NIST SPECIAL PUBLICATION 1800-28

Data Confidentiality:
Identifying and Protecting Assets Against 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

December 2023

DRAFT

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

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SPECIAL PUBLICATION 1800-28

Data Confidentiality: Identifying and Protecting Assets Against 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

DRAFT

December 2023

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 1800-28A

Data Confidentiality:

Identifying and Protecting Assets Against 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

December 2023

DRAFT

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

Executive Summary

CHALLENGE

In our data-driven world, organizations must prioritize cybersecurity as part of their business risk management strategy. Specifically, data security remains a challenge as attacks against an organization's data can compromise emails, employee records, financial records, and customer information thereby impacting business operations, revenue, and reputation. In the event of a data breach, data confidentiality can be compromised via unauthorized exfiltration, leaking, or spills of data or corporate information to unauthorized parties, including the general public. This can be intentional or accidental.

In the event of an ongoing data breach, 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

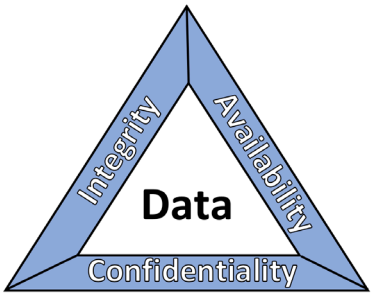
The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) developed this guide to help organizations implement strategies for preventing recovering from data confidentiality attacks. This NIST NCCoE Cybersecurity Practice Guide demonstrates how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

This practice guide can help your organization:

- Identify data on your network that is vulnerable to a data breach
- Identify vulnerabilities to data breaches on your network
- Implement protective technologies to prevent data breaches

APPROACH

This 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 National Institute of Standards and Technology (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 informs organizations of how to **identify** and **protect** assets, including data, against a data confidentiality attack, and in turn understand how to manage data confidentiality risks and implement the appropriate safeguards. A complementary project and accompanying practice guide (SP1800-29) addresses data confidentiality through the lens of detecting, responding, and recovering from a data confidentiality attack.

The NCCoE developed and implemented a solution that incorporates multiple systems working in concert to identify and protect assets and data against detected data confidentiality cybersecurity events. The solution will demonstrate the ability to identify assets and data that are at risk of a data breach and recommend capabilities to help protect them.

In developing this solution, the NCCoE sought existing technologies that provided the following capabilities:

- **Logging**
- **Network protection**
- **User access control**
- **Data management**
- **Data protection**
- **Policy enforcement**
- **Browser isolation**

Collaborator	Security Capability or Component
Avrio Software (now known as Aerstone)	Data Management
Cisco	Policy Enforcement, User Access Control
Dispel	Network Protection
FireEye	Logging
PKWARE	Data Protection
Qcor	Data Protection
Strongkey	Data Protection
Symantec, a Division of Broadcom	Browser Isolation

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 1800-28a: 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 1800-28b: 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 1800-28c: 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 1800-28B

Data Confidentiality:

Identifying and Protecting Assets Against 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

December 2023

DRAFT

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

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-28B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-28B, 61 pages, (December 2023), CODEN: NSPUE2

FEEDBACK

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

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

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

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 concerning 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 identify and protect assets, including data, against a data confidentiality attack.

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

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

60 The Technology Partners/Collaborators who participated in this build submitted their capabilities in
61 response to a notice in the Federal Register. Respondents with relevant capabilities or product

components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Avrio Software (now known as Aerstone)	Avrio SIFT
Cisco Systems	Duo
Dispel	Dispel
FireEye	FireEye Helix
Qcor	Qcor ForceField
PKWARE	PKWARE PKProtect
StrongKey	StrongKey Tellaro
Symantec, a Division of Broadcom	Symantec Web Isolation

DOCUMENT CONVENTIONS

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

CALL FOR PATENT CLAIMS

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

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

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

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

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

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

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

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

Contents

137 # List of Figures

143 # 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 people 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 individuals 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.

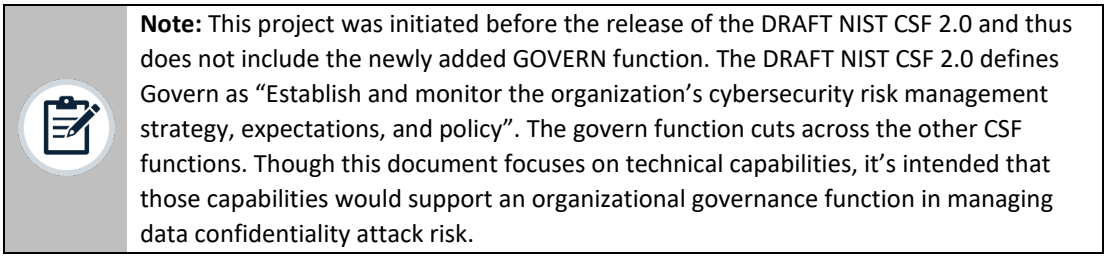
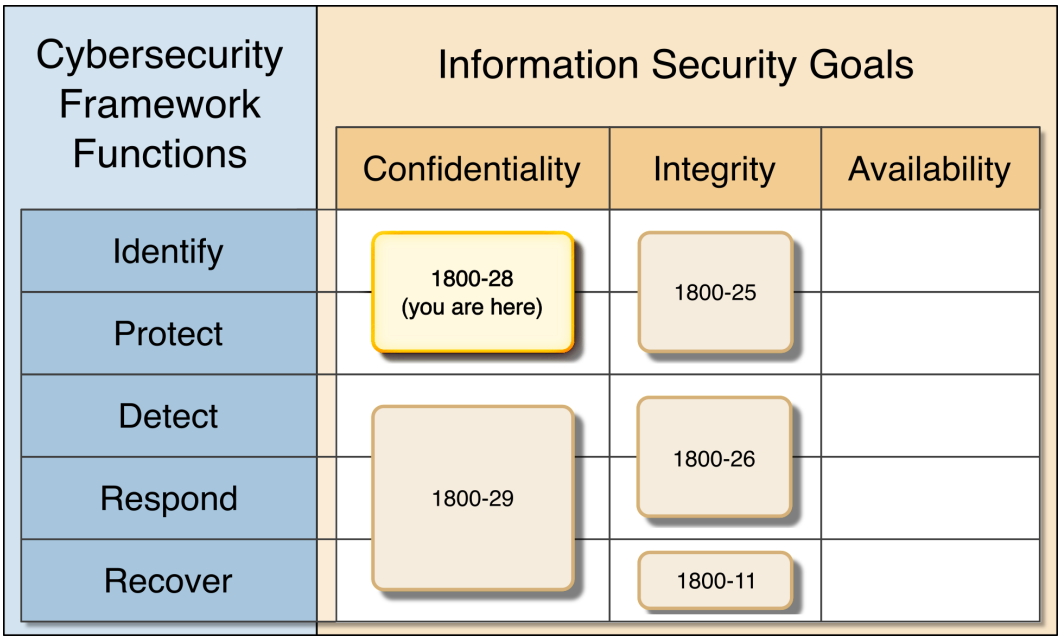


Figure 1-1 Data Security Project Mapping



The goals of this NIST Cybersecurity Practice Guide are to assist organizations in identifying and protecting their assets and data in order to prepare for and prevent a data confidentiality event. This guide will help organizations:

- Inventory data storage and data flows
- Protect against confidentiality attacks against hosts, the network and enterprise components
- Protect enterprise data at rest, in transit, and in use
- Configure logging and audit capabilities to meet organizational requirements
- Provide user access controls to sensitive data
- Provide user authentication mechanisms for host and network access
- 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 to identify and protect data:

- NIST Special Publication 1800-25, Data Integrity: Identifying and Protecting Assets Against Ransomware and other Destructive Events [2]
- 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 Privacy Framework [7]
- NIST Cybersecurity Framework [8]
- NIST Interagency Report 8374, Ransomware Risk Management: A Cybersecurity Framework Profile [9]
- NIST Special Publication 800-160, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach [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 1800-28 focuses on the Identify and Protect 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 identifying potential breaches of data confidentiality as well as protecting against the resulting losses.

Additional challenges arise when defining what it means to "identify" or "protect" data. In the NCCoE's previous work on Data Integrity (1800-25[2], 1800-26[3], and 1800-11[4]), 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 1800-29 addresses an organization's actions during and after a loss of data confidentiality (the remaining NIST CSF Functions of Detect, Respond, and Recover) while this guide's focus is on the needs prior to a loss of data confidentiality (by focusing on the NIST CSF Functions Identify and Protect). The solution utilizes commercially available tools to provide relevant capabilities such as automated data sensitivity detection, user access controls for data, encryption of potential confidential data, and multifactor authentication, 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 1800-28A: Executive Summary
- NIST SP 1800-28B: Approach, Architecture, and Security Characteristics – what we built and why (you are here)
- NIST SP 1800-28C: 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 1800-28A*, which describes the following topics:

- challenges that enterprises face in identifying vulnerable assets and protecting them from data breaches
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-28B*, 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
- Section 3.6, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-28A*, with your leadership team members to help them understand the importance of adopting standards-based solutions to protecting against 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 1800-28C*, 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 a security architecture that protects against data breaches. 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 and privacy controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to ds-nccoe@nist.gov.

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 (uniform resource locator), 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 Core. This project centers on identifying and protecting vulnerable data from attack. Our commercial collaboration partners have volunteered to provide the products that provide this 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, 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 take steps to proactively protect the personal data or personally identifiable information (PII) of individuals they process. The ramifications for failing to adequately protect PII can have severe consequences for both 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 identifying potentially sensitive data and protecting against 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 Core.

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, as such 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.

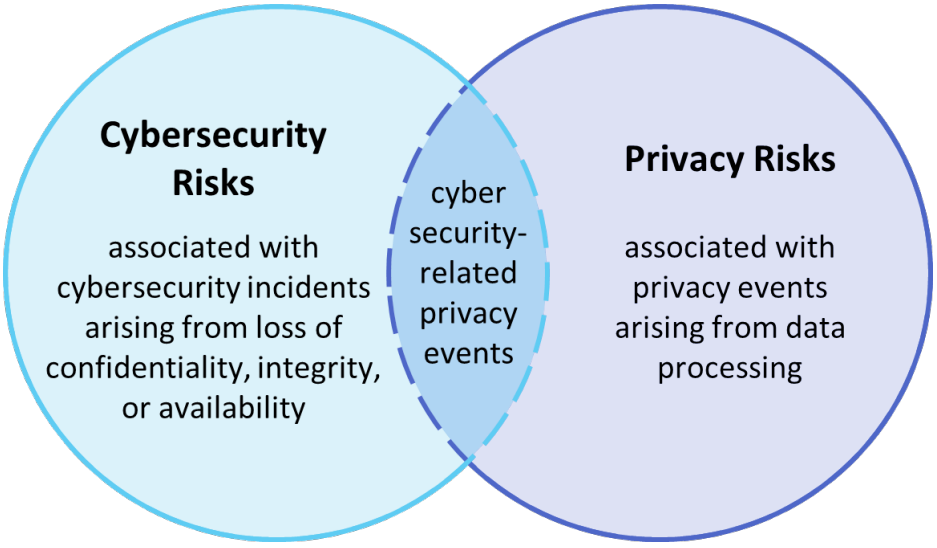
Following an open and transparent development process, NIST published the NIST Privacy Framework, Version 1.0 to help organizations better identify and manage their privacy risks, build trust with customers and partners, and meet their compliance obligations. The Privacy Framework Core provides privacy 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 confidentiality 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. [16] As reflected in the overlap of Figure 31, 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[11]. 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 impact if 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 [7] and Privacy Risk Assessment Methodology (PRAM) [14] 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 action and privacy considerations for this build.

3.6 Technologies

Table 3-1 Products and Technologies 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 Security Control Map for an explanation of the NIST Cybersecurity Framework Subcategory identifiers. Table 3-1 also provides the Privacy Framework Subcategory identifiers, and these are explained in Appendix E.

418 **Table 3-1 Products and Technologies**

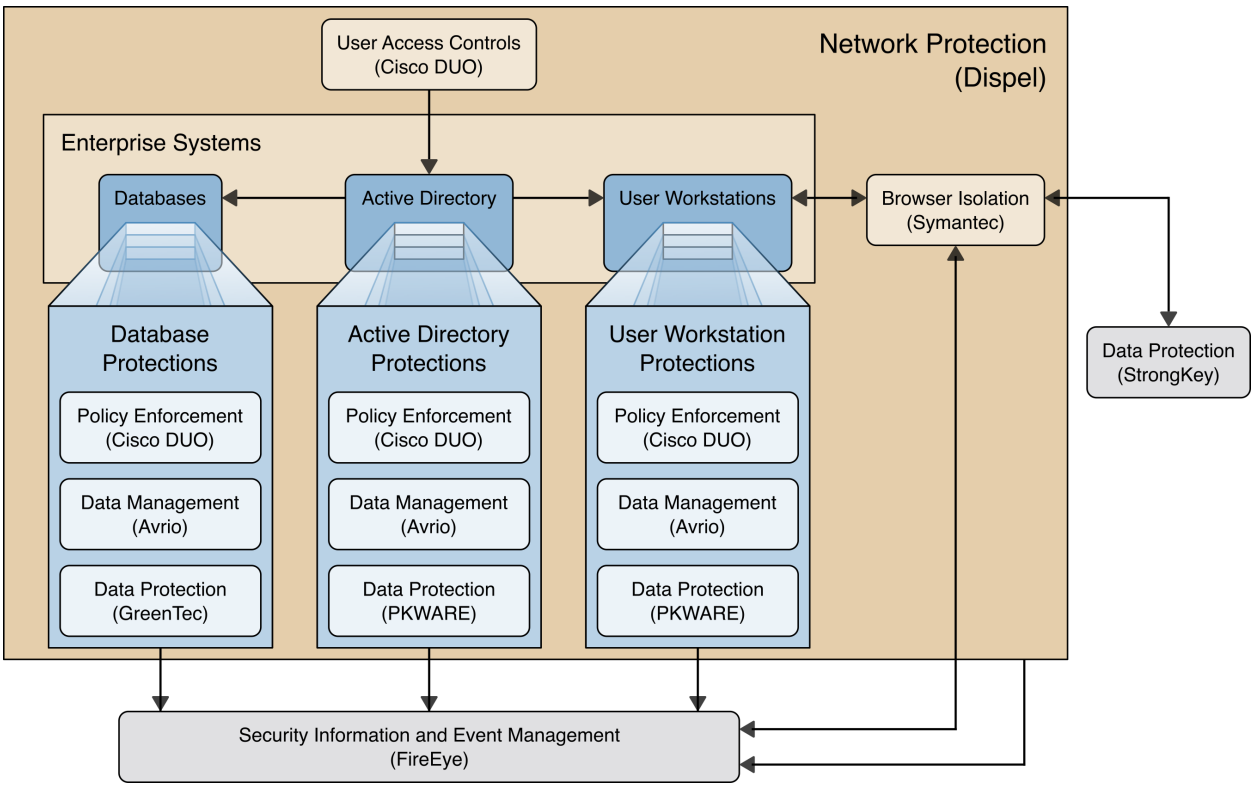
Component	Product	Capability	NIST Cybersecurity Framework Subcategories	NIST Privacy Framework Subcategories
Data Management	Avrio SIFT v1.0.5.R5	• Discovers, tags, and protects sensitive files across the network	ID.AM-2, PR.DS-1, PR.DS-3	ID.IM-P1, PR.DS-P1, PR.DS-P3
Data Protection	Qcor Forcefield v1.9h	• Protects data at-rest from unauthorized access and malicious modification	PR.DS-1	PR.DS-P1
	PKWARE PKProtect v16.40.0010	• Provides data encryption at-rest and in-transit	PR.DS-1, PR.DS-2	PR.DS-P1, PR.DS-P2
	StrongKey Tellaro	• Provides a Web API (application programming interface) for encryption and tokenization, key management, and strong authentication	PR.AC-7, PR.DS-2	PR.AC-P6, PR.DS-P2
User Access Controls	Cisco Duo	• Provides multi-factor authentication	PR.AC-1, PR.AC-4, PR.AC-7	PR.AC-P1, PR.AC-P4, PR.AC-P6
Browser Isolation	Symantec Web Isolation	• Provides isolation of web browsers to protect from risky traffic • Protects from malware and phishing threats • Provides a privacy toggle that allows for user browsing data to be anonymized. • Provides a login banner to inform individuals of data collection practices with web browsing	PR.AC-5, PR.DS-2	PR.AC-P5, PR.DS-P2, CT.DP-P2, CM.AW-P3
Policy Enforcement	Cisco Duo	• Provides policy control on a global or per-application basis	PR.IP-5	PR.PO-P4

Component	Product	Capability	NIST Cybersecurity Framework Subcategories	NIST Privacy Framework Subcategories
Logging	FireEye Helix	• Provides a baseline for normal enterprise operations • Provides logs and enables incident response	ID.RA-1, ID.RA-2, ID.RA-3, PR.PT-1	CT.DM-P8
Network Protection	Dispel	• Provides remote access to network	PR.AC-3, PR.AC-5	PR.AC-P3, PR.AC-P5

4 Architecture

This section presents the high-level architecture and a set of capabilities used in our data confidentiality reference design that identifies and protects assets from unauthorized access and disclosure.

Figure 4-1 High Level Architecture



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

- **Data Management** allows discovery and tracking of files throughout the enterprise.
- **Data Protection** involves encryption and protection against disclosure of sensitive files.
- **User Access Controls** allows organizations to enforce access control policies, ensuring that only authorized users have access to sensitive files.
- **Browser Isolation** protects endpoints in the organization from malicious web-based malware by sandboxing and containing executables downloaded from the internet.
- **Policy Enforcement** ensures that endpoints in the organization conform to specified security policies, which can include certificate verification, installed programs, and machine posture.
- **Logging** creates a baseline of a normal enterprise activity for comparison in the event of a data confidentiality event.
- **Network Protection** 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.

These capabilities work together to provide the functions Identify and Protect for the reference architecture. The data management capability provides data inventory and asset management for files in the enterprise; helps identify potentially sensitive files; and works with the data protection capability to ensure potentially sensitive files are properly protected in the event of a breach. Because organizations can be large and new sensitive files may be created daily, it is important to have the capability to automate identification and protection of files at least partially. The data protection capability and user access controls prevent data from being read by unauthorized parties. By ensuring that only the correct people have access to data, and that data is properly encrypted and stored, it becomes more difficult for adversaries to steal and disclose sensitive data.

The policy enforcement, network protection, and browser isolation capabilities work together to protect endpoints such as laptops and desktops against common attack vectors. Malicious websites distributing malware first pass through the browser isolation capability, which sandboxes webpages to ensure that malware downloaded via malicious webpage cannot spread to the user or enterprise's system. Network segmentation uses network layer policies to group endpoints into segments based on business needs. If an endpoint is infected, network segmentation can limit impact by preventing malware from spreading between segments. Policy enforcement ensures that systems remain up to date with organizationally defined security policies. All of these functions feed into logging capabilities and provide organizations with an understanding of their baseline of normal activity. These logs inform the organization of its security posture before an event, so that the organization can adjust its policies as new information about threats becomes available and take appropriate action.

5 Security & Privacy Characteristic Analysis

The following section is intended to help organizations understand the extent to which the project meets its objective of demonstrating technologies and capabilities to help organizations mitigate data confidentiality risk. To support this, we developed several s 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 and privacy 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

476 capabilities of our architecture would help an organization address the Cybersecurity Framework
477 Functions of **Identify** and **Protect** for that event.

478 Below is a list of the scenarios created to test the security capabilities of this architecture.

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

481 5.2.1 Exfiltration of Encrypted Data

482 **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	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-5, ID.RA-5, PR.AA-01, PR.AA-02, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-04
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 protect sensitive data from this breach, as well as be able to identify the traffic generated by the malware as anomalous.
Identify	The **Data Management** capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk of targeting and the impact to the enterprise in the event of compromise.
Protect	The **Data Protection** capability provides encryption for sensitive data which has been identified as important, protecting it from unauthorized access in the event of an exfiltration attack. Another important aspect of the Protect function is the documentation of audit logs, with respect to sensitive data. The **Logging** capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase to discover anomalies in network traffic and lead to the discovery of malicious exfiltration.

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/deletion.**
Associated DRAFT CSF 2.0 Subcategories	PR.AA-01, PR.AA-02, PR.AA-03, PR.DS-01, PR.DS-02, PR.PS-01, PR.PS-04, DE.CM-09
Organizational Response	In this scenario, someone at the organization with privileged credentials has had their credentials compromised 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 deal with a privileged user account with access to the database being used by a malicious actor and is responsible for protecting assets from the compromised account.
Identify	Though identifying assets is an important function, in this scenario we are specifically focusing on the ability of a compromised user to access an in-use database, and do not have a specific need to identify the database as part of the scenario's resolution, since the target is known.
Protect	The Data Protection capability provides write-protection against alteration or deletion of saved data, as well as protection against reading the data through encryption of data-in-use. Another important aspect of the Protect function is the management of access permissions. The User Access Controls capability allows the database to be protected by a second layer of authentication separate from the user's username and password. In the event of compromised credentials, the database is less likely to be impacted if two factors of authentication are required. Furthermore, acquisition of user credentials does not necessarily imply that a user's physical system has been stolen. Policy Enforcement can take advantage of this by forcing computers connecting to organizational resources to be trusted via certificate or meet other requirements to ensure that a username and password is not enough to compromise critical resources.

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 uploads sensitive files to the malicious host website, which displays a notice that unless a ransom is paid, the sensitive files will remain publicly visible.
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-5, ID.RA-5, PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.IR-01, PR.PS-01, PR.PS-04
Organizational Response	In this scenario, someone at the organization with privileged credentials has had their credentials compromised through a malicious webpage disguised as the organization's email provider. 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.
Identify	The **Data Management** capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk of targeting and the impact to the enterprise in the event of compromise.
Protect	The **Data Protection** capability provides encryption for sensitive data, protecting it from unauthorized access in the event of an exfiltration attack. Even if the data is stolen and released, encryption prevents the data from being used or read. Another important component of the Protect function is the documentation of audit logs, with respect to sensitive data. The **Logging** capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase to discover anomalies in network traffic and user behavior, potentially allowing for the detection of a malicious actor accessing the user's workstation outside of normal hours. **Browser Isolation,** in tandem with **Network Protection,** will prevent downloads of malicious files from websites and unknown ports, limiting the attacker's ability to acquire their ransomware program after the system has been compromised. While the ability to download malicious programs onto the workstation may not completely stop determined attackers, it increases the difficulty and time required for the attack, allowing more time for Detection and Respond activities by the defending organization.

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	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-5, ID.RA-5, PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.IR-01, PR.PS-04
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.
Identify	The **Data Management** capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise in the event of an information leak.
Protect	The **Data Protection** capability provides encryption for sensitive information, protecting it from unauthorized access even if it is accidentally sent to unauthorized users. Another important component of the Protect function is documentation of audit logs, with respect to sensitive data. The **Logging** capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase for reporting on data which has been transferred onto the systems of unauthorized users.

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	ID.AM-01, ID.AM-02, ID.AM-05, ID.AM-07, PR.AA-01, PR.AA-03, PR.DS-01, PR.DS-09, PR.PS-03
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. Although some aspects of this event are easier because of the user's knowledge of the system, it is important for the organization to 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.
Identify	The Data Management capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise in the event of a compromise. The Policy Enforcement capability can be used to force computers connecting to organizational resources to meet requirements regarding which programs are installed. While this capability typically falls under the Protect function, knowing the security posture of assets in the enterprise is an important Identify function. When policy enforcement is used to ensure the presence of encryption capabilities, for example, the enterprise has some assurance that data on the workstation has not been compromised.
Protect	The Data Protection capability provides encryption for the laptop and prevents sensitive data from being read. Another important aspect of the Protect function is the management of access permissions. The User Access Controls capability allows the network to be protected by two layers of authentication. Although the laptop may be compromised, requiring user account credentials as well as a second factor of authentication protects the network from further compromise. Policy Enforcement can be used to force computers connecting to organizational resources to meet requirements regarding which programs are installed, which helps to ensure that lost or stolen machines will have adequate data protection and user access control in place to prevent the loss of data in the event of a lost or stolen laptop.

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 (universal series bus) drive. The insider also prints these files.**
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-02, ID.AM-05, ID.AM-07, ID.RA-03, PR.AA-03, PR.AA-05, PR.AA-06, PR.DS-01, PR.DS-02, PR.DS-09, PR.PS-04, PR.IR-01
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.
Identify	The **Data Management** capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise in the event of a compromise. In the event of a malicious insider attempting to exfiltrate data, it is important to know which data was accessible on the machines accessed by the insider, as well as the sensitivity levels of the affected data.
Protect	The **Data Protection** capability provides encryption for sensitive data , protecting it from unauthorized access. While a malicious insider may be able to decrypt data relevant to their work role, irrelevant data which is encrypted and managed properly will be significantly less useful to the insider. Another important capability within the Protect Function is the management of access permissions. The **User Access Controls** can prevent unauthorized users from accessing sensitive files in the first place, preventing copying and printing functionality. While user access controls and data protection ensure that the user only has access to some data, ultimately, malicious insiders tend to have some level of access to data due to their role in the organization. **Logging** provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase for reporting on data which has been exfiltrated from the organization. In the event of exfiltration by a malicious insider, logs can help determine what data was accessed and printed and can aid the organization in recovering from the exfiltration, potentially in non-technical ways, such as through the legal system or law enforcement.

493 ### 5.2.7 Eavesdropping

494 **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 man-in-the-middle attack. A user begins uploading a sensitive proposal for a new project. The malicious outsider is able to intercept and view these files.**
Associated DRAFT CSF 2.0 Subcategories	ID.AM-01, ID.AM-03, ID.AM-07, PR.AA-05, PR.AA-06, PR.DS-01, PR.DS-02, PR.PS-04, PR.IR-01
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.
Identify	The Data Management capability is used to identify new sensitive data when it is created and track it throughout the organization. The results of this capability are used to inform protection and response capabilities about which data is at risk and the impact to the enterprise. In this scenario, a new project proposal is created - the data management capability is used to identify the creation of new sensitive data and track it throughout the enterprise.
Protect	The Data Protection capability provides encryption for sensitive data, protecting it from unauthorized access. While a malicious third party on the network may be able to intercept the data in transit, encryption prevents the third party from being able to read the intercepted data. Another important component of the Protect Function is the documentation of audit logs, with respect to sensitive data. The Logging capability provides a baseline for normal enterprise activity. This baseline can be used as a comparison point in the Detect phase for noticing anomalous network activity, such as a malicious host on the network acting as a proxy between two systems. Network Protection is also an important capability for protecting network traffic from malicious adversaries. Using network segmentation, zero trust, and moving target defense capabilities, unrecognized devices can be prevented from identifying, reconnoitering, and accessing the network or communicating with trusted hosts.

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 [7]. 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 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 use of a service and securing 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 MFA 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.

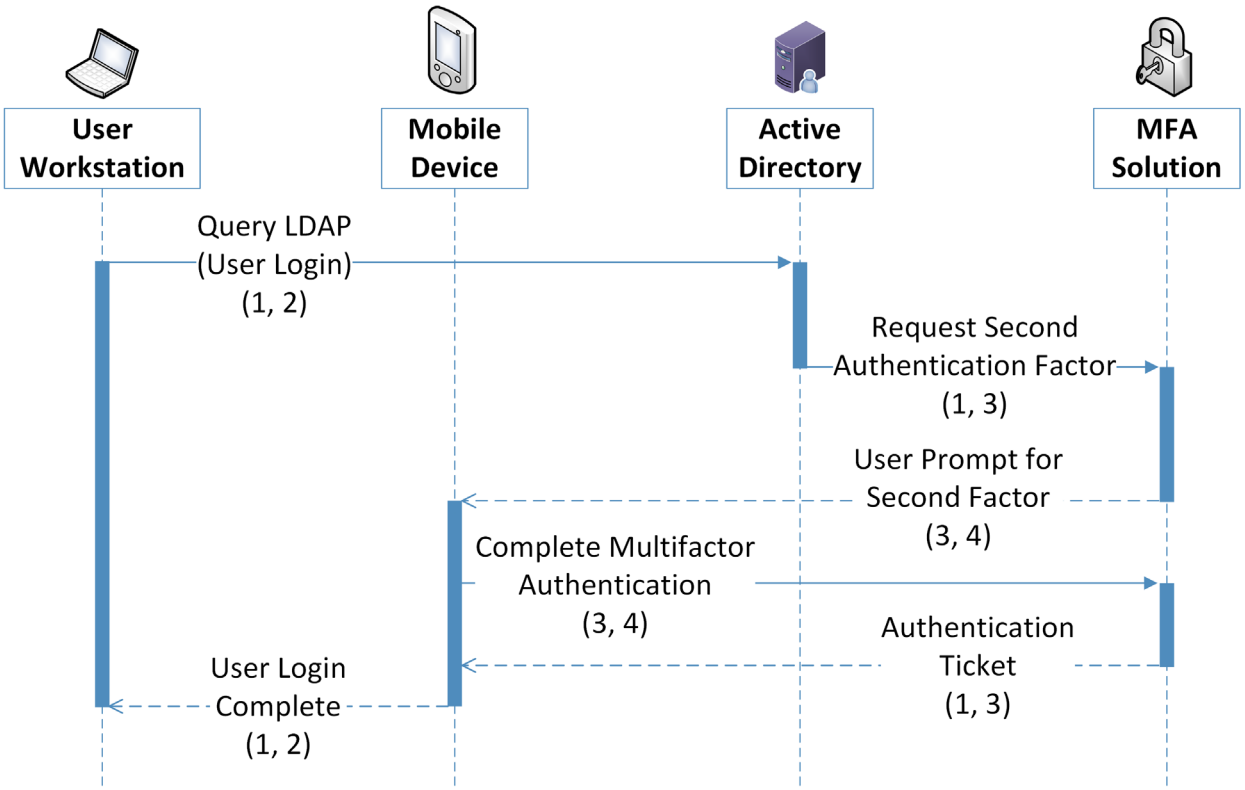
Organizations should consider these types of risks as they design and implement systems. As demonstrated in the scenarios below, risk mitigations should be implemented within the design to limit privacy risks. These privacy risk mitigations might include the following, among others:

- 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 authentication is a security best practice. The architecture recommends the use of a password, pin (personal identification number) or biometric with an asymmetric cryptographic key for authentication. However, it is common practice for organizations to offer a variety of MFA solutions. This can include user-owned mobile devices, which may impact privacy risk [17].

544 **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)

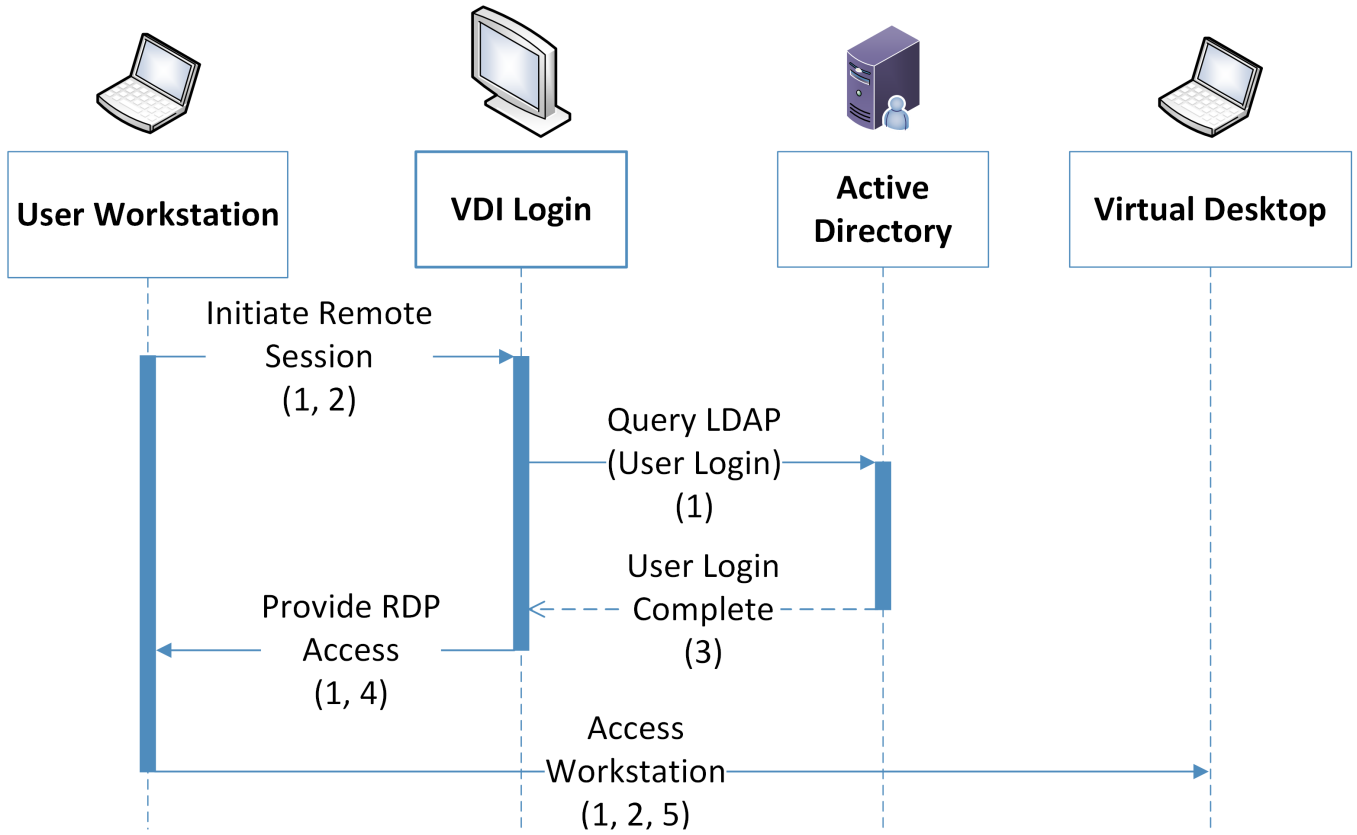
Data Type	Data Action	Privacy Impact
Username	Username is stored by the user workstation and transferred across the authentication process to help identify the transaction.	Usernames potentially contain inferable PII such as user's first and last names
Client IP Address	The client IP (Internet Protocol) address is stored by the user workstation, and transferred as part of communications where it is an endpoint.	IP addresses can be used to derive PII 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-component identifiers for a transaction can be used to re-identify information that was otherwise anonymized, such as connections between a user's name and their cell 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.	Information about a user's mobile device, such as device type and version, can be used to infer privacy-impacting information such as the cost of their personal devices. Furthermore, user cell-phone numbers used in certain MFA transactions are PII.

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
User authentication may use a mobile device as an authenticator, which can be personally or organizationally owned.	Mobile devices are a popular option for authentication processes. Personal information can be transferred in the process of authenticating. This can include phone number and location information. Users' non-work activity may be tracked by an organization.	**Context:** Authentication processes that utilize personally owned mobile devices can require the use of information that is personal to the user, such as phone numbers and other metadata. The tracking could extend beyond the work environment or even within the work environment 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:** 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 is viewed and collected by login tools, 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 optionality 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 audit tools to determine what information they are using and collecting. **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

Data Type	Data Action	Privacy Impact
Username	The username is stored by the user workstation and active directory. It is transferred as part of the	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.
One-time password	A One-time Password is generated by the VDI to authenticate the RDP (remote desktop protocol) connection and is transferred to and stored on the user workstation.	
Client Time Zone	The Client Time Zone is stored by the user workstation and transferred as part of an RDP connection to the virtual desktop.	Along with IP addresses, time zones specifically provide information 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.	User's personal device names can include inferable PII, such as personal names and device locations.

552

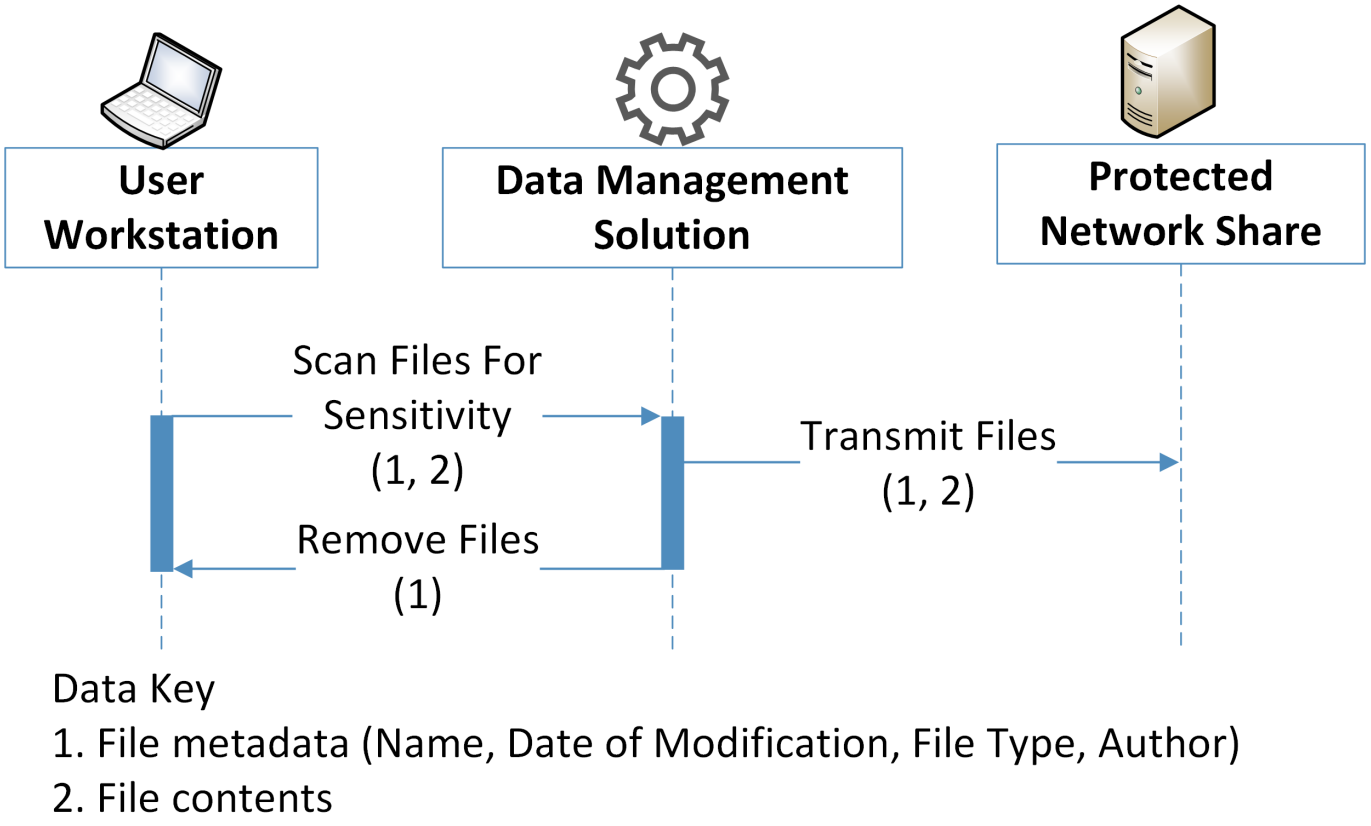
Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
User logs into a Virtual Desktop Interface solution from a personally or organizationally owned device.	Central login platforms can be connected to by a variety of devices, which may be personally owned by the user. Information that 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.	**Context:** Users operating under a BYOD or remote work scheme may not expect that certain data is under organizational purview. This can include their location, personal device metadata, and operating hours. **Problematic Data Action:** Surveillance, Unanticipated Revelation **Problem:** Loss of Trust. Users may not feel comfortable with this information being shared with third-party applications, or the company in general. Dignity Loss. Users may have information, such as their physical location and work hours, revealed to organizations in an undesired fashion.	**Predictability**: Users should be informed of information that is viewed and collected by login and network access tools such as Dispel, through either a login banner or other alert mechanism. Use privacy enhancing technologies and techniques to de-identify user, user ID and IP address like obfuscation, communication 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 and who has access rights **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.

