## Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events

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

Jennifer Cawthra Michael Ekstrom Lauren Lusty Julian Sexton John Sweetnam

FINAL

This publications is available free of charge from <u>https://doi.org/10.6028/NIST.SP.1800-26</u>.

This publication is available free of charge from <a href="https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond">https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond</a>.





# Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events

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

> Jennifer Cawthra National Cybersecurity Center of Excellence NIST

> > Michael Ekstrom Lauren Lusty Julian Sexton John Sweetnam The MITRE Corporation McLean, Virginia

> > > FINAL

DECEMBER 2020



U.S. Department of Commerce Wilbur Ross, Secretary

National Institute of Standards and Technology Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

## **NIST SPECIAL PUBLICATION 1800-26A**

# Data Integrity:

Detecting and Responding to Ransomware and Other Destructive Events

Volume A: Executive Summary

Jennifer Cawthra National Cybersecurity Center of Excellence NIST

Michael Ekstrom Lauren Lusty Julian Sexton John Sweetnam Anne Townsend

The MITRE Corporation McLean, Virginia

December 2020

FINAL

This publications is available free of charge from https://doi.org/10.6028/NIST.SP.1800-26.

This publication is available free of charge from <a href="https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond">https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond</a>.





## **Executive Summary**

The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability, as follows.

- Confidentiality preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity
- Availability ensuring timely and reliable access to and use of information

Data Confidentiality

This series of practice guides focuses on data integrity: the property that data has not been altered in an unauthorized manner. Data integrity covers 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.)

- Destructive malware, ransomware, malicious insider activity, and even honest mistakes all set the stage for why organizations need to detect and respond to an event that impacts data integrity. Businesses must be confident that these events are detected in a timely fashion and responded to appropriately.
- Attacks against an organization's data can compromise emails, employee records, financial records, and customer information—impacting business operations, revenue, and reputation.
- Examples of data integrity attacks include unauthorized insertion, deletion, or modification of data to corporate information such as emails, employee records, financial records, and customer data.
- The National Cybersecurity Center of Excellence (NCCoE) at NIST built a laboratory environment to explore methods to effectively detect and respond to a data



integrity event in various information technology (IT) enterprise environments, to immediately react to the event in an effort to prevent a complete compromise.

• This NIST Cybersecurity Practice Guide demonstrates how organizations can develop and implement appropriate actions during a detected data integrity cybersecurity event.

### **CHALLENGE**

Some organizations have experienced systemic attacks that force operations to cease. One variant of a data integrity attack–ransomware–encrypts data, leaving it modified in an unusable state. Other data integrity attacks may be more dynamic, targeting machines, spreading laterally across networks, and

continuing to cause damage throughout an organization. In either case, behaviors are exhibited—such as files inexplicably becoming encrypted or network activity—that provide an ability to immediately detect the occurrence and respond in a timely fashion to curtail the ramifications.

## **SOLUTION**

NIST published version 1.1 of the Cybersecurity Framework in April 2018 to help organizations better manage and reduce cybersecurity risk to critical infrastructure and other sectors. The framework core contains five functions, listed below.

- Identify develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
- Protect develop and implement appropriate safeguards to ensure delivery of critical services
- Detect develop and implement appropriate activities to identify the occurrence of a cybersecurity event
- Respond develop and implement appropriate activities to take action regarding a detected cybersecurity incident



 Recover – develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

For more information, see the <u>Framework for Improving Critical Infrastructure Cybersecurity v1.1.</u>

Applying the Cybersecurity Framework to data integrity, this practice guide informs organizations of how to quickly **detect** and **respond** to data integrity attacks by implementing appropriate activities that immediately inform about the data integrity events.

The NCCoE developed and implemented a solution that incorporates multiple systems working in concert to **detect** an ongoing data integrity cybersecurity event. Additionally, the solution provides guidance on how to **respond** to the detected event. Addressing these functions together enables organizations to have the necessary tools to act during a data integrity attack.

The NCCoE sought existing technologies that provided the following capabilities:

- event detection
- integrity monitoring
- logging
- reporting
- mitigation and containment
- forensics/analytics

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.

### **BENEFITS**

The NCCoE's practice guide to Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events can help your organization:

- develop a strategy for detecting and responding to a data integrity cybersecurity event
- facilitate effective detection and response to adverse events, maintain operations, and ensure the integrity and availability of data critical to supporting business operations and revenuegenerating activities
- manage enterprise risk (consistent with foundations of the NIST Framework for Improving Critical Infrastructure Cybersecurity)

## SHARE YOUR FEEDBACK

You can view or download the guide at <u>https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond</u>. 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 <u>ds-nccoe@nist.gov</u>.

## **TECHNOLOGY PARTNERS/COLLABORATORS**

Organizations 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). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) 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.

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 challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

#### LEARN MORE

Visit <u>https://www.nccoe.nist.gov</u> nccoe@nist.gov 301-975-0200

## **NIST SPECIAL PUBLICATION 1800-26B**

# Data Integrity:

Detecting and Responding to Ransomware and Other Destructive Events

Volume B: Approach, Architecture, and Security Characteristics

Jennifer Cawthra

National Cybersecurity Center of Excellence NIST

#### Michael Ekstrom Lauren Lusty Julian Sexton John Sweetnam

The MITRE Corporation McLean, Virginia

December 2020

FINAL

This publications is available free of charge from <a href="https://doi.org/10.6028/NIST.SP.1800-26">https://doi.org/10.6028/NIST.SP.1800-26</a>.

This publication is available free of charge from <a href="https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond">https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond</a>.





#### 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 1800-26B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-26B, 54 pages, (December 2020), CODEN: NSPUE2

## **FEEDBACK**

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

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: <u>nccoe@nist.gov</u>

## 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 <u>https://www.nccoe.nist.gov/</u>. To learn more about NIST, visit <u>https://www.nist.gov.</u>

## 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

Ransomware, destructive malware, insider threats, and even honest mistakes present an ongoing threat to organizations that manage data in various forms. Database records and structure, system files, configurations, user files, application code, and customer data are all potential targets of data corruption and destruction.

A timely, accurate, and thorough detection and response to a loss of data integrity can save an organization time, money, and headaches. While human knowledge and expertise is an essential component of these tasks, the right tools and preparation are essential to minimizing downtime and

losses due to data integrity events. The NCCoE, in collaboration with members of the business community and vendors of cybersecurity solutions, has built an example solution to address these data integrity challenges. This project details methods and potential tool sets that can detect, mitigate, and contain data integrity events in the components of an enterprise network. It also identifies tools and strategies to aid in a security team's response to such an event.

## **KEYWORDS**

attack vector; data integrity; malicious actor; malware; malware detection; malware response; ransomware.

## ACKNOWLEDGMENTS

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

Name	Organization
Kyle Black	Bay Dynamics
Sunjeet Randhawa	Broadcom Inc.
Peter Romness	Cisco Systems
Matthew Hyatt	Cisco Systems
Matthew Shabat	Glasswall Government Solutions
Justin Rowland	Glasswall Government Solutions
Greg Rhein	Glasswall Government Solutions
Steve Roberts	Micro Focus
Timothy McBride	NIST
Christopher Lowde	Semperis

Name	Organization
Thomas Leduc	Semperis
Darren Mar-Elia	Semperis
Kirk Lashbrook	Semperis
Mickey Bresman	Semperis
Humphrey Christian	Symantec Corporation
Jon Christmas	Symantec Corporation
Kenneth Durbin	Symantec Corporation
Matthew Giblin	Symantec Corporation
Jim Wachhaus	Tripwire
Nancy Correll	The MITRE Corporation
Chelsea Deane	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Milissa McGinnis	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Denise Schiavone	The MITRE Corporation
Anne Townsend	The MITRE Corporation

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

Technology Partner/Collaborator	Build Involvement
Symantec Corporation	Symantec Information Centric Analytics v6.5.2 Symantec Security Analytics v8.0.1
Cisco Systems	Cisco Identity Services Engine v2.4, Cisco Advanced Malware Protection v5.4, Cisco Stealthwatch v7.0.0
Glasswall Government Solutions	Glasswall FileTrust Advanced Threat Protection (ATP) for Email v6.90.2.5
Tripwire	Tripwire Log Center v7.3.1, Tripwire Enterprise v8.7
Micro Focus	Micro Focus ArcSight Enterprise Security Manager v7.0 Patch 2
Semperis	Semperis Directory Services Protector v2.7

## Contents

1	Sun	nmary	/	1
	1.1	Challe	nge	. 2
	1.2	Solutio	on	. 2
	1.3	Benefi	ts	. 3
2	Hov	v to U	se This Guide	4
	2.1	Турод	raphic Conventions	. 5
3	Арр	roach	1	6
	3.1	Audier	nce	. 6
	3.2	Scope		. 6
	3.3	Assum	iptions	. 7
	3.4	Risk As	ssessment	. 7
		3.4.1	Risk	.8
		3.4.2	Security Control Map	.9
	3.5	Techn	ologies1	13
4	Arc	hitect	ure1	6
	4.1	Archit	ecture Description1	16
		4.1.1	High-Level Architecture1	16
		4.1.2	Architecture Components1	17
5	Sec	urity (	Characteristic Analysis2	0
	5.1	Assum	ptions and Limitations2	20
	5.2	Build 1	۲esting 2	20
	5.3	Scena	rios and Findings2	21
		5.3.1	Ransomware via Web Vector and Self-Propagation2	21
		5.3.2	Destructive Malware via USB Vector	22
		5.3.3	Accidental VM Deletion via Maintenance Script2	23
		5.3.4	Backdoor Creation via Email Vector2	
		5.3.5	Database Modification via Malicious Insider2	25

		5.3.6	File Modification via Malicious Insider	26
		5.3.7	Backdoor Creation via Compromised Update Server	27
6 F	utu	ire Bi	uild Considerations	27
Арро	end	lix A	List of Acronyms	29
Арро	end	lix B	Glossary	30
Арро	end	lix C	References	34
Арро	end	lix D	Functional Evaluation	36
C	D.1	Data I	ntegrity Functional Test Plan	36
C	0.2	Data I	ntegrity Use Case Requirements	37
C	0.3	Test C	ase: Data Integrity DR-1	44
C	0.4	Test C	ase: Data Integrity DR-2	46
D	).5	Test C	Case: Data Integrity DR-3	47
C	0.6	Test C	ase: Data Integrity DR-4	48
C	0.7	Test C	Case: Data Integrity DR-5	50
C	0.8	Test C	ase: Data Integrity DR-6	51
C	0.9	Test C	Case: Data Integrity DR-7	52

## **List of Figures**

Figure 4-1 DI Detect & P	<b>Respond High-Level Architecture</b>	

## **List of Tables**

Table 3-1 DI Reference Design Cybersecurity Framework Core Components Map	LO
Table 3-2 Products and Technologies         1	L3
Table 6-1 Test Case Fields	36
Table 6-2 Capability Requirements	37
Table 6-3 Test Case ID: Data Integrity DR-1	14
Table 6-4 Test Case ID: Data Integrity DR-2	<b>16</b>
Table 6-5 Test Case ID: Data Integrity DR-3	17
Table 6-6 Test Case ID: Data Integrity DR-4         4	18
Table 6-7 Test Case ID: Data Integrity DR-5	50
Table 6-8 Test Case ID: Data Integrity DR-6	51
Table 6-9 Test Case ID: Data Integrity DR-7	52

## **1** Summary

Businesses face a near-constant threat of destructive malware, ransomware, malicious insider activities, and even honest mistakes that can alter or destroy critical data. These types of adverse events ultimately impact data integrity (DI). It is imperative for organizations to be able to detect and respond to DI attacks.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore methods to detect and respond to a data corruption event in various information technology (IT) enterprise environments. The example solution outlined in this guide describes the solution built in the NCCoE lab. It encourages detection and mitigation of DI events while facilitating analysis of these events.

The goals of this NIST Cybersecurity Practice Guide are to help organizations confidently:

- detect malicious and suspicious activity generated on the network, by users, or from applications that could indicate a DI event
- mitigate and contain the effects of events that can cause a loss of DI
- monitor the integrity of the enterprise for detection of events and after-the-fact analysis
- utilize logging and reporting features to speed response time to DI events
- analyze DI events for the scope of their impact on the network, enterprise devices, and enterprise data
- analyze DI events to inform and improve the enterprise's defenses against future attacks

For ease of use, here is a short description of the different sections of this volume.

- Section 1: Summary presents the challenge addressed by the NCCoE project with an in-depth look at our approach, the architecture, and the security characteristics we used; the solution demonstrated to address the challenge; the benefits of the solution; and the technology partners that participated in building, demonstrating, and documenting the solution. Summary also explains how to provide feedback on this guide.
- <u>Section 2</u>: How to Use This Guide explains how readers—business decision-makers, program managers, and IT professionals (e.g., systems administrators)—might use each volume of the guide.
- Section 3: Approach offers a detailed treatment of the scope of the project and describes the assumptions on which the security platform development was based, the risk assessment that informed platform development, and the technologies and components that industry collaborators gave us to enable platform development.

- <u>Section 4</u>: Architecture describes the usage scenarios supported by project security platforms, including Cybersecurity Framework [1] functions supported by each component contributed by our collaborators.
- Section 5: Security Characteristic Analysis provides details about the tools and techniques we used to perform risk assessments.
- <u>Section 6</u>: Future Build Considerations is a brief treatment of other data security implementations that NIST is considering consistent with Cybersecurity Framework Core Functions: Identify, Protect, Detect, Respond, and Recover.

## 1.1 Challenge

Thorough collection of quantitative and qualitative data is important to organizations of all types and sizes. It can impact all aspects of a business, including decision making, transactions, research, performance, and profitability. When these data collections sustain a DI attack caused by unauthorized insertion, deletion, or modification of information, such an attack can impact emails, employee records, financial records, and customer data, rendering them unusable or unreliable. Some organizations have experienced systemic attacks that caused a temporary cessation of operations. One variant of a DI attack—ransomware—encrypts data and holds it hostage while the attacker demands payment for the decryption keys.

When DI events occur, organizations should have the capabilities to detect and respond in real time. Early detection and mitigation can reduce the potential impact of events, including damage to enterprise files, infection of systems, and account compromise. Furthermore, organizations should be able to learn from DI events to improve their defenses. Analysis of malicious behavior at the network level, user level, and file level can reveal flaws in the security of the enterprise. Resolution of these flaws, though out of scope of this guide, is often only possible once they have been exploited and with the right solution in place.

## **1.2 Solution**

The NCCoE implemented a solution that incorporates appropriate actions during and directly after a DI event. The solution is composed of multiple systems working together to detect and respond to data corruption events in standard enterprise components. These components include mail servers, databases, end-user machines, virtual infrastructure, and file share servers. Furthermore, an important function of the Respond Category of the Cybersecurity Framework is improvement of defenses—this guide includes components that aid in analysis of DI events and for improving defenses against them.

The NCCoE sought existing technologies that provided the following capabilities:

- event detection
- integrity monitoring

- logging
- reporting
- mitigation and containment
- forensics/analytics

In developing our solution, we used standards and guidance from the following, which can also provide your organization with relevant standards and best practices:

- NIST Framework for Improving Critical Infrastructure Cybersecurity (commonly known as the NIST Cybersecurity Framework [1]
- NIST Interagency or Internal Report (NISTIR) 8050: *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy* [2]
- NIST Special Publication (SP) 800-30 Rev. 1: Guide for Conducting Risk Assessments [3]
- NIST SP 800-37 Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [4]
- NIST SP 800-39: Managing Information Security Risk [5]
- NIST SP 800-40 Rev. 3: Guide to Enterprise Patch Management Technologies [6]
- NIST SP 800-53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations [7]
- Federal Information Processing Standard 140-2: Security Requirements for Cryptographic Modules [8]
- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response [9]
- NIST SP 800-92: Guide to Computer Security Log Management [10]
- NIST SP 800-100: Information Security Handbook: A Guide for Managers [11]
- NIST SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems [12]
- Office of Management and Budget, Circular Number A-130: Managing Information as a Strategic Resource [13]
- NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide [14]
- NIST SP 800-83 Rev. 1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops [15]
- NIST SP 800-150: Guide to Cyber Threat Information Sharing [16]
- NIST SP 800-184: Guide for Cybersecurity Event Recovery [17]

## **1.3 Benefits**

The NCCoE's practice guide can help your organization:

- develop an implementation plan for detecting and responding to cybersecurity events
- facilitate detection, response, and analysis of DI events to improve defenses and mitigate impact

- maintain integrity and availability of data that is critical to supporting business operations and revenue-generating activities
- manage enterprise risk (consistent with the foundations of the NIST Cybersecurity Framework)

## 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 DI detection and response solution. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-26A: *Executive Summary*
- NIST SP 1800-26B: Approach, Architecture, and Security Characteristics what we built and why (you are here)
- NIST SP 1800-26C: 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 1800-26A, which describes the following topics:

- challenges that enterprises face in detecting and responding to data integrity events
- 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 1800-26B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.1, Risk, provides a description of the risk analysis we performed.
- <u>Section 3.4.2</u>, 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 1800-26A, with your leadership team members to help them understand the importance of adopting a standards-based solution to detect and respond to data integrity events.

**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 1800-26C, 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 DI detection and response solution. 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 3.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. 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 <u>ds-nccoe@nist.gov</u>.

## 2.1 Typographic Conventions

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

The following table presents typographic conventions used in this volume.

## **3** Approach

Based on key points expressed in NISTIR 8050: *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy* (2015), the NCCoE is pursuing a series of DI projects to map the Core Functions of the NIST Cybersecurity Framework. This project is centered on the Core Functions of Detect and Respond, which consist of detecting and responding to DI attacks. Compromise can come from malicious websites, targeted emails, insider threats, and honest mistakes. Monitoring solutions should be in place to detect these events. Once detected, swift response to a threat is critical to mitigate the need for recovery action after an event occurs. NCCoE engineers working with a Community of Interest (COI) defined the requirements for this DI project.

Members of the COI, which include participating vendors referenced in this document, contributed to development of the architecture and reference design, providing technologies that meet the project requirements and assisting in installation and configuration of those technologies. The practice guide highlights the approach used to develop the NCCoE reference solution. Elements include risk assessment and analysis, logical design, build development, test and evaluation, and security control mapping. This guide is intended to provide practical guidance to any organization interested in implementing a solution for detecting and responding to a cybersecurity event.

## 3.1 Audience

This guide is intended for individuals responsible for implementing security solutions in organizations' IT support activities. Current IT systems, particularly in the private sector, often lack the capability to comprehensively detect, mitigate, and learn from cybersecurity events. The platforms demonstrated by this project and the implementation information provided in this practice guide permit integration of products to implement a data integrity detection and response system. The technical components will appeal to system administrators, IT managers, IT security managers, and others directly involved in the secure and safe operation of business IT networks.

## 3.2 Scope

The guide provides practical, real-world guidance on developing and implementing a DI solution consistent with the principles in the NIST Framework for Improving Critical Infrastructure Cybersecurity Volume 1, specifically the Core Functions of Detect and Respond. Detecting emphasizes developing and implementing the appropriate activities to detect events in real time, compare the current system state to a norm, and produce audit logs for use during and after the event. Responding emphasizes real-time mitigation of events, forensic analysis during and after the event, and reporting. Examples of outcomes within these functions are integrity monitoring, event detection, logging, reporting, forensics, and mitigation.

## 3.3 Assumptions

This project is guided by the following assumptions:

- The solution was developed in a lab environment. The environment is based on a basic organization's IT enterprise. It does not reflect the complexity of a production environment: for example, building across numerous physical locations, accommodating extreme working conditions, or configuring systems to meet specific network/user needs. These demands can all increase the level of complexity needed to implement a DI solution.
- An organization has access to the skill sets and resources required to implement an event detection and response system.
- A DI event is taking place, and the organization is seeking to detect and mitigate the damage that an event is causing.

## 3.4 Risk Assessment

<u>NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments</u>, 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 <u>NIST SP 800-37 Revision 2</u>, *Risk Management Framework for* <u>Information Systems and Organizations</u>—publicly available material. The <u>Risk Management Framework</u> (<u>RMF</u>) guidance, as a whole, proved invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

We performed two types of risk assessment:

- Initial analysis of the risk factors discussed with financial, retail, and hospitality institutions. This analysis led to creation of the DI project and the desired security posture. See NISTIR 8050, Executive Technical Workshop, for additional participant information.
- Analysis of how to secure the components within the solution and minimize any vulnerabilities they might introduce. See <u>Section 5</u>, Security Characteristic Analysis.

## 3.4.1 Risk

Using the guidance in NIST's series of publications concerning risk, we worked with financial institutions and the Financial Sector Information Sharing and Analysis Center to identify the most compelling risk factors encountered by this business group. We participated in conferences and met with members of the financial sector to define the main security risks to business operations. From these discussions came identification of an area of concern—DI. Having produced *Data Integrity: Recovering from Ransomware and Other Destructive Events,* which primarily focused on the recovery aspect of DI, we identified a need for guidance in the areas of detecting and responding to cybersecurity events in real time.

When considering risk from the perspective of detecting and responding to cybersecurity events during their execution, we must consider not only the impact of an event on an organization's assets but also the threats to those assets and the potential vulnerabilities these threats could exploit.

When discussing threats to an organization's assets from the perspective of DI, we consider these:

- malware
- insider threats
- accidents caused by human error
- compromise of trusted systems

The types of vulnerabilities we consider in relation to these threats include:

- zero-day vulnerabilities
- vulnerabilities due to outdated or unpatched systems
- custom software vulnerabilities/errors
- social engineering and user-driven events
- poor access control

Finally, the potential impact on an organization from a DI event:

- systems incapacitated
- modification/deletion of the organization's assets
- negative impact on the organization's reputation

Analysis of the threats, vulnerabilities, and potential impact to an organization has given us an understanding of the risk for organizations with respect to DI. NIST SP 800-39, *Managing Information Security Risk*, focuses on the business aspect of risk, namely at the enterprise level. This understanding is essential for any further risk analysis, risk response/mitigation, and risk monitoring activities. The following is a summary of the strategic risk areas we identified and their mitigations:

- Impact on system function—ensuring the availability of accurate data or sustaining an acceptable level of DI reduces the risk of systems' availability being compromised.
- Cost of implementation—implementing event detection and response from DI events once and using it across all systems may reduce system continuity costs.
- Compliance with existing industry standards–contributes to the industry requirement to maintain a continuity of operations plan.
- Maintenance of reputation and public image-helps reduce the damage caused by active events and facilitates the information needed to learn from the events.
- Increased focus on DI-includes not just loss of confidentiality but also harm from unauthorized alteration of data (per NISTIR 8050).

We subsequently translated the risk factors identified to security Functions and Subcategories within the NIST Cybersecurity Framework. In Table 3-1 we mapped the Categories to NIST SP 800-53 Rev. 4 controls.

## 3.4.2 Security Control Map

As explained in <u>Section 3.4.1</u>, we identified the Cybersecurity Framework security Functions and Subcategories that we wanted the reference design to support through a risk analysis process. This was a critical first step in drafting the reference design and example implementation to mitigate the risk factors. Table 3-1 lists the addressed Cybersecurity Framework Functions and Subcategories and maps them to relevant NIST standards, industry standards, and controls and best practices. The references provide solution validation points in that they list specific security capabilities that a solution addressing the Cybersecurity Framework Subcategories would be expected to exhibit. Organizations can use Table 3-1 to identify the Cybersecurity Framework Subcategories and NIST SP 800-53 Rev. 4 controls that they are interested in addressing.

When cross-referencing Functions of the Cybersecurity Framework with product capabilities used in this practice guide, it is important to consider:

- This practice guide, though primarily focused on Detect/Respond capabilities, also uses PR.DS-6, a Protect Subcategory. This is primarily because creation of integrity baselines is used for comparison when detecting attacks but is created prior to the start of an attack.
- Not all the Cybersecurity Framework Subcategories guidance can be implemented using technology. Any organization executing a DI solution would need to adopt processes and organizational policies that support the reference design. For example, some of the Subcategories within the Cybersecurity Framework Function called Respond are processes and policies that should be developed prior to implementing recommendations.

	Cyberse	curity Framework v1.1		Standards &	Standards & Best Practices	
Function	Category	Subcategory	NIST SP 800- 53 R4	ISO/IEC 27001:2013	NIST SP 800- 181	
PROTECT (PR)	Data Security (PR.DS)	PR.DS-6: Integrity check- ing mechanisms are used to verify software, firmware, and infor- mation integrity.	SC-16, SI-7	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4	OM-DTA-001	
	Anomalies and Events (DE.AE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is es- tablished and managed.	AC-4, CA-3, CM-2, SI-4	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2	SP-ARC-001	
DETECT (DE)		DE.AE-2: Detected events are analyzed to understand attack tar- gets and methods.	AU-6, CA-7, IR-4, SI-4	A.12.4.1, A.16.1.1, A.16.1.4	PR-CDA-001	
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	A.12.4.1, A.16.1.7	CO-OPS-001, PR-CIR-001	
		DE.AE-4: Impact of events is determined.	CP-2, IR-4, RA-3, SI-4	A.16.1.4	PR-INF-001	

#### Table 3-1 DI Reference Design Cybersecurity Framework Core Components Map

	Cybersecurity Framework v1.1			Standards &	Best Practices
Function	Category	Subcategory	NIST SP 800- 53 R4	ISO/IEC 27001:2013	NIST SP 800- 181
		DE.AE-5: Incident alert thresholds are estab- lished.	IR-4, IR-5, IR-8	A.16.1.4	PR-CIR-001
		DE.CM-1: The network is monitored to detect po- tential cybersecurity events.	AC-2, AU- 12, CA-7, CM-3, SC-5, SC-7, SI-4		OM-NET-001
		DE.CM-3: Personnel ac- tivity is monitored to de- tect potential cybersecu- rity events.	AC-2, AU- 12, AU-13, CA-7, CM- 10, CM-11	A.12.4.1, A.12.4.3	AN-TWA-001
	Security Con- tinuous Moni- toring (DE.CM)	DE.CM-4: Malicious code is detected.	SI-3, SI-8	A.12.2.1	SP-DEV-001
		DE.CM-5: Unauthorized mobile code is detected.	SC-18, SI-4, SC-44	A.12.5.1, A.12.6.2	SP-DEV-001
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is per- formed.	AU-12, CA- 7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	A.12.4.1, A.14.2.7, A.15.2.1	AN-TWA-001
	Detection Pro- cesses (DE.DP)	DE.DP-2: Detection ac- tivities comply with all applicable requirements.	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14	A.18.1.4, A.18.2.2, A.18.2.3	PR-CDA-001
RESPOND (RS)	Response Planning (RS.RP)	RS.RP-1: Response plan is executed during or af- ter an incident.	CP-2, CP-10, IR-4, IR-8	A.16.1.5	PR-CIR-001

	Cyberse	Standards &	Best Practices		
Function	rtion Category Subcategory		NIST SP 800- 53 R4	ISO/IEC 27001:2013	NIST SP 800- 181
	Communica- tions (RS.CO)	RS.CO-2: Incidents are reported consistent with established criteria.	AU-6, IR-6, IR-8	A.6.1.3, A.16.1.2	IN-FOR-002
		RS.AN-1: Notifications from detection systems are investigated.	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	A.12.4.1, A.12.4.3, A.16.1.5	PR-CDA-001
	Analysis (RS.AN)	RS.AN-2: The impact of the incident is under-stood.	CP-2, IR-4	A.16.1.4, A.16.1.6	PR-CIR-001
		RS.AN-3: Forensics are performed.	AU-7, IR-4	A.16.1.7	IN-FOR-002
		RS.AN-4: Incidents are categorized consistent with response plans.	CP-2, IR-4, IR-5, IR-8	A.16.1.4	PR-CIR-001
	Mitigation	RS.MI-1: Incidents are contained.	IR-4	A.12.2.1, A.16.1.5	PR-CIR-001
	(RS.MI)	RS.MI-2: Incidents are mitigated.	IR-4	A.12.2.1, A.16.1.5	PR-CIR-001

## 3.5 Technologies

Table 3-2 lists all of the technologies used in this project and provides a mapping among the generic application term, the specific product used, and the security control(s) the product provides. Refer to <u>Table 3-1</u> for an explanation of the NIST Cybersecurity Framework Subcategory codes.

Table 3-2 Products and Technologies

Component	Product	Function	Cybersecurity Frame- work Subcategories
Integrity Monitor- ing	Tripwire Enterprise v8.7 Semperis Directory Ser- vices Protector (DSP) v2.7	<ul> <li>Provides file hashes and integrity checks for files and software, regardless of file type.</li> <li>Provides integrity monitoring for data.</li> <li>Provides integrity monitoring for Active Directory.</li> </ul>	PR.DS-6, DE.AE-1, DE.CM-3, DE.CM-7
Event Detection	Cisco Advanced Malware Protection (AMP) v5.4	<ul> <li>Provides the ability to receive information about new threats.</li> </ul>	DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-5,
	Glasswall FileTrust ATP for Email v6.90.2.5 Cisco Stealthwatch v7.0.0	<ul> <li>Provides the ability to statically detect malicious soft- ware.</li> </ul>	DE.CM-7

Component	Product	Function	Cybersecurity Frame- work Subcategories
	Semperis DSP v2.7	<ul> <li>Provides ability to dynamically detect malicious software.</li> <li>Provides ability to detect malicious email attachments.</li> <li>Provides ability to scan the network for anomalies.</li> <li>Provides the ability to monitor user behavior for anomalies.</li> <li>Provides ability to scan email attachments for deviations from file type specifications or organizational policy.</li> </ul>	
Logging	Micro Focus ArcSight En- terprise Security Man- ager (ESM) v7.0 Patch 2	<ul> <li>Provides auditing and logging capabilities configurable to organizational policy.</li> <li>Correlates logs of cybersecurity events with user information.</li> <li>Provides automation for logging.</li> </ul>	DE.AE-1, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-3, DE.CM-7, RS.AN-2
	Tripwire Log Center v7.3.1		
Forensics/Analytics	Cisco AMP v5.4	<ul> <li>Provides forensics to track effects of malware retrospectively.</li> <li>Provides network traffic analysis.</li> <li>Provides ability to analyze files sent over the network.</li> <li>Provides analysis capabilities for finding anomalies in enterprise activity.</li> </ul>	DE.AE-2, DE.AE-4, DE.CM-1, RS.RP-1, RS.AN-1, RS.AN-2, RS.AN-3
	Symantec Security Ana- lytics v8.0.1		
	Micro Focus ArcSight ESM v7.0 Patch 2		
	Symantec Information Centric Analytics (ICA) v6.5.2		
	Cisco AMP v5.4		

Component	Product	Function	Cybersecurity Frame- work Subcategories
Mitigation and Containment	Cisco Identity Services Engine (ISE) v2.4	<ul> <li>Provides ability to sandbox files locally.</li> <li>Provides ability to enforce policy across the enterprise.</li> <li>Provides ability to quarantine devices across the enterprise.</li> </ul>	DE.CM-5, RS.RP-1, RS.MI-1, RS.MI-2
	Glasswall FileTrust ATP for Email v6.90.2.5		
	Semperis DSP v2.7	<ul> <li>Provides ability to sanitize files through file reconstruc- tion.</li> </ul>	
		<ul> <li>Provides ability to revert changes to domain services.</li> </ul>	
Reporting	Micro Focus ArcSight ESM v7.0 Patch 2	<ul> <li>Provides ability to send security alerts based on organi- zational policy.</li> </ul>	DE.AE-5, RS.RP-1, RS.CO-2
		• Provides ability to provide reports of enterprise health.	
		<ul> <li>Provides ability to provide reports of malware detection across the enterprise.</li> </ul>	

## **4** Architecture

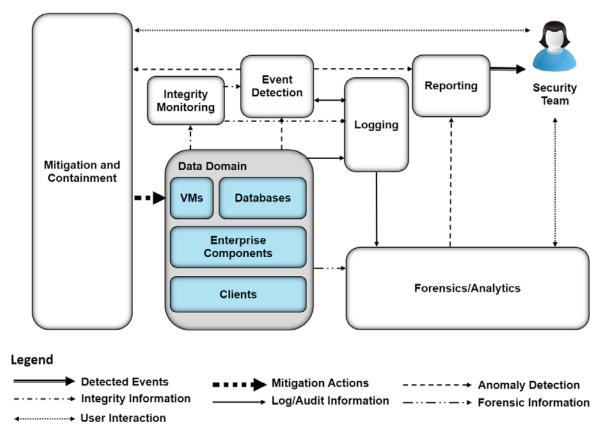
This section presents the high-level architecture used for implementation of a DI solution that detects and responds to ransomware and other destructive events.

## 4.1 Architecture Description

## 4.1.1 High-Level Architecture

The DI solution is designed to address the security Functions and Subcategories described in <u>Table 3-1</u> and is composed of the capabilities illustrated in Figure 4-1.

Figure 4-1 DI Detect & Respond High-Level Architecture



 Integrity monitoring provides capabilities for comparing current system states against established baselines.

- Event detection provides capabilities for detecting ongoing events and can be composed of intrusion detection, malware detection, user anomaly detection, and others, depending on the established threat model of the organization.
- Logging records and stores all the log files produced by components within the enterprise.
- **Forensics/analytics** provides the capability to probe/analyze logs and machines within the enterprise to learn from DI events.
- **Mitigation and containment** allows responding to DI events by containing and limiting the threat's ability to affect the system.
- **Reporting** provides the capability to report on all activities within the enterprise and within the reference architecture for analysis by a security team.

These capabilities work together to provide the Detect and Respond Functions for DI. The integrity monitoring capability collects integrity information prior to attacks so that when an attack happens, records of all file/system changes are preserved. In combination with event detection, these records not only function as a tool to inform recovery but also as early indicators of compromise. Event detection uses these records and its own mechanisms to actively detect events as they happen and to take appropriate action through other components of the reference architecture. Logging collects information from event detection and integrity monitoring for use in response functions. Mitigation and containment provides capabilities to stop ongoing attacks and limit their effect on the system. Forensics/analytics allow analysis of logs and threat behavior to aid the organization in learning from the attack. Reporting provides capabilities for reporting information from analysis and logging to the appropriate parties both during and after an attack. The information gained from these attacks can be used to inform products that fall in the Identify Function of the Cybersecurity Framework to indicate vulnerabilities in the enterprise that need to be remediated.

## 4.1.2 Architecture Components

## 4.1.2.1 Integrity Monitoring

The integrity monitoring component provides the ability to test, understand, and measure attacks that occur on files and components within the enterprise. When considering DI from the perspective of detecting and responding to an active attack, being able to track changes to files is critical. Asset integrity changes can provide an early detection mechanism by tracking changes made at abnormal times or by tracking users who typically do not make such changes. Furthermore, the changes tracked during a DI event can be used to inform the recovery process; they provide information about what changes happened, when changes began to take place, as well as what programs were involved in the changes.

Integrity monitoring typically requires an operation baseline to be taken prior to the start of a DI event—this baseline is used for comparison against the system's state during an attack.

For the integrity monitoring capability, we use a combination of two tools: Tripwire Enterprise and Semperis DSP. Once a baseline is taken prior to an attack, Tripwire Enterprise stores integrity information for selected data across all systems. When a "check" is run, Tripwire collects all the changes that occurred to monitored files on those systems. These changes are forwarded to the logging component, which can then report and alert on them, becoming an indicator of a DI event. Furthermore, these collected changes can be used to help remediate the effects of malware on a system.

Semperis DSP provides a similar function but with a focus on Active Directory. Changes to Active Directory users, groups, and other services are collected and can be used to notify administrators of potentially malicious activity. Given the sensitive nature of Active Directory, Semperis DSP does not rely on a single source of information but instead monitors multiple aspects of Active Directory. This helps ensure that any change to permissions or privileged credentials is captured, including changes that attackers attempt to hide (for example, by circumventing security auditing).

## 4.1.2.2 Event Detection

The event detection component provides the ability to detect events as they happen. This can be achieved through a combination of mechanisms, depending on the needs of the organization. Analysis of integrity monitoring logs can indicate malicious activity. Malware detection, behavior-based anomaly detection, and intrusion detection are all potential examples of event detection. The goal of this component is to detect events as they happen, to trigger the appropriate responses, and to provide information about the attack to the security team.

For the event detection capability, we use a combination of tools. Cisco AMP is used to detect malicious files. Glasswall FileTrust ATP for Email is used to identify malicious email attachments that do not conform to file standards and organizational policies. Cisco Stealthwatch is used to detect malicious network activity. Finally, Semperis DSP is used to detect changes in Active Directory. Information from these four can be correlated to identify malicious patterns of behavior from users.

### 4.1.2.3 Logging

Logging from each component serves several functions in an architecture that aims to detect and respond to active DI events. Logs are produced through integrity monitoring and event detection, which aid other components in responding to active events. Both mitigation and containment and forensics/analytics use logs to inform their actions—logs tell them what systems are being affected and what programs are causing the event. Further, these logs help decide what steps should be taken to remediate the attack and protect against it going forward.

For the logging capability, we use a combination of two tools: Micro Focus ArcSight and Tripwire Log Center. While Tripwire Log Center's purpose in this build is primarily to collect, transform, and forward logs from Tripwire Enterprise to ArcSight, ArcSight performs a wider function. ArcSight collects logs from various sources in the enterprise, such as event detection and integrity monitoring, as well as Windows event logs and Ubuntu syslogs. The goal of this widespread collection is to provide a base for the forensics/analytics component.

#### 4.1.2.4 Mitigation and Containment

The mitigation and containment component provides the ability to limit a destructive event's effect on the enterprise. This component may be able to interact with a security team for greater effectiveness and may have the option to provide automated response to certain DI events. This response can involve stopping execution of associated programs, disabling user accounts, disconnecting a system from the network, and more, depending on the threat. Other actions may involve removing software from a system, restarting services, or copying the threat to a safe environment for analysis.

For the mitigation and containment capability, we use a combination of tools. Cisco AMP provides the ability to remove malicious files on sight—combined with its event detection capability, this can be leveraged to immediately respond to malware on user systems. Cisco ISE provides quarantine functions that can be used to respond to detected malware and poor machine posture as well as to network events in Stealthwatch. Semperis DSP provides the ability to immediately and automatically revert detected changes in Active Directory, mitigating the use of backdoors and other malicious domain changes. Semperis DSP can also disable user accounts to prevent further changes from compromised or maliciously created accounts. Glasswall provides the ability to sanitize malicious or noncompliant email attachments before they ever reach the user's inbox, thereby eliminating malicious content in email attachments.

## 4.1.2.5 Forensics/Analytics

The forensics/analytics component uses the logs generated by event detection and the enterprise to discover the source and effects of the DI event and learn about how to prevent similar events in the future, if possible. This component will typically allow an organization to analyze malware or logs related to the malware's execution and produce information such as: the servers that the malware communicates with, or the executable's signature, to improve detection of the malware in the future. Furthermore, the ability to examine machines affected by malware for lasting effects may be desirable. The information gained from forensic analysis can also be used to enhance the organization's protections against malware and potentially reform policy in the organization.

For the forensics/analytics capability, we use a combination of tools. Cisco AMP provides the ability to review the history of malicious files to determine the source and movement across the enterprise. Symantec Security Analytics provides the ability to analyze network traffic in a similar manner. ArcSight ESM provides event correlation capabilities for logs collected from almost all the other capabilities, allowing processing of events before they are reported to the security team. Symantec ICA provides additional analysis capabilities for logs as well as aggregation and visualization of certain potentially

malicious movements within the enterprise. These products aid in the future prevention of such attacks as well as determine the scope of the event's effect on the system.

### 4.1.2.6 Reporting

The reporting component is primarily an interface between various components of the architecture and the security team. It allows alerting based on events through email and dashboards, depending on the organization's need. The reporting capabilities are best used throughout the entirety of an event—they can be used to alert the security team when an event starts as well as to provide regular status updates when events are not happening or have just finished.

For the reporting capability, we use Micro Focus ArcSight. ArcSight can send email alerts and generate reports based on the log correlation and analysis that it performs. By ensuring integration of as many relevant logs as possible with ArcSight's logging capabilities, we can use various indicators to trigger alerts when certain logs or sets of logs are received by ArcSight.

## **5** Security Characteristic Analysis

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of demonstrating a DI detect-and-respond solution. In addition, it seeks to understand the security benefits and drawbacks of the example solution.

### 5.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- 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 Build Testing

The purpose of the security characteristic analysis is to understand the extent to which the building block meets its objective of detecting and responding to DI events. Furthermore, the project aims to facilitate analysis of these events during and after an attack. In addition, it seeks to understand the security benefits and drawbacks of the reference design.

# 5.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to a Subcategory. The cited sections provide validation points that the example solution would be expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

Below are the scenarios created to test various aspects of this architecture. More detailed resolutions and mappings of these scenarios' requirements to the Cybersecurity Framework can be found in <u>Appendix D</u>.

# 5.3.1 Ransomware via Web Vector and Self-Propagation

## 5.3.1.1 Scenario

The following scenario was simulated to test the architecture's defense against ransomware.

A user mistakenly downloads ransomware from an external web server. When the user executes this malicious software, it generates a cryptographic key, which is sent back to the external web server. The malware then utilizes a privilege escalation exploit to propagate across the network. The malicious software encrypts files on the machines to which it propagated and demands payment in exchange for decryption of these files.

# 5.3.1.2 Resolution

The build provides a significant defense in depth against this use case.

The **event detection** capability provides the ability to detect malicious software on the system and generate logs and alerts based on this activity. It also allows for the detection of suspicious network behavior, such as propagation.

The **mitigation and containment** capability provides the ability to halt execution of the ransomware and remove it from the system. Furthermore, it allows quarantine of the affected machine(s) from the network after detection of malicious activity.

The **integrity monitoring** capability provides the ability to collect changes to files, including changes made by the ransomware as well as the ransomware's first creation or download onto the system.

When forwarded to the **logging** capability, these logs in combination with others can be used to identify the scope of the attack.

The **reporting** capability uses logs from the above capabilities to report on malicious activity and to increase response time.

The **forensics/analytics** capability analyzes logs related to the event to provide information that can be used to strengthen defenses against the attack in the future. This includes the websites it communicated with or was downloaded from, the signature of the executable, and the scope of the attack.

## 5.3.1.3 Other Considerations

Because malware comes in many forms, it is imperative to have multiple layers of defense against it while also working to actively improve these defenses. An early defense against malware means denylisting known malicious sites. However, because this must be done entirely before the attack takes place, it is out of scope of this build.

This build suggests a forensics/analytics capability specifically for informing and strengthening the enterprise's defenses against future attacks. This is a function of the Respond Category—learning from attacks can inform defense of such attacks in the future, both in the Protect and Detect phases of the attack. Denylisting is one such defense that can be informed by the Respond Category, and event detection is another.

## 5.3.2 Destructive Malware via USB Vector

#### 5.3.2.1 Scenario

The following scenario was simulated to test the architecture's defense against destructive malware.

A user finds an unmarked Universal Serial Bus (USB) device and inserts it into his or her system. The USB device contains malicious software that may run automatically or with user interaction. The malicious software modifies and deletes the user's files, removing text from text files and entirely deleting any media files it finds. The software does not offer a recovery mechanism as ransomware might, aiming only to corrupt files.

## 5.3.2.2 Resolution

The build provides several mechanisms to detect and mitigate this use case.

