refences
		the assessed risk of unauthorized access.	and devices.	
			PR.AC-P3: Remote access is managed.	**FIPPS 8: Security** **FIPS Publication 199** **NIST SP 800-46 Rev. 2** **NIST SP 800-53 Rev. 5:** AC-1, AC-17, AC-19, AC-20, SC-15 **NIST SP 800-77** **NIST SP 800-113** **NIST SP 800-114 Rev. 1** **NIST SP 800-121 Rev. 2** **ISO/IEC 27701:2019** 6.6.2.1, 6.6.2.2
			PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** AC-4, AC-10, SC-7, SC-10, SC-20
			PR.AC-P6: Individuals and devices are proofed and bound to credentials and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** AC-14, AC-16, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11, IA-12, PE-2, PS-3 **NIST SP 800-63-3**

Privacy Framework 1.0				Standards and Best Practices
	Function	Category	Subcategory	Informative Refences
			organizational risks).	
		Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.	**PR.PT-P3: Communications and control networks are protected.**	**NIST SP 800-53 Rev. 5 (draft):** AC-4, AC-17, AC-18, CP-8, SC-7 SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC41, SC-43

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.

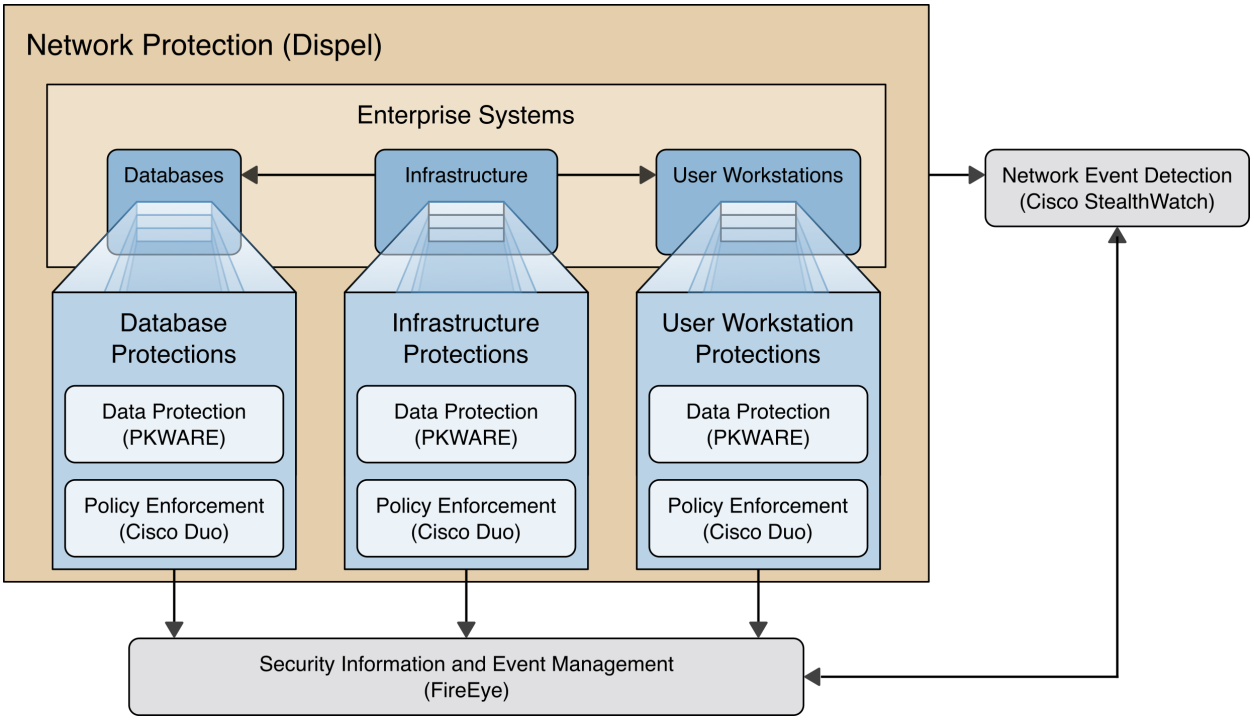
Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the NCCoE Style Guide.
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit.**
`Monospace`	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.

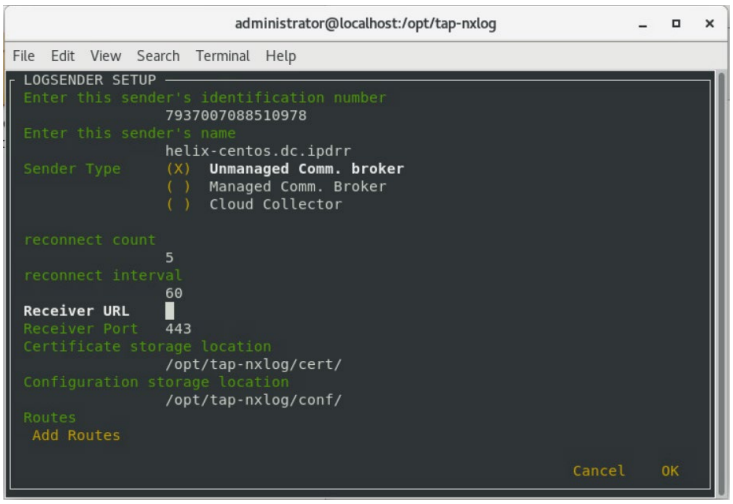
```
> sudo cd ..
```

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.



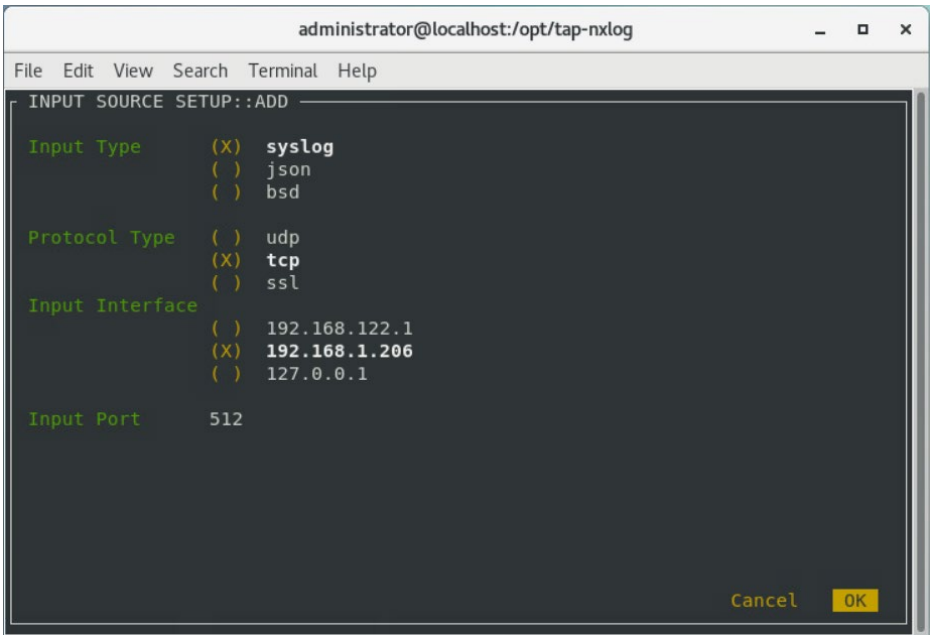
15. Select **Add Routes** and press **Enter**.

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.



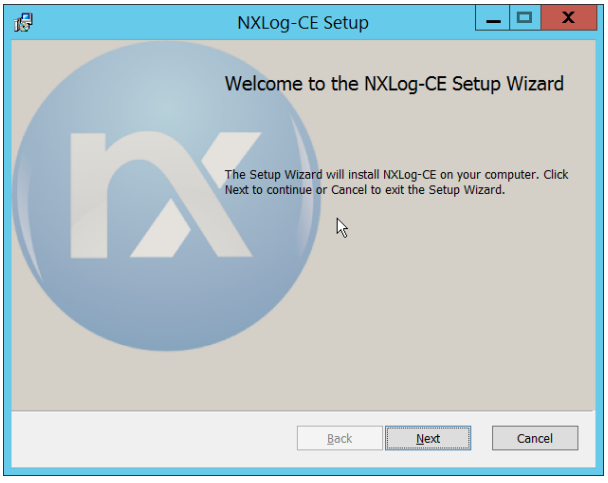
20. Select **OK** and press **Enter**.

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

2.1.2 Forwarding Event Logs from Windows 2012 R2

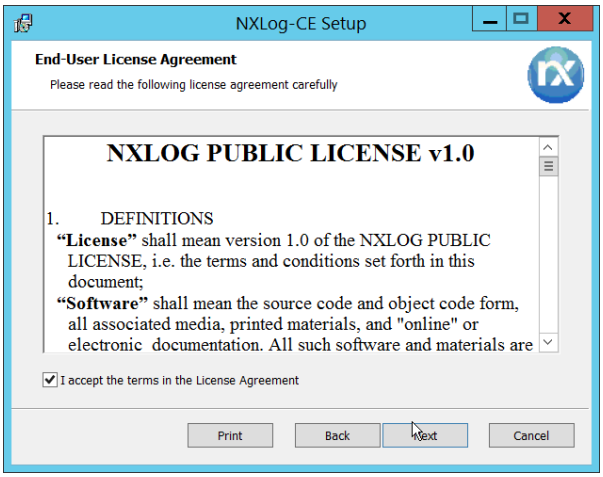
1. Acquire **nxlog-ce-2.10.2150.msi** from http://nxlog.org/products/nxlog-community-edition/download.

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

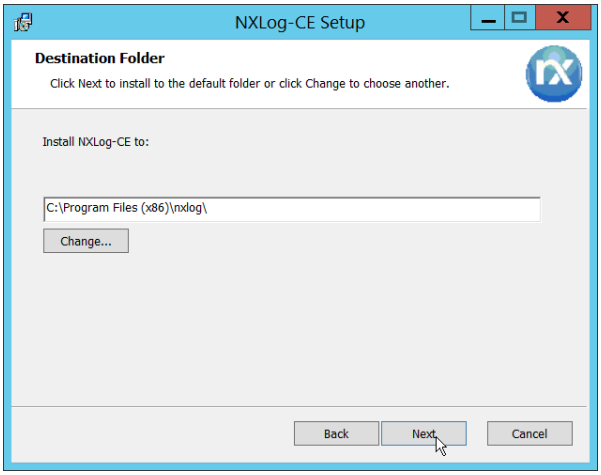


3. Click **Next**.

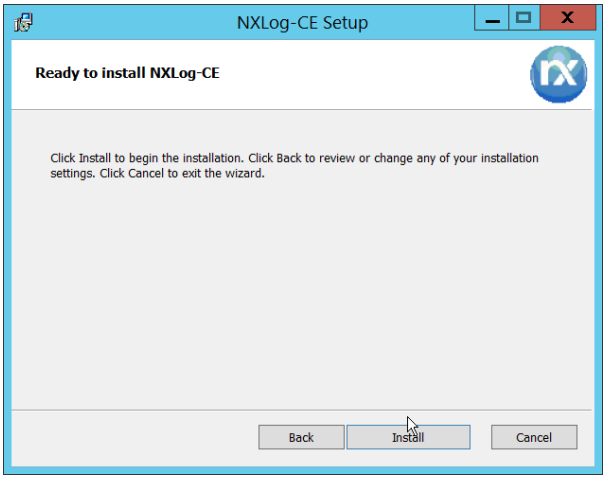
4. Check the box next to **I accept the terms in the License Agreement**.



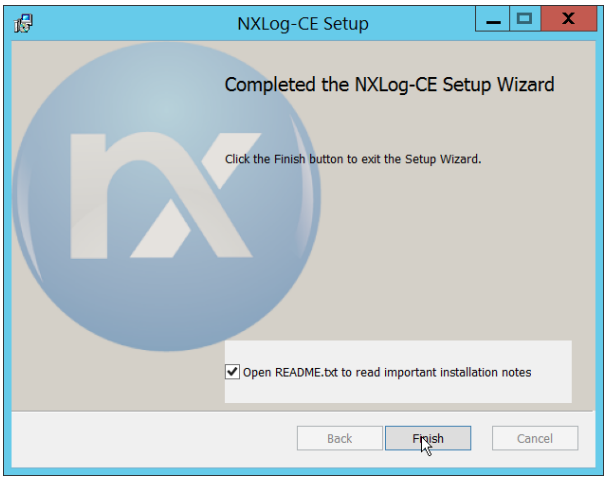
5. Click **Next**.



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.

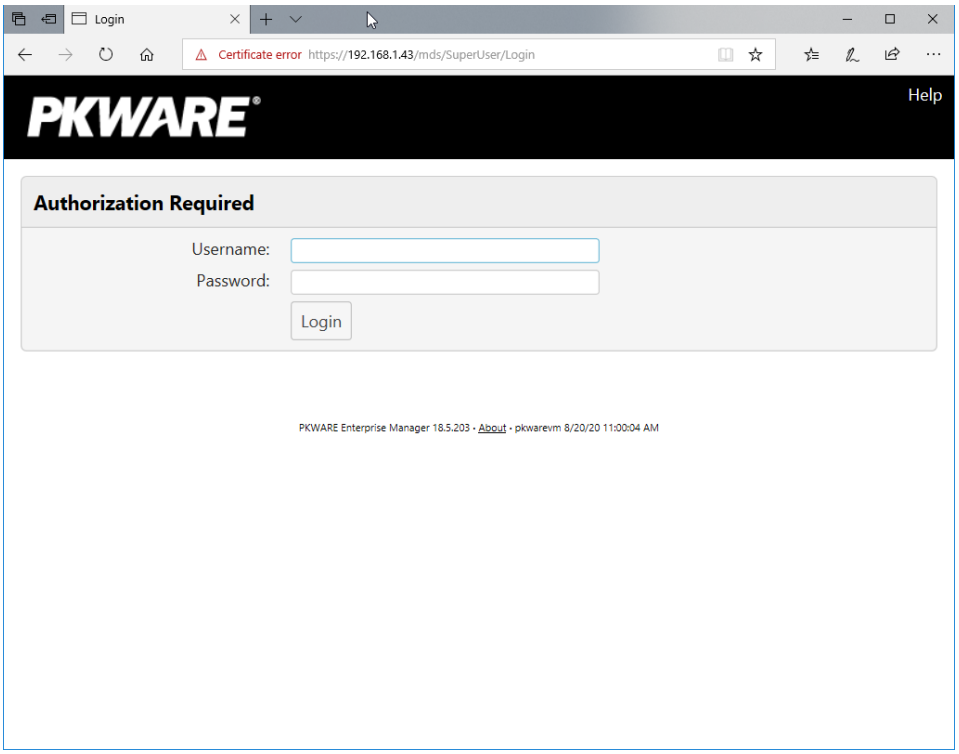
12. You can verify that this connection is working by checking the logs in data\nxlog.log, and by noting an increase in events on the Helix Dashboard.

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.

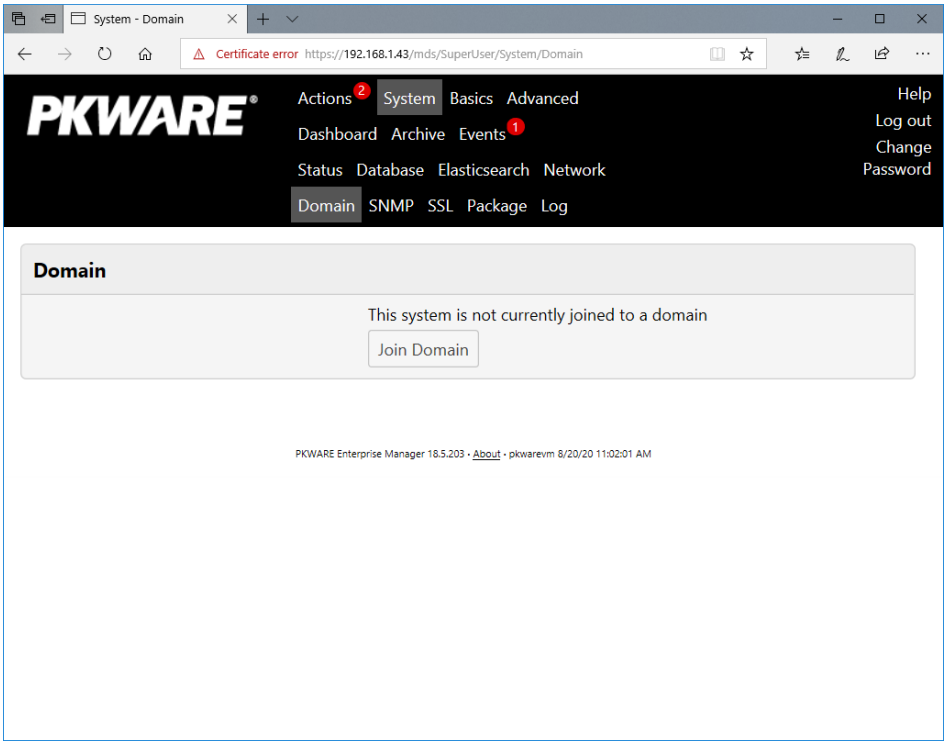
2.2.1 Configure PKWARE with Active Directory

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



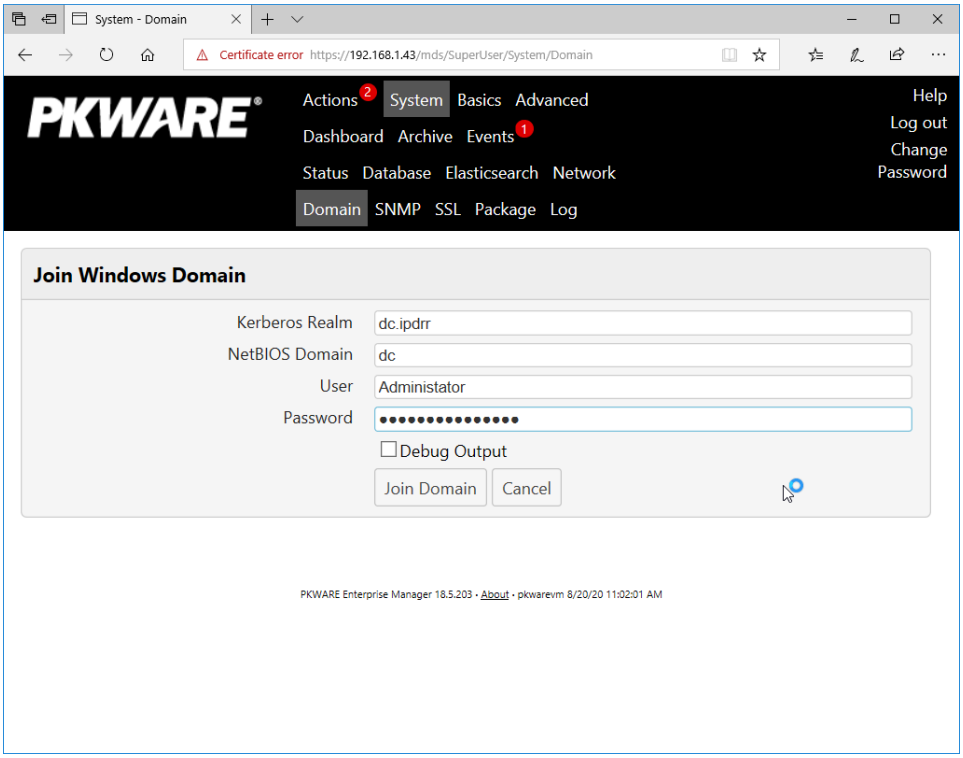
2. Once logged in, you can and should change the password to this administrative account by clicking **Change Password** in the top right corner.

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



4. Click **Join Domain**.

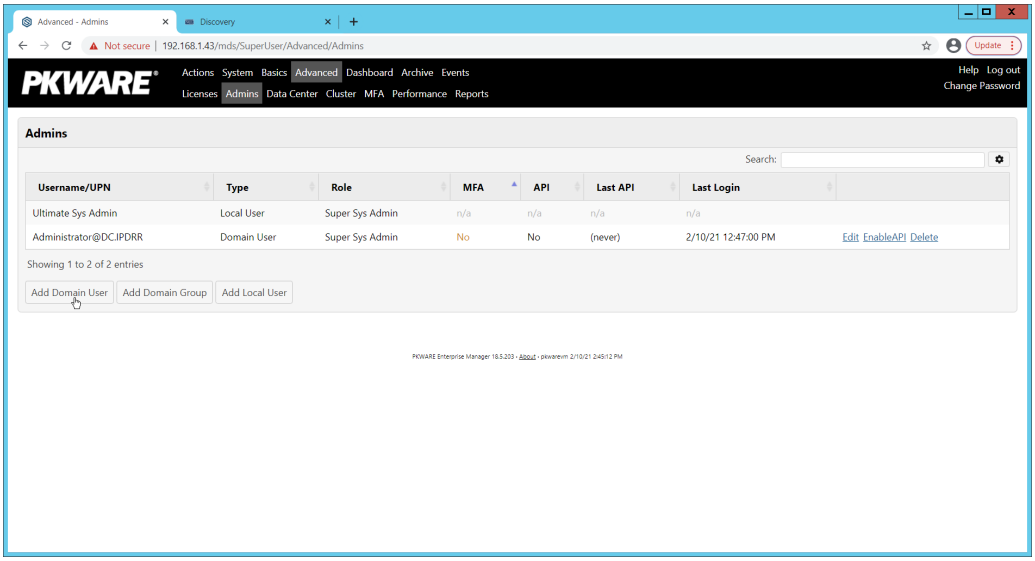
5. Enter the **Kerberos Realm, NetBIOS Domain**, as well as the **username** and **password** of an administrative user on the domain.



6. Click **Join Domain**.

2.2.2 Create a New Administrative User

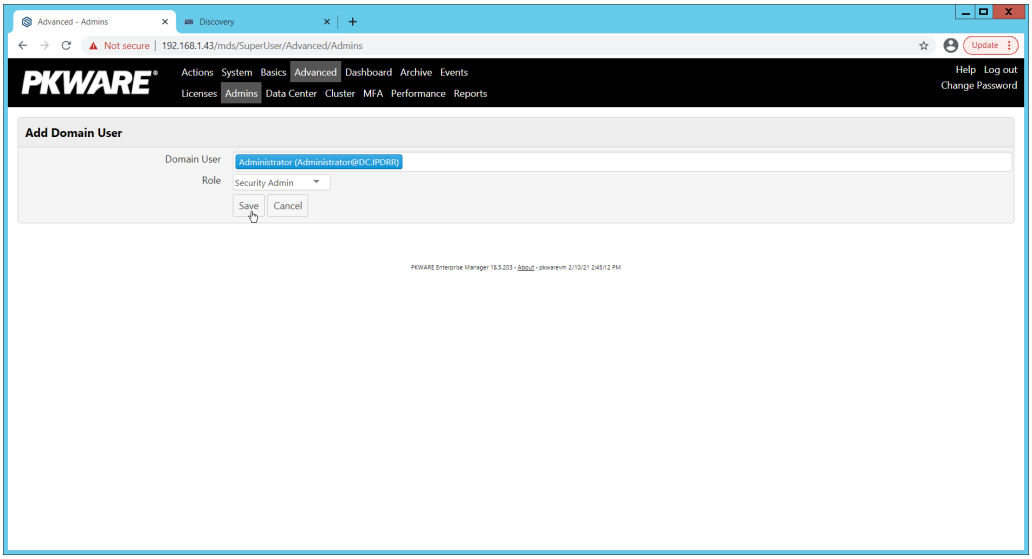
1. Navigate to **Advanced > Admins**.



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.

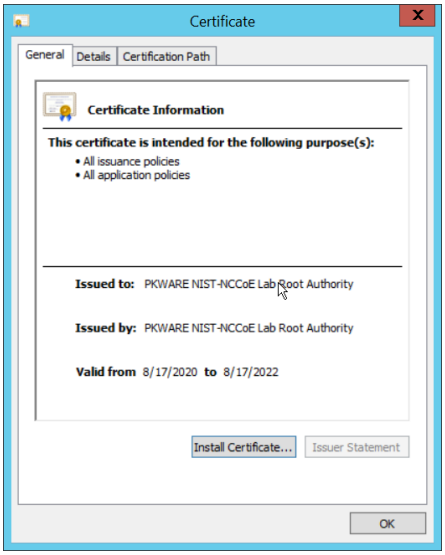


5. Click **Save**.

2.2.3 Install Prerequisites

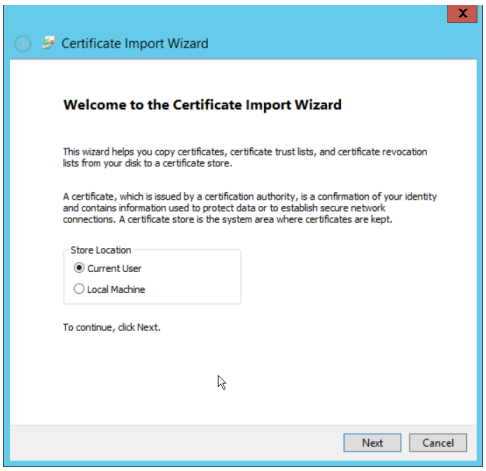
1. If needed for your environment, you may need to install certificates locally before agents can connect to PKProtect - ask your PKProtect representative if this is necessary for your environment.