553

5.3.3 Automated Data Movement with Data Management Solution

The reference architecture uses data management technology that allows for the scanning files for highly sensitive information and establishment of policy that automatically moves sensitive content to secure storage. Files with detected PII or other sensitive information may be moved in ways that are unexpected to the user, potentially creating privacy concerns.

Figure 5-3 Data Management Data Flow Diagram



Data Type	Data Action	Privacy Impact
File metadata	File metadata is stored on the user workstation, along with file contents. It is transferred along with file contents to the Data Management Solution and the Protected Network Share as part of the data movement operation. It is also used to identify data for deletion by the Data Management Solution.	File metadata can include information affecting privacy that is not derivable from file contents, such as the file name, date of modification, and author. This can be used to derive information such as active work hours and can lead to false assumptions about an individual
File contents	File contents are stored on the user workstation and transferred through the Data Management Solution to the Protected Network Share.	The privacy impact of file contents rely heavily on the data being used by an enterprise. This information can include SSNs, credit card information, health data, and other PII. Privacy impact and regulatory burden should be specifically considered and analyzed by organizations implementing these sorts of security solutions.

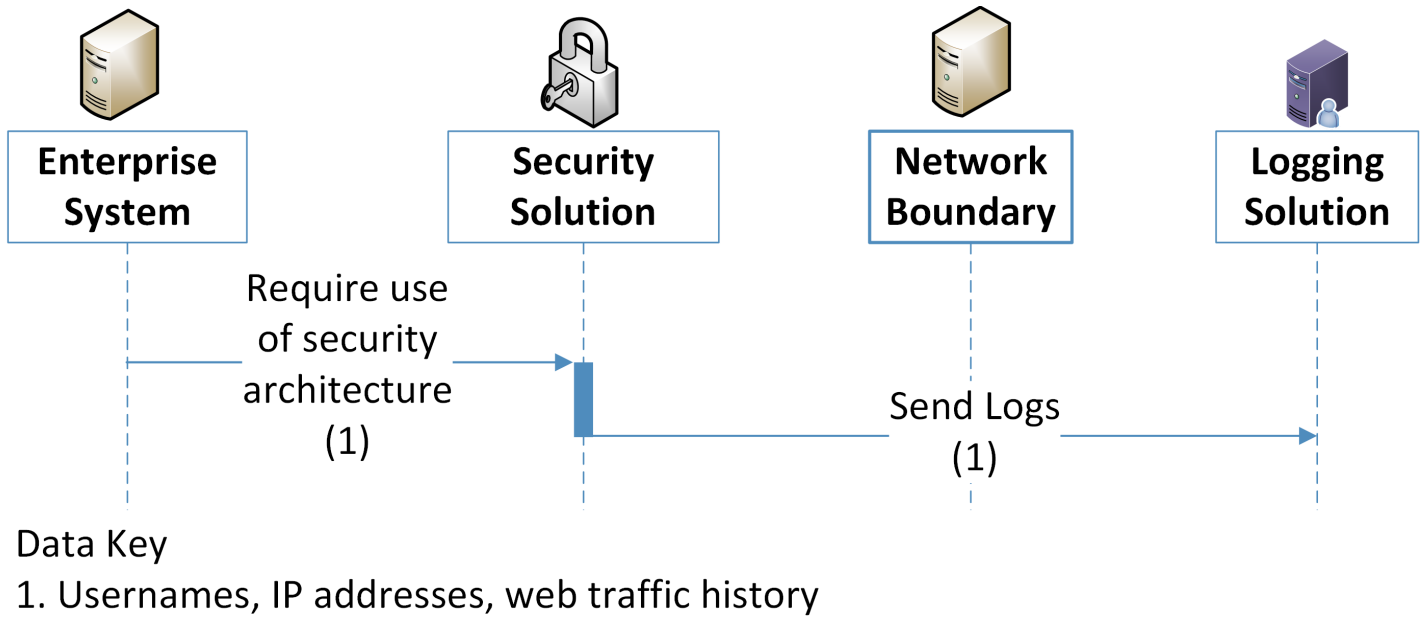
Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
Data generated in areas moderated by data management solutions are potentially duplicated, moved, or deleted in compliance with organizational policy.	Movement of data by external tools can lead to information being placed in unexpected or unintended places. This can lead to user confusion and a loss of trust in the organization, as well as data being made vulnerable to discovery and exfiltration	**Context:** Moving data from the place in which it was created or saved can create confusion for users and expose information in ways the user did not intend. **Problematic Data Action:** Appropriation, Unanticipated Revelation **Problem:** Loss of Trust. Users may be uncomfortable working in protected zones if they do not trust that their data will be kept under their control. Loss of Autonomy. Users may see involuntary data movement as a loss of their ability to govern the data they generate.	**Predictability**: Zones under the purview of data management and protection tools should be clearly defined and expressed to the user, such as through clearly understood network share names. Notice should be given to users who are impacted by the data management solution, such as by leaving a stub file at the original location. **Manageability:** Organizations seeking to include these capabilities should make sure they use solutions that can be configured to mitigate their inherent privacy risk. **Confidentiality**: Tools that provide the ability to analyze and move data should only be governed by system administrators. The automatic movement of data should only move data to locations only accessible by the user who created the original data or to folder with equal or more stringent access rights than the originating location. Furthermore, data locations are protected by IDAM (identity and access management controls) controls such as MFA.

560

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 of information collected by logs when they are created, transmitted and stored.

Figure 5-4 Logging Data Flow Diagram



The utilization of the security architecture, and the logs their user generates, can interact with and generate information that affects privacy. 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:

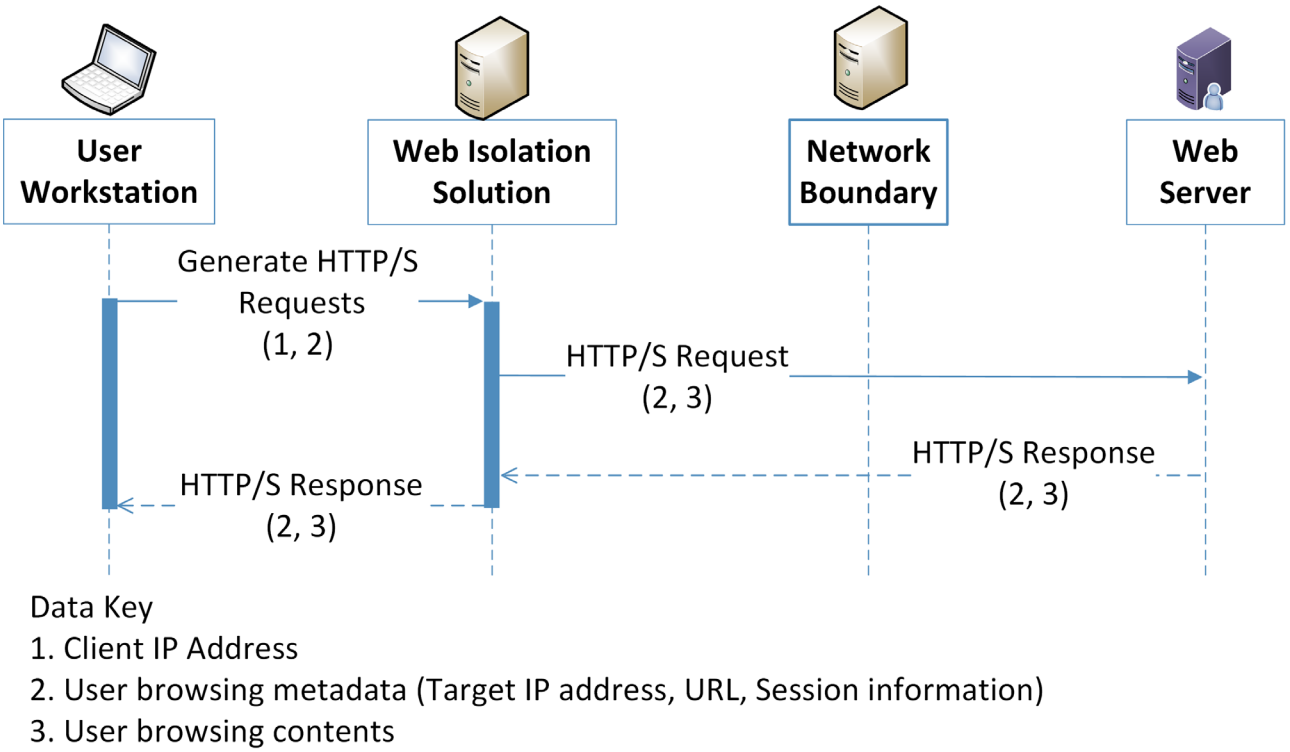
Data Type	Data Action	Privacy Impact
IP Addresses	IP Addresses are stored and transferred by enterprise systems as well as the logging solution. They are transferred by and through the security solutions.	IP addresses can be used to determine rough locations for user-owned machines. Additionally, IP Addresses can be common across logs from many security tools, allowing for anonymized data to be re-identified.
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.

Scenarios	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. This information is transmitted across the network and stored remotely.	**Context:** Logging systems can contain private data. 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 admin user 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 evaluation 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.

5.3.5 User Web Browsing with Browser Isolation Solution

Web isolation solutions must have governance over all user web traffic to be effective. This can generate privacy concerns to users by increasing the risk of their browsing data being misused.

Figure 5-5 Browser Isolation Data Flow Diagram



Data Type	Data Action	Privacy Impact
Client IP Address	IP Addresses are stored on the User Workstation and sent by network connections to and from it.	IP addresses can be used to derive PII such as a user's general location
User browsing metadata	User browsing metadata is generated on the user workstation and sent to and from the user workstation, as well as to and from the web isolation solution to the web server.	HTTP/S traffic, even when encrypted, relies on unencrypted metadata such as time stamps, source IPs, and destination IPs. These materials can be used to generate information that affects privacy, such as a specific user's browsing habits.
User browsing contents	User browsing contents are generated on the user workstation as well as the web server. They are sent back and forth between the web server and the web isolation solution and delivered back to the user workstation.	Tools that can view and inspect the contents of a user's web browsing session could further impact user privacy. This can include a user accessing their bank and checking balance information, accessing information from their healthcare provider, and so on.

Scenarios	Privacy Risk	Problematic Data Actions	Privacy Mitigations
Data from user web browsing flows through web isolation solutions, centralizing information about employee web browsing.	Web monitoring tools are used to detect malicious web traffic patterns or access requests to unsafe domains but may also collect and transmit information that affects the user's privacy.	**Context:** User browsing data can reveal information affecting privacy, such as personal health or financial information. Administrators can centrally view user browsing metadata at this location. This information may also be forwarded to other third-party tools. **Problematic Data Action:** Surveillance, Unanticipated Revelation **Problem:** Loss of Trust. Users may perceive the monitoring of their web traffic as a form of surveillance which may negatively impact the trust they have in their IT systems and/or organization.	**Predictability**: Users should be informed on the capabilities of web monitoring 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 use web monitor tools should assess their privacy preserving capabilities. In this reference architecture Symantec Web Isolation provides a privacy toggle that allows for user browsing data to be anonymized. **Disassociability**: Organizations should employ de-identification options for data when appropriate. In this reference architecture the privacy toggle provided by Symantec Web Isolation was enabled, which anonymized user browsing data. **Confidentiality:** Organizations should mandate strict access controls for security tools that can impact user privacy, including the use of MFA.

576

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 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

API	Application Programming Interface
BYOD	Bring Your Own Device
CIA	Confidentiality Integrity Availability
CIS	Center for Internet Security
CNSSI	Committee on National Security Systems Instruction
COBIT	Control Objectives for Information and Related Technologies
CRADA	Cooperative Research And Development Agreement
CSC	Critical Security Controls
CSF	Cybersecurity Framework
FIPS	Federal Information Processing Standard
FIPPS	Fair Information Privacy Principles
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDAM	Identity and Access Management
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
PDA	Problematic Data Action
PII	Personally Identifiable Information
PIN	Personal Identification Number
PRAM	Privacy Risk Assessment Methodology
RDP	Remote Desktop Protocol
RMF	Risk Management Framework
SMS	Short Messaging Service
SP	Special Publication
URL	Uniform Resource Locator
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
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 1.0
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
Key Management	The activities involving handling of cryptographic keys and other related security parameters (e.g. passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction. SOURCE: CNSSI 4009-2015
Manageability	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure. SOURCE: NISTIR 8062
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. SOURCE: CNSSI 4009-2015
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
Multi-Factor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). SOURCE: CNSSI 4009-2015
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

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

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

[9] 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.

[10] R. Ross *et. al*, *Developing Cyber-Resilient Systems: A Systems Security Engineering* Approach, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 2 Revision 1, Gaithersburg, Md., Dec. 2021, 309 pp. Available: https://doi.org/10.6028/NIST.SP.800-160v2r1

[11] 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.

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

[15] 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.

[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 Cybersecurity Center of Excellence, Mobile Device Security, Bring Your Own Device Practice Guide, NIST SP 1800-22, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-22.pdf

[18] NIST Privacy Framework Repository, 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**
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16

Cybersecurity Framework v1.1			Standards & Best Practices
Function	**Category**	**Subcategory**	**Informative References**
		ID.RA-3: Threats, both internal and external, are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM16
PROTECT (PR)	Identity Management, Authentication and AccessControl (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-3: Remote access is managed	CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC5, AC-6, AC-14, AC-16, AC-24

Cybersecurity Framework v1.1			Standards & Best Practices
Function	**Category**	**Subcategory**	**Informative References**
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12

Cybersecurity Framework v1.1			Standards & Best Practices
Function	**Category**	**Subcategory**	**Informative References**
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
	Information Protection Processes and Procedures (PR.IP)	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
	Protective Technology (PR.PT)	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family

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 (IS0) standard 27701 references were not mapped by NIST, but by an external organization. They are available at the NIST Privacy Framework Repository [18] 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**
	IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.	**FIPPS 7:** Purpose Specification/Use Limitation **NIST SP 800-37 Rev. 2:** Task P-10 **NIST SP 800-53 Rev. 5:** CM-8 (10), CM-12, CM-13, PM-5 **NIST IR 8062** **NIST PRAM:** Worksheet 2 **ISO/IEC 27701:2019** 7.2.8, 8.2.6
	CONTROL-P (CT-P): Develop and Optional (Risk Based) 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

Privacy Framework 1.0				Standards and Best Practices
	Function	Category	Subcategory	Informative Refences
		Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).	**CT.DP-P2:** Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).	**FIPPS 7:** Purpose Specification/Use Limitation **NIST SP 800-53 Rev. 5:** AC-23, AU-3(3), IA-4(8), PE-8(3), SA-8(33), SI-12(1), SI-12(2), SI-19 **NIST SP 800-63-3** **NIST SP 800-188 (draft)** **NIST IR 8053** **NIST IR 8062** **ISO/IEC 27701:2019** 7.4.2, 7.4.4
		Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P3:** System/product/service design enables data processing visibility.	**FIPPS 7:** Purpose Specification/Use Limitation **NIST SP 800-53 Rev. 5:** PL-8, PT-5(1), SA-17, SC-42(4) **NIST IR 8062** **ISO/IEC 27701:2019** 7.3.2, 7.3.3, 8.3.1
	PROTECT-P (PR-P): Develop and Implement appropriate data processing safeguards.	**Data Protection Policies, Processes, and Procedures (PR.PO-P)**: Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and	**PR.PO-P4:** Policy and regulations regarding the physical operating environment for organizational assets are met.	**FIPPS 5:** Quality and Integrity **FIPPS 7:** Purpose Specification/Use Limitation **NIST SP 800-53 Rev. 5:** PE-1 **ISO/IEC 27701:2019** All of 6.8

Privacy Framework 1.0				Standards and Best Practices
	Function	Category	Subcategory	Informative Refences
		management commitment), processes, and procedures are maintained and used to manage the protection of data.		
		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 the assessed risk of unauthorized access.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	**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
			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-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 **NIST SP 800-162**

Privacy Framework 1.0				Standards and Best Practices
	Function	Category	Subcategory	Informative Refences
			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 organizational risks).	**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**
		Data Security (PR.DS-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P1:** Data-at-rest are protected.	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28 **NIST SP 800-175B**
			PR.DS-P2: Data-in-transit are protected.	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** SC-8, SC-11 **NIST SP 800-175B**
			PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	**FIPPS 8: Security** **NIST SP 800-53 Rev. 5:** CM-8, MP-6, PE-16, PE-20

NIST SPECIAL PUBLICATION 1800-28C

Data Confidentiality:
Identifying and Protecting Data Against Data Breaches

Volume C:
How-To Guides

William Fisher
National Cybersecurity Center of Excellence
NIST

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

December 2023

DRAFT

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

DISCLAIMER

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

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

National Institute of Standards and Technology Special Publication 1800-28C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-28C, 86 pages, (December 2023), CODEN: NSPUE2

FEEDBACK

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

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

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

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Attacks that target data are of concern to companies and organizations across many industries. Data breaches represent a threat that can have monetary, reputational, and legal impacts. This guide seeks to provide guidance around the threat of data breaches, exemplifying standards and technologies that are useful for a variety of organizations defending against this threat. Specifically, this guide identifies risks associated with the loss of data confidentiality, and mitigations to protect against those risks.

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

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

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

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

DOCUMENT CONVENTIONS

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

CALL FOR PATENT CLAIMS

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

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

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

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

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

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

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

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

Contents

1 Introduction

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

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

1.1 How to Use this Guide

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

This guide contains three volumes:

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

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

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

- challenges that enterprises face in identifying vulnerable assets and protecting them from data breaches
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-28B*, which describes what we did and why. The following sections will be of particular interest:

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

You might share the *Executive Summary, NIST SP 1800-28A*, with your leadership team members to help them understand the importance of adopting a standards-based solution to identify threats to and protect from a loss of data confidentiality

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800*-28C, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

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

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to ds-nccoe@nist.gov .

1.2 Build Overview

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

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

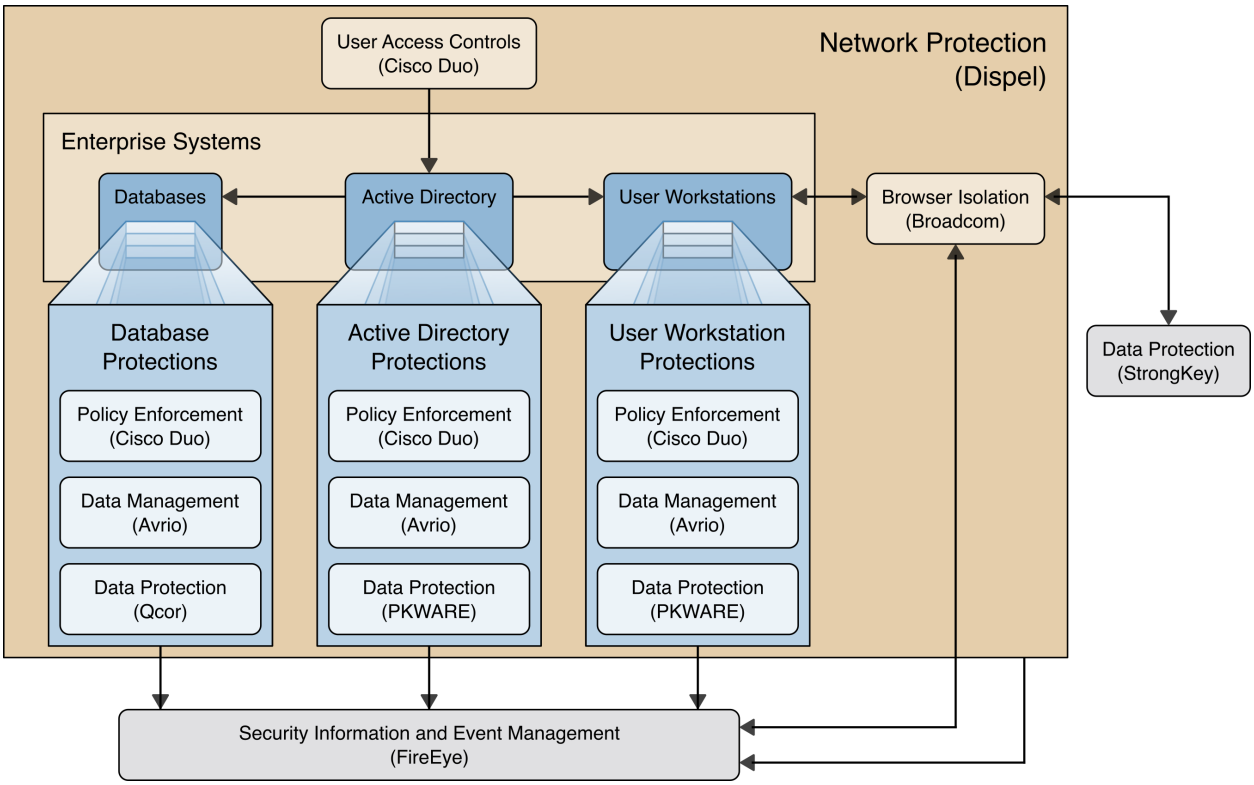
1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

1.4 Logical Architecture Summary

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



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

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

2 Product Installation Guides

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

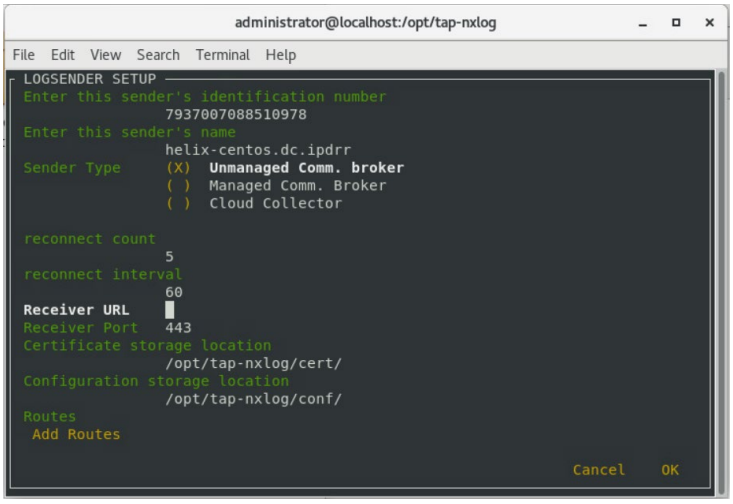
2.1 FireEye Helix

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

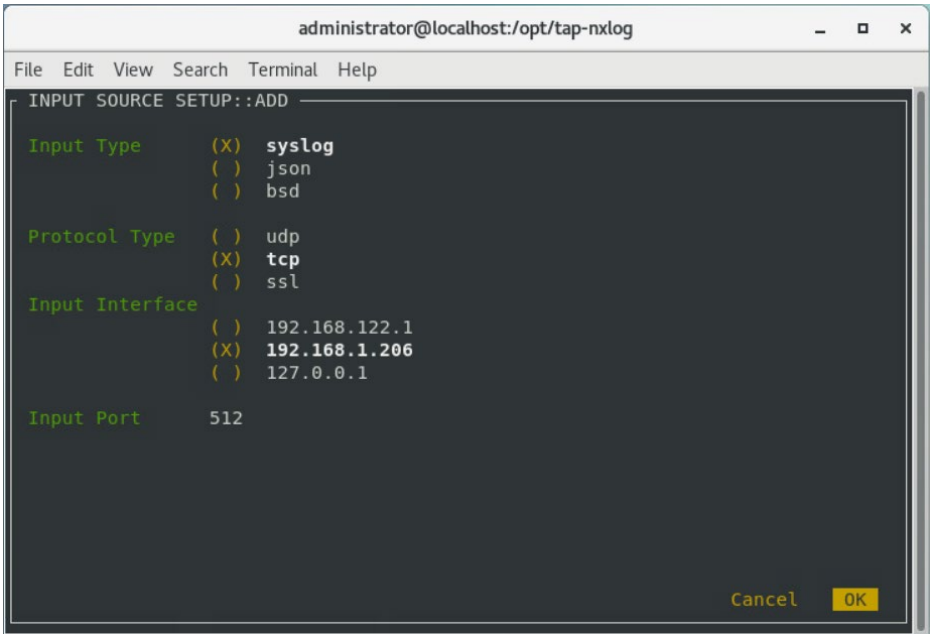
In this setup, we detail the installation of a communications broker which will be used to collect logs from the enterprise and forward them to the cloud deployment. This installation took place on a CentOS 7 Virtual Machine.

Installing the Communications Broker- CentOS 7

1. Acquire the Helix Communications Broker for CentOS 7.
2. Navigate to the folder containing the installer, and run
   ```
   > sudo yum localinstall ./cbs-installer_1.4.2-9.x86_64.rpm
   ```
3. Log on to the Helix web console.
4. Navigate to **Dashboards** > **Operational**.
5. Click **Download Certificate**.
6. Click **Download**. This will download a “bootstrap.zip” file.
7. Copy the zip file to the Helix Communications Broker certificate directory.
   ```
   > sudo cp bootstrap.zip /opt/tap-nxlog/cert
   ```
8. Navigate to the certificate directory.
   ```
   > cd /opt/tap-nxlog/cert
   ```
9. Extract the zip file you just copied.
   ```
   > sudo unzip ./bootstrap.zip
   ```
10. If prompted, select “Yes” to overwrite any previous certificate files.
11. Navigate to one folder above.
    ```
    > sudo cd ..
    ```
12. Run the setup script.
    ```
    > sudo ./setup.sh
    ```
13. Enter the name of the CentOS machine.
14. Enter the receiver URL provided in the Helix welcome email.



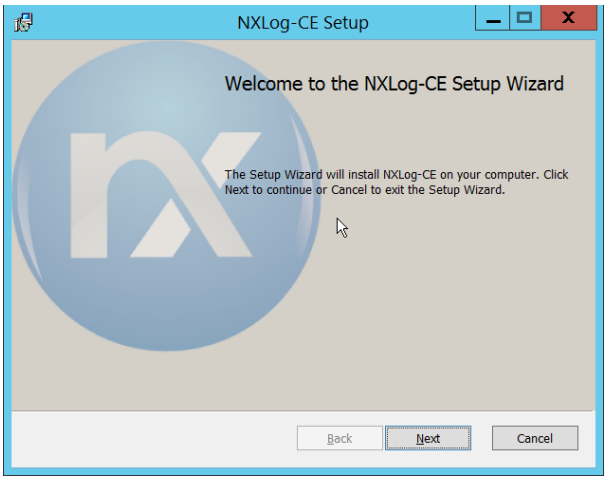
15. Select **Add Routes** and press **Enter**.
16. Select **syslog**.
17. Select **tcp**.
18. Select the IP address of the machine where logs should be sent.
19. Enter 512 for the port number where logs should be sent.



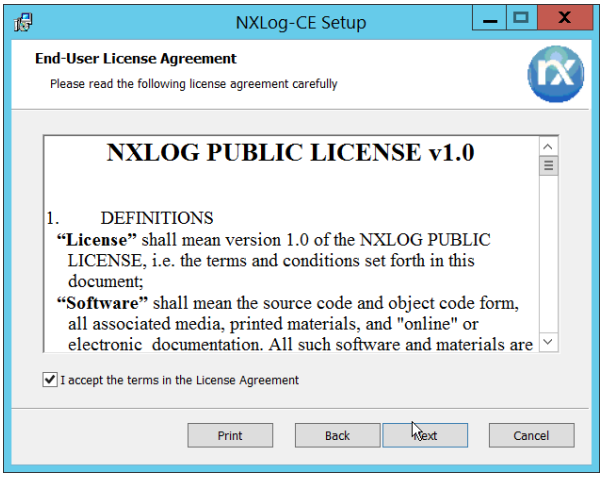
20. Select **OK** and press **Enter**.
21. Review the configuration, then select **OK** and press **Enter**.

Forwarding Event Logs from Windows 2012 R2

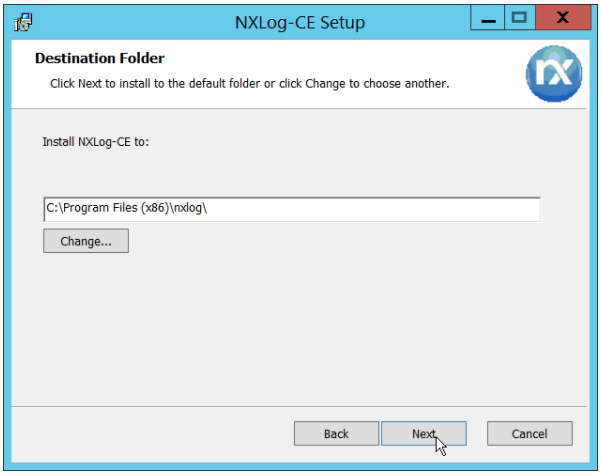
22. Acquire **nxlog-ce-2.10.2150.msi** from http://nxlog.org/products/nxlog-community-edition/download.
23. Run **nxlog-ce-2.10.2150.msi**.



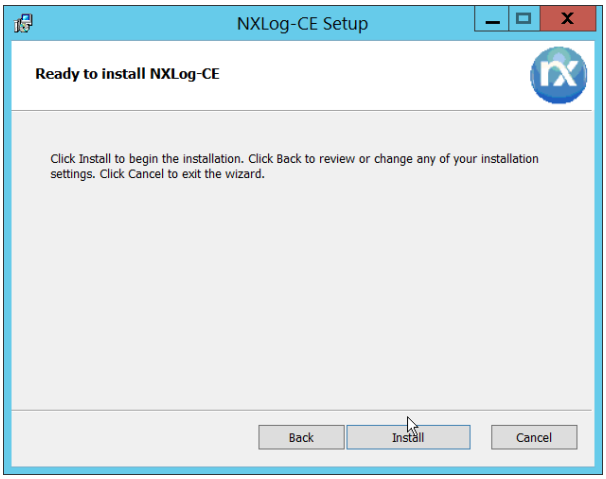
24. Click **Next**.
25. Check the box next to **I accept the terms in the License Agreement**.



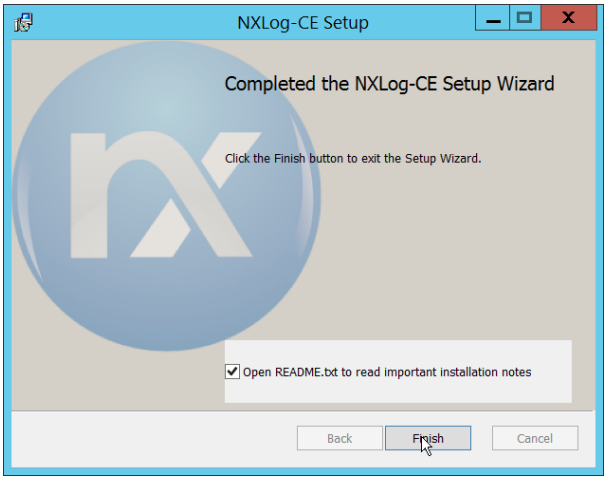
26. Click **Next**.



27. Click **Next**.



299 28. Click **Install**.



300 29. Click **Finish**.