The **integrity monitoring** capability provides the ability to detect changes to the file system, allowing the changes and deletions to be detected and logged. Furthermore, information about what program (and by extension, where the program was located—that is, on a USB drive) is included in the logs.

The **logging** capability is used to collect logs from the integrity monitoring capability for posterity, as well as from Windows event logs to monitor usage of external drives in comparison to normal usage.

The **event detection** capability provides the ability to detect malicious files on the USB inserted into the system. It also can detect execution of these files.

The **mitigation and containment** capability provides the ability to stop malicious files from executing as well as delete the files on the USB drive.

## 5.3.2.3 Other Considerations

USB attacks do not always come in the form of disguised file-based malware. As USB attacks allow direct interfacing with the hardware of the system, they can aim to destroy the system via electrical attacks or involve impersonation of a keyboard or other devices to avoid detection and gain privileges. These attacks may be better mitigated through a thorough physical security policy and restrictions on the types of allowed connected devices. Advanced attacks that involve manipulation of hardware can become increasingly difficult to detect once plugged into the system. A prevention solution involving backups, physical security, and employee education is often more effective.

## 5.3.3 Accidental VM Deletion via Maintenance Script

#### 5.3.3.1 Scenario

The following scenario was simulated to test the architecture's defense against data integrity events that occur on virtual machines.

A routine maintenance script on the system causes an error. During a move operation in the Hyper-V system, the script deletes an important virtual machine (VM). A maintenance script with an error of this type could be a side effect of a normal system function or an error made by a member of the organization. It is expected that the build will mitigate the damage caused to virtual machines in such an incident.

## 5.3.3.2 Resolution

The build provides several methods for detecting and analyzing this use case. Errors in custom code are often difficult to detect at run time and because they are usually run by privileged programs. Classifying them as malware or even as "unintended" changes is often undesirable.

The **integrity monitoring** capability provides the ability to detect changes to VM configurations, allowing the VM deletion to be detected and logged. Furthermore, information about what program (i.e., the routine maintenance script) is included in the logs.

The logging capability provides the ability to collect these events for posterity.

The **forensics/analytics** capability provides the ability to analyze the events after the fact to enable the security team to understand the impact, resolve the error in the script, and inform the restoration process.

#### 5.3.3.3 Other Considerations

This solution will aid in identifying the script that causes a configuration change or deletion, but ultimately some things cannot be automated by the solution. Understanding the impact of the event requires a security team, and this build aims to provide the tools for a security team to do so.

Resolving an error in a maintenance script will also typically require effort on the part of the system administrators. Judgment on whether a script should be deleted, disabled, or left running during the remediation process is necessary and can depend on the size of the script, the affected assets, and the availability of resources to put toward resolving the error. Because of these considerations, the organization is left to decide whether a malfunctioning script should be treated like malware (see other scenarios that deal with malware) or as a part of the enterprise as it is possible that the remediation process is lengthy and exceeds the scope of the Detect/Respond Categories of the NIST Cybersecurity Framework.

# 5.3.4 Backdoor Creation via Email Vector

#### 5.3.4.1 Scenario

The following scenario was simulated to test the architecture's defense against malicious email attachments.

A user unknowingly opens a malicious attachment that was received in an email. When opened, the attachment quietly fetches files from an external web server. It then creates several unapproved backdoor accounts on the authentication server. It is expected that the build will mitigate the impacts of such an incident.

## 5.3.4.2 Resolution

The build provides several layers of defense against this use case. The **integrity monitoring** capability forwards logs of file changes and Active Directory changes to the logging capability, allowing recording and detection of both the malicious attachment's download and the changes it makes to the system account structure.

The **logging** and **reporting** capabilities provide the ability to generate alerts based on events for the security team to quickly take action to resolve them.

The **event detection** capability provides detection at two points in time—both before the attachment reaches the user's inbox and, should this fail, after the attachment downloads to the system.

The **mitigation and containment** capability provides mitigation before the attachment reaches the user's inbox, as well as when it is on the user's system.

The **forensics/analytics** capability provides the ability to view the network traffic generated by the attachment when fetching its malicious files from the web server. This can inform defense of the enterprise in the Protect Category of the Cybersecurity Framework before any similar events happen in the future.

## 5.3.4.3 Other Considerations

Another defense that can partially prevent this use case is detection of the email as spam. However, as this is often a function of the email provider and not a separate security solution, it is out of scope for this build.

This build suggests a forensics/analytics capability specifically for informing and strengthening the defenses of the enterprise against future attacks. This is a function of the Respond Category—learning from attacks can inform the defense of such attacks in the future, both in the Protect and Detect phases of the attack.

## 5.3.5 Database Modification via Malicious Insider

#### 5.3.5.1 Scenario

The following scenario was simulated to test the architecture's defense against unwanted database modification.

A malicious insider has access to an enterprise database through a web page. The insider leverages a vulnerability in the web page to delete a large portion of the database. Though this scenario deals with a web vulnerability, other vulnerabilities could be used to modify the database undesirably. It is expected that the build will mitigate the impact that a user can have on the database.

#### 5.3.5.2 Resolution

The build provides several layers of defense against this use case. The **integrity monitoring** capability is used to detect changes to the database.

These changes are forwarded to the **logging** capability, which also collects information about web requests.

The **reporting** capability provides the ability to generate alerts and quickly inform the security team of an anomaly, based on the logs.

The **forensics/analytics** capability is used to investigate the malicious access as well as identify the page with the vulnerability. Because this vulnerability is a vulnerability in custom code, it is important for information-gathering mechanisms to be in place to provide ample information for the resolution of this vulnerability.

#### 5.3.5.3 Other Considerations

This use case highlights the need for a response-oriented build to collaborate with an identify-oriented build. Identification and resolution of vulnerabilities in custom code are sometimes feasible only through gathering information after the vulnerability has been exploited. This build provides the mechanisms to gather such information, but it is ultimately up to the security team to resolve the vulnerability and learn from the attack.

# 5.3.6 File Modification via Malicious Insider

#### 5.3.6.1 Scenario

The following scenario was simulated to test the architecture's defense against malicious file and backup modification.

A malicious insider is assumed to have stolen administrator-level credentials through non-technical means. The insider, using these credentials, uses remote Windows PowerShell sessions to uniformly modify employee stock information to their benefit across several machines. This attack will also target the enterprise's backup system to modify all records of the previous stock information. It is expected that the aspects of the build described above will mitigate the ability of the user to target and modify enterprise data and backups. The method of securing administrator credentials will be considered out of scope for this solution.

## 5.3.6.2 Resolution

The build has several layers of defense against this use case. The **integrity monitoring** capability detects changes to files and backups caused by a malicious insider.

When forwarded to the **logging** and **reporting** capabilities, the build can report on these changes. Irregularities or differences from the normal backup schedule are important indicators of a compromise.

When the security team is alerted to a malicious insider, they can use the **mitigation and containment** capability to disable the insider's access.

#### 5.3.6.3 Other Considerations

Malicious insiders are powerful adversaries, because they already have some level of access to the system. The existence of malicious insiders widens the threat surface of an enterprise to needing defense against internal machines as well as external machines. For this reason, this build includes mitigations against threats already present inside the enterprise and not just threats that originate externally. This includes the ability to disable user accounts, quarantine machines, and monitor network traffic originating from within the enterprise.

# 5.3.7 Backdoor Creation via Compromised Update Server

#### 5.3.7.1 Scenario

The following scenario was simulated to test the architecture's defense against compromised update servers.

An update server that services an enterprise machine is compromised and provides an update to the enterprise machine that contains a backdoor. The update contains a vulnerable version of vsftpd, allowing an attacker root access into the machine updated by the compromised server. It is expected that the build will mitigate the impact of a compromised update server.

## 5.3.7.2 Resolution

The build has several layers of defense against this use case. **Integrity monitoring** detects changes to programs, providing information about how and when the program was changed. It also detects changes to any files made by an intruder.

The **event detection** capability is used to detect the malicious update through signature detection. Furthermore, it detects the connection to the open port by an attacker.

The **mitigation and containment** capability is used to delete/quarantine the malicious update, stopping the port from being accessible. It can also be used to quarantine the machine from the network, to prevent the spread of the intrusion and remove the attacker's access.

## 5.3.7.3 Other Considerations

The use of the event detection capability to detect largely assumes that the update has been reported as vulnerable, either through a well-known history of being vulnerable or through intelligence-sharing channels. As such, an event detection capability would, in some cases of new custom attacks, be unable to detect this at first sight. However, the build provides other tools, such as monitoring network activity, that can alert security staff to such attacks.

Using a data integrity identify-and-protect build to incorporate denylisting and network protection as part of the defense is beneficial, as a use case that involves connecting to an unused port would be entirely defeated by a network protection allowlist of approved ports.

# 6 Future Build Considerations

The NCCoE is creating an overarching guide to combining the architectures of the various DI projects: Identify and Protect, Detect and Respond, and Recover. These architectures share some commonalities, such as integrity monitoring, as well as some potential integrations and cycles that could not be expressed in just one of the practice guides. The different Functions of the Cybersecurity Framework are intended to prepare and inform one another, and the overarching guide addresses those issues. The NCCoE is also considering additional data security projects that map to the Cybersecurity Framework Core Functions of Identify, Protect, Detect, Respond, and Recover. These projects will focus on data confidentiality—the defense of enterprise systems from attacks that would compromise the secrecy of data.

# Appendix A List of Acronyms

АМР	Advanced Malware Protection		
АТР	Advanced Threat Protection		
COI	Community of Interest		
DE	Detect		
DI	Data Integrity		
DSP	Directory Services Protector		
ESM	Enterprise Security Manager		
ICA	Information Centric Analytics		
ISE	Identity Services Engine		
т	Information Technology		
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission		
NCCoE	National Cybersecurity Center of Excellence		
NIST	National Institute of Standards and Technology		
NISTIR	NIST Interagency or Internal Report		
PR	Protect		
RMF	Risk Management Framework		
RS	Respond		
SP	Special Publication		
USB	Universal Serial Bus		
VM	Virtual Machine		
vsftpd	Very Secure File Transfer Protocol Daemon		

# 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; CNSSI-4009
Architecture	A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution, while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability).
	SOURCE: FIPS 201-2
Audit	Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.
	SOURCE: CNSSI 4009-2015
Backdoor	An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.
	SOURCE: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 2
Backup	A copy of files and programs made to facilitate recovery if necessary.
	SOURCE: NIST SP 800-34 Rev. 1
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
	SOURCE: NIST SP 800-32

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-26.

Continuous	Maintaining ongoing awareness to support organizational risk decisions.		
Monitoring	SOURCE: NIST SP 800-137		
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.		
	SOURCE: CNSSI 4009-2015 (NSPD-54/HSPD-23)		
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted.		
	SOURCE: CNSSI-4009		
Data Integrity	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.		
	SOURCE: CNSSI-4009		
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.		
	SOURCE: FIPS 199 (44 U.S.C., Sec. 3542)		
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.		
	SOURCE: CNSSI 4009-2015 (NIST SP 800-30 Rev. 1)		
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.		
	SOURCE: FIPS 200 (44 U.S.C., Sec. 3502)		
Insider	An entity inside the security perimeter that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.		

	SOURCE: NIST SP 800-82 Rev. 2 (RFC 4949)
Kerberos	An authentication system developed at the Massachusetts Institute of Technology (MIT). Kerberos is designed to enable two parties to exchange private information across a public network.
	SOURCE: NIST SP 800-47
Log	A record of the events occurring within an organization's systems and networks.
	SOURCE: NIST SP 800-92
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.
	SOURCE: NIST SP 800-111
Privacy	Assurance that the confidentiality of, and access to, certain information about an entity is protected.
	SOURCE: NIST SP 800-130
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
Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.
	SOURCE: NIST SP 800-63-2
Risk Management Framework	The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.
	SOURCE: NIST SP 800-82 Rev. 2 (NIST SP 800-37)

Security Control	A protection measure for a system.
	SOURCE: NIST SP 800-123
Virtual Machine	Software that allows a single host to run one or more guest operating systems.
Machine	SOURCE: NIST SP 800-115
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 (adapted from CNSSI 4009)

# Appendix C References

- [1] A. Sedgewick, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, National Institute of Standards and Technology, Gaithersburg, Maryland, Apr. 2018, 55 pp. Available: <u>https://www.nist.gov/cyberframework/framework</u>.
- [2] L. Kauffman, N. Lesser and B. Abe, *Executive Technical Workshop on Improving Cybersecurity* and Consumer Privacy, NISTIR 8050, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2015, 155pp. Availabe: <u>https://nccoe.nist.gov/sites/default/files/library/nistir-8050-draft.pdf</u>
- [3] G. Stoneburner, et al., Guide for Conducting Risk Assessments, NIST Special Publication (SP), 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 95 pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-30r1</u>.
- [4] R. Ross, et al., Guide for Applying the Risk Management Framework to Federal Information Systems, NIST Special Publication (SP) 800-37, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2010, 101pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-37r1</u>.
- [5] R. Ross et al., Managing Information Security Risk, NIST Special Publication (SP) 800-39, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2011, 87pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-39</u>.
- [6] M. Souppaya *et al., Guide to Enterprise Patch Management Technologies*, NIST Special Publication (SP) 800-40 Revision 3, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013, 25pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-40r3</u>.
- [7] R. Ross *et al.*, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013, 461pp. Available: <u>https://doi.org/10.6028/NIST.SP.800-53r4</u>.
- [8] U.S. Department of Commerce. Security Requirements for Cryptographic Modules, Federal Information Processing Standards (FIPS) Publication 140-3, Mar. 2019, 65pp. Available: <u>https://csrc.nist.gov/publications/detail/fips/140/3/final</u>.
- K. Kent *et al., Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication (SP) 800-86, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2006, 121pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-86</u>.

34

- K. Kent and M. Souppaya, *Guide to Computer Security Log Management*, NIST Special Publication (SP) 800-92, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2006, 72pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-92</u>.
- P. Bowen et al., Information Security Handbook: A Guide for Managers, NIST Special Publication (SP) 800-100, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2006, 178pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-100</u>.
- M. Swanson *et al., Contingency Planning Guide for Federal Information Systems*, NIST Special Publication (SP) 800-34 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2010, 148pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-34r1</u>.
- [13] Office of Management and Budget (OMB), Management of Federal Information Resources, OMB Circular No. A-130, November 2000. Available: <u>https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a13</u> <u>Orevised.pdf</u>.
- P. Cichonski *et al., Computer Security Incident Handling Guide*, NIST Special Publication (SP) 800-61 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2012, 79pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-61r2</u>.
- [15] M. Souppaya and K. Scarfone, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, NIST Special Publication (SP) 800-83 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013, 46pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-83r1</u>.
- [16] C. Johnson *et al., Guide to Cyber Threat Information Sharing*, NIST Special Publication (SP) 800-150, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2016, 42pp. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-150</u>.
- [17] M. Bartock et al., Guide for Cybersecurity Event Recovery, NIST Special Publication (SP) 800-184, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2016, 52pp. <u>http://dx.doi.org/10.6028/NIST.SP.800-184</u>.

# Appendix D Functional Evaluation

A functional evaluation of the data integrity (DI) example implementation, as constructed in our laboratory, was conducted to verify that it meets its objective of detecting and responding to DI events. Furthermore, this project aims to analyze the events to aid recovery and protection of the enterprise against future attacks. The evaluation verified that the example implementation could perform the following functions:

- Detect malicious network activity, malicious mobile code, malicious code execution, and unauthorized user behavior.
- Contain and analyze these types of incidents.
- Mitigate the impact of these incidents as they occur.
- Report relevant details for use in mitigation and protection against future events.

Section D.1 describes the format and components of the functional test cases. Each functional test case is designed to assess the capability of the example implementation to perform the functions listed above and detailed in Section D.1.

# D.1 Data Integrity Functional Test Plan

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to that Subcategory. The cited sections provide validation points that the example solution is expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

This plan includes the test cases necessary to conduct the functional evaluation of the DI example implementation, which is currently deployed in a lab at the National Cybersecurity Center of Excellence. The implementation tested is described in <u>Section 4</u>.

Each test case consists of multiple fields that collectively identify the goal of the test, the specifics required to implement the test, and how to assess the results of the test. Table 6-1 describes each field in the test case.

Table 6-1 Test Case Fields

Test Case Field	Description
Parent requirement	Identifies the top-level requirement or the series of top-level require- ments leading to the testable requirement.

Test Case Field	Description	
Testable requirement	Drives the definition of the remainder of the test case fields. Specifies the capability to be evaluated.	
Description	Describes the objective of the test case.	
Associated Cybersecu- rity Framework Subcate- gories	Lists the National Institute of Standards and Technology Special Publica- tion 800-53 rev 4 controls addressed by the test case.	
Preconditions	The starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content.	
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure.	
Expected results	The expected results for each variation in the test procedure.	
Actual results	The observed results.	
Overall result	The overall result of the test as pass/fail. In some test-case instances, the determination of the overall result may be more involved, such as determining pass/fail based on a percentage of errors identified.	

# D.2 Data Integrity Use Case Requirements

Table 6-2 identifies the DI functional requirements addressed in the test plan and associated test cases.

#### Table 6-2 Capability Requirements

Capability Re- quirement (CR) ID	Parent Requirement	Sub Requirement 1	Test Case
CR 1	The DI example imple- mentation shall detect and respond to malware that encrypts files and displays notice demand- ing payment.		Data Integrity DR-1
CR 1.a		File integrity changes are col- lected and logged.	Data Integrity DR-1
CR 1.b		Access is halted.	Data Integrity DR-1

Capability Re- quirement (CR) ID	Parent Requirement	Sub Requirement 1	Test Case
CR 1.c		Executable is identi- fied as malicious, using a denylist.	Data Integrity DR-1
CR 1.d		Executable is identi- fied as malicious through analysis, and denylist is up- dated.	Data Integrity DR-1
CR 1.e		Execution is halted.	Data Integrity DR-1
CR 1.f		Downloads are identified as mali- cious, using a denyl- ist.	Data Integrity DR-1
CR 1.g		Downloads are identified as mali- cious through analy- sis, and denylist is updated.	Data Integrity DR-1
CR 1.h		Downloads are pre- vented.	Data Integrity DR-1
CR 1.i		Attempts to propa- gate are detected.	Data Integrity DR-1
CR 1.j		Machines attempt- ing to propagate are prevented from propagating.	Data Integrity DR-1
CR 1.k		Suspicious network traffic is detected, and denylist is up- dated.	Data Integrity DR-1

Capability Re- quirement (CR) ID	Parent Requirement	Sub Requirement 1	Test Case
CR 2	The DI example imple- mentation shall detect and respond to malware inserted via Universal Serial Bus (USB) that modifies and deletes user data.		Data Integrity DR-2
CR 2.a		File integrity changes are col- lected and logged.	Data Integrity DR-2
CR 2.b		The insertion of a USB device is de- tected and logged.	Data Integrity DR-2
CR 2.c		The executable is identified as mali- cious, using a denyl- ist.	Data Integrity DR-2
CR 2.d		The executable is identified as mali- cious through analy- sis, and the denylist is updated.	Data Integrity DR-2
CR 2.e		Malicious executa- ble is halted or de- leted.	Data Integrity DR-2
CR 3	The DI example imple- mentation shall detect and respond to virtual machine deletion.		Data Integrity DR-3
CR 3.a		Virtual machine in- tegrity changes are collected and logged.	Data Integrity DR-3

Capability Re- quirement (CR) ID	Parent Requirement	Sub Requirement 1	Test Case
CR 3.b		The event causing deletion of the vir- tual machine is ana- lyzed.	Data Integrity DR-3
CR 4	The DI example imple- mentation shall detect and respond to malware received via phishing email.		Data Integrity DR-4
CR 4.a		Configuration integ- rity changes are col- lected and logged.	Data Integrity DR-4
CR 4.b		Email is identified as malicious, using a denylist.	Data Integrity DR-4
CR 4.c		Email is identified as malicious through analysis, and the denylist is updated.	Data Integrity DR-4
CR 4.d		Email is deleted or sorted into spam.	Data Integrity DR-4
CR 4.e		The attachment is identified as mali- cious, using a denyl- ist.	Data Integrity DR-4
CR 4.f		The attachment is identified as mali- cious through analy- sis, and the denylist is updated.	Data Integrity DR-4
CR 4.g		Execution of the spreadsheet is stopped, and the denylist is updated if necessary.	Data Integrity DR-4

Capability Re- quirement (CR) ID	Parent Requirement	Sub Requirement 1	Test Case
CR 4.h		The downloads are identified as mali- cious, using a denyl- ist.	Data Integrity DR-4
CR 4.i		The downloads are identified as mali- cious through analy- sis, and the denylist is updated.	Data Integrity DR-4
CR 4.j		The malicious exe- cutable is halted or deleted.	Data Integrity DR-4
CR 4.k		Suspicious network traffic is detected, and denylist is up- dated.	Data Integrity DR-4
CR 5	The DI example imple- mentation shall detect and respond to changes to the database made through a web server vulnerability in custom code.		Data Integrity DR-5
CR 5.a		Database integrity changes are col- lected and logged.	Data Integrity DR-5
CR 5.b		Information about the client interact- ing with the web service is collected and logged.	Data Integrity DR-5
CR 5.c		Information from the attack is re- ported for use in protection against future events.	Data Integrity DR-5

Capability Re- quirement (CR) ID	Parent Requirement	Sub Requirement 1	Test Case
CR 6	The DI example imple- mentation shall detect and respond to targeted modification by mali- cious insiders with ele- vated privileges.		Data Integrity DR-6
CR 6.a		File integrity changes are col- lected and logged.	Data Integrity DR-6
CR 6.b		Backup integrity changes are col- lected and logged.	Data Integrity DR-6
CR 6.c		Detected changes are reported.	Data Integrity DR-6
CR 6.d		Associated user ac- counts are con- tained.	Data Integrity DR-6
CR 7	The DI example imple- mentation shall detect and respond to an intru- sion via compromised update server.		Data Integrity DR-7
CR 7.a		Program integrity changes are col- lected and logged.	Data Integrity DR-7
CR 7.b		The downloaded service is identified as malicious, using a denylist.	Data Integrity DR-7
CR 7.c		The downloaded service is identified as malicious through analysis, and the denylist is updated.	Data Integrity DR-7

Capability Re- quirement (CR) ID	Parent Requirement	Sub Requirement 1	Test Case
CR 7.d		The service is halted and reverted or de- leted.	Data Integrity DR-7
CR 7.e		The download site is temporarily added to the denylist.	Data Integrity DR-7
CR 7.f		The port opened by the service is de-tected.	Data Integrity DR-7
CR 7.g		The opened port is closed.	Data Integrity DR-7
CR 7.h		The intrusion into the infected ma- chine is detected.	Data Integrity DR-7
CR 7.i		The intrusion into the infected ma- chine is contained.	Data Integrity DR-7

# D.3 Test Case: Data Integrity DR-1

Table 6-3 Test Case ID: Data Integrity DR-1

Parent requirement	(CR 1) The DI example implementation shall detect and respond to malware that encrypts files and displays notice demanding payment.
Testable requirement	(CR 1.a) Integrity Monitoring, Logging, Reporting, (CR 1.c, CR 1.d, CR 1.f, CR 1.g, CR 1.i) Event Detection, (CR 1.b, CR 1.e, CR 1.j) Mitigation and Containment, (CR 1.h, CR 1.k) Forensics and Analytics
Description	Show that the DI solution has capabilities to detect behaviors typical of ransomware, and mitigate these behaviors appropriately.
Associated Cybersecurity Framework Subcategories	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2,DE.CM-4, DE.CM-7, DE.DP-2, DE.AE-1, DE.CM-1
Preconditions	User navigates to a malicious website and clicks on an ad for a virus cleaner. The virus cleaner is ransomware, which propagates across the domain and encrypts user files.
Procedure	<ul> <li>The integrity monitoring capability is used to monitor and log changes to the integrity of files.</li> <li>The logging capability and the reporting capability are used to notify the security team of changes to the integrity of files and of potentially malicious events.</li> <li>The event detection capability is used to detect the ransomware in real time before or during its execution. It is also used to detect propagation of the ransomware.</li> <li>The mitigation and containment capability is used to halt the ransomware's execution and delete it from the system. It is also used to quarantine affected machines once a breach is discovered.</li> <li>The forensics/analytics capability is used to discover malicious hosts and websites accessed by the ransomware.</li> </ul>
Expected Results (pass)	The build can monitor and report changes to the integrity of files (CR 1.a). The machine is quarantined when malware is detected (CR 1.b).

	Malicious executables are identified through signature detection or analysis (CR 1.c, CR 1.d).
	Malicious executables are prevented from executing (CR 1.e).
	Malicious downloads are identified through signature detection or analysis (CR 1.f, CR 1.g).
	Malicious downloads are prevented (CR 1.h).
	Propagation of malicious executables is detected (CR 1.i).
	Propagation of malicious executables is prevented (CR 1.j).
	Network traffic is captured and analyzed for suspicious activity (CR 1.k).
Actual Results	<b>Tripwire Enterprise (integrity monitoring)</b> is used to successfully detect changes to files on the affected systems.
	<b>ArcSight ESM (logging)</b> is used to successfully log events from event detection and integrity monitoring for use in reporting and forensics/analytics.
	<b>ArcSight ESM (reporting)</b> is used to successfully report on malicious activity detected in logs.
	<b>Cisco AMP (event detection)</b> is used to successfully detect the malicious executable.
	<b>Cisco AMP (mitigation and containment)</b> is used to successfully remove malicious executables from the affected systems.
	<b>Cisco Stealthwatch (event detection)</b> is used to successfully capture malicious or suspicious network traffic from the executable.
	<b>Cisco ISE (mitigation and containment)</b> is used to successfully quarantine affected machines.
	<b>Symantec Security Analytics (forensics/analytics)</b> is used to successfully review network traffic generated by the ransomware for potentially malicious hosts and websites.

	<b>Symantec ICA (forensics/analytics)</b> successfully displays relevant events from ArcSight for analysis to aid in identifying the malicious files for use in future event detection as well as for removal by the security team.
Overall Result	Pass. All requirements for this use case are met.

# D.4 Test Case: Data Integrity DR-2

Table 6-4 Test Case ID: Data Integrity DR-2

Parent requirement	(CR 2) The DI example implementation shall detect and respond to malware inserted via USB that modifies and deletes user data.
Testable requirement	(CR 2.a) Integrity Monitoring, (CR 2.b, CR 2.c) Event Detection, (CR 2.d) Forensics and Analytics, (CR 2.e) Mitigation and Containment
Description	Show that the DI solution can detect behaviors of destructive malware and can mitigate these behaviors appropriately.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-4, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	A user inserts an unidentified USB drive into their computer. They click on a file on the drive, which immediately destroys any files on their machine.
Procedure	The <b>integrity monitoring</b> capability is used to monitor integrity changes to the system. The <b>logging</b> capability is used to collect logs from the integrity monitoring capability. The <b>event detection</b> capability is used to detect malicious files on the USB inserted into the system. The <b>mitigation and containment</b> capability is used to prevent malicious files from executing.
Expected Results (pass)	The build can monitor and report changes to the integrity of files (CR 2.a). The build can detect insertion of a USB (CR 2.b). Malicious executables are identified through signature detection or analysis (CR 2.c, CR 2.d).

	Malicious executables are prevented from executing (CR 2.e).
Actual Results	<b>Tripwire Enterprise (integrity monitoring)</b> successfully detects changes made by an executable running from a USB.
	<b>ArcSight ESM (logging)</b> successfully collects logs from the integrity monitoring capability. Furthermore, USB insertions can be collected by using Windows group policy.
	<b>Cisco AMP (event detection)</b> successfully detects malicious files on the USB drive.
	<b>Cisco AMP (mitigation and containment)</b> immediately deletes these malicious files on the system if they are copied. It also prevents execution if the file is run from the USB drive.
Overall Result	Pass (partial). Cisco AMP does not immediately delete the file from the USB drive when it is plugged in if the user does not make any action (copy or execution). However, because both these actions trigger deletion, this is not a significant shortcoming as the file is otherwise harmless.

# D.5 Test Case: Data Integrity DR-3

Table 6-5 Test Case ID: Data Integrity DR-3

Parent requirement	(CR 3) The DI example implementation shall detect and respond to virtual machine deletion.
Testable requirement	(CR 3.a) Integrity Monitoring, (CR 3.b) Forensics and Analytics
Description	Show that the DI solution can detect and analyze DI events that involve virtual machines.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	A routine maintenance script contains an error that accidentally deletes a virtual machine.
Procedure	The <b>integrity monitoring</b> capability is used to monitor integrity changes to the system.
	The <b>logging</b> capability is used to collect logs from the integrity monitoring capability.

	The forensics/analytics capability is used to analyze logs and
	determine the cause of integrity events.
	<b>C</b> ,
Expected Results (pass)	The build can monitor and report changes to the integrity of virtual machines (CR 3.a).
	The build can analyze the impact of DI events (CR 3.b).
Actual Results	Tripwire Enterprise (integrity monitoring) successfully monitors and
	logs changes to configurations of virtual machines.
	<b>ArcSight ESM (logging)</b> successfully collects logs and reports on the events generated by the integrity monitoring capability, enabling faster response time.
	<b>Symantec ICA (forensics/analytics)</b> successfully displays relevant events from ArcSight for analysis to aid in identifying the file that causes the deletion.
Overall Result	Pass. All requirements for this use case are met.

# D.6 Test Case: Data Integrity DR-4

Table 6-6 Test Case ID: Data Integrity DR-4

Parent requirement	(CR 4) The DI example implementation shall detect and respond to malware received via phishing email.
Testable requirement	(CR 4.a) Integrity Monitoring and Logging, (CR 4.b, CR4.e, CR 4.h, CR 4.k) Event Detection, (CR 4.c, CR 4.f, CR 4.i) Forensics and Analytics, (CR 4.d, CR 4.g, CR 4.j) Mitigation and Containment
Description	Show that the DI solution can detect malicious attachments and respond to malicious configuration changes.
Associated Cybersecurity Framework Subcategories	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	The user receives a phishing email with a malicious spreadsheet attached. The spreadsheet is downloaded and opened, causing account changes in Active Directory.
Procedure	The <b>integrity monitoring</b> capability is used to detect and log the account creation.

	This information is forwarded to the <b>logging</b> capability, along with other available Active Directory information.
	The email attachment is detected as malicious by the <b>event</b> <b>detection</b> capability and mitigated by the <b>mitigation and</b> <b>containment</b> capability, both when the file is in the inbox and when it is on the user's system.
	The solution can review the network traffic generated by the file when it calls out to the malicious web server to download files through <b>forensics/analytics</b> .
Expected Results (pass)	The build can monitor and report changes to the integrity of configurations (CR 4.a).
	Malicious emails are identified through signature detection or analysis (CR 4.b, CR 4.c).
	Emails identified as malicious are sorted into spam or deleted (CR 4.d).
	Malicious attachments are identified through signature detection or analysis (CR 4.e, CR 4.f).
	Malicious attachments are prevented from executing (CR 4.g).
	Malicious downloads are identified through signature detection or analysis (CR 4.h, CR 4.i).
	Malicious executables are prevented from executing (CR 4.j). Network traffic is captured and analyzed for suspicious activity (CR 4.k).
Actual Results	Semperis DSP (integrity monitoring) successfully monitors and logs changes to Active Directory.
	<b>ArcSight ESM (logging)</b> successfully collects logs and reports on the events generated by the integrity monitoring capability, enabling faster response time.
	<b>Glasswall FileTrust (event detection)</b> successfully identifies the malicious attachment before it reaches the user's inbox.

	Glasswall FileTrust (mitigation and containment) successfully mitigates the malicious attachment before it reaches the user's inbox.
	The malicious file is successfully uploaded to <b>Cisco AMP (event</b> detection) for signature detection.
	<b>Cisco AMP (event detection)</b> successfully mitigates the file when found on user workstations.
	Symantec Security Analytics (forensics/analytics) is used to successfully detect network traffic involving download of files from the malicious server.
Overall Result	Pass (partial). Emails are not sorted into spam (CR 4.b–d); rather, the attachment is mitigated before reaching the user's inbox. Sorting emails into spam is often a function of the email infrastructure.

# D.7 Test Case: Data Integrity DR-5

Table 6-7 Test Case ID: Data Integrity DR-5

Parent requirement	(CR 5) The DI example implementation shall detect and respond to changes to the database made through a web server vulnerability in custom code.
Testable requirement	(CR 5.a) Integrity Monitoring, (CR 5.b) Logging, (CR 5.c) Reporting
Description	Show that the DI solution can detect and respond to an exploitation a vulnerability in custom code that leads to an attack on the database.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	A vulnerability in the source code of an intranet web page is discovered by a malicious insider. The insider exploits this vulnerability to delete significant portions of the database.
Procedure	The <b>integrity monitoring</b> capability is used to detect changes to the database.
	The <b>logging</b> capability is used to monitor changes to the database and to log web requests.

	The <b>reporting</b> capability is used to alert the security team of
	significant changes to the database.
	The forensics/analytics capability is used to investigate the
	malicious access as well as identify the page with the vulnerability.
Expected Results (pass)	The build can monitor and report changes to the integrity of the database (CR 5.a).
	Malicious interaction with the web server is detected (CR 5.b).
	Information about the attack is reported for use in maintaining the enterprise systems (CR 5.c).
Actual Results	<b>Tripwire Enterprise (integrity monitoring)</b> successfully monitors changes to the database configuration.
	ArcSight ESM (logging) successfully logs changes to the database and web requests.
	ArcSight ESM (reporting) successfully alerts the security team of changes to the database.
	Symantec Security Analytics (forensics/analytics) allows
	identification of web requests that could have caused the deletion,
	helping identify the web server's vulnerability in custom code.
Overall Result	Pass. All requirements for this use case are met.

# D.8 Test Case: Data Integrity DR-6

Table 6-8 Test Case ID: Data Integrity DR-6

Parent requirement	(CR 6) The DI example implementation shall detect and respond to targeted modification by malicious insiders with elevated privileges.
Testable requirement	(CR 6.a, 6.b) Integrity monitoring, (CR 6.c) Reporting, (CR 6.d) Mitigation and Containment
Description	Show that the DI solution can detect and respond to targeted modification of assets and backups by malicious insiders.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2

Preconditions	A malicious insider attempts to modify targeted information in both the enterprise systems and the backup systems by using elevated credentials obtained extraneously.
Procedure	The <b>integrity monitoring</b> capability is used to detect changes to the file system.
	The <b>reporting</b> capability is used to notify the security team of changes to critical data assets.
	The <b>mitigation and containment</b> capability is used to prevent the malicious user from making further modifications.
Expected Results (pass)	The build can monitor and report changes to the integrity of files and backups (CR 6.a, CR 6.b).
	Information about the attack is reported for use in responding to the threat (CR 6.c).
	User accounts associated with the attack are contained (CR 6.d).
Actual Results	<b>Tripwire Enterprise (integrity monitoring)</b> successfully detects changes to files and backups caused by a malicious insider.
	ArcSight ESM (reporting) successfully reports and alerts administrators via email on changes made to files by a malicious insider.
	Semperis DSP (mitigation and containment) successfully disables the user accounts associated with malicious insider activity.
Overall Result	Pass. All requirements for this use case are met.

# D.9 Test Case: Data Integrity DR-7

Table 6-9 Test Case ID: Data Integrity DR-7

Parent requirement	(CR 7) The DI example implementation shall detect and respond to an intrusion via compromised update server.
Testable requirement	(CR 7.a) Integrity Monitoring, (CR 7.b) Event Detection, (CR 7.c) Forensics and Analytics, (CR 7.d, CR 7.e) Mitigation and Containment
Description	Show that the DI solution can detect a malicious update from a compromised update server as well as detect and respond to a resulting intrusion.

Associated Cybersecurity Framework Subcategories	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2, DE.CM-4, DE.CM-7, DE.AE-1, DE.CM-1,
Preconditions	An external update server has been compromised, and a user workstation attempts to update from this server.
Procedure	The <b>integrity monitoring</b> capability is used to detect changes to the integrity of programs and files. The <b>event detection</b> capability is used to detect the malicious
	update. It is also used to detect the connection to the machine.
	The <b>mitigation and containment</b> capability is used to halt execution of the update and delete it. It is also used to contain the intrusion.
Expected Results (pass)	The build can monitor and report changes to the integrity of programs (CR 7.a).
	The malicious update is identified through signature detection or analysis (CR 7.b, CR 7.c).
	The malicious service is halted and reverted or deleted (CR 7.d).
	Other users are temporarily prevented from accessing this update server (CR 7.e).
	The port opened by the service is detected (CR 7.f).
	The port opened by the service is closed (CR 7.g).
	The intrusion is detected (CR 7.h).
	The intrusion is contained (CR 7.i).
Actual Results	<b>Tripwire Enterprise (integrity monitoring)</b> is used to identify changes in programs on the system as well as any changes made by the attacker.
	<b>Cisco AMP (event detection)</b> is used to detect the malicious update.
	<b>Cisco Stealthwatch (event detection)</b> is used to detect a connection to the machine via an unusual port.

	<b>Cisco AMP (mitigation and containment)</b> is used to halt the execution of the file and delete it, thereby closing the vulnerable port.
	<b>Cisco ISE (mitigation and containment)</b> is used to disconnect the affected machines from the network to prevent the spread of the intrusion.
Overall Result	Pass (partial). Cisco AMP does not seem to support network blocking for Unix machines at the time this practice guide was written—it supports only detection (it does support network blocking for Windows use cases, though, so a similar use case on Windows machines would potentially work). Instead, we rely on network protection, a DI Protect capability, to prevent further access to the update server; and on Cisco AMP's mitigation capabilities to remedy any known malicious files downloaded from the server.

# **NIST SPECIAL PUBLICATION 1800-26C**

# Data Integrity:

Detecting and Responding to Ransomware and Other Destructive Events

Volume C: How-To Guides

#### **Jennifer Cawthra**

National Cybersecurity Center of Excellence NIST

#### Michael Ekstrom Lauren Lusty Julian Sexton

#### John Sweetnam

The MITRE Corporation McLean, Virginia

# December 2020

FINAL

This publications is available free of charge from <a href="https://doi.org/10.6028/NIST.SP.1800-26">https://doi.org/10.6028/NIST.SP.1800-26</a>.

This publication is available free of charge from <a href="https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond">https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond</a>.





## **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 1800-26C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-26C, 442 pages, (December 2020), CODEN: NSPUE2

## **FEEDBACK**

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

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: <u>nccoe@nist.gov</u>

## 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 <u>https://www.nccoe.nist.gov/</u>. To learn more about NIST, visit <u>https://www.nist.gov.</u>

### 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

Ransomware, destructive malware, insider threats, and even honest mistakes present an ongoing threat to organizations that manage data in various forms. Database records and structure, system files, configurations, user files, application code, and customer data are all potential targets of data corruption and destruction.

A quick, accurate, and thorough detection and response to a loss of data integrity can save an organization time, money, and headaches. While human knowledge and expertise is an essential component of these tasks, the right tools and preparation are essential to minimizing downtime and

losses due to data integrity events. The NCCoE, in collaboration with members of the business community and vendors of cybersecurity solutions, has built an example solution to address these data integrity challenges. This project details methods and potential tool sets that can detect, mitigate, and contain data integrity events in the components of an enterprise network. It also identifies tools and strategies to aid in a security team's response to such an event.

## **KEYWORDS**

attack vector; data integrity; malicious actor; malware; malware detection; malware response; ransomware.

### **ACKNOWLEDGMENTS**

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

Name	Organization		
Kyle Black	Bay Dynamics		
Sunjeet Randhawa	Broadcom Inc.		
Peter Romness	Cisco Systems		
Matthew Hyatt	Cisco Systems		
Matthew Shabat	Glasswall Government Solutions		
Justin Rowland	Glasswall Government Solutions		
Greg Rhein	Glasswall Government Solutions		
Steve Roberts	Micro Focus		
Timothy McBride	NIST		
Christopher Lowde	Semperis		
Thomas Leduc	Semperis		
Darren Mar-Elia	Semperis		

Name	Organization		
Kirk Lashbrook	Semperis		
Mickey Bresman	Semperis		
Humphrey Christian	Symantec Corporation		
Jon Christmas	Symantec Corporation		
Kenneth Durbin	Symantec Corporation		
Matthew Giblin	Symantec Corporation		
Jim Wachhaus	Tripwire		
Nancy Correll	The MITRE Corporation		
Chelsea Deane	The MITRE Corporation		
Sallie Edwards	The MITRE Corporation		
Milissa McGinnis	The MITRE Corporation		
Karri Meldorf	The MITRE Corporation		
Denise Schiavone	The MITRE Corporation		
Anne Townsend	The MITRE Corporation		

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

Technology Partner/Collaborator	Build Involvement
Symantec Corporation	Symantec Information Centric Analytics v6.5.2 Symantec Security Analytics v8.0.1
Cisco Systems	Cisco Identity Services Engine v2.4, Cisco Advanced Malware Protection v5.4, Cisco Stealthwatch v7.0.0
Glasswall Government Solutions	Glasswall FileTrust ATP for Email v6.90.2.5
Tripwire	Tripwire Log Center v7.3.1, Tripwire Enterprise v8.7
Micro Focus	Micro Focus ArcSight Enterprise Security Manager v7.0 Patch 2
Semperis	Semperis Directory Services Protector v2.7

# Contents

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-26.