2. Double click the certificate you wish to install.



3. Click **Install Certificate**.

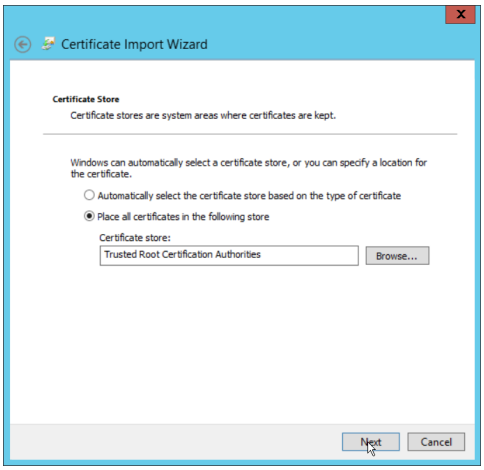
4. Select **Current User**.



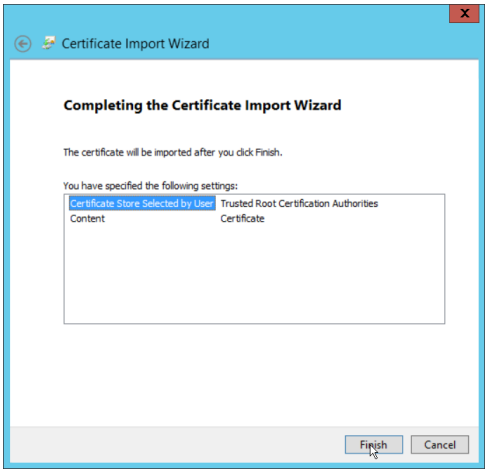
5. Click **Next**.

6. Click **Browse**.

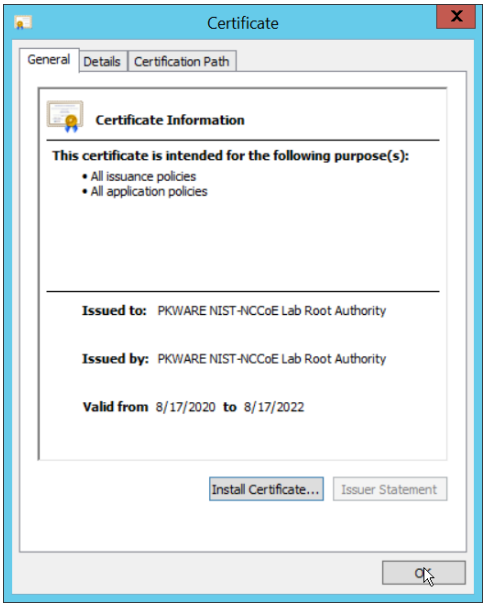
7. Select **Trusted Root Certification Authorities**.



8. Click **Next**.



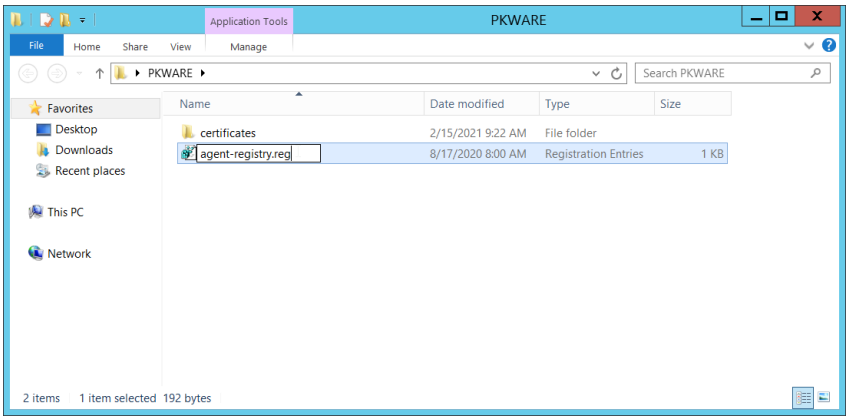
9. Click **Finish**.



10. Click **OK.**

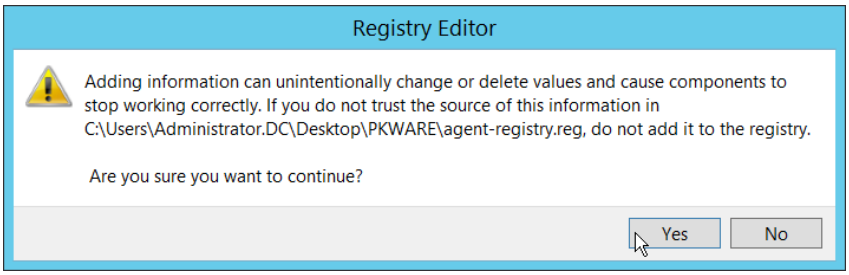
11. Repeat steps 1 through 10 but select **Personal** instead of **Trusted Root Certification Authorities.**

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

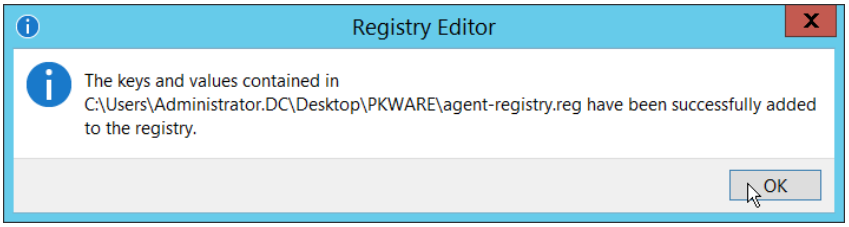


13. Rename *agent-registry.txt* to *agent-registry.reg*.

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



15. Click **Yes.**

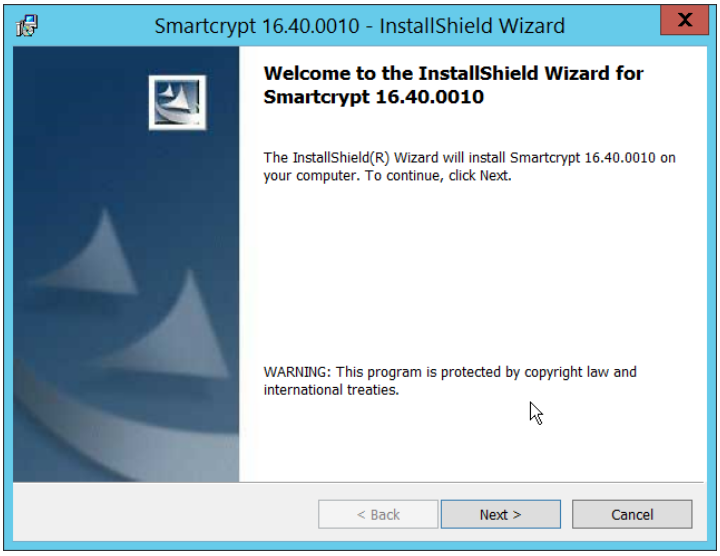


16. Click **OK**.

17. Restart the machine to apply these changes.

2.2.4 Install the PKProtect Agent

1. Run the PKProtect Installation executable.

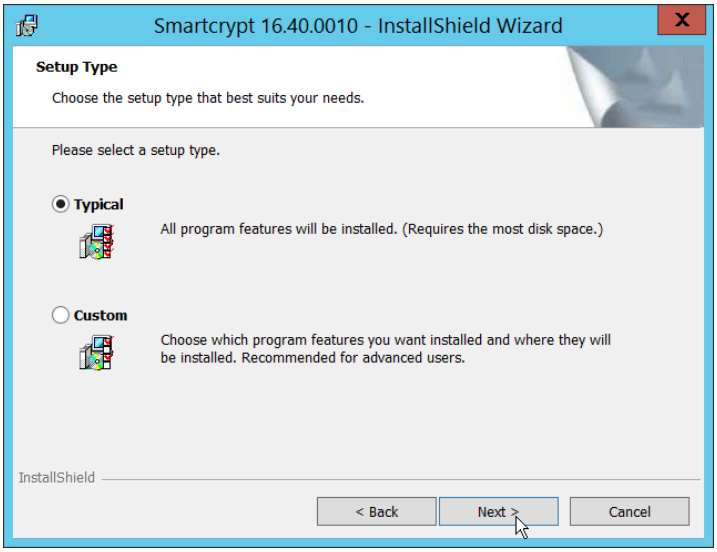


2. Click **Next**.

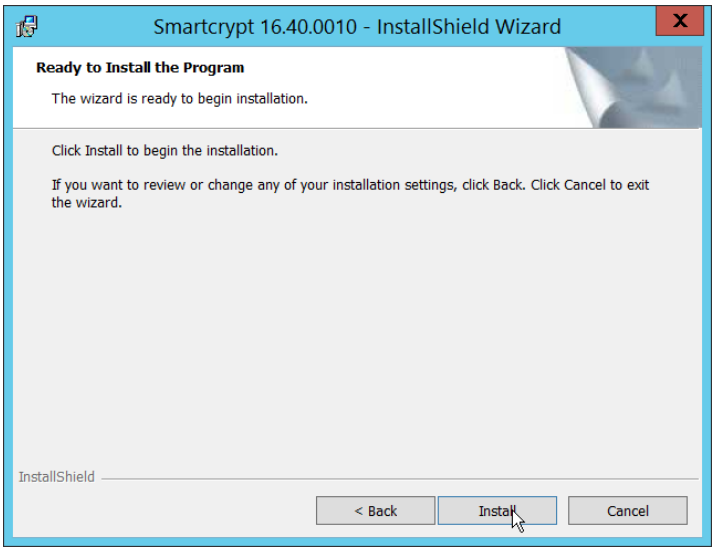
3. Select **I accept the terms in the license agreement**.

4. Click **Next**.

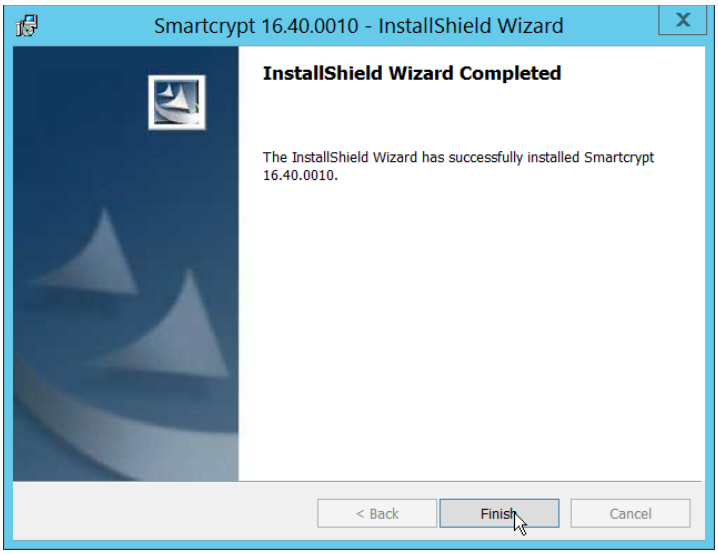
5. Select **Typical**.



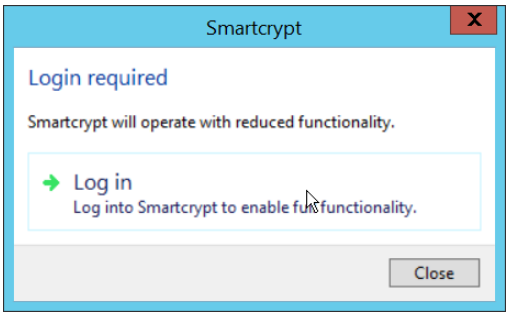
6. Click **Next**.



7. Click **Install**.

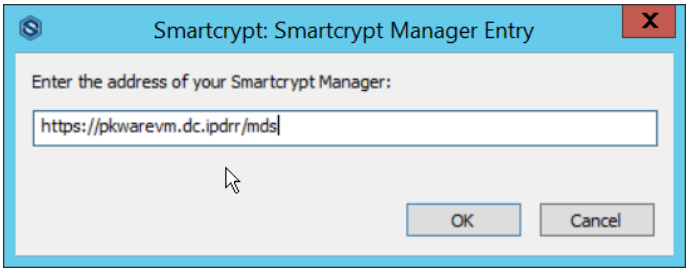


8. Click **Finish**.



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).

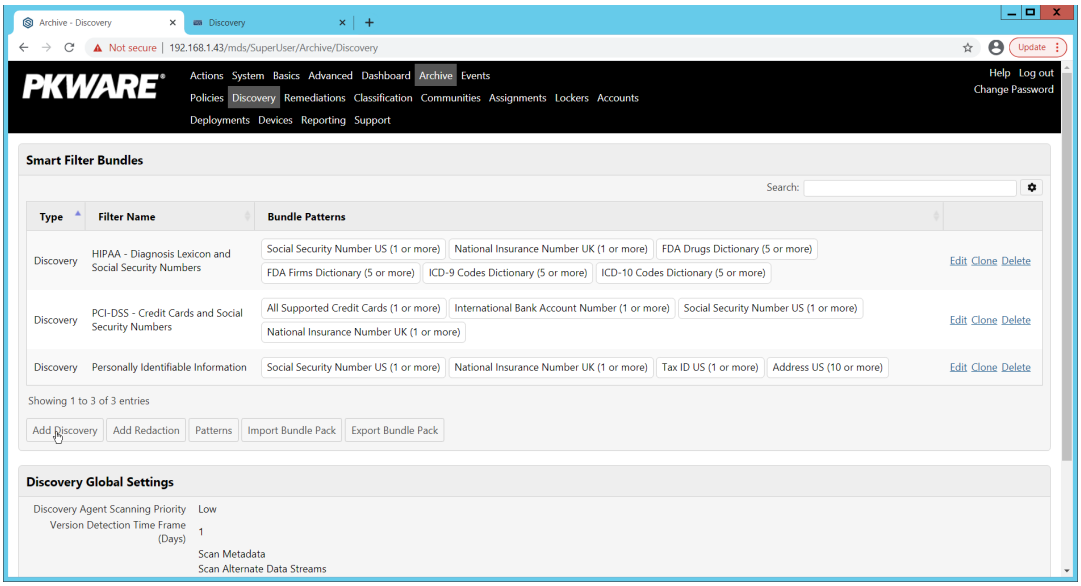


11. Enter the address of the PKWARE server.

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**.

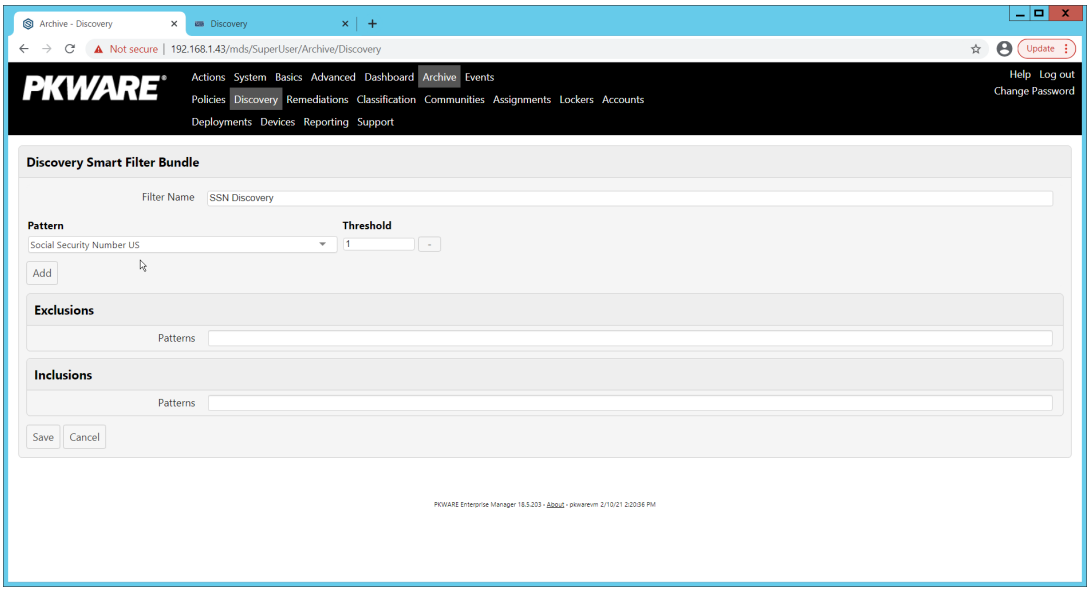


2. Click **Add Discovery**.

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

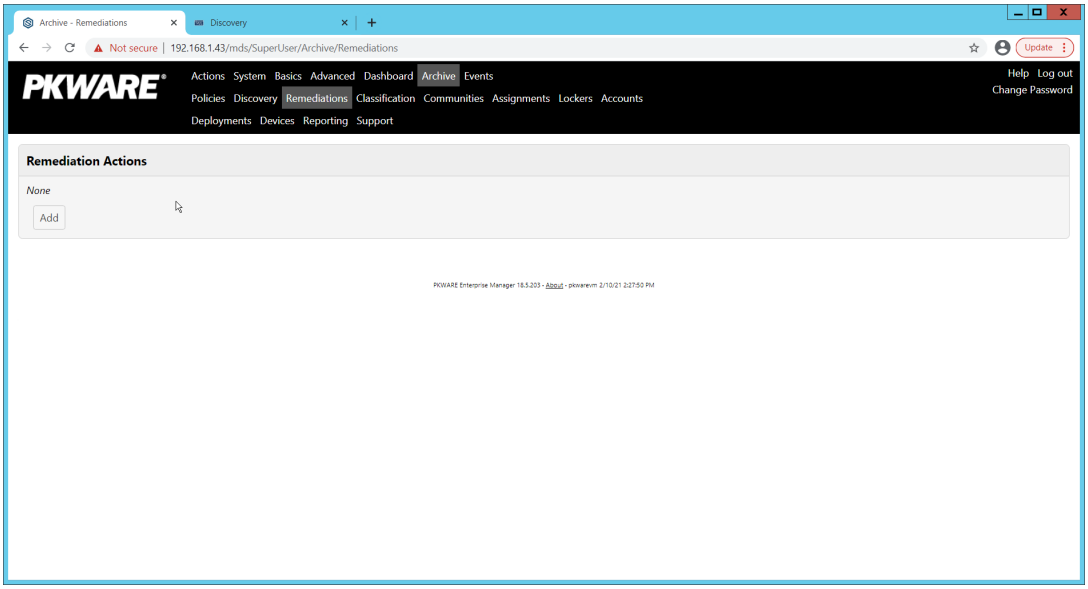
4. Select a **pattern** for the rule to discover. In this case, we are setting up a rule to detect social security numbers in files for reporting/remediation.

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



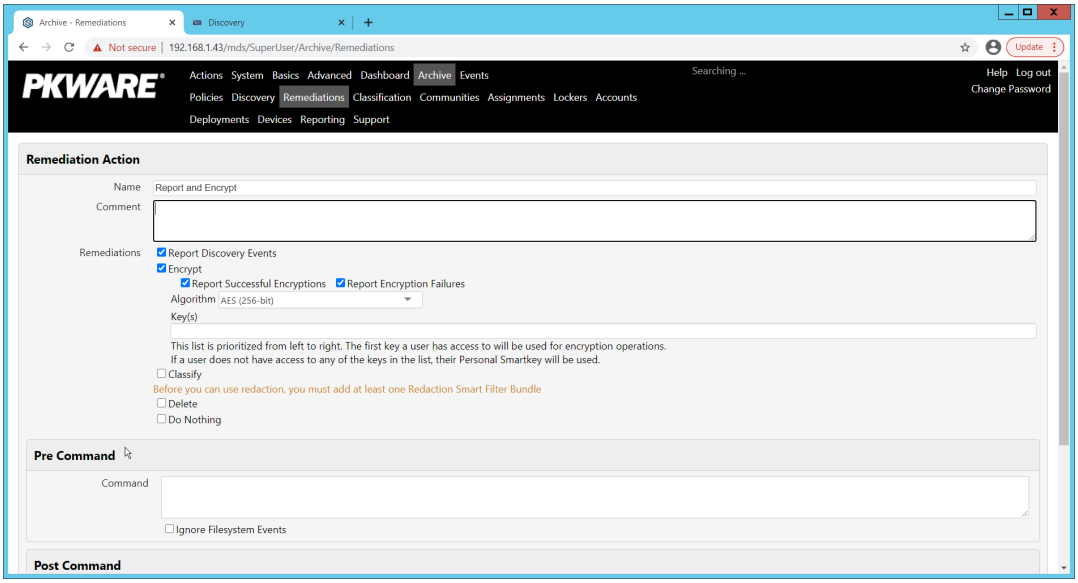
6. Click **Save**.

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



8. Click **Add**.

9. Enter a name for the remediation.

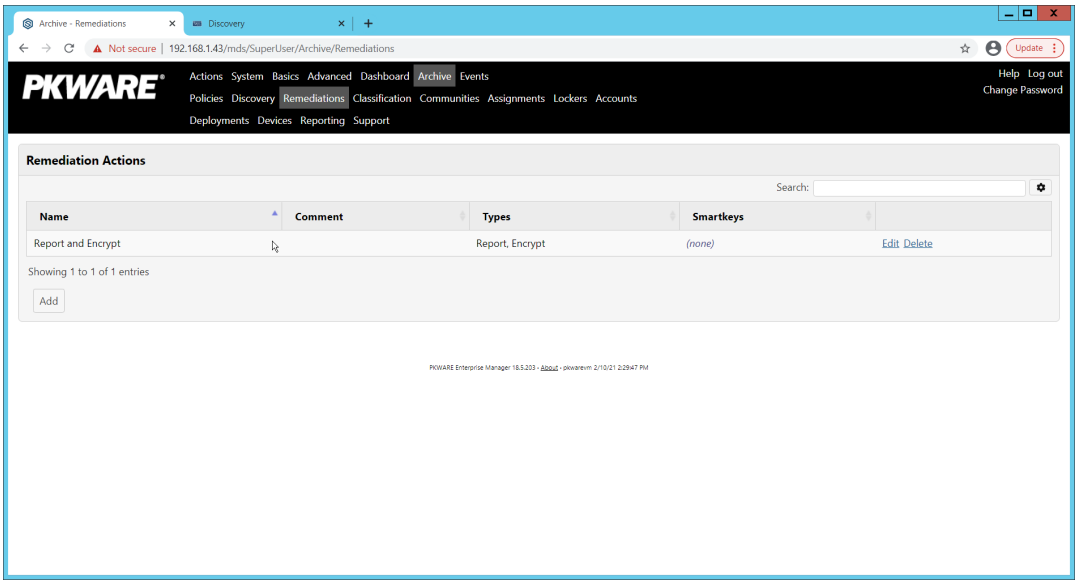


10. Check the box next to **Report Discovery Events**.

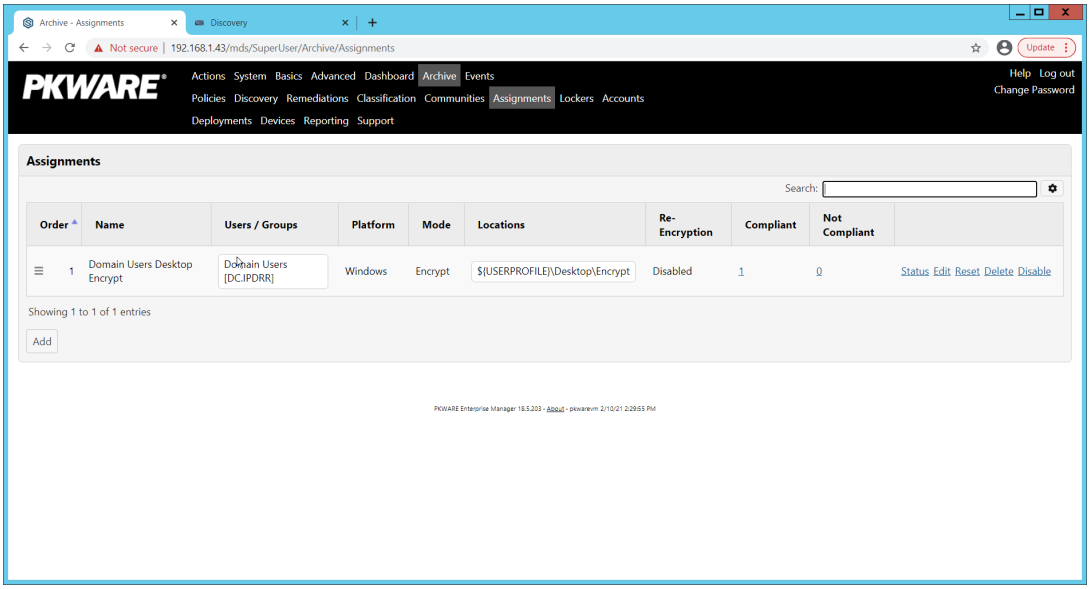
11. Check the box next to **Encrypt**.