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

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

```
Panic Soft
#NoFreeOnExit TRUE

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

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

<Extension _syslog>
    Module      xm_syslog
</Extension>

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

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

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

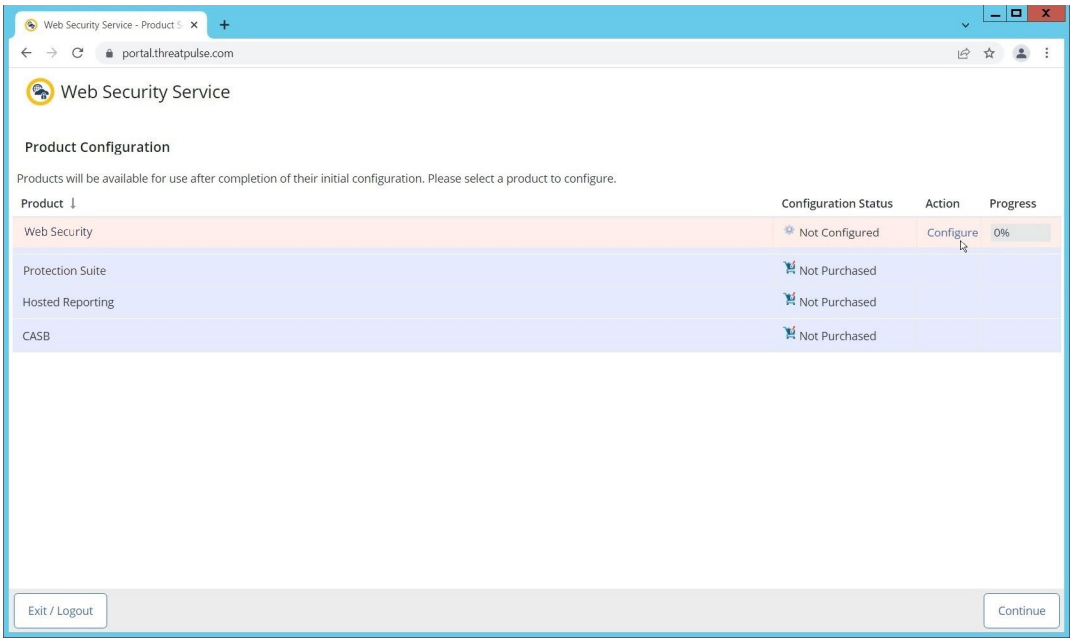
32. Restart the **nxlog** service.
33. You can verify that this connection is working by checking the logs in *data\nxlog.log*, and by noting an increase in events on the Helix Dashboard.

2.2 Symantec Cloud Secure Web Gateway

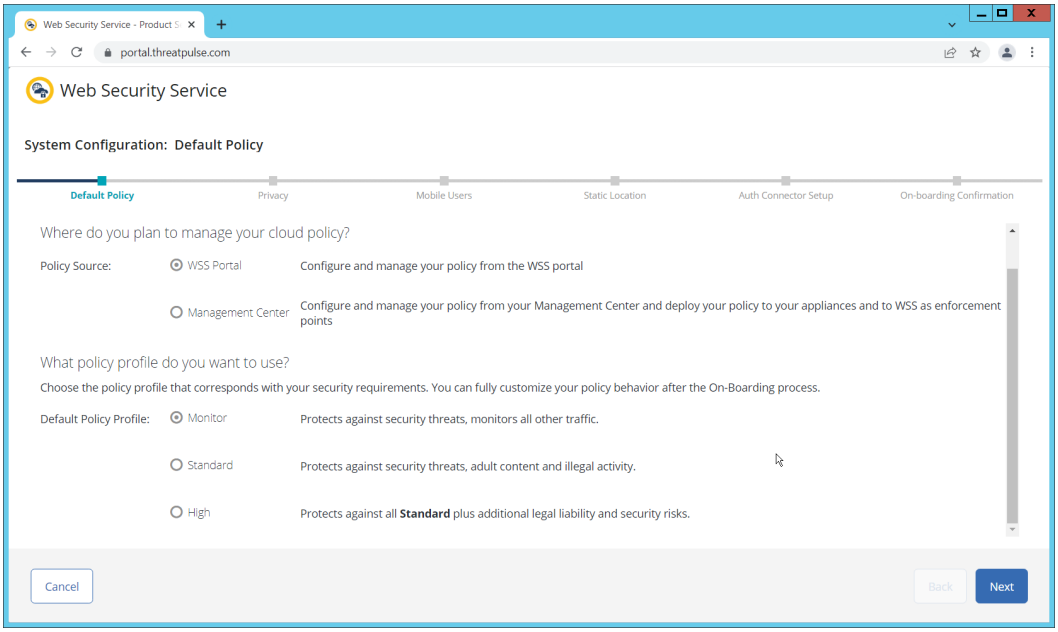
This installation and configuration guide for Symantec SWG uses a cloud instance of Web Isolation. In this guide, Web Isolation is used to isolate threats to the user through the browser. It does this through the use of a web proxy, which captures traffic and assigns a threat level to it, and based on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

Configure Web Security Service

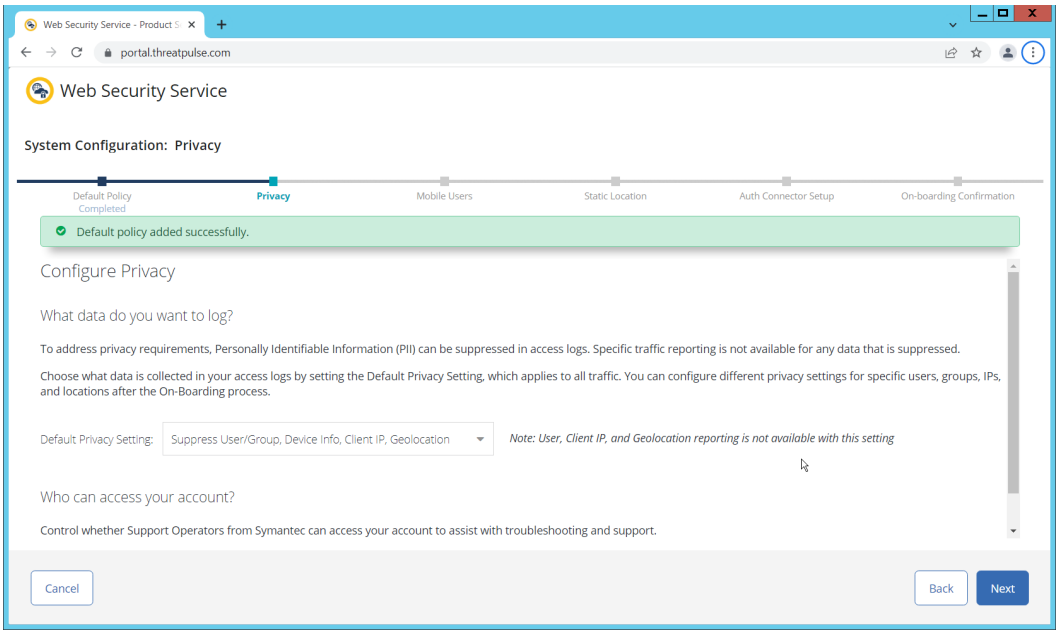
1. Login to the Symantec portal by navigating to https://portal.threatpulse.com/.



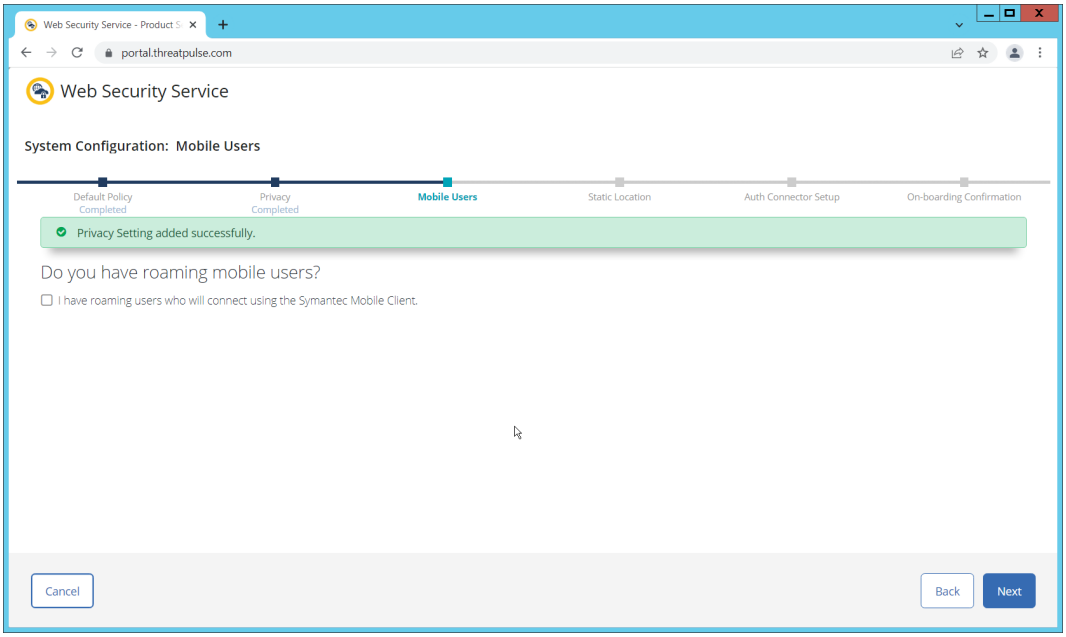
2. Click **Configure** next to Protection Suite.
3. Select **WSS Portal**.
4. Select **Monitor**.



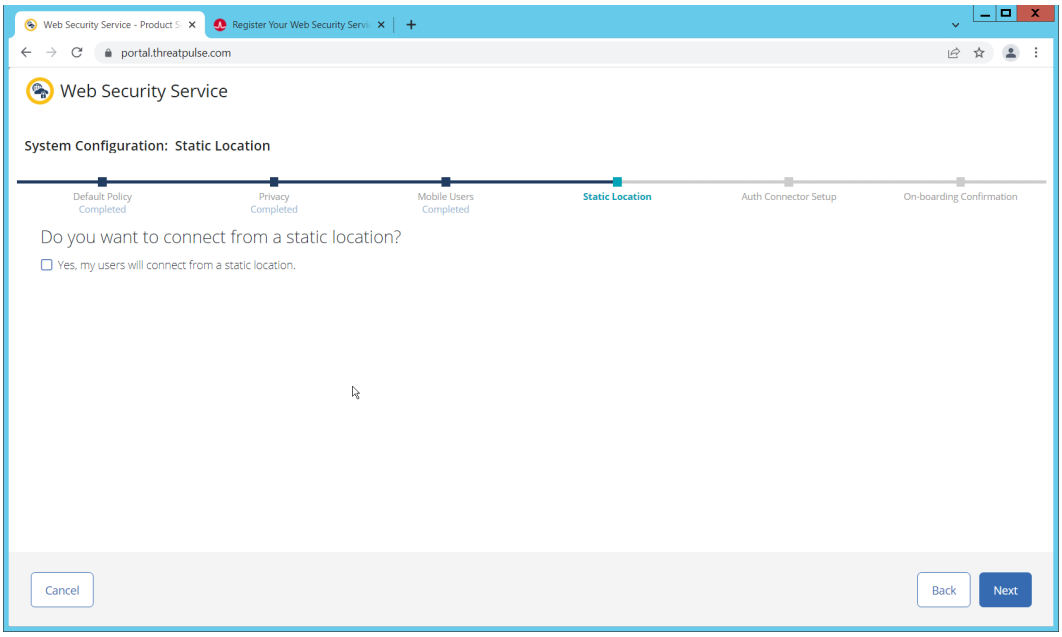
5. Click **Next**.
6. Select **Suppress User/Group, Device Info, Client IP, Geolocation**. (Note: If you are planning to use this tool for network monitoring of organizational users, a less strict privacy policy may be preferable; however, for this build, we are using Web Isolation primarily for external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



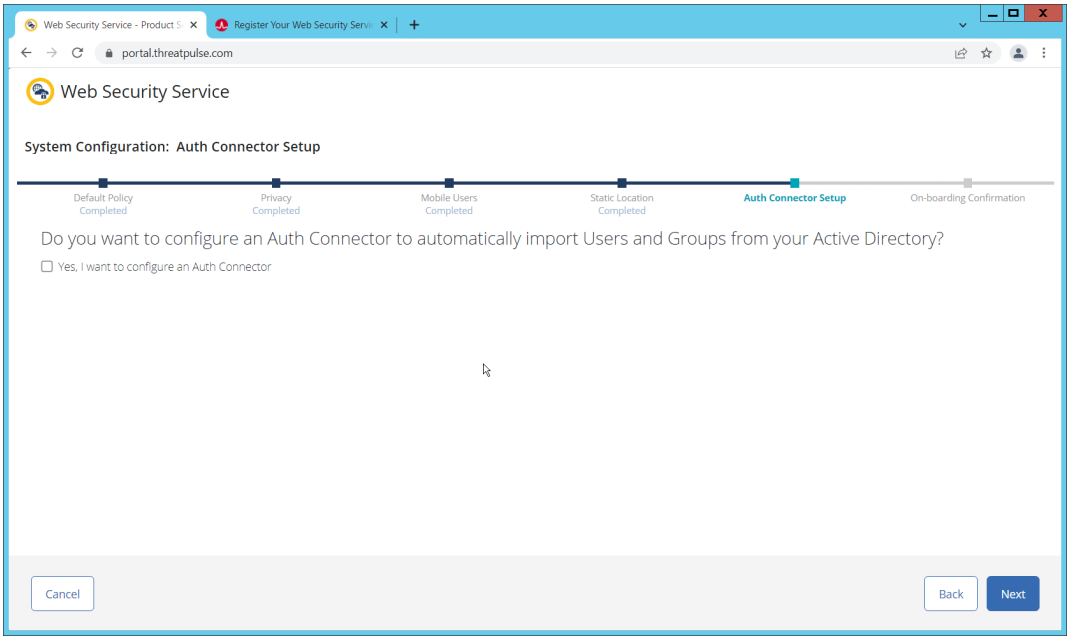
7. Click **Next**.
8. Indicate whether you have mobile users.



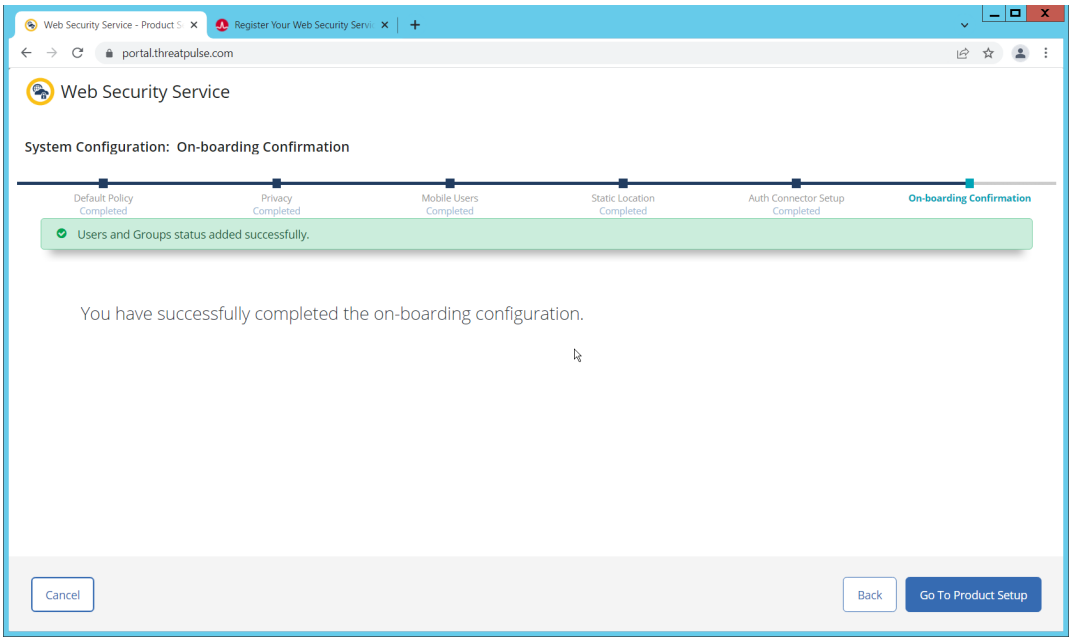
9. Click **Next**. Indicate whether your users connect from a static location.



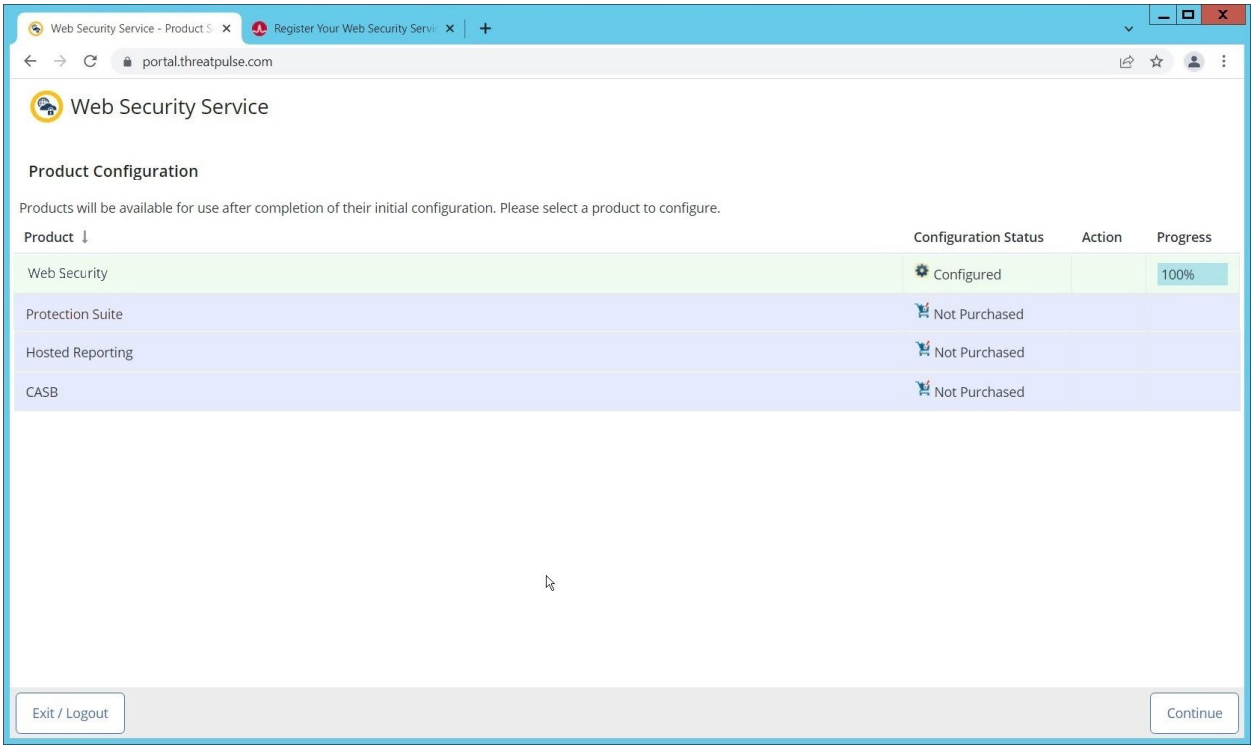
325 10. Click **Next**. Indicate whether you want to configure an Auth Connector.



326 11. Click **Next**.



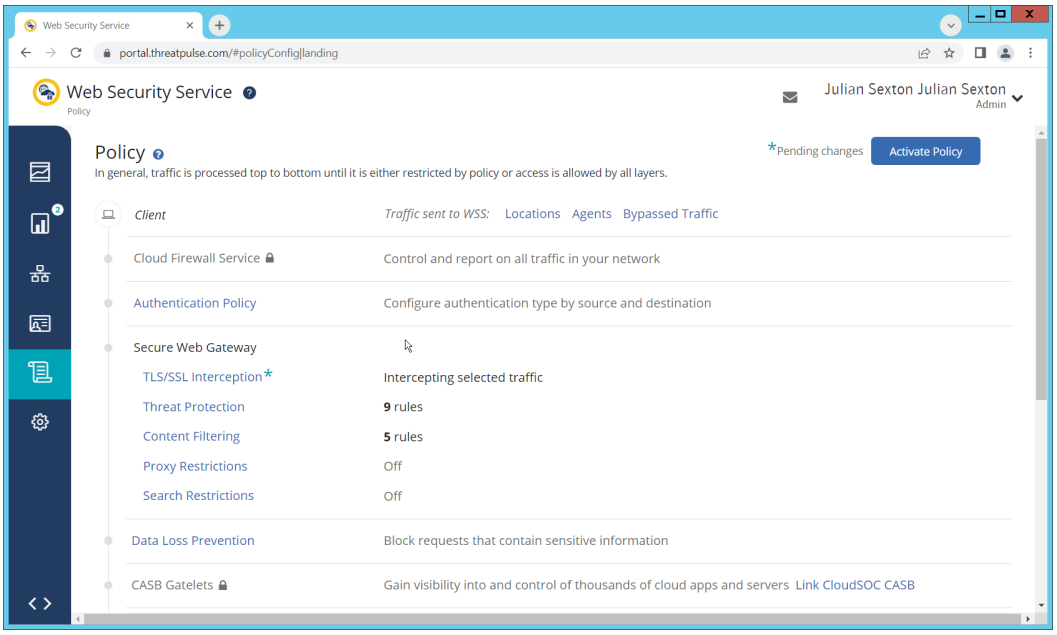
12. Click **Go To Product Setup**.



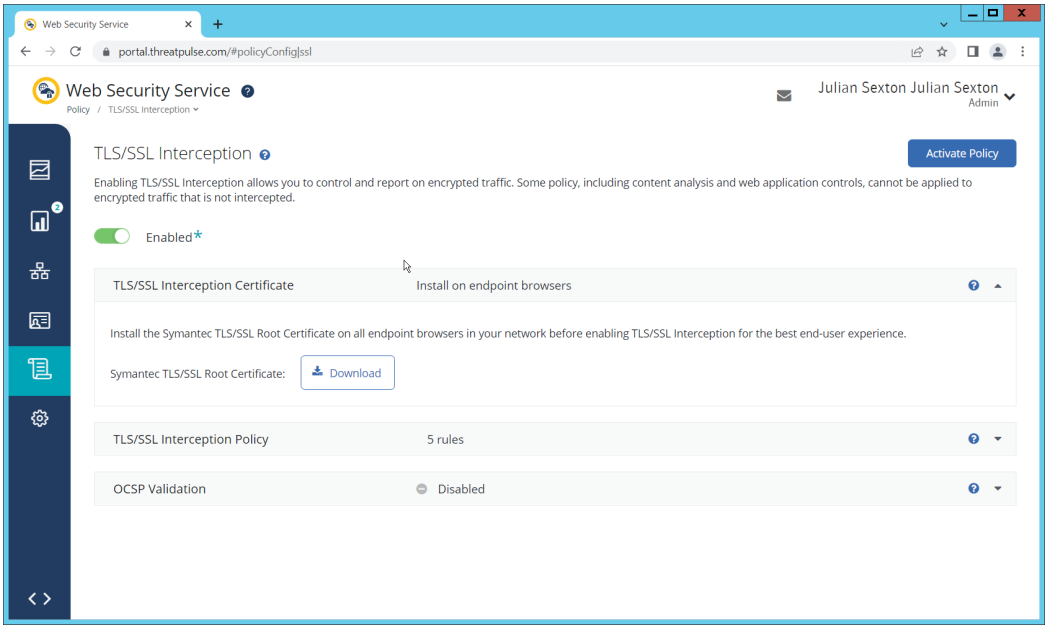
13. Click **Continue**.

Install Proxy Certificates and enabling TLS/SSL Interception

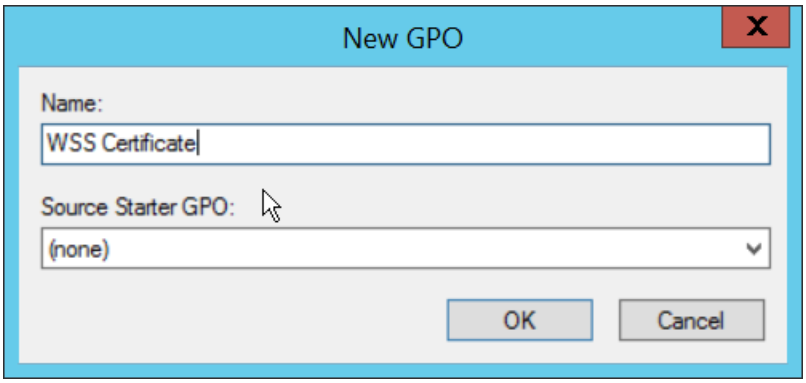
1. Click the **Policy** tab.



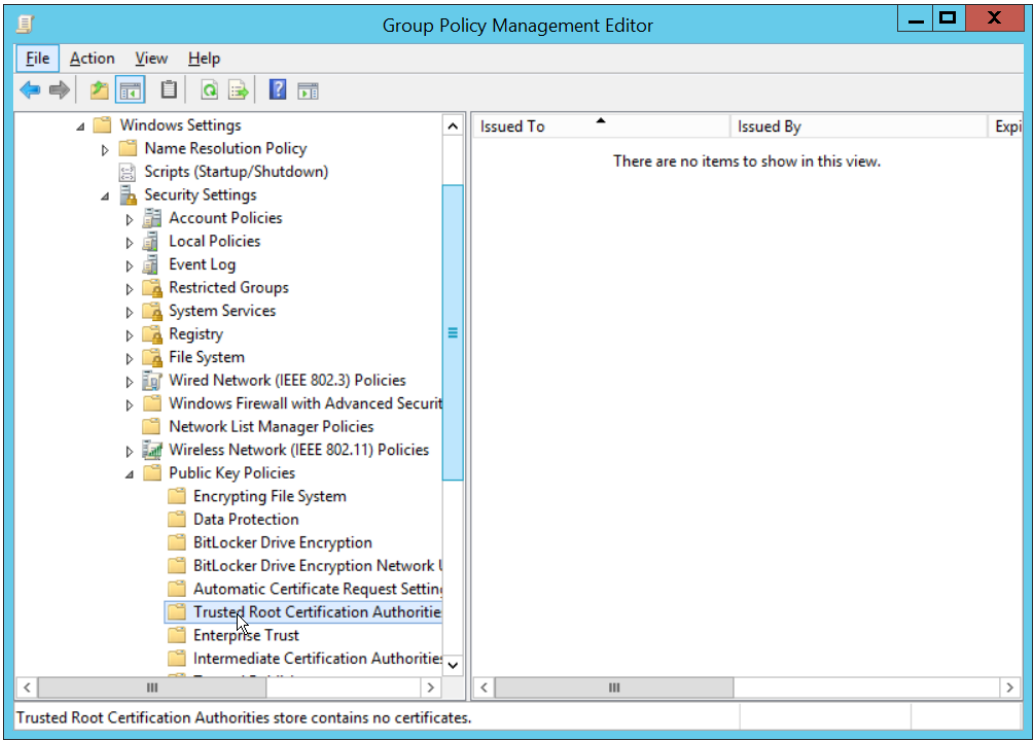
2. Click **TLS/SSL Interception**.
3. Enable TLS/SSL interception by clicking the toggle.



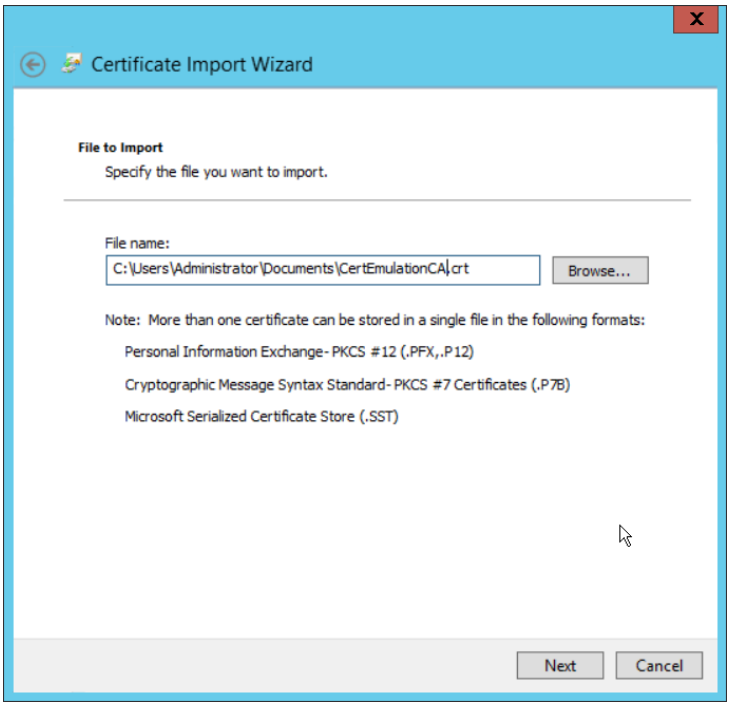
4. Download the certificate here. You can either install this individually in the Trusted Root Certification Authorities store on individual machines or follow the below steps to distribute the certificate via Group Policy.
5. Open the **Group Policy Management Console**.
6. Right click the **Domain**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



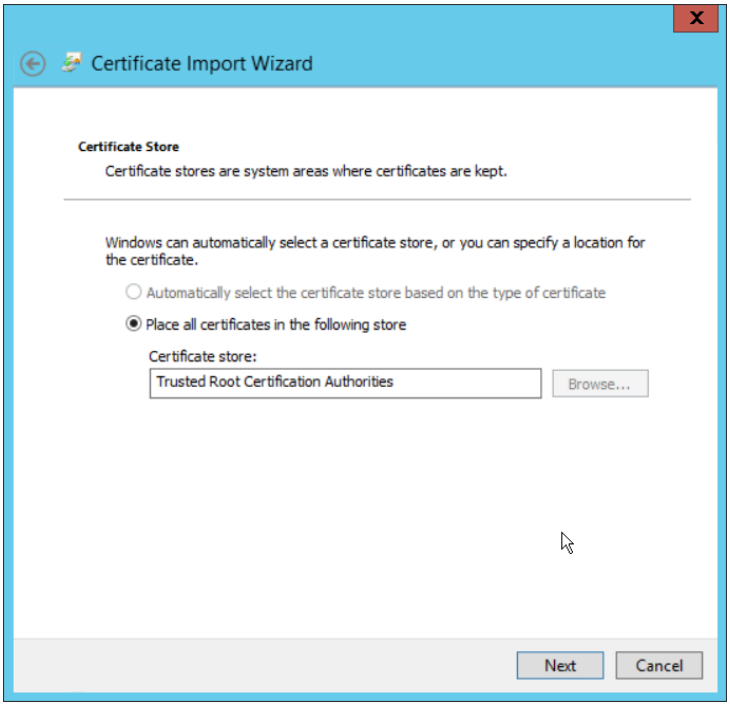
7. Enter a name and click **OK**.
8. Right click the newly created GPO and click **Edit…**.



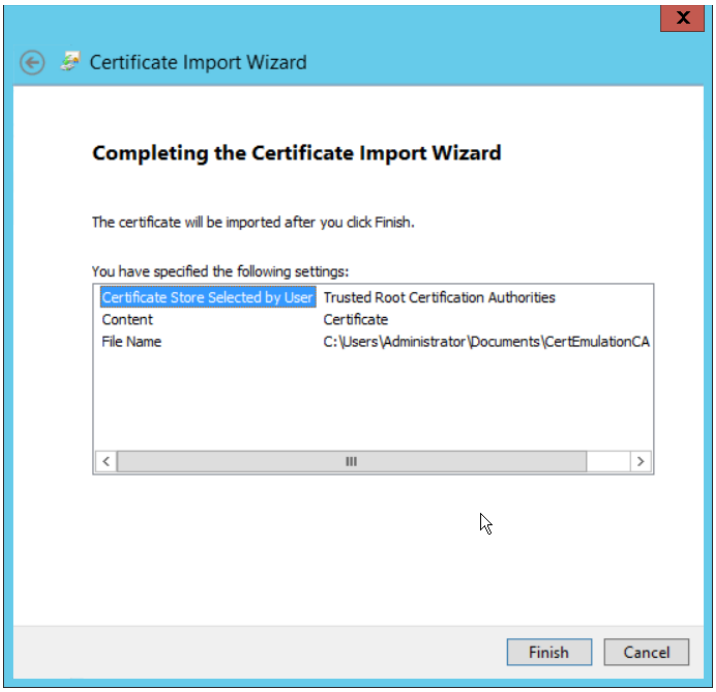
9. Navigate to **Computer Configuration > Policies > Window Settings > Security Settings > Public Key Policies**, and right click **Trusted Root Certification Authorities**.
10. Click **Import**.
11. Click **Next**.
12. Select the certificate you just downloaded.



345 13. Click **Next**.



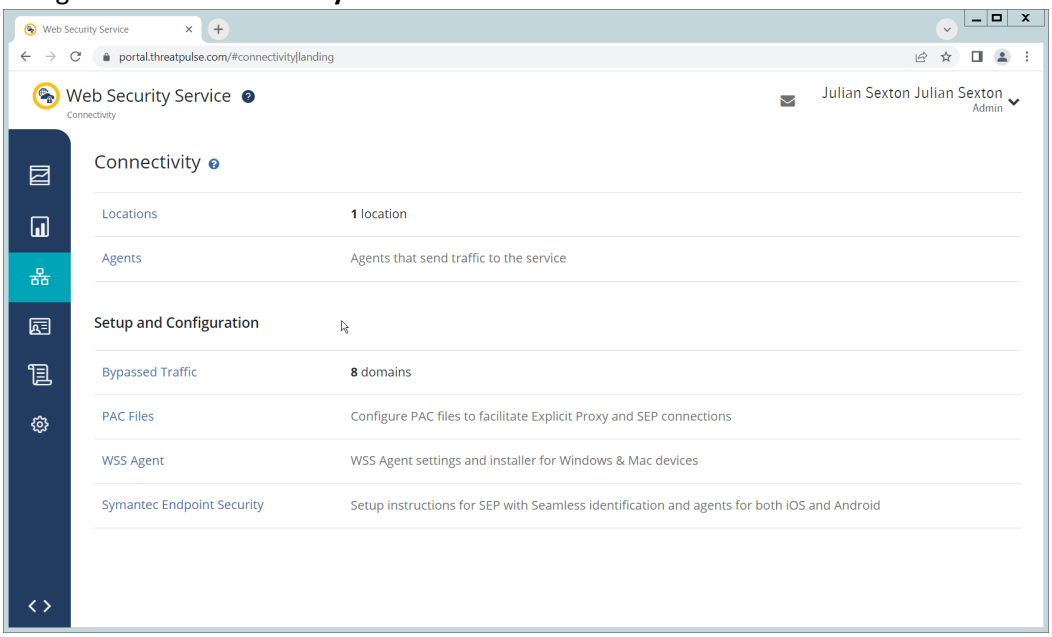
346 14. Click **Next**.



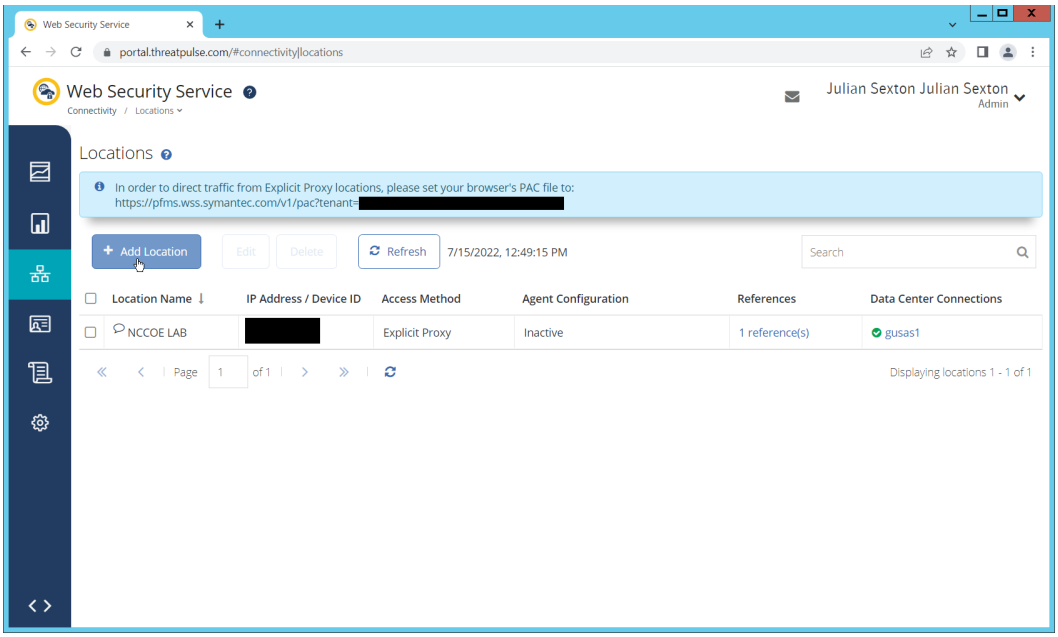
15. Click **Finish**.
16. Click **OK**.

Configure Symantec Web Security Service Proxy

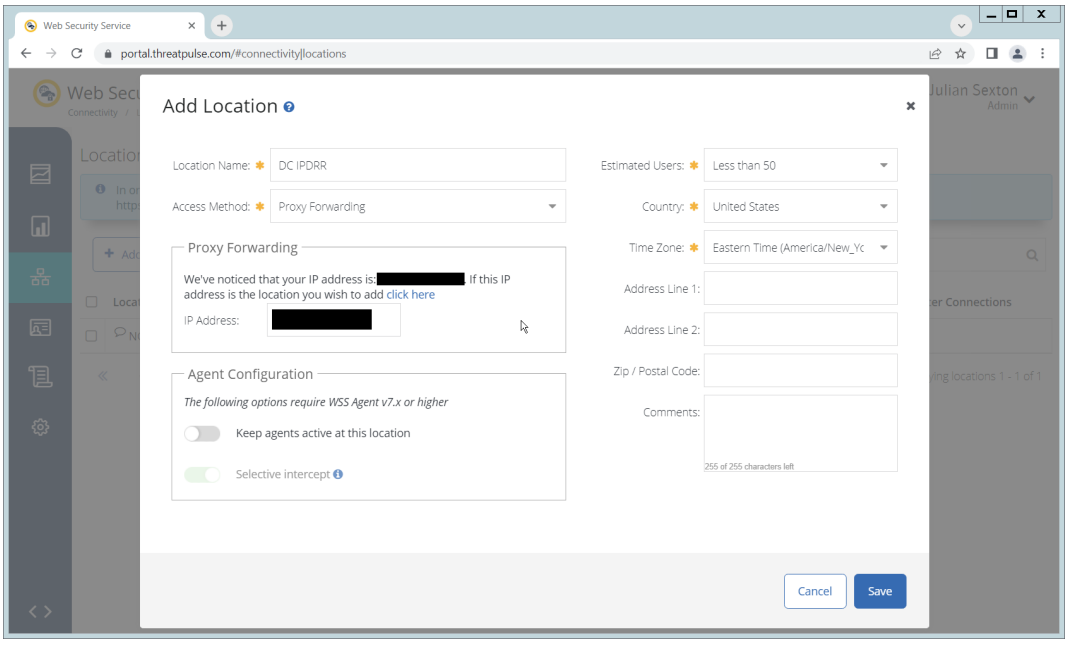
1. Navigate to the **Connectivity** tab.



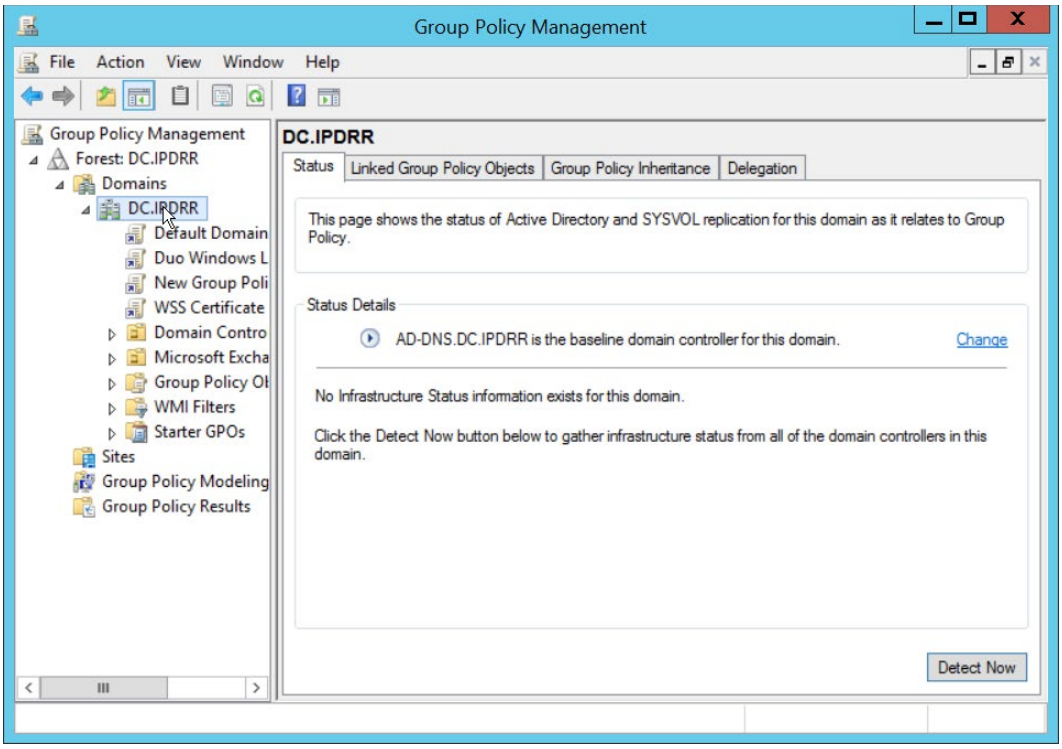
2. Click **Locations**.



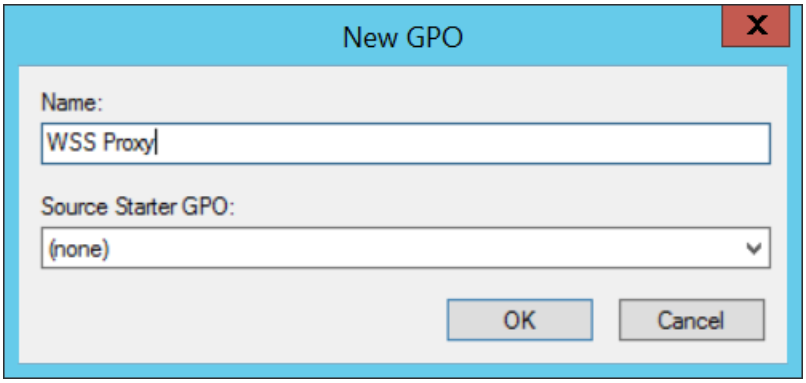
3. Click **Add Location**.
4. Enter a name for the **Location**.
5. Select **Proxy Forwarding** for **Access Method**.
6. Enter any public IP addresses of your organization, to ensure that traffic sent through the WSS proxy is redirected to the proper dashboard.



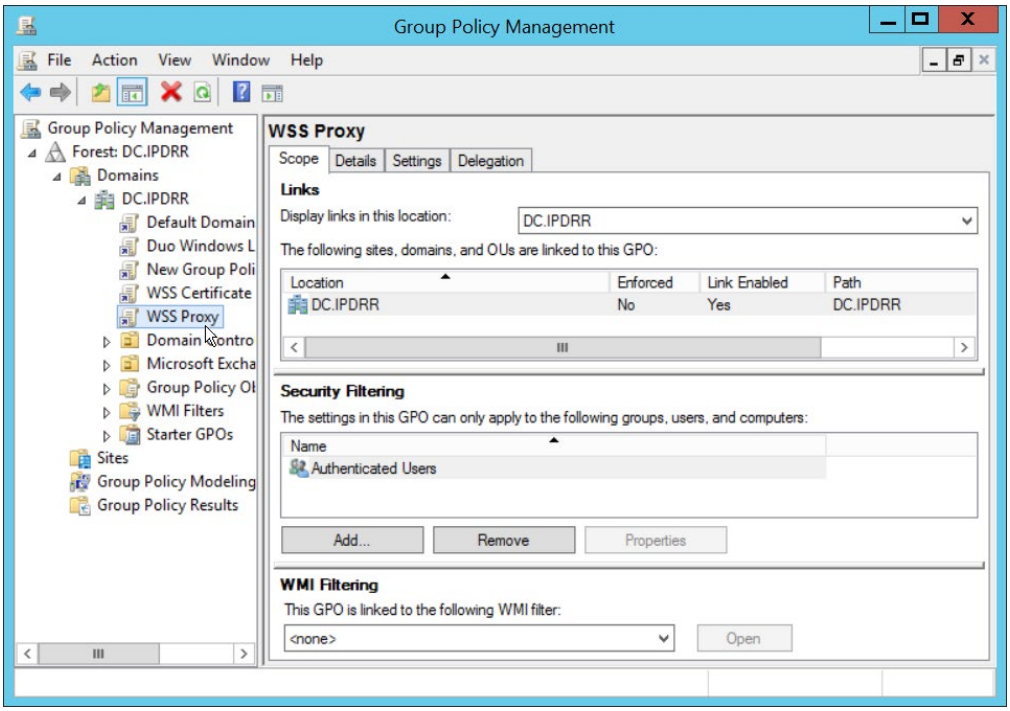
7. Click **Save**.
8. This page will now provide a URL to a PAC file which can be distributed to browsers across the organization via GPO. If you wish to create a custom PAC file, you can navigate to **Connectivity > PAC Files**.
9. Open the **Group Policy Management Console**.



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

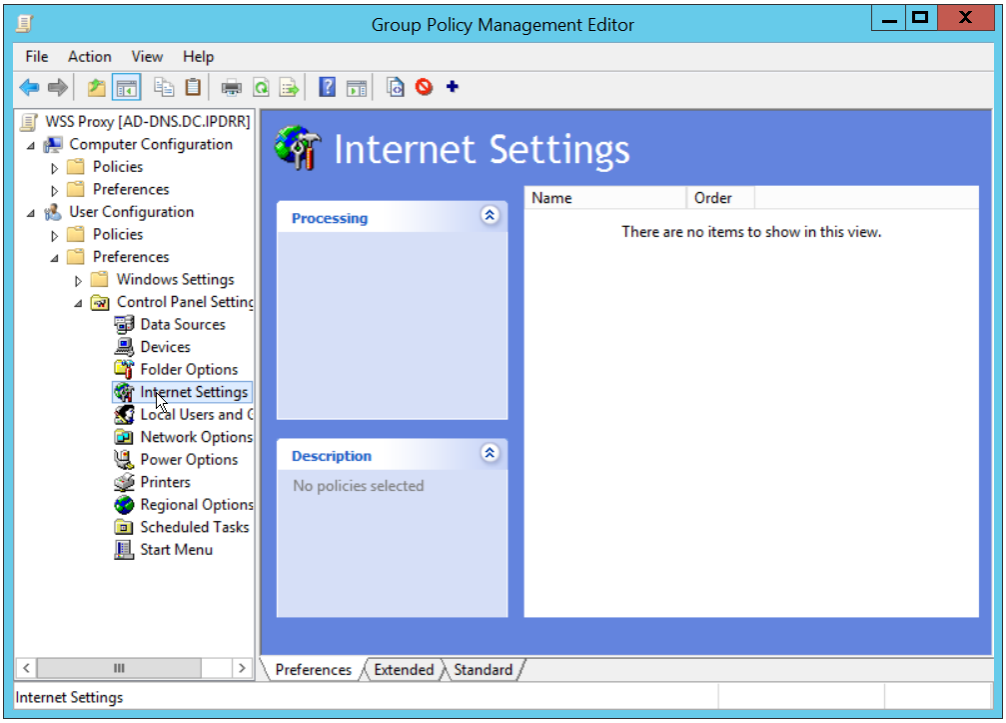


363 11. Enter a name and click **OK**.



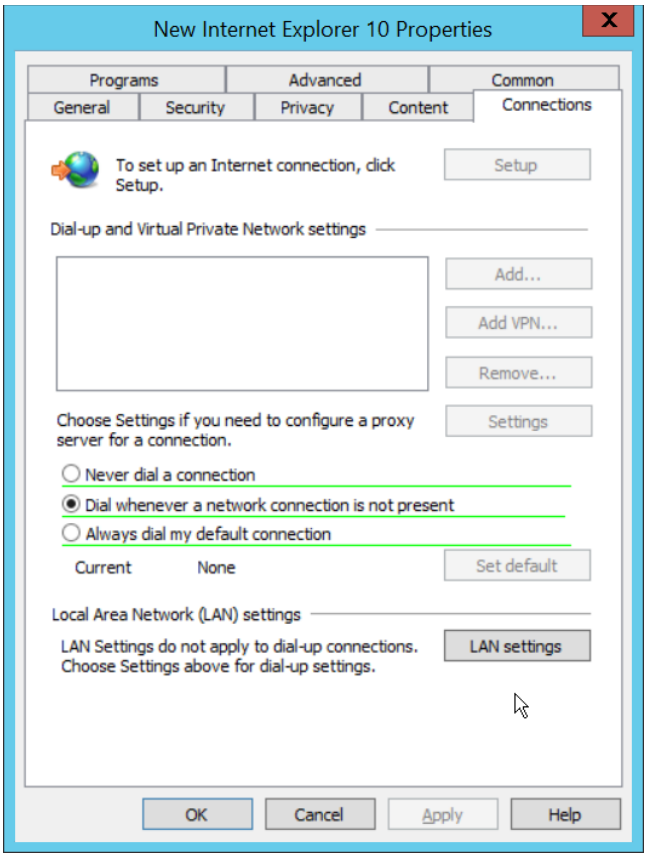
364 12. Right click the newly created GPO and click **Edit…**.

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

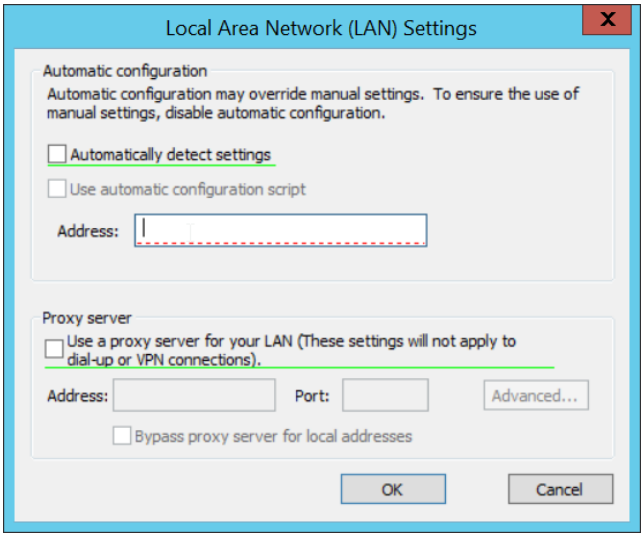


366 14. Right click **Internet Settings** and select **New** > **Internet Explorer 10 Properties**.

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



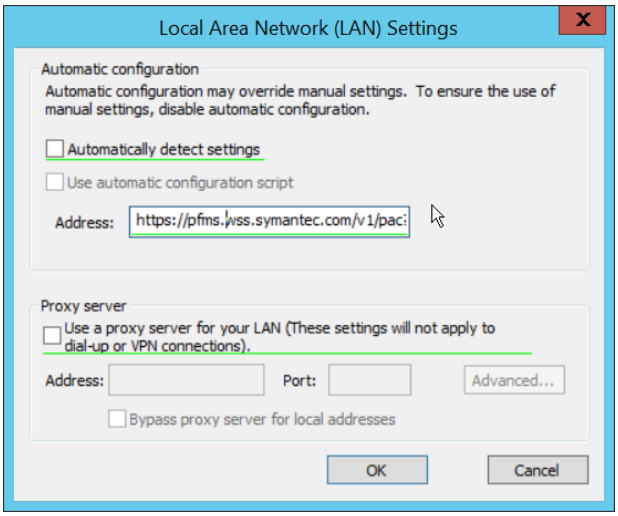
368 16. Click **Local Area Network (LAN Settings)**.



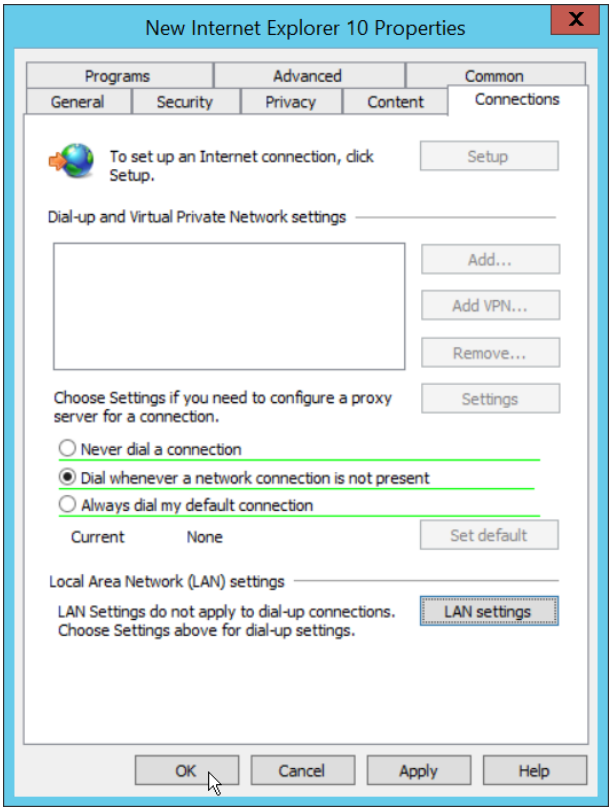
369 17. Select the **Address** field.

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

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

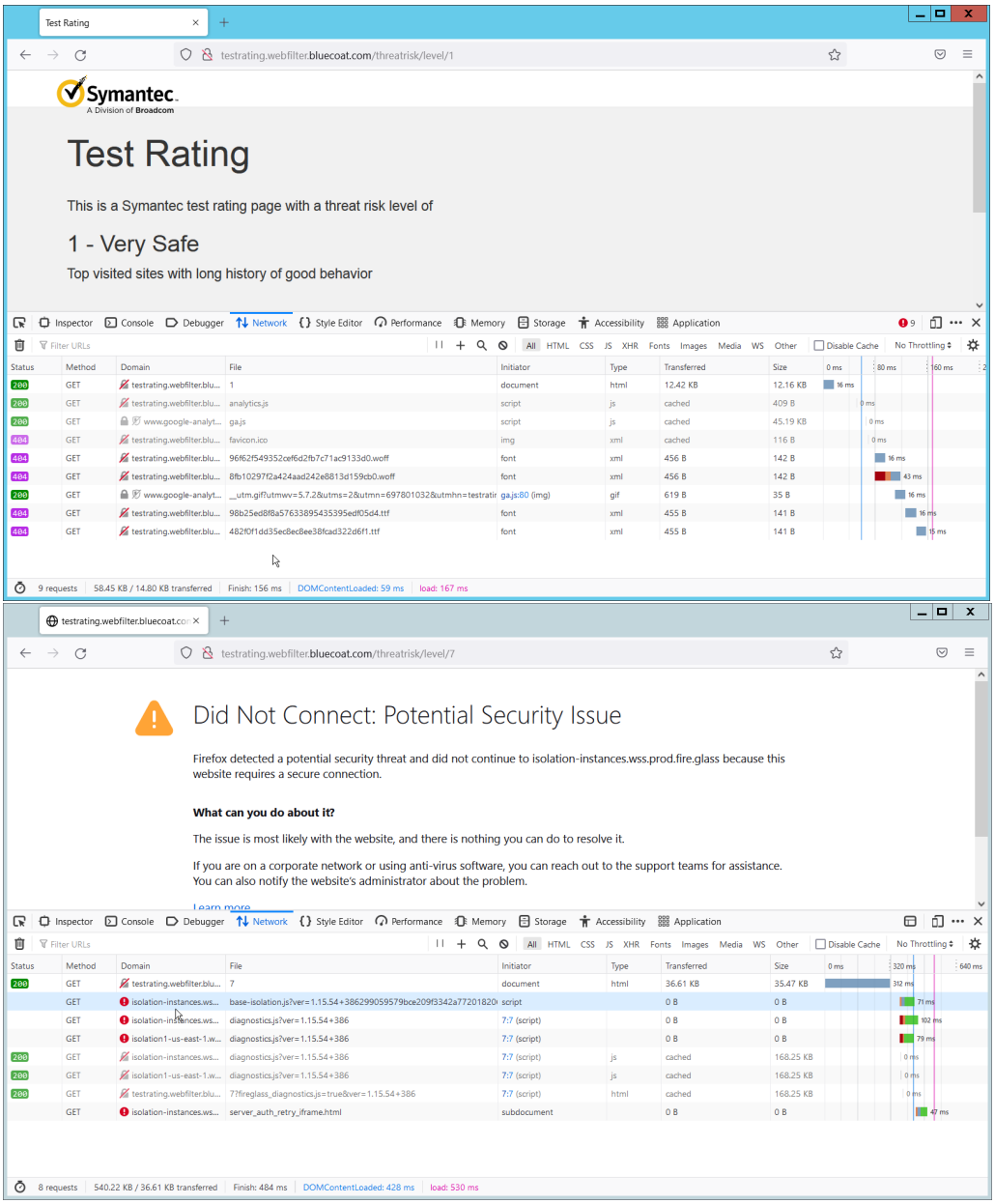


372 20. Click **OK**.



373 21. Click **OK**.

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



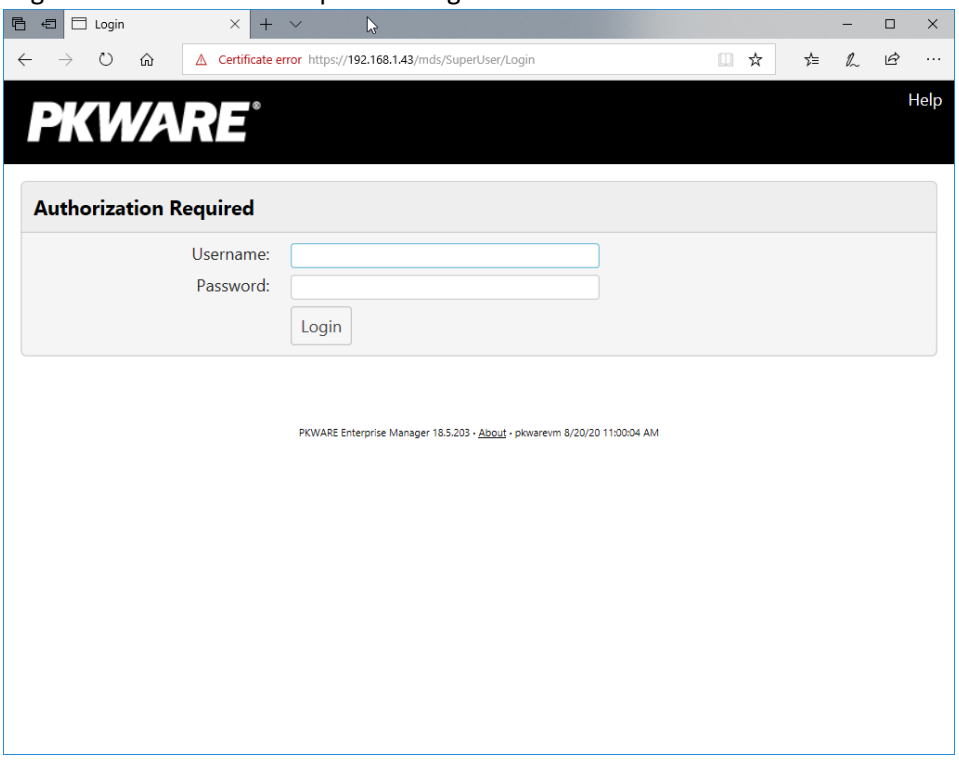
23. On this test URL (tested July 2022), levels 5-7 will go through isolation, and you will be able to see the isolation traffic from the network tab in developer mode (**F12**) on the browser. Levels 8-10 will be blocked by the content filter, and levels 1-4 will not go through isolation or content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