Intr	oduct	ion	1
1.1	Practic	ce Guide Structure	1
1.2	Build C	Overview	2
1.3	Туроді	raphical Conventions	3
Pro	duct lı	nstallation Guides	3
2.1	Active	Directory and Domain Name System Server	3
	2.1.1	Install Features	3
	2.1.2	Create a Certificate Authority	17
	2.1.3	Configure Account to Add Computers to Domain	30
	2.1.4	Add Machines to the Domain	36
	2.1.5	Configure Active Directory to Audit Account Activity	41
	2.1.6	Configure Reverse Lookup Zones	43
2.2	Micros	soft Exchange Server	48
	2.2.1	Install Microsoft Exchange	49
2.3	Windo	ows Server Hyper-V Role	59
	2.3.1	Production Installation	59
2.4	MS SQ	۱۲ Server	65
	2.4.1	Install and Configure MS SQL	65
	2.4.2	Open Port on Firewall	73
	2.4.3	Add a New Login to the Database	78
2.5	Micros	soft IIS Server	80
	2.5.1	Install IIS	80
	2.5.2	IIS Configuration	87
2.6	Sempe	eris Directory Services Protector	91
	2.6.1	Configure Active Directory for Semperis DSP	91
	2.6.2	Install Semperis DSP	103
	2.6.3	Roll Back Changes with Semperis DSP	116
	2.6.4	Configure Reporting with Semperis DSP	117
	<ol> <li>1.1</li> <li>1.2</li> <li>1.3</li> <li>Proc</li> <li>2.1</li> <li>2.2</li> <li>2.3</li> <li>2.4</li> <li>2.5</li> </ol>	<ol> <li>Praction</li> <li>Build (1)</li> <li>Typog</li> <li>Typog</li> <li>Product I</li> <li>2.1</li> <li>2.1.1</li> <li>2.1.2</li> <li>2.1.3</li> <li>2.1.4</li> <li>2.1.5</li> <li>2.1.6</li> <li>2.2</li> <li>Microson</li> <li>2.3.1</li> <li>2.4</li> <li>MS SC</li> <li>2.4.1</li> <li>2.4.2</li> <li>2.4.3</li> <li>Scalar</li> <li>2.5.1</li> <li>2.5.2</li> <li>Semple</li> <li>2.6.1</li> <li>2.6.2</li> <li>2.6.3</li> </ol>	1.2       Build Overview

	2.6.5	Configu	e Email Alerts with Semperis DSP	118
2.7	Glassw	vall FileT	rust <sup>™</sup> for Email	
	2.7.1	Install P	rerequisites	120
		2.7.1.1	Install the IIS web server	120
		2.7.1.2	Install Microsoft SQL 2014 Enterprise	122
		2.7.1.3	Install Microsoft Visual C++ 2015	122
	2.7.2	Install th	ne Glasswall FileTrust Server Component	124
		2.7.2.1	Install Glasswall Hub	124
		2.7.2.2	Install Glasswall Integration Service	128
		2.7.2.3	Install Glasswall Administrator Console	131
		2.7.2.4	Add the Server's Certificate	133
		2.7.2.5	Install the Smtp Analysis Agent	147
		2.7.2.6	Distribute the Glasswall License File	149
	2.7.3	Configu	e Glasswall FileTrust	151
		2.7.3.1	Create a New Administrator Account	152
		2.7.3.2	Configure Notifications and Policies	157
		2.7.3.3	Configure Inbound SMTP Policy	158
		2.7.3.4	Create a Receiver Group	159
		2.7.3.5	Create a ThreatCensor Policy Set	161
		2.7.3.6	Create a Processing Rule	162
	2.7.4	Configu	e Intelligence Sharing	163
2.8	Micro I	Focus Arc	Sight Enterprise Security Manager	165
	2.8.1	Install th	ne ArcSight Console	165
	2.8.2	Install In	dividual ArcSight Windows Connectors	179
	2.8.3	Install In	dividual ArcSight Ubuntu Connectors	197
	2.8.4	Install a	Connector Server for ESM on Windows 2012 R2	210
	2.8.5	Install P	re-Configured Filters for ArcSight	221
		2.8.5.1	Install Activate Base	221
		2.8.5.2	Install Packages	223
	2.8.6	Apply Fi	lters to a Channel	224

	2.8.7	Configu	re Email Alerts in ArcSight	225
		2.8.7.1	Configure a New Destination	225
		2.8.7.2	Configure a New Rule	226
2.9	Tripwir	e Enterpr	ise	229
	2.9.1	Install T	ripwire Enterprise	230
	2.9.2	Install th	ne Axon Bridge	242
	2.9.3	Install th	ne Axon Agent (Windows)	242
	2.9.4	Install th	ne Axon Agent (Linux)	243
	2.9.5	Configu	re Tripwire Enterprise	244
		2.9.5.1	Terminology	244
		2.9.5.2	Tags	245
		2.9.5.3	Rules	247
		2.9.5.4	Tasks	251
2.10	Tripwir	e Log Cer	nter	254
	2.10.1	Install T	ripwire Log Center Manager	254
	2.10.2	Configu	re Tripwire Log Center Manager	255
	2.10.3	Install T	ripwire Log Center Console	260
2.11	Cisco lo	dentity Se	rvices Engine	
	2.11.1	Initial Se	etup	261
	2.11.2	Invento	ry: Configure SNMP on Routers/Network Devices	261
	2.11.3	Invento	ry: Configure Device Detection	261
	2.11.4	Policy E	nforcement: Configure Active Directory Integration	265
	2.11.5	Policy E	nforcement: Enable Passive Identity with AD	268
	2.11.6	Policy E	nforcement: Developing Policy Conditions	273
	2.11.7	Policy E	nforcement: Developing Policy Results	274
	2.11.8	Policy E	nforcement: Enforcing a Requirement in Policy	275
	2.11.9	Policy E	nforcement: Configuring a Web Portal	276
	2.11.10	) Configu	ring RADIUS with your Network Device	277
	2.11.11	L Configu	ring an Authentication Policy	278
	2.11.12	2 Configu	ring an Authorization Policy	
2.12	Cisco A	dvanced	Malware Protection	

	2.12.1	Dashboard Configuration	281
	2.12.2	Installing the Connector on a Windows Server	281
	2.12.3	Installing the Connector on a Windows 10 Machine	283
	2.12.4	Scanning using AMP	284
	2.12.5	Configure AMP Policy	285
2.13	Cisco St	tealthwatch	287
	2.13.1	Configure Stealthwatch Flow Collector, Stealthwatch Management Console, Stealthwatch UDP Director and Stealthwatch Flow Sensor	287
	2.13.2	Change Default Stealthwatch Console Passwords	292
	2.13.3	Configure the Stealthwatch Management Console Web Interface	296
	2.13.4	Configure the Stealthwatch UDP Director, Stealthwatch Flow Collector and	
		Stealthwatch Flow Sensor Web Interfaces	
2.14		tec Analytics	
		Initial Setup	
		Capturing Data	
2.15	-	tec Information Centric Analytics	
		Installing MS SQL 2017	
	2.15.2	Install Windows Services	317
	2.15.3		
	2.15.4	Configuring Symantec ICA for Analysis	332
		2.15.4.1 Installing Integration Packs	332
		2.15.4.2 Create a View	333
		2.15.4.3 Open an Existing View	334
		2.15.4.4 Viewing Detailed Analyzer Data	336
2.16	Integra	tion: Cisco Identity Services Engine and Cisco Stealthwatch	336
	2.16.1	Configuring Certificates for pxGrid	336
	2.16.2	Configuring Stealthwatch to Quarantine through ISE	348
2.17	Integra	tion: Tripwire Log Center and Tripwire Enterprise	353
2.18	Integra	tion: Symantec ICA and ArcSight ESM	360
	2.18.1	Export the CSV File from ArcSight Console	360
	2.18.2	Import the CSV File to Symantec ICA	362

	2.18.3	Create a Mapping between ArcSight events and Symantec ICA	366
	2.18.4	View ArcSight Events in the Analyzer	371
2.19	Integra	ation: Micro Focus ArcSight and Tripwire	372
	2.19.1	Install Micro Focus ArcSight	372
2.20	Integra	ation: Micro Focus ArcSight and Cisco AMP	
	2.20.1	Create API Credentials for ArcSight to access AMP	
	2.20.2	Install Micro Focus ArcSight	
	2.20.3	Create a Parser for Cisco AMP REST events	
2.21	Integra	ation: Micro Focus ArcSight and Cisco ISE	394
	2.21.1	Configure Cisco ISE to Forward Logs	395
	2.21.2	Select Logs for Forwarding	396
2.22	Integra	ation: Micro Focus ArcSight and Semperis DSP	398
	2.22.1	Configure Semperis DSP to Forward Logs	398
2.23	Integra	ation: Micro Focus ArcSight and Symantec Analytics	
	2.23.1	Configure Symantec Analytics to Forward Logs	
	2.23.2	Install Symantec Analytics Package for ArcSight	401
2.24	Integra	ation: Micro Focus ArcSight and Glasswall FileTrust	409
	2.24.1	Install Micro Focus ArcSight	409
2.25	Integra	ation: Micro Focus ArcSight and Cisco Stealthwatch	424
	2.25.1	Install Micro Focus ArcSight	424
	2.25.2	Configure Cisco Stealthwatch	433
Append	lix A	List of Acronyms	

# **1** Introduction

The following guides show 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 recreate the product manufacturers' documentation, which is presumed to be widely available. Rather, these guides show how we incorporated the products together in our 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 Practice Guide Structure

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the data integrity detection and response solution. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-26A: *Executive Summary*
- NIST SP 1800-26B: Approach, Architecture, and Security Characteristics what we built and why
- NIST SP 1800-26C: 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 1800-26A)*, which describes the:

- challenges enterprises face in detecting and responding to data integrity events
- 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 1800-26B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.1, Risk, provides a description of the risk analysis we performed.
- Section 3.4.2, 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 1800-26A*, with your leadership team members to help them understand the importance of adopting standards-based data integrity solutions.

**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 1800-26C*, to replicate all or parts of the build created in our lab. The How-To 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 data integrity detection and response solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Volume B, Section 3.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. 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 <u>ds-nccoe@nist.gov</u>.

### **1.2 Build Overview**

The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively detect and respond to a data corruption event in various Information Technology (IT) enterprise environments. NCCoE also explored the issues of analysis and reporting to support incident response. 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 Integrity Community of Interest to develop a diverse (but non-comprehensive) set of use case scenarios against which to test the reference implementation. These are detailed in Volume B, Section 5.2. For a detailed description of our architecture, see Volume B, Section 4.

# **1.3 Typographical Conventions**

The following table presents typographic conventions used in this volume.

Typeface/ Symbol	Meaning	Example
Italics	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the NCCoE Glossary.
Bold	names of menus, options, command buttons and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, on- screen computer output, sample code examples, sta- tus codes	mkdir
Monospace Bold	command-line user input contrasted with computer output	service sshd start
<u>blue text</u>	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at <u>http://nccoe.nist.gov</u>

# 2 Product Installation Guides

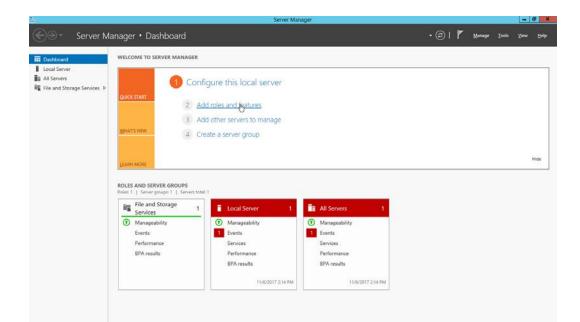
This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution.

# 2.1 Active Directory and Domain Name System Server

As part of our enterprise emulation, we included an Active Directory server that doubles as a Domain Name System (DNS) server. This section covers the installation and configuration process used to set up Active Directory and DNS on a Windows Server 2012 R2 machine.

### 2.1.1 Install Features

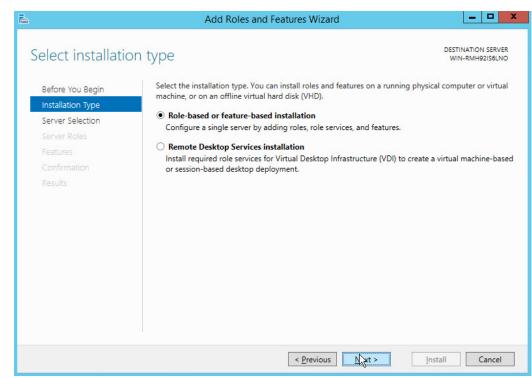
1. Open Server Manager.



2. Click the link Add roles and features.

	Add Roles and Features Wizard
efore you begi	n Destination services with restrict the service of the service service service service services and services services services and services servic
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	<ul> <li>This wizard helps you install roles, role services, or features. You determine which roles, role services, features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.</li> <li>To remove roles, role services, or features:</li> <li>Start the Remove Roles and Features Wizard</li> <li>Before you continue, verify that the following tasks have been completed:</li> <li>The Administrator account has a strong password</li> <li>Network settings, such as static IP addresses, are configured</li> <li>The most current security updates from Windows Update are installed</li> <li>If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.</li> <li>To continue, click Next.</li> </ul>

- 3. Click Next.
- 4. Select Role-based or feature-based installation.



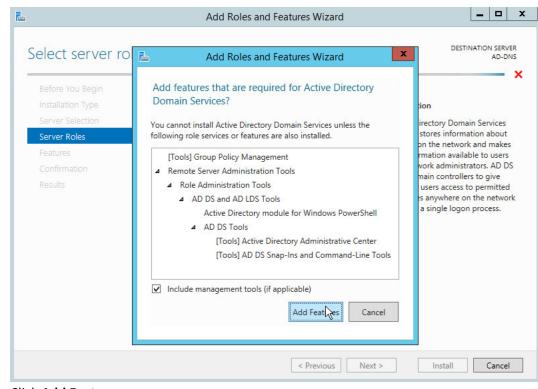
- 5. Click Next.
- 6. Select Select a server from the server pool.
- 7. Select the intended active directory server.

Select destinati	on server		DESTINATION SER AD-I	
Before You Begin	Select a server or a	virtual hard disk on which	to install roles and features.	
Installation Type	Select a server f	from the server pool		
Server Selection	O Select a virtual	<ul> <li>Select a virtual hard disk</li> </ul>		
Server Roles	Server Pool			
Features Confirmation	Filter:			
Results	Name	IP Address	Operating System	
	AD-DNS	192.168.78.4	Microsoft Windows Server 2012 R2 Standard	
		rvers that are running Wir	ndows Server 2012, and that have been added by using ffline servers and newly-added servers from which data	
	Add Servers comm	complete are not shown.		

Select server ro	es	DESTINATION SERV AD-D
Before You Begin Installation Type	Select one or more roles to install on the selected server.	Description
Server Selection Server Roles Features Confirmation Results	<ul> <li>Active Directory Certificate Services</li> <li>Active Directory Domain Services</li> <li>Active Directory Federation Services</li> <li>Active Directory Lightweight Directory Services</li> <li>Active Directory Rights Management Services</li> <li>Application Server</li> <li>DHCP Server</li> <li>DNS Server</li> <li>Fax Server</li> <li>File and Storage Services (1 of 12 installed)</li> <li>Hyper-V</li> <li>Network Policy and Access Services</li> <li>Print and Document Services</li> <li>Remote Access</li> <li>Remote Desktop Services</li> </ul>	<ul> <li>Active Directory Domain Services (AD DS) stores information about objects on the network and make this information available to users and network administrators. AD D uses domain controllers to give network users access to permitter resources anywhere on the networ through a single logon process.</li> </ul>

9. Check the box next to Active Directory Domain Services.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-26.



10. Click Add Features.

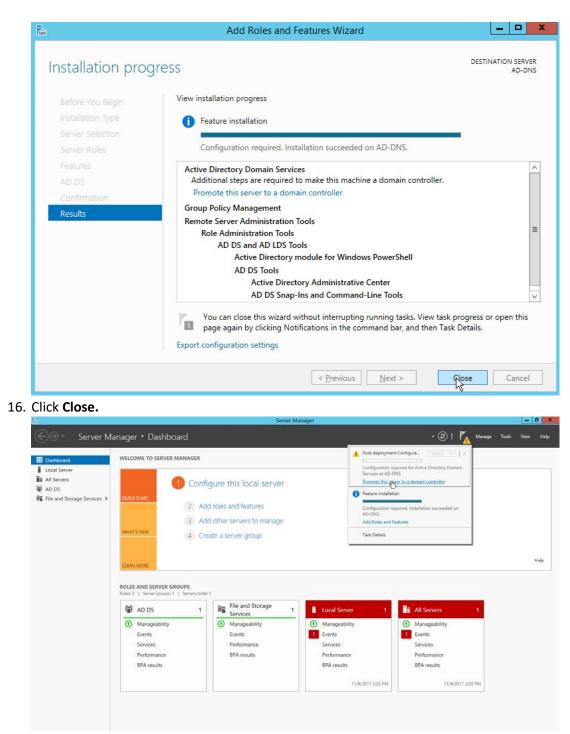
Select server ro	les	DESTINATION SER AD-I
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection	Active Directory Certificate Services	Active Directory Domain Services
Server Roles	Active Directory Domain Services	(AD DS) stores information abou objects on the network and make
Features	Active Directory Federation Services	this information available to user
AD DS	Active Directory Lightweight Directory Services	and network administrators. AD
Confirmation	Active Directory Rights Management Services	uses domain controllers to give network users access to permitte
	Application Server	resources anywhere on the netwo
	DHCP Server	through a single logon process.
	DNS Server	
	Fax Server	
	File and Storage Services (1 of 12 installed)     Hyper-V	
	Network Policy and Access Services	
	Print and Document Services	
	Remote Access	
	Remote Desktop Services	
		<b>~</b>

11. Click Next.

Add Roles and Features Wizard \_ **D** X a DESTINATION SERVER Select features AD-DNS Select one or more features to install on the selected server. Before You Begin Installation Type Features Description Server Selection .NET Framework 3.5 combines the ~ .NET Framework 3.5 Features power of the .NET Framework 2.0 Server Roles NET Framework 4.5 Features (2 of 7 installed) APIs with new technologies for Features ≣ Background Intelligent Transfer Service (BITS) building applications that offer appealing user interfaces, protect AD DS BitLocker Drive Encryption your customers' personal identity Confirmation BitLocker Network Unlock information, enable seamless and BranchCache secure communication, and provide the ability to model a range of Client for NFS business processes. Data Center Bridging Direct Play Enhanced Storage Failover Clustering Group Policy Management IIS Hostable Web Core Ink and Handwriting Services 11 < Previous Install Cancel Next 12. Click Next. \_ 🗆 🗙 Add Roles and Features Wizard A DESTINATION SERVER Active Directory Domain Services AD-DNS Active Directory Domain Services (AD DS) stores information about users, computers, and other devices Before You Begin on the network. AD DS helps administrators securely manage this information and facilitates resource Installation Type sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy. Server Selection Server Roles Things to note: Features · To help ensure that users can still log on to the network in the case of a server outage, install a AD DS minimum of two domain controllers for a domain. · AD DS requires a DNS server to be installed on the network. If you do not have a DNS server Confirmation installed, you will be prompted to install the DNS Server role on this machine. Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by AD DS. < <u>P</u>revious Nert > Install Cancel

Confirm installa	tion selections	N SERV
Before You Begin Installation Type Server Selection Server Roles	To install the following roles, role services, or features on selected server, click Install. Restart the destination server automatically if required Optional features (such as administration tools) might be displayed on this page because they been selected automatically. If you do not want to install these optional features, click Previous	have
Features AD DS	their check boxes. Active Directory Domain Services	
Confirmation	Group Policy Management	
Results	Remote Server Administration Tools Role Administration Tools AD DS and AD LDS Tools Active Directory module for Windows PowerShell AD DS Tools Active Directory Administrative Center AD DS Snap-Ins and Command-Line Tools	
	Export configuration settings Specify an alternate source path	

- 14. Click Install.
- 15. Wait for the installation to complete.



- 17. Click Promote this server to a domain controller.
- 18. Select Add a new forest.
- 19. Enter a Root domain name.

E.	Active Directory Domain Service	es Configuration Wizard	_ <b>D</b> X
Deployment Conf	iguration		TARGET SERVER AD-DNS
Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select the deployment operation <ul> <li>Add a domain controller to an existing</li> <li>Add a new domain to an existing</li> <li>Add a new forest</li> </ul> Specify the domain information for the Root domain name: More about deployment configuration	forest his operation DLIPDR	
		Previous Next	ll Cancel

- 20. Click Next.
- 21. Select Windows Server 2012 R2 for Forest functional level and Domain functional level.
- 22. Check the box next to Domain Name System (DNS) server.
- 23. Enter a password.

È.	Active Directory Domain Service	es Configuration Wizard	_ <b>_</b> ×
Domain Controlle	r Options		TARGET SERVER AD-DNS
Deployment Configuration Domain Controller Options DNS Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new for Forest functional level: Domain functional level: Specify domain controller capabilitie Opmain Name System (DNS) ser Global Catalog (GC) Read only domain controller (RO Type the Directory Services Restore I Passworg: Confirm password:	Windows Server 2012 R2 Windows Server 2012 R2 s ver DC)	<b>v</b>
	More about domain controller optio	ns	Install Cancel
4. Click Next.			
B	Active Directory Domain Service	es Configuration Wizard	_ <b>_</b> X
DNS Options			TARGET SERVER AD-DNS
Deployment Configuration Domain Controller Options DNS Options Additional Options	Specify DNS delegation options		
Paths Review Options Prerequisites Check Installation Results	More about DNS delegation		

### 26. Verify the domain name.

<b>a</b>	Active Directory Domain Service	es Configuration Wizard	- <b>-</b> X
Additional Option	าร		TARGET SERVER AD-DNS
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Verify the NetBIOS name assigned to	D the domain and change it if necessary	
	More about additional options		
		<u>Previous</u>	tall Cancel
27. Click Next.			_ <b>D</b> X
	Active Directory Domain Service	s Configuration Wizard	
Paths			TARGET SERVER AD-DNS
Deployment Configuration Domain Controller Options	Specify the location of the AD DS dat	abase, log files, and SYSVOL	
DNS Options	<u>D</u> atabase folder:	C:\Windows\NTDS	
Additional Options	Log files folder: SYSVOL folder:	C:\Windows\NTDS C:\Windows\SYSVOL	
Paths Review Options Prerequisites Check Installation Results			
	More about Active Directory paths		
	<	Previous Nyt > Insta	all Cancel

Click Next. Click Next. Active Directory Domain Services Configuration Wizard  Active Directory Domain Services Configuration Wizard  ARGET SERVAD-  Prerequisites Check  Additional Options Paths Review Options  Prerequisites Check  View results  Additional Options Prerequisites Check  Additional Options Prerequisites Check Prerequis		Active Directory Domain Services Configuration Wizard	
Domain Controller Options       Onfigure this server as the first Active Directory domain controller in a new forest.         The new domain name is "DLIPDR". This is also the name of the new forest.       The new domain name is "DLIPDR". This is also the name of the new forest.         Paths       Review Options       Forest Functional Level: Windows Server 2012 R2         Domain Functional Level: Windows Server 2012 R2       Domain functional Level: Windows Server 2012 R2         Additional Options:       Global catalog: Yes         DNS Server: Yes       Create DNS Delegation: No         These settings can be exported to a Windows PowerShell script to automate additional installations       View script         More about installation options       More about installation options         Click Next:       Active Directory Domain Services Configuration Wizard       View script         Prerequisites Check       Show more       Show more       Show more         Optionin Controller Options       Prerequisites need to be validated before Active Directory Domain Services is installed on this computer         Prerequisites Check       Prerequisites check       Show more       Sho	Review Options		
< Previous	Domain Controller Option DNS Options Additional Options Paths Review Options Prerequisites Check Installation	Configure this server as the first Active Directory domain controller in a new The new domain name is "DI.IPDR". This is also the name of the new forest The NetBIOS name of the domain: DI Forest Functional Level: Windows Server 2012 R2 Domain Functional Level: Windows Server 2012 R2 Additional Options: Global catalog: Yes DNS Server: Yes Create DNS Delegation: No These settings can be exported to a Windows PowerShell script to automate additional installations	e
<ul> <li>Active Directory Domain Services Configuration Wizard</li> <li>Prerequisites Check</li> <li>All prerequisite checks passed successfully. Click 'Install' to begin installation.</li> <li>Show more</li> <li>All prerequisite checks passed successfully. Click 'Install' to begin installation.</li> <li>Show more</li> <li>Perequisite checks passed successfully. Click 'Install' to begin installation.</li> <li>Show more</li> <li>Prerequisite checks passed successfully. Click 'Install' to begin installation.</li> <li>Prerequisites checks</li> <li>Prerequisites check</li> <li>View results</li> <li>View results</li> <li>View results</li> <li>View results</li> <li>Mindows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.</li> <li>For more information about this setting, see Knowledge Base article 942564 (http:// go.microsoft.com/fwlink/?Linkld=104751).</li> <li>This computer has at least one physical network adapter that does not have static IP agdress(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP address(es) assigned to its IP address(es) assignes and its IP address(es) assigned to its IP address(es) assigne</li></ul>		< <u>P</u> revious <u>Nev</u>	nstall Cancel
Image: Active Directory Domain Services Configuration       TARGET SERV AD-D         Image: Prerequisites check       TARGET SERV AD-D         Image: Deployment Configuration Domain Controller Options DNS Options       Prerequisites need to be validated before Active Directory Domain Services is installed on this computer         Image: Deployment Configuration Domain Controller Options Paths Review Options       Prerequisites need to be validated before Active Directory Domain Services is installed on this computer         Prerequisites Check       Image: Deployment Configuration Domain Controller Options         Paths Review Options       View results         Installation Results       Image: Deployment Configuration Discontrom/fwlink/?Linkld=104751).         Installation Results       Tor more information about this setting, see Knowledge Base article 942564 (http:// go.microsoft.com/fwlink/?Linkld=104751).         Image: Deployment Configuration Results       This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapter for reliable Domain Name System			
Prerequisites Check       AD-D                 All prerequisite checks passed successfully. Click 'Install' to begin installation.        Show more              2                 Deployment Configuration             Domain Controller Options             DNS Options             Additional Options             Paths             Review Options        Prerequisites check               Prerequisites check               View results               Windows Server 2012 R2 domain controllers have a default for the security setting             named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents             weaker cryptography algorithms when establishing security channel sessions.               For more information about this setting, see Knowledge Base article 942564 (http://             go.microsft.com/fwlink/?Linkl=104751).               This computer has at least one physical network adapter that does not have static IP             address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network             adapter, both IPv4 and IPv6 are enabled for a network             adapter, both IPv4 and IPv6 attic IP address(es) assignment             should be done to all the physical network adapter. Such static IP address(es) assignment             should be done to all the physical network adapter for reliable Domain Name System	lick <b>Next.</b>		
Deployment Configuration Domain Controller Options       Prerequisites need to be validated before Active Directory Domain Services is installed on this computer         DNS Options       Additional Options         Paths       Review Options         Prerequisites Check       Mindows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.         Installation Results       For more information about this setting, see Knowledge Base article 942564 (http:// go.microsoft.com/fwlink/?Linkld=104751).         M       This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System		Active Directory Domain Services Configuration Wizard	
More about prerequisites	Prerequisites Ch	eck	TARGET SERV AD-D

- 30. Click Install.
- 31. Wait for the installation to complete.
- 32. The server automatically reboots.

# 2.1.2 Create a Certificate Authority

1. Open Server Manager.

			Server	Manager		- 0
💬 🕘 🐐 Server Ma	anager • Dash	board			• 🗇   🚩 Marage	Iools Yiew Help
Dashboard	WELCOME TO SERV	ER MANAGER				
Local Server All Servers AD DS DNS	QUICK START	1 Cont	figure this local server			
ENS     File and Storage Services	QUEKSTART		<u>id roles and features</u> id other servers to manage			
	WHAT'S NEW		eate a server group			
	LEARN MORE					Hide
	ROLES AND SERVER	GROUPS				
	Roles: 3   Server group		1	1 File and Storage 1	Local Server 1	
	Manageabilit	у	Manageability	Manageability	Manageability	
	Events Services		Events Services	Events Services	1 Events Services	
	Performance		Performance	Performance	Performance	
	BPA results		BPA results	BPA results	BPA results	
					11/6/2017 3:01 PM	
	All Servers	1				
	<li>Manageabilit</li>	У				

2. Click Add roles and features.

3	Add Roles and Features Wizard	_	-	x
Before you begin		DESTINATION AD-DNS		
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	This wizard helps you install roles, role services, or features. You determine which features to install based on the computing needs of your organization, such as sh hosting a website. To remove roles, role services, or features: Start the Remove Roles and Features Wizard Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, complete the steps, and then run the wizard again. To continue, click Next.	naring documen	nts, o	
	Skip this page by default			
	< Previous In	stall C	ancel	
ick <b>Next.</b> Nect <b>Role-based or</b> :	feature-based installation.			
	Add Roles and Features Wizard	-		x
Select installation t	ype	DESTINATION AD-DNS		
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	<ul> <li>Select the installation type. You can install roles and features on a running physic machine, or on an offline virtual hard disk (VHD).</li> <li>Role-based or feature-based installation Configure a single server by adding roles, role services, and features.</li> <li>Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a or session-based desktop deployment.</li> </ul>			

3. 4.

< Previous Next

Cancel

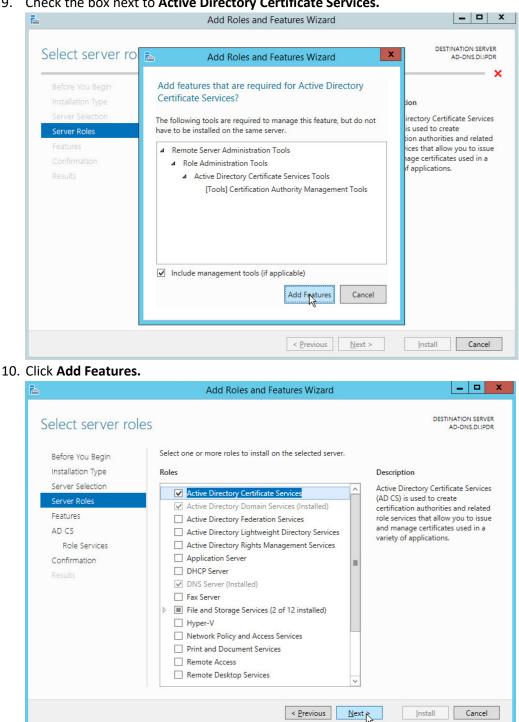
Install

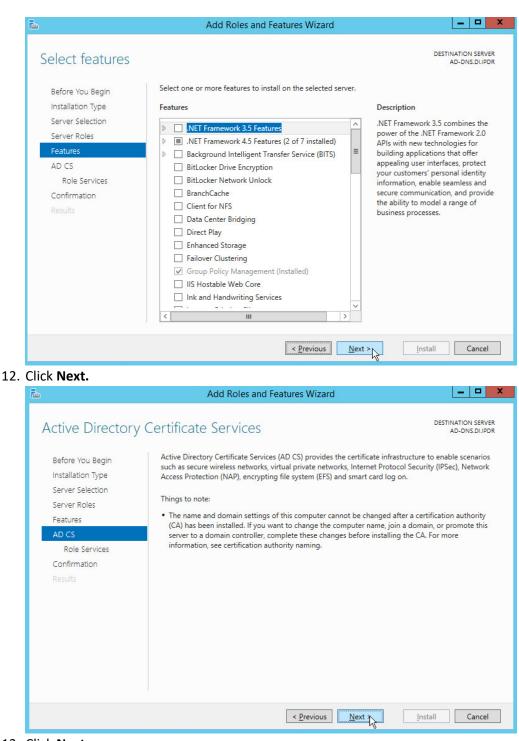
### 6. Select Select a server from the server pool.

7. Select the intended Active Directory server.

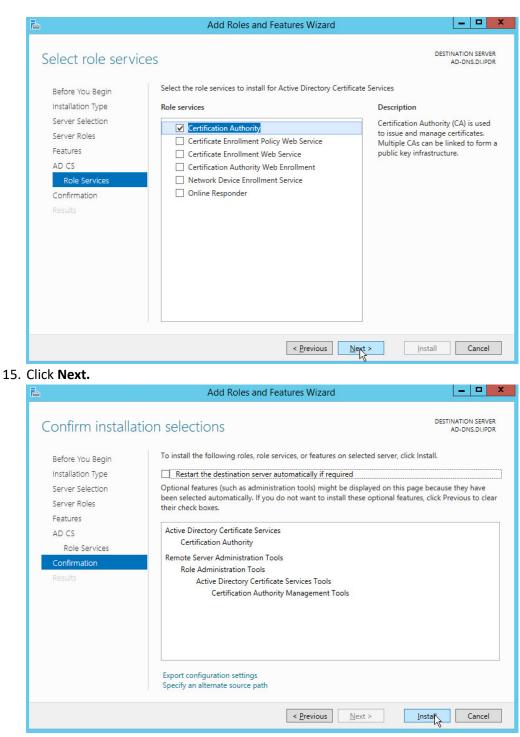
Select destination	DN SERVER DESTINATION SERVER AD-DNS.DLIPDR
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select a server or a virtual hard disk on which to install roles and features. <ul> <li>Select a server from the server pool</li> <li>Select a virtual hard disk</li> </ul> Server Pool         Filter:         Name       IP Address         AD-DNS.DI.IPDR       192.168.78.4         Microsoft Windows Server 2012 R2 Standard
	1 Computer(s) found         1 his page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.         < Previous
Click <b>Next.</b>	v
	Add Roles and Features Wizard
Colorteonus	DESTINATION SERVER
Select server ro	Select one or more roles to install on the selected server.
Select server ro Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	

#### 9. Check the box next to Active Directory Certificate Services.

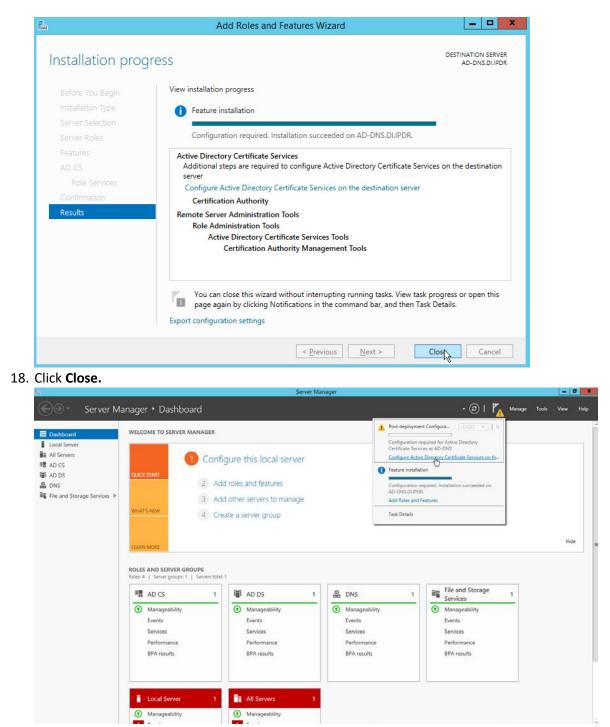




- 13. Click Next.
- 14. Check the box next to Certification Authority.



- 16. Click Install.
- 17. Wait for the installation to complete.



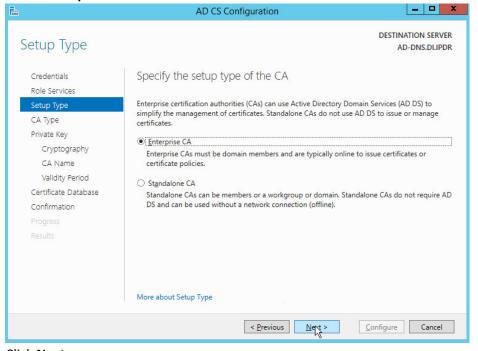
19. Click Configure Active Directory Certificate Services on the destination server.

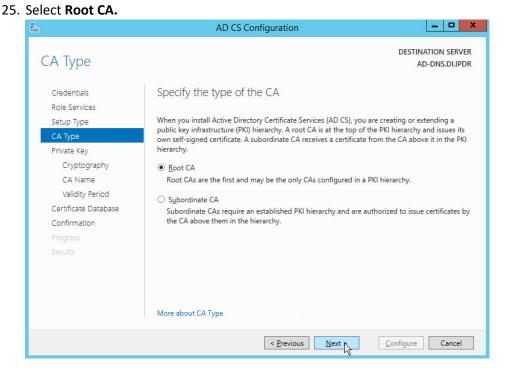
A	AD CS Configuration
Credentials	DESTINATION SERVER AD-DNS.DI.IPDR
Credentials Role Services	Specify credentials to configure role services
Confirmation Progress Results	To install the following role services you must belong to the local Administrators group:  Standalone certification authority  Certification Authority Web Enrollment Online Responder  To install the following role services you must belong to the Enterprise Admins group: Enterprise certification authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Network Device Enrollment Service Credentials: DI\Administrator
	More about AD CS Server Roles
	< <u>Previous</u> <u>Next</u> > <u>Configure</u> Cancel

#### 21. Check the box next to Certification Authority.

<b>b</b>	AD CS Configuration	_ <b>_</b> ×
Role Services		DESTINATION SERVER AD-DNS.DI.IPDR
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Select Role Services to configure  Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service	
	More about AD CS Server Roles	
	< Previous Net >>	<u>C</u> onfigure Cancel

#### 23. Select Enterprise CA.





### 27. Select Create a new private key.

<b>a</b>	AD CS Configuration
Private Key	DESTINATION SERVER AD-DNS.DI.IPDR
Credentials Role Services	Specify the type of the private key
Setup Type	To generate and issue certificates to clients, a certification authority (CA) must have a private key.
СА Туре	Create a new private key
Private Key	Use this option if you do not have a private key or want to create a new private key.
Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	<ul> <li>Use existing private key</li> <li>Use this option to ensure continuity with previously issued certificates when reinstalling a CA.</li> <li>Select a certificate and use its associated private key</li> <li>Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.</li> <li>Select an existing private key on this computer</li> <li>Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.</li> </ul>
	More about Private Key
	< Previous Next Configure Cancel

- 28. Click Next.
- 29. Select RSA#Microsoft Software Key Storage Provider.
- 30. Set the Key length to 2048.
- 31. Select SHA512 from the list.

	AD CS Configuration	_ <b>_</b> ×
Cryptography fo	or CA	DESTINATION SERVER AD-DNS.DI.IPDR
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Specify the cryptographic options         Select a cryptographic provider:         RSA#Microsoft Software Key Storage Provider         Select the hash algorithm for signing certificates issued by this CA         SHA256         SHA384         SHA512         SHA1         MD5         Allow administrator interaction when the private key is accessed	<ul><li>▲</li><li>■</li><li>✓</li></ul>
	More about Cryptography	
lick <b>Next.</b>	< Previous Netz >	<u>C</u> onfigure Cancel
lick Next.	< Previous №4ৣर> AD CS Configuration	Configure Cancel
	AD CS Configuration	
2	AD CS Configuration Specify the name of the CA Type a common name to identify this certification authority (CA). certificates issued by the CA. Distinguished name suffix values are be modified. Common name for this CA: DI-AD-DNS-CA Distinguished name suffix: DC=DI,DC=IPDR Preview of distinguished name: CN=DI-AD-DNS-CA,DC=DI,DC=IPDR	DESTINATION SERVER AD-DNS.DI.IPDF
Credentials Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress	AD CS Configuration Specify the name of the CA Type a common name to identify this certification authority (CA). certificates issued by the CA. Distinguished name suffix values are be modified. Common name for this CA: DI-AD-DNS-CA Distinguished name suffix: DC=DI,DC=IPDR Preview of distinguished name:	DESTINATION SERVER AD-DNS.DI.IPDR

#### 34. Set the validity period of the certificate according to the needs of your organization.

<b>b</b>	AD CS Configuration	_ <b>_</b> ×
Validity Period		DESTINATION SERVER AD-DNS.DI.IPDR
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Specify the validity period Select the validity period for the certificate generated for this certific 5 Years CA expiration Date: 11/6/2022 3:19:00 PM The validity period configured for this CA certificate should exceed to certificates it will issue.	-215 3
	More about Validity Period	Configure Cancel
35. Click <b>Next.</b>		
<b>b</b>	AD CS Configuration	_ <b>_</b> ×
CA Database		DESTINATION SERVER AD-DNS.DI.IPDR
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Specify the database locations <u>C</u> ertificate database location: C:\Windows\system32\CertLog Cgrtificate database log location: C:\Windows\system32\CertLog	
	< <u>P</u> revious <u>Nyxt &gt;</u>	Configure Cancel

	AD CS Con	figuration	
Confirmation			DESTINATION SERVER AD-DNS.DI.IPDR
Credentials Role Services	To configure the following roles <ul> <li>Active Directory Certificat</li> </ul>	, role services, or features, click Configur e Services	e.
Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Certification Authority CA Type: Cryptographic provider: Hash Algorithm: Key Length: Allow Administrator Interaction: Certificate Validity Period: Distinguished Name: Certificate Database Location: Certificate Database Log Location:	11/6/2022 3:19:00 PM CN=DI-AD-DNS-CA,DC=DI,DC=IPDR	rovider
Click <b>Configure.</b>	AD CS Co	< <u>Previous</u> <u>Next &gt; </u>	Configure Cancel
Results			DESTINATION SERVE AD-DNS.DI.IPD
Credentials Role Services	The following roles, role service		
Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Certification Authority More about CA Configuration	S Configuration st	ucceeded
and the second sec			

#### 38. Click Close.

## 2.1.3 Configure Account to Add Computers to Domain

- 1. Open the Start menu.
- 2. Enter **dsa.msc,** and run the program.

Start				Search Everywhere v dsa.msd	
L	Windows PowerShell			dsa msc	
Server Manager	PowerShell				
Control Panel	Internet Explorer				
Desktop Generative Tools					
۲					

3. Right-click on **Users** in the left panel.

ile Action View Help				
• 🔿 📶 🕷 🗐 🗙 🗐	a 🔒 🛿 🖬	1 🙎 🐮 🕅	7 🔁 🗽	
Active Directory Users and Com	Name	Туре	Description	
Saved Queries	Administrator	User	Built-in account for ad	
DI.IPDR	& Allowed RO	Security Group	Members in this group c	
Builtin	& Cert Publish	Security Group	Members of this group	
Computers	& Cloneable D	Security Group	Members of this group t	
Domain Controllers	& Denied ROD	Security Group	Members in this group c	
ForeignSecurityPrincipal:	& DnsAdmins	Security Group	DNS Administrators Gro	
Managed Service Accour	& DnsUpdateP	Security Group	DNS clients who are per	
Users	& Domain Ad	Security Group	Designated administrato	
~	& Domain Co	Security Group	All workstations and ser	
	& Domain Con	Security Group	All domain controllers i	
	& Domain Gue	Security Group	All domain guests	
	& Domain Users	Security Group	All domain users	
	Senterprise A	Security Group	Designated administrato	
	Senterprise R	Security Group	Members of this group	
	Stroup Polic	Security Group	Members in this group c	
	🛃 Guest	User	Built-in account for gue	
	Reprotected Us	Security Group	Members of this group	
	& RAS and IAS	Security Group	Servers in this group can	
	용 Read-only D	Security Group	Members of this group	
		Security Group	Designated administrato	

## 4. Click Delegate Control.

### Delegation of Control Wizard

# x

### Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.

5. Click Next.

Delegation of Control Wizard
Users or Groups Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
< Back Next > Cancel Help

- 6. Click Add to select users or groups.
- 7. Add users or groups.

Select this object type:			_
Users, Groups, or Built-in	security principals	 Object Types.	••
From this location:		 	_
DI.IPDR		Locations	
Enter the object names to	select (examples):		
Domain Admins		 Check Names	
		Chook Hamor	
Advanced		OK Cancel	
Advanced		Lancer Cancer	
		- X.	

8. Click OK.

Delegation of Control Wizard
Users or Groups Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
Domain Admins (DI\Domain Admins)
Add Remove       < Back

### 10. Choose Create a custom task to delegate.

	Delegation of Control Wizard	X
Tasks to D You can	elegate select common tasks or customize your own.	P
O <u>D</u> eleg	jate the following common tasks:	
	Create, delete, and manage user accounts  Reset user passwords and force password change at next logon Read all user information Create, delete and manage groups Modify the membership of a group Create, delete, and manage inetOrgPerson accounts Reset inetOrgPerson passwords and force password change at next lc	
<	III >	
● Creat	e a custom task to delegate	
	< Back Sat > Cancel	Help
	< Back Cancel	Help

- 11. Click Next.
- 12. Choose Only the following objects in the folder.

- 13. Check the box next to **Computer objects.**
- 14. Check the box next to Create selected objects in this folder.
- 15. Check the box next to Delete selected objects in this folder.

Delegation of Control Wizard	x
Active Directory Object Type Indicate the scope of the task you want to delegate.	2
Delegate control of:	
account objects     aCSResourceLimits objects     application Version objects     bootableDevice objects     certificationAuthority objects     Computer objects     ✓     Create selected objects in this folder     ✓     Delete selected objects in this folder	
< Back Next > Cancel Help	>

- 16. Click Next.
- 17. Check the boxes next to **Reset password**, **Read and write account restrictions**, **Validated write to DNS host name**, and **Validated write to service principal name**.