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

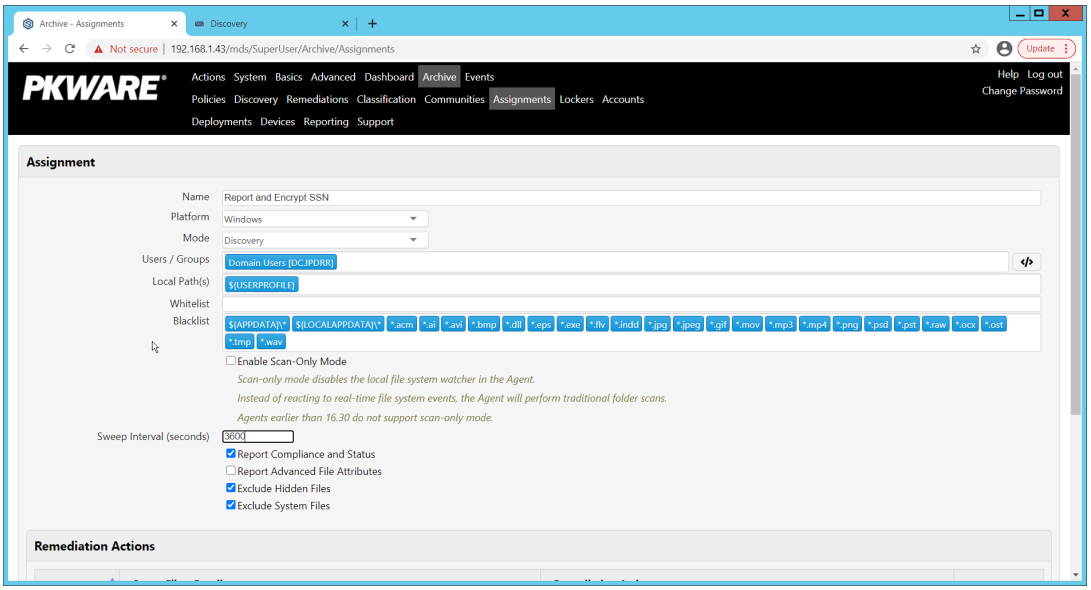
13. Click **Save**.



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.

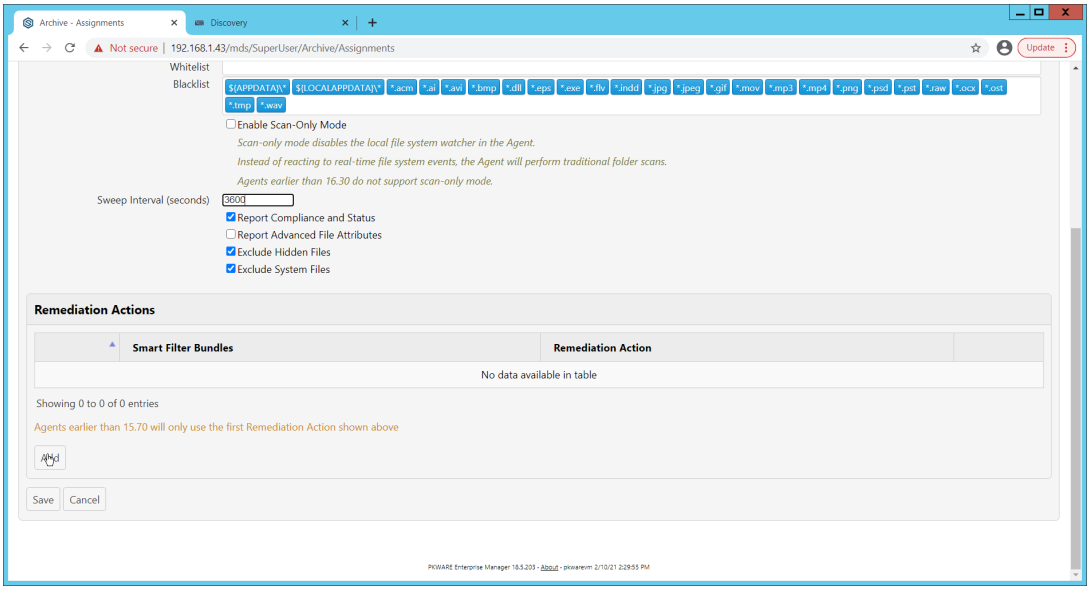
18. Select **Discovery** for the **Mode**.

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.

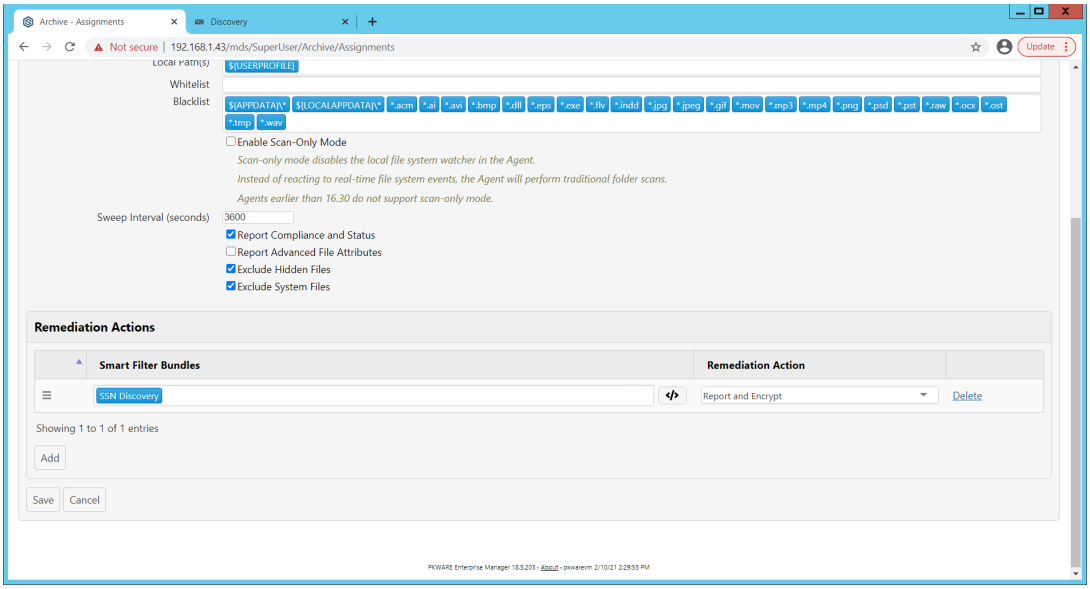
22. Enter the interval for this rule to run in **Sweep Interval**.



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.

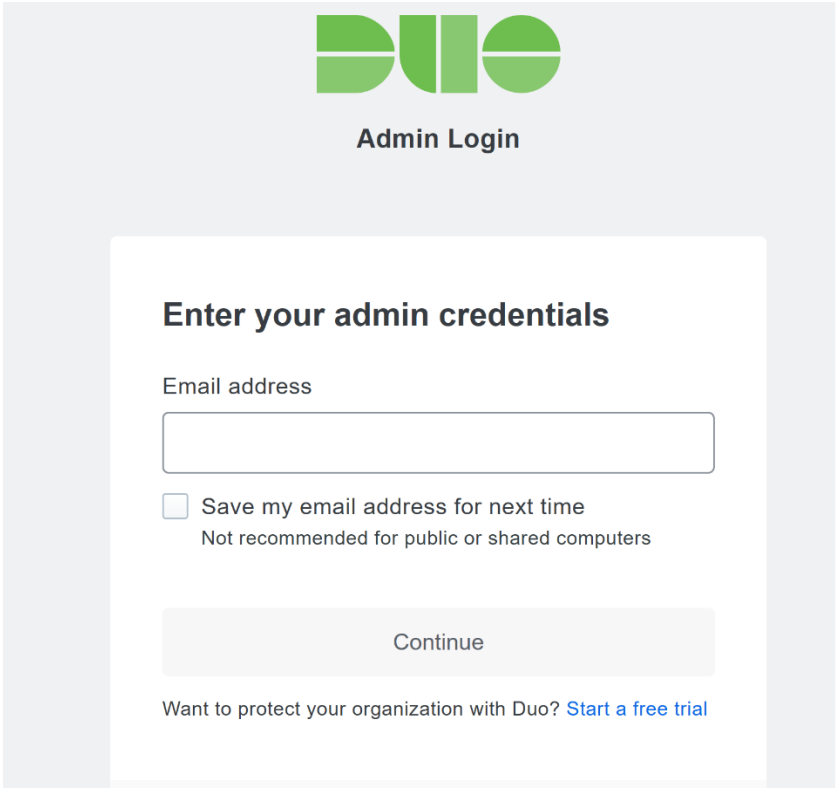
2.3 Cisco Duo

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.

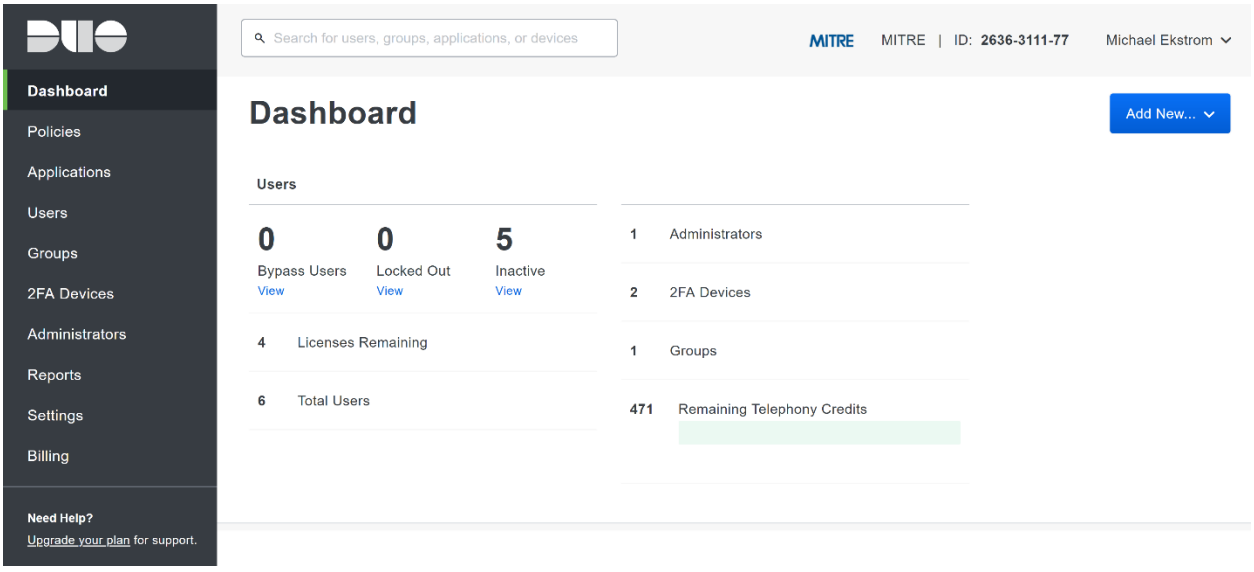
In the following section, we demonstrate the installation of Cisco Duo on an internal system in such a way that Remote Desktop Protocol (RDP) and local login to that system are protected by multifactor authentication.

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/.

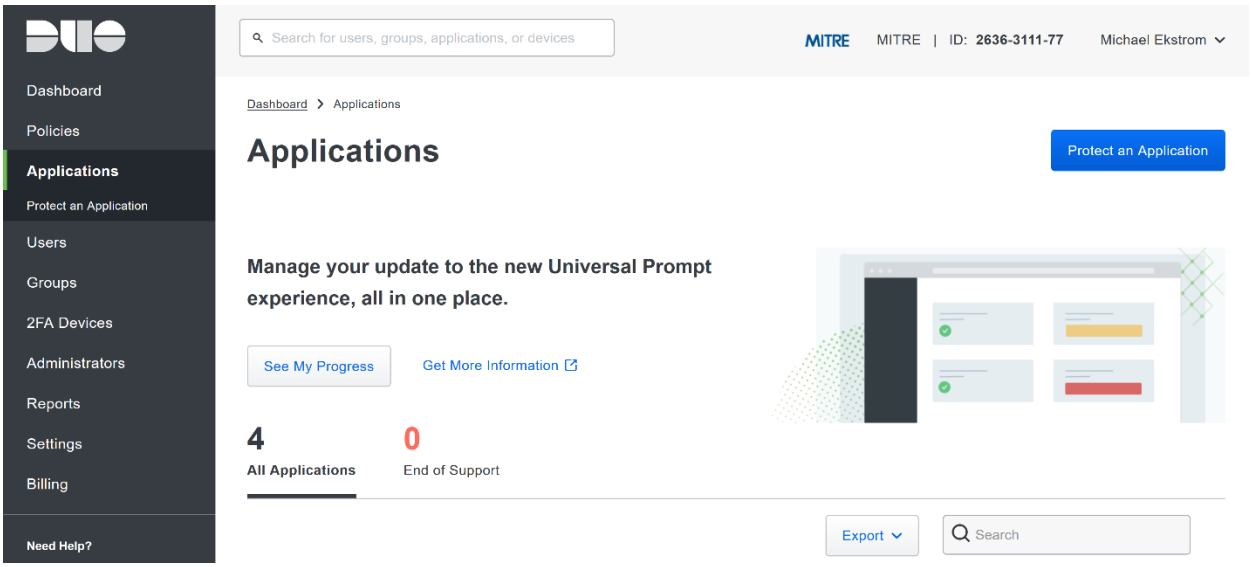


3. Login with your admin credentials and dual factor authentication to reach the administrator dashboard.



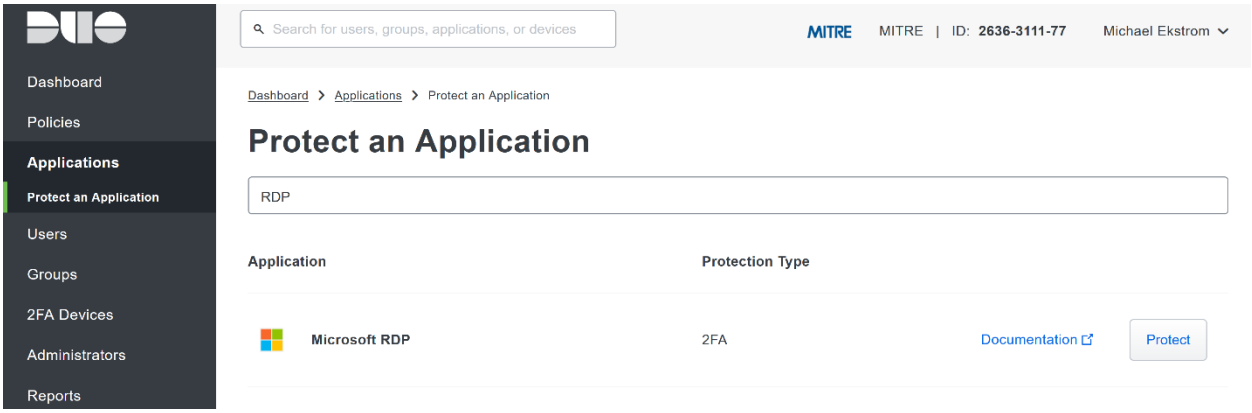
4. Click **Applications** in the sidebar.

5. Click **Protect an Application**.

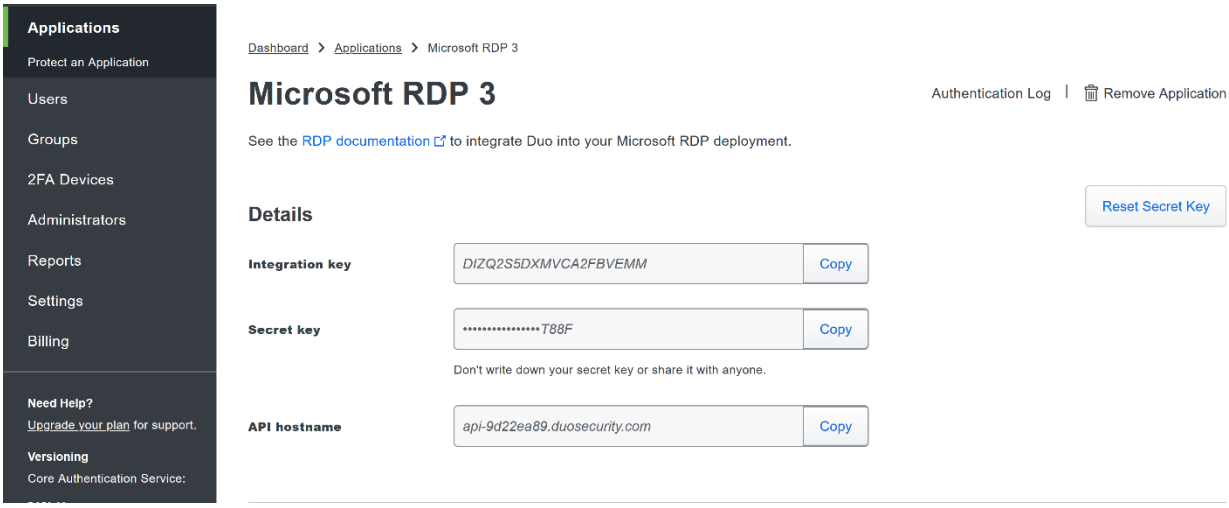


6. Search for, or scroll down to, **Microsoft RDP**.

7. Click **Protect**.

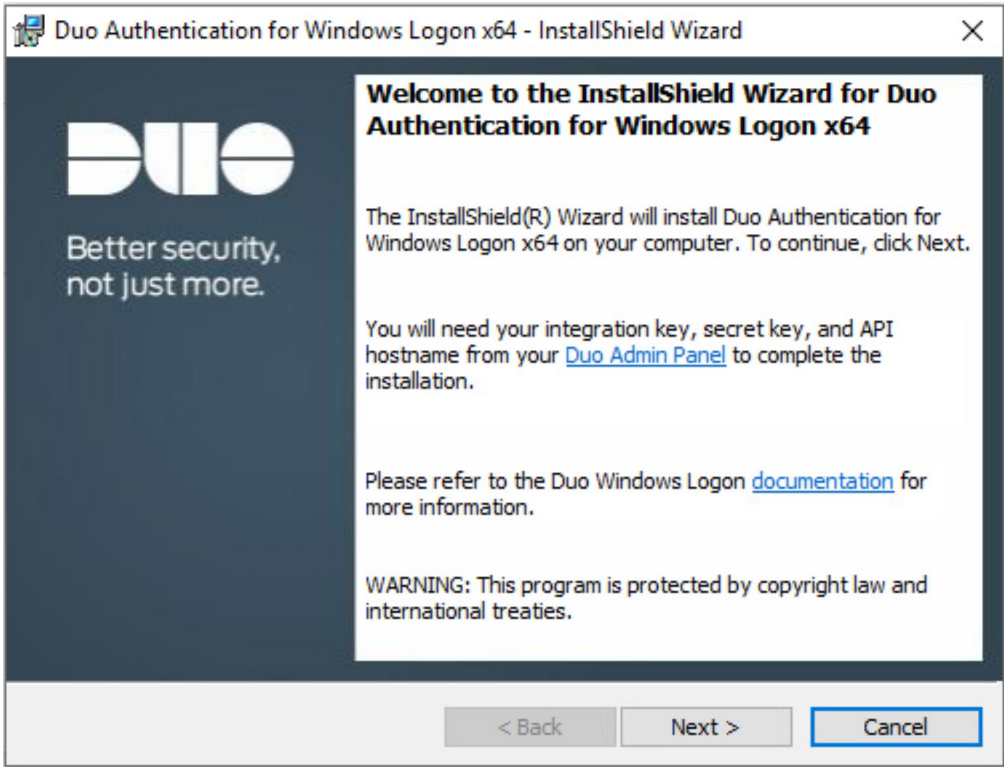


8. The next screen will provide policy configuration options, as well as the **Integration Key**, **Secret Key**, and **API hostname**, which are required information for the next step. Either keep this window open or copy down those three pieces of information.



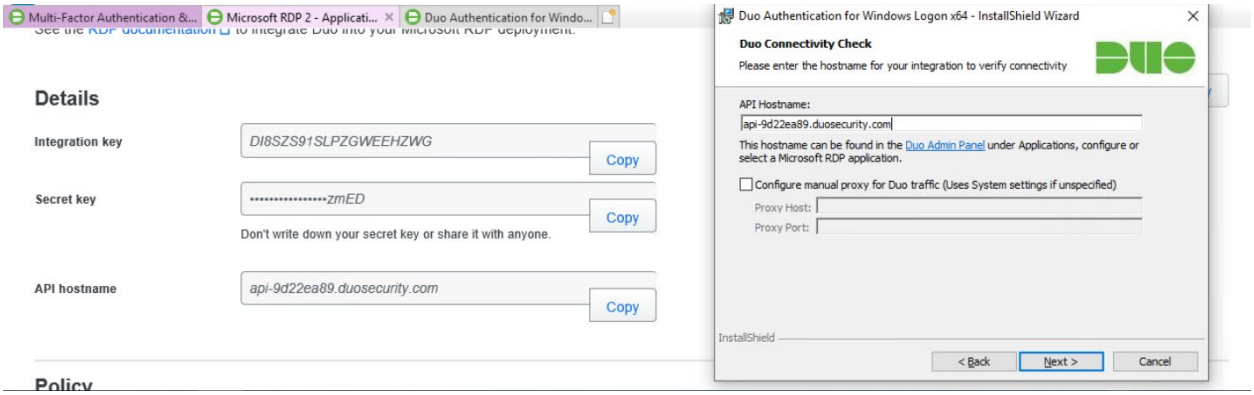
9. Download the **Duo Authentication for Windows Logon** installer package, located at https://dl.duosecurity.com/duo-win-login-latest.exe.

10. Run the downloaded EXE file.



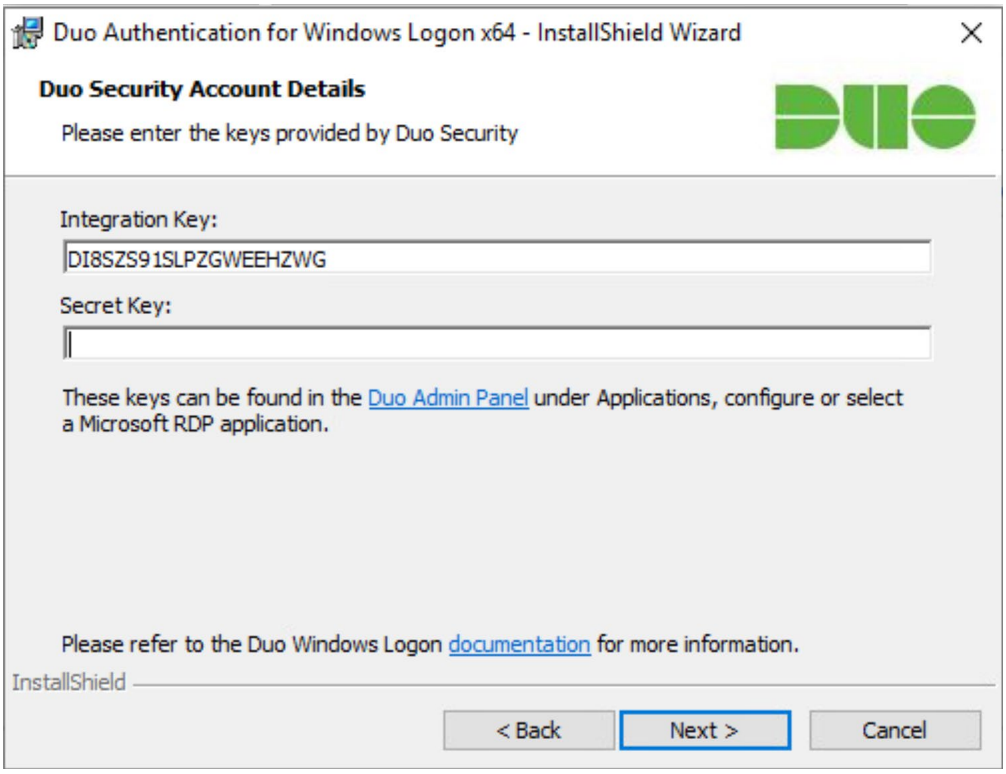
11. Click **Next**.