2.3 PKWARE PKProtect

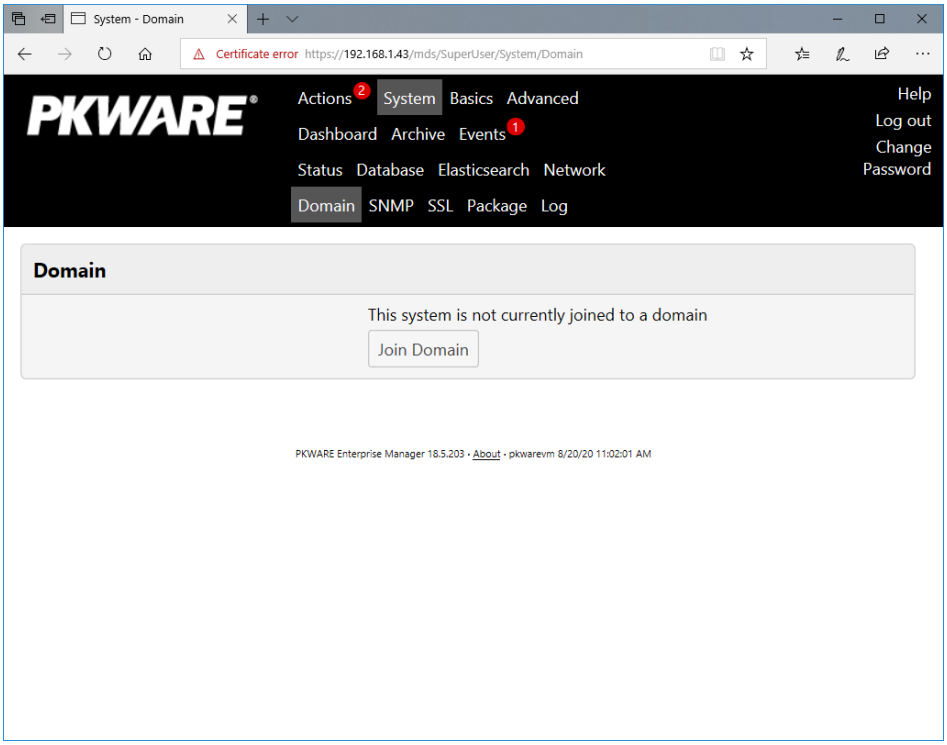
This installation and configuration guide for PKWARE PKProtect uses a physical PKWARE server, and as such will not delve into the installation of server components. In this guide, PKWARE is used to automatically perform data inventory and data protection functions. PKWARE provides users with the ability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

Configure PKWARE with Active Directory

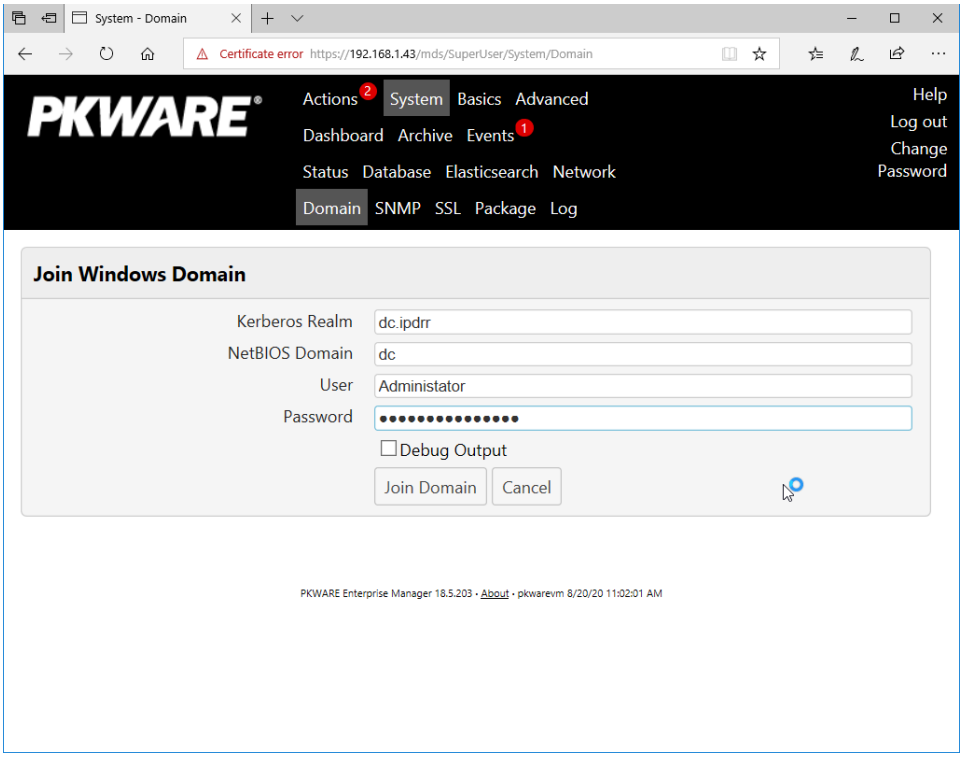
1. Login to the PKWARE web portal using the administrative credentials.



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



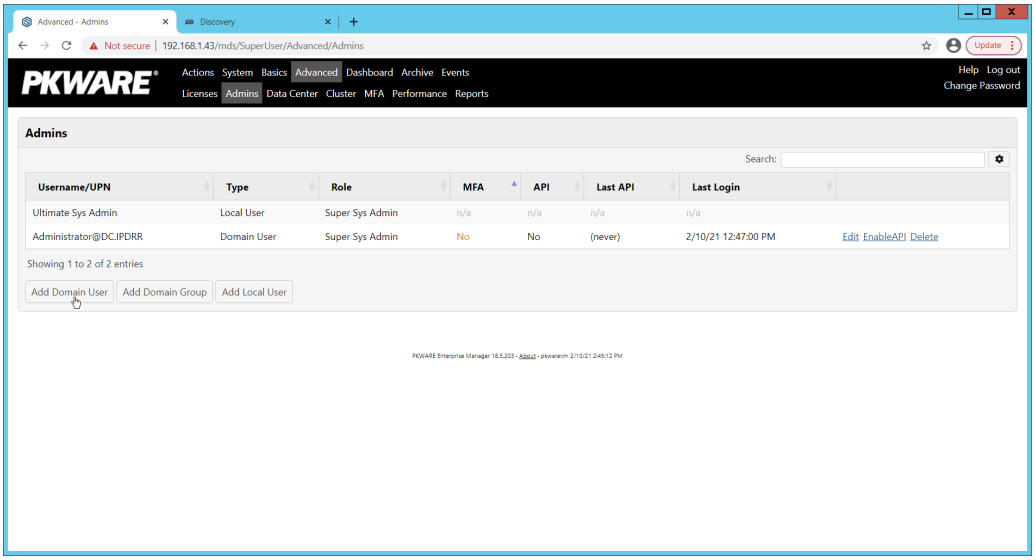
4. Click **Join Domain.**
5. Enter the **Kerberos Realm, NetBIOS Domain,** as well as the **username** and **password** of an administrative user on the domain.



6. Click **Join Domain.**

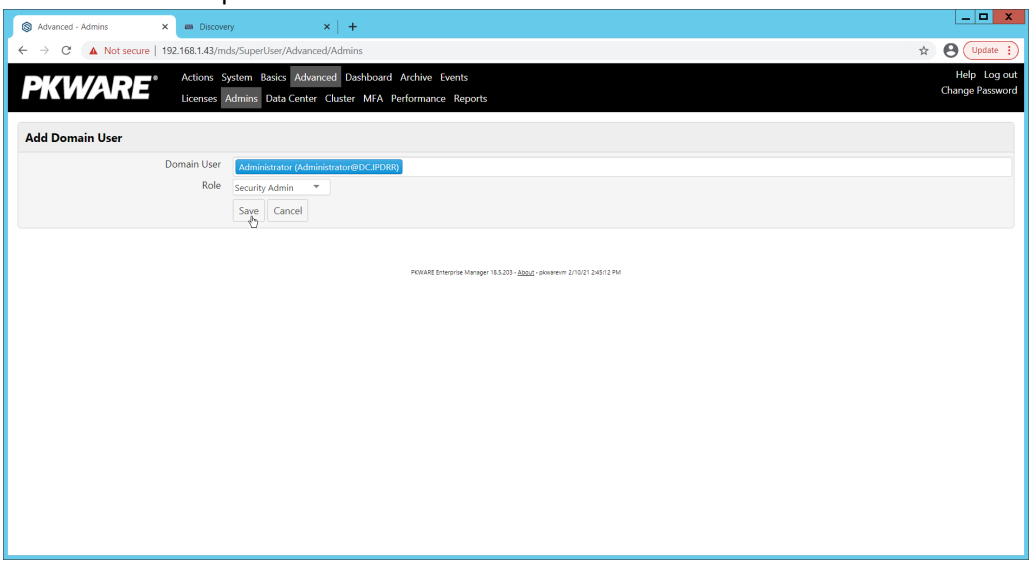
Create a New Administrative User

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



2. Click **Add Domain User.**
3. Enter the username of a user on the domain that should be able to login through the PKWARE management portal (this is meant for administrators only).

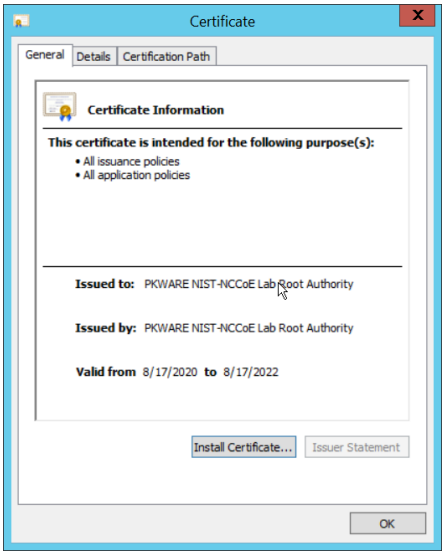
4. Select the level of permissions the user should have.



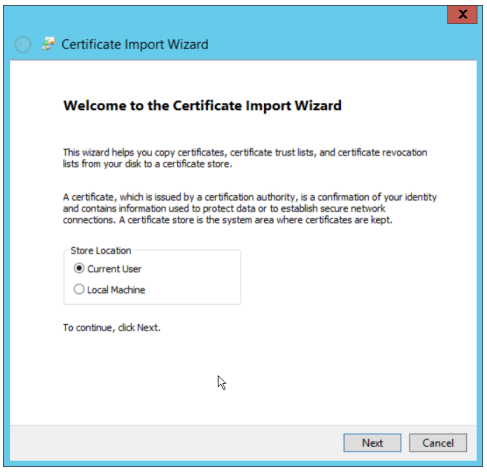
5. Click **Save.**

Install Prerequisites

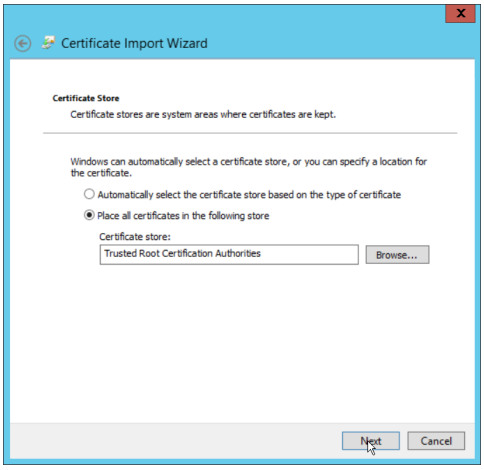
1. If needed for your environment, you may need to install certificates locally before agents can connect to PKProtect - ask your PKWARE representative if this is necessary for your environment.
2. Double click the certificate you wish to install.



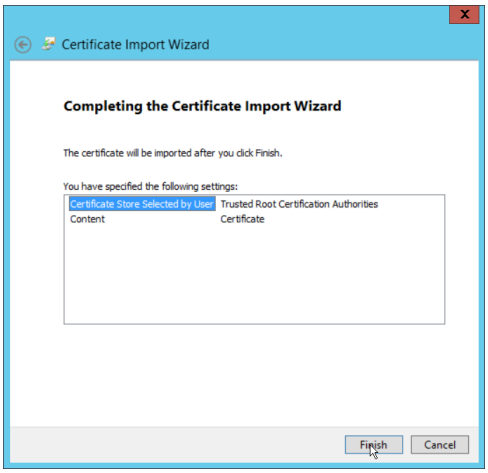
3. Click **Install Certificate….**
4. Select **Current User.**



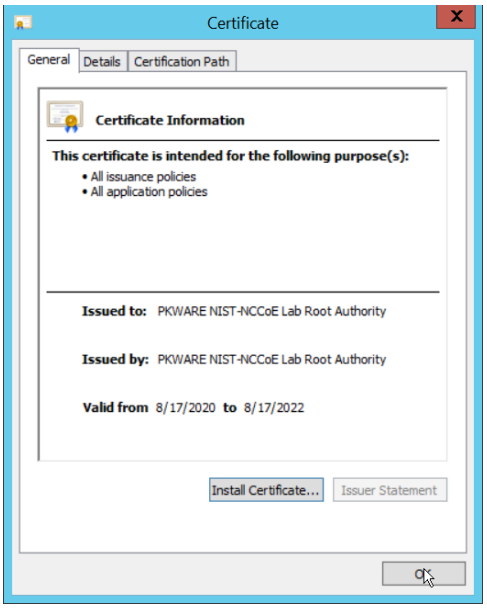
5. Click **Next.**
6. Click **Browse.**
7. Select **Trusted Root Certification Authorities.**



8. Click **Next.**



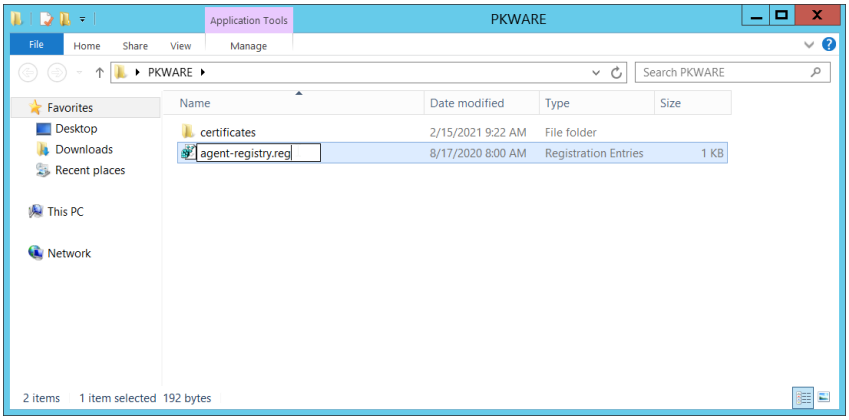
9. Click **Finish.**



413 10. Click **OK.**

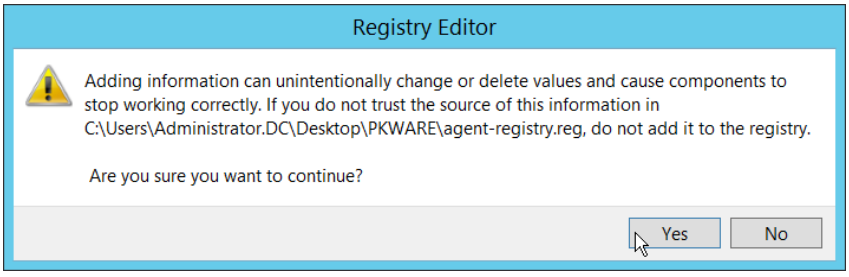
414 11. Repeat steps 1 through 10 but select **Personal** instead of **Trusted Root Certification Authorities.**

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

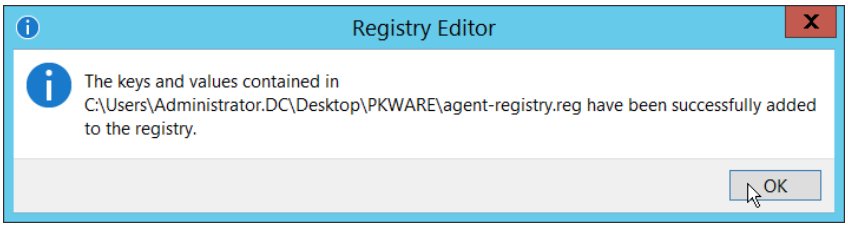


416 13. Rename agent-registry.txt to agent-registry.reg.

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



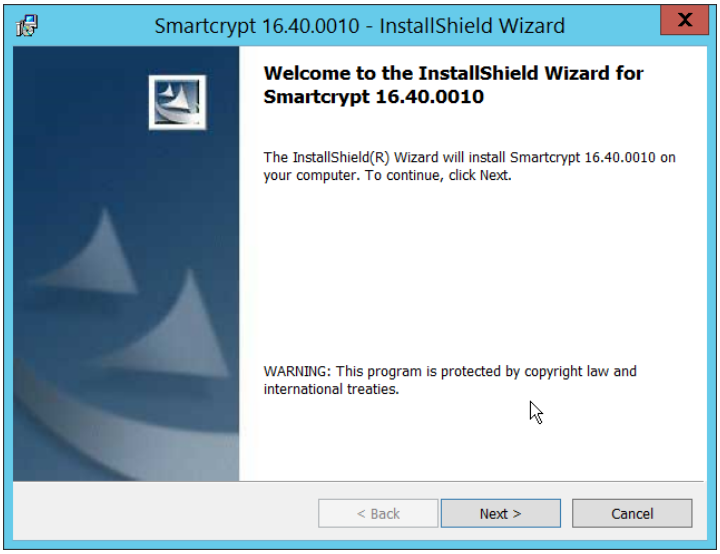
418 15. Click **Yes.**



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

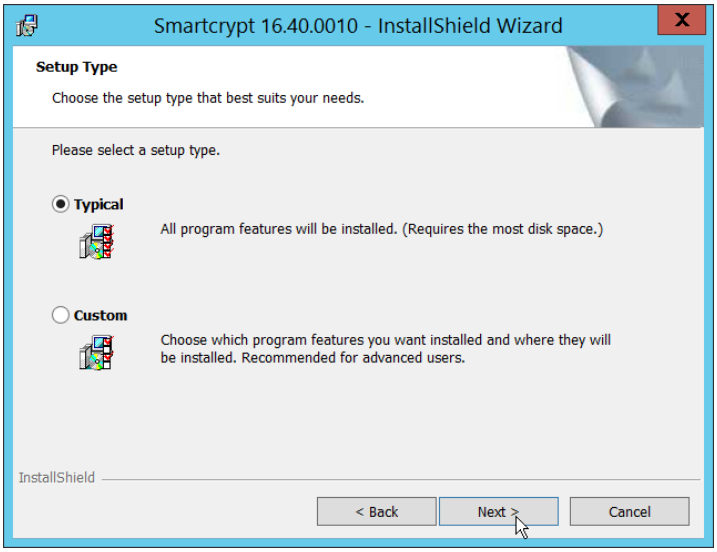
Install the PKProtect Agent

1. Run the PKProtect Installation executable.

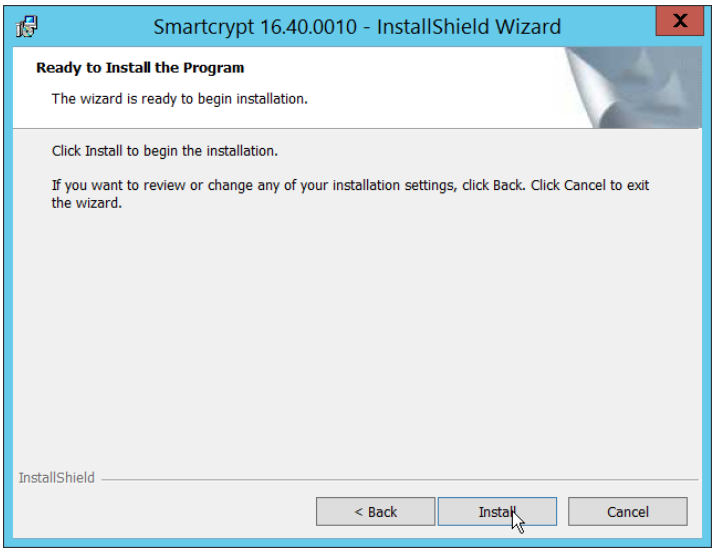


2. Click **Next.**
3. Select **I accept the terms in the license agreement.**

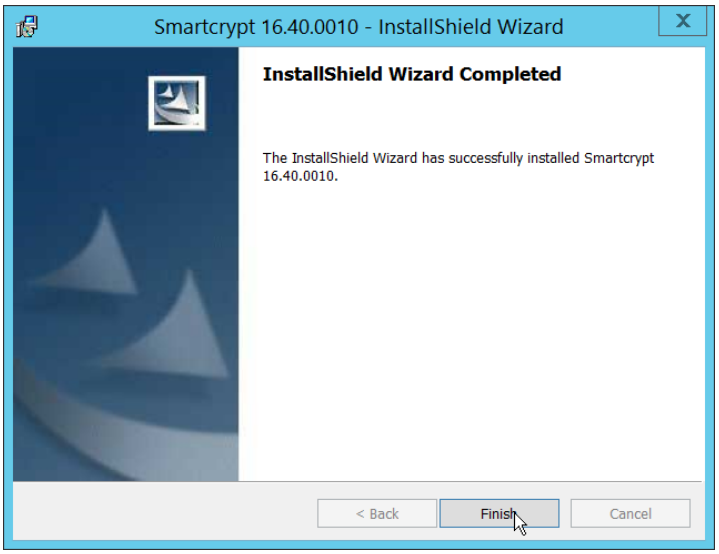
4. Click **Next.**
5. Select **Typical.**



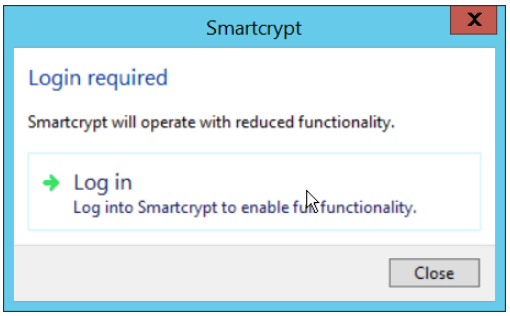
427 6. Click **Next.**



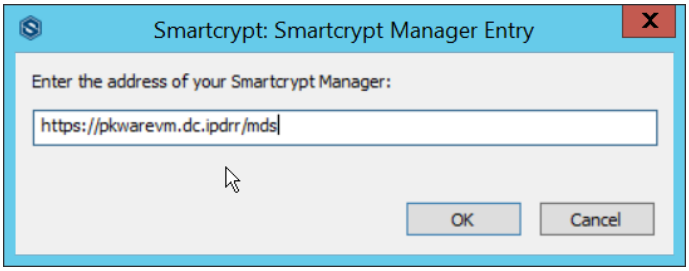
428 7. Click **Install.**



8. Click **Finish.**



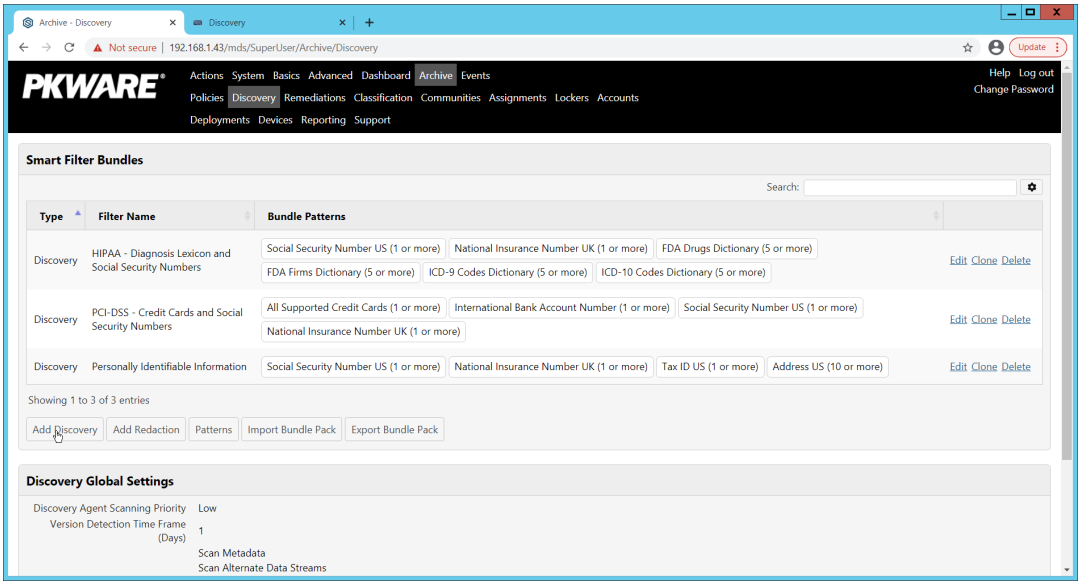
9. If a window to login is not automatically shown, you can right click the PKProtect icon in the Windows taskbar and click **Login….** If a window is automatically shown, click **Log in.**
10. Login using the username of the account in the domain, in email format (such as administrator@domain.id).



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

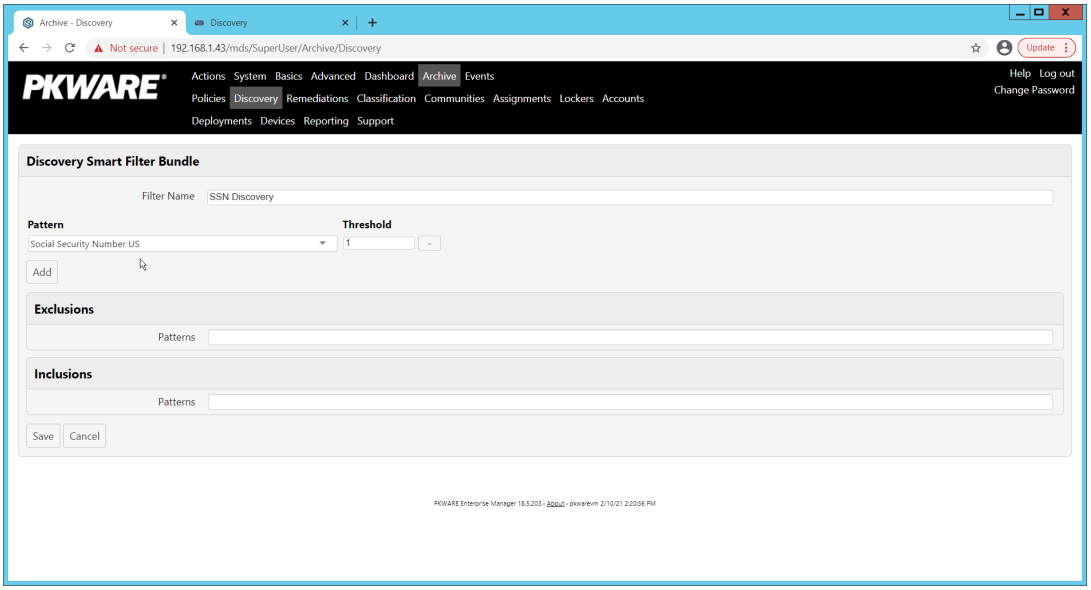
Configure Discovery and Reporting

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

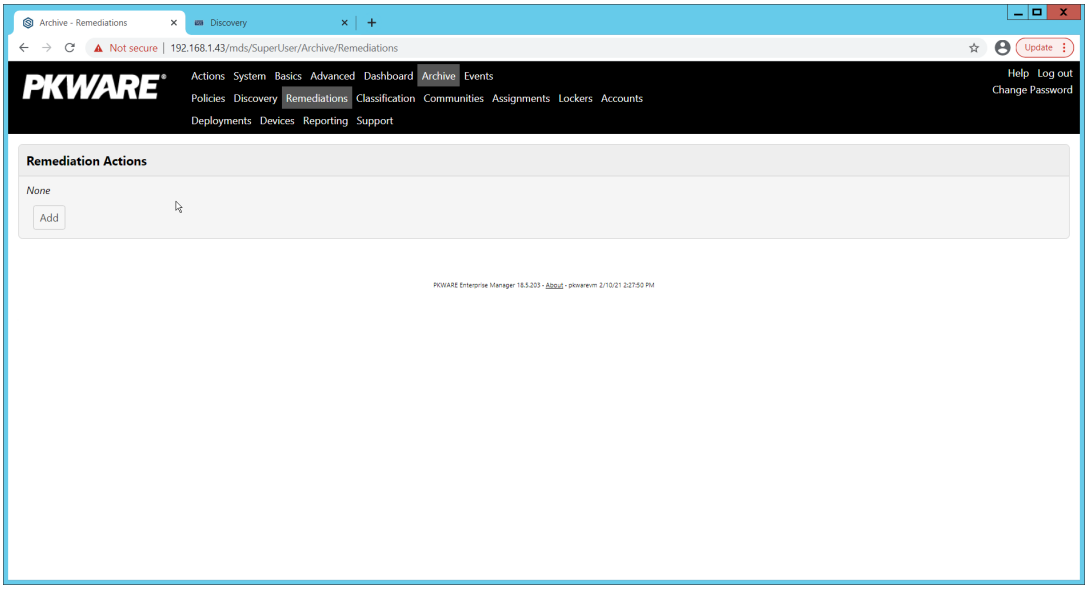


2. Click **Add Discovery.**
3. Enter a **name** for the discovery rule.

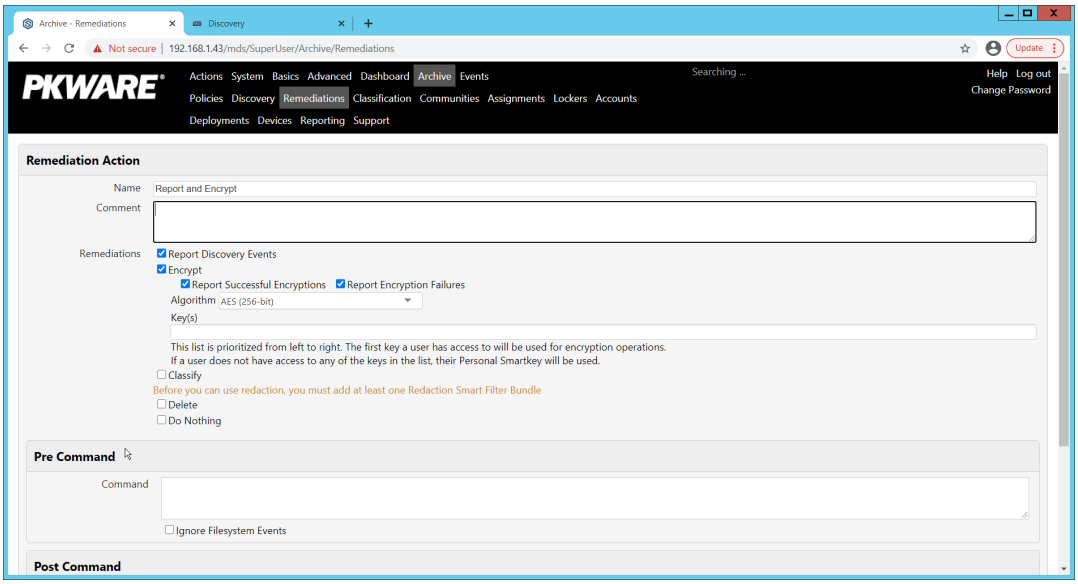
4. Select a **pattern** for the rule to discover. In this case, we are setting up a rule to detect social security numbers in files for reporting/remediation.
5. The **Threshold** field refers to how many of those patterns must be present in a document for the rule to be applied.



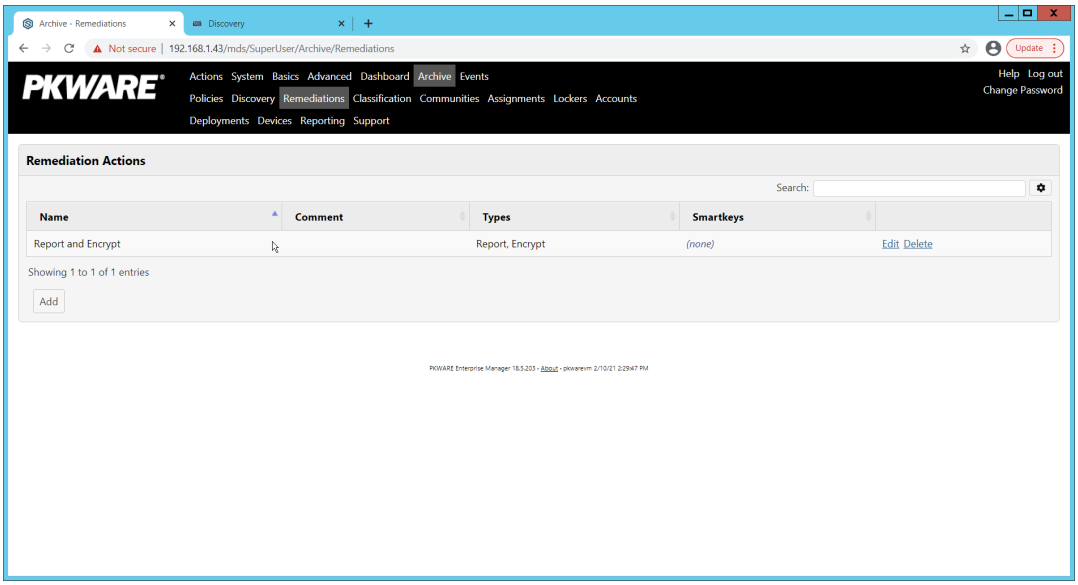
6. Click **Save.**
7. Navigate to **Archive > Remediations.**



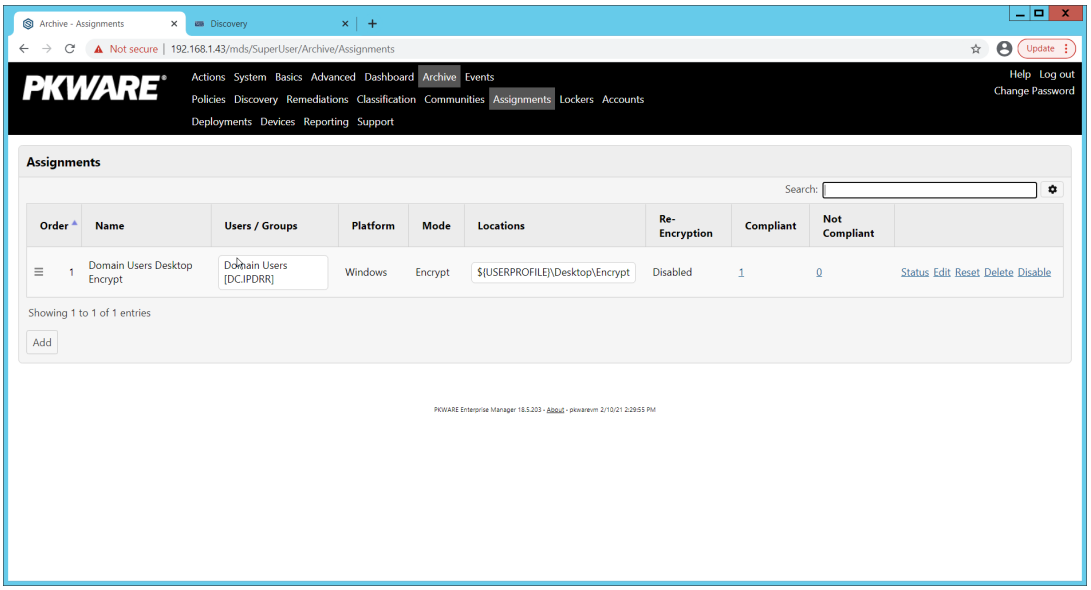
8. Click **Add.**
9. Enter a name for the remediation.



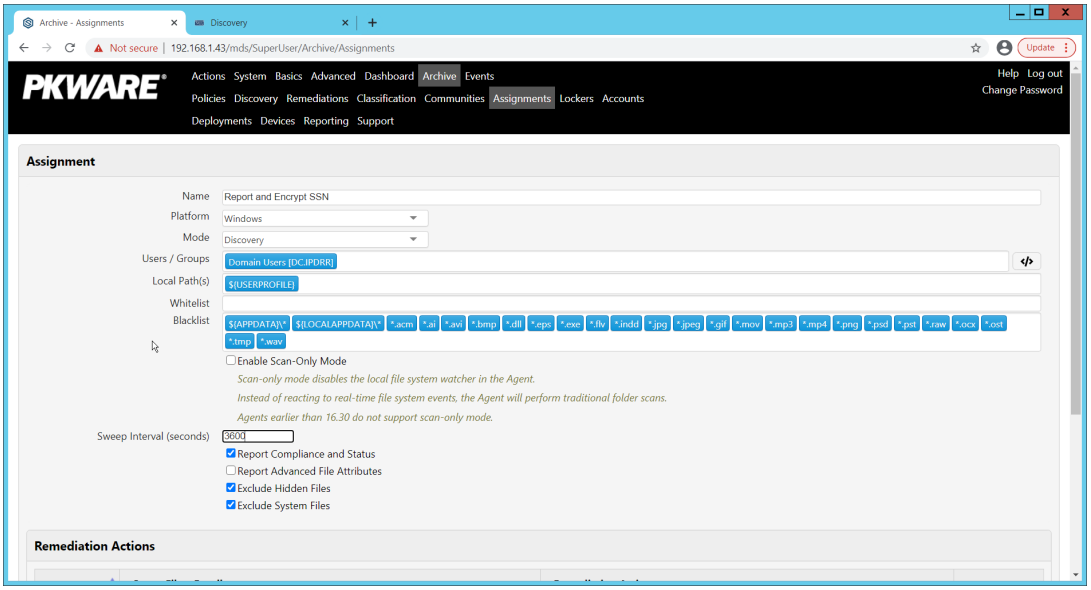
10. Check the box next to **Report Discovery Events.**
11. Check the box next to **Encrypt.**
12. Ensure that **AES (256-bit)** is selected.
13. Click **Save.**



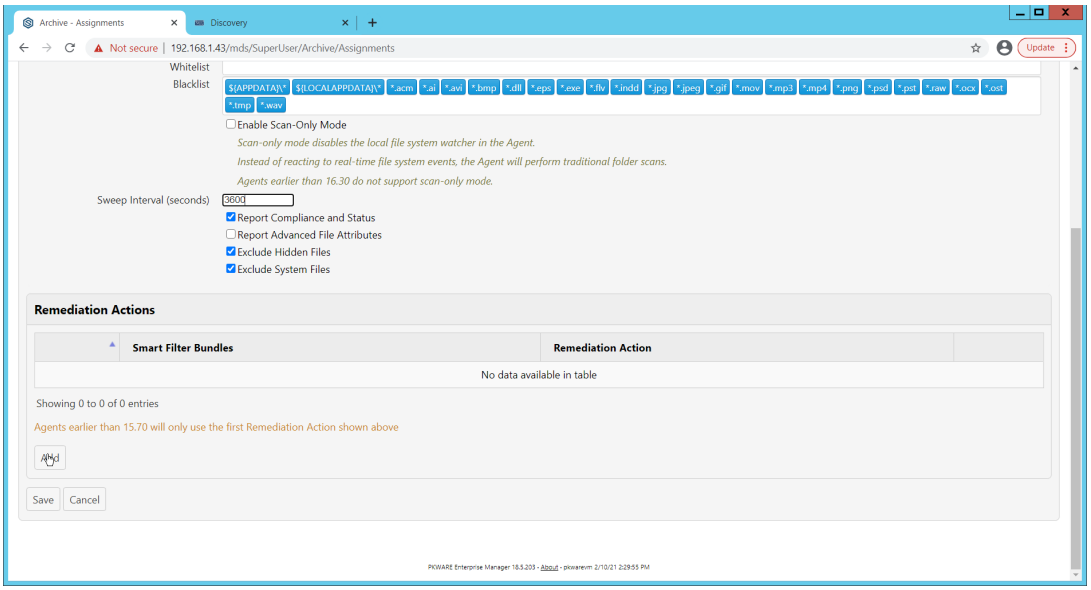
14. Navigate to **Archive > Assignments.**



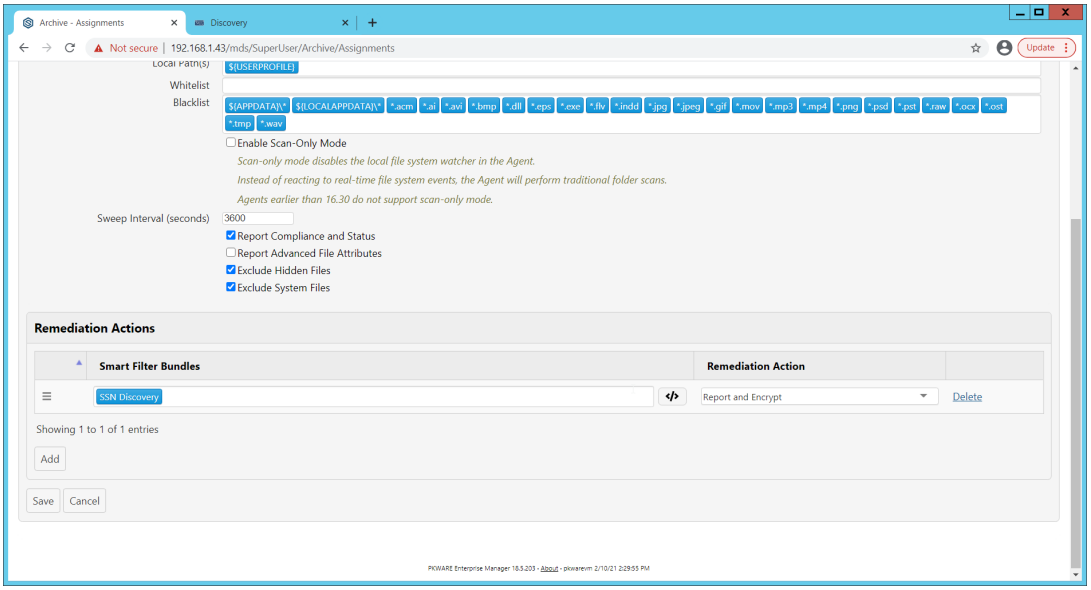
454 15. Click **Add.**



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



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



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

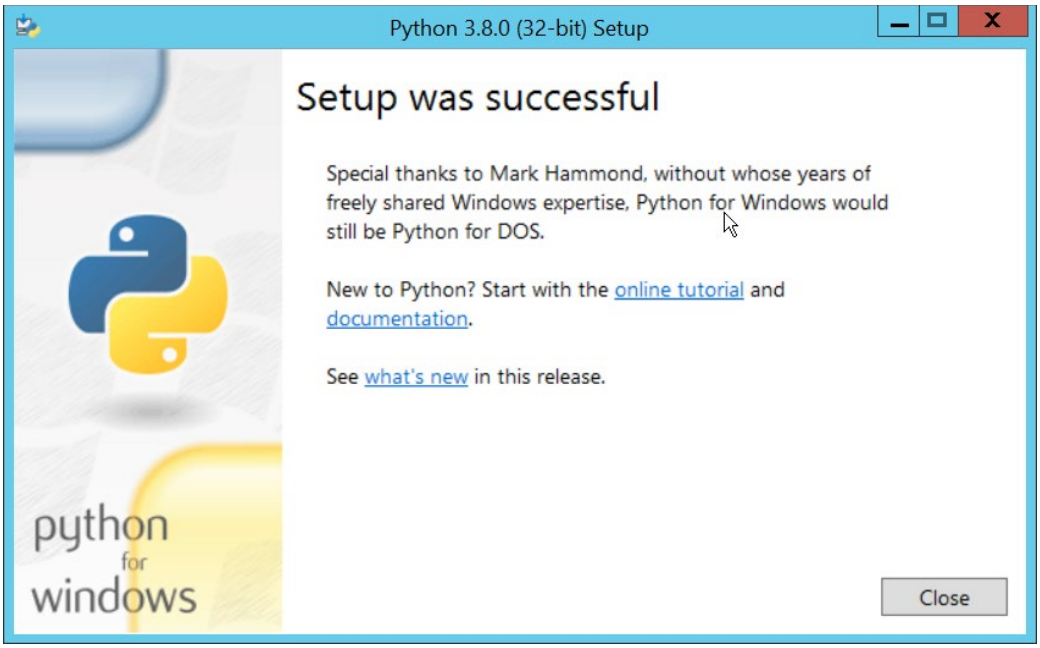
2.4 StrongKey Tellaro

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

Python Client for StrongKey – Windows Executable Creation and Use

1. Ensure that the following script (see end of section) is filled out with information specific to your enterprise, including the variables **skdid, skuser,** and **skpass.**
2. Save the file as **strongkey-client.py.**
3. This example will demonstrate how to create an executable from the script below. Download Python 3.8.0 from the Python website: https://www.python.org/downloads/release/python-380/. Specifically, download the **Windows x86 executable installer**. The 32-bit version will provide better access to Active Directory packages and interfaces.
4. Run the installer.
5. Check the box next to **Add Python 3.8 to PATH.**

6. Click **Install Now.**



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