Permissions Select the permissions	s you want to delegate.	P
Show these permission	ns:	
General		
Property-specific		
Creation/deletion o	of specific child objects	
Permissions:		
Receive as		^
Read and write a	account restrictions	
Read and write p	ersonal information	
Read and write p		=
<ul> <li>Validated write to</li> </ul>		
Validated write to	service principal name	~
Click <b>Next.</b>		
	Delegation of Control Wizard Completing the Delegation of Control Wizard	of
<b>Received</b>	Completing the Delegation o	
	Completing the Delegation of Control Wizard	
	Completing the Delegation of Control Wizard You have successfully completed the Delegation of wizard. You chose to delegate control of objects	
	Completing the Delegation of Control Wizard You have successfully completed the Delegation of wizard. You chose to delegate control of objects in the following Active Directory folder:	Control
	Completing the Delegation of Control Wizard You have successfully completed the Delegation of wizard. You chose to delegate control of objects in the following Active Directory folder: DI.IPDR/Users The groups, users, or computers to which you have given control are:	Control
	Completing the Delegation of Control Wizard         You have successfully completed the Delegation of wizard.         You chose to delegate control of objects in the following Active Directory folder:         DI.IPDR/Users         The groups, users, or computers to which you have given control are:         Domain Admins (DI\Domain Admins)	Control
	Completing the Delegation of Control Wizard You have successfully completed the Delegation of wizard. You chose to delegate control of objects in the following Active Directory folder: DI.IPDR/Users The groups, users, or computers to which you have given control are:	Control
	Completing the Delegation of Control Wizard         You have successfully completed the Delegation of wizard.         You chose to delegate control of objects in the following Active Directory folder:         DI.IPDR/Users         The groups, users, or computers to which you have given control are:         Domain Admins (DI\Domain Admins)	Control

19. Click Finish.

## 2.1.4 Add Machines to the Domain

- 1. Right-click the network icon in the task bar, on a computer that you wish to add to the domain.
- 2. Click Open Network and Sharing Center.

-	Network and Sharing Cen			- S.A
🍥 – 🛧 💐 🕨 Control P	Panel   Network and Internet  Network and Sharing Center	r v C	Search Control Panel	
Control Panel Home	View your basic network information and s	set up connections		
Change adapter settings	View your active networks			
Change advanced sharing settings	Network Public network	Access type: Internet Connections: Internet	D	
	Change your networking settings			
	Set up a new connection or network Set up a broadband, dial-up, or VPN connecti	ion; or set up a router or acces	is point.	
	Troubleshoot problems Diagnose and repair network problems, or ge	at troubleshooting information		
	biogrose and repair netholic problems, or ge			
See also				
See also Internet Options				

3. Click the name of the internet adapter.

Contraction of the second s	
General	
Connection	
IPv4 Connectivity	: Interne
IPv6 Connectivity	No Internet access
Media State:	Enabled
Duration:	02:16:05
Speed:	1.0 Gbp
Details	
Activity	
Activity	Sent — Received
Activity Bytes:	Sent — Received 3,043,324 2,073,372
Bytes:	3,043,324   2,073,372
Bytes:	3,043,324 2,073,373

	Gigabit Network Connecti	
		Configure
This connection uses	the following items:	
Client for Micro	osoft Networks	
File and Printe	er Sharing for Microsoft Net	tworks
QoS Packet S	cheduler	
A Microsoft Net	work Adapter Multiplexor P	rotocol
🗹 🚣 Link-Layer To	pology Discovery Mappe	r I/O Driver
		and Durier
🗹 📥 Link-Layer To	pology Discovery Respor	A. M.
	pology Discovery Respor col Version 6 (TCP/IPv6)	
🗹 🛶 Internet Proto		A. M.
🗹 🛶 Internet Proto	col Version 6 (TCP/IPv6)	A. M.
Internet Proto     Internet Proto	col Version 6 (TCP/IPv6) col Version 4 (TCP/IPv4)	nder
Internet Proto     Install  Description	col Version 6 (TCP/IPv6) col Version 4 (TCP/IPv4)	nder Properties

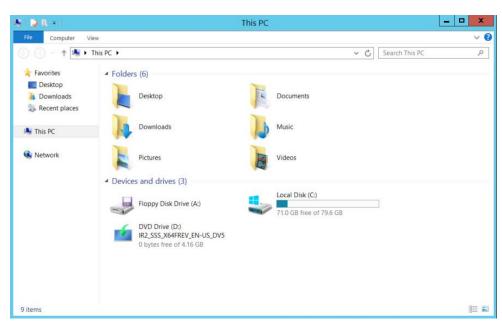
- 5. Double-click Internet Protocol Version 4 (TCP/IPv4).
- 6. Select Use the following DNS server addresses.
- 7. Enter the IP address of the DNS server.

General Alter	nate Configuration				
supports this	P settings assigned auto capability. Otherwise, y for the appropriate IP s	ou need to			ork
Obtain a	In IP address automatic	ally			
Use the	following IP address:				
IP address				19	
Subnet ma	isk:		-	34	1
Default ga	teway:	- N	÷.	12	1
-	DNS server address auto following DNS server a				
Preferred	DNS server:	192.16	8.78	3.4	
Alternate (	ONS server:				
Validat	e settings upon exit			Advi	anced
			OK	1	Can

#### 9. Click **OK.**

General		
Connection -	11	
IPv4 Connect	ivity:	Interne
IPv6 Connect	ivity:	No Internet access
Media State:		Enabled
Duration:		02:30:01
Speed:		1.0 Gbp:
Details		
Details	Sent —	Received
Details	Sent — 3,043,845	- Received

- 10. Click Close.
- 11. Navigate to This PC.



### 12. Right-click in the window, and click Properties.

R.			System	
	🕥 – 🛧 🍓 🕨 Control P	anel   System and Security   System and Secu	tem	✓ C Search Control Panel
	Control Panel Home	View basic information	about your computer	
V	Device Manager	Windows edition		
V	Remote settings	Windows Server 2012 R2 S	Windows Server 2012 R2 Standard	
¥	Advanced system settings			Windows Server 2012 R
		System		
		Processor:	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz 2.20 GHz	
		Installed memory (RAM):	8.00 GB	
		System type:	64-bit Operating System, x64-based processor	
		Pen and Touch:	No Pen or Touch Input is available for this Display	
		Computer name, domain, and	workgroup settings	
		Computer name:	REMOTEDESKTOP1	Schange settings
		Full computer name:	REMOTEDESKTOP1	
		Computer description:		
		Workgroup:	WORKGROUP	
		Windows activation		
		Windows is not activated.	Read the Microsoft Software License Terms	
		Product ID: 00252-70000-	00000-AA535	Activate Window
	See also			
	Action Center			
	Windows Update			

#### 13. Click Change Settings.

Computer Name Hardware Advanced Remote Windows uses the following information to identify your of the network. Computer description: For example: "IIS Production Server" of Server". Full computer name: REMOTEDESKTOP1 Workgroup: WORKGROUP To rename this computer or change its domain or workgroup, click Change. Click Change. Click Change. Click Change. Computer Name/Domain Change You can change the name and the membership of this of Changes might affect access to network resources. Computer name: REMOTEDESKTOP1 Full computer name: REMOTEDESKTOP1 Full computer name: REMOTEDESKTOP1 Full computer name: REMOTEDESKTOP1 Full computer name: REMOTEDESKTOP1	
the network. Computer description: For example: "IIS Production Server" o Server". Full computer name: REMOTEDESKTOP1 Workgroup: WORKGROUP To rename this computer or change its domain or workgroup, click Change. OK Cancel Click Change. elect Domain. Computer Name/Domain Change You can change the name and the membership of this of Changes might affect access to network resources. Computer name: REMOTEDESKTOP1 Full computer name:	"Account
For example: "IIS Production Server" o Server". Full computer name: REMOTEDESKTOP1 Workgroup: WORKGROUP To rename this computer or change its domain or workgroup, click Change. Ick Change. elect Domain. nter the domain. Computer Name/Domain Change You can change the name and the membership of this of Changes might affect access to network resources. Computer name: REMOTEDESKTOP1 Full computer name:	Change
Server". Full computer name: REMOTEDESKTOP1 Workgroup: WORKGROUP To rename this computer or change its domain or workgroup, click Change. OK Cancel Iick Change. elect Domain. nter the domain. Computer Name/Domain Change You can change the name and the membership of this of Changes might affect access to network resources. Computer name: REMOTEDESKTOP1 Full computer name:	Change
Workgroup:       WORKGROUP         To rename this computer or change its domain or workgroup. click Change.         OK       Cancel         Iick Change.         elect Domain.         Inter the domain.         Computer Name/Domain Change         You can change the name and the membership of this of Changes might affect access to network resources.         Computer name:         REMOTEDESKTOP1         Full computer name:	
To rename this computer or change its domain or workgroup, click Change.	
OK       Cancel         Ilick Change.       Cancel         elect Domain.       Computer Name/Domain Change         You can change the name and the membership of this of Changes might affect access to network resources.       Computer name:         REMOTEDESKTOP1       Full computer name:	
lick Change. elect Domain. nter the domain. Computer Name/Domain Chang You can change the name and the membership of this of Changes might affect access to network resources. Computer name: REMOTEDESKTOP1 Full computer name:	Apj
nter the domain. Computer Name/Domain Chang You can change the name and the membership of this of Changes might affect access to network resources. Computer name: REMOTEDESKTOP1 Full computer name:	
You can change the name and the membership of this of Changes might affect access to network resources. Computer name: REMOTEDESKTOP1 Full computer name:	
Changes might affect access to network resources. Computer name: REMOTEDESKTOP1 Full computer name:	es
REMOTEDESKTOP1 Full computer name:	ompute
Full computer name:	
REMOTEDESKTOP1	
	More
Mamharaf	
Member of	
Domain:     DUPDR	
Dirok	
O Workgroup:	
WORKGROUP	
ОК	

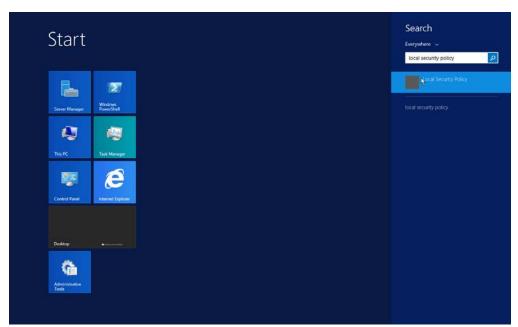
- 17. Click OK.
- 18. Enter the name and password of an account with privileges to add computers to the domain.

	Windows Security	x
	Computer Name/Domain Changes Enter the name and password of an account with permission to join the domain.	9
	DI\Administrator	
	OK Cance	
9 (	Click <b>OK</b> .	a
5	Computer Name/Domain Changes	
	You must restart your computer to appl these changes Before restarting, save any open files and close all programs.	у
	OK	

20. Click **OK** when prompted to restart the computer.

## 2.1.5 Configure Active Directory to Audit Account Activity

1. Open the **Start** Menu.



- 2. Enter Local Security Policy in the search bar, and open the program.
- 3. Navigate to Local Policies > Audit Policy.
- 4. Right-click Audit account management.

	Local Security Policy	
File       Action       View       Help         Image: Security Settings       Image: Security Policies         Image: Security Options       Image: Security Options         Image: Security Options       Image: Software Restriction Policies         Image: Software Restriction Policies       Image: Software Restriction Policies	Policy  Audit account logon events Audit account Nanagement Audit directory service access Audit logon events Audit object access Audit policy change Audit privilege use Audit privilege use Audit process tracking Audit system events Audit system events	Security Setting No auditing No auditing No auditing No auditing No auditing No auditing No auditing No auditing No auditing
<		

5. Click Properties.

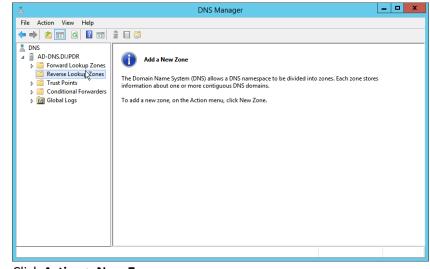
6. Check the boxes next to Success and Failure.

A	udit account management Properties [ ?	
Local Security S	etting Explain	
Audit	account management	
Audit these		
Succes	S	
✓ Failure		
🔔 overrid	etting might not be enforced if other policy is configured to fe category level audit policy. pre information, see <u>Audit account management</u> . (Q921468)	20.00
	OK Cancel Ap	ply

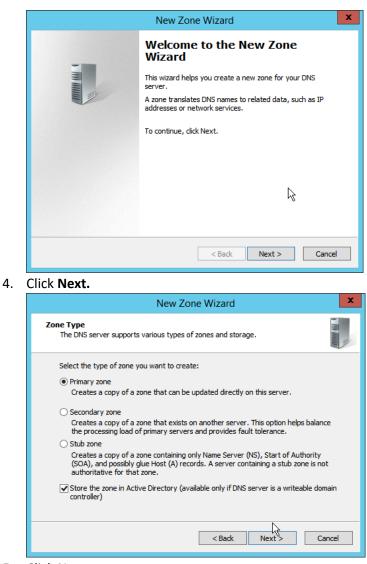
7. Click **OK.** 

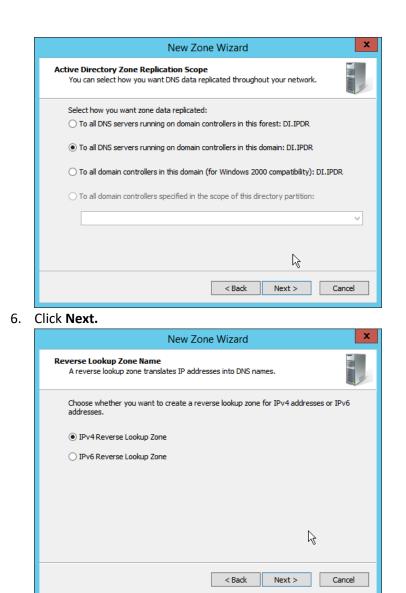
## 2.1.6 Configure Reverse Lookup Zones

- 1. Open DNS Manager by right-clicking the DNS server in Server Manager.
- 2. Click Reverse Lookup Zones.



3. Click Action > New Zone.





- 7. Click Next.
- 8. Enter the first three parts of the IP address of the AD/DNS server (for example, 192.168.1).

	New Zone Wizard
Re	A reverse lookup zone translates IP addresses into DNS names.
	To identify the reverse lookup zone, type the network ID or the name of the zone.
Click	<back next=""> Cancel</back>
	New Zone Wizard
Dy	ynamic Update You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
	<ul> <li>Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.</li> <li>Select the type of dynamic updates you want to allow: <ul> <li>Allow only secure dynamic updates (recommended for Active Directory) This option is available only for Active Directory-integrated zones.</li> <li>Allow both nonsecure and secure dynamic updates pynamic updates of resource records are accepted from any client.</li> <li>This option is a significant security vulnerability because updates can be accepted from untrusted sources.</li> <li>Do not allow dynamic updates pynamic updates pynamic updates of resource records are not accepted by this zone. You must update these records manually.</li> </ul> </li> </ul>

10. Click Next.

New Zone Wizard
Completing the New Zone Wizar
You have successfully completed the New Zone Wizard. You specified the following settings:
Name: 1.168.192.in-addr.arpa
Type: Active Directory-Integrated Primary
Lookup type: Reverse
×
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.
To close this wizard and create the new zone, click Finish.
< Back Finish Cano

- 11. Click Finish.
- 12. Click on the newly created reverse lookup zone.

å	[	ONS Manager		_ 🗆 X				
File Action View Help								
<ul> <li>DNS</li> <li>DNS</li> <li>AD-DNS.DI.IPDR</li> <li>Forward Lookup Zones</li> <li>Reverse Lookup Zones</li> <li>I.168.192.in-addr.arp</li> <li>Trust Points</li> <li>Conditional Forwarders</li> <li>Global Logs</li> </ul>	Name (same as parent folder) (same as parent folder)	Type Start of Authority (SOA) Name Server (NS)	Data [1], ad-dns.di.ipdr., hostm ad-dns.di.ipdr.	Timestamp static static				
< III >								

- 13. Right-click in the window and select New Pointer (PTR)....
- 14. Enter the IP address of the AD/DNS server.
- 15. Enter the **hostname** of the AD/DNS server.

_	New Resource Record
ſ	Pointer (PTR)
	Host I <u>P</u> Address:
	192.168.1.12
	Eully qualified domain name (FQDN):
	12. 1. 168. 192. in-addr.arpa
	Host name:
	ad-dns.di.ipdr Browse
	k}
L	OK Cancel
-	ick <b>OK.</b>
CI	
ار ۱	
å	

å		DNS Manager		_ <b>□</b> ×
File Action View Help				
🗢 🄿 📶 🛅 🗔 🔒 👔				
<ul> <li>DNS</li> <li>A-DNS.DI.IPDR</li> <li>Forward Lookup Zones</li> <li>Reverse Lookup Zones</li> <li>1.168.192.in-addr.arp</li> <li>Trust Points</li> <li>Conditional Forwarders</li> <li>III Global Logs</li> </ul>	Name (same as parent folder)	Type Start of Authority (SOA) Name Server (NS) Pointer (PTR)	Data [1], ad-dns.di.ipdr., hostm ad-dns.di.ipdr ad-dns.di.ipdr	Timestamp static static
<				

## 2.2 Microsoft Exchange Server

As part of our enterprise emulation, we include a Microsoft Exchange server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-26.

## 2.2.1 Install Microsoft Exchange

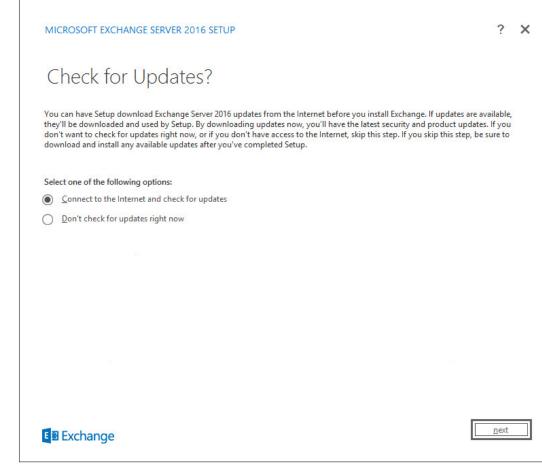
- 1. Run Exchange2016-x64.exe.
- 2. Choose the directory for the extracted files.

Choose Directo	ry For Extracted File	5
	es\Microsoft\Exchar	

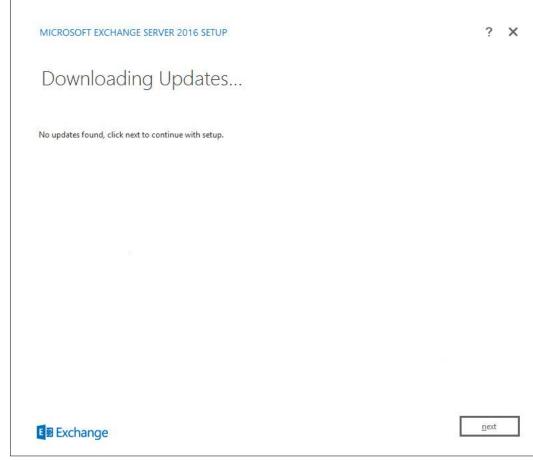
3. Click OK.

🕞 🕕 = 1	Application Tools	Exchar	nge Server		
ile Home Sha	re View Manage				
) 🕘 🔻 🕇 🚺 «	Local Disk (C:) 🔸 Program Files 🕨 Microsoft 🕨	Exchange Server 🕨	~ C	Search Exchange Server	
<b>Favorites</b>	Name	Date modified	Туре	Size	
Desktop	sı sı	8/14/2017 10:22 AM	File folder		
🚺 Downloads	sv sv	8/14/2017 10:22 AM	File folder		
🔛 Recent places	sw	8/14/2017 10:22 AM	File folder		
	ta ta	8/14/2017 10:22 AM	File folder		
💂 This PC	te te	8/14/2017 10:22 AM	File folder		
	th th	8/14/2017 10:22 AM	File folder		
Network	📕 tr	8/14/2017 10:22 AM	File folder		
	uk uk	8/14/2017 10:22 AM	File folder		
	🚡 ur	8/14/2017 10:22 AM	File folder		
	\mu vi	8/14/2017 10:22 AM	File folder		
	🎉 zh-hans	8/14/2017 10:22 AM	File folder		
	퉬 zh-hant	8/14/2017 10:22 AM	File folder		
	autorun 👔	9/20/2015 4:41 AM	Setup Information	1 KB	
	🕞 exchangeserver	9/20/2015 4:41 AM	Windows Installer	22,388 KB	
	imicrosoft.exchange.cabutility.dll	9/20/2015 4:41 AM	Application extens	278 KB	
	🗟 microsoft.exchange.data.common.dll	9/20/2015 4:41 AM	Application extens	1,684 KB	
	microsoft.exchange.diagnostics.dll	9/20/2015 4:41 AM	Application extens	1,648 KB	
	🚳 microsoft.exchange.setup.acquirelangu	a 9/20/2015 4:41 AM	Application extens	68 KB	
	microsoft.exchange.setup.bootstrapper	.c 9/20/2015 4:41 AM	Application extens	90 KB	
	inicrosoft.exchange.setup.signverfwrap	p 9/20/2015 4:41 AM	Application extens	83 KB	
	setup	9/20/2015 4:41 AM	Application	31 KB	

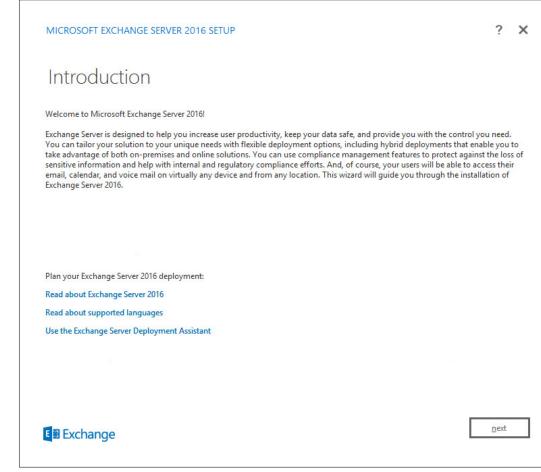
- 4. Enter the directory and run **setup.exe.**
- 5. Select Connect to the Internet and check for updates.



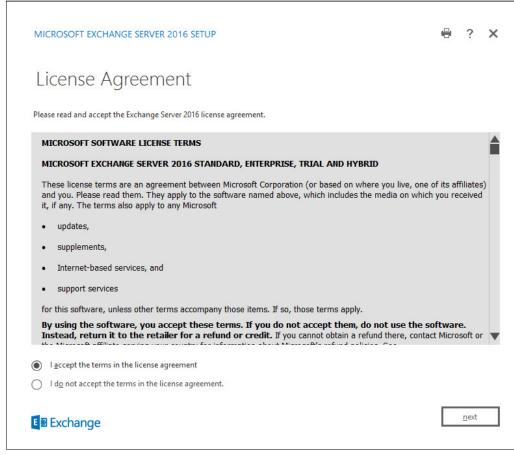
- 6. Click Next.
- 7. Wait for the check to finish.



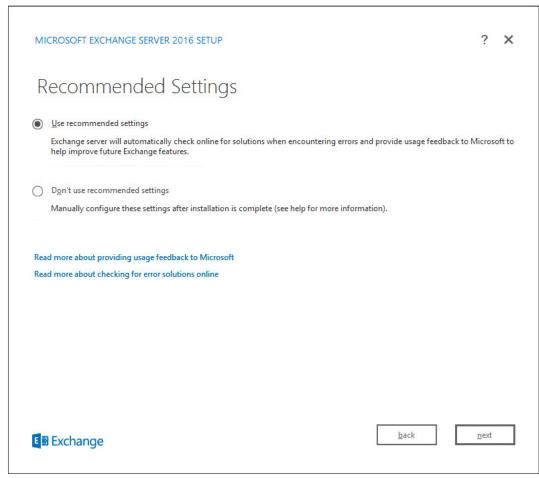
- 8. Click Next.
- 9. Wait for the copying to finish.



- 10. Click Next.
- 11. Click I accept the terms in the license agreement.



13. Click Use Recommended Settings.



- 14. Click Next.
- 15. Check Mailbox role.
- 16. Check Automatically install Windows Server roles and features that are required to install Exchange Server.

MICROSOFT EXCHANGE SERVER 2016 SETUP	? X
Server Role Selection	
Select the Exchange server roles you want to install on this computer:         Mailbox role         Management tools         Edge Transport role	
Automatically install <u>W</u> indows Server roles and features that are required to install Exchange Server	
E S Exchange	next

18. Specify the installation path for MS Exchange.

MICROSOFT EXCHANGE SERVER 2016 SETUP	?	×
Installation Space and Location		
Disk space required: 8696.2 MB Disk space available: 19407.9 MB		
Specify the path for the Exchange Server installation: C:\Program Files\Microsoft\Exchange Server\V15 b_cowse		
E Exchange	<u>n</u> ext	

- 19. Click Next.
- 20. Specify the name for the Exchange organization, for example, DI.
- 21. Decide whether to apply split permissions, based on the needs of the enterprise.

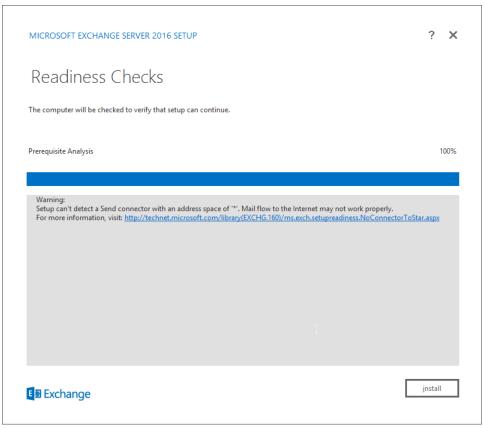
MICROSOFT EXCHANGE SERVER 2016 SETUP	?	×
Exchange Organization		
Specify the name for this Exchange organization:		
Apply Active Directory split permissions security model to the Exchange organization The Active Directory split permissions security model is typically used by large organizations that completely separate for the management of Exchange and Active Directory among different groups of people. Applying this security mod ability for Exchange servers and administrators to create Active Directory objects such as users, groups, and contacts. manage non-Exchange attributes on those objects is also removed. You shouldn't apply this security model if the same person or group manages both Exchange and Active Directory. Cl information.	el removes the The ability to	
Exchange	<u>n</u> ext	

- 22. Click Next.
- 23. Select No.

MI	CROSOFT EXCHANGE SERVER 2016 SETUP	?
Ν	1alware Protection Settings	
	ware scanning helps protect your messaging environment by detecting messages that may contain viruses or spy ed off, replaced, or paired with other premium services for layered protection.	ware. It can be
	ware scanning is enabled by default. However, you can disable it if you're using another product for malware scan ose to disable malware scanning now, you can enable it at any point after you've installed Exchange.	ning. If you
Disa	ble malware scanning.	
0	<u>Y</u> es	
۲	No	
Inte	rnet access is required to download the latest anti-malware engine and definition updates.	

- 24. Click Next.
- 25. Install any **prerequisites** listed.

26. If necessary, restart the server and re-run **setup.exe**, completing steps 3-22 again.



27. Click Install.

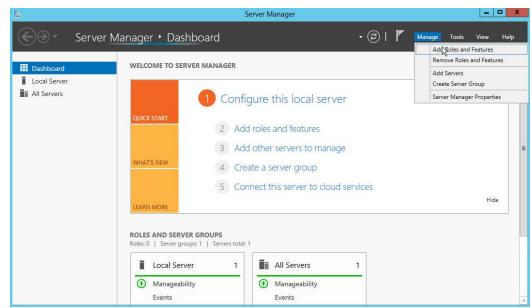
## 2.3 Windows Server Hyper-V Role

As part of our simulated enterprise, we include a Windows Hyper-V server. This section covers the instructions for installing Windows Server Hyper-V on a Windows Server 2012 R2 machine.

The instructions for enabling the Windows Server Hyper-V Role are retrieved from <u>https://technet.microsoft.com/en-us/library/hh846766(v=ws.11).aspx</u> and are replicated below for preservation and ease of use.

## 2.3.1 Production Installation

1. In Server Manager, on the Manage menu, click Add Roles and Features.



2. On the **Before you begin** page, verify that your destination server and network environment are prepared for the role and feature you want to install.

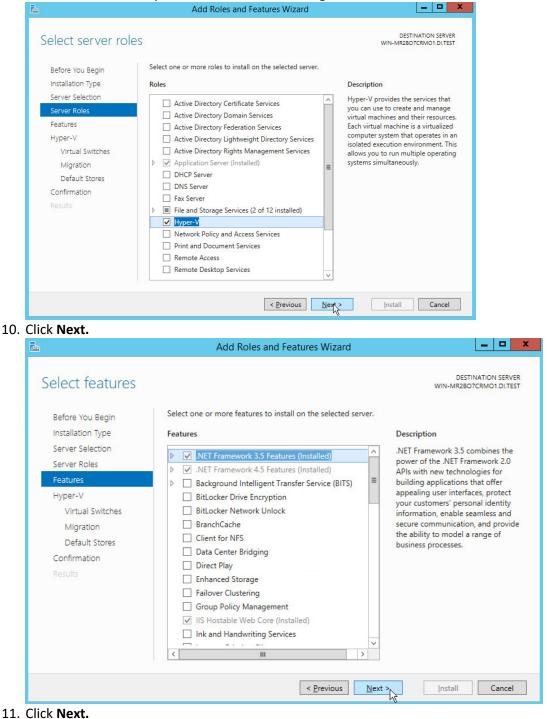
<b>b</b>	Add Roles and Features Wizard	_ 0	x
Before you begin	DESTI WIN-MR2BO	NATION SER CRMO1.DI.1	
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	This wizard helps you install roles, role services, or features. You determine which roles, rol features to install based on the computing needs of your organization, such as sharing de hosting a website.         To remove roles, role services, or features:         Start the Remove Roles and Features Wizard         Before you continue, verify that the following tasks have been completed:         • The Administrator account has a strong password         • Network settings, such as static IP addresses, are configured         • The most current security updates from Windows Update are installed         If you must verify that any of the preceding prerequisites have been completed, close the complete the steps, and then run the wizard again.         To continue, click Next.	ocuments,	
	< Previous Install	Canc	el

- 3. Click Next.
- 4. On the Select installation type page, select Role-based or feature-based installation.

Select installation	on type Destination se Win-Mr2807crM01.Di
Before You Begin Installation Type	Select the installation type. You can install roles and features on a running physical computer or vi machine, or on an offline virtual hard disk (VHD).
Server Selection Server Roles	<ul> <li>Role-based or feature-based installation</li> <li>Configure a single server by adding roles, role services, and features.</li> <li>Remote Desktop Services installation</li> </ul>
Features Confirmation Results	Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine- or session-based desktop deployment.
	< <u>Previous</u> <u>Net</u> Install Can
Click <b>Next.</b> On the <b>Select dest</b>	tination conver page, select a conver from the conver pool
On the <b>Select dest</b>	tination server page, select a server from the server pool. Add Roles and Features Wizard
On the <b>Select dest</b>	Add Roles and Features Wizard
On the <b>Select dest</b>	Add Roles and Features Wizard
On the <b>Select dest</b>	Add Roles and Features Wizard
On the Select dest	Add Roles and Features Wizard  DESTINATION SERV  WIN-MR2807CRM01.DLTE  Select a server or a virtual hard disk on which to install roles and features.  Select a server from the server pool
Don the Select dest Select destination Before You Begin Installation Type Server Selection	Add Roles and Features Wizard  DESTINATION SERV WIN-MR22607CRM01.DLTE  Select a server or a virtual hard disk on which to install roles and features.  Select a server from the server pool Select a virtual hard disk
On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles	Add Roles and Features Wizard  DESTINATION SERV  WIN-MR2807CRM01.DLTE  Select a server or a virtual hard disk on which to install roles and features.  Select a server from the server pool
On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles Features	Add Roles and Features Wizard  DESTINATION SERV WIN-MR22607CRM01.DLTE  Select a server or a virtual hard disk on which to install roles and features.  Select a server from the server pool Select a virtual hard disk
On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles	Add Roles and Features Wizard  DESTINATION SER  ON SERVER  Select a server or a virtual hard disk on which to install roles and features.  Select a server from the server pool  Select a virtual hard disk Server Pool  Filter:
On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation	Add Roles and Features Wizard       DESTINATION SERVER       Select a server or a virtual hard disk on which to install roles and features.       © Select a server from the server pool       O Select a virtual hard disk       Server Pool       Filter:       Name     IP Address       Operating System
On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation	Add Roles and Features Wizard  DESTINATION SER  ON SERVER  Select a server or a virtual hard disk on which to install roles and features.  Select a server from the server pool  Select a virtual hard disk Server Pool  Filter:
On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation	Add Roles and Features Wizard       DESTINATION SERVER       Select a server or a virtual hard disk on which to install roles and features.       © Select a server from the server pool       O Select a virtual hard disk       Server Pool       Filter:       Name     IP Address       Operating System
On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation	Add Roles and Features Wizard       DESTINATION SERVER       Select a server or a virtual hard disk on which to install roles and features.       © Select a server from the server pool       O Select a virtual hard disk       Server Pool       Filter:       Name     IP Address       Operating System

- 7. Click Next.
- 8. On the Select server roles page, select Hyper-V.

## 9. To add the tools that you use to create and manage virtual machines, click Add Features.



	Add Roles and Features Wizard
Hyper-V	DESTINATION SER WIN-MR2B07CRM01.DLT
Before You Begin Installation Type Server Selection Server Roles Features Hyper-V Virtual Switches Migration Default Stores Confirmation Results	<ul> <li>Hyper-V allows you to virtualize your server workloads by running those workloads on virtual maching You can use virtual machines to consolidate multiple workloads on one physical server, to improve server availability, and to increase efficiency in developing and testing software.</li> <li>Things to note: <ul> <li>Before you install this role, you should identify which network connections on this server you wan use for setting up virtual switches.</li> <li>After you install Hyper-V, you can use Hyper-V Manager to create and configure your virtual machines.</li> </ul> </li> </ul>
	More information about Hyper-V
	< <u>P</u> revious <u>Next</u> Install Cance
on the <b>Create Virtu</b>	< Previous

Next >

Cancel

Install

< <u>P</u>revious

### 15. On the Virtual Machine Migration page, select the appropriate options.

Before You Begin Installation Type Server Selection Server Roles Features Hyper-V Virtual Switches Migration Default Stores Confirmation Results	<ul> <li>Hyper-V can be configured to send and receive live migrations of virtual machines on this server. Configuring Hyper-V now enables any available network on this server to be used for live migratio you want to dedicate specific networks for live migrations, use Hyper-V settings after you install the</li> <li>Allow this server to send and receive live migrations of virtual machines</li> <li>Authentication protocol</li> <li>Select the protocol you want to use to authenticate live migrations.</li> <li> <ul> <li>● Use Credential Security Support Provider (CredSSP)</li> <li>This protocol is less secure than Kerberos, but does not require you to set up constrained delegation. To perform a live migration, you must be logged on to the source server.</li> <li>○ Use Kerberos</li> <li>This protocol is more secure but requires you to set up constrained delegation in your environment to perform tasks such as live migration when managing this server remotely.</li> </ul> </li> <li> All this server will be part of a cluster, do not enable migration now. Instead, you will configure server for live migration, including specifying networks, when you create the cluster. </li> </ul>
--	---

### 17. On the **Default Stores** page, select the appropriate options.

Default Stores	UESTINA WIN-MR2B07C	RMO1.DI.TE
Before You Begin Installation Type Server Selection Server Roles	Hyper-V uses default locations to store virtual hard disk files and virtual machine configura unless you specify different locations when you create the files. You can change these defa now, or you can change them later by modifying Hyper-V settings. Default location for virtual hard disk files:	
Features	C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks	Brows
Hyper-V	Default location for virtual machine configuration files:	
Virtual Switches	C:\ProgramData\Microsoft\Windows\Hyper-V	Brows
Migration		
Default Stores		
Confirmation		
	< Previous N4.2 > Install	Cance

19. On the **Confirm installation selections** page, select **Restart the destination server automati**cally if required.

Ъ	Add Roles and Features Wizard	_ <b>D</b> X
Confirm installa Before You Begin Installation Type Server Selection Server Roles Features Hyper-V Virtual Switches Migration Default Stores Confirmation Results	tion selections To install the following roles, role services, or features of Restart the destination server automatically if requ Optional features (such as administration tools) might I been selected automatically. If you do not want to insta- their check boxes. Hyper-V Remote Server Administration Tools Role Administration Tools Hyper-V Management Tools Hyper-V Module for Windows PowerSh Hyper-V GUI Management Tools Export configuration settings Specify an alternate source path	ired be displayed on this page because they have all these optional features, click Previous to clear
	< <u>P</u> revious	Next > Install Cancel

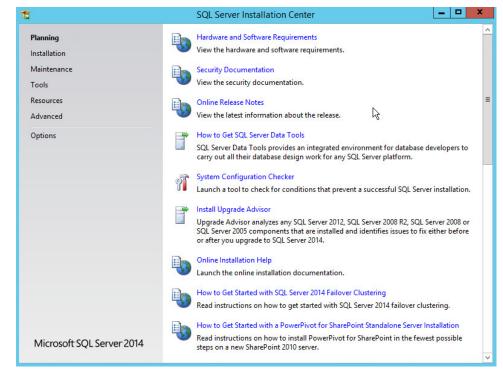
- 20. Click Install.
- 21. When installation is finished, verify that Hyper-V installed correctly. Open the **All Servers** page in Server Manager, and select a server on which you installed Hyper-V. Check the **Roles and Features** tile on the page for the selected server.

# 2.4 MS SQL Server

As part of both our enterprise emulation and data integrity solution, we include a Microsoft Structured Query Language (SQL) Server. This section covers the installation and configuration process used to set up Microsoft SQL Server on a Windows Server 2012 R2 machine.

# 2.4.1 Install and Configure MS SQL

- 1. Acquire SQL Server 2014 Installation Media.
- 2. Locate the installation media in the machine and click on SQL2014\_x64\_ENU to launch SQL Server Installation Center.



### 3. On the left menu, select Installation.

<b>1</b>	SQL Server Installation Center
Planning Installation Maintenance Tools Resources Advanced Options	<ul> <li>New SQL Server stand-alone installation or add features to an existing installation</li> <li>Launch a wizard to install SQL Server 2014 in a non-clustered environment or to add features to an existing SQL Server 2014 instance.</li> <li>New SQL Server failover cluster installation</li> <li>Launch a wizard to install a single-node SQL Server 2014 failover cluster.</li> <li>Add node to a SQL Server failover cluster</li> <li>Launch a wizard to add a node to an existing SQL Server 2014 failover cluster.</li> <li>Upgrade from SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012</li> <li>Launch a wizard to upgrade SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012</li> </ul>
Microsoft SQL Server 2014	

- 4. Select **New SQL Server stand-alone installation or add features to an existing installation.** This will launch the SQL Server 2014 setup.
- 5. In the **Product Key** section, enter your product key.

1	SQL Server 2014 Setup	-		x	
Product Key Specify the edition of SQL Server Specify the edition of SQL Server Product Key License Terms Global Rules Product Updates Install Setup Files Install Setup Files Install Rules Setup Role Feature Selection Feature Rules Feature Configuration Rules Ready to Install Installation Progress		erver, d in S	such	x	
Complete	< Back	C	ancel		]

- 6. Click Next.
- 7. In the License Terms section, read and click I accept the license terms.

1	SQL Server 2014 Setup
License Terms To install SQL Server 2014, Product Key License Terms Global Rules Product Updates Install Setup Files Install Rules Setup Role	you must accept the Microsoft Software License Terms.  MICROSOFT SOFTWARE LICENSE TERMS  MICROSOFT SQL SERVER 2014 ENTERPRISE SERVER/CAL EDITION  These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft  updates,
Feature Selection Feature Rules Feature Configuration Rules Ready to Install Installation Progress Complete	updates,     updates,     supplements,

### 9. In the Install Rules section, note and resolve any further conflicts.

1	SQL Server 2014 Setup		-		x
Install Rules Setup rules identify potential pr can continue.	oblems that might occur while running Setup. Failures must be correcte	ed before Setup			
Product Key License Terms Global Rules Product Updates Install Setup Files Install Rules	Operation completed. Passed: 6. Failed 0. Warning 1. Skipped 0. Hide details << <u>View detailed report</u>			<u>R</u> e-ru	ın
Setup Role Feature Selection Feature Rules Feature Configuration Rules Ready to Install Installation Progress Complete	Rule         Image: Second Se	Status Passed Passed Passed Passed Warning Passed			
	< <u>B</u> ack	Cancel	ł	Help	

### 11. In the Setup Role section, select SQL Server Feature Installation.

1	SQL Server 2014 Setup
Setup Role Click the SQL Server Feature In feature role to install a specific	stallation option to individually select which feature components to install, or click a configuration.
Product Key License Terms Global Rules Product Updates Install Setup Files Install Rules Setup Role Feature Selection Feature Rules Feature Configuration Rules Ready to Install Installation Progress Complete	<ul> <li>SQL Server Feature Installation Install SQL Server Database Engine Services, Analysis Services, Reporting Services, Integration Services, and other features.</li> <li>SQL Server PowerPivot for SharePoint Install PowerPivot for SharePoint on a new or existing SharePoint server to support PowerPivot data access in the farm. Optionally, add the SQL Server relational database engine to use as the new farm's database server.</li> <li>Add SQL Server Database Relational Engine Services to this installation.</li> <li>All Features With Defaults Install all features using default values for the service accounts.</li> </ul>
	< <u>B</u> ack <u>Next</u> > Cancel Help

- 12. Click Next.
- 13. In the Feature Selection section, select the following:
  - a. Database Engine Services
  - b. Client Tools Connectivity
  - c. Client Tools Backwards Compatibility
  - d. Client Tools SDK
  - e. Management Tools Basic
  - f. Management Tools Complete
  - g. SQL Client Connectivity SDK
  - h. Any other desired features

Feature Selection	SQL Server 2014 Setup	
Select the Enterprise features to	o install.	
Product Key	<u>F</u> eatures:	Feature description:
License Terms Global Rules Product Updates Install Setup Files Install Rules Setup Role Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules	Instance Features         Image: Construct of the service of the serv	Prerequisites for selected features:     Already installed:     Windows PowerShell 2.0     Microsoft_NFT Framework 3.5     Soft Disk Space Requirements     Drive C: 2534 MB required, 21593 MB available
Ready to Install Installation Progress Complete	Shared feature directory: C:\Program Files	\Microsoft SQL Server\ \Microsoft SQL Server\ (x86)\Microsoft SQL Server\

## 15. In the Instance Configuration section, select Default instance.

1		SQL Server 2014	Setup		_ 🗆 X
Instance Configuration Specify the name and instance		QL Server. Instance	ID becomes part of t	he installation path.	
Product Key License Terms Global Rules	Default instance Named instance:	MSSQLSERVER			
Product Updates Install Setup Files Install Rules Setup Role	etup Files Instance ID: MSSQLSERVER ules				
Setup Role Feature Selection Feature Rules Instance Configuration	SQL Server directory: Insta <u>l</u> led instances:	C:\Program Files\M	∕licrosoft SQL Server∖	MSSQL12.MSSQLSERVER	
Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	Instance Name	Instance ID	Features	Edition	Version
		[	< <u>B</u> ack	Ne > Cancel	Help

Server Configuration	d collation configuration.				
Product Key License Terms Global Rules	Service Accounts Collation	use a separate account for each	SQL Server serv	ice.	
Product Updates	Service	Account Name	Password	Startup Type	2
Install Setup Files	SQL Server Agent	NT Service\SQLSERVERA		Manual	~
Install Rules	SQL Server Database Engine	NT Service\MSSQLSERVER		Automatic	~
Setup Role	SQL Server Browser	NT AUTHORITY\LOCAL		Disabled	~
Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules					
Ready to Install Installation Progress Complete					

- 17. In the Server Configuration section, click Next.
- 18. In the Database Engine Configuration section, make sure Mixed Mode is selected.
- 19. Add all desired users as Administrators under Specify SQL Server Administrators by pressing Add Current User.
  - a. For Domain accounts, type in **\$DOMAINNAME\\$USERNAME** into **Enter the object names to select** textbox.
  - b. Click OK.
  - c. For local computer accounts, click on **locations** and select the computer's name.
  - d. Click OK.
  - e. Type the username into the Enter the object names to select textbox.
  - f. Once you are finished adding users, click Next.