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



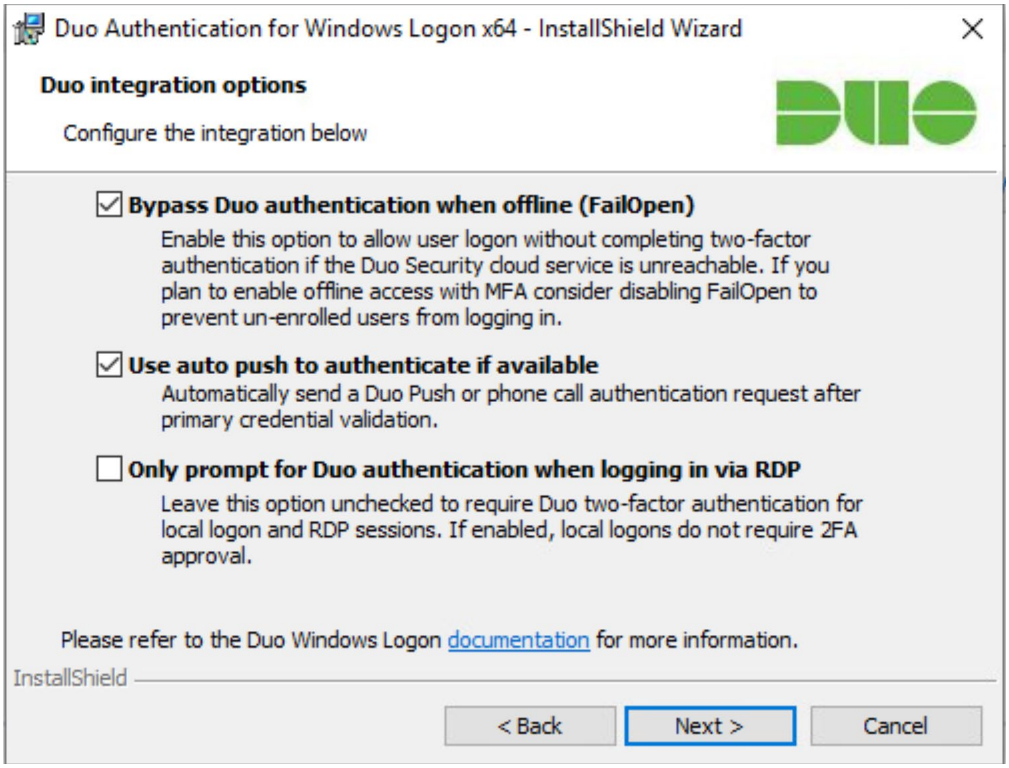
13. Click **Next**.

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



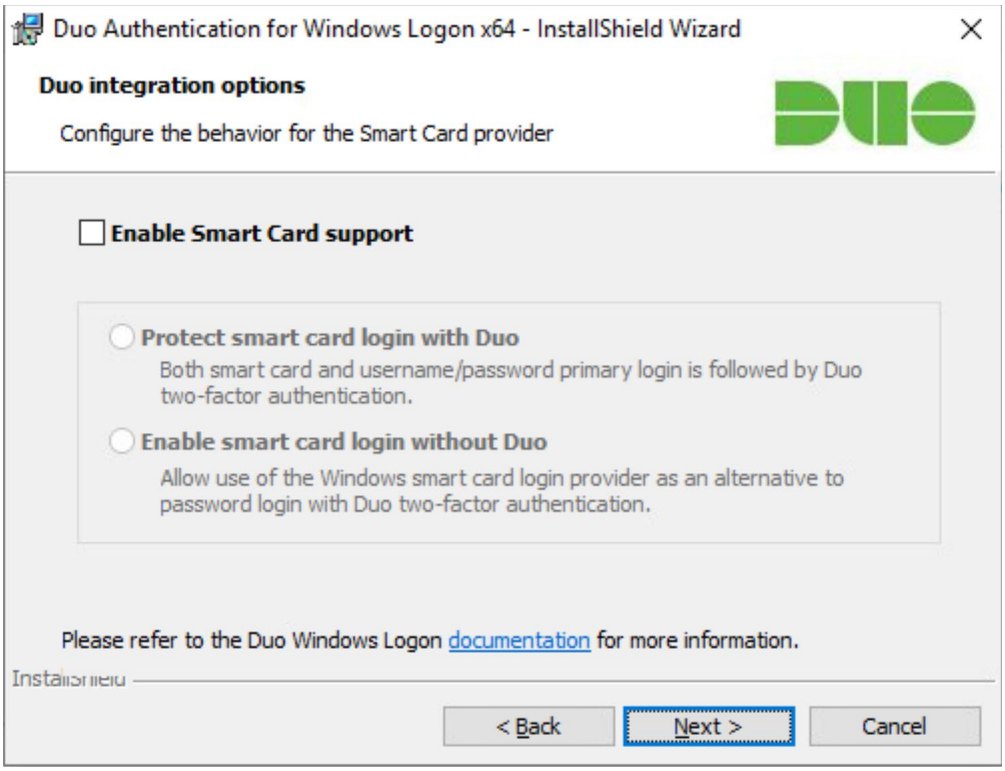
15. Click **Next**.

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.



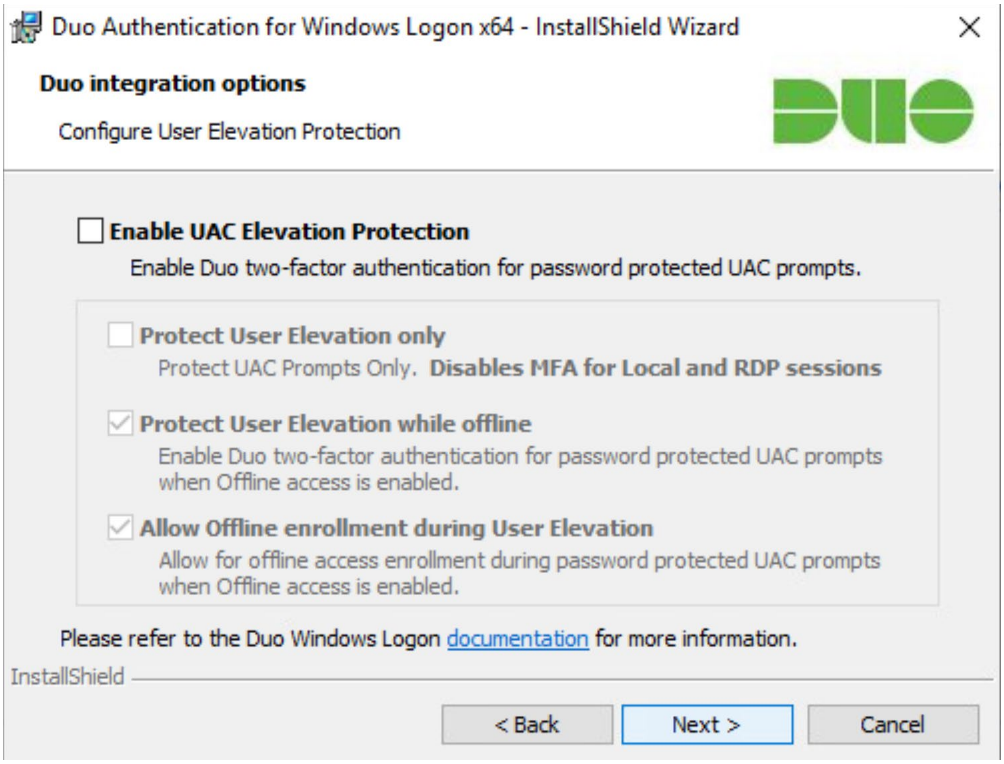
17. Click **Next**.

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

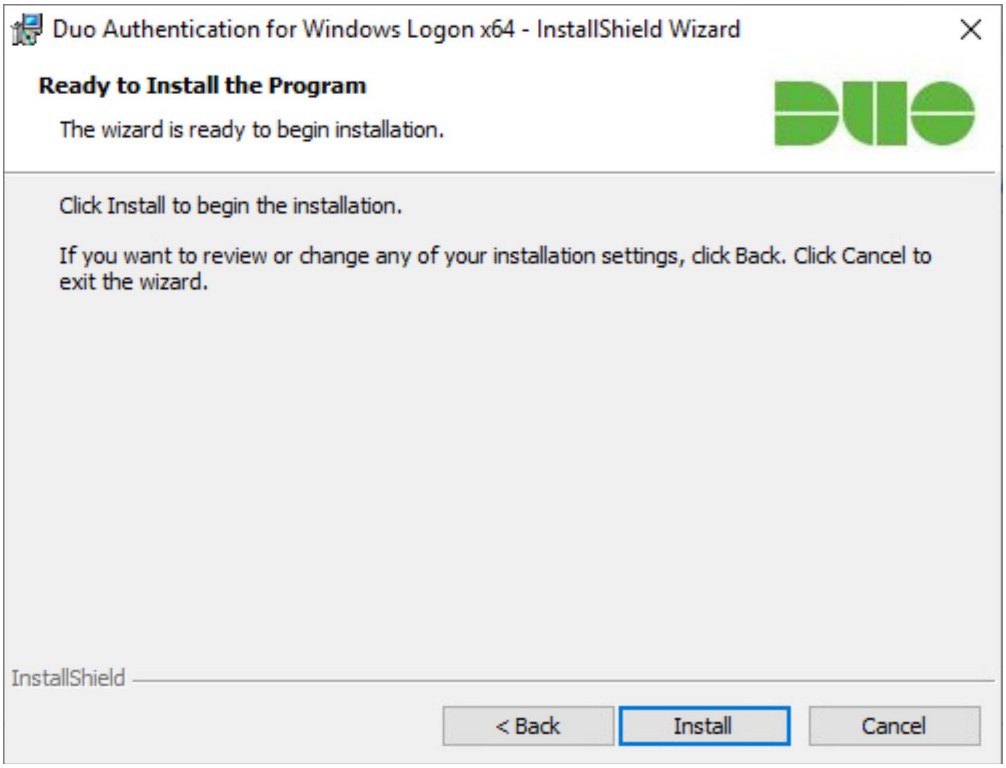


19. Click **Next**.

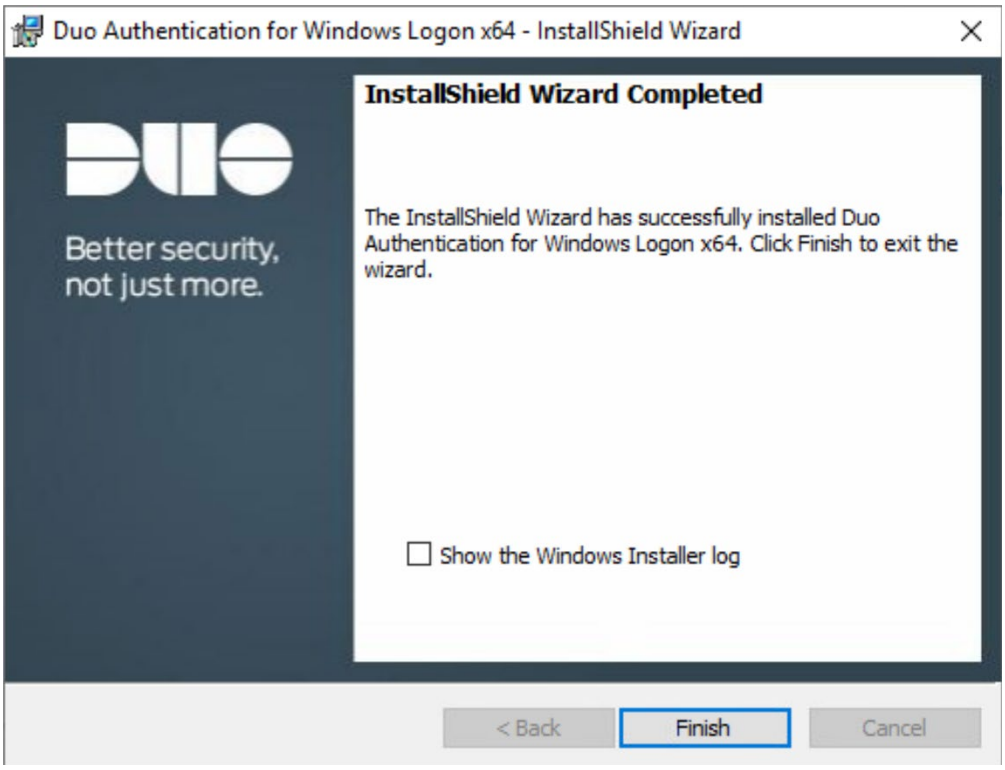
20. Leave **Enable UAC Elevation Protection** unchecked.



21. Click **Next**.



22. Click **Install**.

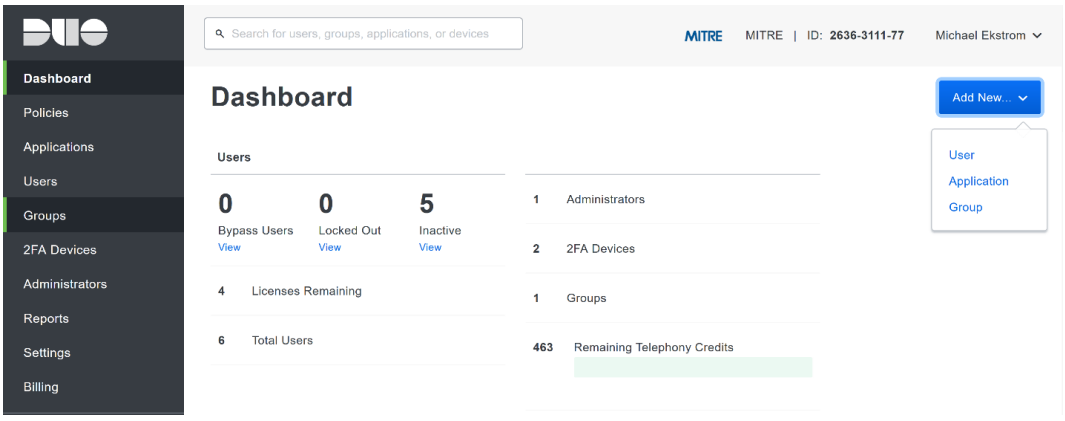


23. Click **Finish**.

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

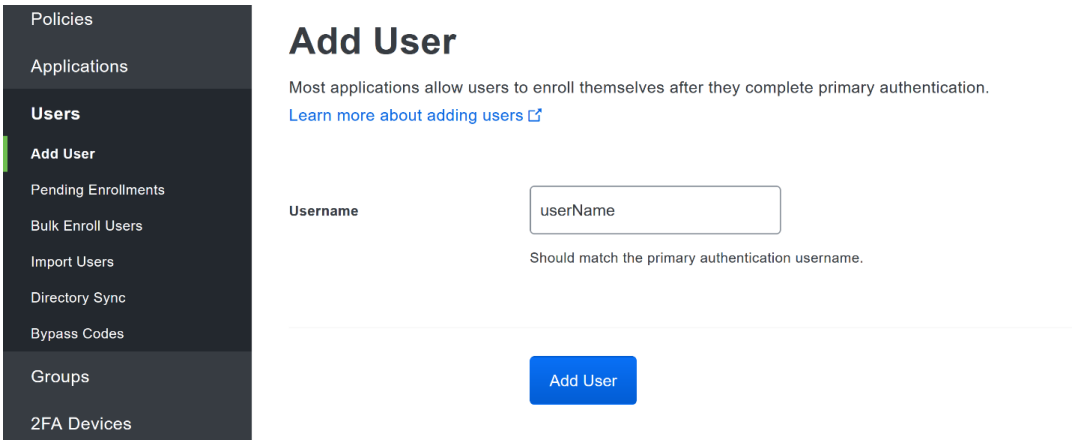
2.3.2 Registering a Duo User

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.*

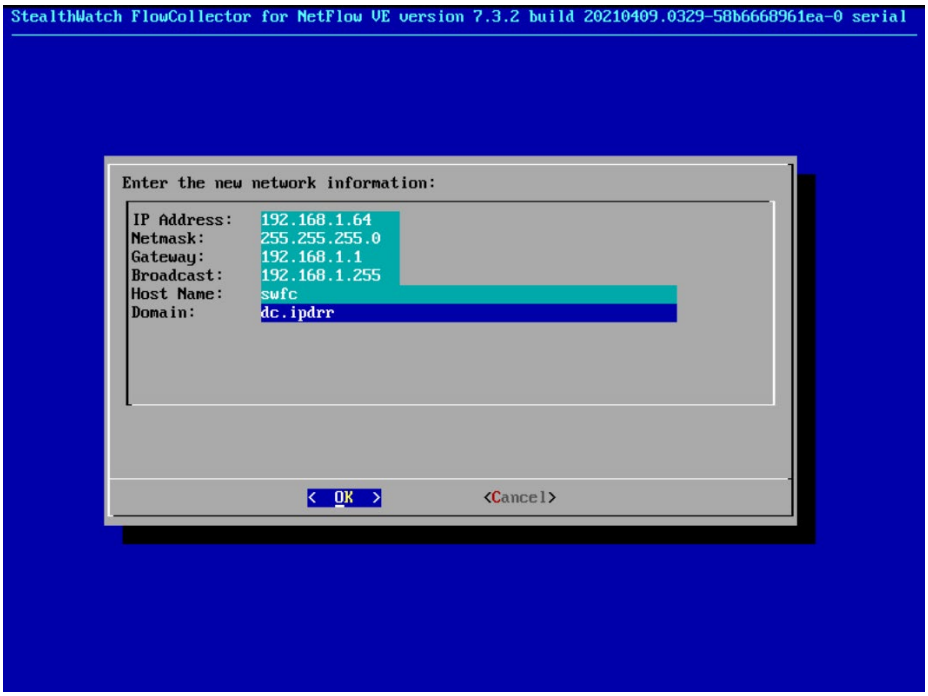
2.4 Cisco Stealthwatch

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.

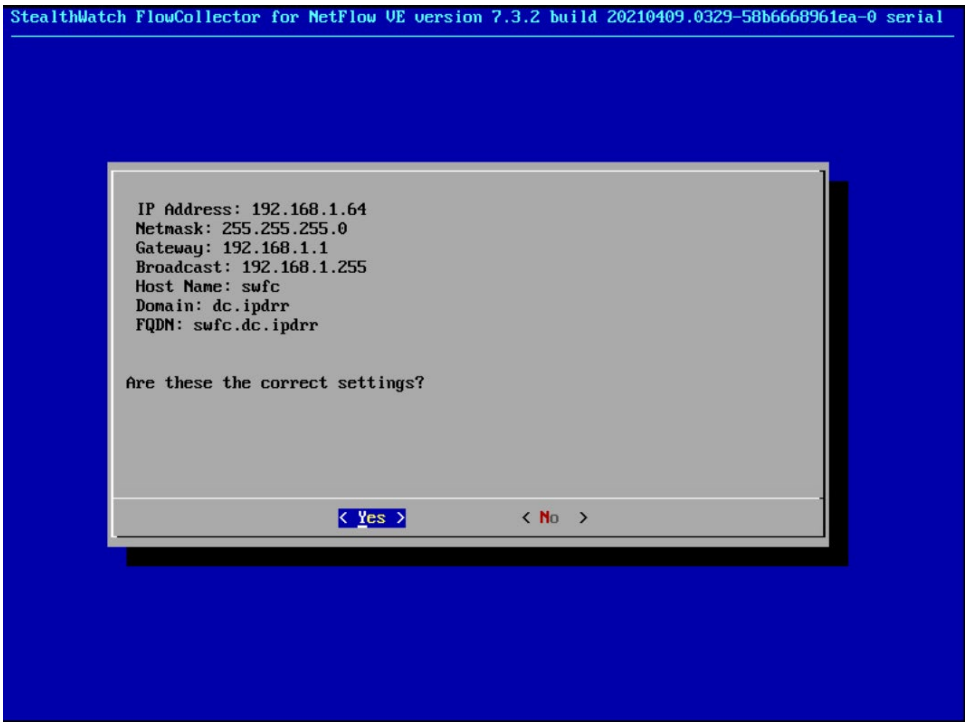
2. Enter the networking information for the machine.



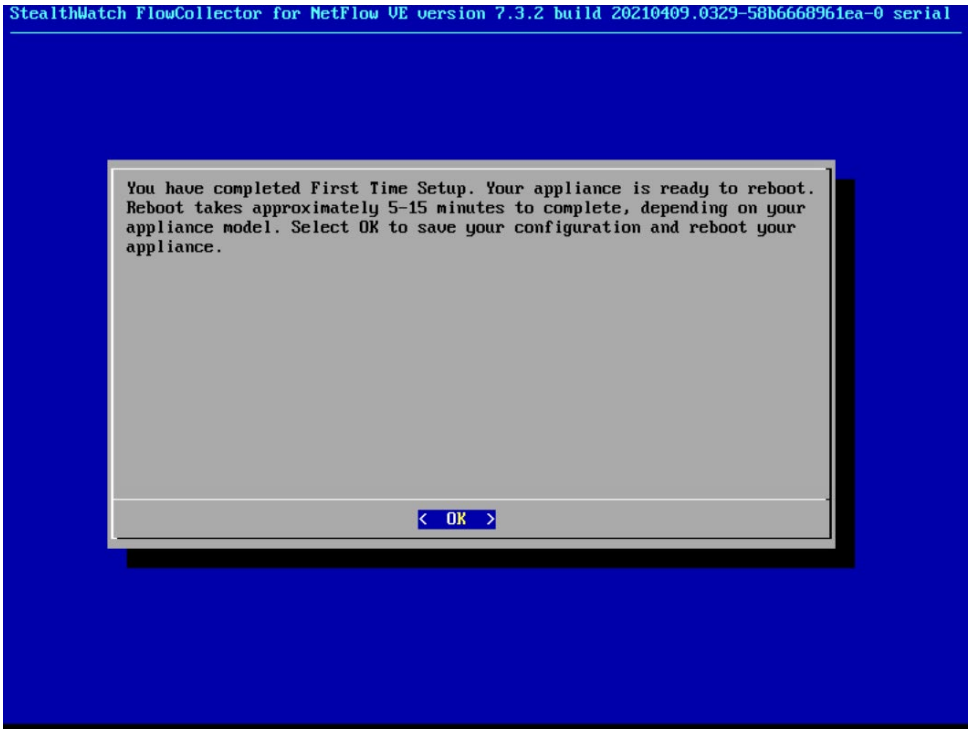
3. Select **OK** and press **Enter**.

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

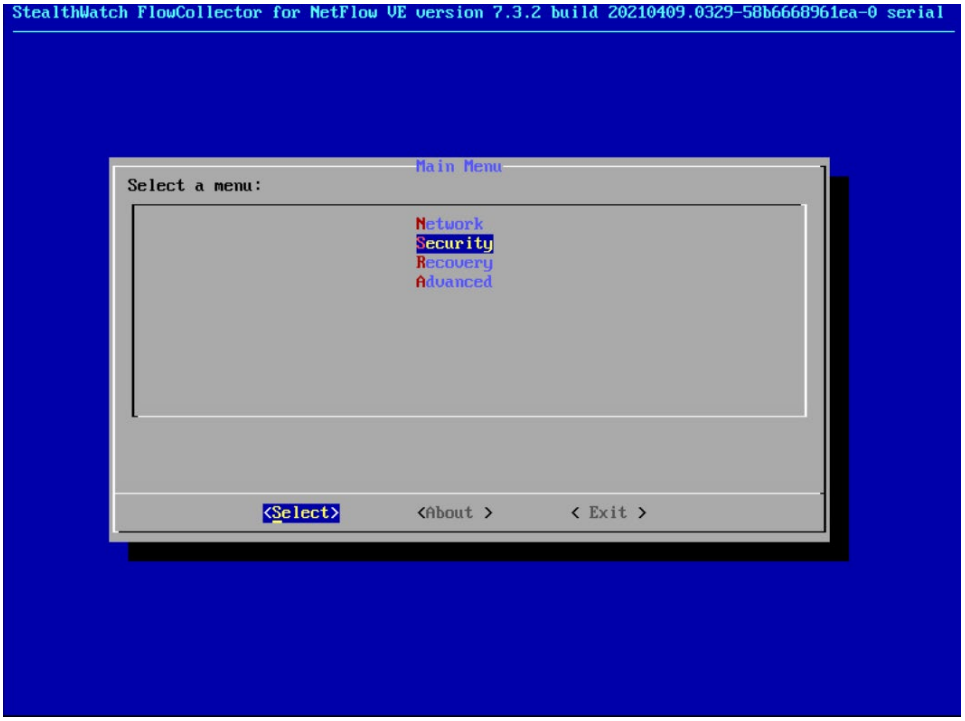
5. Confirm the settings.