```
> pip install pyinstaller
```

10. Run the following command to install **requests.**

```
> pip install requests
```

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

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

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

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

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

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

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

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

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

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

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

```
import requests
import json
import argparse

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

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

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


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

    req["authzinfo"] = {
        "username": "encryptdecrypt",
        #"userdn": "cn=encryptdecrypt,did="+skdid+",ou=us-
ers,ou=v2,ou=SKCE,ou=StrongAuth,ou=Applications,dc=strongauth,dc=com",
        "authgroups": "cn=EncryptionAuthor-
ized,did="+skdid+",ou=groups,ou=v2,ou=SKCE,ou=StrongAuth,ou=Applica-
tions,dc=strongauth,dc=com",
        "requiredauthorization": 0
    }

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

```

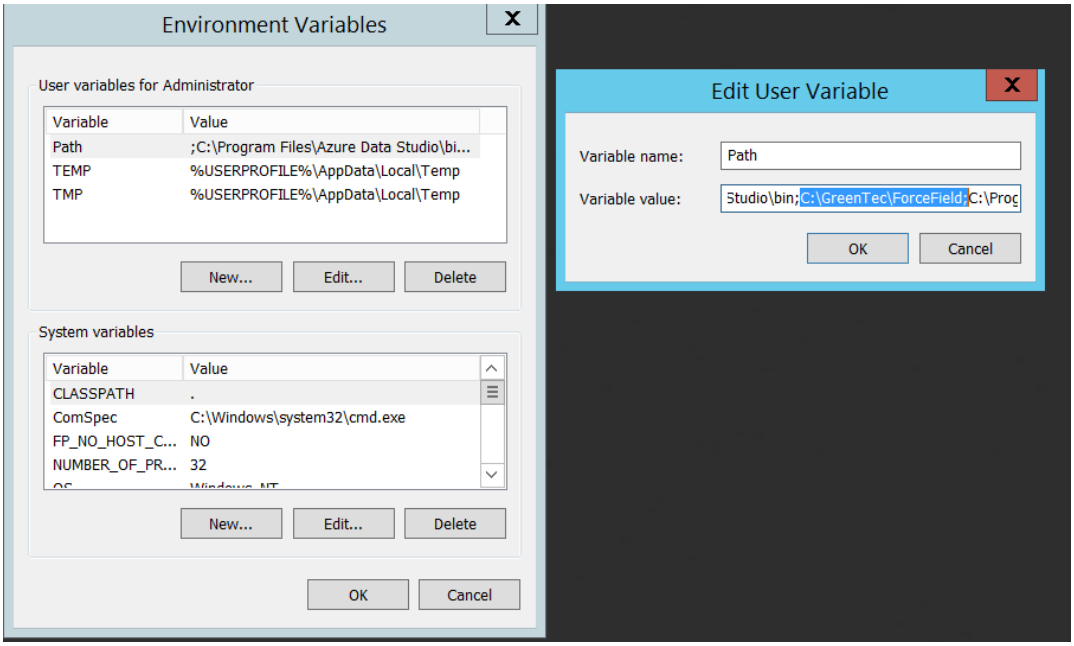
```
    return req

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

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


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

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

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

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

a = parser.parse_args()

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

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

2.5 Qcor ForceField

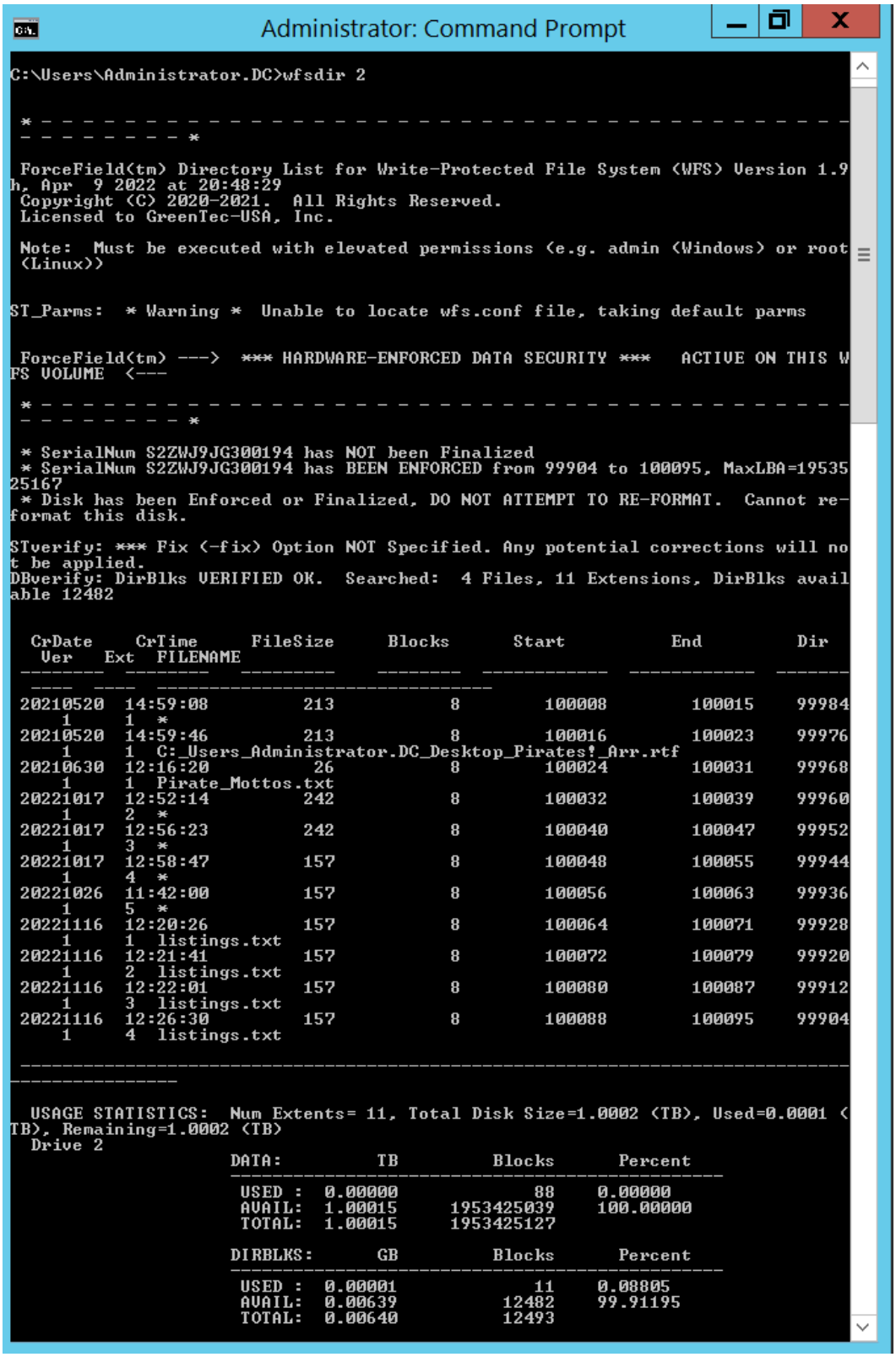
ForceField is a Write-Protected File System (WFS) combining hardware device security and encryption. In this build, ForceField is primarily used to backup data while maintaining confidentiality through encryption. In this build, we used ForceField is for the protection of a transactional database which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

Installation and Usage of ForceField

1. Either a CD or zip file will be provided by Qcor containing the WFS API and associate utilities. Copy the contents of *GreenTec**Release* onto the C: drive of the Qcor ForceField server.
2. Add the destination folder to the command line PATH variable if necessary. To do this, from the start menu search for **Environment Variables**.



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



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

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

```
> wfsdir N
```

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

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

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

options may be:
-DirX or **-x** <power of 10> (optional power of 10 for max number of files, default is 10)
1 will format for 1,243 files, 10 will allow 12,489 files, 100 allows 124,993 files, 1000 allows 1,249,930 files
-vuser <username> specifies a volume user name, DO NOT FORGET THIS USE NAME IF USED!
-vpass <password> specifies a volume password, DO NOT FORGET THIS PASSWORD IF USED!
-cache ON|OFF will turn on or off the disk drive internal cache (default is ON).
-verifywrite ON|OFF will turn write verify on or off for the WFS volume (default is OFF). The write verify status may be toggled ON or OFF using the WFScache utility. NOTE: turning write verify ON may significantly degradeI/O performance.

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

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

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

Examples of wfscopy using Windows:

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

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

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

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

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

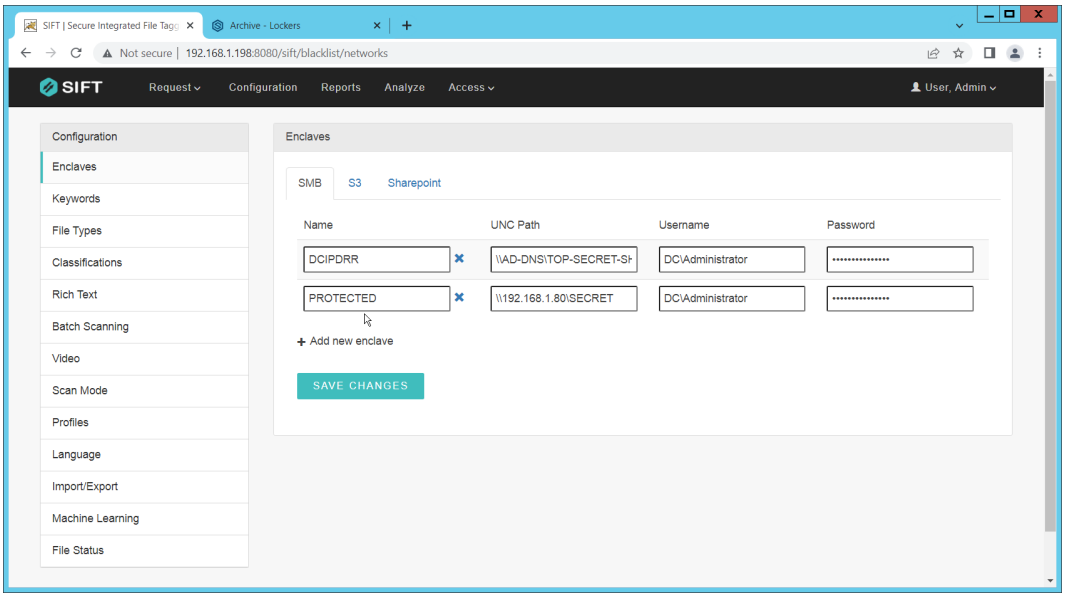
The above command will display the contents of the WFS file myfile.txt from disk 4 onto the console. This is similar to using the type command in the Windows command line.

2.6 Avrio SIFT

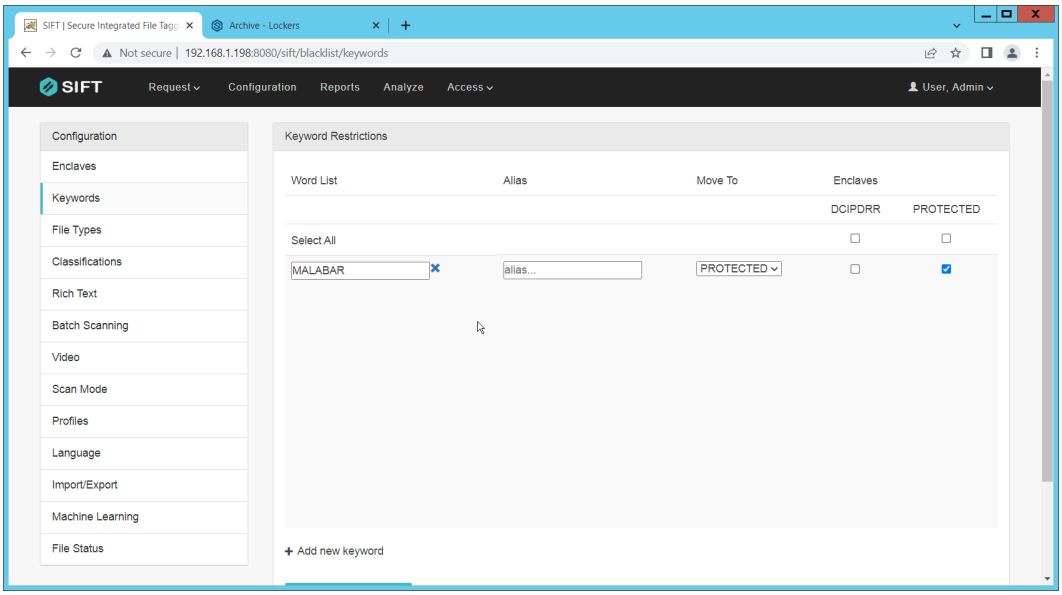
Avrio SIFT is a data inventory and management capability designed to enforce data policies. The installation of Avrio SIFT is typically done in a managed fashion by the vendor, and the deployment seen in the NCCoE lab may not resemble other deployments. In the case of a Docker deployment, configuration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

Configuring Avrio SIFT

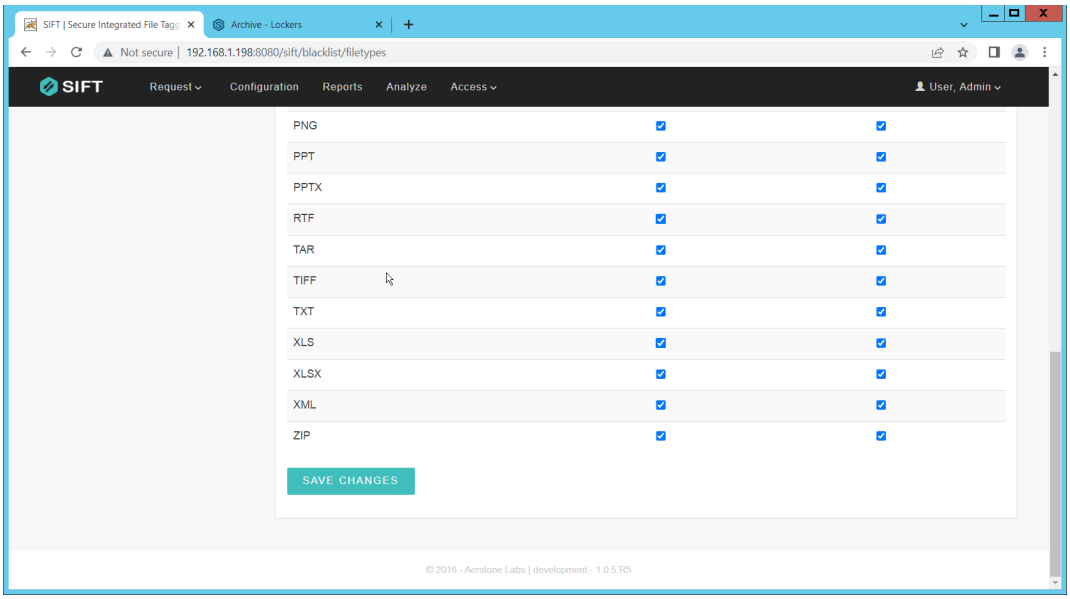
1. Navigate to the SIFT dashboard (default address: http://IP-address:8080/sift/) and login.
2. Click **Configuration**.
3. Under **Enclaves**, enter two locations. First, the path to the public Windows share, and second, the path to the one protected by PKProtect. We will use this second path later in the integration between PKProtect and SIFT. In this example, DCIPDRR is the path to the public share, and PROTECTED is the path to the one protected by PKProtect. Enter user accounts that can access each share. In production, it is recommended to create a separate user account for SIFT to use to access these shares.