Database Engine Conf	iguration				
Specify Database Engine auth	entication security mode, adr	ministrators and	data directories.		
Product Key License Terms Global Rules Product Updates Install Setup Files Install Rules Setup Role Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	Server Configuration D Specify the authentica Authentication Mode Windows authentic Mixed Mode (SQL S Specify the password Enter password: Confirm password: Specify SQL Server add	tion mode and a ation mode server authentica for the SQL Serve	dministrators for tion and Window er system administ	s authentication)	
	WIN-MR2B07CRM01           Add Current User	\Administrator (	Administrator) move		SQL Server administrato have unrestricted access to the Database Engine.

# 20. In the Ready to install section, verify the installation and click Install.

Ready to Install Verify the SQL Server 2014 featu	ires to be installed.
Product Key License Terms Global Rules Product Updates Install Setup Files Install Rules Setup Role Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules <b>Ready to Install</b> Installation Progress Complete	Ready to install SQL Server 2014:         Summary         Edition: Enterprise         Action: Install (Product Update)         Prerequisites         Arready installed:         Windows PowerShell 2.0         Microsoft .NET Framework 3.5         Microsoft Visual Studio 2010 Redistributables         Microsoft Visual Studio 2010 Redistributables         Microsoft Visual Studio 2010 Shell         General Configuration         Features         Client Tools Backwards Compatibility         Client Tools SDK         Management Tools - Razic         Kanagement Tools - Razic         Configuration file path:

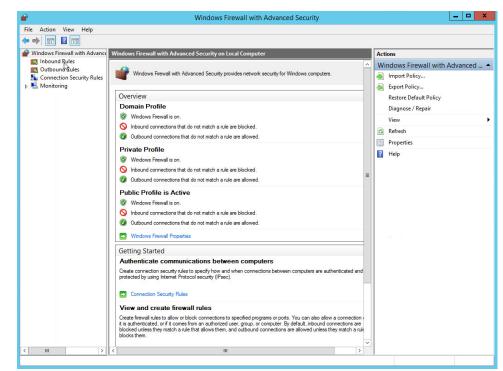
#### 21. Wait for the install to finish.

5	SQL Server 2014 Setu	ip 📃 🗖	
Complete			
Your SQL Server 2014 installa	tion completed successfully with product updates.		
Product Key	Information about the Setup operation or possi	ble next steps:	
License Terms	Feature	Status	1
Global Rules	Management Tools - Complete	Succeeded	
Product Updates	Client Tools Connectivity	Succeeded	
Install Setup Files	Client Tools SDK	Succeeded	
Install Rules	Client Tools Backwards Compatibility	Succeeded	ľ
Setup Role	Management Tools - Basic	Succeeded	
Feature Selection	🐼 Database Engine Services	Succeeded	
Feature Rules			
Instance Configuration	<u>D</u> etails:		
Server Configuration	Viewing Product Documentation for SQ	L Server	
Database Engine Configuration			
Feature Configuration Rules		and manage the documentation for SQL Server have component uses the online library. After installing	
Ready to Install		Vanager component to download documentation to	
Installation Progress		see Use Microsoft Books Online for SQL Server	
Complete	( <http: ?linkid="29&lt;/td" fwlink="" go.microsoft.com=""><td><u>99578&gt;)</u>.</td><td>-</td></http:>	<u>99578&gt;)</u> .	-
	J Summary log file has been saved to the followin	alocation	
	C:\Program Files\Microsoft SQL Server\120\Set MR2BO7CRMO1 20170814 070653.txt	up Bootstrap\Log\20170814_070653\Summary_WIN-	
	MR2B07CRM01_20170814_070653.txt	40	
		Close Help	

22. Click Close.

# 2.4.2 Open Port on Firewall

1. Open Windows Firewall with Advanced Security.



#### 2. Click Inbound Rules.

<b>@</b>	Windows	Firewall with Advanced S	ecurity				
File Action View Help							
🗢 🏟 🙎 📰 🗟 🚺							
Windows Firewall with Advance	Inbound Rules					Actions	
<ul> <li>Windows Firewall with Advance</li> <li>Inbound Rules</li> <li>Othound Rules</li> <li>Othound Rules</li> <li>Connection Security Rules</li> <li>Monitoring</li> </ul>	Name PranchCache Content Retrieval (HTTP-In) BranchCache Peer Discovery (WSD-In) COM- Network Access (DCOM-In) COM- Network Administration (DCOM-In) COM- Retworking - Destination Unreacha Core Networking - IPHTTPS (TCP-In) Core Networking - IPHTTPS (TCP-In) Core Networking - Multicast Listener Rou Core Networking - Multicast Listener Rep Core Networking - Nathicast Core Nathicast	COM+ Network Access COM+ Remote Administrati Core Networking Core Networkin	All All All All All All All All All All	Enabled No No No Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes		Actions       Inbound Rules       In       New Ruffing       Filter by State       Filter by State       Filter by Group       View       Refresh       Export List       Image: Help	
	File and Printer Sharing (Echo Request - I File and Printer Sharing (Echo Request - I File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing File and Printer Sharing File and Printer Sharing	All All All	No No No	A A A		
	File and Printer Sharing (NB-Datagram-In) File and Printer Sharing (NB-Name-In)	File and Printer Sharing File and Printer Sharing	All All	No No	A A		
< III >	< III				>		

3. Click New Rule.

- 4. Select Port.
- 5. Click Next.
- 6. Select **TCP** and **Specific local ports.**
- 7. Type **1433** into the text field.

	New Inbound Rule Wizard	×
Protocol and Ports Specify the protocols and ports	to which this rule applies.	
Specify the protocols and ports I Steps: Protocol and Ports Action Profile Name	to which this rule apply to TCP or UDP?	
	< Back Net > Cancel	

- 8. Click Next.
- 9. Select Allow the connection.

<i>🖌</i>	New Inbound Rule Wizard
Action Specify the action to be taken w	hen a connection matches the conditions specified in the rule.
Steps: Protocol and Ports Action Profile Name	<ul> <li>What action should be taken when a connection matches the specified conditions?</li> <li>Allow the connection         This includes connections that are protected with IPsec as well as those are not.</li> <li>Allow the connection if it is secure         This includes only connections that have been authenticated by using IPsec. Connections         will be secured using the settings in IPsec properties and rules in the Connection Security</li> </ul>
	Rule node.         Customize         O         Block the connection
	< <u>B</u> ack Next > Cancel

- 10. Click Next.
- 11. Select all applicable locations.

<b>@</b>	New Inbound Rule Wizard
Profile Specify the profiles for white	ch this rule applies.
Steps:	When does this rule apply?
<ul> <li>Rule Type</li> <li>Protocol and Ports</li> </ul>	
<ul> <li>Action</li> <li>Profile</li> </ul>	Domain     Applies when a computer is connected to its corporate domain.
Name	<ul> <li>Private         Applies when a computer is connected to a private network location, such as a home         or work place.</li> <li>Public         Applies when a computer is connected to a public network location.</li> </ul>
	< Back Next > Cancel

- 12. Click Next.
- 13. Name the rule Allow SQL Access.

<b>@</b>	New Inbound Rule Wizard	
Name Specify the name and description of	of this rule.	
Steps:		
<ul><li>Rule Type</li><li>Protocol and Ports</li></ul>		
<ul> <li>Action</li> <li>Profile</li> </ul>	Name:	
<ul> <li>Name</li> </ul>	Allow SQL Access	
	Description (optional):	
	< Back Einis	Cancel

14. Click Finish.

# 2.4.3 Add a New Login to the Database

1. Open SQL Server Management Studio.

Edit View Tools Window Help		Server Management Studio (			- 0
• 🔄 • 😂 🕼 🥔 🔔 New Query 🔥 🔂 🔂 🚳 🔺 🖓 🖄	17-17-12-12/12/11			· · · · · · · · · · · · · · · · · · ·	
ct Explorer + 3 ×					
ned• # # # 7 E S					
	-				
	*	Connect to Server	×		
	Microsoft	SQL Server 2014			
			_		
	Server type:	Database Engine			
	Server name:	WALMERSON CREAT	. <del>v</del>		
	Athentication	Windows Authentication	v .		
	User name.	WIN-MR2807CRM01\Admin	istrator 🔍 🔍		
	Password				
		Paranter passed			
	Con	nerd Cancel Help	Options >>		
	10				

- 2. Click **Connect** to connect to the database.
- 3. In the **Object Explorer** window, expand the **Security** folder.

	Microsoft SQL S	Server Management	t Studio (Administrator)		- 0 x
le Edit View Debug Tools Window Help			Constant and the state		
🗊 • 💷 - 🧱 🚽 🔔 New Query 🐚 📆 🔂 🗿	「「「「「」」、「」、「」」」、「」」、「」」、「」」、「」」、「」」、「」」	-		· 🔍 🕆 x 🗈 • .	
bject Dyber + 0 × 0 Connect + 2 × 0 × 0 × 0 0 WM-M02007C8M01 (20): Sover 120. × 0 Dubbases → 0 Soundy × 0 Soler → 0 Controls → 0 Controls → 0 Controls → 0 Controls					
Cryptographic revolues     Colored     Server Audit Specifications     Server Objects     Server Objects     Preplication     Preplication     Server Objects					
<ul> <li>a Averyton High Availabelity</li> <li>Management</li> <li>a Integration Services Catalogs</li> <li>SGL Server Agent (Agent XPs disable)</li> </ul>					
dy					

- 4. Right-click on the Logins folder and click New Login....
- 5. Input the desired user.

Connect * 3/ 32 = 7 2 3	1	Login -	New	- 0 X	
Detabases     Security	Select a page	Sout + D Hep			
Eogins     Server Roles     Eogram Roles     Eogram Condensials     Eogram Cryptographic Providers	Server Roles     Server Roles     Securables     Securables	Login game:	douter1	] Spech	
Audits     Server Audit Specifications		<ul> <li>SQL Server authentication Password</li> </ul>			
Server Objects     Replication		Confirm password		=	
🕫 🧰 AlwaysOn High Availability 🕷 📴 Management		C Specify old pastword			
Integration Services Catalogs     SQL Server Agent (Agent XPs disabl		Enforce password polo			
		Der must change pass			
		<ul> <li>Mapped to ceptilizate</li> <li>Mapped to asymmetric key</li> </ul>	1	(v)	
	Connection	Map to Credential			
	Server: WIN-MR2B07CRM01	Mapped Credentials	Credential Provider		
	Connection: WIN-MR2B07CRM01-Administration				
	Ven correction properties				
	Progress Ready	Default database:	master	Familys	
	0	Default language:	ctelado	v	
			0	Cancel	
				13	

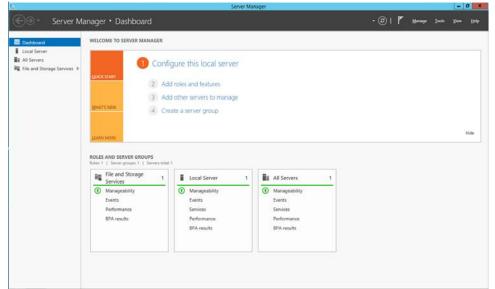
6. Click **OK.** 

# 2.5 Microsoft IIS Server

As part of our enterprise emulation, we include a Microsoft Internet Information Services (IIS) server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine. This was conducted on the same machine as <u>Section 2.4</u>.

# 2.5.1 Install IIS

### 1. Open Server Manager.



### 2. Click Add Roles and Features.

<b>a</b>	Add Roles and Features Wizard
Before you begin	DESTINATION SERVER MSSQLDLIPDR
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website. To remove roles, role services, or features: Start the Remove Roles and Features Wizard Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again. To continue, click Next.
	Skip this page by default <pre></pre>
	< Previous Next > Install Cancel

### 3. Click Next.

#### 4. Select Role-based or feature-based installation.

Select installation	on type Destination see
Before You Begin	Select the installation type. You can install roles and features on a running physical computer or vir
Installation Type	machine, or on an offline virtual hard disk (VHD).
Server Selection	Role-based or feature-based installation
Server Roles	Configure a single server by adding roles, role services, and features.
Features	O Remote Desktop Services installation
	Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-b or session-based desktop deployment.
	< Previous Next > Install Canc

NIST SP 1800-26C: Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events

### 6. Select **MSSQL** (or the correct Windows Server name) from the list.

	Add	Roles and Features V	Vizard	
Select destinati	ion server			DESTINATION SERVER MSSQLDLIPDR
Before You Begin Installation Type Server Selection Server Roles Features	Select a server or a v  Select a server fro Select a virtual ha Server Pool Filter:	om the server pool	to install roles and features.	
Confirmation Results	Name	IP Address	Operating System	
	Add Servers comman	ers that are running Wind	Microsoft Windows Server 2012 dows Server 2012, and that have be line servers and newly-added serve	een added by using the
		< Pre-	vious Next > In	stall Cancel

### 7. Click Next.

elect server roles	5	DESTINATION SER MSSQLDI.IF
Before You Begin Installation Type	Select one or more roles to install on the selected server.	Description
Server Selection		
Server Roles	Application Server DHCP Server	Web Server (IIS) provides a reliab manageable, and scalable Web application infrastructure.
Features	DNS Server	appression must detailed
Confirmation	Fax Server	

### 8. Check the box next to **Web Server (IIS).**

Select server ro	Add Roles and Features Wizard		MSSQLDLIF
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add features that are required for Web Server The following tools are required to manage this feature, b have to be installed on the same server. Web Server (IIS) Management Tools [Tools] IIS Management Console		ion ver (IIS) provides a reliab able, and scalable Web ion infrastructure.
	Include management tools (if applicable) Add Features	Cance	1
	< Previous	Next >	Install
lick Add Features		Next >	Install Cance
lick Add Features		Next >	
	• Add Roles and Features Wizard	Next >	
2	• Add Roles and Features Wizard		
Select server rol	• Add Roles and Features Wizard		

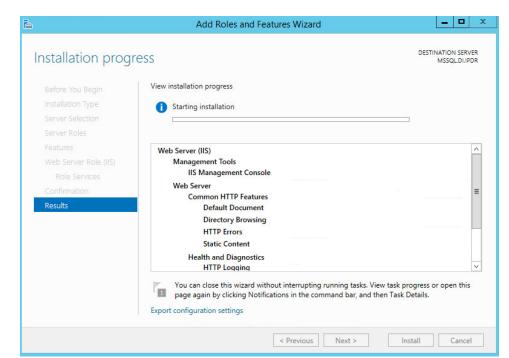
### 11. Ensure that all desired features are selected.

	Add Roles and Features Wizard	_ □
Select features		DESTINATION SERVER MSSQLDLIPDR
Before You Begin	Select one or more features to install on the selected server.	
Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	INET Framework 3.5 Features (1 of 3 installed)     NET Framework 3.5 Features (2 of 7 installed)     Background Intelligent Transfer Service (BITS)     BitLocker Drive Encryption     BitLocker Network Unlock     Grient for NFS	Vescription NET Framework 3.5 combines the ower of the .NET Framework 2.0 PIs with new technologies for uilding applications that offer ppealing user interfaces, protect our customers' personal identity information, enable seamless and ecure communication, and provide he ability to model a range of usiness processes.
	□ IIS Hostable Web Core       □ Ink and Handwriting Services       ✓	
	< Previous Next >	Install Cancel
ick <b>Next.</b>	< Previous Next > Add Roles and Features Wizard	Install Cancel
ick <b>Next.</b> • Web Server Role	Add Roles and Features Wizard	DESTINATION SERVER
B Web Server Role Before You Begin Installation Type Server Selection	Add Roles and Features Wizard	DESTINATION SERVER MSSQLDIJPDR Internet, or through intranets and es (IIS) 8.5 with enhanced security,
Web Server Role Before You Begin Installation Type	Add Roles and Features Wizard e (IIS) Web servers are computers that let you share information over the extranets. The Web Server role includes Internet Information Service diagnostic and administration, a unified Web platform that integrate	DESTINATION SERVER MSSQLDUPOR Internet, or through intranets and ts (IIS) 8.5 with enhanced security, es IIS 8.5, ASP.NET, and Windows ure equitable servicing of Web
Before You Begin Installation Type Server Selection Server Roles Features	Add Roles and Features Wizard e (IIS) Web servers are computers that let you share information over the extranets. The Web Server role includes Internet Information Service diagnostic and administration, a unified Web platform that integrate Communication Foundation. Things to note: • Using Windows System Resource Manager (WSRM) can help ensi	DESTINATION SERVER MSSQLDLIPDR Internet, or through intranets and is (IIS) 8.5 with enhanced security, es IIS 8.5, ASP.NET, and Windows ure equitable servicing of Web iputer. Installation of role services that uch as default documents and HTTI
Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation	Add Roles and Features Wizard (IIS) Web servers are computers that let you share information over the l extranets. The Web Server role includes Internet Information Service diagnostic and administration, a unified Web platform that integrate Communication Foundation. Things to note: Using Windows System Resource Manager (WSRM) can help ensi- server traffic, especially when there are multiple roles on this com The default installation for the Web Server (IIS) role includes the i enable you to serve static content, make minor customizations (s errors), monitor and log server activity, and configure static content	DESTINATION SERVER MSSQLDUPDR Internet, or through intranets and is (IIS) 8.5 with enhanced security, es IIS 8.5, ASP.NET, and Windows ure equitable servicing of Web iputer. Installation of role services that uch as default documents and HTTI
Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation	Add Roles and Features Wizard e (IIS) Web servers are computers that let you share information over the l extranets. The Web Server role includes Internet Information Service diagnostic and administration, a unified Web platform that integrate Communication Foundation. Things to note: • Using Windows System Resource Manager (WSRM) can help ensis server traffic, especially when there are multiple roles on this com • The default installation for the Web Server (IIS) role includes the i enable you to serve static content, make minor customizations (s	DESTINATION SERVER MSSQLDUPDR Internet, or through intranets and is (IIS) 8.5 with enhanced security, es IIS 8.5, ASP.NET, and Windows ure equitable servicing of Web uputer. Installation of role services that uch as default documents and HTTF

14. Ensure that Default Document, Directory Browsing, HTTP Errors, Static Content, HTTP Logging,

Select role servi	Add Roles and Features Wizard	DESTINATION SERVER
Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Select the role services to install for Web Server (IIS) Role services	Description Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
	< Previous Next >	Install Cancel
Click <b>Next.</b>	Add Roles and Features Wizard	DESTINATION SERVE
		DESTINATION SERVE MSSQL.DIJPDI d server, click Install. red on this page because they have
Before You Begin Installation Type Server Selection Server Roles	To install the following roles, role services, or features on selecte Restart the destination server automatically if required Optional features (such as administration tools) might be display been selected automatically. If you do not want to install these o	DESTINATION SERVE MSSQL.DIJPDI d server, click Install. red on this page because they have

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-26.



17. Wait for the installation to complete.

	View installation progress	
	Feature installation	
	Installation succeeded on MSSQL.DI.IPDR.	
	Web Server (IIS)	
	Management Tools	
	IIS Management Console Web Server	
Confirmation	Common HTTP Features	
Results	Default Document	
	Directory Browsing	
	HTTP Errors Static Content	
	Health and Diagnostics	
	HTTP Logging	
	You can close this wizard without interrupting running tasks. View task progress or page again by clicking Notifications in the command bar, and then Task Details.	r open th

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-26.

# 2.5.2 IIS Configuration

1. Open Windows Explorer and click This PC.

🚢 l 🗋 📮 l	Drive Tools	Local D	Disk (C:)		□ X
File Home Shar	e View Manage				~ <b>(</b> )
۰ 🕁 🐑 🛞 🛞	This PC 🕨 Local Disk (C:)		~ ¢	Search Local Disk (C:)	,p
🛠 Favorites	Name	Date modified	Туре	Size	
Desktop	퉬 inetpub	1/26/2018 1:52 PM	File folder		
🐌 Downloads	PerfLogs	8/22/2013 8:52 AM	File folder		
Recent places	Program Files	11/9/2017 6:26 PM	File folder		
	Program Files (x86)	11/9/2017 6:26 PM	File folder		
파트 This PC	Users	11/9/2017 6:27 PM	File folder		
	Windows	1/26/2018 1:52 PM	File folder		
6 items					:== <b>&gt;</b>

- 2. Right-click, and select Create Folder.
- 3. Name the folder **www.**

🚣 l 💽 🚺 🗢 l		Local Disk (C:)			D X
File Home Share	View				~ <b>(</b> )
🔄 🎯 👻 🕆 👗 🕨 Th	iis PC → Local Disk (C:) →		~ ¢	Search Local Disk (C:)	Q
☆ Favorites	Name	Date modified	Туре	Size	
Desktop	퉬 inetpub	1/26/2018 5:52 PM	File folder		
퉳 Downloads	PerfLogs	8/22/2013 8:52 AM	File folder		
🔛 Recent places	퉬 Program Files	1/29/2018 4:04 PM	File folder		
	퉬 Program Files (x86)	1/29/2018 2:40 PM	File folder		
🖳 This PC	🔒 Users	1/26/2018 5:52 PM	File folder		
	퉬 Windows	1/29/2018 2:25 PM	File folder		
🗣 Network	www	2/1/2018 1:38 PM	File folder		
7 items 1 item selected					

### 4. Open the Internet Information Services (IIS) Manager.

9		Internet Informa	ation Services (IIS) Manager	_ <b>_</b> ×
🕥 🖣 🕻 Start Page				<b>∞</b> ≥ ≙ @ ·
File View Help				
Connections	Morrosoft Internet Inf Application Server Ma	ormation Se	ervices 8	
	Recent connection	18	Connection tasks	Online resources
	Name MMSSQL	Server localhost	Connect to localhost Connect to a server Connect to a site Connect to an application	IIS News and Information IIS Downloads IIS Forums TechNet MSDN ASP.NET News Microsoft Web Platform
		, click the Enable IIS Nev	vs link to get the most recent online news.	Linabie lis riews
< III >				
eady				

- 5. Click the arrow next to **MSSQL** (or the chosen name of the server).
- 6. Click Sites.

s > Filten Name A Default Web Site	ID Status	All   Group by: No Groupin Binding *580 (http)	1g * Path %SystemDrive%D\inetpub\www.vroot	Actions and Webste Set Webste Defaults We Help
Filter:	ID Status	Binding	Path	Add Website Set Website Defaults
Filter:	ID Status	Binding	Path	Add Website Set Website Defaults
Name *	ID Status	Binding	Path	
Name *				1 Help
🚭 Default Web Site	1 Started (ht	":80 (http)	%SystemDrive%\inetpub\www.voot	
c Features View 🚓	Content View	н		
		Content View		

7. Click Add Website....

		Add Website	e			?	
Site name:		Application pool: DefaultAppPool			Select.		
Content Directory					Jelect		
Physical path:							
Pass-through authen	tication						
Connect as	Test Settings						
Connect as	lest settings						
Binding							
Type:	IP address:			Port:			
http 🗸	All Unassigner	d	~	80			
Host name:							
Example: www.conto	so.com or marke	ting.contoso.com					
		-					
	liately						
<ul> <li>Start Website immed</li> </ul>							
<ul> <li>Start Website immed</li> </ul>	inately						

### 8. Enter the desired site name.

	Add We	bsite	?
Site name:	Application MSSQLSITE		
MSSQLSITE	MISSQLSITE		Select
Content Directory			
Physical path:			
Pass-through authe	ntication		
Connect as	Test California		
Connect as	Test Settings		
Binding		1210/15	
Туре:	IP address:	Port:	
http	All Unassigned	♥ 80	
Host name:			
Example: www.cont	oso.com or marketing.contoso.	com	
Example: www.com	oso.com or marketing.contoso.	com	
<ul> <li>Start Website imme</li> </ul>	diately		
		OK	Cance

9. Click ... under Physical path:.

	Add Website ?
Site name: MSSQLSITE	Application pool: MSSQLSITE Select
Content Directory Physical path:	
Pass-through authentication	Browse For Folder X
Connect as Test Settings	Select a directory for the application.
Binding Type: IP address: http  Host name: Example: www.contoso.com or mar	▷     Videos     ∧       ▷     Hoppy Disk Drive (A:)     ▷       ▷     Local Disk (C:)     ▷       ▷     DVD Drive (D:) SQLSERVER     □       ▷     DVD Drive (D:) SQLSERVER     □       ▷     Wetwork     □       ▷     Control Panel     □       □     Recycle Bin     ∨
✓ Start Website immediately	Make New Folder OK Cancel
y start website infinediately	OK Cancel

### 10. Locate and select the folder created in Step 3.

	Add Website	3
Site name:	Application pool:	
MSSQLSITE	MSSQLSITE Select.	
Content Directory Physical path:		
Pass-through authentication	Browse For Folder	x
Connect as Test Settings	Select a directory for the application.	
Binding Type: IP address: http V All Unassign Host name: Example: www.contoso.com or man	Pigram Files     Program Files     Vigram Files (x86)     Vigram Files (x86)     Vigram Files (x86)     Vigram Vigra	∧ ≡ ∨ rcel
Start Website immediately		
	OK	Cancel

- 11. Click **OK.**
- 12. Set Type to http and Port to 80.
- 13. Ensure the **IP address** and **Host name** fields are filled in with the correct information for the machine.

#### 14. Ensure that Start Website immediately is selected.

	Add Website	?
Site name:	Application pool:	
MSSQLSITE	MSSQLSITE Select	
Content Directory		_
Physical path:		
C:\www		
Pass-through authenticati	on	
Connect as Test S	Settings	
Binding		
	address: Port:	
	2.168.81.107 🗸 80	
Host name:		
MSSQL.di.ipdr		
·		
Example: www.contoso.co	om or marketing.contoso.com	
Start Website immediately		
	ОК	Cance
	UK UK	Jance

15. Click OK.

# 2.6 Semperis Directory Services Protector

This section details the installation of **Semperis Directory Services Protector (DSP)**, a tool used for monitoring Active Directory environments. This installation requires both a copy of SQL Server Express as well as the **Semperis Wizard**. See the **Semperis DS Protector v2.5 Technical Requirements** document for specifics on the requirements. For a Windows Server 2012 R2 installation, meet the following requirements:

- .NET Framework Version 3.5 SP1
- .NET Framework Version 4.5.2 or later
- Joined to the Active Directory Domain it is protecting
- Either the installer for SQL Express Advanced or connection information and credentials for a full version of Microsoft SQL (MSSQL)

# 2.6.1 Configure Active Directory for Semperis DSP

1. Open Active Directory Users and Computers.

	Active Directory	Users and Computers		_ <b>_</b> ×
File Action View Help				
le ⇒ 🖄 🖬 🔏 🗎 🗙 🛙	] Q 🔒 🛛 🖬 🔧 🗽 🐨 🍸 🧕	(B)		
Active Directory Users and Com	Name	Last Name	Туре	Description
Saved Queries	& Abraham	Leptoceratops	User	User Account
⊿ 🚔 DI.IPDR	& Administrator		User	Built-in account
Builtin	& Allowed RODC Password Replication		Security Group	Members in thi
Computers	A Cert Publishers		Security Group	Members of thi
Domain Controllers	& Cloneable Domain Controllers		Security Group	Members of thi
ForeignSecurityPrincipal:	& Denied RODC Password Replication		Security Group	Members in thi
Managed Service Accour	🐍 DiscoverySearchMailbox {D919BA05	MsExchDiscoveryMailbox D919BA05-46A6-41	User	
Microsoft Exchange Secu Users	A DnsAdmins		Security Group	DNS Administra
Users	A DnsUpdateProxy		Security Group	DNS clients wh
	🎎 Domain Admins		Security Group	Designated adr
	& Domain Computers		Security Group	All workstations
	& Domain Controllers		Security Group	All domain con
	🎎 Domain Guests		Security Group	All domain gue
R	🎎 Domain Users		Security Group	All domain use
.0	🎎 Enterprise Admins		Security Group	Designated adr
	🎎 Enterprise Read-only Domain Contro		Security Group	Members of thi
	🐍 Exchange Online-ApplicationAccount		User	
	🐍 FederatedEmail.4c1f4d8b-8179-4148	FederatedEmail.4c1f4d8b-8179-4148-93bf-00a	User	
	Franklin	Delano Raptorvelt	User	User Account
	& Group Policy Creator Owners		Security Group	Members in thi
	🐍 Guest		User	Built-in accoun
	🐍 Harry	S Triceratops	User	User Account
	🐍 John	Quincy Ankylosaurus	User	User Account
	🐍 Lyndon	Brontosaurus Johnson	User	User Account
	<b>3</b> M <sup>2</sup>	MC		>

- 2. Right-click **Users** in the left pane, and select **New > User**.
- 3. Enter the information for a new user for the DSP service.

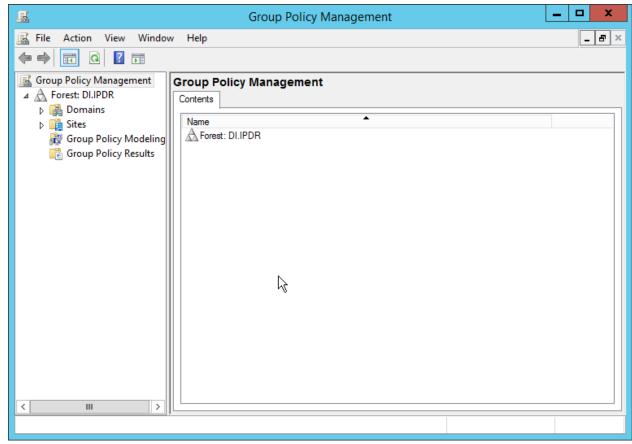
New Object - User		
Create in:	DI.IPDR/Users	
First name:	DSP Initials:	
Last name:	Service	
Full name:	DSP Service	
User logon name:		
dspservice	@DI.IPDR v	
User logon name (pre	-Windows 2000):	
DI\	dspservice	
	< Back Next > Canc	el

- 4. Click Next.
- 5. Enter a **password** twice for this user.
- 6. Set the password policy.

New Object - User
Create in: DI.IPDR/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back Next > Cancel

New Object - User	x
Create in: DI.IPDR/Users	
When you click Finish, the following object will be created:	
Full name: DSP Service	^
User logon name: dspservice@DI.IPDR	
The password never expires.	
	~
< Back Finish	Cancel

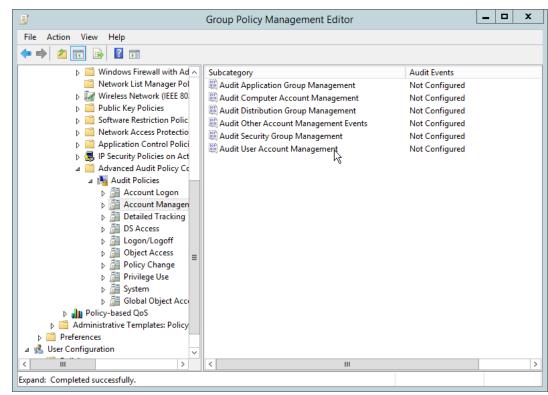
- 8. Click Finish.
- 9. Open Group Policy Management.



10. Right-click **Domains > DI.IPDR > Domain Controllers > Default Domain Controllers Policy,** and click **Edit.** 

J.	Group Policy Manag	ement Editor		_ 🗆 X
File Action View Help File Action Policies File Action View Help File Action Policies File Action View Help File Action Policies File Action View Help File Action Controllers Policies File Action Controllers Policies File Action View Help File Action Controllers Policies File Action Controllers Policies File Action Policies	Default Domain Controllers     Select an item to view its description.		Policy	
< III >	Extended Standard			

11. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management.



- 12. Edit the Audit User Account Management field by double-clicking it.
- 13. Check the box next to Configure the following audit events.
- 14. Check the box next to Success.

Audit User Account Management Properties	x
Policy Explain	_
Audit User Account Management	
☑ Configure the following audit events:	
Success	
Eailure	
k	
v	
OK Cancel Apply	

- 15. Click OK.
- 16. Go to Audit Policies > DS Access.
- 17. Double-click Audit Directory Services Changes.

Audit Directory Service Changes Properties
Policy Explain
Audit Directory Service Changes
Configure the following audit events:
Eailure
OK Cancel Apply

- 18. Check the box next to **Configure the following audit events.**
- 19. Check the box next to **Success.**
- 20. Click OK.

File Action View Help     Image: Stress of the st	J.	Group Policy Management Editor		 x
>       Windows Firewall with Ad         >       Network List Manager Pol         >       Wireless Network (IEEE 80)         >       Public Key Policies         >       Subcategory         Audit Directory Service Replication       Not Configured         >       Audit Directory Service Changes       Success         >       Application Control Polici       >         >       Advanced Audit Policics       >         >       Advanced Audit Policics       >         >       Account Logon       >         >       Account Logon       >         >       Detailed Tracking       >         >       Object Access       >         >       Policy-based QoS       >         >       Preferences       >         >       Wardinstructive Templates: Policy       >         >       West Configuration       >	File Action View Help			
<ul> <li>Network List Manager Pool</li> <li>Wireless Network (IEEE 80</li> <li>Public Key Policies</li> <li>Software Restriction Policie</li> <li>Application Control Policie</li> <li>Advanced Audit Policies</li> <li>Advanced Audit Policies</li> <li>Advanced Audit Policies</li> <li>Account Manager</li> <li>Account Manager</li> <li>Account Logon</li> <li>Account Logon</li> <li>Account Logon</li> <li>Bobletaled Tracking</li> <li>Dobletalecess</li> <li>Dobletalecess</li> <li>Bobletalecess</li> <li>Bobletalecess</li> <li>Bobletalecess</li> <li>Complexity of the second secon</li></ul>	⊨ 🔿 🚾 📑 🔒			
<ul> <li>▷ jiii Object Access</li> <li>▷ jiii Policy Change</li> <li>▷ jiii Policy Change</li> <li>▷ jiii System</li> <li>▷ jiiii System</li> <li>▷ jiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii</li></ul>	Advanced Audit Policy Cc     Advanced Policy Cc	Audit Detailed Directory Service Replication     Audit Directory Service Access     Audit Directory Service Changes	Not Configured Not Configured Success	
	<ul> <li>▷ Diject Access</li> <li>▷ Policy Change</li> <li>▷ Privilege Use</li> <li>▷ System</li> <li>▷ Global Object Acco</li> <li>▷ Policy-based QoS</li> <li>▷ Administrative Templates: Policy</li> <li>▷ Preferences</li> <li>✓ User Configuration</li> </ul>			
		<		

- 21. Open Active Directory Users and Computers.
- 22. Ensure View > Advanced Features is enabled.
- 23. Right-click the domain (for example, DI.IPDR) created earlier, and click Properties.

		DI.IPI	OR Prop	erties		?	x
General	Managed By	Object	Security	Attribute Editor	]		
	DI.IPDR						
Domain	name (pre-Win	dows 200	<b>DO)</b> :				
DI							
Descript	tion:						
Domain	functional leve	l:					
Window	s Server 2008						
	unctional level:						
Window	s Server 2008						
				] [			
	ОК		Cancel	Apply		He	elp

24. Click the Security tab.

Group or user names:				
Everyone SELF				
Authenticated User				
SYSTEM	5			
& NETWORK SERVI	CE			
& Organization Manad		(DI\Organi	zation Manager	ment)
			Add	Remove
Permissions for Everyone	•		Allow	Deny
Full control				
Read				
Write				
Create all child objects	;			
Delete all child objects	;			
For special permissions o	r advan	iced settin	ns click	
Advanced.		oo oo oo oo ah		Advanced
				~v

25. Click Advanced.

s Auditing Effective A	ccess		
al information, double-click a per	mission entry. To modify	nermission entry sele	ect the entry and click Edit (if avail
	mission entry. To moungar	permission entry, sele	cer the entry and click cure (if avail
	Access	Inherited from	Applies to
			Special
	2.1		Special
2			Descendant InetOrgPerson
		None	Descendant User objects
		None	Descendant InetOrgPerson
· · · · · · · · · · · · · · · · · · ·	1	None	Descendant Group objects
Pre-Windows 2000 Compatib	Special	None	Descendant User objects
Authenticated Users	Enable per user reversi	None	This object only
ENTERPRISE DOMAIN CONT	Replicating Directory	None	This object only
Authenticated Users	Unexpire password	None	This object only
Authenticated Users	Update password not r	None	This object only
ENTERDRICE DOMAIN CONT	Dealisetice Disectory	News	This shires sub.
Remove View			Restore de
	al information, double-click a per entries: Principal Exchange Windows Permissi Exchange Servers (DI\Exchan Exchange Servers (DI\Exchan Pre-Windows 2000 Compatib Pre-Windows 2000 Compatib Pre-Windows 2000 Compatib Pre-Windows 2000 Compatib Authenticated Users ENTERPRISE DOMAIN CONT Authenticated Users Authenticated Users	al information, double-click a permission entry. To modify entries: Principal Access Exchange Windows Permissi Change password Exchange Windows Permissi Reset password Exchange Servers (DI\Exchan Special Pre-Windows 2000 Compatib Special Authenticated Users Unexpire password not r Publications Disorders	al information, double-click a permission entry. To modify permission entry, sele entries: Principal Access Inherited from Exchange Windows Permissi Change password None Exchange Servers (DI\Exchan Special None Exchange Servers (DI\Exchan Special None Pre-Windows 2000 Compatib Special None Authenticated Users Enable per user reversi None ENTERPRISE DOMAIN CONT Replicating Directory None Authenticated Users Unexpire password None Authenticated Users Update password not r None

- 27. Click Add.
- 28. Enter Everyone.

Select User, Computer, Service Account, or	Group 🛛 🗙
Select this object type:	
User, Group, or Built-in security principal	Object Types
From this location:	
DI.IPDR	Locations
Enter the object name to select ( <u>examples</u> ):	Check Names
Advanced OK	Cancel

For		al information, double-click an au		udit entry, select the entr	y and click Edit (if available).
88		Principal Everyone	Access	Inherited from None	Applies to Special
98. 98.		Everyone Domain Users (DI\Domain Us	All extended rights	None None	Special This object only
82		Administrators (DI\Administr	All extended rights	None	This object only
<u>8</u>	Succ	Everyone	Special 났	None	This object only
	Add	Remove View			Restore defaults

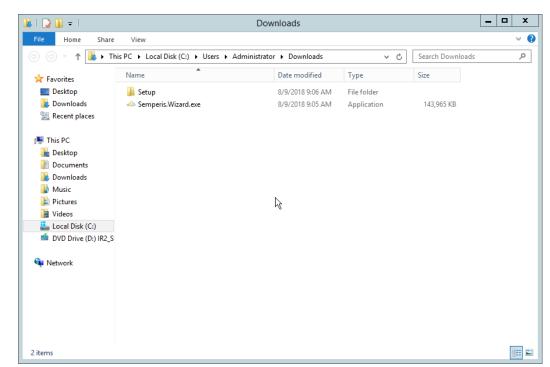
- 30. Double-click Everyone.
- 31. Check the boxes next to Write all properties, Delete, Delete subtree, Modify permissions, Modify owner, All validated writes, All extended rights, Create all child objects, Delete all child objects.

		Auditing Entry for DI	_ □
Туре:	Success V		
Applies to:	This object and all descendant objects		
Permissions	s:	✓ Create msExchOmaDeliveryProvider objects	
	List contents	Delete msExchOmaDeliveryProvider objects	
	Read all properties	✓ Create msExchOmaDeviceCapability objects	
	Write all properties	Delete msExchOmaDeviceCapability objects	
	✓ Delete	Create msExchOmaDeviceType objects	
	Delete subtree	Delete msExchOmaDeviceType objects	
	Read permissions	Create msExchOrganizationContainer objects	
	Modify permissions	Delete msExchOrganizationContainer objects	
	Modify owner	Create msExchPoliciesContainer objects	
	✓ All validated writes	Delete msExchPoliciesContainer objects	
	✓ All extended rights	Create msExchProtocolCfgHTTPContainer objects	
	Create all child objects	Delete msExchProtocolCfgHTTPContainer objects	
	Delete all child objects	Create msExchProtocolCfgHTTPFilters objects	
	Create Computer objects	Delete msExchProtocolCfgHTTPFilters objects	
	Delete Computer objects	Create msExchProtocolCfgIMAPContainer objects	
	Create Contact objects	Delete msExchProtocolCfgIMAPContainer objects	
	Delete Contact objects	Create msExchProtocolCfgIMContainer objects	
	Create friendlyCountry objects	Delete msExchProtocolCfgIMContainer objects	

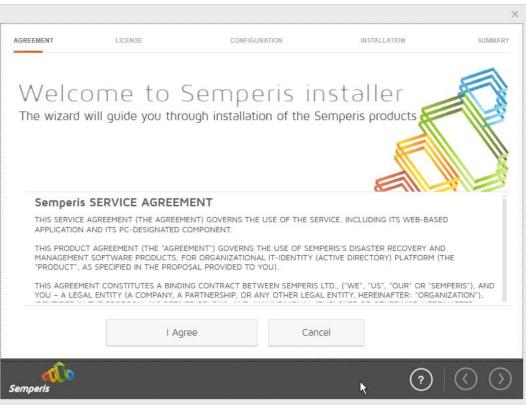
	DI.IPDR P	roperties	?
General Managed By	Object Secu	urity Attribute Edito	r
Group or user names:		-	
Everyone			^
SELF			
& Authenticated Us	ers		
SYSTEM .			
& NETWORK SER			
Section Mar 2017	agement (DI\O	rganization Manage	ment)
		Add	Remove
			_
Permissions for Everyo	ne	Allow	Deny
Full control			
Read			
Write			
Create all child obje	cts		
Delete all child obje	cts		
For special permission: Advanced.	s or advanced s	ettings, click	Advanced
ОК	Cano		

## 2.6.2 Install Semperis DSP

 If you are using a local SQL Express Advanced server, place the SQLEXPRADV\_x64\_ENU.exe installer in a directory called *Setup*, and ensure that the Semperis Wizard is adjacent to the Setup folder (not inside it). If a SQL Express Advanced server is not being used, no Setup folder is required.