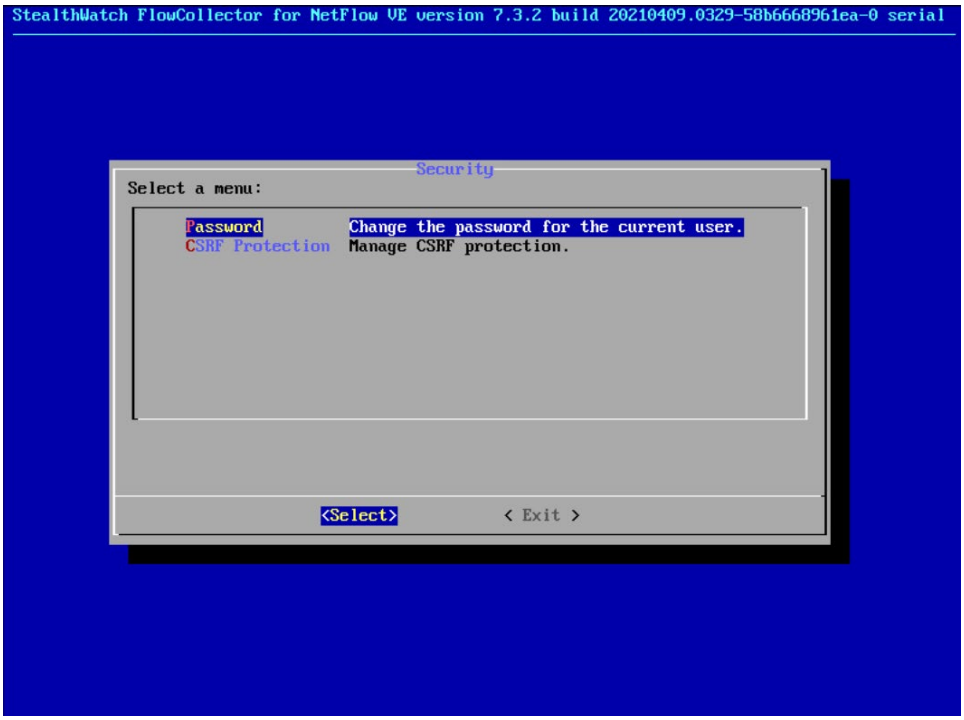
6. Select **Yes** and press **Enter**.



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



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



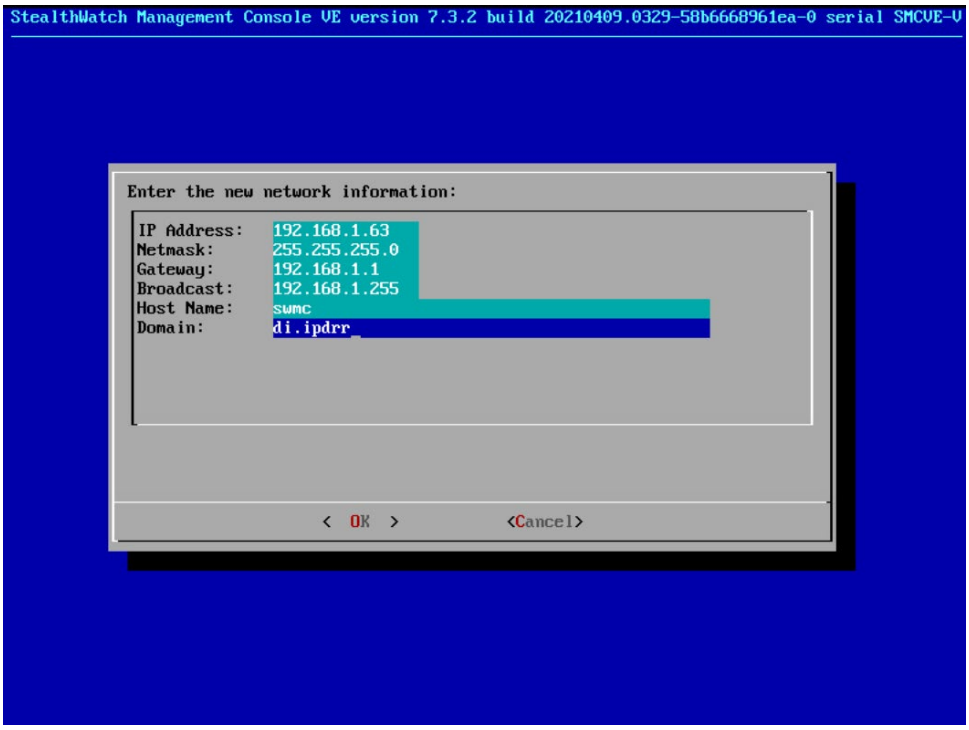
9. Select **Password** and press **Enter**.

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

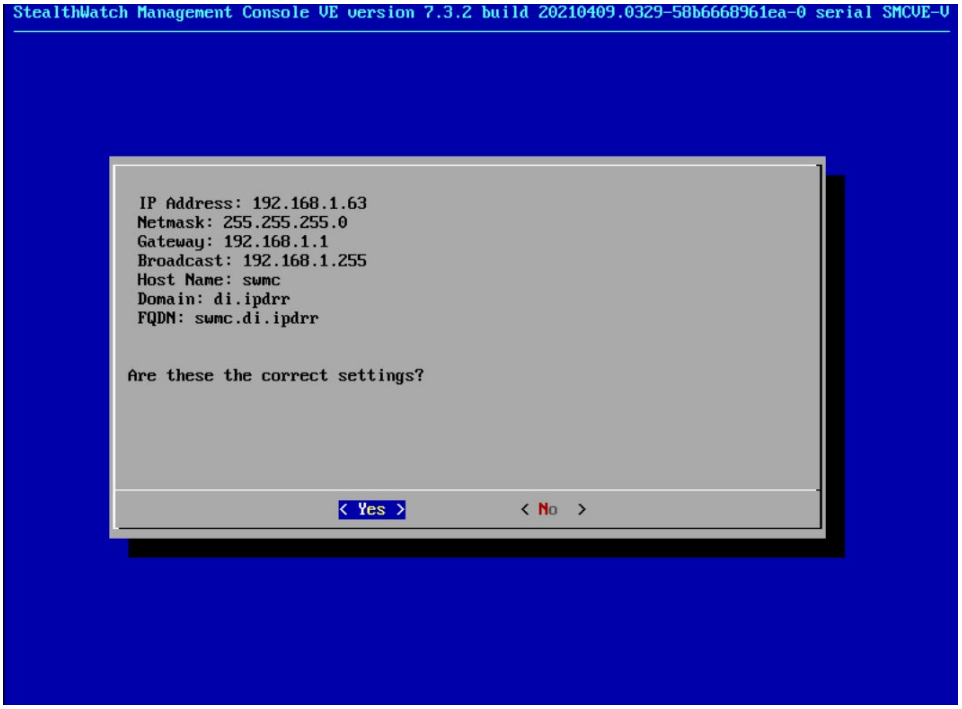
2.4.2 Configure Stealthwatch Management Console

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

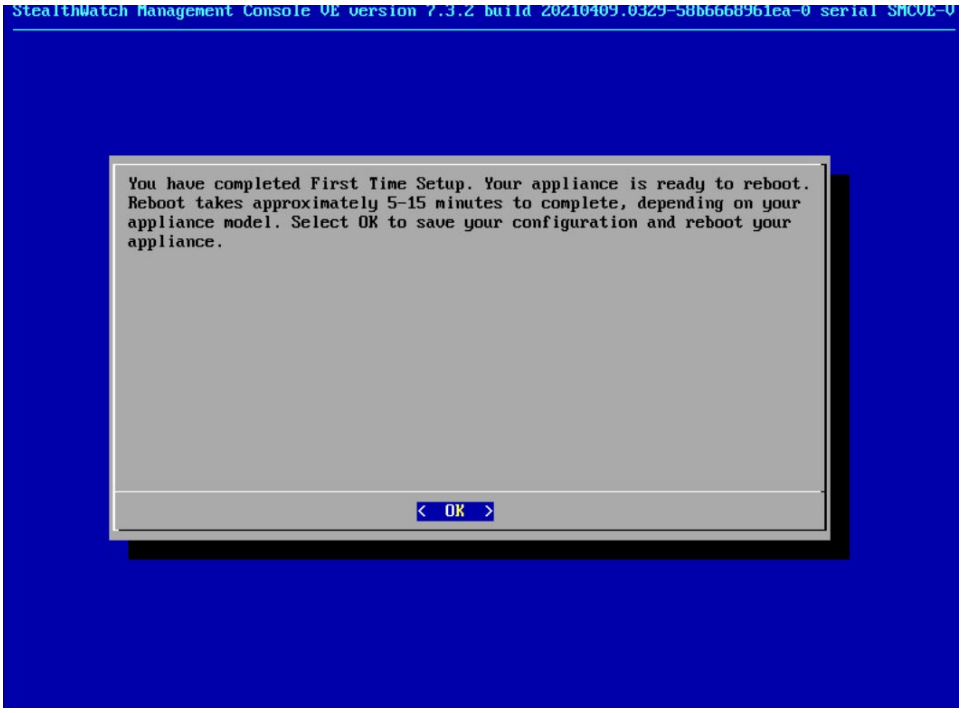
2. Enter the networking information for the machine.



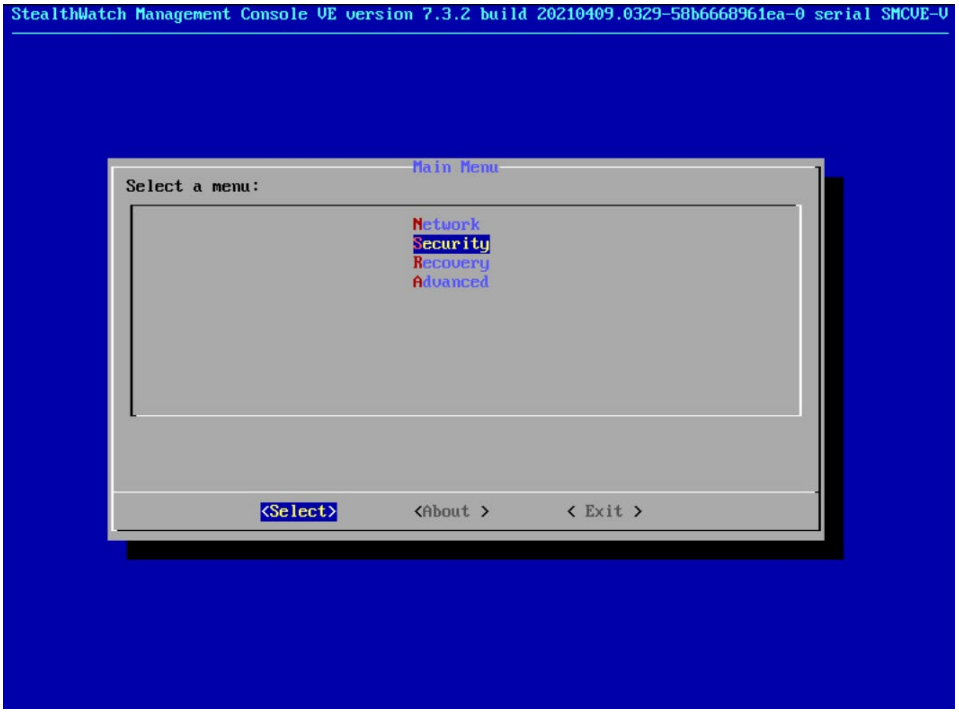
3. Select **OK** and press **Enter**.



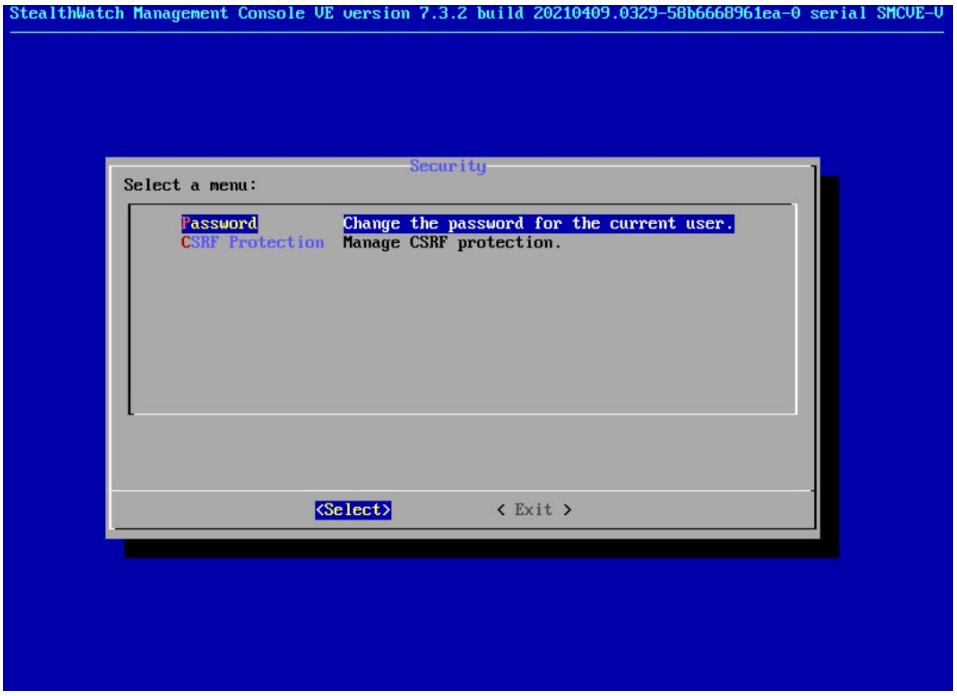
4. Select **Yes** and press **Enter**.



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



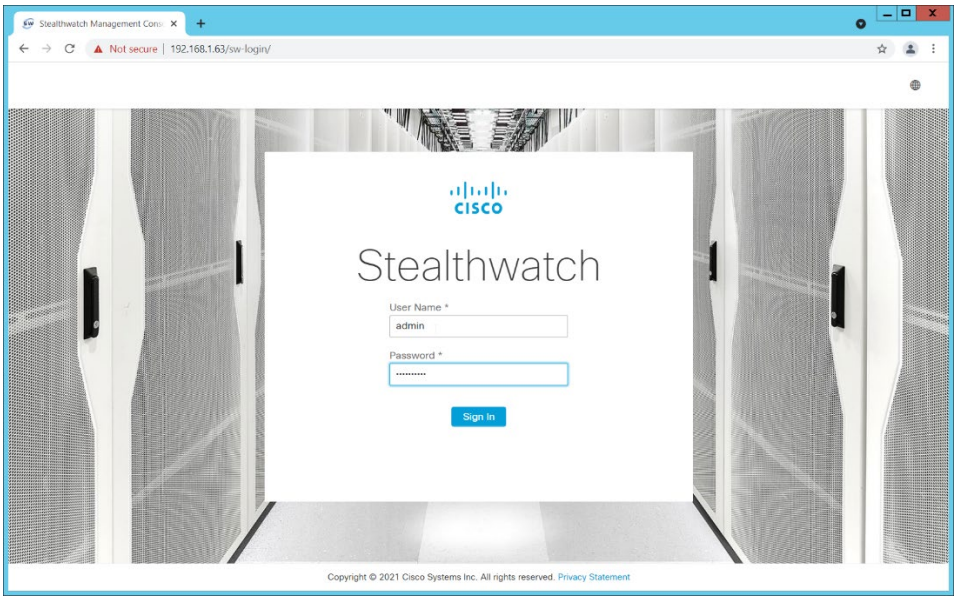
6. Once the machine restarts, navigate to **Security**, and press **Enter**.



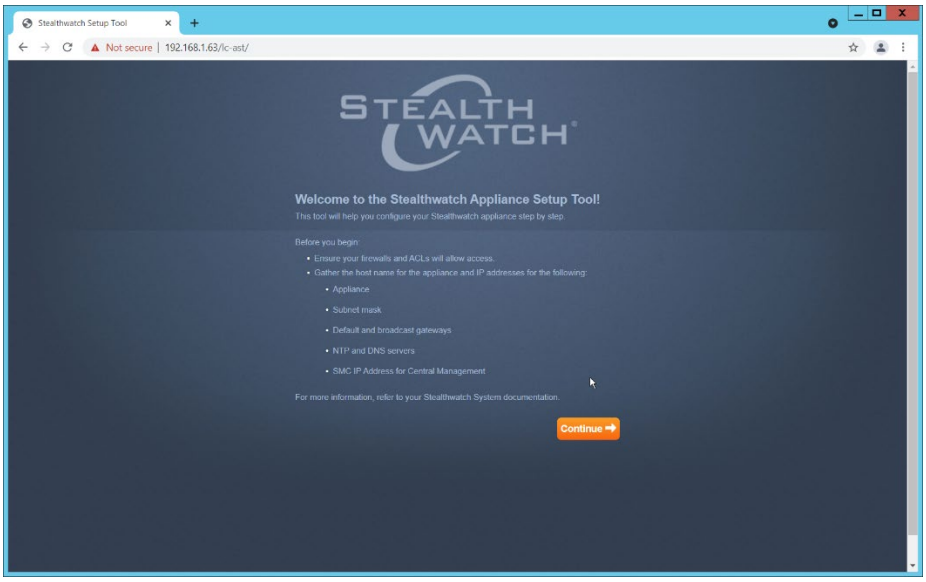
7. Select **Password** and press **Enter**.

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*>>.

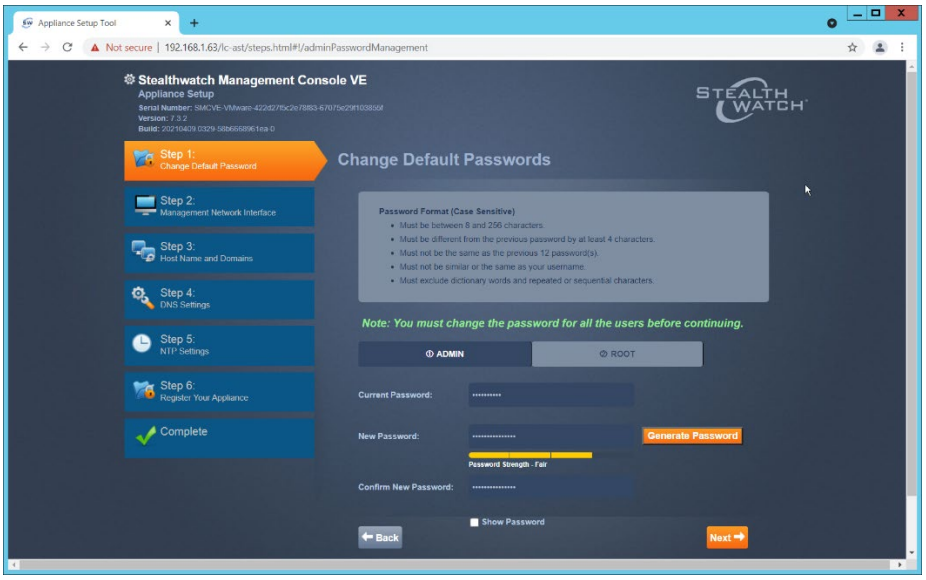


10. Login using the default username and password (should be provided by product vendor).



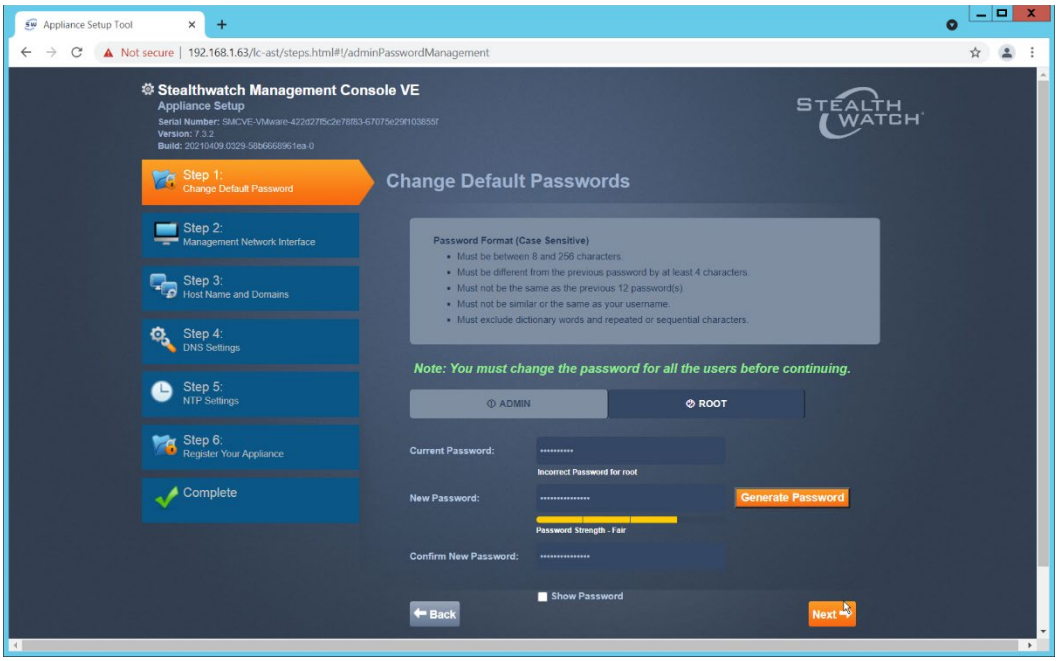
11. Click **Continue**.

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



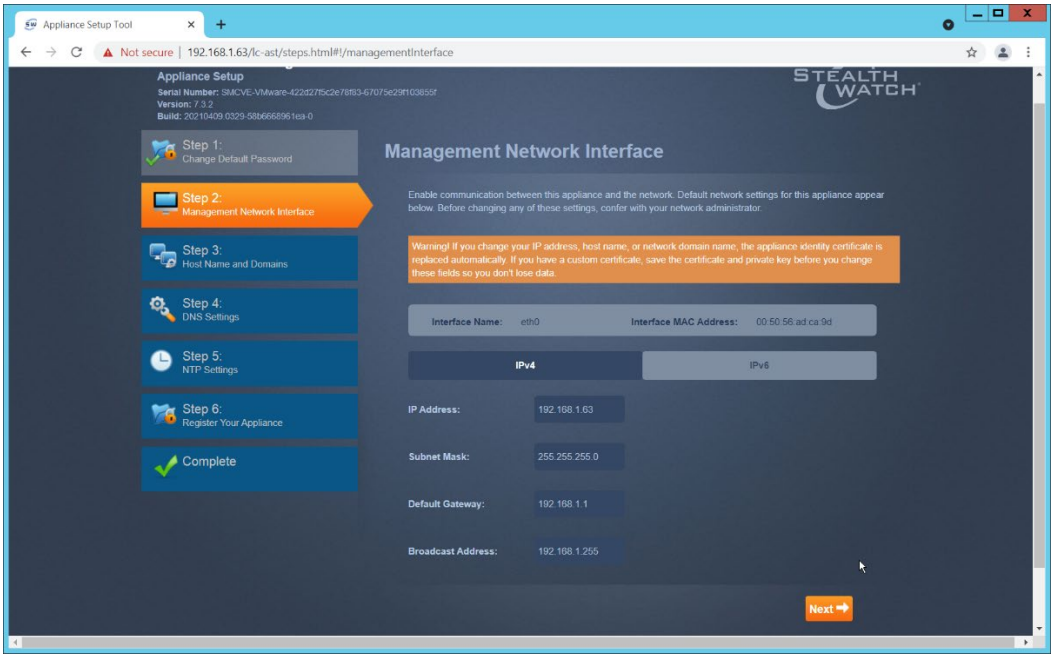
13. Click **Next**.