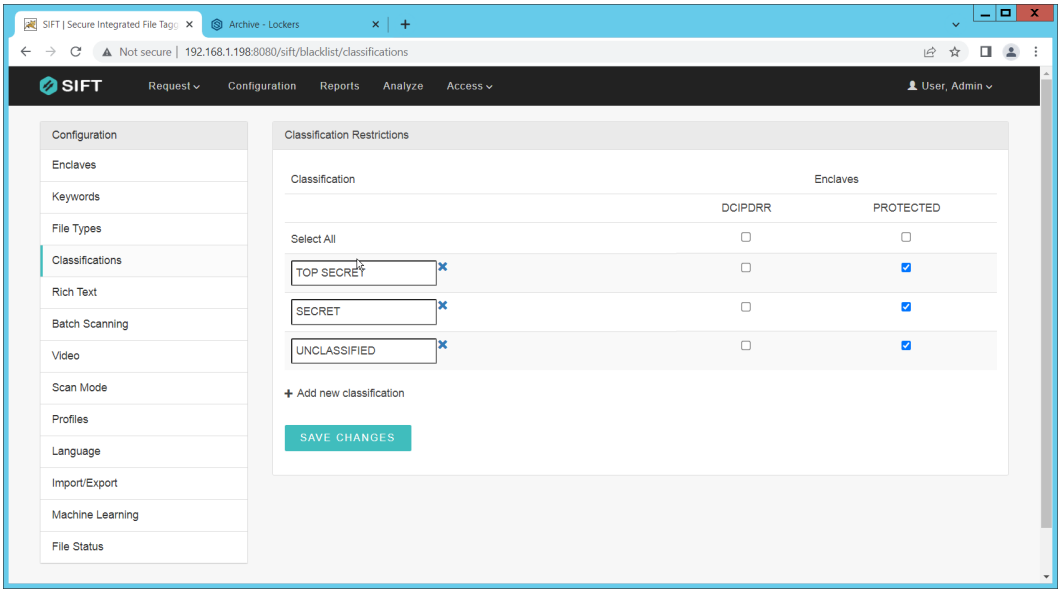
4. Click **Save Changes**.
5. Click **Keywords** on the left menu.
6. Click **Add new keyword**.
7. Enter the keyword under **Name**, and an **Alias** (if desired). Check the box next to any enclaves which are allowed to have this keyword – SIFT will be able to move files matching it to the enclaves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



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

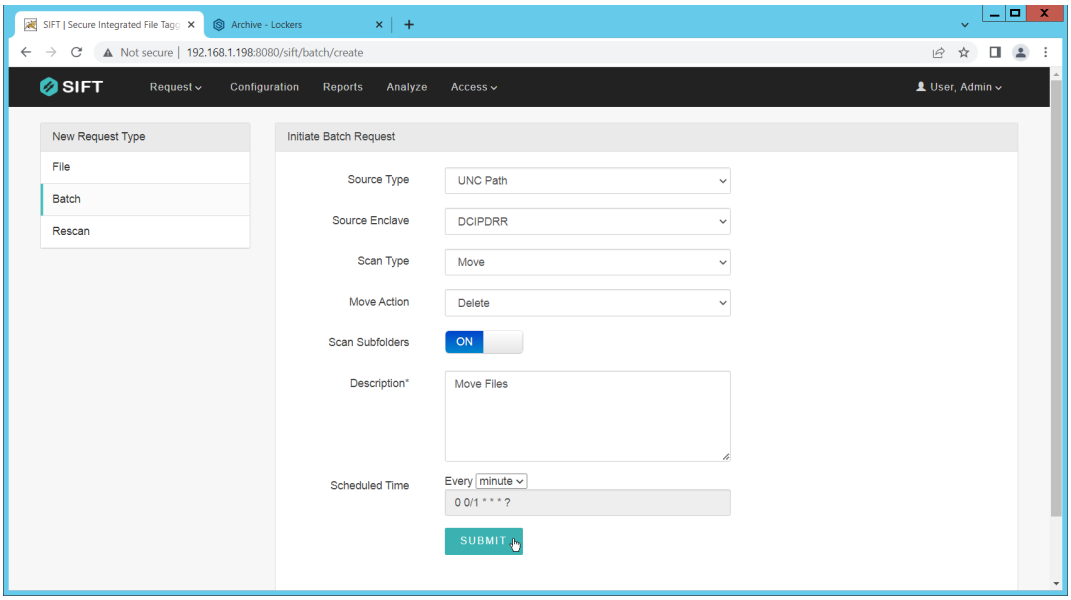


707 12. Click **Save Changes**.
708 13. Click **Classifications**.
709 14. Designate the classifications which are allowed to exist under each enclave.



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

22. Set **Scan Subfolders** to **ON**.
23. Enter a **description** for the scan.
24. Set the frequency of the scan. Note that the efficiency of the scan will likely depend on the size of the organization, and it may be more desirable to scan once an hour rather than once a minute.



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

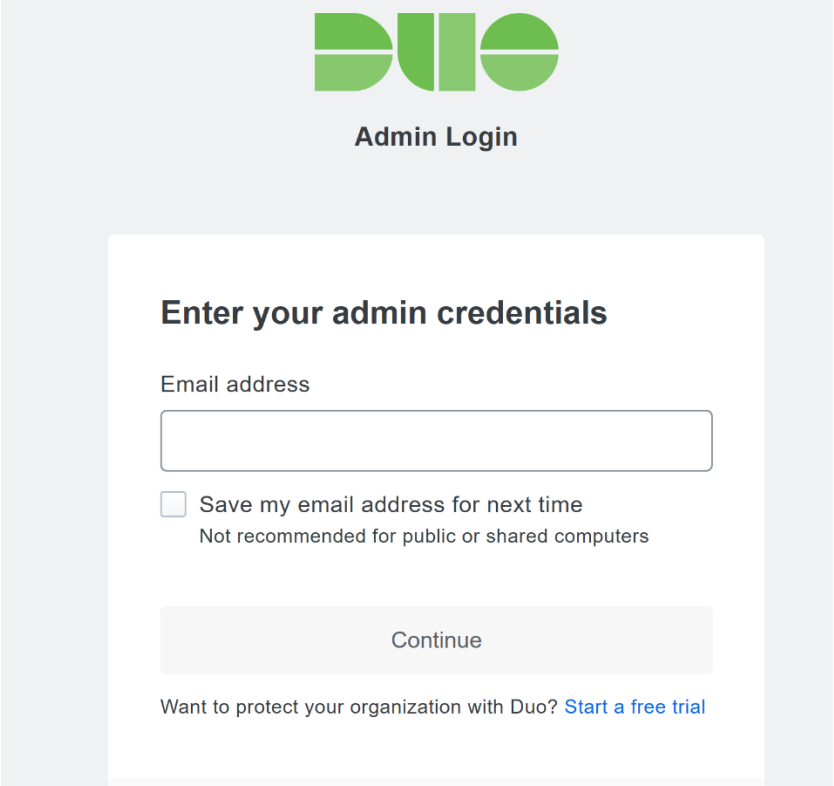
2.7 Cisco Duo

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

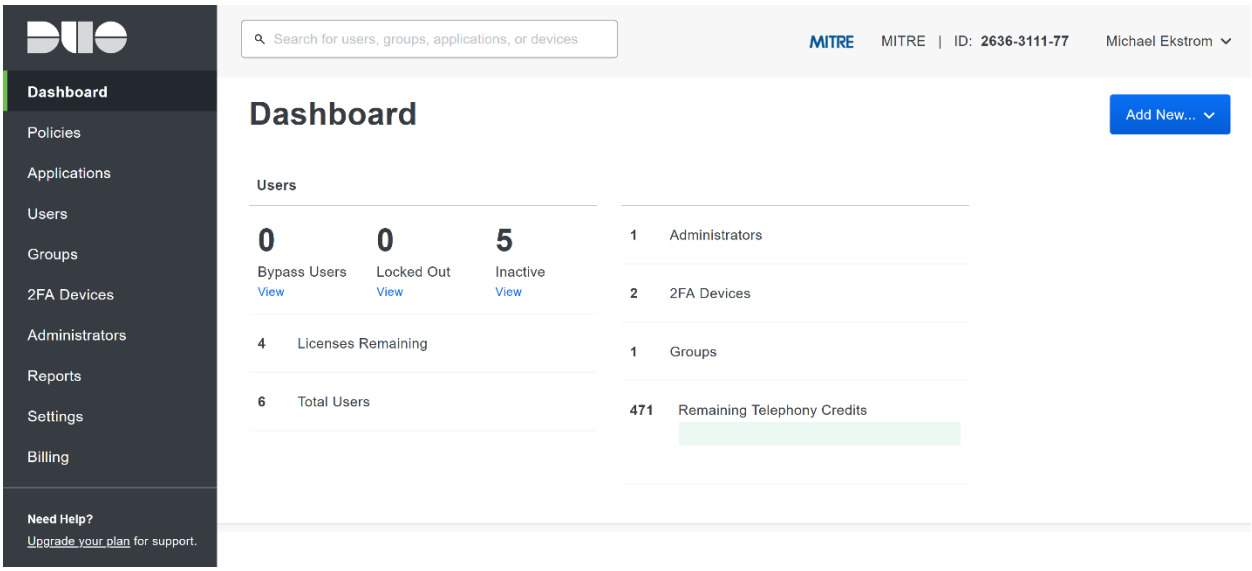
In the following section, we demonstrate the installation of Cisco Duo on an internal system in such a way that RDP and local login to that system is protected by multifactor authentication.

Installing Cisco Duo

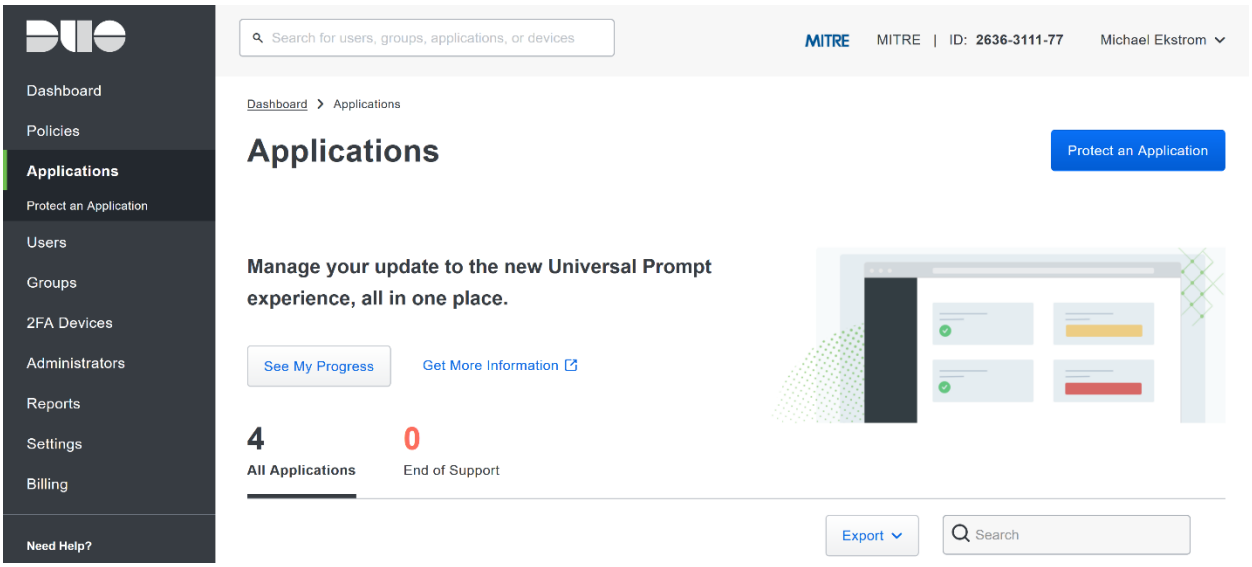
1. Begin by logging into the system you wish to protect with Duo.
2. Then connect to the internet, if not connected already, and go to the Duo Admin login page at https://admin.duosecurity.com/.



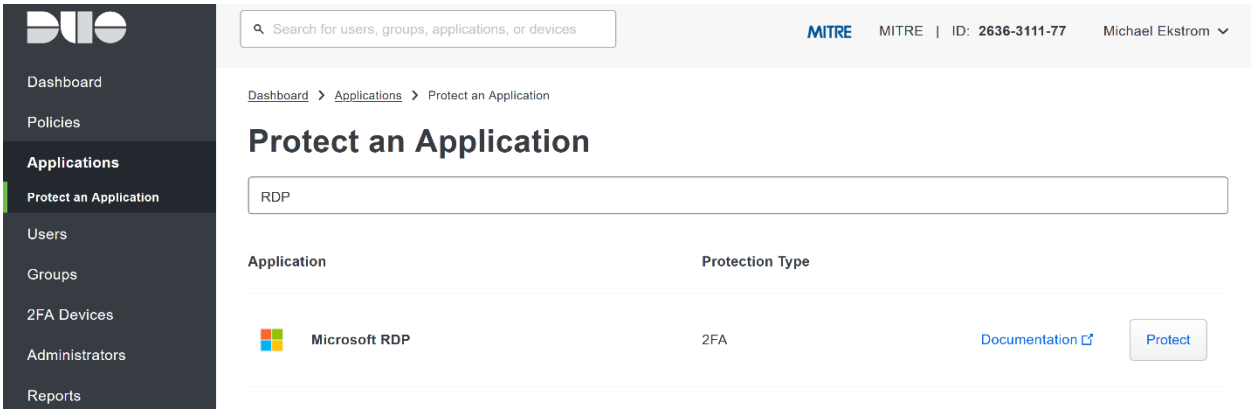
3. Login with your admin credentials and dual factor authentication until the admin dashboard is reached.



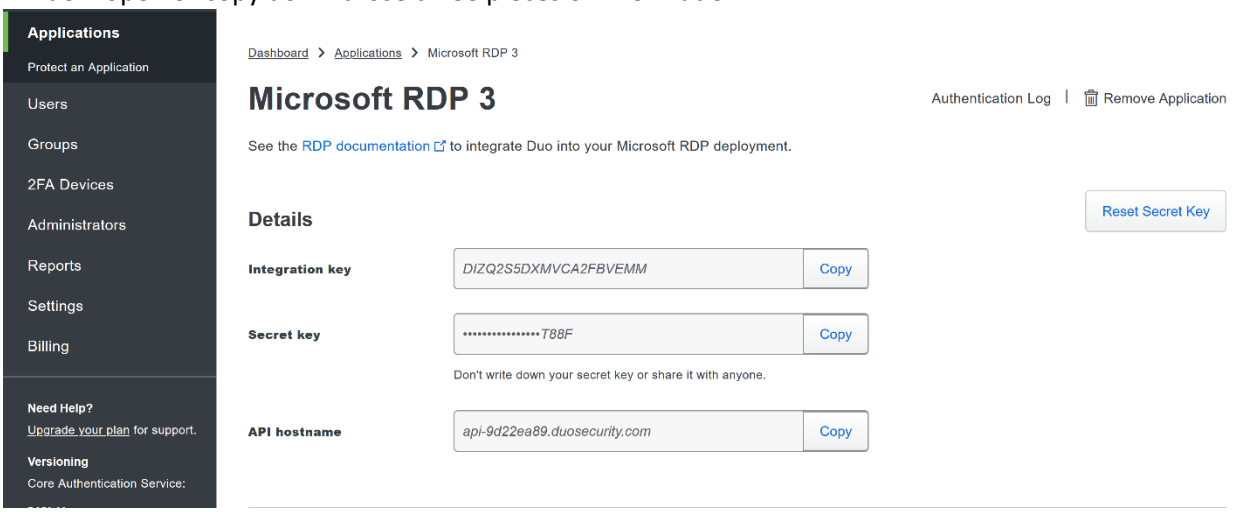
4. Click **Applications** in the sidebar.
5. Click **Protect an Application**.



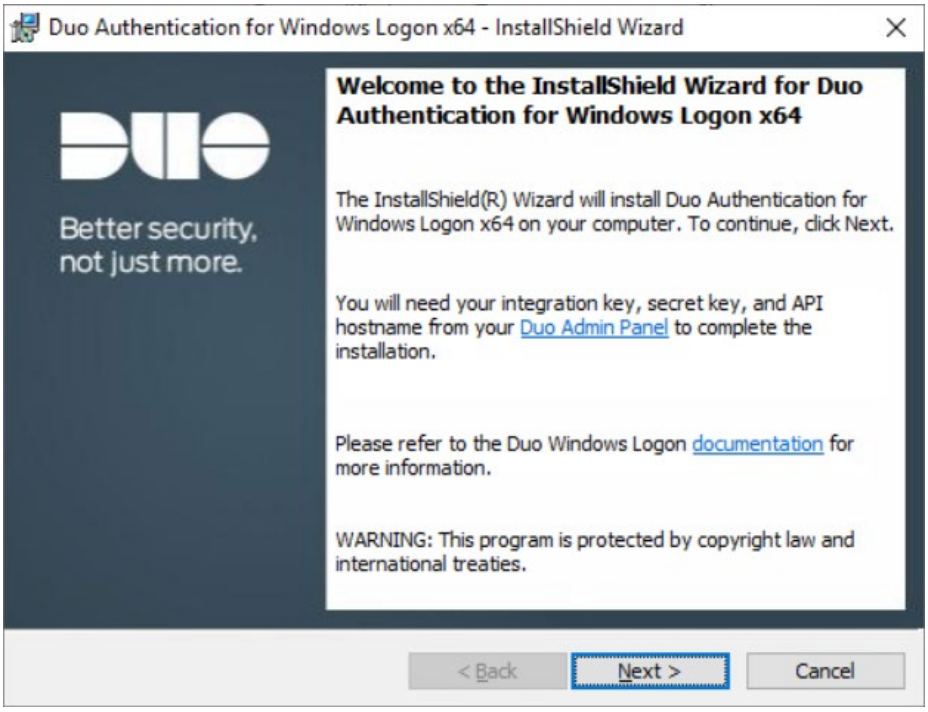
745 6. Search for, or scroll down to, **Microsoft RDP**.
746 7. Click **Protect**.



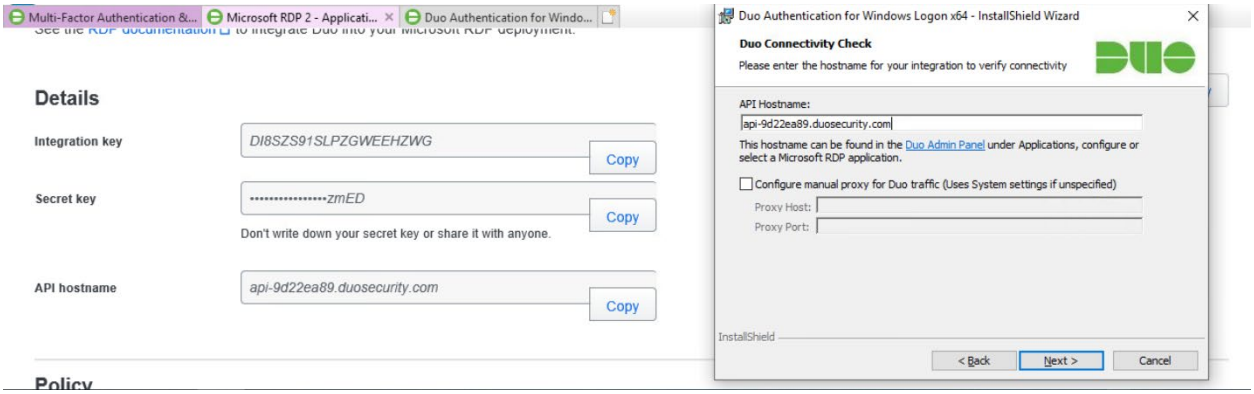
747 8. The next screen will provide policy configuration options, as well as the **Integration Key**, **Secret**
748 **Key**, and **API hostname**, which are required information for the next step. Either keep this
749 window open or copy down those three pieces of information.



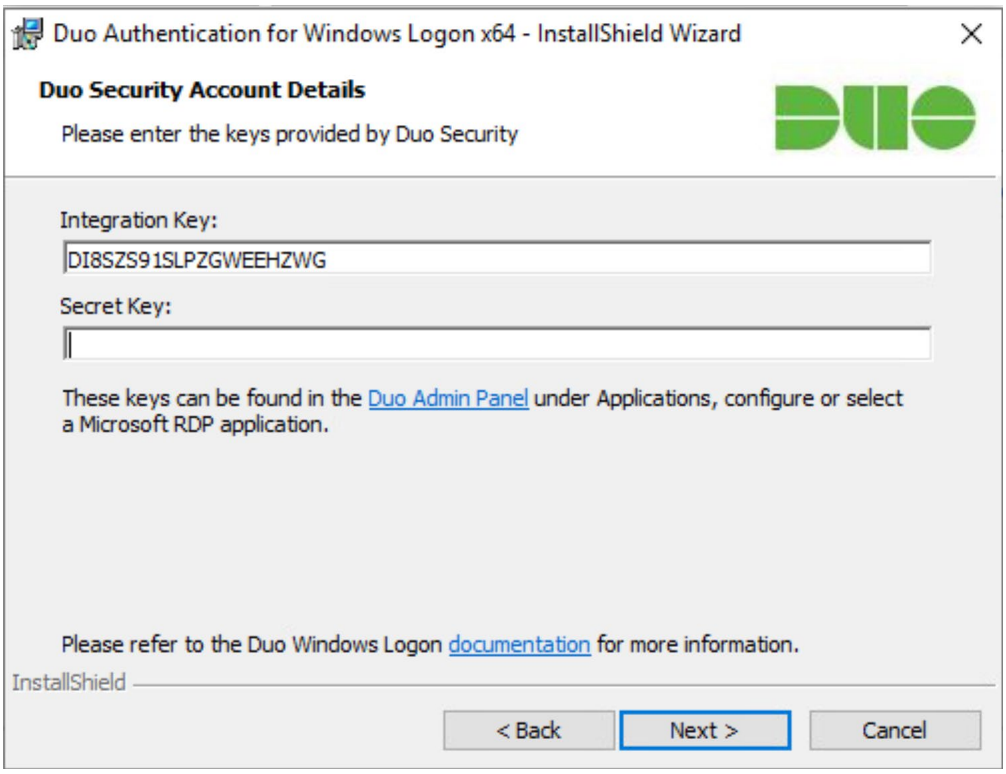
9. Download the **Duo Authentication for Windows Logon** installer package, located at https://dl.duosecurity.com/duo-win-login-latest.exe.
10. Run the downloaded EXE file.



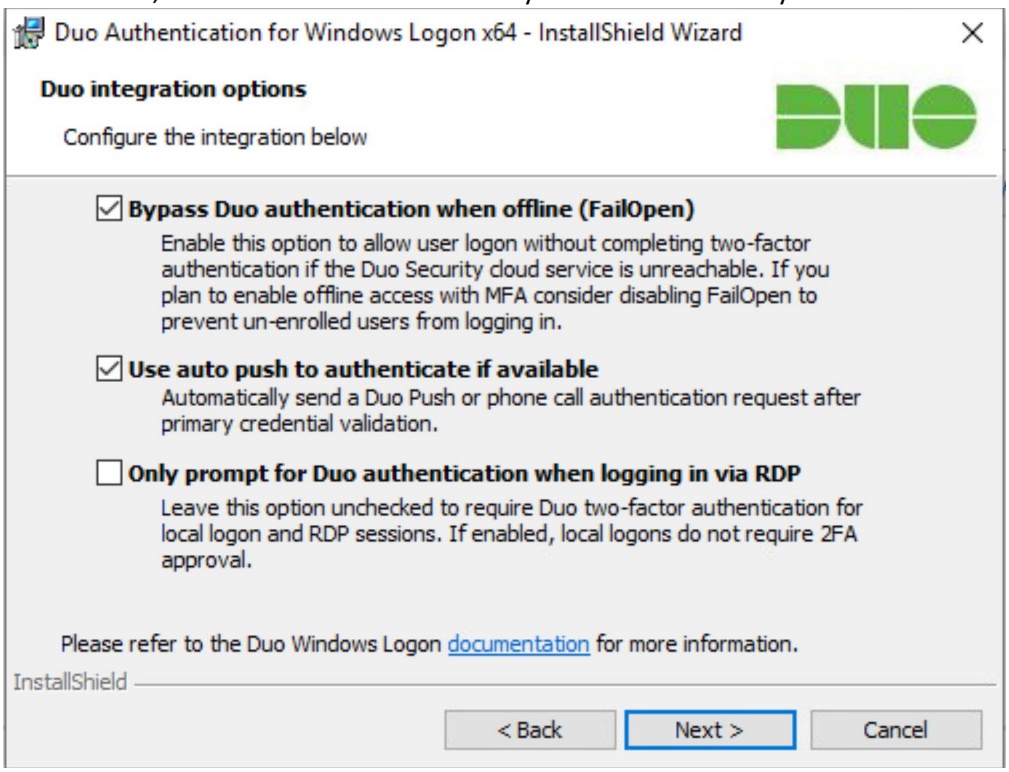
11. Click **Next**.
12. Copy the **API Hostname** into the labeled field.



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

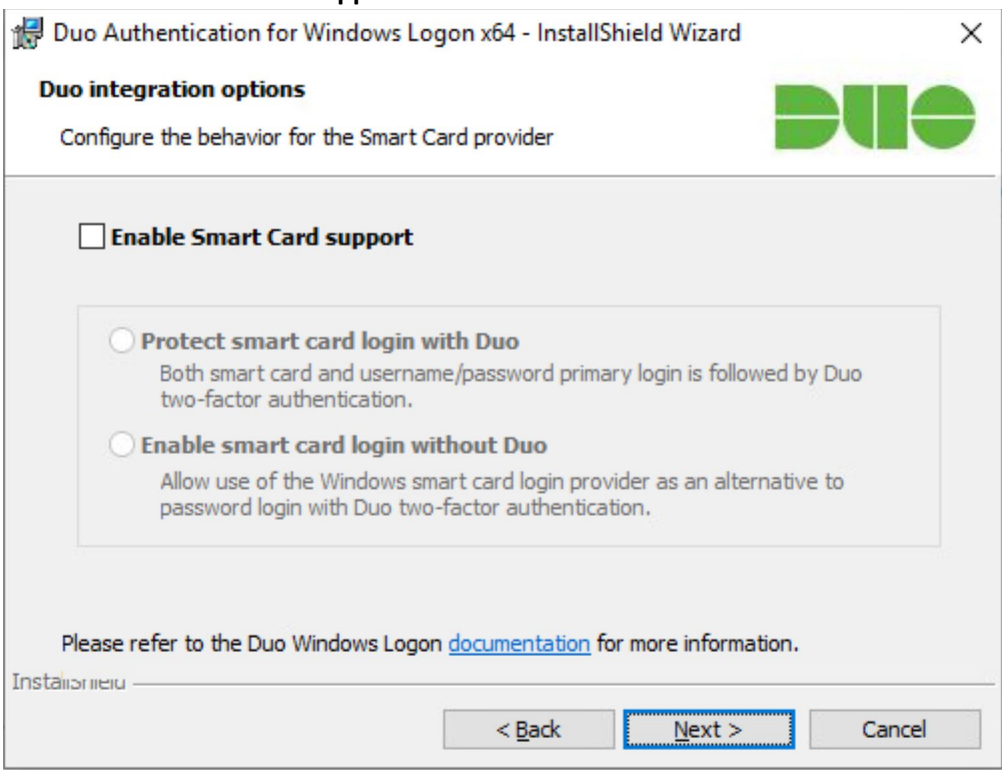


15. Click **Next**.
16. Configure Duo's integration options according to the needs of your organization. Note that **Bypass Duo authentication when offline** will allow users to skip the two-factor authentication when offline, which increases the availability of their files but may increase risk.



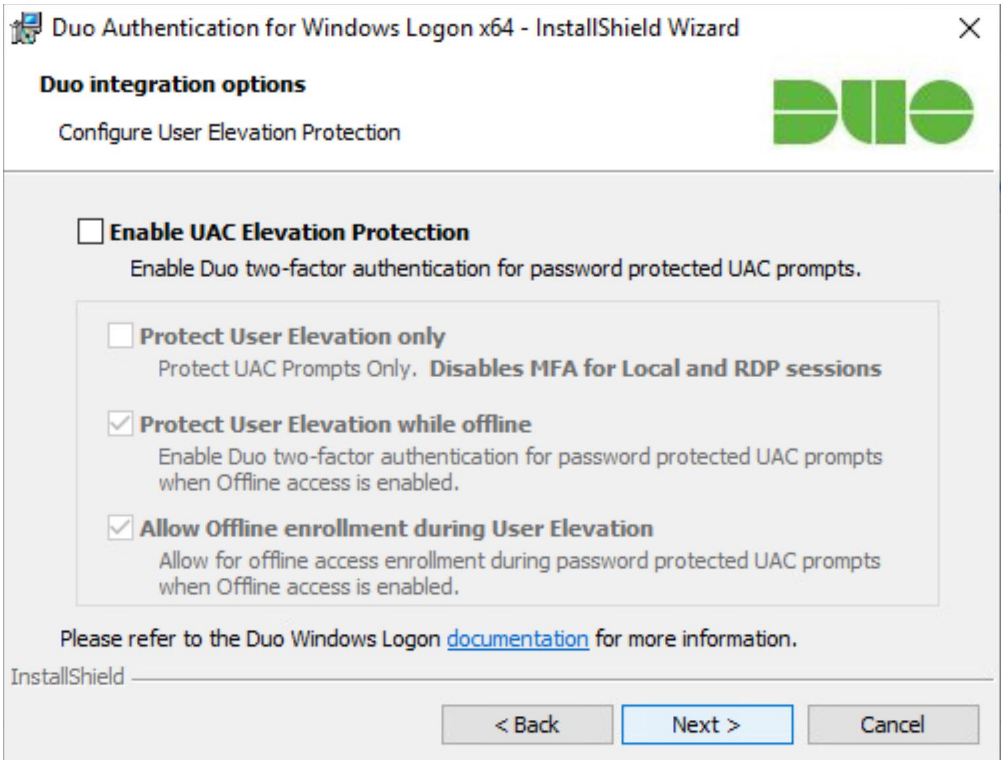
17. Click **Next**.

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

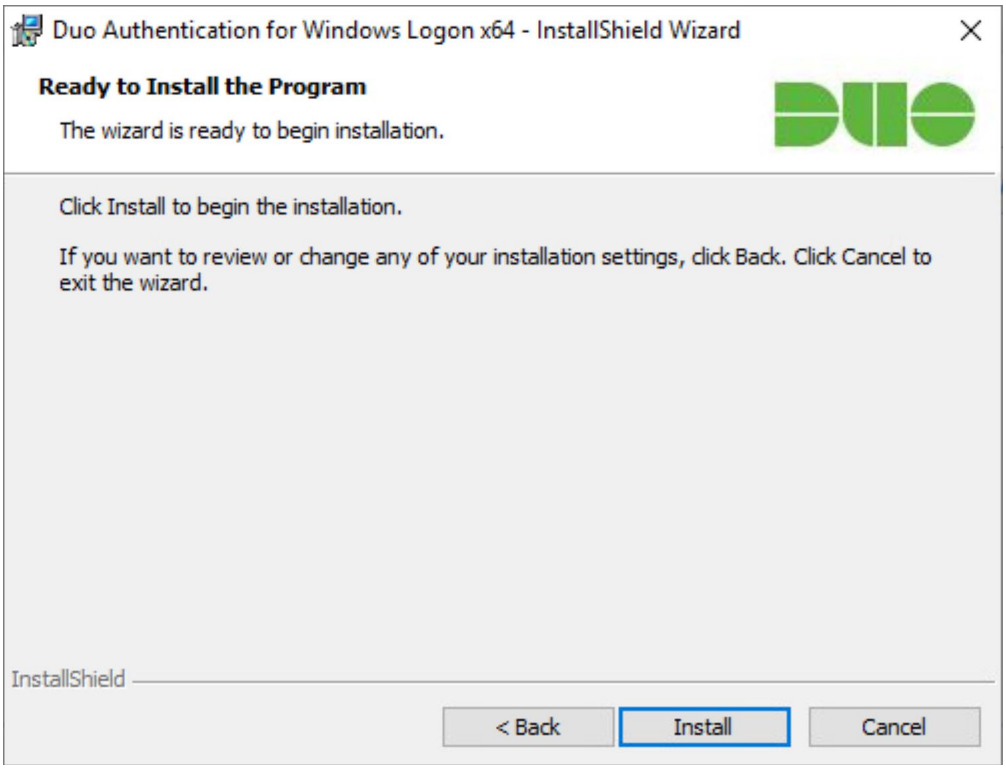


19. Click **Next**.

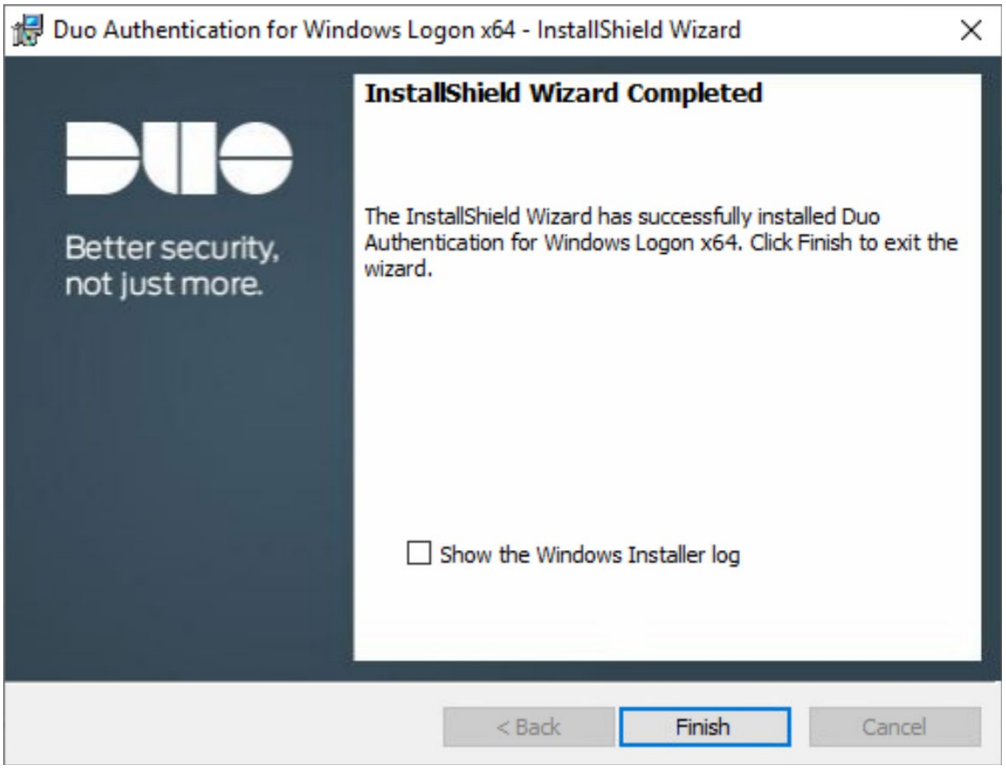
20. Leave **Enable UAC Elevation Protection** unchecked.



21. Click **Next**.



765 22. Click **Install**.

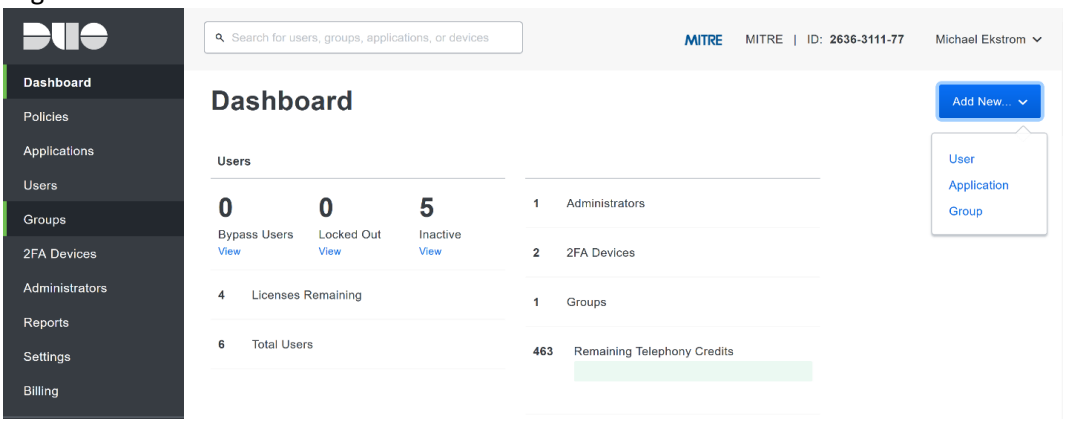


766 23. Click **Finish**.

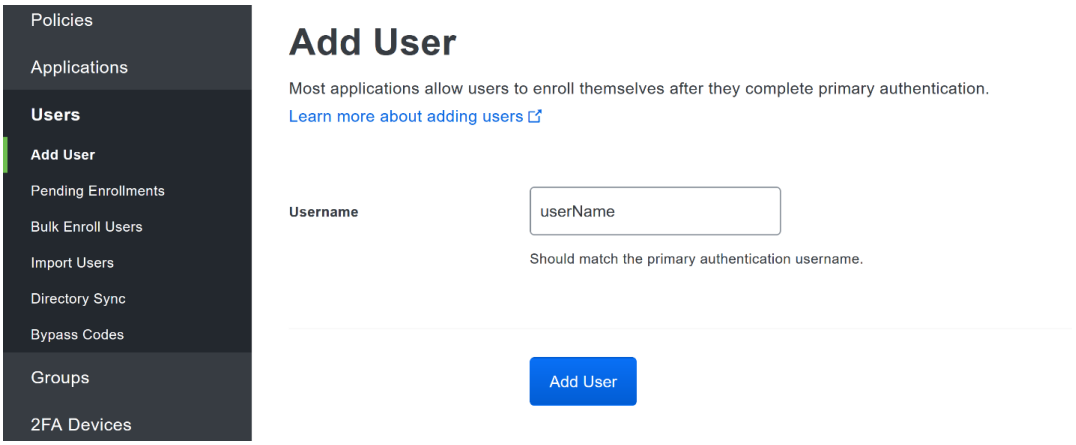
767 24. Installation should now be complete. Users registered on the Duo Dashboard with a linked
768 phone will be allowed access to the system.