2. If prompted to restart the computer, do so.



- 3. Click I Agree.
- 4. Select Evaluation License.
- 5. Select Active Directory State Management.

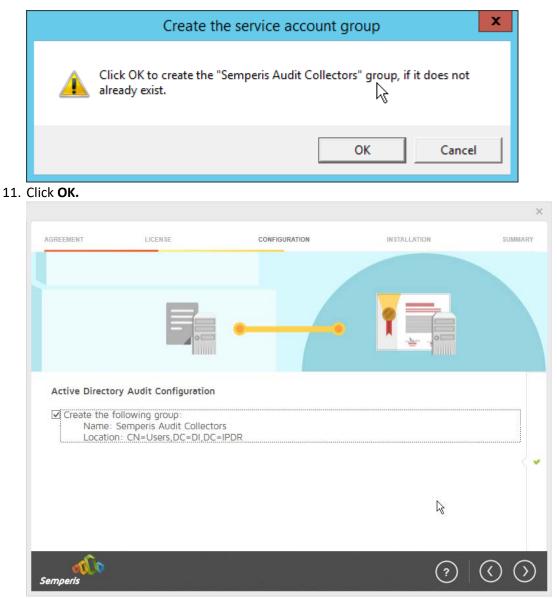
AGREEMENT	LICENSE	CONFIGURATION	INSTALLATION	SUMMARY
Evaluation	license			
	Directory Forest Recove			
Active	Directory State Manage	ement		
O Full License	2			
Br	owse			
emperis			?	$\bigcirc$

- 6. Click the > button.
- 7. Enter the **username** and **password** of the account created earlier.

AGREEMENT	LICENSE	CONFIGURATION	INSTALLATION	SUMN
Serv	ice Acc	ount		
the Semperis	Management Server	t to use for the ADSM service acco to communicate with the ADSM a	agents.	ed by
Forest Name: DLIPDR		Service account: DI\dspservice	Password:	
emperis			?	() ()
k the > but	tton.			
		e Account to the autho	rization group	x
	dd the Servic	e Account to the autho e Service Account to the "Ser The group will be created in t	mperis ADSM Service	x

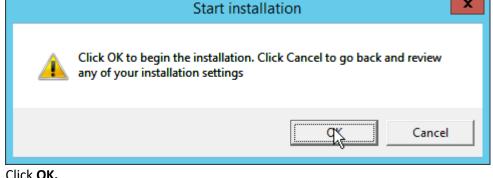
8.

10. Check the box next to Create the following group.

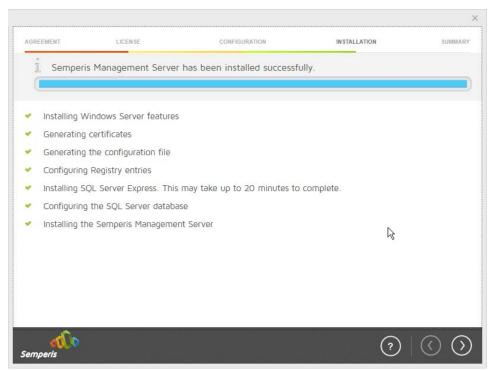


- 12. Click the > button.
- 13. Select the appropriate database option, and enter any required information.

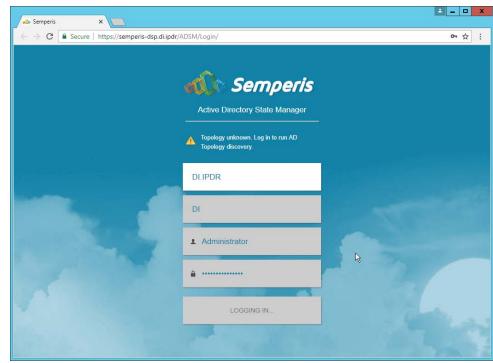
AGREE	-MENT LICENSE	CONFIGURATION	INSTALLATION	SUMMARY
ſ	( <b>_</b> •• [		••••	
	elect installation type Create a new database reate a new database on an existin Use an existing database se an existing database on an exis Install SQL Express locally se Microsoft SQL Express 2014 run	ng SQL server Server ting SQL server Win uning locally User		2
Semp			$\bigcirc$	
14. Click th	he > button.	Start installation		×



15. Click OK.



- 16. Click the > button after the installation completes.
- 17. There should now be a shortcut on the desktop linking to the web console for **Semperis DS Protector.**
- 18. On the login page, enter the full domain as well as the NetBIOS name.
- 19. Enter the **username** and **password** of an administrator on the domain.

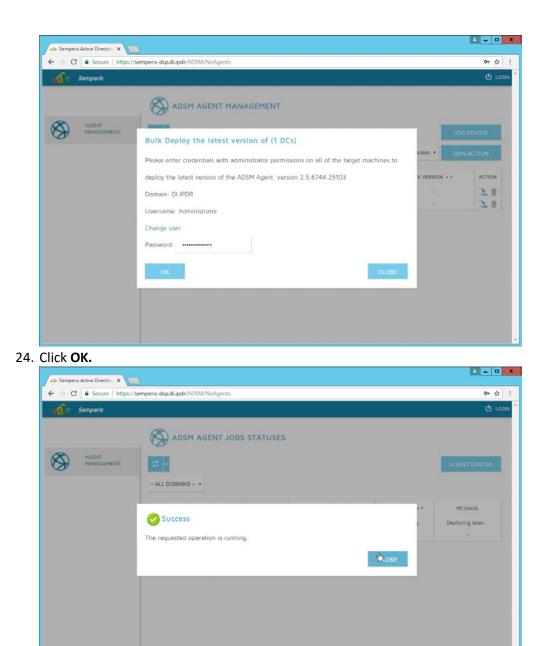


### 20. Click Login.

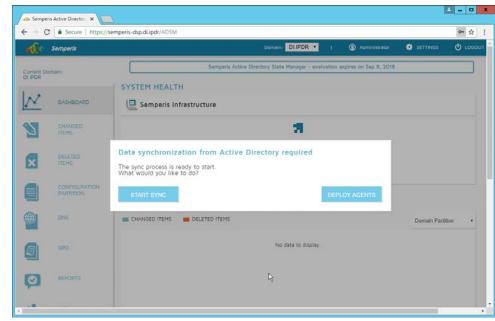
21. Check the box next to the domain controllers that should be monitored by DSP.

Semperis	Ø	ADSM AGENT	MANAGEMENT				ტ .
AGENT MANAGEMENT	0					JOE	STATUS
	- ALL D	OMAINS - • DOW	NLOAD AGENT INSTAL	LER	Deploy	Latest Velation + RUN	ACTION
	0	NAME •	DOMAIN + *	STATUS + +	VERSION + *	OS VERSION + +	ACTION
		AD-DNS	DUIPDR	No agent	0.0.0.0		3.0
		AD-DNS08	DI. IPDR	No agent	0.0.0.0	1	3.0

- 22. Click Run Action.
- 23. Enter the **password** for the account.



- 25. Click Close.
- 26. After the agent finishes deploying, click **Login** at the top of the page, and log in.

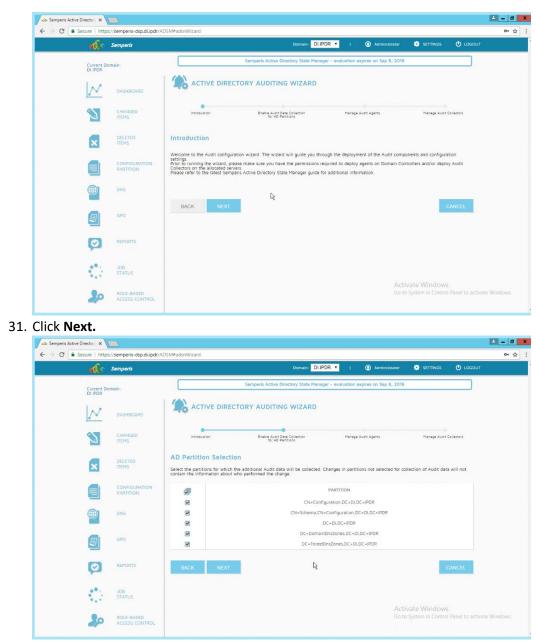


### 27. Click Start Sync.

28. After this completes, click **Settings** at the top of the page.

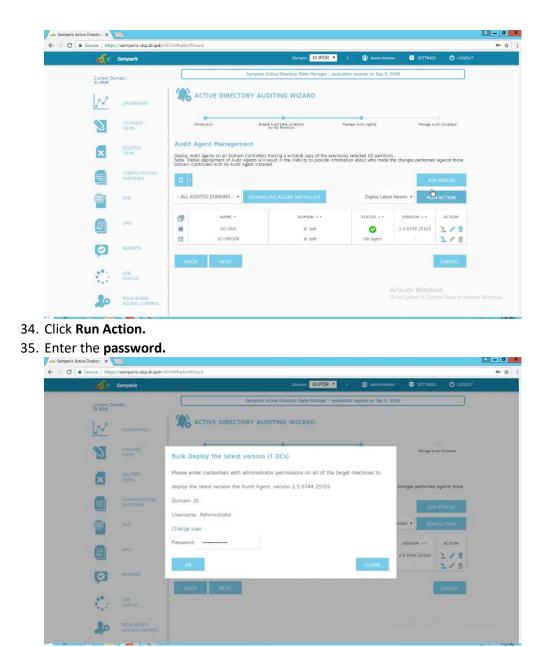
d)r	Semperis		Domain: DLIPDR •	l 💿 Admini	strator 🥵 SETTINGS 🕻	D LOCOUT
Current Do DI IPDR	main:					
N	DASHBOARD	> Agents (DI.IPDR)				
~	CHANGED	> Database				
2	ITEMS	> Email Alerts				
×	DELETED ITEMS	> Group Policy				
-	CONFIGURATION	> Data Collection				
	PARTITION	✓ Audit				
	DNS	Audit Configuration Wizard				Run
	GPO.	Define audit settings and manage Audit A	gents and Audit Collectors.			
		Audit Agent			Download A	igent
Ø	REPORTS	Audit Collector			Download Colli	ector
	JOB STATUS	> General		¢		
	STRIUS	> Operation Log			Activate Windows	
20	ROLE-BASED ACCESS CONTROL				Go to System in Control Par	el to activate

- 29. Click Audit.
- 30. Click Run.

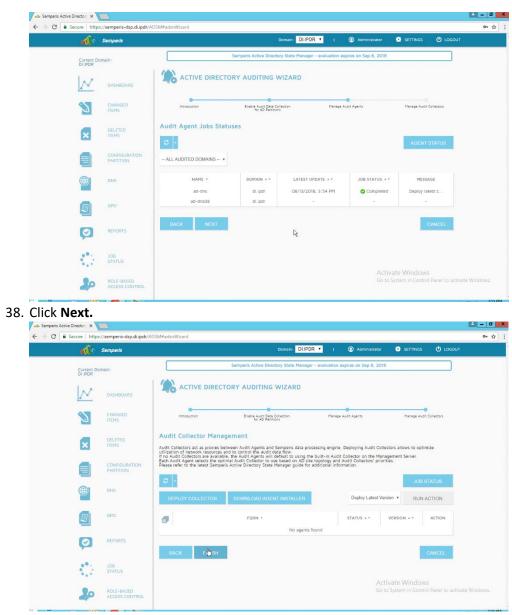


#### 32. Click Next.

33. Check the boxes next to any Domain Controllers that should be monitored.



- 36. Click OK.
- 37. Wait for the deployment to finish.



39. Click Finish.

# 2.6.3 Roll Back Changes with Semperis DSP

- 1. Go to **Changed Items** on the left navigation bar.
- 2. Check the box next to any undesired Active Directory changes.
- 3. Click the ... button to view more details about the change.

Semperis						Domein: DLIP	DR •	Administrator	SETTINGS	<u>ტ</u> ით
Current Domain: DLIPDR	Ø	C	HAN	GED ITEMS				Live		
DASHBOARD	AUG 9	AUG	10	AUG 11	AUG 12		Â	JG 13 Aug 13,	12:00 PM	ксні
CHANGED ITEMS	L. L	UNDO	ტ.	ECTED			F	ILTER RESULTS	۹	Ľ
DELETED		wing		: 1 - 9 of 9 ₿• 9 ung < PREVIOUS 1	rouped results NEXT >	LAST »	20 V Go to		up results by opera	
	0	OP	CLASS	DN	ATTRIBUTE	OLD VALUE	NEW VALUE	TIME	CHANGED BY	
DNS		0	1	Administrator	lastLogonT	2018-08-03	2018-08-13	08/13/2018, 3 50 37 PM		0
		0	1	HealthMailboxff.	lastLogon T	2018-08-03	2018-08-13	08/13/2018, 3:36:26 PM	ť e	Θ
GPO GPO	0	1	0 0	WINDOWS10-1	dBCSPwd	<not set=""></not>	<not set=""></not>	08/13/2018, 1:19:54 PM 08/13/2018, 1:19:54 PM		Θ
				WINDOW510-1	ntPwdHisto	( <secret></secret>	( <secret></secret>	08/13/2018. 1:19:54 PM		Θ
		0	0	WINDOWS10-1	pwdLastSet	2018-07-14	2018-08-13 <secret></secret>	08/13/2018, 1:19:54 PM 08/13/2018, 1:19:54 PM		Θ
REPORTS		0	0	WINDOW510-1	ImPwdHisto.	( <secret>,</secret>	[ <secret>,</secret>	08/13/2018, 1 19 54 PM		Θ
JOB STATUS										

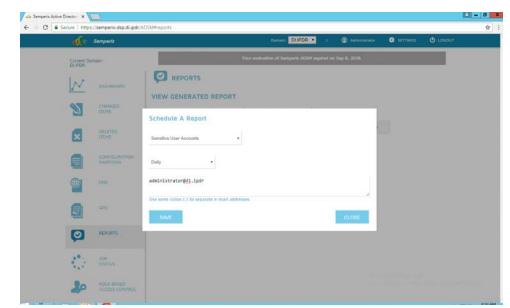
4. Click **Undo Selected** to roll back these changes.

# 2.6.4 Configure Reporting with Semperis DSP

- 1. Click **Reports** on the left sidebar in the **Semperis DSP** web console.
- 2. Under **Generate Report**, reports can be viewed instantly, by selecting a type of report and clicking **Create**.

- ŵ	Semperis	D	main: DLIPDF	R 🔹 🕴	Administrator	SETTINGS	U LOGOUT
Current Di DI IPDR	omain	Your evaluation	of Semperis AD	5M expired on	Sep 8, 2018.		
N	DASHBOARD	VIEW GENERATED REPORT					
$\mathbf{S}$	CHANGED	Sensitive User Accounts		•			
×	DELETED	GENERATE REPORT	,	VIEW	DOWNLOAD		
	CONFIGURATION PARTITION	Sensitive User Accounts	l.				
	DNS	SCHEDULED REPORTS		14			
	GPD						
Ø	REPORTS						
<.';	JOB STATUS				12.504		
20	ROLE-BASED ACCESS CONTROL					vate Windows System in Control	5 I Panel to activate V

- 3. Under Scheduled Reports, click Generate to automatically email specific reports.
- 4. Select a report type and a schedule.
- 5. Enter the email addresses of anyone who should receive this report.



6. Click Save.

## 2.6.5 Configure Email Alerts with Semperis DSP

- 1. Click Settings on the Semperis DSP web console.
- 2. Expand the Email Alerts section.
- 3. Click Edit.
- 4. Enter the information of the organization's email server as well as an email address from which to send.

- dû	Semperis		Domain: DLIPDR •	I   Administrator	🔹 SETTINGS 🛛 LO
Current Di DI.IPDR	omain		Your evaluation of Semperts ADSM exp	sired on Sep 8, 2018.	
N	DASHBOARD				
3	CHANGED	> Agents (DI.IPDR)			
		> Database			
×	DELETED	✓ Email Alerts			
-	CONFIGURATION	Authentication Requirements	Anonymous:		Cancel
	PARTITION	Settings required to send notifications	Enable SSL:		
	DNS	and alerts	Server:	EXCHANGE DI IPDR	
	GPO		Port:	25	
			Username:	USERNAME	
Ø	REPORTS		Password:	PASSWORD	
	JOB		Mail from:	semperis@di.ipdr	
1.1	STATUS			santo Activ	
	ROLE-BASED ACCESS CONTROL				System in Control Panel to

5. Click Save.

6. Enter an email address to which to send a test email.

Semperis		Domain DIJPDR •	1 C.	Anninistrator	SETTINGS	😃 цовоит
Current Domain Dr. IPDR		Your evaluation of Samperis ADSM	expired on t	Sep 8, 2018.		
		5				
Снаное птене	o Agents (DI IPI	DR)				
DELETER TENS	Validate SMTP s	10000000-1	validator			
	JRATION	iss to test and validate SMTP settings. If settings natically be saved.	r ventilitet			Cancel
D015						
<b>9</b>		Username	10	CLOSE		
P REPORT		Password		ASSWORD		
JOE		Mail from:		mperis@dl.ipdr		
				and the second sec		

- 7. Click Validate & Save.
- 8. Under Alert Recipients, add any desired recipients of alerts.

- <b>4</b> 04	Semperis		Domain: DLIPDR 🔻	l 💿 Admini	istrator 🔅 SETTINGS	O LOGOUT	
Current Dom DLIPDR	เอเกา		Port:	25			
41.21			Username	-			
$\sim$	DASHBOARD		Password:	-			
$\mathbf{N}$	CHANGED ITEMS		Mail from:	semperis@di.ip	dr		
×	DELETED ITEMS	Alert Recipients					
	CONFIGURATION PARTITION	Add a recipient administrator@di.ipdi	ADD				
	DNS	EMAIL ADDRESS	No alert recipients fi	ound			
	GPD	Daily Status Reports	Send daily status report:	true		Edit	
Ø	REPORTS	A daily status report sent to the Alert Recipients	At:	1:00 AM			
	JOE	Repeating Error Notification Threshold	Threshold:	60 minutes		Edit	
S	STATUS	Define the minimum amount of time that					
		must pass between error notification			Activate Windows		

- 9. Click Add.
- 10. Configure any schedule settings according to your organization's needs.

# 2.7 Glasswall FileTrust™ for Email

The following sections will detail the installation of **Glasswall FileTrust<sup>™</sup> for Email**, an email security product, on a new Windows 2012 R2 machine. For the purposes of this guide, we use Microsoft Exchange as the email service provider.

# 2.7.1 Install Prerequisites

### 2.7.1.1 Install the IIS web server

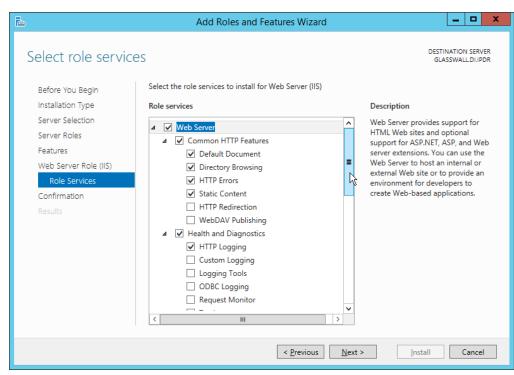
- 1. In Server Manager, click Add Roles and Features.
- 2. Click Next.
- 3. Select Role-based or feature-based installation.

B	Add Roles and Features Wizard	□ X
Select installation		LL.DI.IPDR
Before You Begin Installation Type	Select the installation type. You can install roles and features on a running physical computer or machine, or on an offline virtual hard disk (VHD).	or virtual
Server Selection Server Roles Features Confirmation Results	<ul> <li>Role-based or feature-based installation Configure a single server by adding roles, role services, and features.</li> <li>Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machi or session-based desktop deployment.</li> </ul>	ine-based
	< Previous Next > Install (	Cancel

- 4. Click Next.
- 5. Select the current server.

	Add F	Roles and Features V	Wizard		_		x
Select destinati	on server				NATION		
Before You Begin	Select a server or a vi	rtual hard disk on which	to install roles and features.				
Installation Type	Select a server from the se	m the server pool					
Server Selection	O Select a virtual ha	rd disk					
Server Roles	Server Pool						
Features							
	Filter:						
	Name	IP Address	Operating System				
	GLASSWALL.DI.IPDR	192.168.1.133	Microsoft Windows Serve	er 2012 R2 Stan	dard		
	1 Computer(s) found						
	Add Servers comman		ndows Server 2012, and that fiftine servers and newly-adde				the
		< <u>P</u> re	evious <u>N</u> ext >	Install	C	ancel	I

- 6. Click Next.
- 7. Select Web Server (IIS).
- 8. Click Next.
- 9. Select .NET Framework 4.5 Features.
- 10. Click Next.
- 11. Select the following Role Services: Web Server, Common HTTP Features, Default Document, Directory Browsing, HTTP Errors, Static Content, Health and Diagnostics, HTTP Logging, Performance, Static Content Compression, Security, Request Filtering, Client Certificate Mapping Authentication, Application Development, .NET Extensibility 4.5, ASP.NET 4.5, ISAPI Extensions, ISAPI Filters, Management Tools, and IIS Management Console.



- 12. Click Next.
- 13. Check the box next to **Restart the destination server automatically if required.**
- 14. Click Install.

### 2.7.1.2 Install Microsoft SQL 2014 Enterprise

Please see <u>Section 2.4</u> for an installation guide for MS SQL 2014; for simplicity it should be installed on the same server as Glasswall FileTrust. Ensure that Mixed Mode authentication is selected when installing.

### 2.7.1.3 Install Microsoft Visual C++ 2015

1. Run the vcredist\_x64 installer.

C++ RunTi Applica	ation Tools		. 🗆 X
e View Ma	anage		~ (
Std ► Visual C	~ ¢	Search Visual C++ Ru	nTime 🔎
Name	•	Date n	nodified
🕼 vcredist x64	N	1/30/2	2018 12:00 PM
-	4		
2			
<	III		
13.8 MB			:== E
ext to lagree	to the liv	onso torms	and cor
+ 2015 Redistribu	(abie (x04) -	14	
oft Visual C	++ 201	5	
		0	
اردا ما ما معريها ت	CA) 14	0.22026	
ributable (xe	64) - 14	.0.23026	
ributable (xe RE LICENSE TERMS	64) - 14	.0.23026	1
RE LICENSE TERMS	-	^	]
	-	^	
	e View Ma Std → Visual C Name Ø vcredist_x64 22 23 24 24 25 25 25 25 25 25 25 25 25 25	e View Manage	e View Manage Std • Visual C • © Search Visual C++ Ru Name Date r Vcredist_x64 1/30/2 2 2 2 2 2 2 2 2 2 2 2 2 2

2. itions.

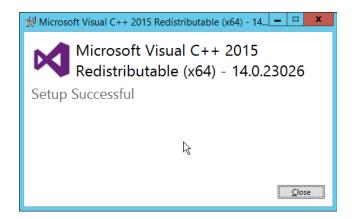
 $\bigcirc$ 

<u>I</u>nstall

<u>C</u>lose

- 3. Click Install.
- 4. After the installation is complete, click **Close.**

✓ I agree to the license terms and conditions



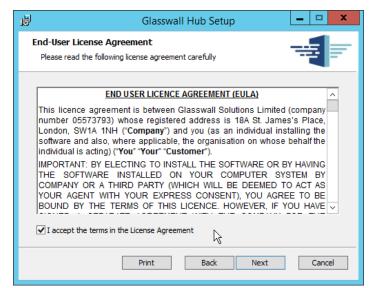
# 2.7.2 Install the Glasswall FileTrust Server Component

## 2.7.2.1 Install Glasswall Hub

### 1. Run HubInstaller.msi.

谩	Glasswall Hub Setup 📃 🗖 🗙
	Welcome to the Glasswall Hub Setup Wizard
SSW EVERY	The Setup Wizard will install Glasswall Hub on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
- ∃= GLA	k}
	Back Next Cancel

2. Click Next.



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

#### 4. Click Next.

년 Glasswall Hu	ıb Setup 📃 🗖 🗙			
Custom Setup Select the way you want features to be installe	. =			
Click the icons in the tree below to change the	way features will be installed			
Management Service     File Release Request Service     Database	Installs the Glasswall Management Service to the local machine This feature will be installed on the local hard drive			
$L_{S}$				
	<u>B</u> ack <u>N</u> ext Cancel			

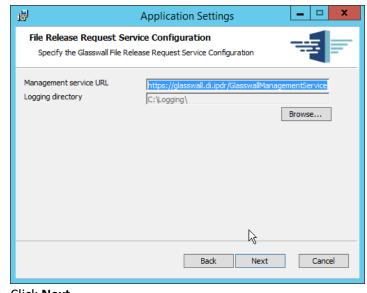
- 5. Click Next.
- 6. Enter **localhost** for the **Database Server**.
- 7. Enter HubDatabase for the Database Name.
- 8. Enter a username and password (and take note of these for later).

븅	Glasswall Hub Setup
Database Confi Specify the Glass	guration wall Database Configuration
Database Server	localhost LS
Database Name	HubDatabase
Database Login	GWDBuser
Database Passwo	ord
	Back Next Cancel

- 9. Click Next.
- 10. Select Windows Authentication.

<b>B</b>	Glasswall Hub Setup					
	Database Installation Settings Specify the Installation Setting for the Glasswall Database					
Database Administrate	or Credentials : that will be used to create the database (all fields required)					
Authentication Method User name Password	Windows Authentication					
	Database Installation Log File         Location of the database installation log file         Installation Log File         C: \Logging \gw-Database-Install.log					
	Back Next Cancel					

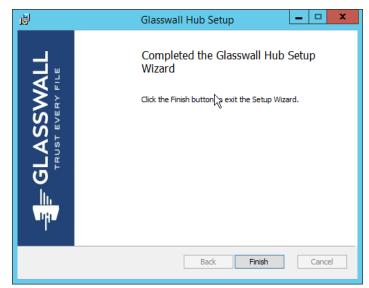
- 11. Click Next.
- 12. Replace the domain of the **management service URL** with the address of the current machine, such as **glasswall.di.ipdr.**



13. Click Next.

1	Glasswall Hub Setup	- 🗆 X
F	Ready to install Glasswall Hub	=
	Click Install to begin the installation. Click Back to review or change any of installation settings. Click Cancel to exit the wizard.	your
	l≩	
	Back Install	Cancel

14. Click Install.



- 15. Click Finish.
- 2.7.2.2 Install Glasswall Integration Service
  - 1. Run GlasswallIntegrationService.msi.

谩	Glasswall Integration Service Setup
	Welcome to the Glasswall Integration Service Setup Wizard
ASSW UST EVERY	The Setup Wizard will install Glasswall Integration Service on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
≡_ GL/	μζ
- The second sec	Back Next Cancel

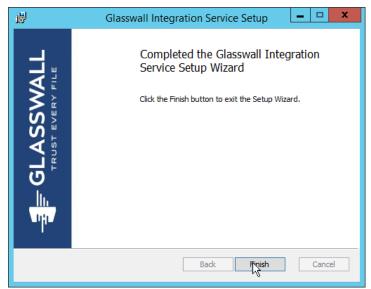
- 2. Click Next.
- 3. Check the box next to I accept the terms in the License Agreement.

岁 Glasswall Integration Service Setup	D X
End-User License Agreement Please read the following license agreement carefully	<b>=</b>
END USER LICENCE AGREEMENT (EULA)	^
This licence agreement is between Glasswall Solutions Limited (com number 05573793) whose registered address is 18A St. James's F London, SW1A 1NH ("Company") and you (as an individual installin software and also, where applicable, the organisation on whose beha individual is acting) ("Your" "Customer").	place, g the
IMPORTANT: BY ELECTING TO INSTALL THE SOFTWARE OR BY HA THE SOFTWARE INSTALLED ON YOUR COMPUTER SYSTEM COMPANY OR A THIRD PARTY (WHICH WILL BE DEEMED TO AC YOUR AGENT WITH YOUR EXPRESS CONSENT), YOU AGREE TO BOUND BY THE TERMS OF THIS LICENCE. HOWEVER, IF YOU I	I BY CT AS O BE
☑ I accept the terms in the License Agreement	
Print Back Next	Cancel

- 4. Click Next.
- 5. For **Database Server**, **Database Name**, **Database User**, and **Database Password**, enter the information entered in the **Glasswall Hub Installer**.
- 6. Create a username and password for API User Name and API Password.
- 7. Enter an email address to be used for notifications in Notifications Smtp Mail From.
- 8. Enter the address for the mail server for Notifications Smtp Host.
- 9. Enter a port (25 is used here) for Notifications Smtp Port.

[	谩	Application Settings	-		x	
	Database Server	localhost				
	Database Name	HubDatabase				
	Database User	GWDBUser				
	Database Password	•••••				
	API User Name	APIUSERNAME				
	API Password	•••••				
	Logging directory	C:\Logging\				
	Log level	Info (and above) 🗸 🗸				
	Notifications Smtp Mail From	Administrator @DI.IPDR				
	Notifications Smtp Host	192.168.1.134				
	Notifications Smtp Port	25				
		This SMTP Server F quires Authentication	I			
	Notifications Smtp Username					
	Notifications Smtp Password					
		Back Next		Cano	al	
				Cano		
10.	Click <b>Next.</b>					
	岗 Glass	wall Integration Service Setup	-		x	
	Ready to install Glasswall Integration Service					
	Click Install to begin the inst installation settings. Click Ca	allation. Click Back to review or change any of ancel to exit the wizard.	your			
			6			
		Back Install		Cano	el	

11. Click Install.



- 12. Click Finish.
- 2.7.2.3 Install Glasswall Administrator Console

### 1. Run AdministratorConsoleInstaller.msi.

閿	Glasswall Administrator Console Setup
	Welcome to the Glasswall Administrator Console Setup Wizard
SSV T EVERY	The Setup Wizard will install Glasswall Administrator Console on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
≓ GLA	l≩
THE	
	Back Next Cancel

- 2. Click Next.
- 3. Check the box next to I accept the terms in the License Agreement.

閿	Glasswall Administrator Console Setup 🛛 – 🗖 🗙
	r License Agreement ead the following license agreement carefully
	END USER LICENCE AGREEMENT (EULA)
number London, software	ence agreement is between Glasswall Solutions Limited (company 05573793) whose registered address is 18A St. James's Place, , SW1A 1NH ("Company") and you (as an individual installing the e and also, where applicable, the organisation on whose behalf the al is acting) ("You" "Your" "Customer").
THE SO COMPAN YOUR A	ANT: BY ELECTING TO INSTALL THE SOFTWARE OR BY HAVING OFTWARE INSTALLED ON YOUR COMPUTER SYSTEM BY NY OR A THIRD PARTY (WHICH WILL BE DEEMED TO ACT AS AGENT WITH YOUR EXPRESS CONSENT), YOU AGREE TO BE DBY THE TERMS OF THIS LICENCE. HOWEVER, IF YOU HAVE V
✓ I accep	pt the terms in the License Agreement
	Print Back Next Cancel

- 4. Click Next.
- 5. For **Database Server**, **Database Name**, **Database User**, and **Database Password**, enter the information entered in the **Glasswall Hub Installer**.
- 6. For Notifications Smtp Mail From, Notifications Smtp Host, Notifications Smtp Port, enter the information entered in the Glasswall Integration Service Installer.
- 7. For Notifications Smtp Port Security, select StartTlsWhenAvailable.

閿	Application Settings
Database Server	localhost
Database Name	HubDatabase
Database User	GWDBUser
Database Password	•••••
Notifications Smtp Mail From	Administrator@DI.IPDR
Notifications Smtp Host	192.168.1.134
Notifications Smtp Port	25
Notifications Smtp Port Security	StartTlsWhenAvailable 🗸
	This SMTP Server Requires Authentication
Notifications Smtp Username	
Notifications Smtp Password	
	Back Next Cancel

8. Click Next.



10. Click Finish.

### 2.7.2.4 *Add the Server's Certificate*

- For the purposes of this build, a self-signed certificate is used, but this is dependent on the needs of the organization. Ensure that the certificate used is issued to the domain, such as \*.di.ipdr.
- 2. Open mmc.
- 3. Click File > Add/Remove Snap-In....
- 4. Select Certificates from the left pane, and click Add.

### 5. Select Computer Account.

	Certificate	s snap-in		
This snap-in will always manag	ge certificates for:			
O My user account				
<ul> <li>Service account</li> </ul>				
<ul> <li>Computer account</li> </ul>				
			$\searrow$	
			10	
		< Back	Next >	Cancel
		L		

- 6. Click Next.
- 7. Select Local computer.

Select Computer	x
Select the computer you want this snap-in to manage. This snap-in will always manage:	
<u>Local computer: (the computer this console is running on)</u> <u>Another computer:</u> <u>Browse</u>	]
Allow the selected computer to be changed when launching from the command line. This only applies if you save the compose.	
< <u>B</u> ack Finish Canc	el

8. Click Finish.

Snap-in	Vendor	~	Console Root		Edit Extensions
ActiveX Control	Microsoft Cor	-		(Local Computer)	Euri Extensions
Authorization Manager			Cer directes	(cocor comparer)	Remove
Certificates	Microsoft Cor	=			
	Microsoft Cor				Mauralla
Computer Managem	Microsoft Cor				Move Up
Device Manager	Microsoft Cor				Move Down
Disk Management	Microsoft and		Add >		
Event Viewer	Microsoft Cor				
🗎 Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
Internet Informatio	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor				
Link to Web Address	Microsoft Cor	~			Advanced

- 9. Click OK.
- 10. Right-click the **Personal** certificate store, and select **All tasks > Import...**

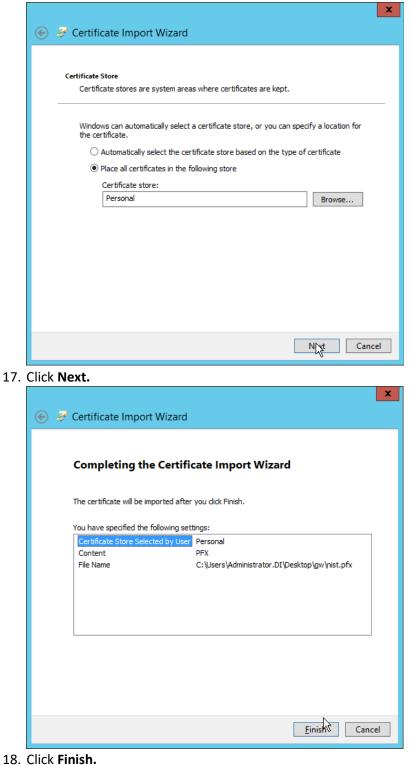
📀 🔗 Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
C:\Users\Administrator.DI\Desktop\gw\nist.pfx Browse
Note: Mars that are writen by the start is a single fit is the following formula:
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange - PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Next <sup>1/3</sup> Cancel

- 11. Enter the file name of the certificate.
- 12. Click Next.
- 13. Enter the **password** for the certificate.
- 14. Check the box next to Mark this key as exportable.

<ul> <li>Ertificate Import Wizard</li> </ul>
Private key protection To maintain security, the private key was protected with a password. Type the password for the private key. Password: Display Password
Import options:         □ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.         ☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.         ☑ Include all extended properties.
Rext Cancel

#### 15. Click Next.

16. Ensure that the Certificate store says Personal.



#### 19. Re-open the certificate import wizard but this time for Trusted Root Certification Authorities.

	x
💿 😼 Certificate Import Wizard	
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Store Location	
O Current User	
Local Machine	
To continue, click Next.	
	_
Next Cance	:

#### 20. Click Next.

21. Select the same certificate.

<ul> <li>Certificate Import Wizard</li> </ul>
File to Import Specify the file you want to import.
File name: C:\Users\Administrator.DI\Desktop\gw\nist.pfx Browse
Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certi Sates (.P7B) Microsoft Serialized Certificate Store (.SST)
Next Cancel

- 22. Click Next.
- 23. Enter the certificate's password.
- 24. Check the box next to Mark this key as exportable.

Pri	vate key protection
	To maintain security, the private key was protected with a password.
	Type the password for the private key.
	Password:
	•••••
	Display Password
	Import options:
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your
	keys at a later time.
	$\checkmark$ Include all extended properties.
	N
	Next Can
	v+
ICK <b>Ne</b>	xt.
ick Ne	<b>xt.</b> Certificate Import Wizard
€ ∌ (	
€ ∌ (	Certificate Import Wizard
€ ₽ (	Certificate Import Wizard tificate Store Certificate stores are system areas where certificates are kept.
) 🦻 (	Certificate Import Wizard
) 🦻 (	Certificate Import Wizard Tificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for
-) 🝠 (	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.
) 🦻 (	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate
) 🦻 (	Certificate Import Wizard  ttificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Elace all certificates in the following store
€ ₽ (	Certificate Import Wizard  Tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Automatically select the following store Certificate store: Certificate store:
€ ₹	Certificate Import Wizard  Tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Automatically select the following store Certificate store: Certificate store:
€ ₹	Certificate Import Wizard  Tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Automatically select the following store Certificate store: Certificate store:
€ ₽ (	Certificate Import Wizard  Tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Automatically select the following store Certificate store: Certificate store:
€ ∌ (	Certificate Import Wizard  Tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Automatically select the following store Certificate store: Certificate store:
€ ₽ (	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Automatically select the following store  Certificate store:  Trusted Root Certification Authorities  Browse
) 🖉 (	Certificate Import Wizard  tificate Store Certificate stores are system areas where certificates are kept.  Windows can automatically select a certificate store, or you can specify a location for the certificate.  Automatically select the certificate store based on the type of certificate  Automatically select the following store  Certificate store:  Trusted Root Certification Authorities  Browse

E	🦻 Certificate Import Wi	2010
	Completing the Co	ertificate Import Wizard
	The certificate will be importe	ed after you dick Finish.
	You have specified the follow	ving settings:
	Certificate Store Selected b	y User Trusted Root Certification Authorities
	File Name	C: \Users \Administrator.DI \Desktop \gw \nist.pfx
		N
_		
		<u>F</u> inish Cance

28. Open the Certificate Import Wizard again for the Personal store.

	*
💿 🝠 Certificate Import Wizard	
Welcome to the Certificate Import Wizard	
·····	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network	
connections. A certificate store is the system area where certificates are kept.	
Store Location	
O Current User	
Local Machine	
To continue, click Next.	
N	
Next Cance	

#### 29. Click Next.

30. Browse to the **GlasswallLicenseValidation** certificate.

	Open					×
🔄 🕘 ▾ ↑ 🚺 ▸ T	his PC → Desktop → gw → NIST	~ ¢	Search NIS	T		Q,
Organize 🝷 New folder				•	-	
🔆 Favorites	Name	Date mod	dified	Туре		Size
Desktop	GlasswallLicenceValidation	1/26/2018	3 3:04 PM	Security	Certificate	2
퉳 Downloads 📃 Recent places						
🖳 This PC						
👊 Network						
	<					>
File n	name: GlasswallLicenceValidation	~	X.509 Cert	tificate (*.	cer;*.crt)	~
			Oper	n	Cance	el
ick <b>Open.</b>				<u>N</u>		đ
		×				
File to Import Specify the file you v Eile name: C:\Users\Administra Note: More than on Personal Informal	want to import. ator.DI\Desktop\gw\\IIST\GlasswallLicenceValid: e certificate can be stored in a single file in the following f tion Exchange- PKCS #12 (.PFX,.P12)	/se				
File to Import Specify the file you v Elle name: C:\Users\Administra Note: More than on Personal Informal Cryptographic Me	vant to import. ator.DI\Desktop\gw\NIST\GlasswallLicenceValide e certificate can be stored in a single file in the following f	/se				

#### 32. Click Next.

e certificates are kept.
icate store, or you can specify a location for
store based on the type of certificate
g store
Browse
N
$\sim$

33. Click Next.

📀 🍠 Certificate Import Wizard	X
Completing the Certifi	icate Import Wizard
The certificate will be imported afte	r you click Finish.
You have specified the following se	
Certificate Store Selected by User Content	Trusted Root Certification Authorities
File Name	C:\Users\Administrator.DI\Desktop\gw\nist.pfx
	2
	<u> </u>

- 34. Click Finish.
- 35. Open IIS Manager by right-clicking the server in Server Manager.

<b>e</b> i	Internet Informa	ation Services (IIS) Manager	_ <b>D</b> ×
🕥 💐 🕨 Start Page			📴 🖂 🟠 🕡 🗸
<u>File V</u> iew <u>H</u> elp			
Connections	Meresoft Internet Information Serv Application Server Manager	ices 8	-
▶ - ♥ GLASSWALL (DI\Administrate	Recent connections	Connection tasks	Online resources
	Name     Server       ♥     GLASSWALL     Iocalhost       <	Connect to localhost Connect to a server Connect to a site Connect to an application	IIS News and Information IIS Downloads IIS Forums TechNet MSDN ASP.NET News Microsoft Web Platform Enable IIS News
	IIS News is disabled, click the Enable IIS News lin	ik to get the most recent online news.	
	- - -	-	
<			
Ready			

#### 36. Navigate to the **Default Website** in the tree.

<b>V</b> j	Internet Information Services (IIS) Manager	_ <b>□</b> ×
GLASSWALL > Sites	Default Web Site	😰 🗵 🟠 😰
File View Help		
Connections	Default Web Site Home	Actions  Construction  Actions  Construction  Actions  Construction  Con
< <u> </u>	Authentic Compression Default Directory Document Document Directory Default Directory Default Directory Dire	Configure Limits ? Help
Ready		e

37. Click **Bindings** on the right sidebar.

			Site	Bindings	? X
Type http	Host Name	Port 80	IP Address *	Binding Informa	<u>A</u> dd <u>E</u> dit <u>R</u> emove <u>B</u> rowse
					<u>C</u> lose

38. Click Add.

- 39. Select https for the Type.
- 40. Select All Unassigned for IP address.
- 41. Select the **domain certificate** for **SSL certificate**.

	Add Site	e Binding			?	x
<u>T</u> ype: https	IP address:		P <u>o</u> rt:			
Host name:	ame Indication	 L3				
SSL certi <u>f</u> icate: *di.ipdr		~	Se <u>l</u> ect	Vi	ew	
			ОК	С	ancel	

- 42. Click OK.
- 43. Select the http binding.

			Site B	indings		?
Type http https	Host Name	Port 80 443	IP Address * *	Binding Informa		Add Edit Remove Browse
Click Re	move.		Site Bind	lings		<u>C</u> lose
(	Are you	sure yo	u want to re	move the select	ted bindin	g?
		Ŗ	es	<u>N</u> o	Can	icel

45. Click Yes.

Site Bindings					?
Туре	Host Name	Port	IP Address	Binding Informa	<u>A</u> dd
https		443	*		<u>E</u> dit
					Remove
					<u>B</u> rowse
			R		
			~		
					<u>C</u> lose

- 46. Click Close.
- 47. Restart the IIS server. The Glasswall FileTrust console should now be accessible through a browser. (For example, https://glasswall.di.ipdr/AdministratorConsole). Ensure that there are no certificate errors.

# 2.7.2.5 Install the Smtp Analysis Agent

#### 1. Run SmtpAnalysisAgentInstaller.msi.

😥 Glasswall Inbo	und SMTP Analysis Agent Setup 📃 🗖 🗴
	Welcome to the Glasswall Inbound SMTP Analysis Agent Setup Wizard
ASSV UST EVERY	The Setup Wizard will install Glasswall Inbound SMTP Analysis Agent on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Ъ Е	, , , , , , , , , , , , , , , , , , ,
ľ	Back Next Cancel

- 2. Click Next.
- 3. Check the box next to I accept the terms in the License Agreement.