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

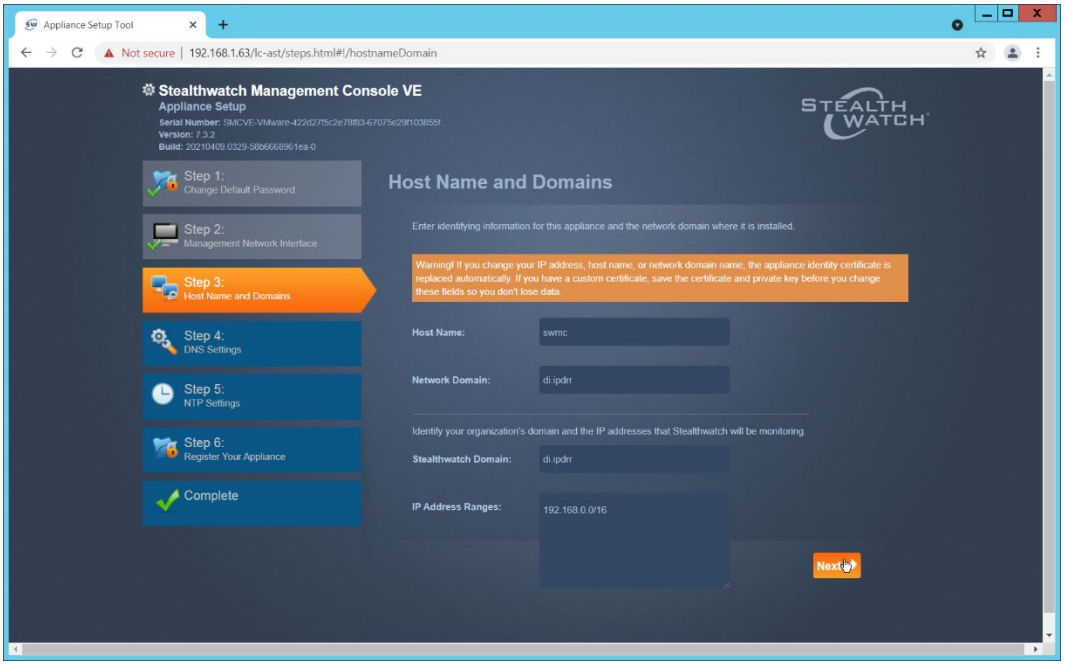


15. Click **Next**.

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

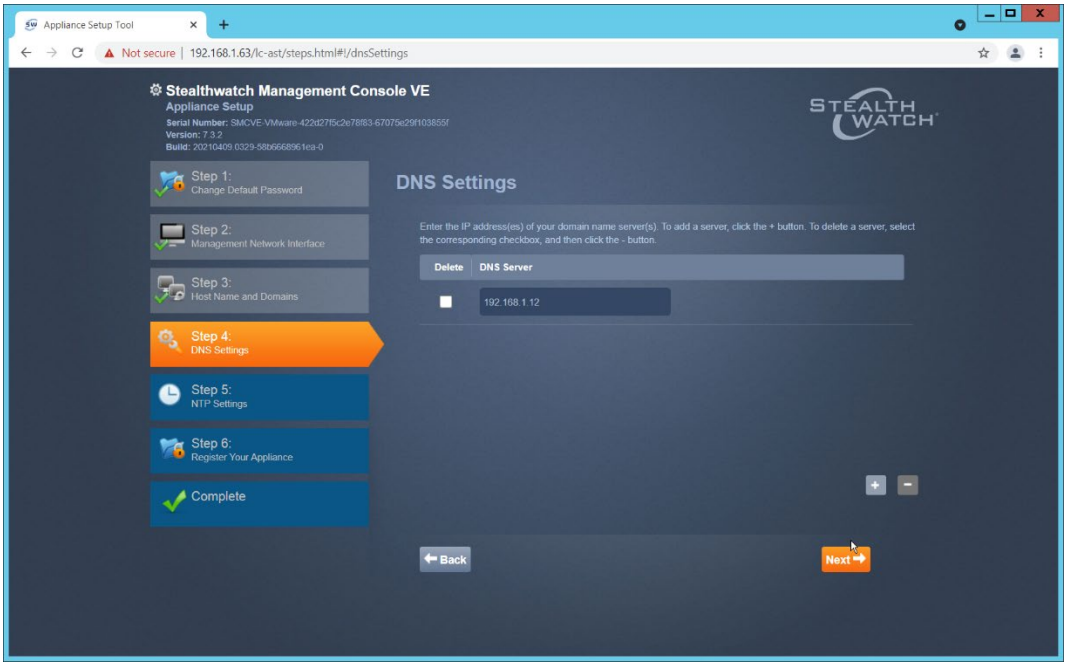


17. Enter the domain for Stealthwatch, and the IP addresses Stealthwatch will be monitoring.



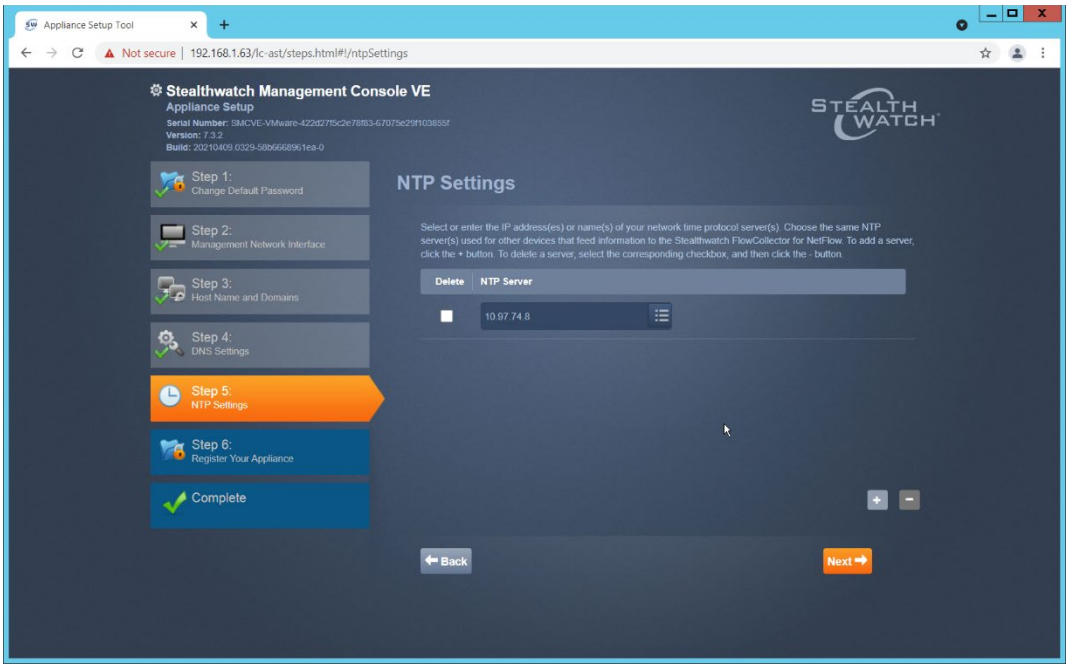
18. Click **Next**.

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

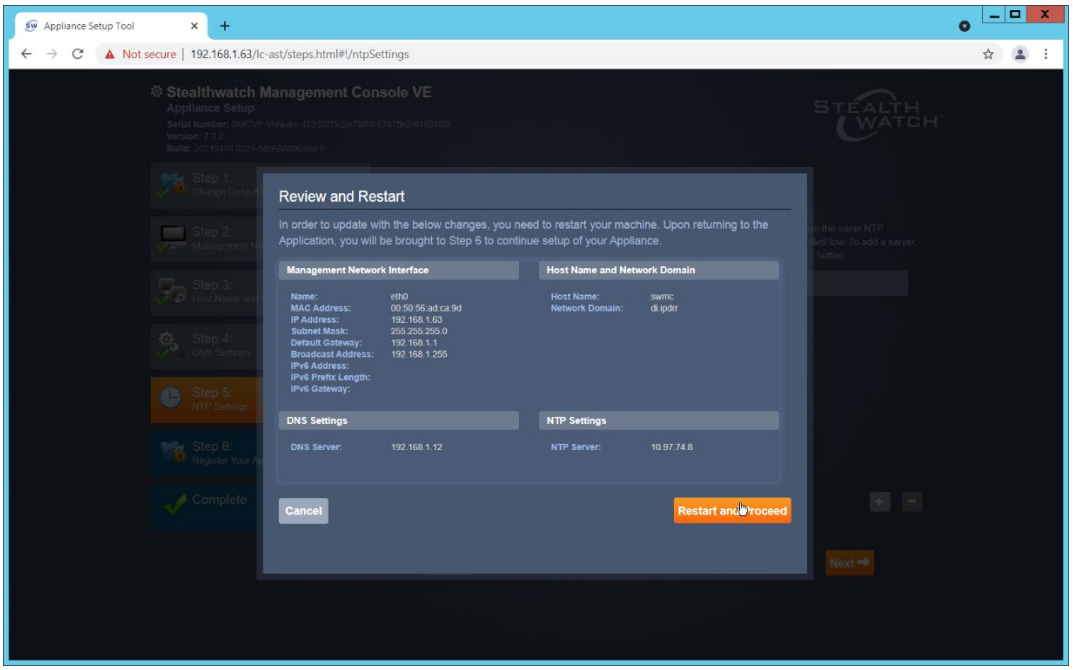


20. Click **Next**.

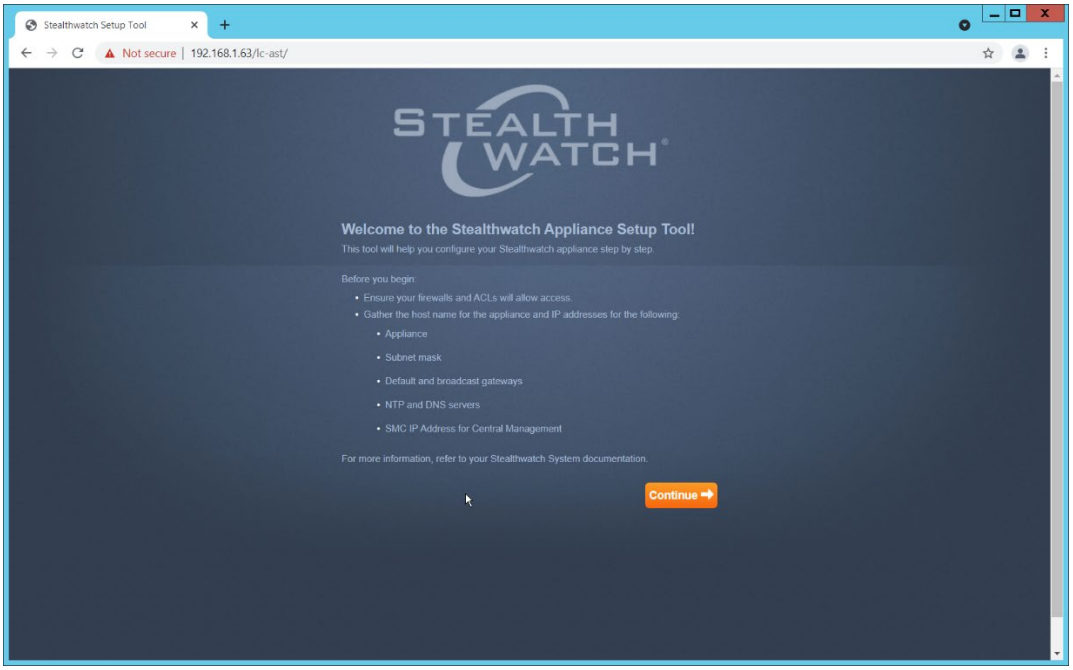
21. Enter the Network Time Protocol (NTP) server(s) Stealthwatch should use.



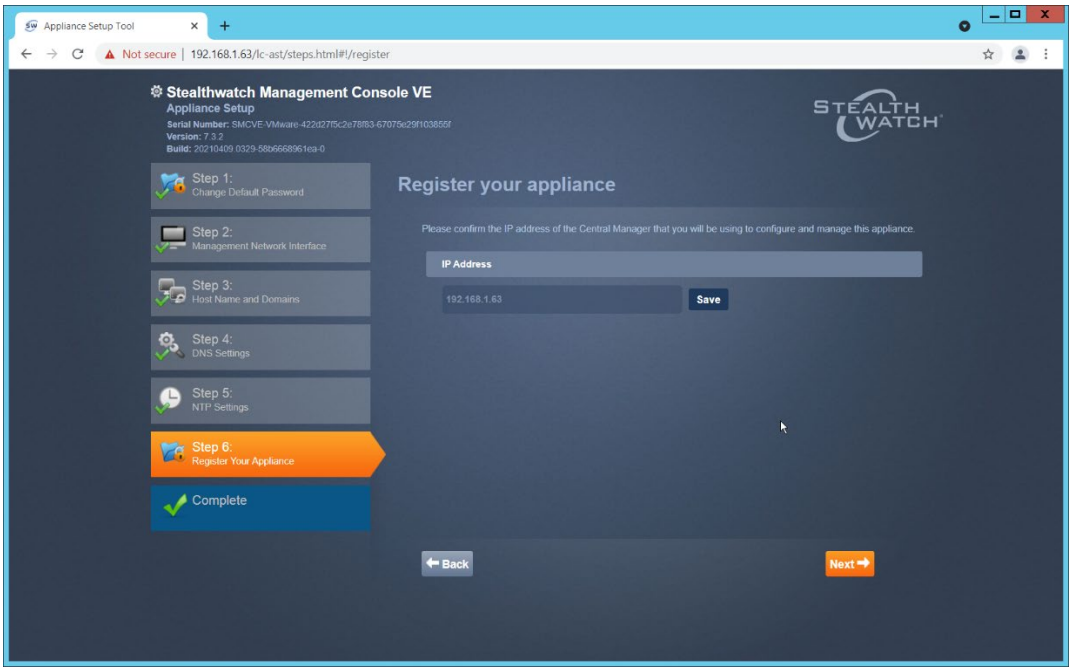
22. Click **Next**.



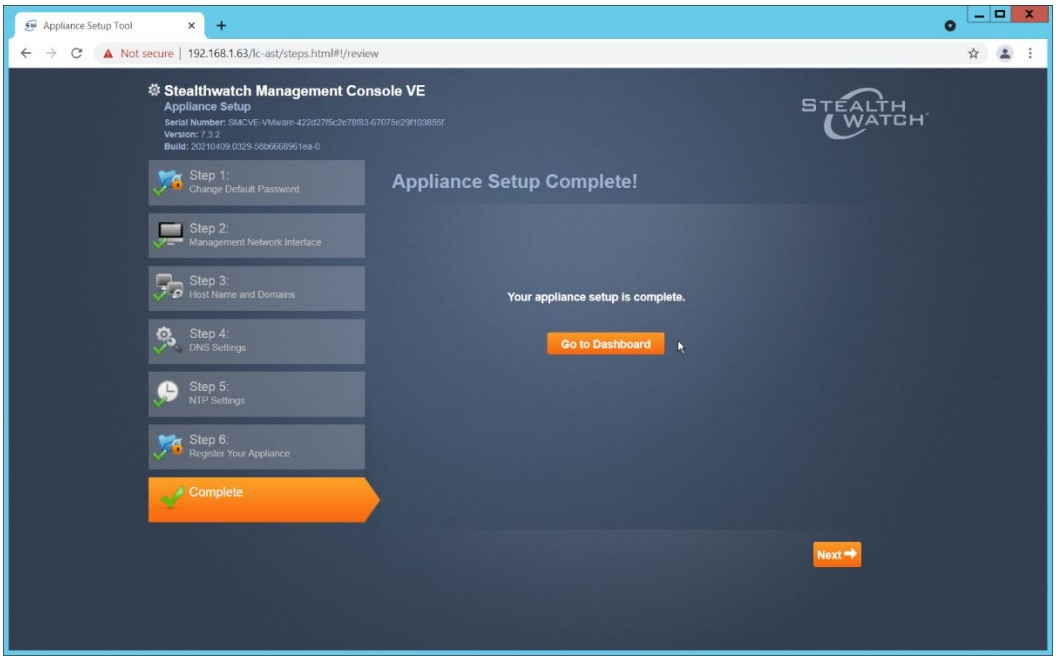
23. Click **Restart and Proceed**.



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



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

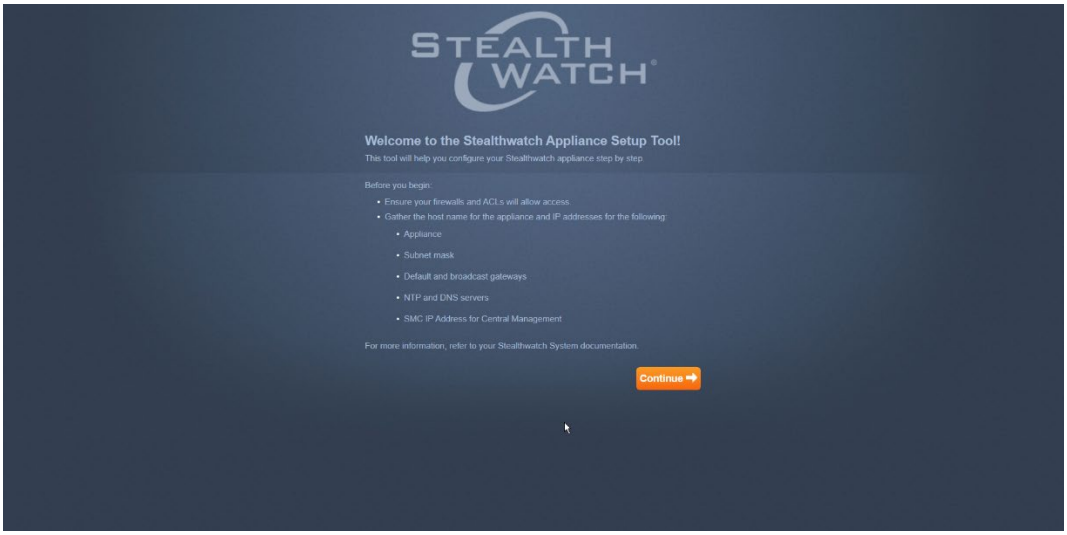


26. Click **Go to Dashboard**.

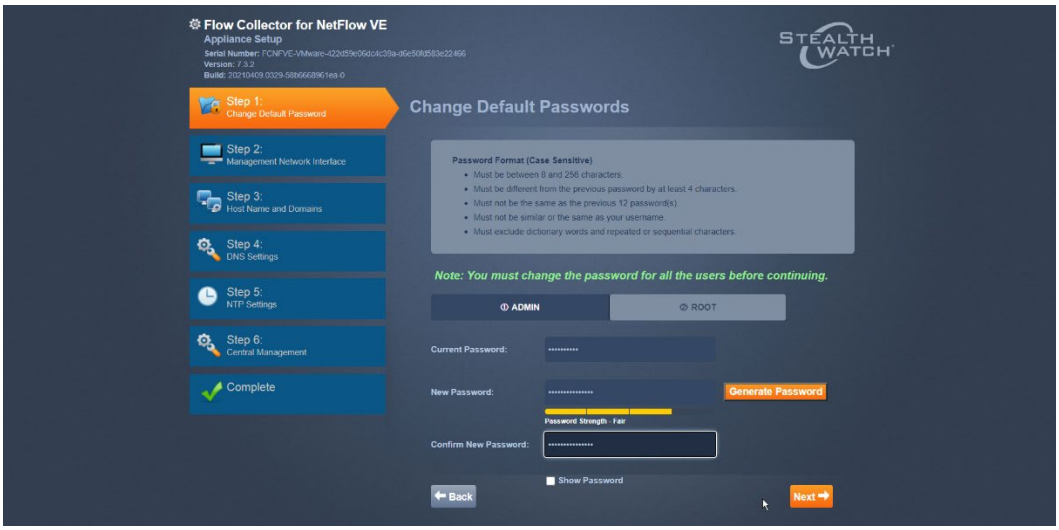
2.4.3 Add Stealthwatch Flow Collector to the Management Console

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).

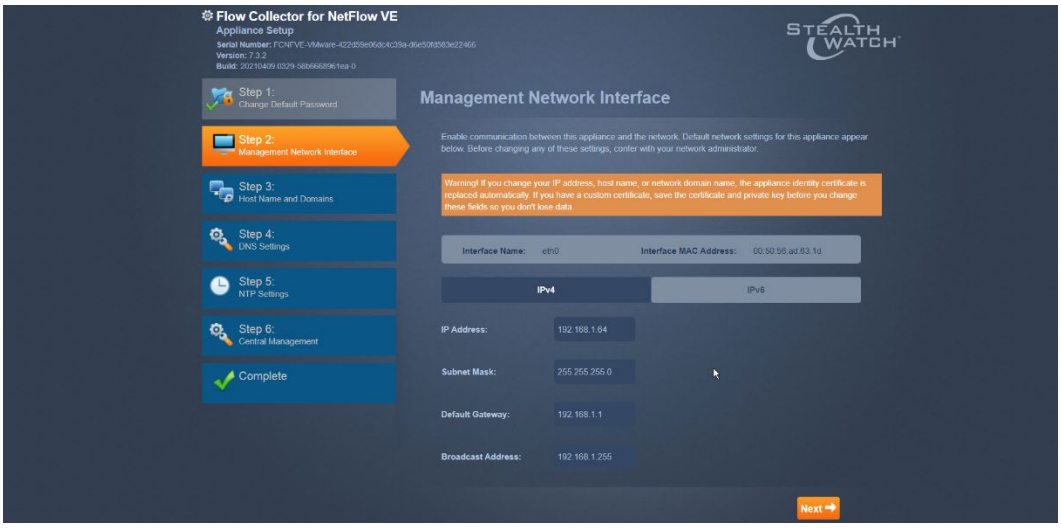


3. Click **Continue**.



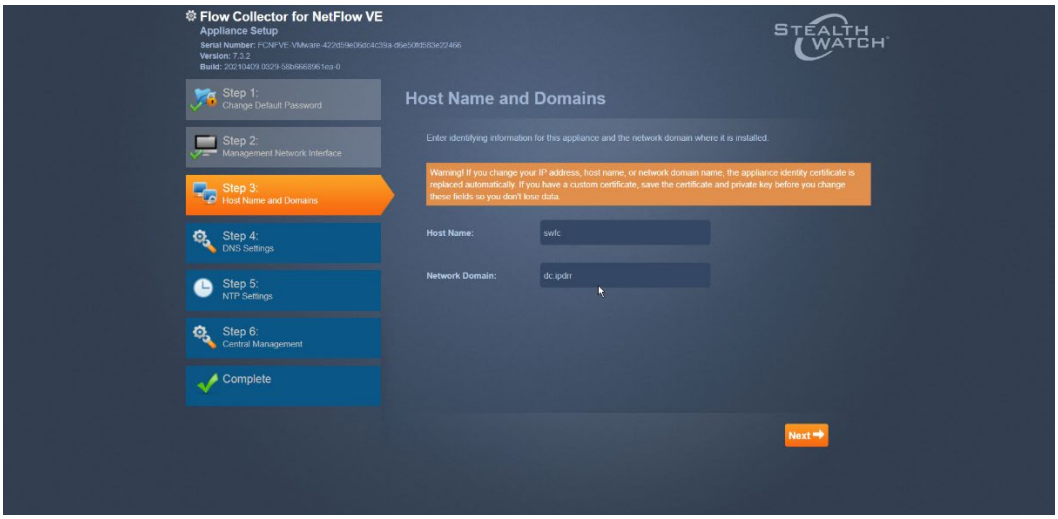
4. Change the passwords for the admin and root accounts.

5. Click **Next**.



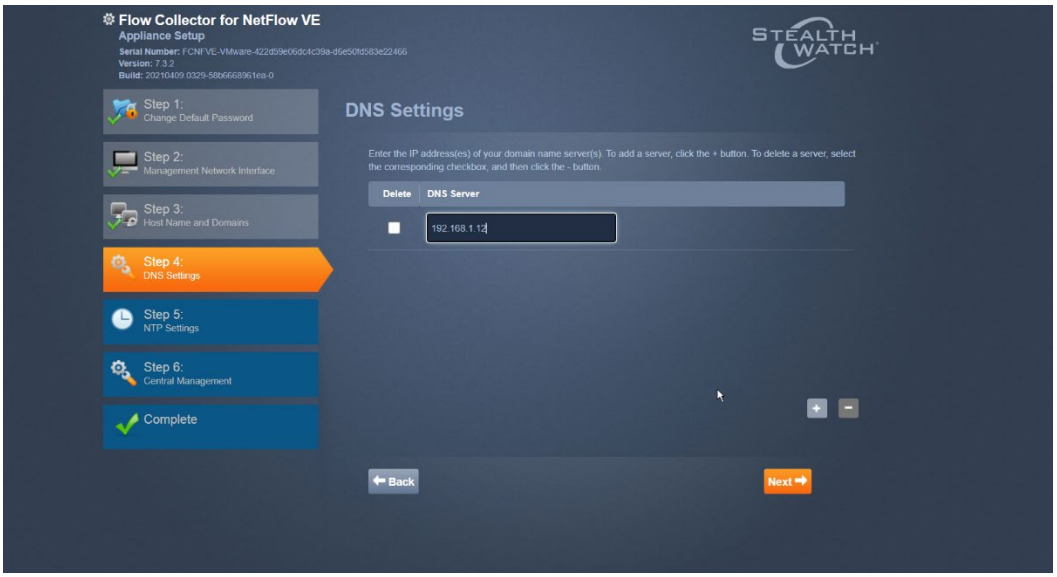
6. Confirm the networking information is correct and click **Next**.

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



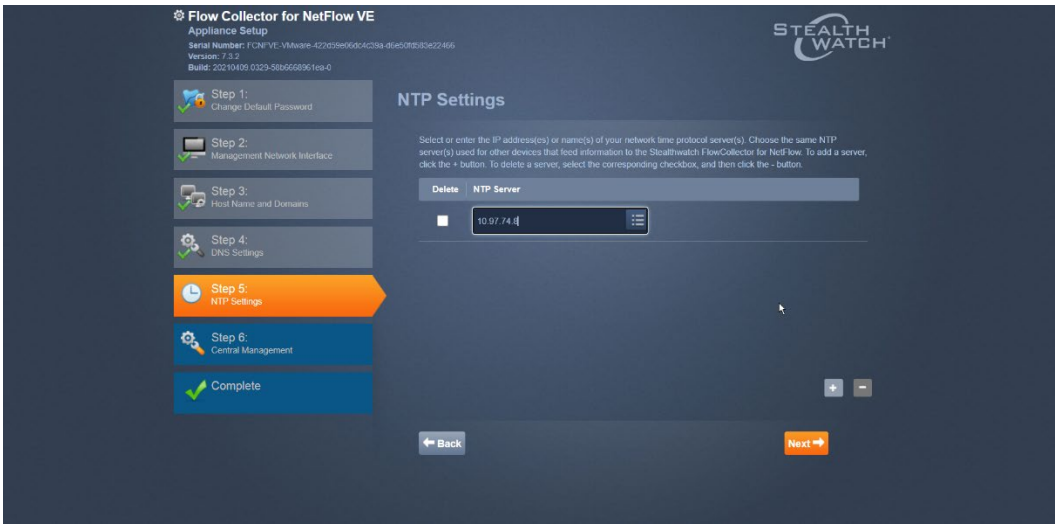
8. Click **Next**.