Registering a Duo User

1. Login to the Duo Admin Dashboard.



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



4. Click **Add User**.
5. This will lead you to that user's information page, where additional information (full name, email, phone number) and Duo authenticators (phone numbers, 2FA hardware tokens, WebAuthn, etc.) can be associated with that username. **Note:** A user will not be able to log into a Duo protected system unless the user is registered and has an authentication device associated with their username.

2.8 Dispel

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

Installation

1. Deploy an Ubuntu machine with the provided specifications, ensuring that a provided ISO is attached to the device.
2. Login with username “dispel” and the password provided.

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

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

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

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

dispel@dispelwicket:~$
```

3. Being the installation process

```
> install image
```

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

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

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

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

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


Install the image on? [sda]:

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

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

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

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

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

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

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

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

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

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


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

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

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

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

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

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

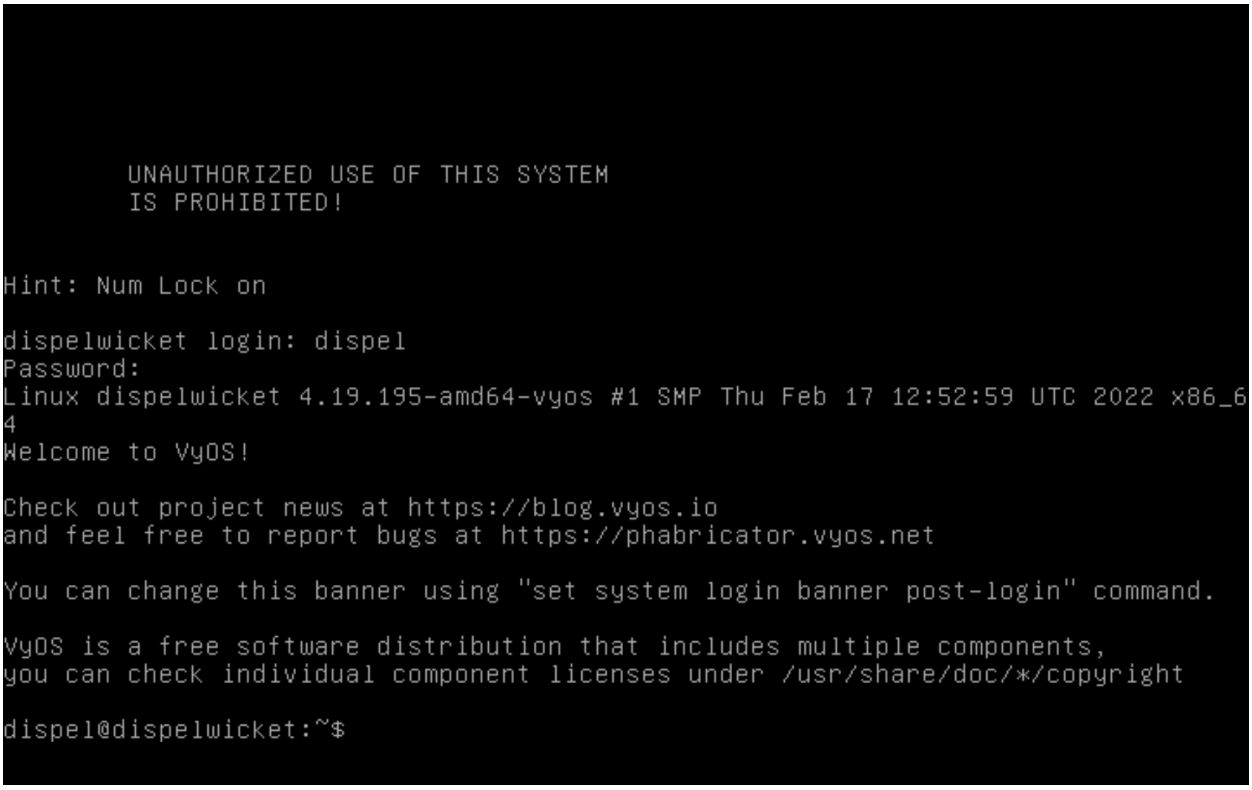
```
        UNAUTHORIZED USE OF THIS SYSTEM
        IS PROHIBITED!


Hint: Num Lock on

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

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

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

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

dispel@dispelwicket:~$ _
```

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

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

Configuring IP Addresses

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



2. Type in the command > `configure`.

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

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

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

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

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

5. Type in the command > `commit`.

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

6. Type in the command > `save`.

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

7. Type in the command > `exit`.

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

Configuring Network

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

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

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

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

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

3. Type in the command > `commit`.

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

4. Type in the command > `save`.

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

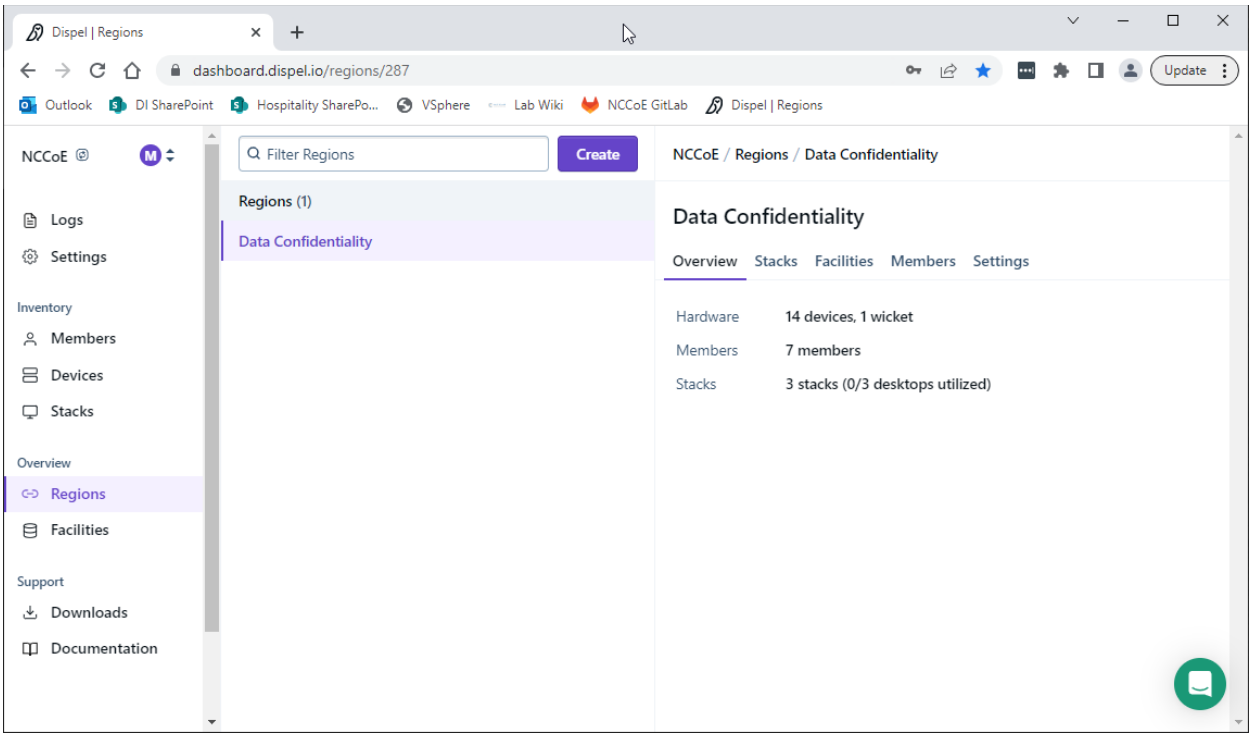
5. Type in the command > `exit`.

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

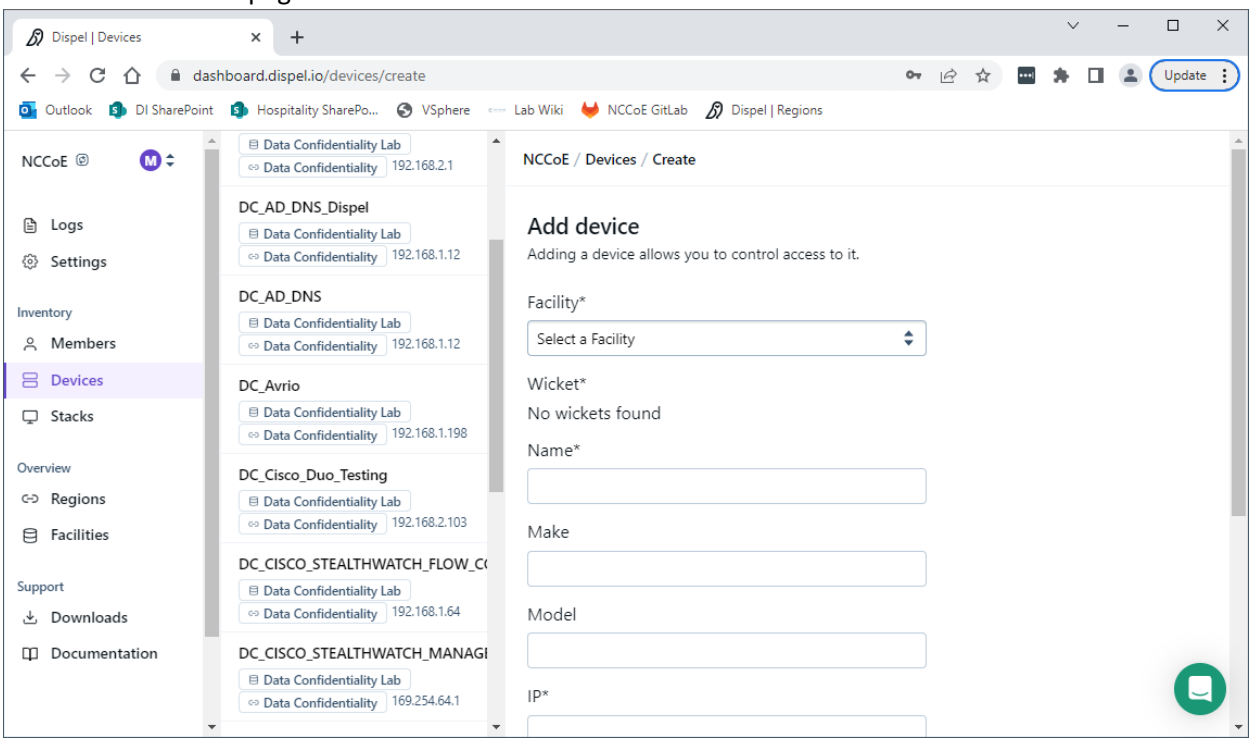
6. On the designated router or firewall, ensure UDP is allowed from the Dispel device on the provided port. For the NCCoE deployment, port 1194 was utilized. A target destination for the traffic will be provided by Dispel.
7. Modify the IP addresses of the south-side network interface to properly align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

Adding a Device

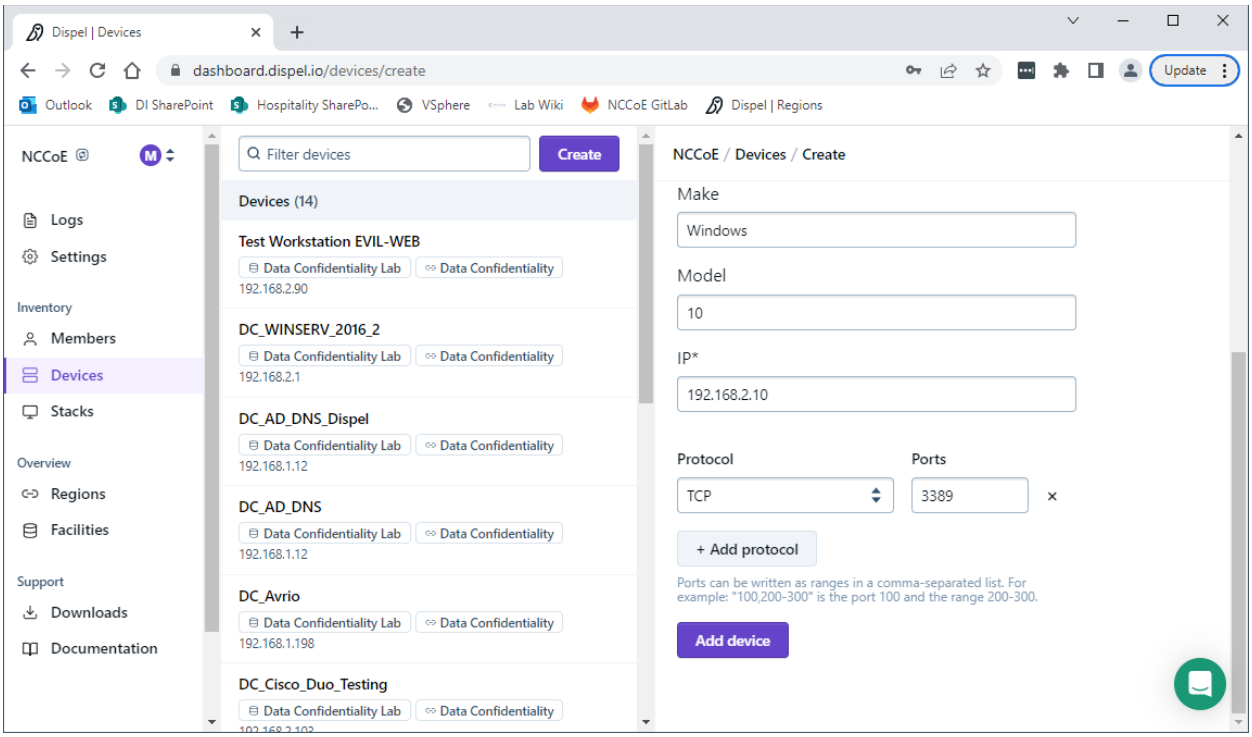
1. On the workstation in question, ensure that ping and RDP are accessible, including allowing such connections through a local firewall.
2. Authenticate to the Dispel webpage with the provided credentials.



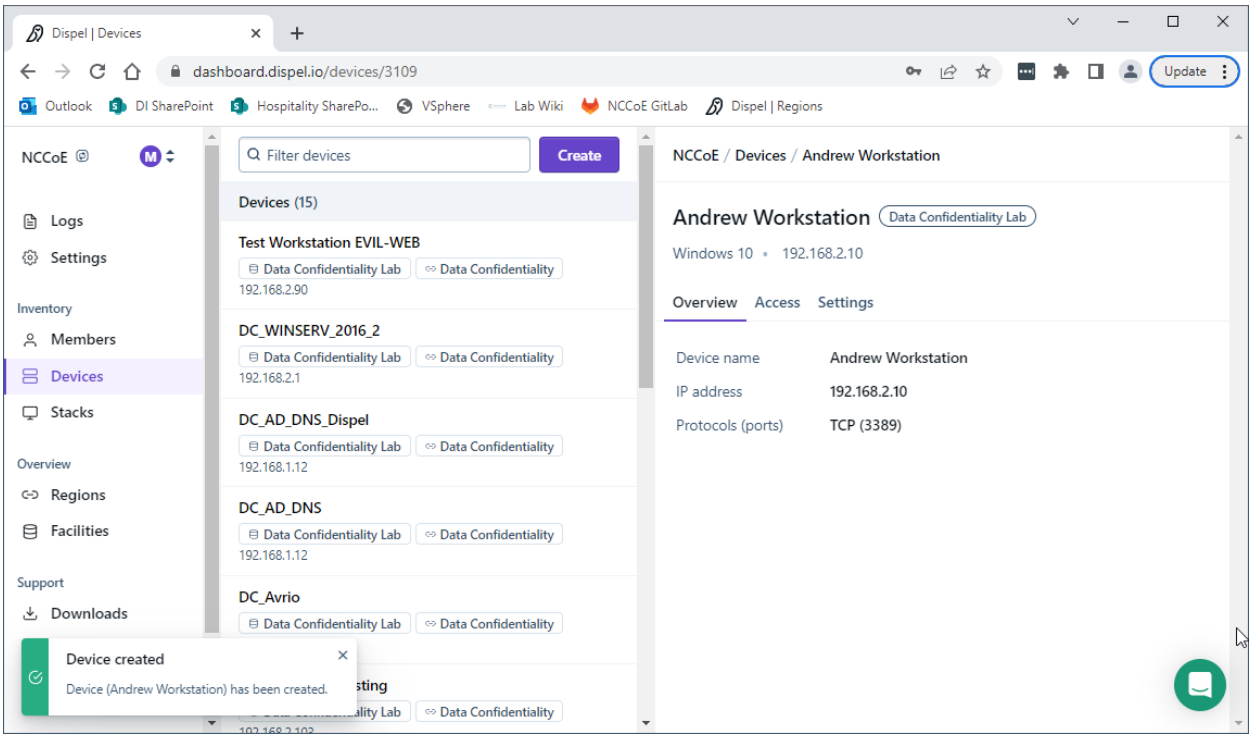
3. Click on the **Devices** page on the sidebar and click **Create**.



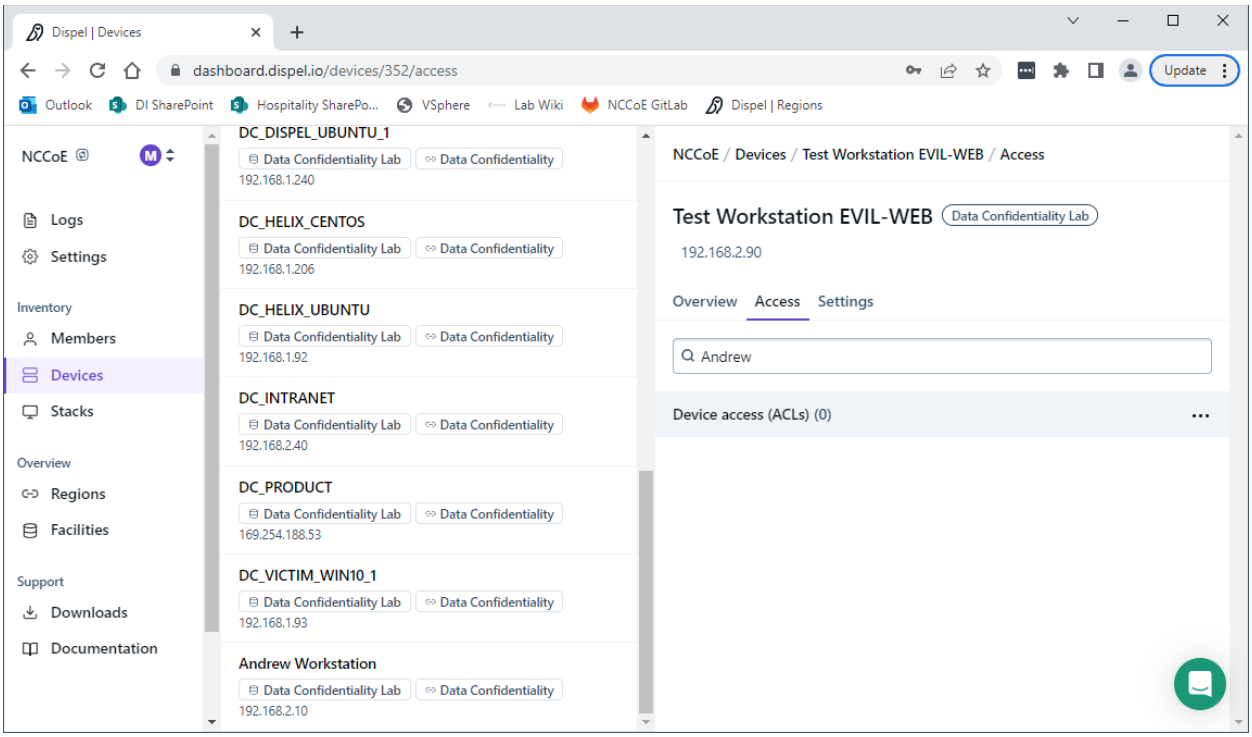
4. Under the **Add Device** window, fill out all fields, including **Facility**, **Wicket**, **Name**, **Make**, **Model**, **IP**, and **Protocol**.



833 5. Click **Add Device**.



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



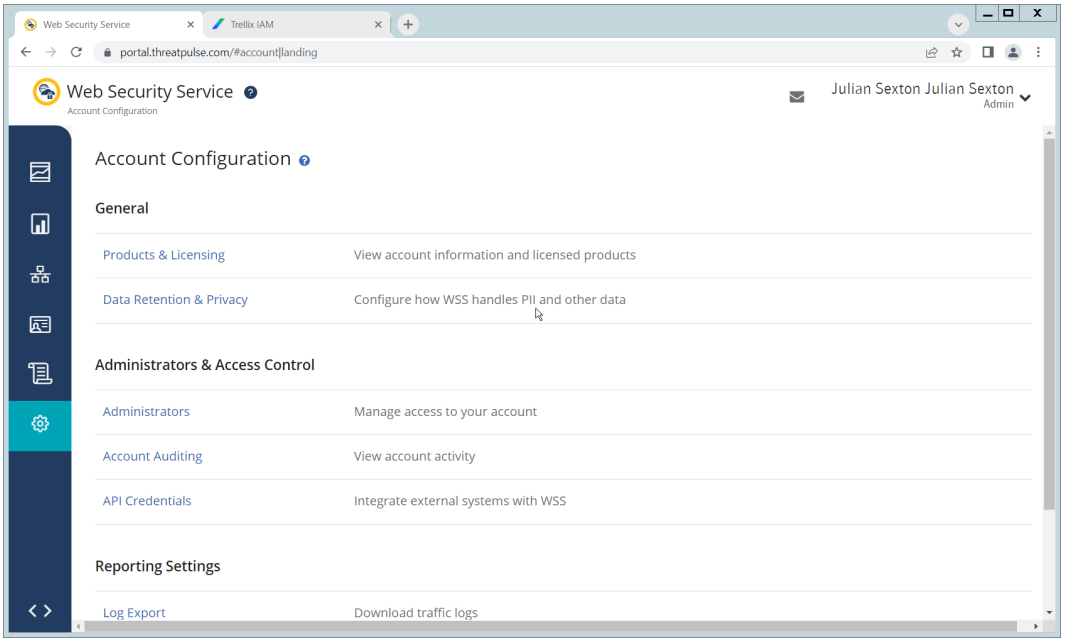
7. If a user is not already a member of the region, click **Members** in the sidebar and click **Invite.** Fill out relevant information for this individual and click **Invite this Member.**

2.9 Integration: FireEye Helix and Symantec SWG

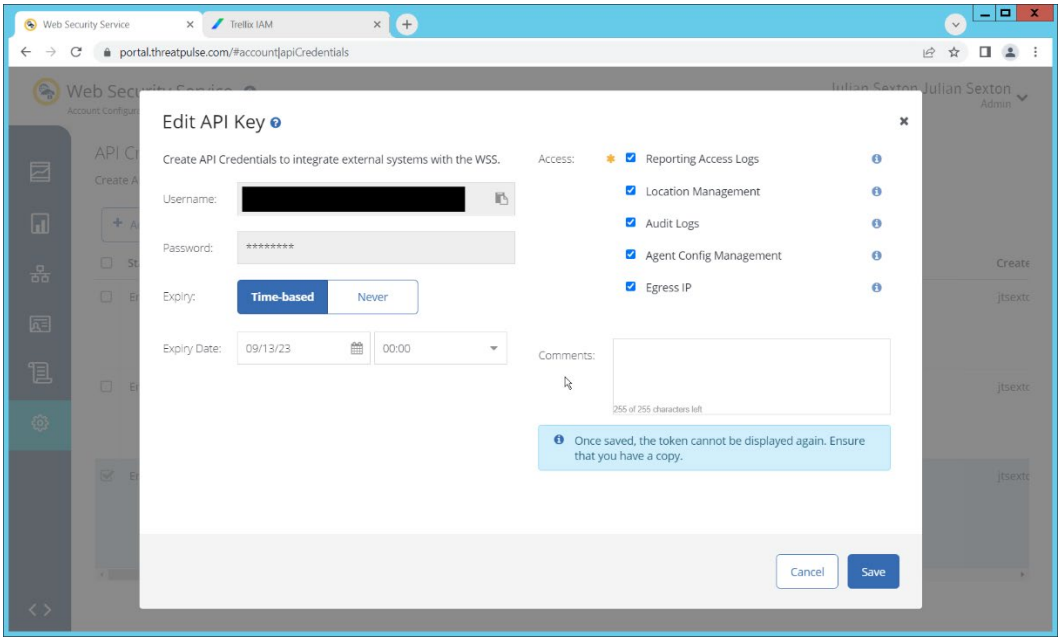
In this integration the output of the web isolation tool, Symantec SWG, will be forwarded to our SIEM, FireEye Helix. In this guide, we will aim to forward most logs to our SIEM, which can collect, analyze, and report on these logs to better maintain awareness of our systems and provide a single interface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

Configure Fireye Helix to Collect Logs from Symantec SWG

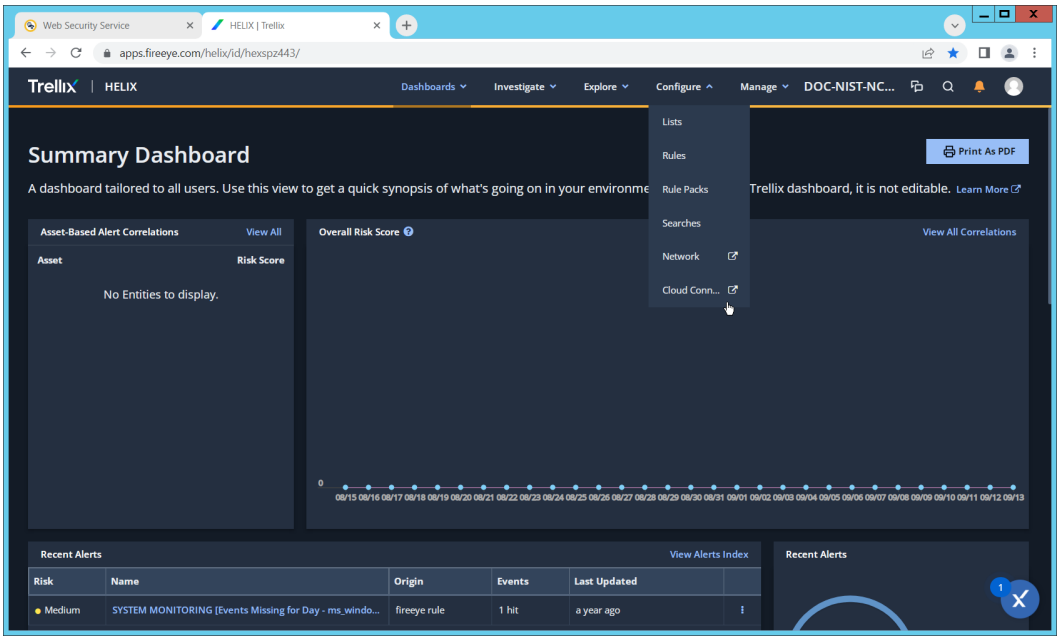
1. Navigate to the Symantec dashboard, and login.
2. Navigate to **Account Configuration** by clicking the gear icon on the left sidebar.



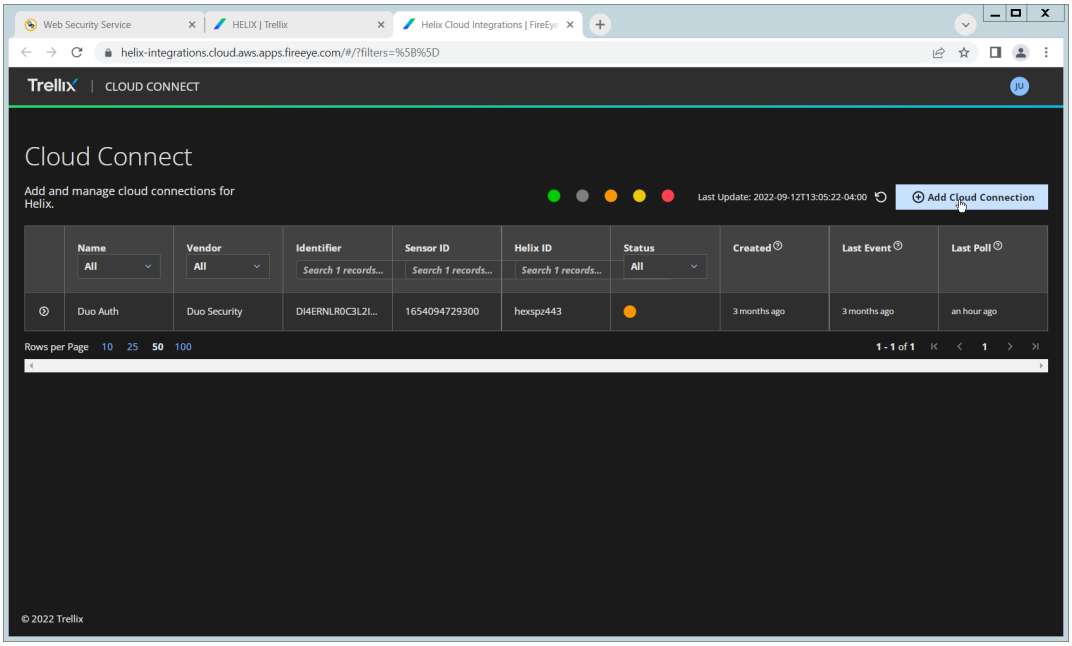
3. Click **API Credentials**.
4. Click **Add**.
5. Check the boxes next to **Reporting Access Logs**, **Location Management**, **Audit Logs**, **Agent Config Management**, and **Egress IP**.
6. Set an **Expiration Date** for the credential (1 year recommended).
7. Copy the **Username** and **Password**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



8. Click **Save**.

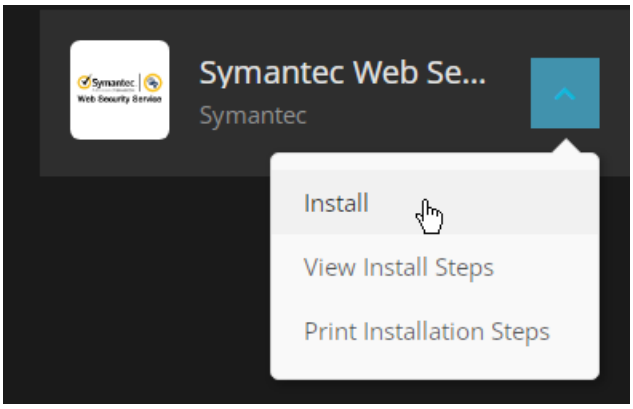


855 9. On the Helix Dashboard, click **Configure > Cloud Connect**.

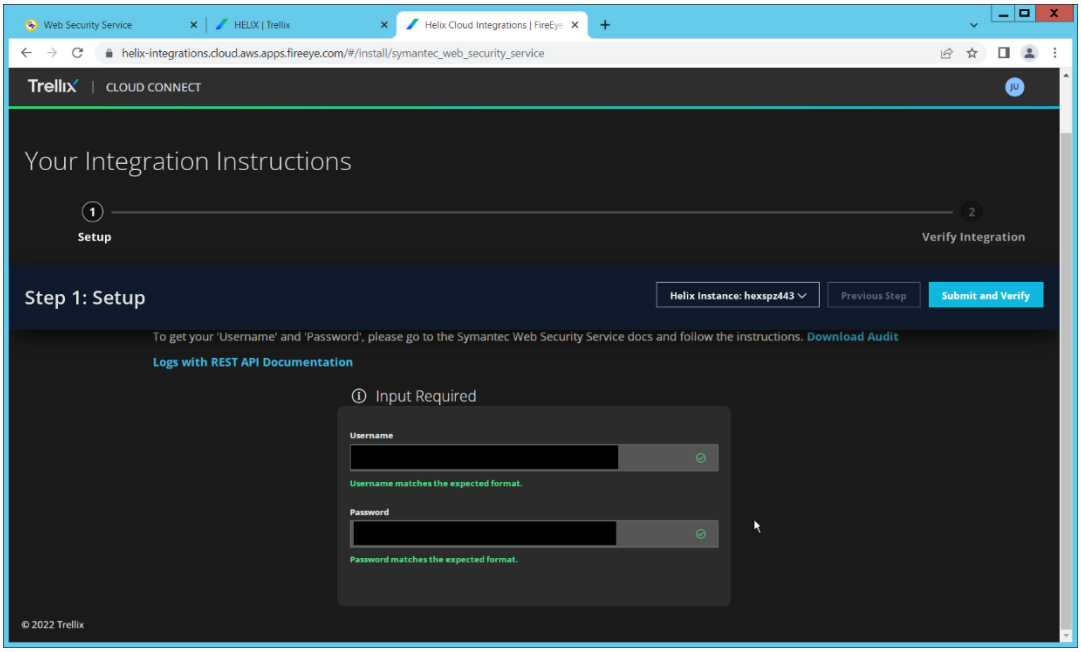


856 10. Click **Add Cloud Connection**.

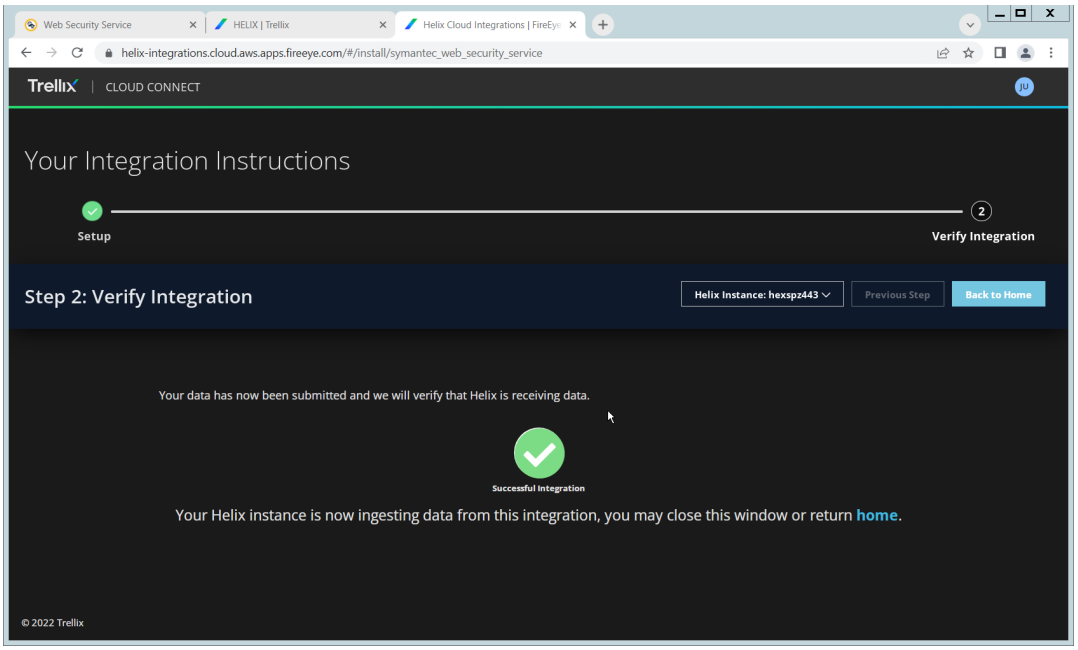
857 11. Click the arrow next to Symantec Web Security Service.



858 12. Click **Install**.



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



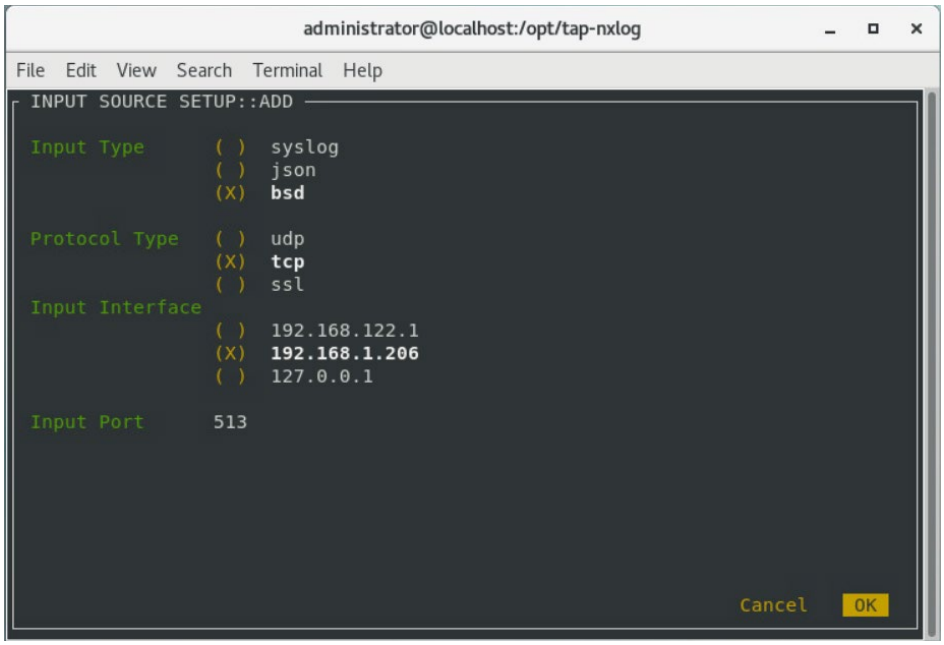
14. Click **Submit and Verify**.
15. Click **Back to Home**. You will now be able to see events from Symantec WSS in Helix.

2.10 Integration: FireEye Helix and PKWARE PKProtect

In the following section, PKWARE PKProtect, which has been configured to identify and encrypt sensitive data, will be configured to forward these events to FireEye Helix. Logs from PKWARE PKProtect will allow us to monitor the use of encryption throughout the enterprise, and catch any suspicious decryptions which may indicate a breach. This section assumes the Helix Communications Broker has already been installed.

Configure the Helix Communications Broker

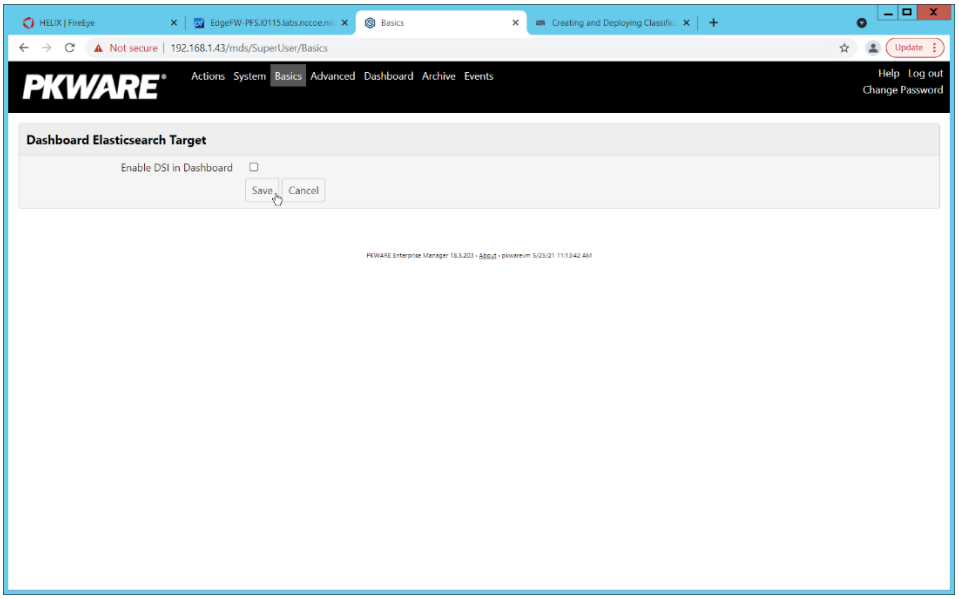
1. On the CentOS system with the Helix Communications Broker installed, run the following commands:
   ```
   > cd /opt/tap-nxlog
   > sudo ./setup.sh
   ```
2. Select **Add Routes** and press **Enter**.
3. Select **bsd**.
4. Select **tcp**.
5. Select the IP address of the network interface which should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



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

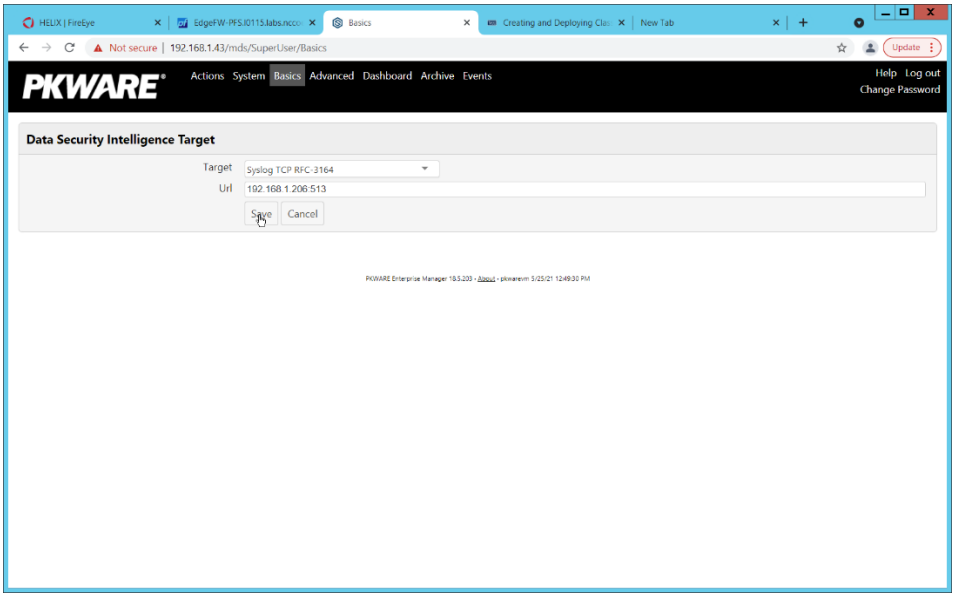
880 ## Configure PKWARE PKProtect to Forward Events

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



887 7. Click **Save**.
888 8. In the **Data Security Intelligence** section, click **Internal** next to **Target**.

9. Select **Syslog TCP RFC-3164** for **Target**.
10. Enter the URL and port of the Helix Communications Broker that was just configured.



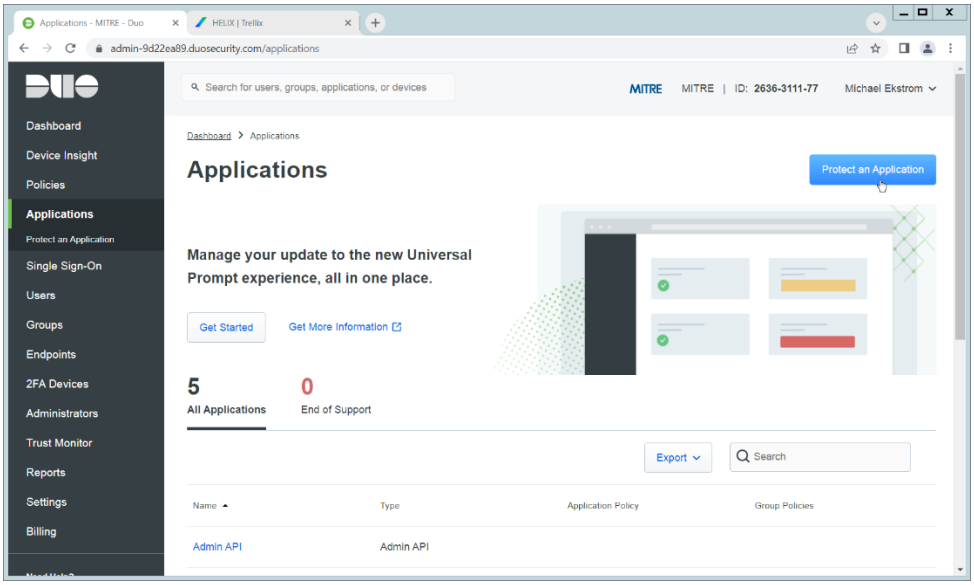
11. Click **Save**.
12. Verify that PKWARE logs now show up in Helix.

2.11 Integration: FireEye Helix and Cisco Duo

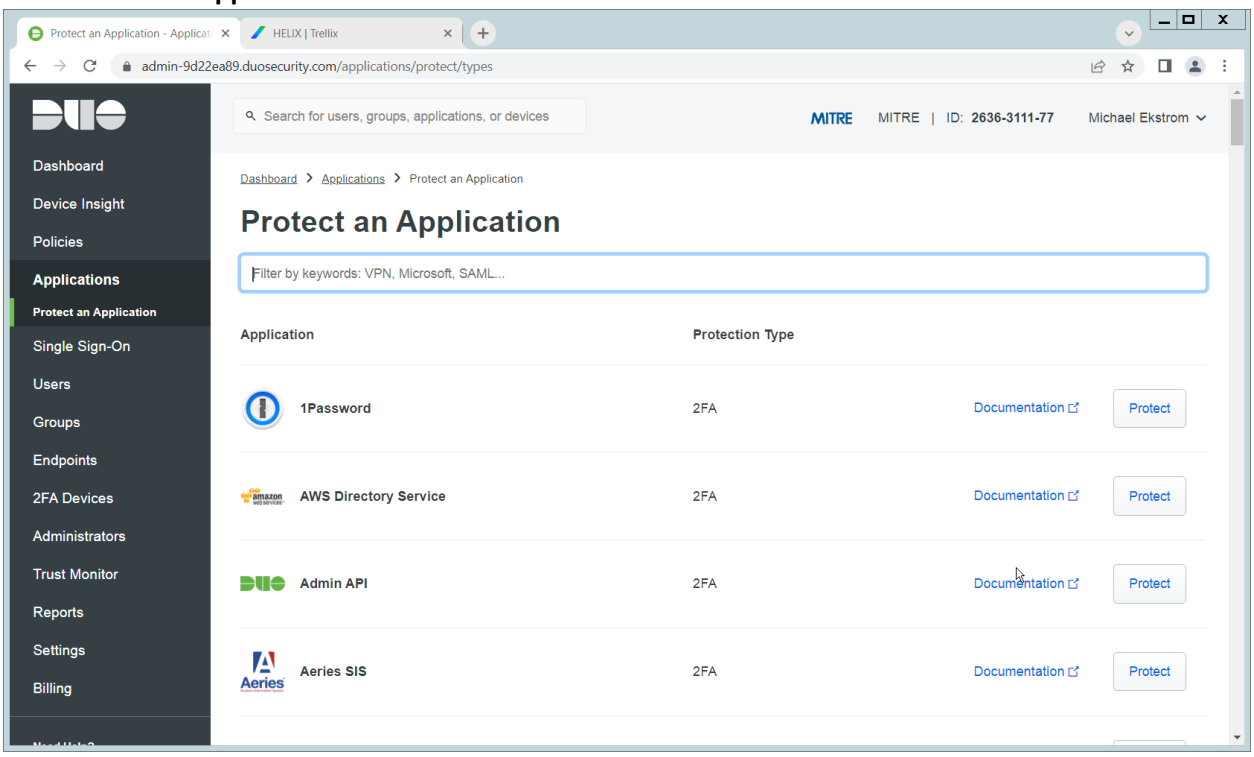
In this integration, FireEye Helix will be configured to collect logs from Cisco Duo. Cisco Duo is our multi-factor authentication mechanism and acts as source of information both for detecting breaches and for detecting insider threats. Information about a login, such as the username, time, location,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

Configure Fireye Helix to Collect Logs from Cisco Duo

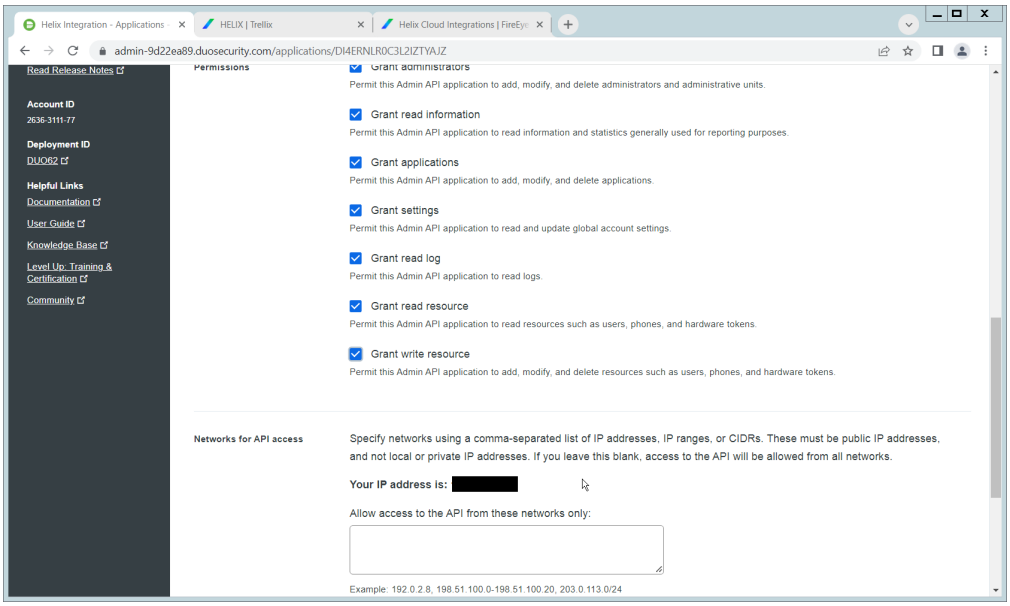
1. On the Cisco Duo dashboard navigate to **Applications**.



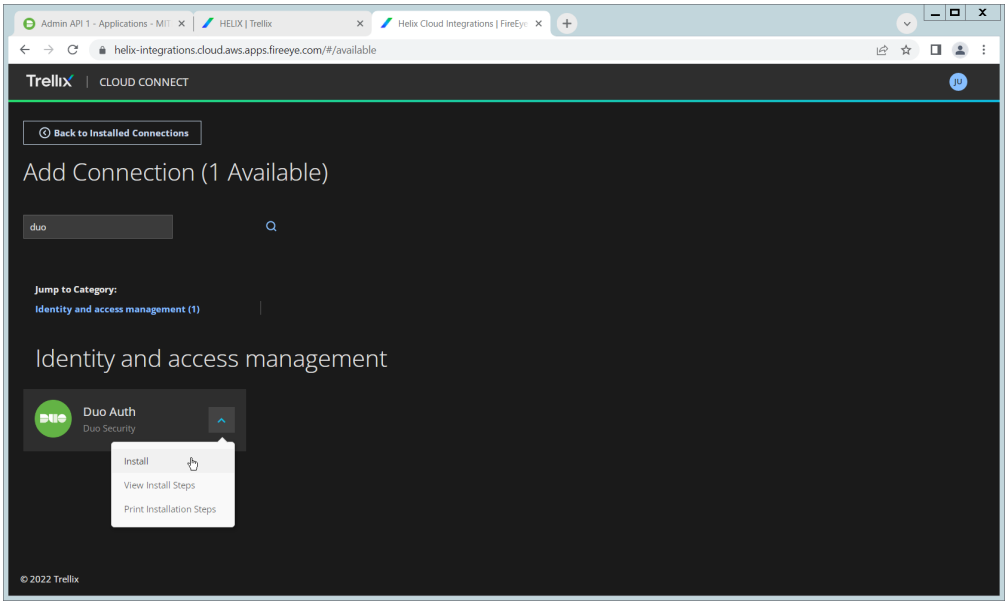
901 2. Click **Protect an Application**.



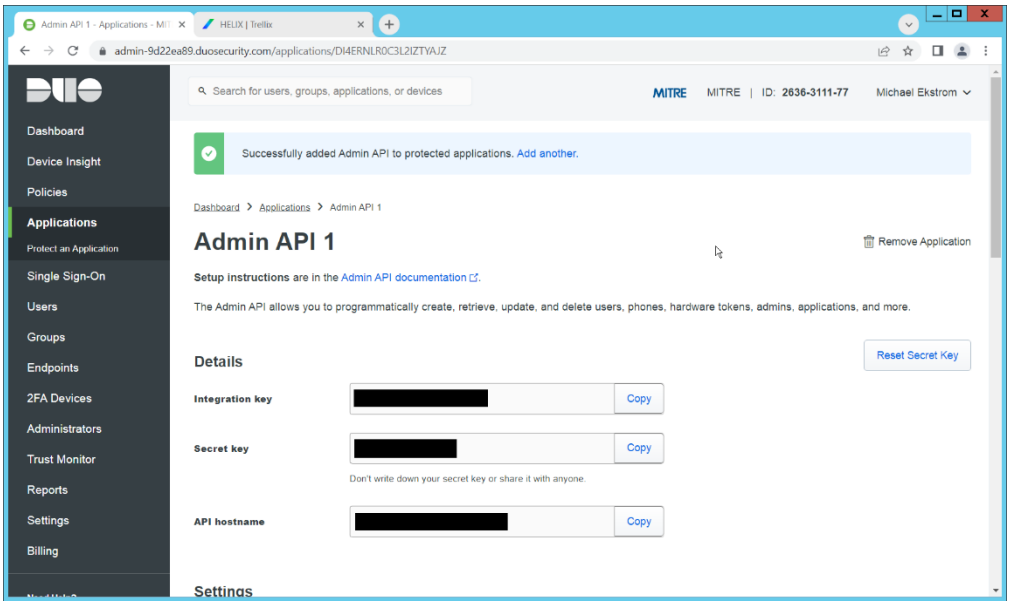
902 3. Click **Admin API**.



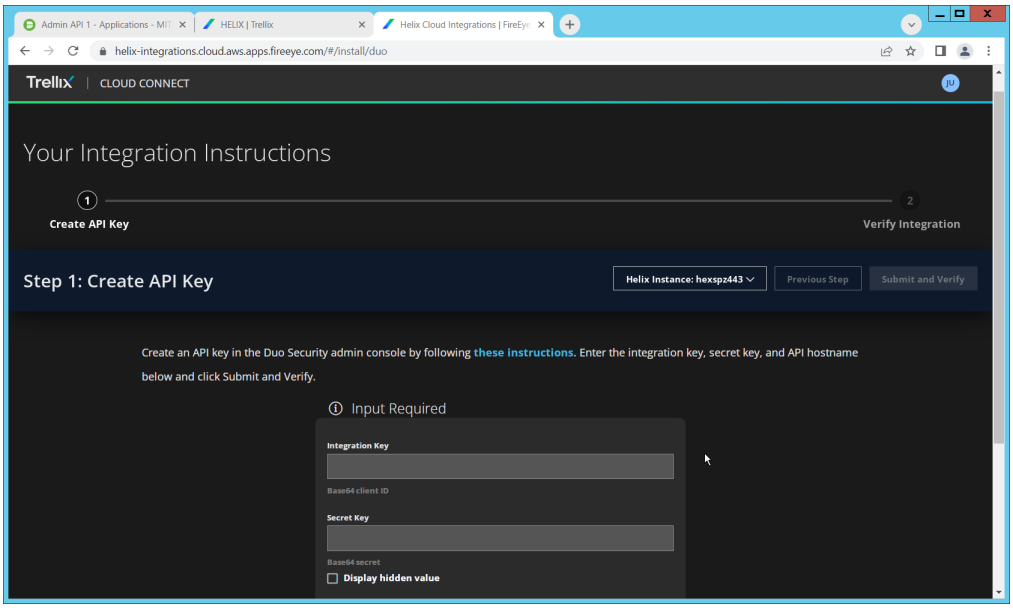
4. Scroll down and check the boxes next to **Grant administrators**, **Grant read information**, **Grant applications**, **Grant settings**, **Grant read log**, **Grant read resource**, and **Grant write resource**
5. Click **Save**.
6. Login to the Helix dashboard.
7. Navigate to **Configure** > **Cloud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



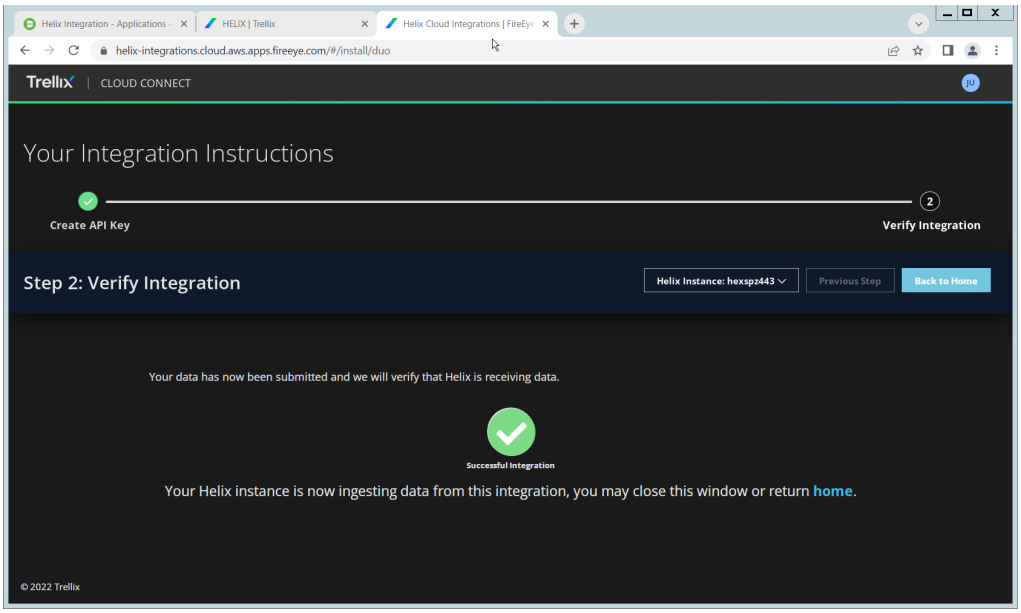
10. Click the **Arrow** next to the Cisco Duo integration and click **Install**.



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



12. Click **Submit and Verify**.



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

2.12 Integration: FireEye Helix and QCOR ForceField

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

Configure an SFTP server on Windows

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

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

1. Download OpenSSH from here (https://github.com/PowerShell/Win32-OpenSSH/releases). During the creation of this guide, version V8.9.1.0p1-Beta was used.
2. Extract to `C:\Program Files\OpenSSH`.
3. In a Powershell window, navigate to the folder you extracted it to, and run the following command to install the server.

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

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

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

5. Open **services.msc** and start the **OpenSSH SSH server**.
6. Create a file called **authorized_keys** in **C:\Users\<Your Username>\.ssh**. If needed, create the **.ssh** folder (Windows will not allow you to create it by default – naming the folder **.ssh.** will allow you to bypass this restriction.)
7. Generate a key using **./ssh-keygen**. Copy the contents of the generated public key (.pub file) into the **authorized_keys** file created earlier. The private key should be placed in the **~/.ssh** folder on the Linux machine.
8. Right click the **authorized_keys** file and click **Properties**.
9. Click **Disable Inheritance**.
10. Select **Convert inherited permissions into explicit permissions on this object**.
11. Using the remove button, remove all accounts other than SYSTEM from the list. Ensure that the SYSTEM account has full control.
12. Under **C:\ProgramData\ssh**, open **sshd_config**.
13. Comment out these lines by adding '#' characters before each line, like so:

```
#Match Group administrators
#       AuthorizedKeysFile
__PROGRAMDATA__/ssh/administrators_authorized_keys
```

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

```
PubkeyAuthentication yes
PubkeyAcceptedKeyTypes=+ssh-rsa
```

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

```
ForceCommand internal-sftp
ChrootDirectory C:\GreenTec\ForceField\log
```

17. Alternatively, if it's preferable to set the root directory somewhere else and move the log file, you can also do that. To edit the log file location, simply open **C:\GreenTec\Forcefield\wfs.conf** and change **Logpath** to a different directory, and update **ChrootDirectory** to point to that.
18. After doing this, you should be able to authenticate over SSH to the server. If the authentication fails, you can check the logs in Event Viewer on the server, under **Applications and Services Logs > OpenSSH > Operational** to see the reason for the failure.

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

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

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

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

```
Crontab -e
```

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

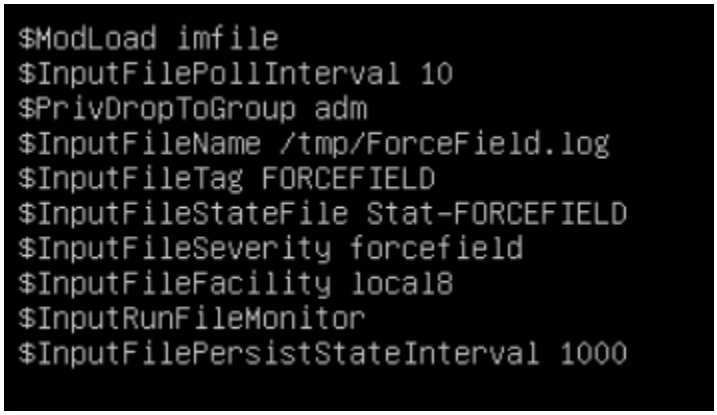
```
0 * * * * sftp
administrator@forcefield.dc.ipdrr:/ForceField.log
/tmp/ForceField.log
```

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

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

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

```
sudo nano /etc/rsyslog.d/forcefield.conf
$ModLoad imfile
$InputFilePollInterval 10
$PrivDropToGroup adm
$InputFileName /tmp/ForceField.log
$InputFileTag FORCEFIELD
$InputFileStateFile Stat-FORCEFIELD
$InputFileFacility local8
$InputRunFileMonitor
$InputFilePersistStateInterval 1000
```



25. Restart rsyslog.

```
sudo service rsyslog restart
```

2.13 Integration: FireEye Helix and Dispel

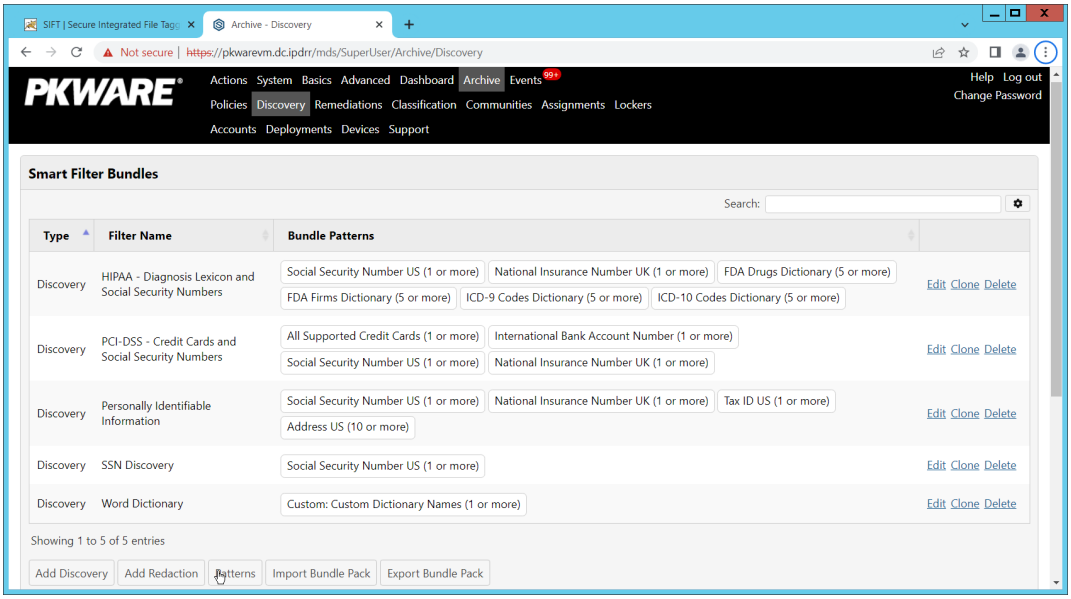
In this integration, we configure the collection of logs from Dispel, our network protection solution. Because Dispel controls access from users to enterprise systems it is important to have an overview of its actions through log collection and reporting. Dispel personnel can perform this integration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

2.14 Integration: Avrio SIFT and PKWARE PKProtect

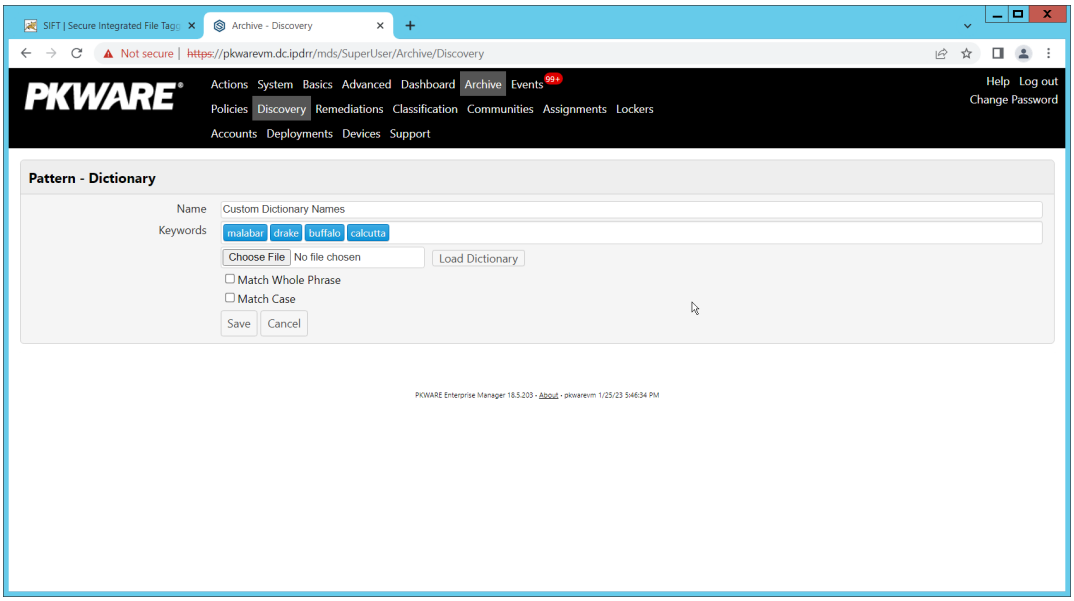
When used together, SIFT and PKProtect can protect sensitive data accidentally dropped into public shares on the enterprise. In Section 2.6, we detail how to configure SIFT to detect sensitive data in a Windows Share and move it to a location designated for sensitive information. Now, we will demonstrate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

Configuring PKWARE PKProtect

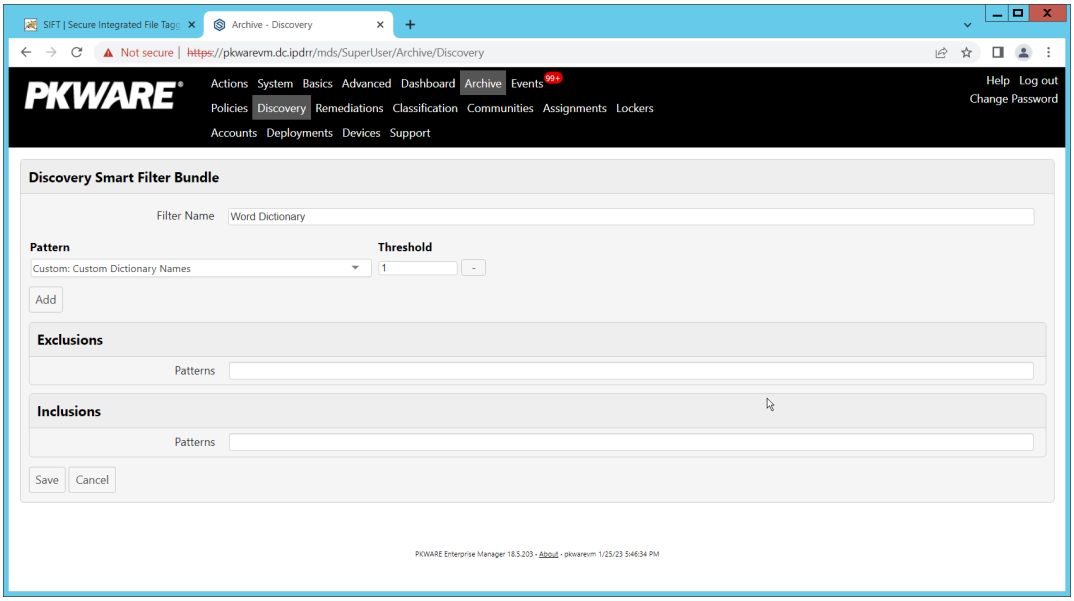
1. Navigate to the PKProtect dashboard and login.
2. Navigate to **Archive > Discovery**.



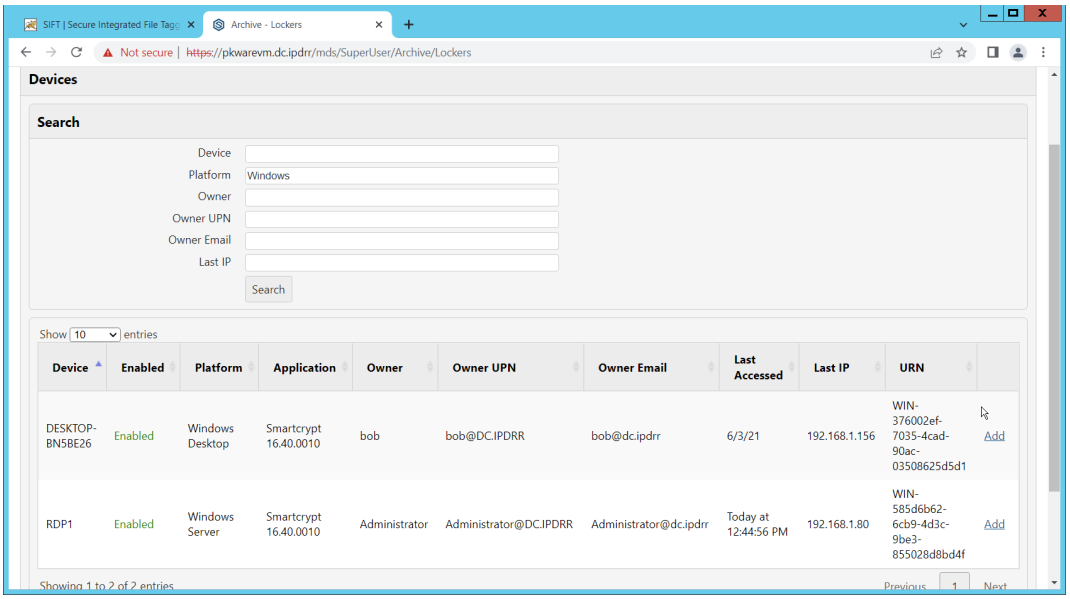
3. Click **Pattern – Dictionary.**
4. Enter a name for these patterns in the **Name** field.
5. Enter keywords to match in the **Keywords** field.



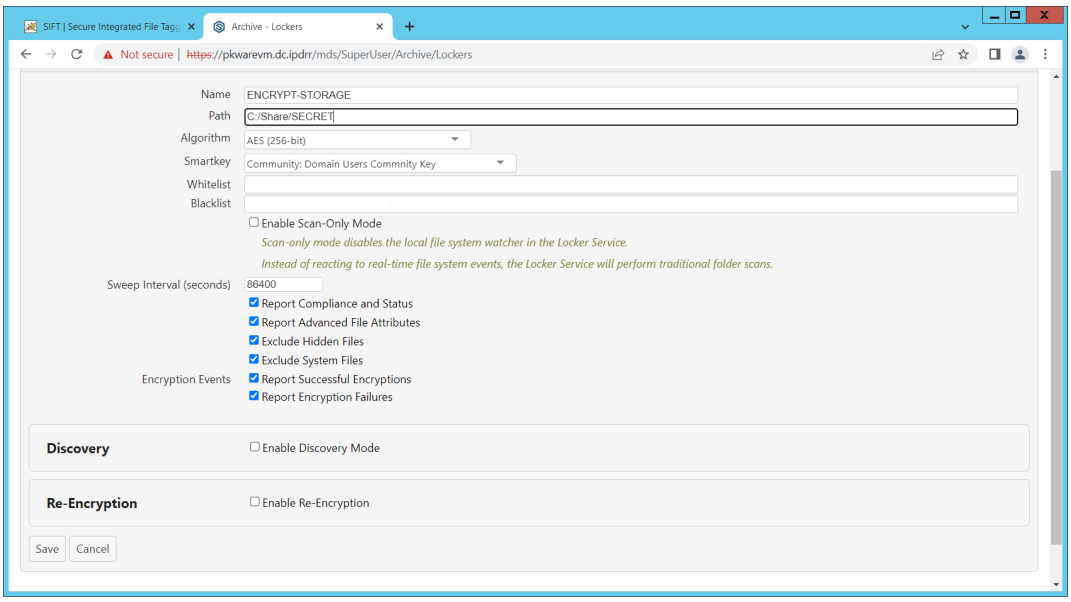
6. Click **Save**.
7. Click **Add Discovery**.
8. Under **Pattern**, select the name of the **Pattern** you just created.
9. For **Threshold**, enter the number of matches of this pattern needed to consider the file sensitive.



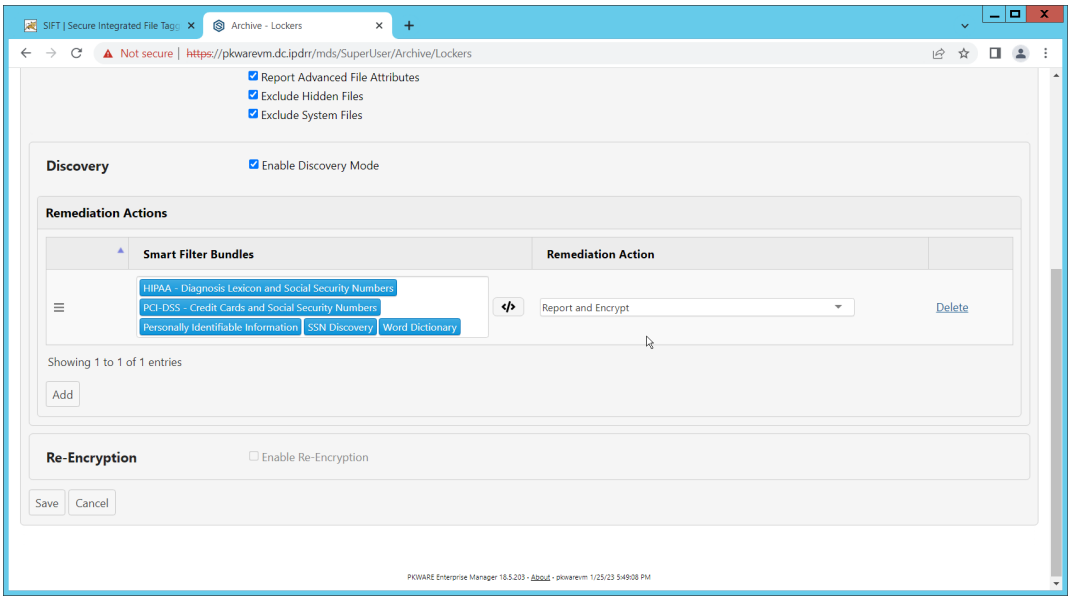
10. Click **Save**.
11. Navigate to **Archive > Lockers**.
12. Ensure that a PKWARE client is installed on the device which will be monitored for encryption. The device should show up in the list. If it doesn't you can search for the device and select it from the list.



13. Click **Add** on the device you wish to add a locker for.
14. Enter a **Name** for the locker.
15. Enter the **path** to the protected folder.
16. Select **AES 256** for the **Algorithm**.
17. Select the PKWARE Smartkey to use.
18. Check all the boxes next to **Encryption Events**.



19. Check the box next to **Enable Discovery Mode**.
20. Add the relevant rules to the **Smart Filter Bundles** box.
21. Select **Report and Encrypt** for **Remediation Action**.



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

2.15 Integration: Dispel and Cisco Duo

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

In this particular integration, no extra work was required other than installing Cisco Duo (see Section 2.7) on systems to control remote desktop access between Dispel machines and the other machines. However, it is important for organizations to check that this integration works and is present, to ensure that multifactor authentication is being applied to users who are logging in remotely.

Appendix A List of Acronyms

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

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