😸 Glasswall Inbound SMTP Analysis Agent Setup 📃 🗖 🗙
End-User License Agreement Please read the following license agreement carefully
END USER LICENCE AGREEMENT (EULA)
This licence agreement is between Glasswall Solutions Limited (company number 05573793) whose registered address is 18A St. James's Place, London, SW1A 1NH ("Company") and you (as an individual installing the software and also, where applicable, the organisation on whose behalf the individual is acting) ("You" "Your" "Customer"). IMPORTANT: BY ELECTING TO INSTALL THE SOFTWARE OR BY HAVING THE SOFTWARE INSTALLED ON YOUR COMPUTER SYSTEM BY COMPANY OR A THIRD PARTY (WHICH WILL BE DEEMED TO ACT AS YOUR AGENT WITH YOUR EXPRESS CONSENT), YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENCE. HOWEVER, IF YOU HAVE V
Print Back Next Cancel

- 4. Click Next.
- 5. For Listening port, enter 25.
- 6. For **Management service URL**, correct the domain to be the web domain of the IIS server (for example, glasswall.di.ipdr).
- 7. For the **Relay endpoints,** enter the address of the Exchange server, followed by the port (for example, exchange.di.ipdr:25).
- 8. For the **TLS certificate thumbprint**, enter the value from the **thumbprint** field on the certificate, without any spaces.

闄		Applicatio	n Settings	<b>– – X</b>
	Basic Settings Listening port Unique agent Id Agent queue directory Management service URL Relay endpoints (;) DownStream Username DownStream Password Max message size (bytes) TLS Settings Relay port security TLS certificate thumbprint Ignore Mail Server Certificate	25         Inbound-SMTP-Agent-1         C:\ProgramData\Glasswall Agent\         https://glasswall.di.jpdr/GlasswallManagementServi         exchange.di.jpdr:25	Logging Settings Logging directory Log level Performance logging enabled Advanced Settings Scanning interval (ms) Event upload interval (ms) Mail relay interval (ms) No. Instances No. parallel hub uploads Minimum Disk Space Threshold (MB) Disk Space Warning Threshold (MB)	C:\Logging\         Info (and above)         False         3000         3000         3000         3000         1         1         100         200
				Back Next Cancel

#### 9. Click Next.

1		
	😸 Glas	swall Inbound SMTP Analysis Agent Setup
	Ready to i	nstall Glasswall Inbound SMTP Analysis Agent
		to begin the installation. Click Back to review or change any of your settings. Click Cancel to exit the wizard.
		L <sub>o</sub>
		Back Install Cancel
10.	Click Instal	
	👸 Glas	swall Inbound SMTP Analysis Agent Setup
		Completed the Glasswall Inbound SMTP Analysis Agent Setup Wizard Click the Finish button to exit the Setup Wizard.
	GLASSWA	L <sub>3</sub>
		Back <b>Finish</b> Cancel

11. Click Finish.

### 2.7.2.6 Distribute the Glasswall License File

1. Copy the **Glasswall License** file to the following locations, assuming **Glasswall** was installed to *C:/Program Files/Glasswall*.

File Home Sh	are	View				~
€ ⊚ - ↑ 👅 •	Thi	s PC → Desktop → gw → NIST		✓ 🖒 Search I	NIST	, A
🐌 Downloads	^	Name	Date modified	Туре	Size	
🖳 Recent places		Glasswall.lic	7/20/2018 4:09 PM	LIC File	2 KB	
🖳 This PC		GlasswallLicenceValidation	1/26/2018 3:04 PM	Security Certificate	4 KB	
📜 Desktop						
Documents						
🐌 Downloads		R				
🌗 Music		7				
📄 Pictures	≡					
1000						
Videos						
📕 Videos 🊢 Local Disk (C:)						

2. First copy it to C:/Program Files/Glasswall/ManagementService/bin.

🗲 🍥 🔻 🕇 📕 « I	Program Files 🔸 Glasswall 🕨 Manageme	ntService 🕨	✓ 🖒 Search I	ManagementService	
☆ Favorites	Name	Date modified	Туре	Size	
Desktop	\mu bin	7/24/2018 6:33 PM	File folder		
📙 Downloads	Licenses	7/24/2018 6:33 PM	File folder		
🔢 Recent places	🔊 Global	6/28/2018 7:03 PM	ASP.NET Server A	1 KB	
	🚯 NLog	6/28/2018 7:03 PM	XML Configuratio	3 KB	
This PC Desktop Documents Downloads Music Pictures Videos Local Disk (C:) DV Drive (D:) SC	i Web k	7/24/2018 6:34 PM	XML Configuratio	7 KB	

3. Then copy it to C:/Program Files/Glasswall/InboundSmtpAnalysisAgent.

1 2 = 1		InboundSmtpA	nalysisAgent		_	×
F Home S	hare	View				$\checkmark$
	« Pro	gram Files 🕨 Glasswall 🕨 InboundSmtpAnalys	isAgent 🕨	✓ C Search In	nboundSmtpAnal	ysis 🔎
🔆 Favorites	^	Name	Date modified	Туре	Size	
Desktop		🌗 Licenses	7/25/2018 5:04 PM	File folder		
鷆 Downloads		AppSettings	7/25/2018 5:05 PM	XML Configuratio	2 KB	
📃 Recent places		ARSoft.Tools.Net.dll	9/30/2017 9:27 PM	Application extens	293 KB	
		BouncyCastle.Crypto.dll	4/8/2018 8:30 PM	Application extens	2,316 KB	
🌉 This PC		🚳 CommandLine.dll	1/10/2018 11:05 PM	Application extens	182 KB	
膧 Desktop	≡	🚳 DiscUtils.dll	6/14/2013 5:28 PM	Application extens	979 KB	
Documents		EntityFramework.dll	10/23/2017 1:15 PM	Application extens	5,103 KB	
鷆 Downloads		glasswall.classic.dll	7/5/2018 1:19 PM	Application extens	41,777 KB	
🌗 Music		🚳 Glasswall.Common.dll	7/6/2018 4:04 PM	Application extens	147 KB	
📄 Pictures		Glasswall.lic	7/20/2018 4:09 PM	LIC File	2 KB	
📔 Videos		Glasswall.SecuritySolution.AnalysisAgent	7/6/2018 4:05 PM	Application extens	91 KB	
🚢 Local Disk (C:)		Glasswall.SecuritySolution.DataTransferO	7/6/2018 4:04 PM	Application extens	80 KB	
🚺 DVD Drive (D:) S	SC	🚳 Glasswall.SecuritySolution.Domain.dll	7/6/2018 4:05 PM	Application extens	684 KB	
	$\sim$	Interpretended States Contract States Sta	7/6/2018 4:05 PM	Application	46 KB	_

4. Lastly copy it to C:/Program Files/Glasswall/AdministratorConsole/bin.

F Home Share H S € ⊚ ▼ ↑ 🚺 « Pro	View V ogram Files ► Glasswall ► AdministratorConso	le ▶ bin	✓ ♂ Search b	in	پ م
★ Favorites	Name	Date modified	Туре	Size	
Desktop	System.Net.Http.Formatting.dll	5/10/2018 10:38 PM	Application extens	181 KB	
Downloads	System.Web.Cors.dll	5/10/2018 10:37 PM	Application extens	34 KB	
Recent places	🗟 System.Web.Helpers.dll	5/10/2018 10:42 PM	Application extens	141 KB	
	🗟 System.Web.Http.Cors.dll	5/10/2018 10:39 PM	Application extens	45 KB	
💷 This PC	🚳 System.Web.Http.dll	5/10/2018 10:39 PM	Application extens	452 KB	
E Desktop ≡	🔊 System.Web.Mvc.dll	5/10/2018 10:38 PM	Application extens	543 KB	
Documents	System.Web.Optimization.dll	2/11/2014 2:26 PM	Application extens	70 KB	
Downloads	System.Web.Razor.dll	5/10/2018 10:38 PM	Application extens	265 KB	
Music	🚳 System.Web.WebPages.Deployment.dll	5/10/2018 10:42 PM	Application extens	49 KB	
Pictures	🚳 System.Web.WebPages.dll	5/10/2018 10:42 PM	Application extens	209 KB	
Videos	🚳 System.Web.WebPages.Razor.dll	5/10/2018 10:42 PM	Application extens	47 KB	
Local Disk (C:)	T4MVCExtensions.dll	5/15/2018 7:04 PM	Application extens	37 KB	
	WebActivatorEx.dll	10/5/2016 1:11 PM	Application extens	12 KB	

# 2.7.3 Configure Glasswall FileTrust

Please see <u>https://docs.glasswallsolutions.com/cloud/Content/Configuring/Office365-Integration.htm</u> for an example configuration that routes email with attachments from Office365 to Glasswall FileTrust. Glasswall then forwards email back to Office365, after processing. Note that this linked configuration does not work with on-premise Exchange setups.

Instead, to achieve the goal of routing email through Glasswall, we redirect local mail exchange (MX) records to Glasswall FileTrust. We implemented it this way because of limitations of the lab environment, but organizations should consult with the vendor for the best solution to route email through the email sanitization component, as other options may be available depending on the enterprise.

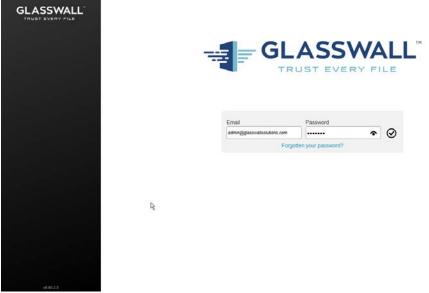
## 2.7.3.1 Create a New Administrator Account

#### 1. Open Task Manager.

2. In the Services tab, start the InboundSmtpAnalysisAgent service.

<u>File</u> Options <u>V</u> iew						
Processes Performance Use	rs Details	Services				
Name	PID	Description	Status	Group	•	
🥋 InboundSmtpAnalysisAgent		Glasswall Inbound SMTP Analysi	Starting			
🔍 wmiApSrv		WMI Performance Adapter	Stopped			:
🔍 VSS		Volume Shadow Copy	Stopped			
🔍 vmvss		VMware Snapshot Provider	Stopped			
Section 2018	1416	VMware Tools	Running			
🔍 VGAuthService	1388	VMware Alias Manager and Tick	Running			
🔍 vds		Virtual Disk	Stopped			
🔍 VaultSvc		Credential Manager	Stopped			
🔍 UI0Detect		Interactive Services Detection	Stopped			
🔍 TrustedInstaller		Windows Modules Installer	Stopped			
🌼 TieringEngineService		Storage Tiers Management	Stopped			
🔍 SQLWriter	1272	SQL Server VSS Writer	Running			
SQLSERVERAGENT		SQL Server Agent (MSSQLSERVER)	Stopped			
SQLBrowser		SQL Server Browser	Stopped			
🔍 sppsvc		Software Protection	Stopped			
Spooler 🔍	1044	Print Spooler	Running			
SNMPTRAP		SNMP Trap	Stopped			
🔍 SamSs	528	Security Accounts Manager	Running			
RSoPProv		Resultant Set of Policy Provider	Stopped			
RpcLocator		Remote Procedure Call (RPC) Lo	Stopped			
RefHost		Performance Counter DLL Host	Stopped			
NetTcpPortSharing		Net.Tcp Port Sharing Service	Stopped			
🥋 Netlogon	528	Netlogon	Running			•

- 3. Close Task Manager.
- 4. Open a browser and navigate to the **Glasswall Administration Console** (for example, http://glasswall.di.ipdr/AdministratorConsole).
- 5. If this is the first time logging in, the default account will be **admin@glasswallsolutions.com**, and the password is **Welcome1?**.



6. Log in using these credentials.

GLASSWALL	Supported File Types			Other File Types	
Administrator Console	Files 0	Sanitised / Remediated 0		Files 0	
Contraction of Contra	Outbound Emails				
File Release Requests 💿	Total Emails 0	Total Files 0			
	Supported File Types			Other File Types	
Outbound SMTP Policy	Files 0	Sanitised / Remediated		Files 0	
Configuration	Inbound SMTP Age	nt Status			
Accounts	Active	Inactive	Inbound Queues	Scan Queues	Inspection Queues
Your Account	1 Outbound Queues 0	0 Reporting Queues 0	0 Failed Queues 0	0 Unprocessable Queues 0	0
) Logout	Outbound SMTP Ag	jent Status			
	Active	Inactive 0	Inbound Queues	Scan Queues	Inspection Queues te Window0

7. On the left sidebar, click Accounts.

GLASSWALL TRUST EVERY PILE		nt P + B × O glasswall.dupd	×				•
THOST EVENY FILE	Accoun	ts					
Administrator Console		Name	En	nail		Security Group	Account Locked
Transaction Log	0	Administrator	admin@glassw	allsolutions.com	Pri	ncipal Administrator	
File Release Requests ()			() Add	Je Edit	Unlock 👔	Delete	
Inbound SMTP Policy	Security	y Groups					
Outbound SMTP Policy		Name				Security Roles	
Reporting					Edit le	nbound Policy Catalogue abound Policy Catalogue lish of Inbound Policy Catalog	jue
Configuration						lish of Inbound Policy Catalog utbound Policy Catalogue	jue
Accounts					Edit O	utbound Policy Catalogue sh of Outbound Policy Catalo	ave
Your Account	0	Principal Admir	vistrator		Approve Publi Ac E	sh of Outbound Policy Catalo count Administration Export Retained File Delete Retained File	
Logout					R Viev	ve File Release Request lequest File Release v System Configuration System Configuration Create Reports	
	0	Standard U	lser			Activate Windows	
			Ð	Add 🖉 Ed	t 💼 Delet		Panel to activate Windows.

- 8. Under Accounts, click Add.
- 9. Enter the name and email address of an administrator account from the email server.
- 10. Select Principal Administrator for Security Group.

🕢 🦉 https://glasswall.dl.ipde/Administ	torConsole/Account D - 🖶 C 🧔 Glasswall   Accounts 🛛 🕅	L= 0
GLASSWALL	Create Account	
Administrator Console	Name	
Transaction Log	Administrator	
File Release Requests (a)	Email	
Inbound SMTP Policy	Administrator@d.ipdr	
	Security Group	
Outbound SMTP Policy	Principal Administrator	
Reporting	$\otimes$	
Configuration	1.8	
Accounts		
Your Account		
Logout		
		Activate Windows
		Go to System in Control Panel to activate Windows.

11. Click the **checkmark** button when finished.

GLASSWALL		anne - I hereda he					
TRUST EVERY FILE			User	Administrator@di.ipdr	created succes	istutly.	
Administrator Console	Accounts						
Transaction Log		Name		Email		Security Group	Account Locked
🚡 File Release Requests 💿	0	Administrator	admin@glas	swallsolutions.com		Principal Administrator	
Inbound SMTP Policy	0 &	Administrator	Adminis	trator@di.ipdr		Principal Administrator	
Outbound SMTP Policy	D <sub>2</sub>		Add	/ Edit	Unlock	Doleto	
Reporting	Security	Groups					
Configuration		Name				Security Roles	
Accounts					l Reques Approve Vi E	New Inbound Policy Catalogue Edit Inbound Policy Catalogue I Publish of Inbound Policy Catalogu Publish of Inbound Policy Catalogue ew Outbound Policy Catalogue dit Outbound Policy Catalogue	20
U Logout	0	Principal Adminis	strator		Approve	Publish of Outbound Policy Catalog Publish of Outbound Policy Catalog Publish of Outbound Policy Catalog Export Retained File Detect Retained File Detect Retained File Request File Release New System Configuration Own Create Reports	ue

12. The new administrator account should be created.

Mail						Ū.	?
earch Mail and Peopl	e P	😧 New   👻 🧯 Delete Archi	ive Junk Sweep	Move to Y Catego	ries 🗸 🚥		2
Favorites		Inbox	All 🗸	Your acco	ount has been created		
Inbox	168	Today	~	_			
Sent Items Drafts		Administrator@DI.IPDR	8.23 PM		histrator@DI.IPDR istrator; ¥	Reph Wed 7/25/20	
Administrator		Account Created Your account has been a	Printed, Pre				
Inbex	368	Mik Un hey hey lookie	337 PM				
Drafts		No preview is available.	441100				
Sent Items		Yesterday			CLASS	214/411	
Deleted Items		Mik Un			GLAS	SWALL	
Junk Email Notes		(No subject) No preview is available.	Tue 11:23 PM		Account Created		
		Mik Un testing omg adfeedheidede	Tue 11:23 PM From		Your account has been created. Please con password by clicking <u>here</u> .	firm your email address and set up a	
		Mik Un			© 2018 Glasswall Solutions	TRUST EVERY FILE	
		please work No preview is available.	Tue 11:22 PM				
		Mik Un 223542345 No preview is available.	Tue 11:22 PM				
		Mik Un	Tue 11/21 PM			Activate Windows Se to System in Control Panel to activate Windo	

13. Check the email inbox of the specified email address for a confirmation email, and click the link in the email.

GNO			_ 0
and the second sec	vstratorConsole/Account P = 🔒 C 🧭 Glasswall   Accounts	Mail - Administrator - Outlook 🖉 Glasswall   Accounts	*
GLASSWALL	Reset Password		
Administrator Console	Email		
Transaction Log	Password		
File Release Requests 💿	Confirm password		
Disbound SMTP Policy			
Cutbound SMTP Policy	$\odot$		
Reporting			
Configuration			
Accounts			
Account			
ப் Logout			
			Activate Windows Go to System in Control Panel to activate Windows.
STREET, STREET			

- 14. Enter the email address as well as a password for this account.
- 15. Log in as this user, and then go to Accounts.
- 16. Select the old (default) Administrator account.

Administrator Console     Administrator Console     Transaction Log     File Release Requests	•	Name					
- 	•	1990 (1997) 2	En	nail		Security Group	Account Locked
File Release Requests		Administrator	admin@glassw	allsolutions com		Principal Administrator	
	•	Administrator	Administra	tor@di.ipdr		Principal Administrator	
Inbound SMTP Policy	Securit	y Groups	🕀 Add	🖍 Edit	🚹 Unlock	<b>B</b> pelete	
Outbound SMTP Policy	Securit	Name				Security Roles	
Reporting					1	View Inbound Policy Catalogue	
Configuration					Reques Approve	Edit Inbound Policy Catalogue t Publish of Inbound Policy Catalogue e Publish of Inbound Policy Catalogue iew Outbound Policy Catalogue	
Your Account	0	Principal Admi	nistrator		E Request	dit Outbound Policy Catalogue Publish of Outbound Policy Catalogu Publish of Outbound Policy Catalogu Account Administration Export Relained File	
ს Logout						Delete Retained File Approve File Release Request Request File Release View System Configuration Edit System Configuration Create Reports Approvements and the second seco	

17. Click Delete.

GLASSWALL	Administrator 0	Console / Accounts			
			User admin@glasswallsol	ations com deleted successfully	
Administrator Console	Account	ts			
Transaction Log		Name	Email	Security Group	Account Locked
File Release Requests 💿	0	Administrator	Administrator@dl.ipdr	Principal Administrator	
Inbound SMTP Policy			🕀 Add 🛛 🥒 Edit	Unlock 📋 Defete	
Outbound SMTP Policy	Security	Groups			
Reporting		Name		Security Roles	
				View Inbound Policy Catalogu Edit Inbound Policy Catalogu Reguest Publish of Inbound Policy C	e
Accounts				Approve Publish of Inbound Policy G View Outbound Policy Catalog	atalogue
Your Account	0	Principal Admini	strator	Edit Outbound Policy Gatalog Edit Outbound Policy Gatalogu Request Publish of Outbound Policy C Approve Publish of Outbound Policy C Account Administration	ue Catalogue
) Logout				Export Retained File Delete Retained File Approve File Release Reques	et
				Request File Release View System Configuration Edit System Configuration	
	0	Standard Us	er		

18. This should remove the old administrator account (note: failure to remove this can result in a significant vulnerability for this server).

# 2.7.3.2 *Configure Notifications and Policies*

- 1. Click **Configuration** on the left sidebar.
- 2. Click the **Notifications** tab.

🕘 🝘 https://glasswall.dk.ipdr/AdministratorConsole/Configur 🔎 + 🖨 🗘 🜌 Mail - Administrator - Outlook 🛛 🗐 Glasswall   Configuration	×
Butter // gittermarkt & index : Seminarity Console Configur D	Subject Line The subject of the email used to release a file. Vear tile has been released by Glasswall Email Body The content of the email used to release a file. The antached file(a) have been checked and released in accordance with regramisation policy. %ReleaseDetails%
Reporting         Mail Footer Text           The text inserted at the bottom of processed emails.         Configuration           Configuration         This mail has been protected by Glasswall.           Accounts         V	Please contact IT support for more information.
Your Account	Email Body The content of the email used to deny a file release. The following file(s) have been denied for release in accordance with organication policy. %Release Details% Please contact IT support for more information
-0 (C 2 A	Go to System in Control Panel to activate Windo

3. On this page, enter the web domain in the first input box (for example, glasswall.di.ipdr).

- 4. The various input boxes on this page allow you to specify the messages sent when files are quarantined, released, or prevented from being released.
- 5. Click the **Inbound Agents** tab.
- 6. Select **Analysis and Protect** for **Processing Mode.** (This analyzes and quarantines/reconstructs files based on policy.)
- 7. Select **Active** for **File Preview Mode.** (This provides clients with a preview of their received files if they were quarantined, so they can determine whether they should request the file be released.)
- 8. Enter the **domain** for **Allowed Domains** (for example, di.ipdr).

	Console/Configu 🔎 * 🗎 C 🔤 Mail - Administrator - Outlook 🛛 Glasswall   Configuration 🛛 🛛		0
and a state of the second s			- UU
GLASSWALL	Processing Mode		
TRUST EVERY FILE	Configure Glasswall Inbound SMTP Agent Processing Mode		
Administrator Console	Analysis and Protect		
Transaction Log	File Release Service Hostname		
File Release Requests	The Hostname to be used for File Release service		
	https:// glasswalt.di.jpdr //GlasswallFileReleaseRequestService		
Inbound SMTP Policy	and the second se		
	File Preview Mode		
Outbound SMTP Policy			
	Disabled - File Preview is not generated Active - Generate and attach to emails		
Reporting	Passive - Generate but do not attach to emails		
Configuration	Active V		
Accounts	File Preview Timeout		
and the second			
Your Account	Maximum File Preview processing time in seconds	De .	
	300	·~	
) Logout	Allowed Domains		
	Domains that the Inbound SMTP Agent is allowed to relay mail to (separate with semicolon)		
	dipar		
		Activate Windows	
v100.2.5		Go to System in Control Panel to activate	Save
Do you	want AutoComplete to remember web form entries? Learn about AutoComplete	Yes No x	

9. Click Save.

# 2.7.3.3 Configure Inbound SMTP Policy

This section discusses Simple Mail Transfer Protocol (SMTP) policy under Glasswall FileTrust. There are several layers of granularity for configuring Email policy. Because policy is dependent on the organization's needs, we will not prescribe a policy but will showcase how a policy is formed.

Policy in Glasswall FileTrust consists of **Sender Groups, Receiver Groups, Content Management Policies,** and **ThreatCensor Policy Sets. Receiver groups** allow for the specification of users who receive email. **Sender groups** allow for the specification of emails received from specific senders. **Content Management Policies** refer to the default policy on various filetypes. Lastly, **ThreatCensor Policy Sets** allow for the specification of policy on specific error codes; through this it is possible to place policies on encrypted email, for example, depending on the organization's needs.

### 2.7.3.4 Create a Receiver Group

- 1. On the left sidebar, click Inbound SMTP Policy.
- 2. Click Draft Policy Catalogue.

-			L-
🕖 💮 Mtps://gianwall.dLipdr/Admin	satustorConsole/Inbound (D + 🗎 C 🔤 Mail - Administrato	r - Outlook 🧔 Glasswall   Policy Catalogue 🛛 🛛	
GLASSWALL	Administrator Console / Inbound SMTP Policy	Ŷ	
TRUST EVERY PILE	Inbound SMTP Policy Cat	alogues	
Administrator Console		Published	Published By
Transaction Log	Current Policy Catalogue	7/25/2018 1:33:50 AM	Admin
The second se		Updated	Updated By
File Release Requests 🕕	Draft Policy Catalogue	7/25/2018 1:33:50 AM	Admin
Inbound SMTP Policy			Publish
Outbound SMTP Policy			
Reporting			
Configuration			
Accounts			
Your Account			
) Logout			
			Activate Windows Go to System in Control Panel to activate Windo
	Do you want AutoComplete to remember web form entries?	Learn about AutoComolete	Yes No ×

3. Under Receiver Groups, click Add.

-		- 0
🕘 👩 https://glasses9.dLipde/Admia	atisterCensels/inbound D + 🔒 C 📷 Mail - Administrator - Outlook 🦪 Gasswall   Draft Inbound S., 🗵	n s
GLASSWALL TRUST EVERY FILE	Al Senders V	ecy 🔽
Administrator Console	ThreatCensor Policy Set Organisation ThreatCensor Policy Set Add	
Transaction Log		
Inbound SMTP Policy	Sender Groups There are no Sender Groups in this Policy Catalogue.	⊕ Add
Outbound SMTP Policy		
Reporting	Receiver Groups	(†) Add
Configuration	There are no Receiver Groups in this Policy Catalogue.	0
Accounts	3	
Your Account	Content Management Policies	() Add
	Name	
) Logout	Organisation Content Management Policy	Details .
	ThreatCensor Policy Sets	DbA 🕀
		vate Windows
	Organisation ThreatCensor Policy Set	System in Control Panel to activate Windows. Details

4. Under User Defined Mailboxes, click Edit.

🗧 🛞 🦉 https://glasswall.dkipde/Adm	nistratorConsole Tebeund D + 🔒 C 🔯 Mail - Administrator - Outlook 🖉 Glasswall   Receiver G		
GLASSWALL	Administrator Console / Inbound SMTP Policy / Policy Catalogue / Receive	r Group Details	
	New Receiver Group 2		
Administrator Console			🖍 Edi
📰 Transaction Log	LDAP Synchronisation Settings		
File Release Requests 💿			🖌 Edi
D Inbound SMTP Policy	Server		
Outbound SMTP Policy	myserver/CN+instance.DC=company.DC=COM		
Reporting	User Name		
Configuration	Password		
	******		
Accounts	Query		
Your Account	(& (department-department name) (co-country code))		
in the second	Mailbox Attribute Name		
	mat	Da la	
Logout			0
	User Defined Mailboxes		
	There are currently no user-defined mailboxes for this receiver group		Activate Windows
+8.00.2.5			

5. Enter the email address(es) of users who should be in this receiver group.

			- 0 ×
🗲 🛞 🗿 https://glasswall.dkipde/Admin	stratorConsole/Inbound 🔎 = 🔒 🖒 🔤 Mail - Administrator - Outlook 🛛 🙋 Gasswall	Receiver Group	n * 0
GLASSWALL TRUST EVERY FILE	New Description Course 0 Mailleanes	- concerned setting settings - scale concerned setting reasonable	
	New Receiver Group 2 Mailboxes		
Administrator Console	Add User-Defined Mailbox		
Transaction Log	E-Mail Address		
File Release Requests 💿	Add		
Inbound SMTP Policy	User Defined Mailboxes	14	
Outbound SMTP Policy	There are currently no user-defined mailboxes for this receiver group		
Reporting			
Configuration			
Accounts			
Your Account			
db tours			
U Logout			
		Activate Windows Go to System in Control Panel I	lo activate Windows.
+6.00.2.5			

- 6. Click Add.
- 7. When finished, return to the **Policy Catalogue** page.

				- 0
🕤 🗊 https://glasswall.dk.ipde/Admir	nistratorConsole/Inbound D + 🖶 X 🔤 Mail - Administrator - Outlook 🔿 Waiting for glasswalldsipdr - X			•
GLASSWALL	Threat/Censor Policy Set Organisation Threat/Censor Policy Set Add			
Administrator Console				
Transaction Log	Sender Groups			🕀 Ad
File Release Requests 💿	There are no Sender Groups in this Policy Catalogue.			
Inbound SMTP Policy	Persiliar Crame			(+) Ad
Outbound SMTP Policy	Receiver Groups			<b>.</b>
Reporting	New Receiver Group-4		Details	+ Undo
Configuration	allowed to receive encryption		Details	Delete
Accounts				
Your Account	Content Management Policies	R		( Ad
	Name			
Logout	Organisation Content Management Policy		Details.	
	ThreatCensor Policy Sets			(+) Ad
	Name	Activate Windows Go to System in Control		te Windows.
	Organisation ThreatCensor Policy Set		Details	

## 2.7.3.5 Create a ThreatCensor Policy Set

### 1. Under ThreatCensor Policy Sets, click Add.

	inen inneutoeniot	or Policy Set	1
Administrator Console	Explicit ThreatCenso	r Policies	
Transaction Log	There are no Explicit ThreatCer	nsor Policies in the Pol	
File Release Requests 💿	Default ThreatCenso	r Policies	1
Inbound SMTP Policy	File Type	Action	
-) Outbound SMTP Policy	Microsoft Excel (Binary)	Disallow	
	Microsoft Excel (OOXML)	Disallow	
Reporting	Microsoft Word (Binary)	Disallow	
Configuration	Microsoft Word (OOXML)	Disallow	
Accounts	Microsoft PowerPoint (Binary)	Disallow	
Your Account	Microsoft PowerPoint (OOXML)	Disallow	
	PDF	Disallow	
	GIF	Disallow	
Logout	JPG	Disallow	
	PNG	Disallow	
	ZIP	Disallow	

2. Under Explicit ThreatCensor Policies, click Edit.

🗲 🕤 💋 https://glasswall.di.jpdr/Adminis	stratorConsole/Inbound 🔎 👻 🚔 🖒 🔛 Ma	il - Administrator - Outlock 🖉 Glassi	wall   Edit Explicit Thre ×		_ <b>0 ×</b> ∩ ★ 0
GLASSWALL TRUST EVERY FILE	Administrator Console / Inbound		e / ThreatCensor Set Policy Details / Edi	t Explicit ThreatCensor Policies	
Administrator Console	Add Explicit ThreatCer	nsor Policy			
File Release Requests     The Release Requests     The Release Requests     The Release Requests	File Type	Action	Issue Signed Files	🕀 Add	
Outbound SMTP Policy	Issue Id 0B250696		Description Digital signatures present in file		Threat Level Medium
Configuration	Explicit ThreatCensor There are no Explicit ThreatCensor		e		
Counts					
() Logout					
				Activate Windows Go to System in Control Panel	to activate Windows.

- 3. Select the File Type and Action for the rule.
- 4. Under **Issue**, click the magnifying glass to search for an error code.
- 5. Return to the Policy Catalogue page when finished.

### 2.7.3.6 Create a Processing Rule

1. Under Processing Rules, select the appropriate Sender Group, Receiver Group, Content Management Policy, and ThreatCensor Policy Set.

						- 0 >
C () S https://glasswall.di.ipde/Admini [4] [dit Yiew Fgvorites Icols Help	stratorConsole/Inbound D + 🔒 C 🖾 Mail - Au	dministrator - Outlook 🦉 Glasswo	ill   Draft Inbound S	×		ń *
GLASSWALL	Sender Group	Receiver Group		Mail Delivery	Action	
TROST EVENT FILE	All Senders	✓ All Receivers	~	Blacklist	<b>·</b>	Add
Administrator Console						
Transaction Log						
File Release Requests 💿	Processing Rules Sender Group	Receiver Group	Content Mana	gement Policy	ThreatCensor Policy Set	ř.
D Inbound SMTP Policy	All Senders	All Receivers	Organisatio Managem		Organisation ThreatCenso Policy Set	r
Outbound SMTP Policy				,	13 13	
Reporting	Sender Group	Receiver Group		Content Mana	gement Policy	
Configuration	Ail Senders	allowed to receive encrypti	on 🖌	Organisation Co	ntent Management Policy	
Accounts	ThreatCensor Policy Set					
Your Account	New ThreatCensor Policy Set 1	Add				
U Logout	Sender Groups					🕀 Add
	There are no Sender Groups in this P	olicy Catalogue.				
	Receiver Groups				Activate Wind Go to System in C	Iows ontrol Panel to activate Wite Add
		N	ame			

- 2. Click Add.
- 3. This allows for granular policy for email inspection, quarantine, and reconstruction.

# 2.7.4 Configure Intelligence Sharing

1. Run DataCollectorInstaller.msi.

閿	Glasswall Data Collector Setup
	Welcome to the Glasswall Data Collector Setup Wizard
	The Setup Wizard will install Glasswall Data Collector on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	Back Next Cancel

- 2. Click Next.
- 3. Check the box next to I accept the terms in the License Agreement.

岗 Glasswall Data Collector Setup 🗕 🗖 🗙
End-User License Agreement Please read the following license agreement carefully
END USER LICENCE AGREEMENT (EULA)
This licence agreement is between Glasswall Solutions Limited (company number 05573793) whose registered address is 18A St. James's Place, London, SW1A 1NH ("Company") and you (as an individual installing the software and also, where applicable, the organisation on whose behalf the individual is acting) ("You" "Your" "Customer"). IMPORTANT: BY ELECTING TO INSTALL THE SOFTWARE OR BY HAVING THE SOFTWARE INSTALLED ON YOUR COMPUTER SYSTEM BY COMPANY OR A THIRD PARTY (WHICH WILL BE DEEMED TO ACT AS YOUR AGENT WITH YOUR EXPRESS CONSENT), YOU AGREE TO BE
BOUND BY THE TERMS OF THIS LICENCE. HOWEVER, IF YOU HAVE
I accept the terms in the License Agreement
Print Back Next Cancel

- 4. Click Next.
- 5. Select **Hashed** for **Collection Mode** (especially if your data is sensitive; this will prevent the release of any identifying information).

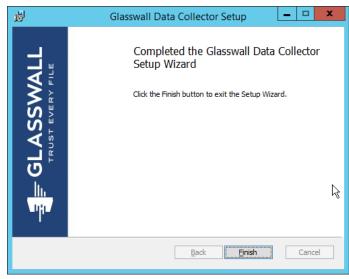
- 6. For **Integration Service Url** replace **localhost** with the name of the computer running the **Integration Service.**
- 7. Enter the **username** and **password.**

🚽 🛛 🚽 Glasswall	l Data Collector Setup 📃 🗕 🗖 🗙
Data Collector Installation Set	tings
Specify the Installation Setting for t	he Glasswall Data Collector
Collection Mode	Hashed V
License File Path	C:\Program Files\Glasswall\AdministratorConsole
Integration Service Url	https://glasswall.di.ipdr/GlasswallIntegrationServ
Integration Service Username	Administrator
Integration Service Password	
Ignore Integration Service Certificate	False ¥
Use Proxy?	False V
Web Proxy Endpoint	
Web Proxy Port	
Web Proxy Username	·
Web Proxy User Domain	·
Web Proxy Password	
Logging Directory	C:\Logging
Logging Level	Debug (and above)
	Back Next Cancel
lick <b>Next.</b>	
Glasswall	I Data Collector Setup 📃 🗖 🗙
Ready to install Glasswall Data	a Collector

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
L3
Back Install Cancel

9. Click Install.

8.



10. Click Finish.

# 2.8 Micro Focus ArcSight Enterprise Security Manager

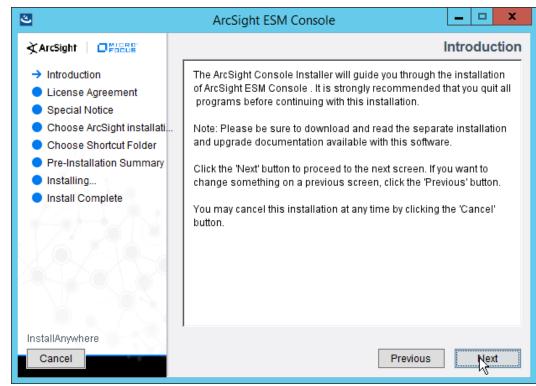
Micro Focus ArcSight Enterprise Security Manager (ESM) is primarily a log collection/analysis tool with features for sorting, filtering, correlating, and reporting information from logs. It is adaptable to logs generated by various systems, applications, and security solutions.

This installation guide assumes a pre-configured CentOS 7 machine with ESM already installed and licensed. This section covers the installation and configuration process used to set up ArcSight agents on various machines, as well as some analysis and reporting capabilities.

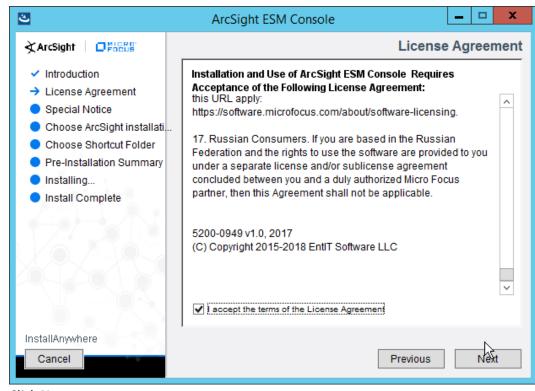
Installation instructions are included for both Windows and UNIX machines, as well as for collecting from multiple machines. Furthermore, integrations with other products in the build are included in later sections.

## 2.8.1 Install the ArcSight Console

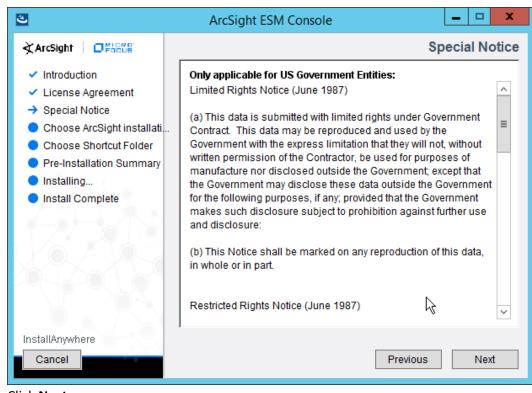
1. Run ArcSight-7.0.0.2436.1-Console-Win.exe.



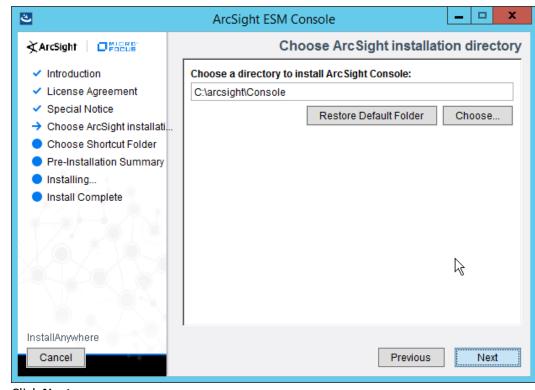
- 2. Click Next.
- 3. Check the box next to I accept the License Agreement.



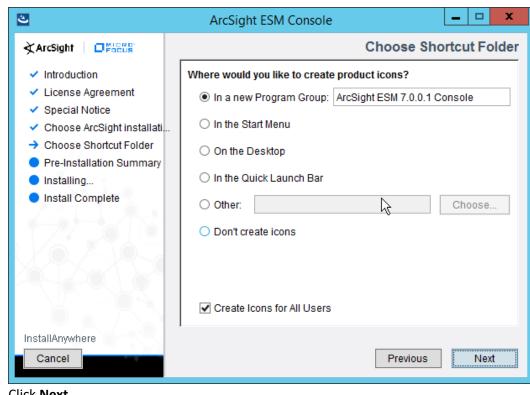
4. Click Next.



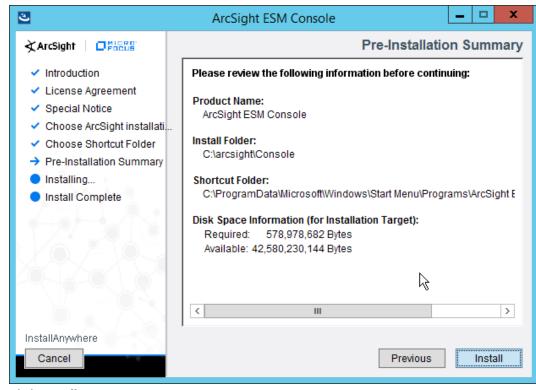
5. Click Next.



6. Click Next.



7. Click Next.

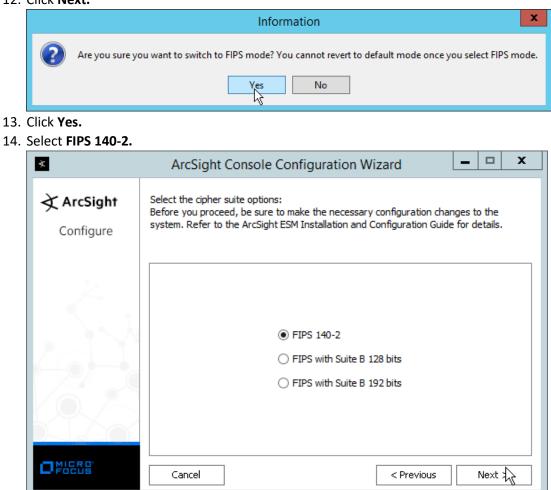


- 8. Click Install.
- 9. Select No, I do not want to transfer the settings.

*	ArcSight Console Configuration Wizard 📃 🗖 🗙
ArcSight	Do you want to transfer configuration settings from a previous ArcSight Console installation? If you installed ArcSight Console before, choosing this option will transfer settings from your previous ArcSight Console configuration to the new version.
	<ul> <li>Yes, I want to transfer the settings</li> <li>No, I do not want to transfer the settings</li> </ul>
	Cancel < Previous Next >

11. Select **Run console in default mode.** (This can be changed later according to your organization's compliance requirements.)

*	ArcSight Console Configuration Wizard 📃 🗖 🗙
ArcSight Configure	Select the mode for console to run in: WARNING 1: Do not install in FIPS 140-2, FIPS with Suite B 128 bits and FIPS with Suite B 192 bits mode unless • you are a federal agency required to comply with the FIPS 140-2, FIPS with Suite B 128 bits and FIPS with Suite B 192 bits standard, AND • you have reviewed the setup and configuration steps required for enabling FIPS 140-2, FIPS with Suite B 128 bits and FIPS with Suite B 192 bits mode • Solution of the State of
	<ul> <li>Run console in default mode</li> <li>Run console in FIPS mode</li> </ul>
	Cancel



- 15. Click Next.
- 16. Enter the hostname of the ESM server for Manager Host Name.
- 17. Enter the port that ESM is running on for Manager Port (default: 8443).

*	ArcSight Console Configuration Wizard					
ArcSight Configure	Please complete the following ArcSight Manager information. NOTE: Only IPv4 is available as a Preferred IP Protocol.					
	Manager Host Name       arcsight-esm         Manager Port       8443         Cancel       < Previous					

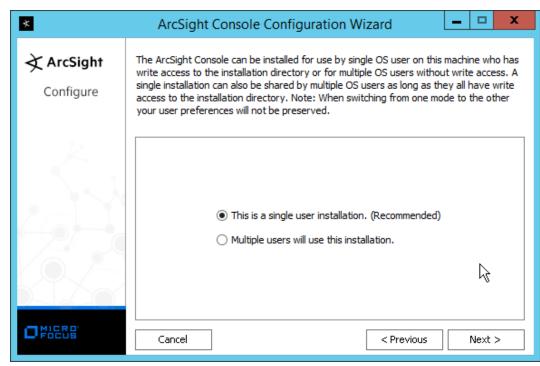
19. Select Use direct connection.