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

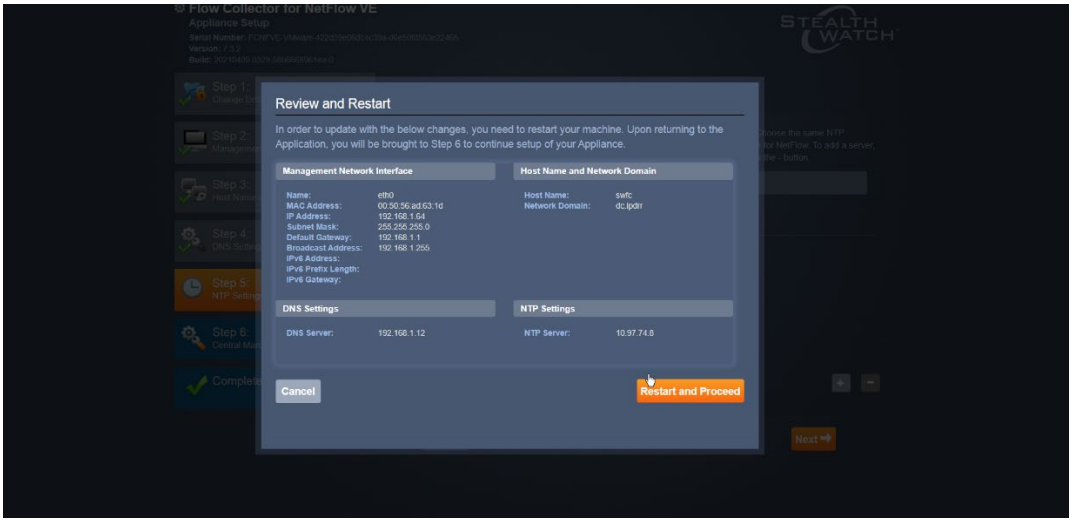


10. Click **Next**.

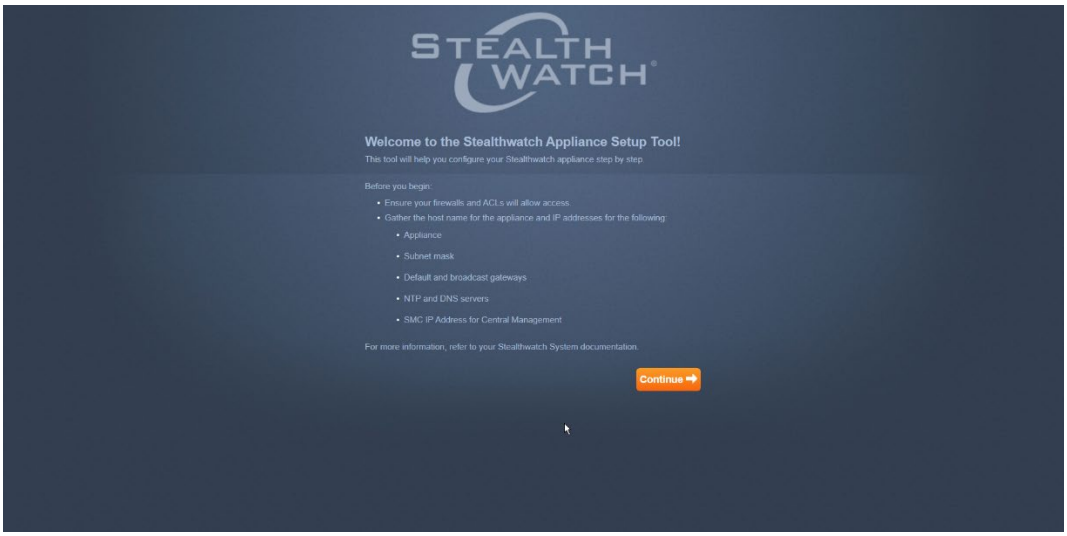
11. Enter the NTP server(s) Stealthwatch should use.



12. Click **Next**.

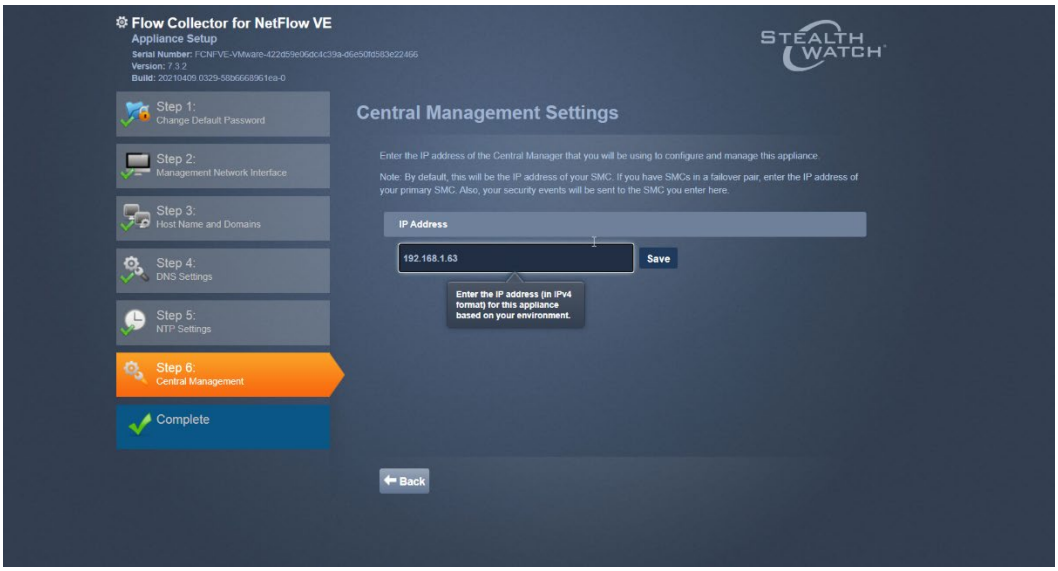


13. Click **Restart and Proceed**.

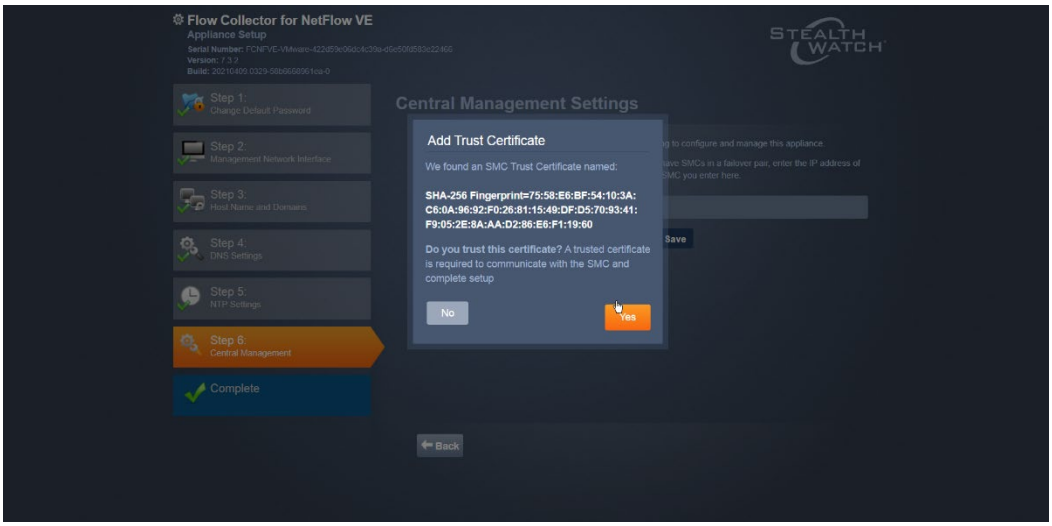


14. After it restarts, log in again, and click **Continue**.

15. Enter the IP of the Stealthwatch Management Console.

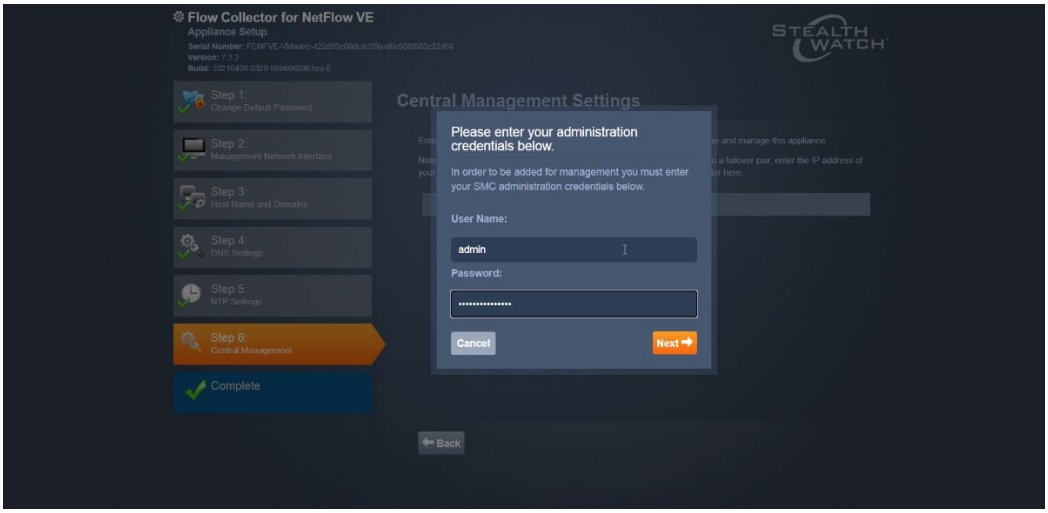


16. Click **Save**.



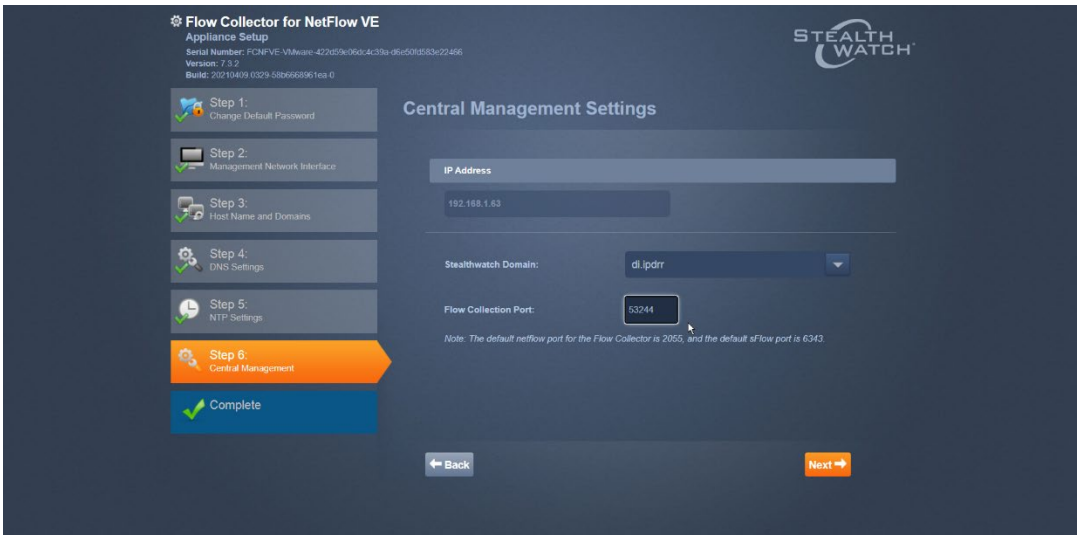
17. Accept the certificate by clicking **Yes**.

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

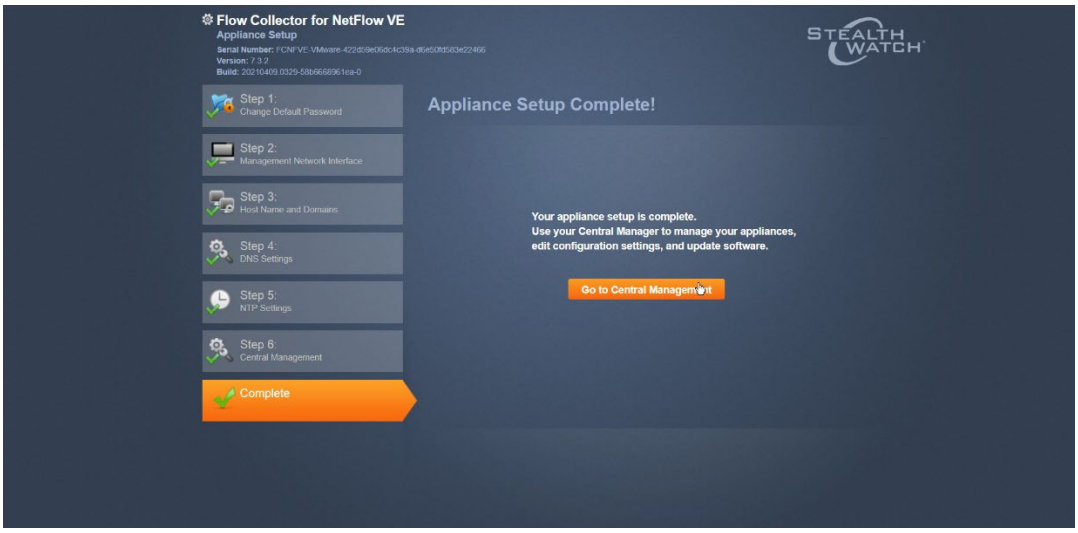


19. Click **Next**.

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.

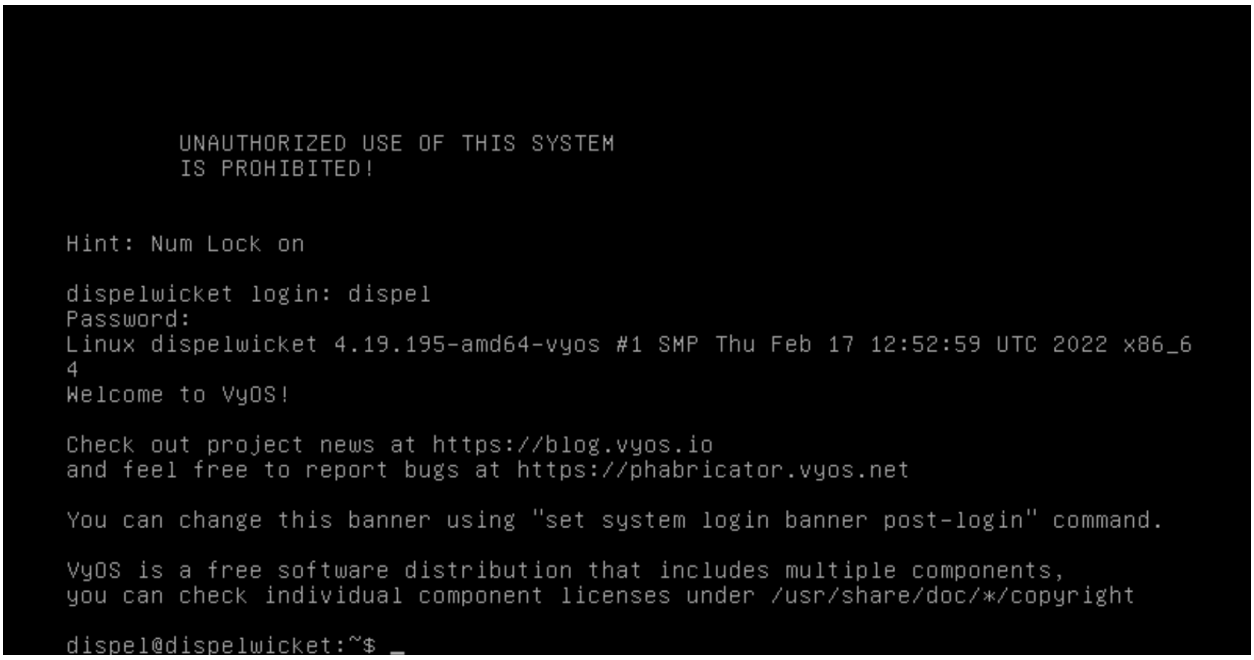
```
Enter password for administrator account
Enter password for user 'dispel':
Retype password for user 'dispel':
I need to install the GRUB boot loader.
I found the following drives on your system:
 sda    150323MB


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

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

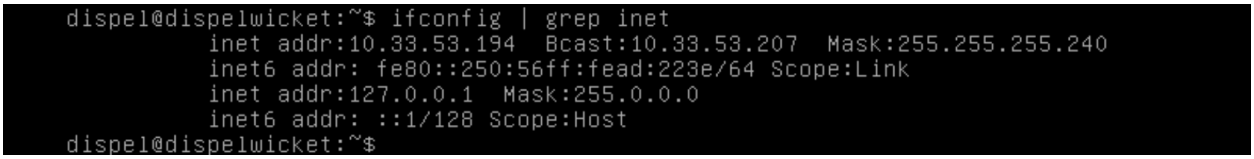
```
Which drive should GRUB modify the boot partition on? [sda]:

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`.

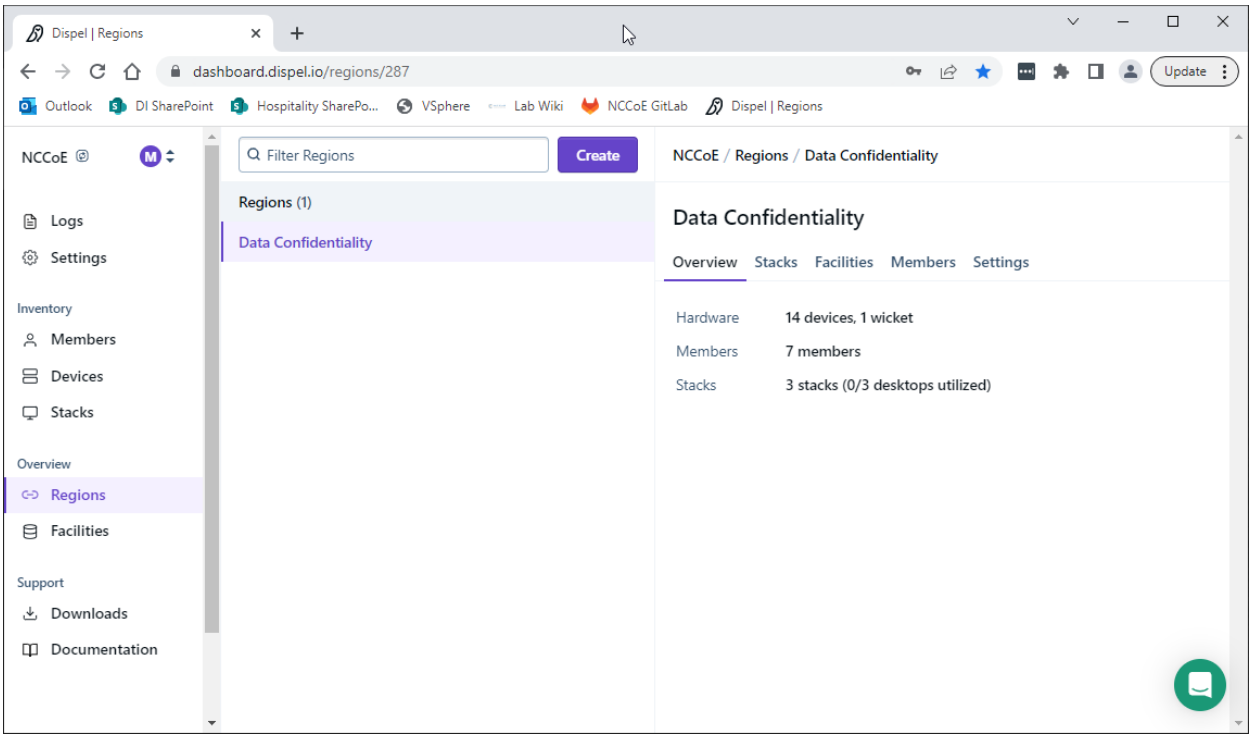
```
dispel@dispelwicket# exit
exit
dispel@dispelwicket:~$
```

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.

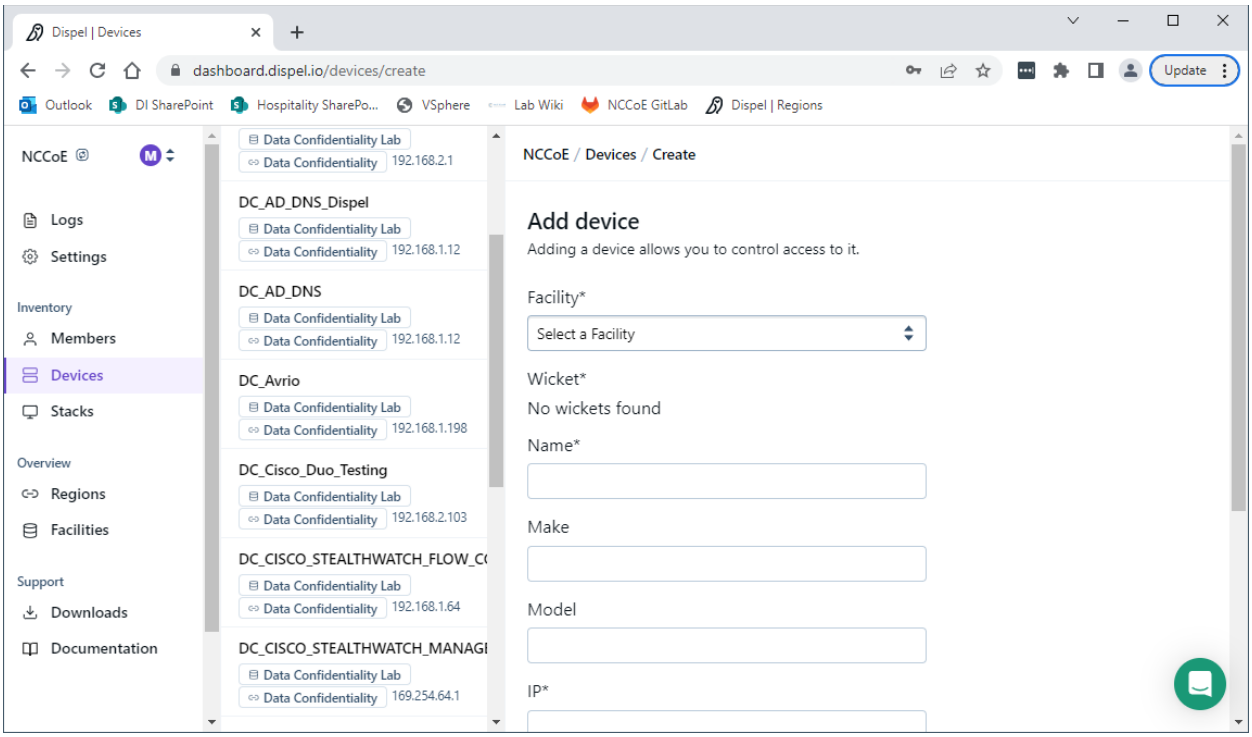
7. Modify the IP addresses of the south-side network interface to properly align with your network. See the “Configuring IP Addresses” section above.

2.5.4 Adding a Device

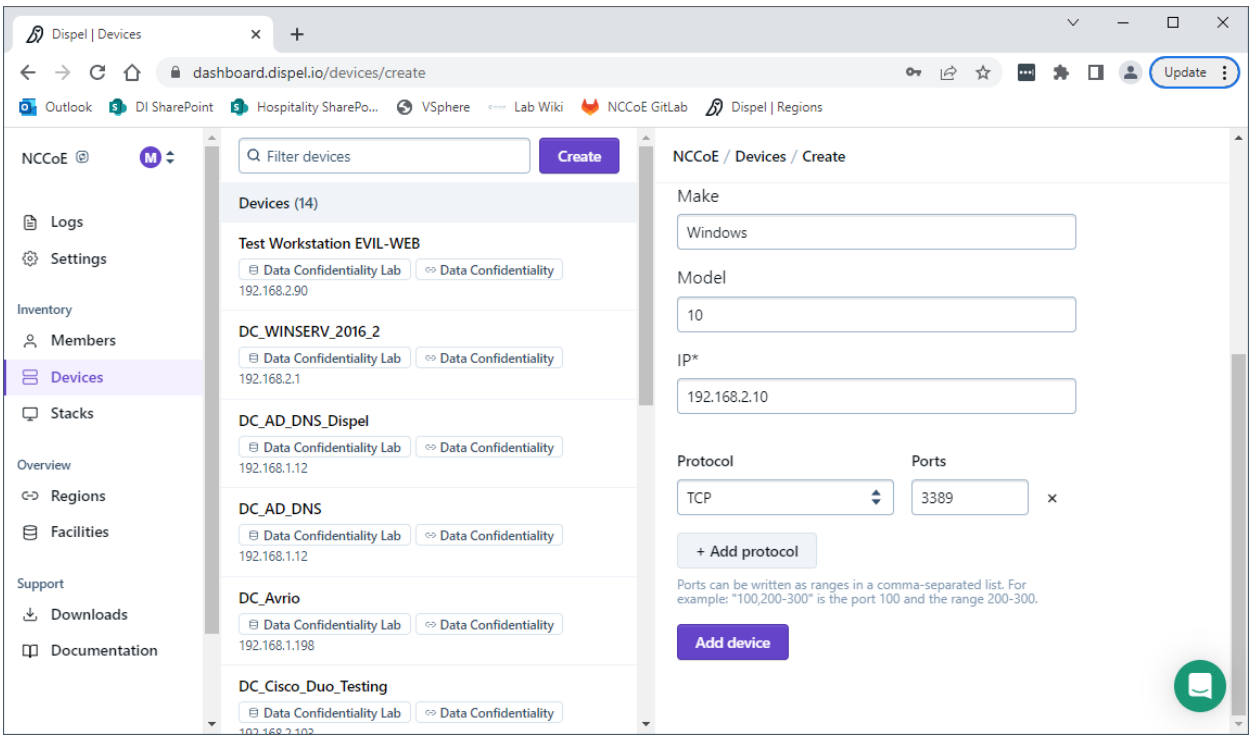
1. On the workstation in question, ensure that ping and RDP are accessible, including allowing such connections through a local firewall.
2. Authenticate to the Dispel webpage with the provided credentials.



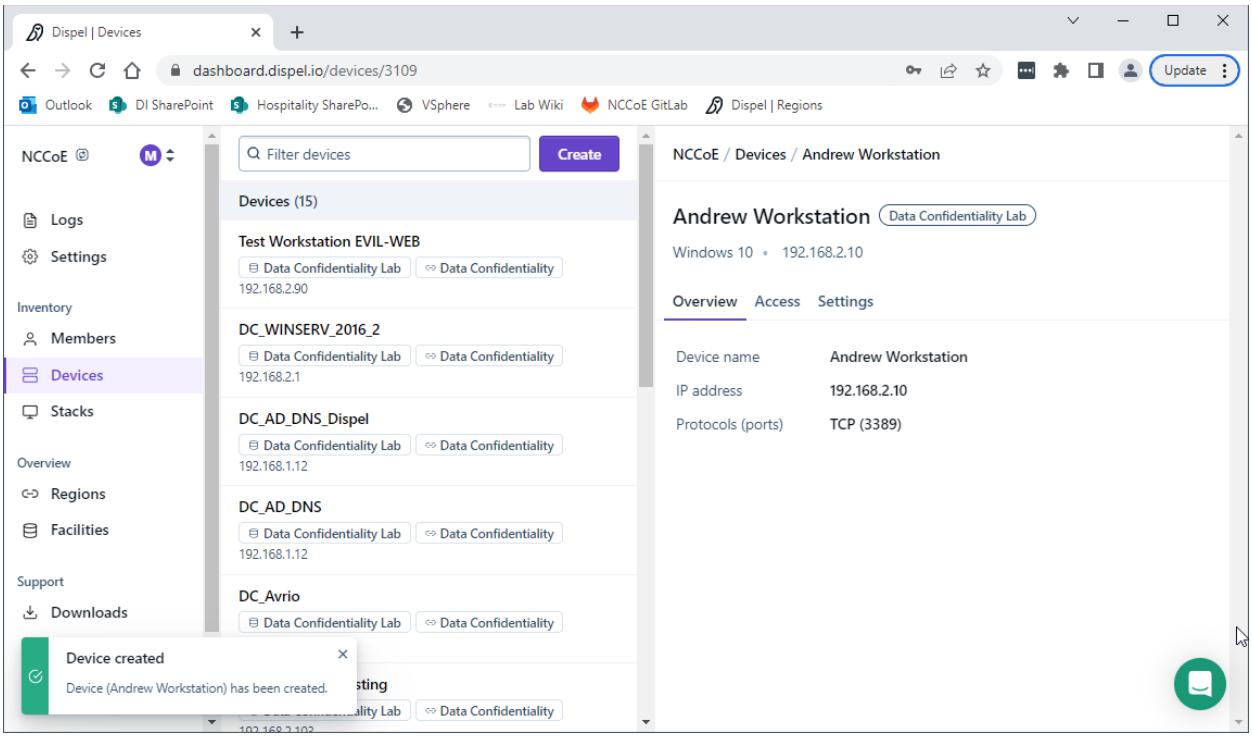
3. Click on the **Devices** page on the sidebar and click **Create**.



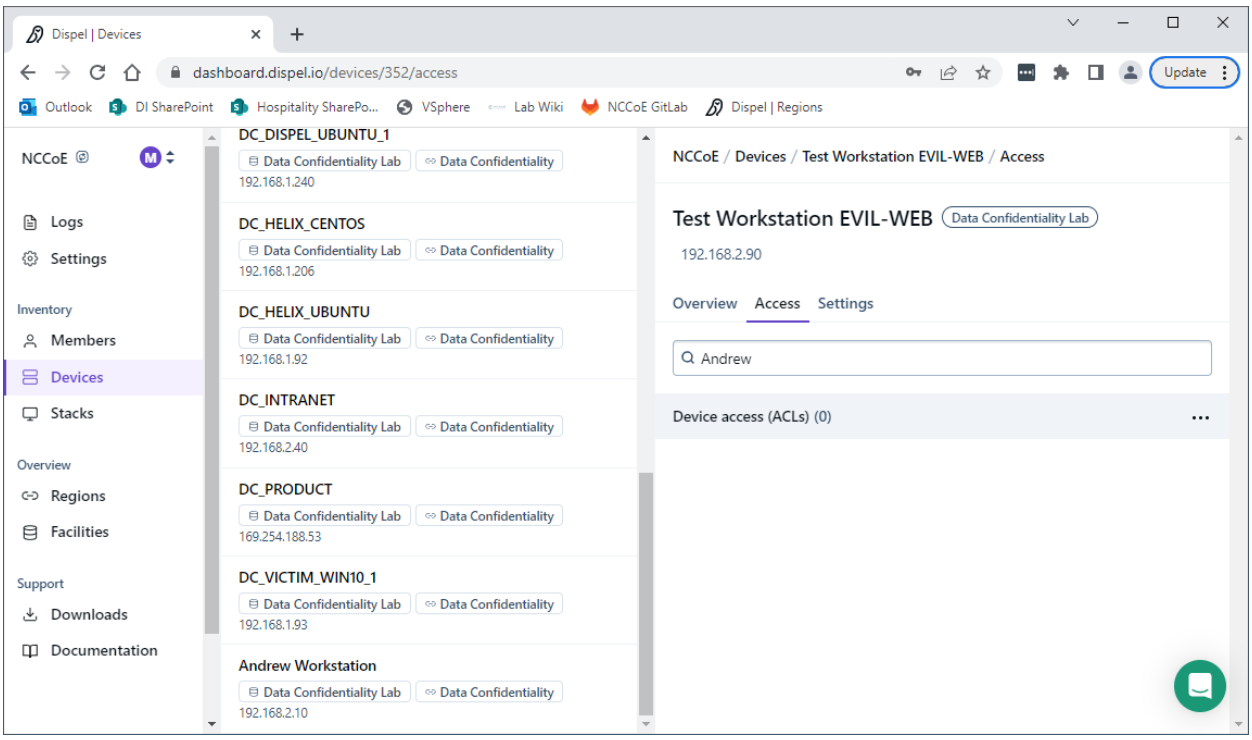
4. Under the **Add Device** window, fill out all fields, including **Facility**, **Wicket**, **Name**, **Make**, **Model**, **IP**, and **Protocol**.



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

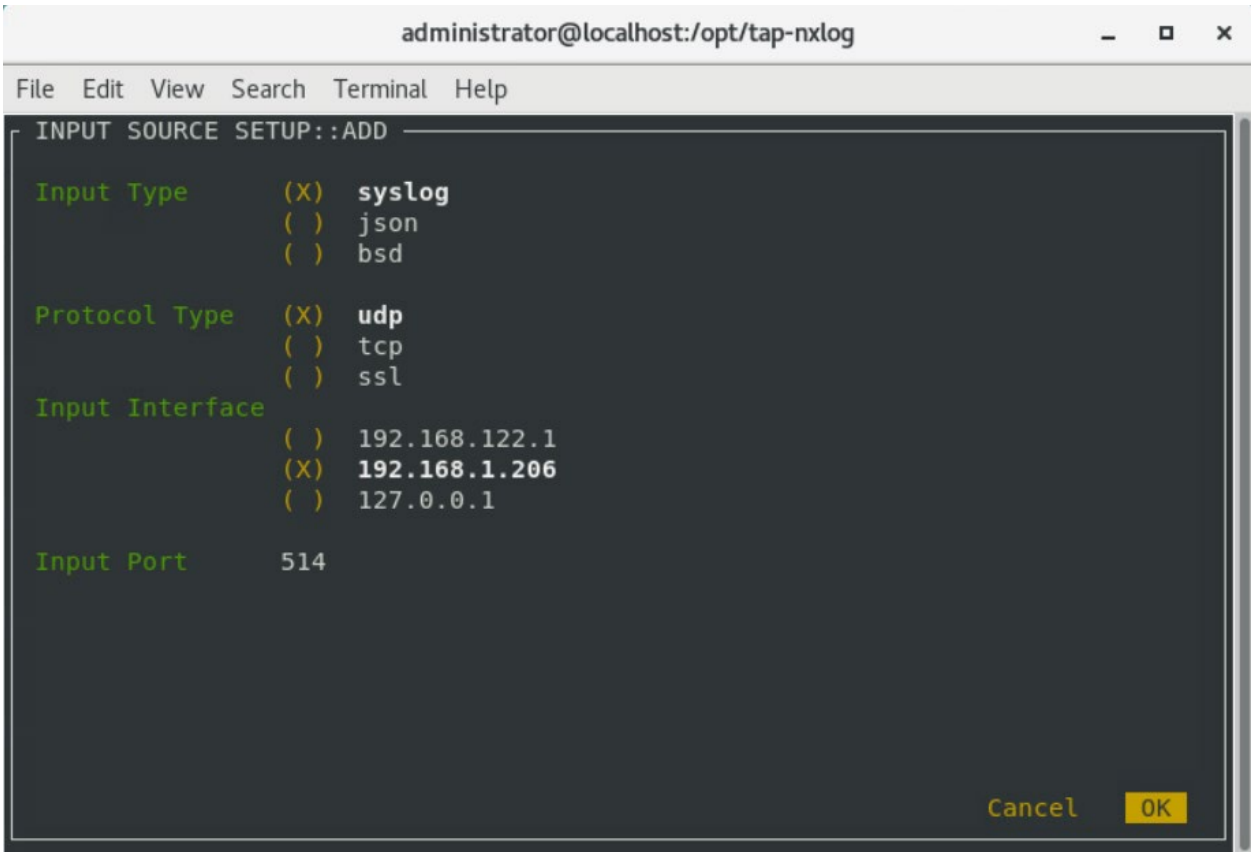
In the following section, Cisco Stealthwatch will be configured to forward logs to an on-premise Helix Communications Broker. Cisco Stealthwatch, as a network monitoring solution, can provide logs relevant to malicious network activity, potential data egress, as well as contextual information that can 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**.

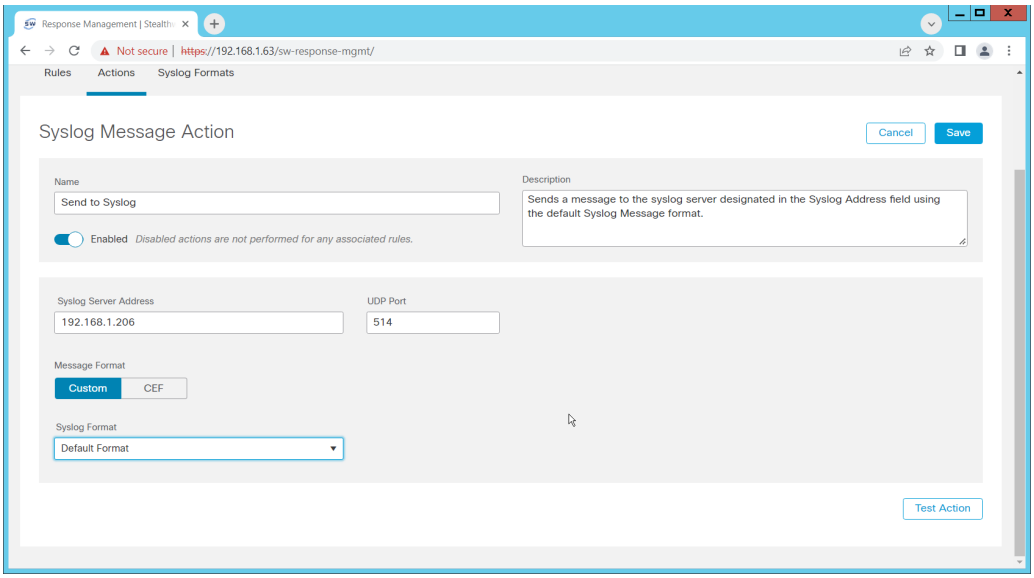
3. Click the **Actions** tab.

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.

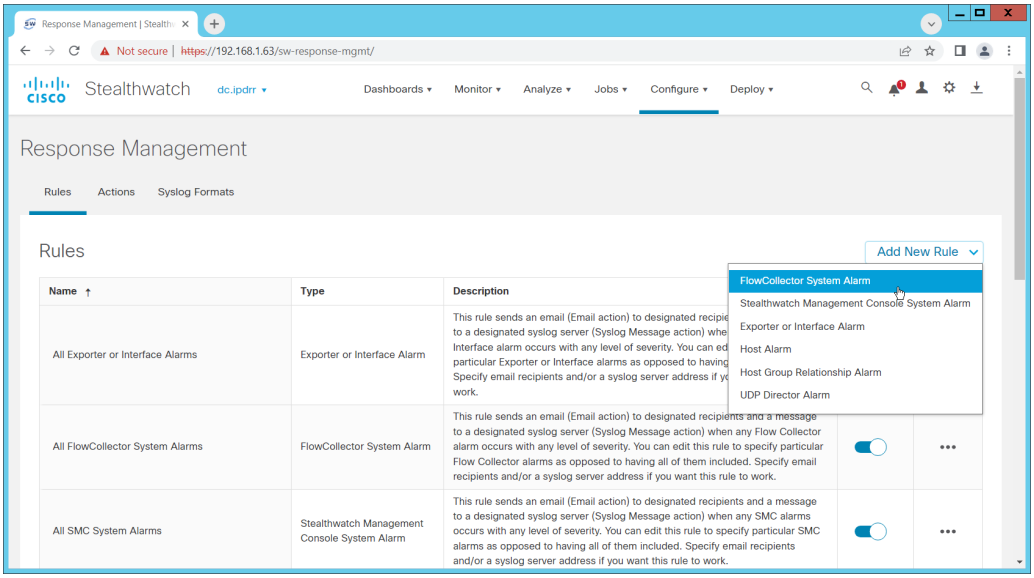
7. Enter the port that you selected earlier.



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.

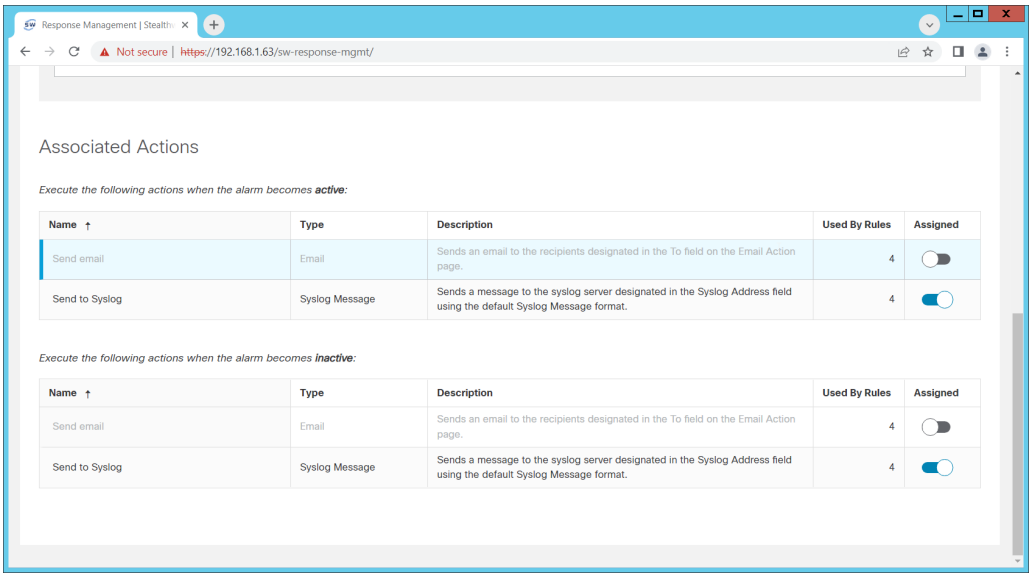


11. To create your own, click **Add New Rule**. For the purposes of this example, we select **FlowCollector System Alarm**.

12. Enter a name for the rule.

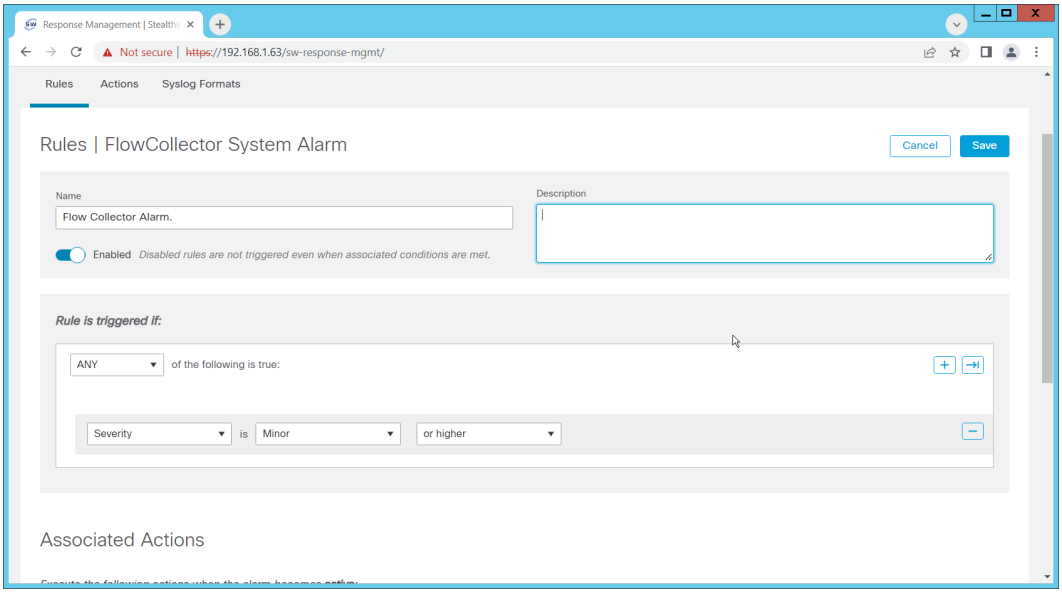
13. Ensure the rule is **Enabled**.

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

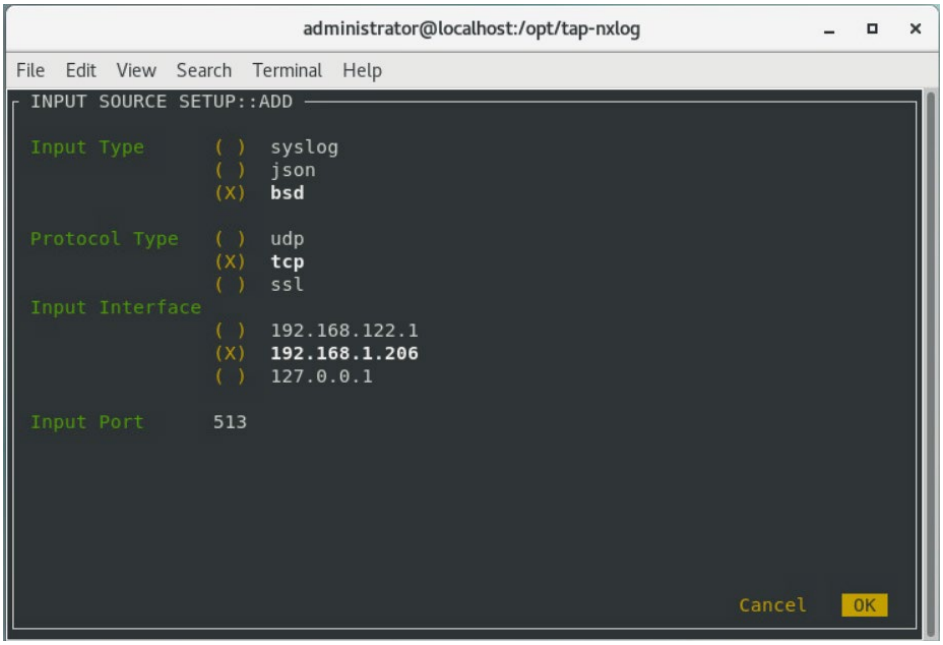
attack. An integration with the logging capability is useful for contextualizing information provided by other tools, generating alerts, and providing historical archives for reporting and compliance purposes. This section assumes the Helix Communications Broker has already been installed.

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**.

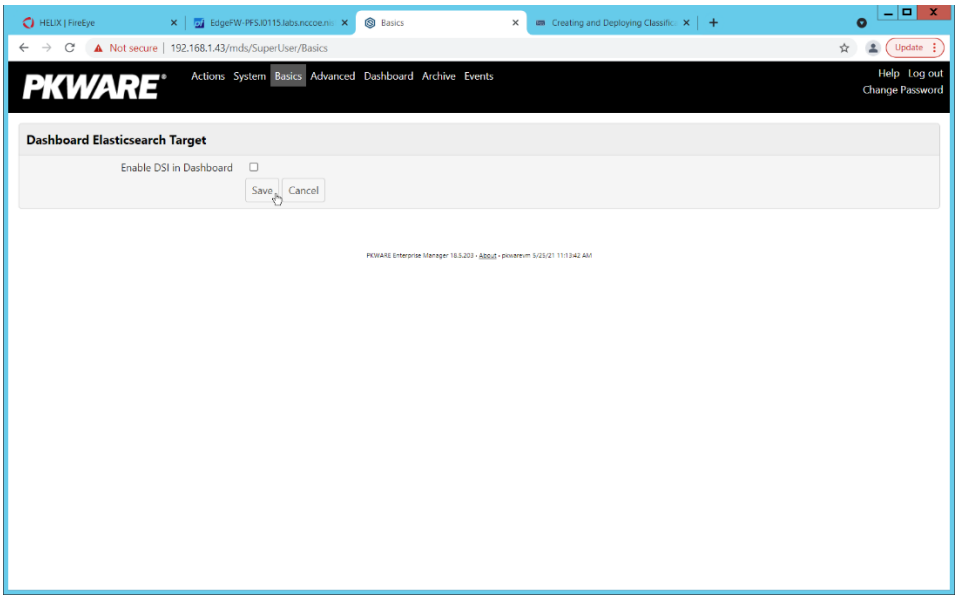
2.7.2 Configure PKWARE PKProtect to Forward Events

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**.

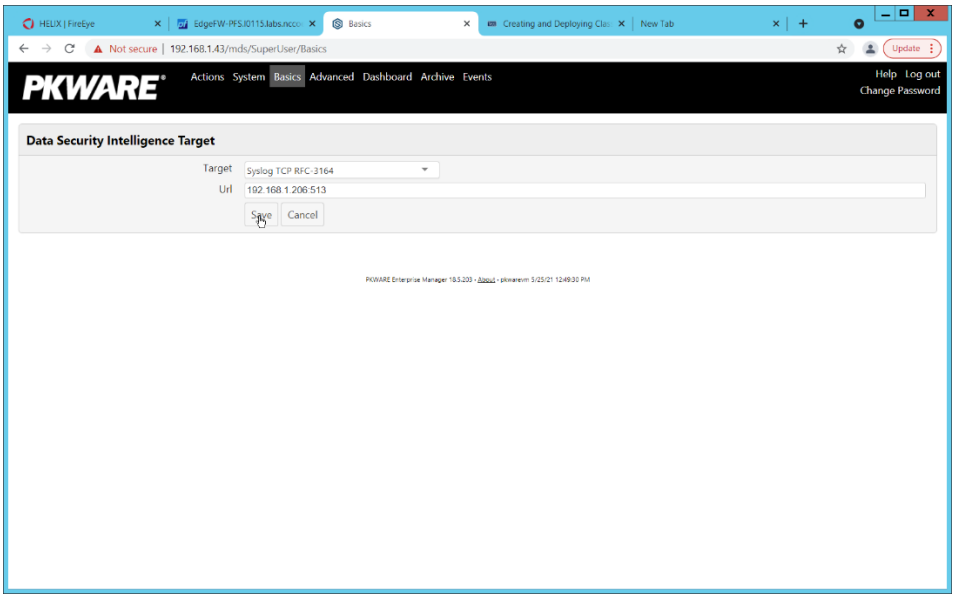


7. Click **Save**.

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