*	ArcSight Console Configuration Wizard	_		x			
ArcSight Configure	ArcSight Console can connect to ArcSight Manager using a HTTP proxy server. Please choose whether you would like to configure ArcSight Console for a proxy connection.						
	<ul> <li>Use direct connection.</li> <li>Use proxy server.</li> </ul>						
	Cancel	1	Vext >				

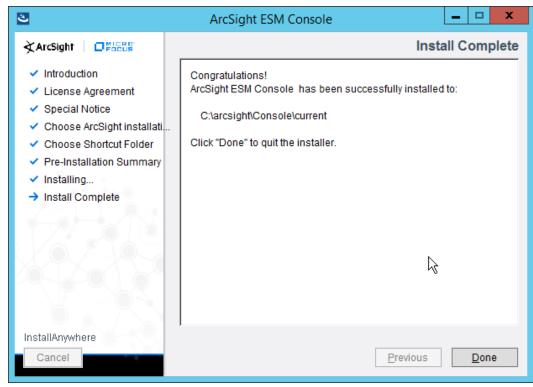
*	ArcSight Console Configuration Wizard 📃 🗖 🗙
ArcSight Configure	Please choose the authentication configuration to match the settings on ArcSight Manager. If unsure, select the first option.
	<ul> <li>Password Based Authentication</li> <li>Password Based and SSL Client Based Authentication</li> <li>Password Based or SSL Client Based Authentication</li> <li>SSL Client Only Authentication</li> </ul>
	Cancel Next >

- 21. Click Next.
- 22. Select your preferred browser.

*	ArcSight Console Configuration Wizard
ArcSight	Browser information: Please enter the path to your prefered web browser. This will be used by the console when opening any web-based application in an external browser.
	Browser Executable ome\Application\chrome.exe
	Cancel < Previous Next >



- 24. Click Next.
- 25. Click Finish.



- 26. Click Done.
- 27. Run ArcSight Console from the start menu.
- 28. Enter the username and password.

\star ArcSi	ght Console 7.0.0.2436.1 – 🗖 🗙
∢ ArcSight	Please log in
© Copyright 2018 Micro Focus or one User ID Password	arcsight
Manager	arcsight-esm 🔻

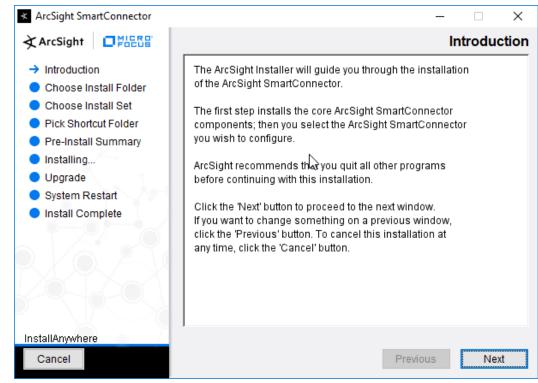
29. Click **Login.** (If you are unable to connect, ensure that the hostname of the ESM server is present in your DNS server.)

SSL Certificate	x
Do you want to trust the certificate of server's signer?	
Certificate Details Version 3	
Signature BUcFKSdkHa5dtkW6e1XIRZdLtm5eEwyM+CLFnDBIILdDAUqqVDwAFrWtl7kAevErq0qhT2lajfkg ixQ0eTQr3EvfmbKFum3BRUsBLZ0Ycnti5VQQb3nX4zjBe1YJwvzxu0dgoOVSz5/bxJeXUY0EzcO x1+N+ji7v8Kwc4o59cjnYBKlufnTMZ2AESJD+HP7cZJ5+ZWtwAO1Y7avb1xF6+JPnjEKym8kNxwM cJzz78dNAbDWsc1epmYM2P8E7u0BSQOTWtV2ErykawtEXhjocg/111gUYrHLpi8eAkagNIorXySW Cgfd9qvjLXr61x3rg7dFjrHhDe0aeIxmMk/wJA==	
Issued To CN=arcsight-esm,OU=ESM,O=Arcsight,L=95014,ST=CA,C=US	
Issued By CN=arcsight-esm,OU=ESM,O=Arcsight,L=95014,ST=CA,C=US	
Issued On Sunday, August 19, 2018 8:16:31 AM PDT	
Expires On Monday, August 21, 2023 8:16:31 AM PDT	
$\searrow$	
<u>O</u> K <u>C</u> ar	ncel

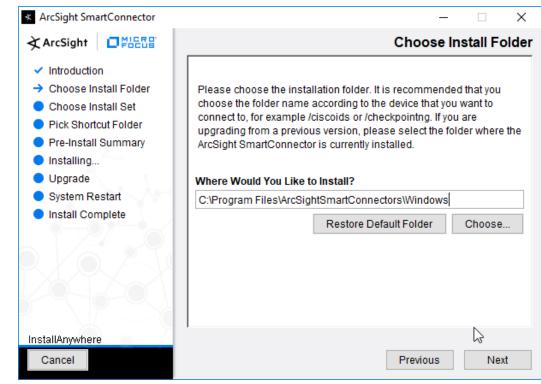
30. Click OK.

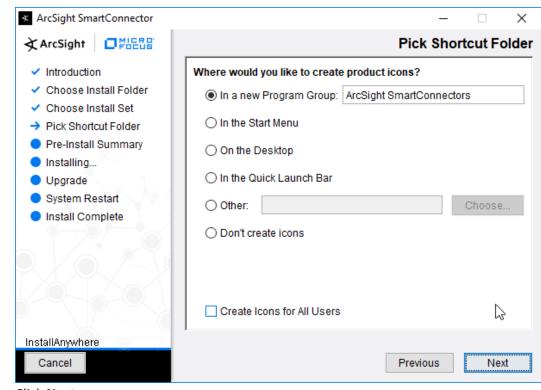
# 2.8.2 Install Individual ArcSight Windows Connectors

1. Run ArcSight-7.9.0.8084.0-Connector-Win64.exe.

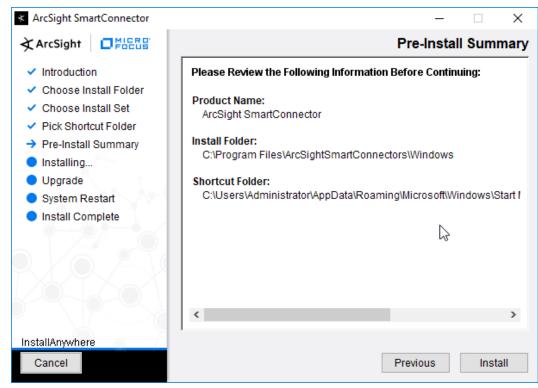


- 2. Click Next.
- 3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.





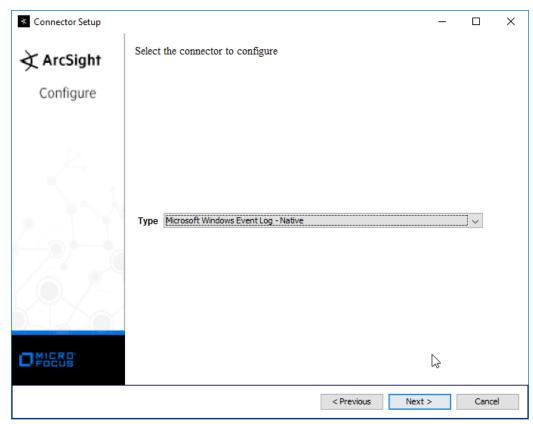
5. Click Next.



- 6. Click Install.
- 7. Select Add a Connector.

Connector Setup		ß	_		×
À ArcSight	What would you like to do?	-0			
Configure					
R					
		Add a Connector			
		<ul> <li>Set Global Parameters</li> </ul>			
		< Previous	Next >	Canc	el

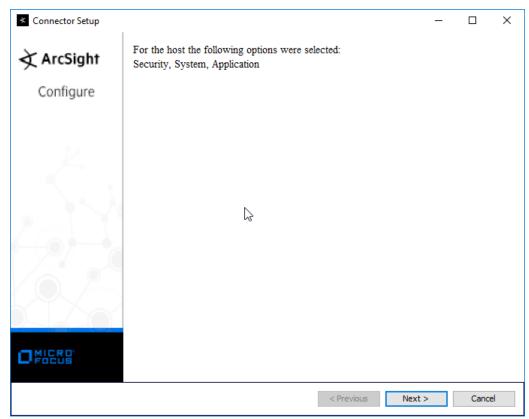
- 8. Click Next.
- 9. Select Microsoft Windows Event Log Native.



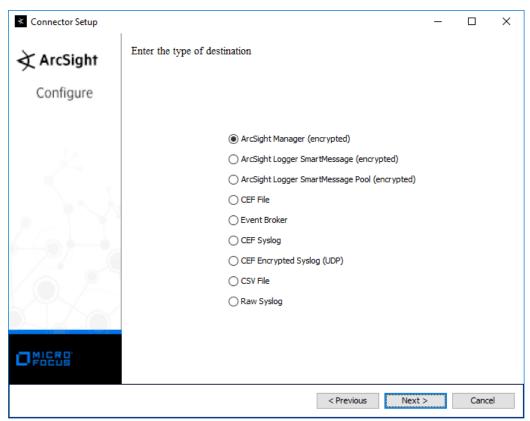
10. Click Next.

Connector Setup	- 0	×
ArcSight	Configure Parameters Select logs for event collection from local host	^
Configure	<ul> <li>✓ Security log</li> <li>✓ System log</li> </ul>	
K.	Application log ForwardedEvents log Countern loss	
5	Custom logs Source hosts for all forwarded events Do not use any source for Windows OS version	
	Use Active Directory for OS version	
	Parameters to add hosts for event collection	
	Use Active Directory	~
	< Previous Next > Ca	ncel

11. Click Next.



- 12. Click Next.
- 13. Select ArcSight Manager (encrypted).



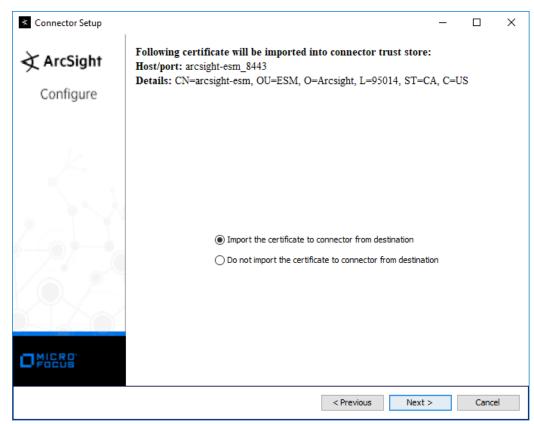
- 14. Click Next.
- 15. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.

Connector Setup				_		×
À ArcSight	Enter the destination para	meters				
Configure						
14	Manager Hostname	arcsight-esm				
	Manager Port	8443				
$\rightarrow$ $\lambda$	User	administrator				
	Password	•••••				
	AUP Master Destination	false			$\sim$	
	Filter Out All Events	false			~	
	Enable Demo CA	false			~	
MICRO						
L Focus				$\square$		
			< Previous	Next >	Can	icel

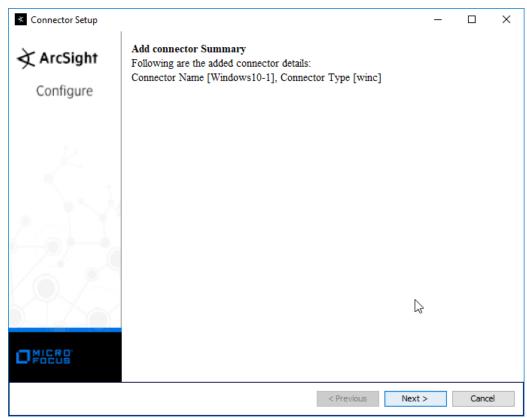
- 16. Click Next.
- 17. Enter identifying details about the system (only **Name** is required).

Connector Setup				_		×
🖈 ArcSight	Enter the connec	ctor details				
Configure						
k.						
	Name Location	Windows 10-1				
	DeviceLocation Comment	Windows 10-1 Client				
		G				
			< Previous	Next >	Cance	el

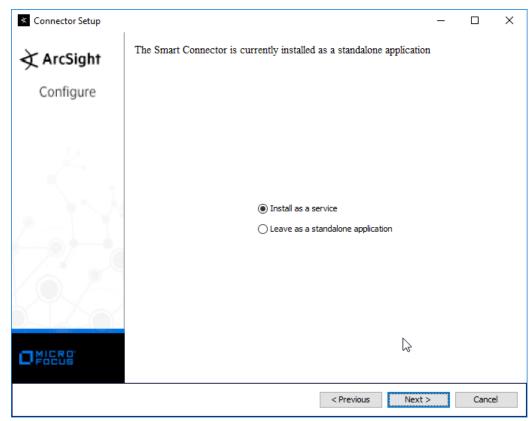
- 18. Click Next.
- 19. Select Import the certificate to connector from destination.



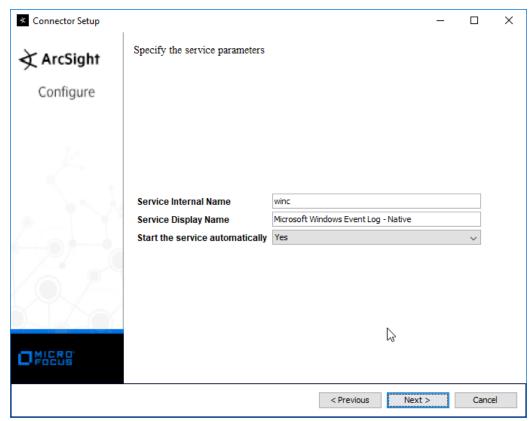
20. Click Next.



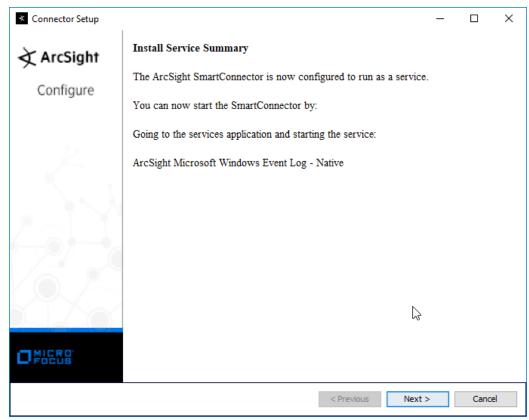
- 21. Click Next.
- 22. Select Install as a service.



23. Click Next.

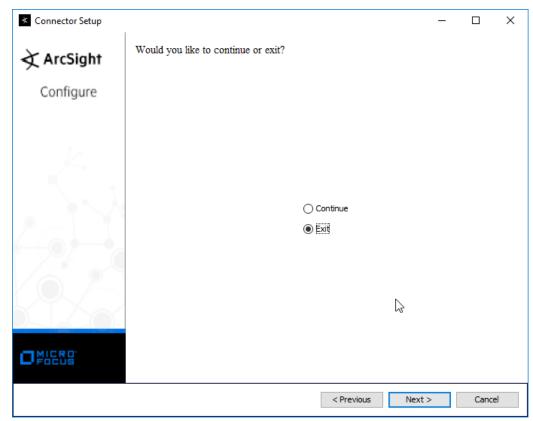


24. Click Next.

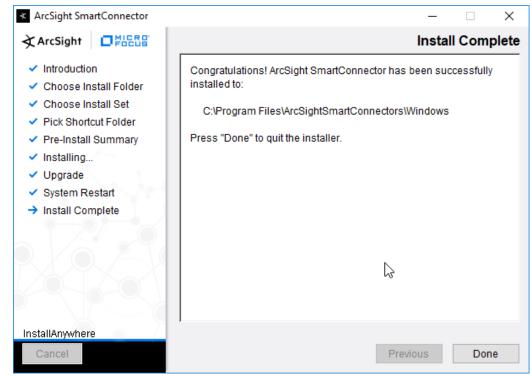


- 25. Click Next.
- 26. Select Exit.

195



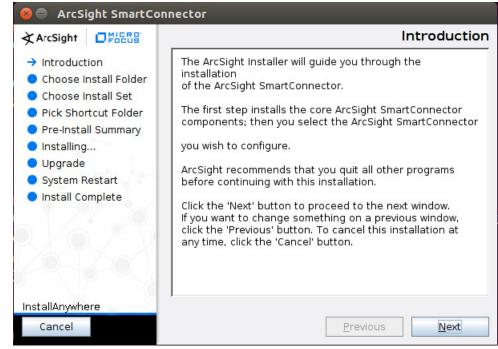
27. Click Next.



28. Click Done.

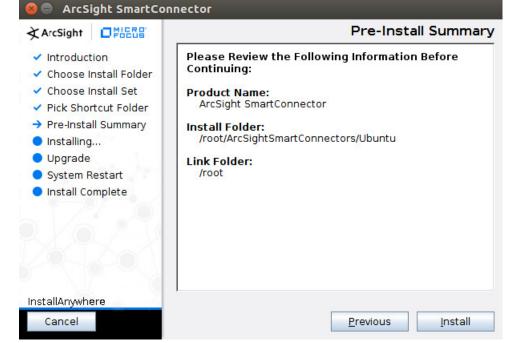
## 2.8.3 Install Individual ArcSight Ubuntu Connectors

- 1. From the command line, run:
  - > sudo ./ArcSight-7.9.0.8084.0-Connector-Linux64.bin
- 2. Enter the **password** if prompted.



- 3. Click Next.
- 4. Enter /root/ArcSightSmartConnectors/Ubuntu.
- 5. Click Next.

😣 🖨 ArcSight SmartCor	nnector
ArcSight	Choose Link Folder
<ul> <li>Introduction</li> <li>Choose Install Folder</li> <li>Choose Install Set</li> <li>Pick Shortcut Folder</li> <li>Pre-Install Summary</li> <li>Installing</li> <li>Upgrade</li> <li>System Restart</li> <li>Install Complete</li> </ul>	Where would you like to create links?         In your home folder         Other:       Choose         Don't create links
InstallAnywhere Cancel	Previous Next



- 7. Click Install.
- 8. Select Add a Connector.

🐌 🖨 🗊 Connector	Setup
À ArcSight	What would you like to do?
Configure	
2.2	
1	
1.1	Add a Connector
	Add a Connector Set Global Parameters
	< <u>P</u> revious <u>Next</u> > <u>Cancel</u>

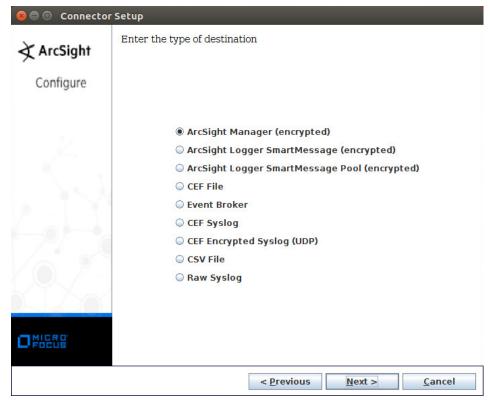
- 9. Click Next.
- 10. Select Syslog File.

🕫 🔿 💿 Connector Setup		
À ArcSight	What would you like to do?	
Configure		
K.		
1	Add a Connector Set Global Parameters	
67		
	< <u>P</u> revious <u>N</u> ext > <u>Cancel</u>	

- 11. Click Next.
- 12. Enter /var/log/syslog for the File Absolute Path Name.

Sonnecto	r Setup		
À ArcSight	Enter the parameter details		
Configure			
	File Absolute Path Name	/var/log/syslog	
	Reading Events Real Time or Batch		-
	Action Upon Reaching EOF	None	-
	File Extension If Rename Action	processed	
OFOCUS	<b>(</b>		
	< <u>P</u> rev	ious <u>N</u> ext > <u>C</u> ance	el

- 13. Click Next.
- 14. Select ArcSight Manager (encrypted).



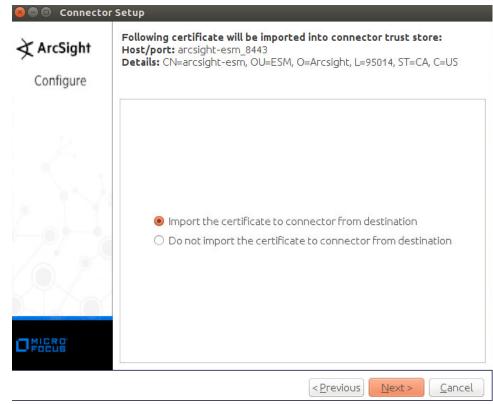
- 15. Click Next.
- 16. Enter the hostname, port, username, and password for ArcSight ESM.

Manager Hostname Manager Port User Password AUP Master Destina Filter Out All Events Enable Demo CA	8443 administrator
AUP Master Destina Filter Out All Events	nation false
Enable Demo CA	false

- 17. Click Next.
- 18. Enter identifying details about the system (only Name is required).

😣 🖨 🗊 Connector	Setup	
द्रे ArcSight	Enter the connector details	
Configure	Name Ubuntu Client Location DeviceLocation Comment	
	<	Previous Next > Cancel

- 19. Click Next.
- 20. Select Import the certificate to connector from destination.



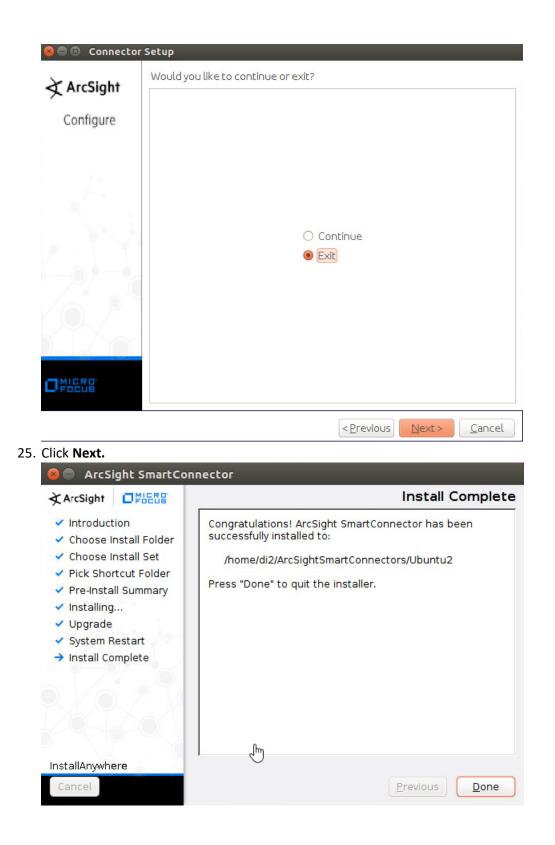
21. Click Next.

Sonnector	Setup
🖈 ArcSight	<b>Add connector Summary</b> Following are the added connector details: Connector Name [Ubuntu Client], Connector Type [syslog_file]
Configure	
D MICRD'	
	< <u>Previous</u> <u>Next &gt;</u> <u>Cancel</u>

22. Click Next.

😣 🖨 🗊 Connector	Setup
À ArcSight	To modify service configuration, you must be running as root To manually configure, log on as root and execute the following script:
Configure	/home/di2/ArcSightSmartConnectors/Ubuntu2/current/bin/arcsight agentsvc -i -u user
	To manually remove the service, log on as root and execute the following script:
	/home/di2/ArcSightSmartConnectors/Ubuntu2/current/bin/arcsight agentsvc -r
	< <u>P</u> revious <u>N</u> ext > <u>C</u> ancel
Click Novt	

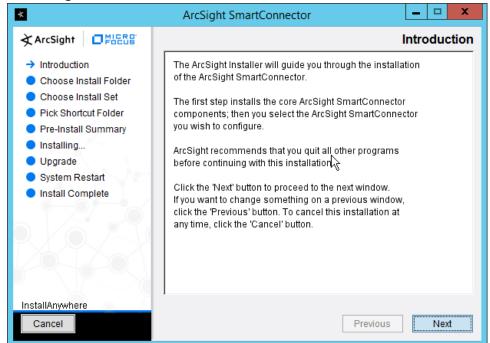
- 23. Click Next.
- 24. Select Exit.



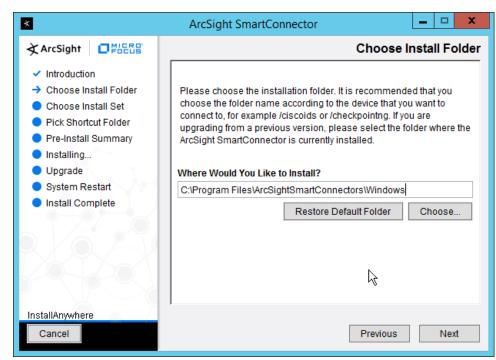
### 26. Click Done.

## 2.8.4 Install a Connector Server for ESM on Windows 2012 R2

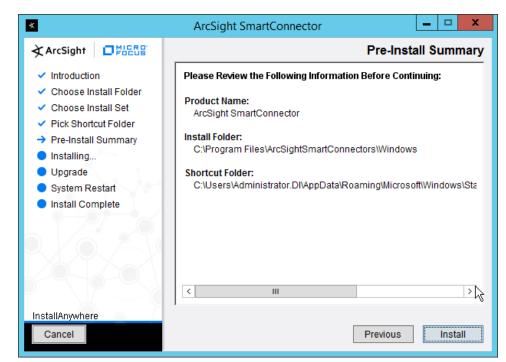
1. Run ArcSight-7.9.0.8084.0-Connector-Win64.exe.



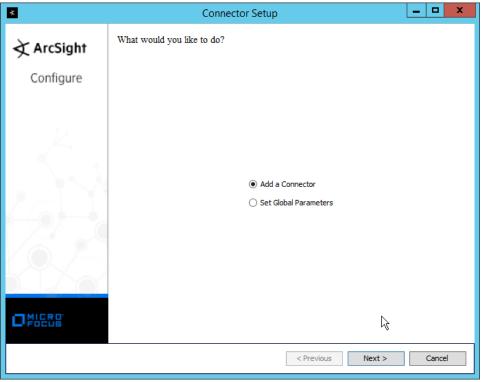
- 2. Click Next.
- 3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.



×.	ArcSight SmartConnector
À ArcSight □ ₩₩₩₩₩₩	Pick Shortcut Folder
<ul> <li>Introduction</li> <li>Choose Install Folder</li> <li>Choose Install Set</li> <li>Pick Shortcut Folder</li> <li>Pre-Install Summary</li> <li>Installing</li> <li>Upgrade</li> <li>System Restart</li> <li>Install Complete</li> </ul>	Where would you like to create product icons? <ul> <li>In a new Program Group: ArcSight SmartConnectors</li> <li>In the Start Menu</li> <li>On the Desktop</li> <li>In the Quick Launch Bar</li> <li>Other:</li> <li>Don't create icons</li> </ul>
	Create Icons for All Users
nstallAnywhere Cancel	Previous Next



- 6. Click Install.
- 7. Select Add a Connector.



- 8. Click Next.
- 9. Select Microsoft Windows Event Log Native.

*	Connector Setup	D X
文 ArcSight	Select the connector to configure	
Configure		
	Type Microsoft Windows Event Log - Native	]
	Ŗ	
	< Previous Next > Ci	ancel

- 10. Click Next.
- 11. Check the box next to Use Active Directory.

*	Connector Setup	x
À ArcSight	Configure Parameters Select logs for event collection from local host	
Configure	✓ Security log	
	System log	
	Application log	
K.	ForwardedEvents log	
	Custom logs	
	Source hosts for all forwarded events	
201	□ Do not use any source for Windows OS version	-
$P \rightarrow 0 / - c$	Use Active Directory for OS version	
	Use file for OS version	
	Parameters to add hosts for event collection	ĺ.
	Use common domain credentials	
	☑ Use Active Directory	
	Enter manually	~
	< Previous Next > Cancel	

- 12. Click Next.
- 13. Enter information about your Active Directory server (it is recommended to create a new administrator account for ArcSight to use).
- 14. Set Use Active Directory host results for to Replace Hosts.

*	l	Connector Se	tup 📃 🗖 🗙
•	Configure	Enter the parameter details	
		Domain Name	DI
	<i>R</i>	Domain User Name	arcsight_admin
		Domain User Password	•••••
		Active Directory Domain	DI.IPDR
		Active Directory User Name	arcsight_admin
		Active Directory User Password	•••••
5		Active Directory Server	ad-dns.di.ipdr
		Active Directory Filter	(&(cn=*)(operatingsystem=*)(whencreated=*))
		Active Directory Protocol	non_ssl v
1		Use Active Directory host results for	Replace Hosts V
1		19	
			< Previous Next > Cancel

16. Check the boxes under any event types that should be forwarded to this connector, for each individual host. For example: **Security, System, Application.** 

*				Со	nnecto	or Setup	D							-		x
Andiaha	Enter t	he device details														
ArcSight Configure	~	Host Name	Do	Use	Pas	Win	Is	Sec	Sys	Appl	For	Cus	Filter	Locale	Enc	
Configuro	$\checkmark$	EXCHANGE.DI.IPDR			•••••	Wind		~	~	~			*	en_US	UIF-8	^
Conligure	$\checkmark$	REMOTEDESKTOP3.DI			****	Wind		~	~	~			*	en_US	UTF-8	1
	✓	WINDOWS 10-1.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	1
	✓	WINDOWS 10-2.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	1
	~	HYPERV.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	1
K.	~	MSSQL.DI.IPDR			****	Wind		-	~	~			*	en_US	UTF-8	1
	~	WINDOWS 10-3.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	1
	~	UC-TEST-SERVER.DI.IP			****	Wind		~	~	~			*	en_US	UTF-8	1
	~	DESKTOP-7REQ7K0.DI			****	Wind		~	~	~			*	en_US	UTF-8	
	✓	TRIPWIRE-E.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	1
	✓	WIN-0LIQ7SM6HS2.DI			****	Wind		~	~	~			*	en_US	UTF-8	
	✓	WIN-K8I2P6E60K8.DI.I			****	Wind		~	~	~			*	en_US	UTF-8	1
	~	WIN-JH4L7J215VT.DI.I			****	Wind		-	~	~			*	en_US	UTF-8	1
	✓	AD-DNS08.DI.IPDR			****	Wind		✓	~	✓			*	en_US	UTF-8	1
	<b>v</b>	BACKUP-STORAGE.DI.I			****	Wind		<ul><li>✓</li></ul>	<ul><li>✓</li></ul>						UTF-8	
	~	BACKUPSERV.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	
	~	GLASSWALL.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	
MICON	$\checkmark$	SEMPERIS-DSP.DI.IPDR			****	Wind		~	✓	~			*	en_US	UTF-8	~
					A	bb	Import	Ex	port							
						R				< Pre	evious	N	ext >		Cancel	

*	Connector Setup	-		x
À ArcSight	Will use Active Directory at: ad-dns.di.ipdr Microsoft Windows Event Collection connector is configured to collect events from 22 hosts.			
Configure	whenesser wheness hvent confection connector is configured to confect events from 22 flosts.			
	l∕∉			
	< Previous Next >		Cancel	

- 18. Click Next.
- 19. Select ArcSight Manager (encrypted).

8		Connector Setup	_ 🗆 X	
ArcSight	Enter the type of destination			
Configure				
		ArcSight Manager (encrypted)		
12		<ul> <li>ArcSight Logger SmartMessage (encrypted)</li> </ul>		
		ArcSight Logger SmartMessage Pool (encrypted)		
1. A. A.		○ CEF File		
19		○ Event Broker		
		CEF Syslog		
		CEF Encrypted Syslog (UDP)		
		CSV File		
		🔿 Raw Syslog		
O FOCUS				
	4			_
		< Previous Next >	Cancel	1

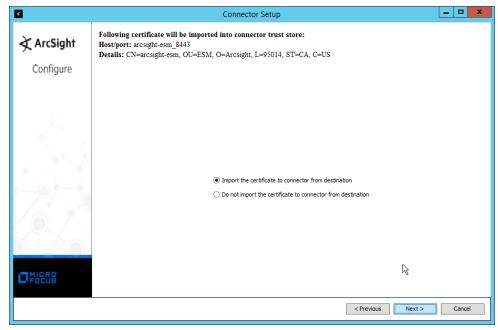
- 20. Click Next.
- 21. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.

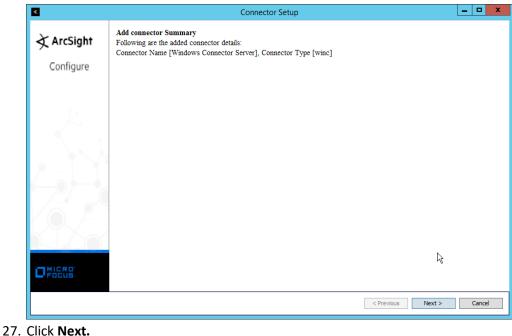
*		Connector Setup	_ <b>D</b> X
ArcSight	Enter the destination para	meters	
Configure			
14	Manager Hostname	arcsight-esm	
	Manager Port	8443	
	User	administrator	
	Password	••••••	
	AUP Master Destination	false	~
$P \rightarrow Q / T \sim c$	Filter Out All Events	false	¥
	Enable Demo CA	false	*
			l≩
			< Previous Next > Cancel

- 22. Click Next.
- 23. Enter identifying details about the system (only Name is required).

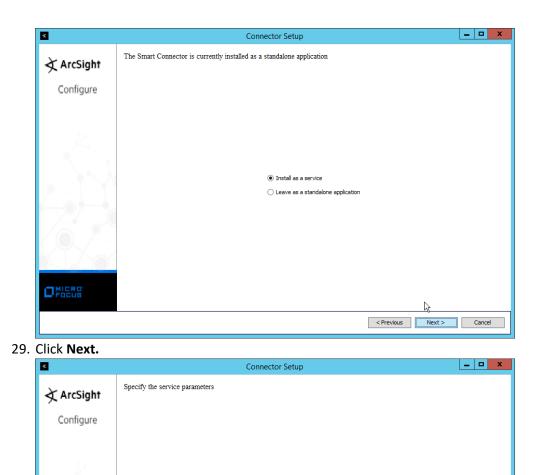
*		Con	nector Setup		_	. 🗆	x
ArcSight	Enter the connect	or details					
	Name Location DeviceLocation Comment	Windows Connector Server					
			R.				
				< Previous	lext >	Cance	:

- 24. Click Next.
- 25. Select Import the certificate to connector from destination.





28. Select Install as a service.



30. Click Next.

Service Internal Name

Service Display Name

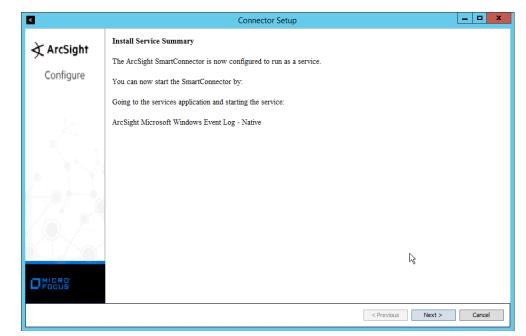
Start the service automatically Yes

winc

Microsoft Windows Event Log - Native

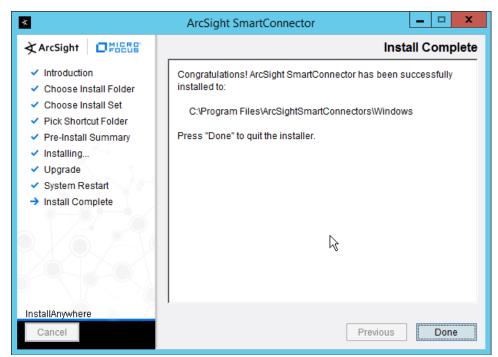
< Previous

Next > Cancel



- 31. Click Next.
- 32. Select Exit.

*	Connector Setup	_ 0	х
À ArcSight	Would you like to continue or exit?		
ArcSight Configure			
	○ Continue		
	• Exit		
	L <sub>g</sub>		
	< Previous Next >	Cano	
	< Previous Next >	Cano	51



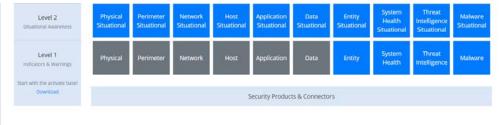
### 34. Click Done.

35. Note: Ensure that all machines selected do not block traffic from this device through their firewalls.

## 2.8.5 Install Pre-Configured Filters for ArcSight

## 2.8.5.1 *Install Activate Base*

 Go to the ArcSight Content Brain web app (<u>https://arcsightcontentbrain.com/app/</u>) and log in. This page allows you to keep track of packages to be installed—which packages should be installed is dependent on the needs of the organization, but the "activate base" is required for all products.



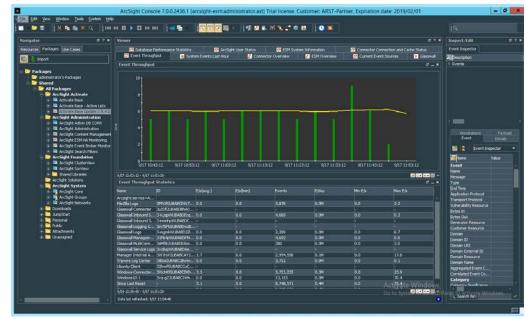
- 2. Click the **Download** link for the activate base. (Note: This package should be installed on the Arcsight Console, not on the ESM.)
- 3. Copy the contents of the zip file to ARCSIGHT\_HOME. The default for this is C:\arcsight\Console\current, assuming a Windows Server.

4. In PowerShell, navigate to the ARCSIGHT\_HOME directory (C:\arcsight\Console\current), and run:

```
run:
> .\ActivateBaseInstallAndUpdate2540.bat

PG c(\arccight\console\current>.\ActivateBaseInstallAndUpdate2540.bat
ATTENTION
ATTE
```

- 5. Enter the **hostname** of the ArcSight machine, the **port** (default: **8443**), and the **username** and **password** used to connect to the **ESM.**
- 6. Delete Activate\_Base\_Updated\_2.5.4.0.arb from the ARCSIGHT\_HOME directory.
- 7. Log in to ArcSight Console.



8. Under Packages > Shared > All Packages > ArcSight Activate, right-click Activate Base Update 2.5.4.0, and select Delete Package.

## 2.8.5.2 Install Packages

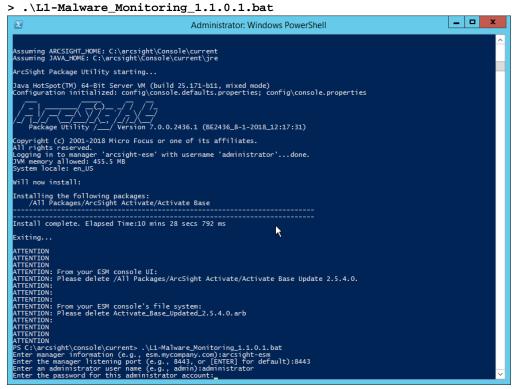
Once the Activate Base is installed, packages can be installed to monitor for specific types of events. As an example, find below instructions for the Malware Monitoring package.

- 1. Navigate to the ArcSight Content Brain web app.
- 2. Select the Level 1 box labeled Malware.

Level 1 indicators & Warnings	Physical	Perimeter N	Network	Host	Application	Data	Entity	System Health	Threat Intelligence	Mahwar	e
Start with the activate base! Download				Se	curity Products &	& Connectors					
Track Execution									Devices		. 0
Track Execution <ul> <li>Business Challenges</li> </ul>	•	⑦ Associated P	Packages		⑦ Status ▼	⑦ Attack Ve	ctor Solutio	ns		Expand All	

3. In the Track Execution section, under Associated Packages, you can see the list of packages used to address the challenge of "Malware Monitoring." In this case, there is just one package, "L1 – Malware Monitoring – Indicators and Warnings." Click the link to be taken to a download page for the package, and download it. (Note: This package should be installed on the Arcsight Console, not on the ESM.)

- 4. Copy the contents of the zip file to ARCSIGHT\_HOME. The default for this is C:\arcsight\Console\current, assuming a Windows Server.
- 5. In PowerShell, navigate to the *ARCSIGHT\_HOME* directory (*C:\arcsight\Console\current*), and run:



6. Enter the **hostname** of the ArcSight machine, the **port** (default: **8443**), and the **username** and **password** used to connect to the **ESM**.

## 2.8.6 Apply Filters to a Channel

- 1. In the ArcSight Console, click File > New > Active Channel.
- 2. Enter a **name** for the channel.
- 3. Select a time frame.
- 4. For Filter, select one the filters that was imported from the packages you installed.

*	New Active Channe	I			x
Channel Name:	unresolved malware				
Start Time:	\$Now - 30m 🔻	End Time:	\$Now		▼
Use as Timestamp:	🛃 End Time				-
	<ul> <li>Continuously evaluate time parameters (like \$Now)</li> <li>Evaluate time parameters once at attach time</li> </ul>				
Filter	All Unresolved Malware Events 🔹	Define			
Fields:	Select a Field Set 🔹 🔻	Define			
	For time ranges over a day, the end time will be evaluated	in hourly basis			
Examples 🔻				ОК	Cancel

 Click OK. All events that match the filter can be displayed in the newly created channel. Filters from imported packages can be found under Filters > Shared > All Filters > ArcSight Activate > Solutions.

# 2.8.7 Configure Email Alerts in ArcSight

## 2.8.7.1 *Configure a New Destination*

- 1. In ArcSight Console, click File > New > Destination.
- 2. Enter a name for the **Destination.**
- 3. For Destination Type, select Email Address.
- 4. For **Email Address**, enter the email that should be associated with this destination.

File Edit View Window Tools System Help				
ब ये व व 📲 👘 🖉 २ व 🔤 स्व स 💵 🚺 🖬 २२ व		1 🛄 💷 🞑 📖 👻 1 🕅 🛍 🐘 👫 1	L 🔍 🖻 📋 🕒 🔛 🔤 🔍	
Navigator d'	? ж	Inspect/Edit		ď
Resources Packages Use Cases		💭 Destination Editor		
✓ Rules Ctrl+Alt+L	-	Attributes Notes		
		- Destination		
Shortcuts		🗯 Name	Administrator	
		🗯 Start Time	12:00:00 AM	
🗆 🧑 Rules		🗯 End Time	11:59:59 PM	
- 107 Rules		Destination Type	Email Address	
Automistrator's Rules		Email Address	administrator@di.ipdr	
🖻 🗁 All Rules		User/Group	/All Users/Administrators/administrator	
ArcSight Activate				
+ C ArcSight Administration		External ID		
ArcSight Foundation		Alias (Display Name)		
🗄 🥅 ArcSight Solutions		Description		
🗄 🥅 ArcSight System		Version ID		
🗉 🚞 Downloads		Deprecated		
🗉 🧮 Personal		- Assign		
🕀 🛄 Public		Owner	<b>X</b>	
Real-time Rules     Unassigned		Notification Groups		
		(tiame) (Description)		
[[0:17:35] 4 of the 121 fields in the selected field set for condition editor are custom fields or n				Apply He

- 5. Click **OK.**
- 6. Select a place to save the new **Destination**.
- 7. Click **OK.**

# 2.8.7.2 Configure a New Rule

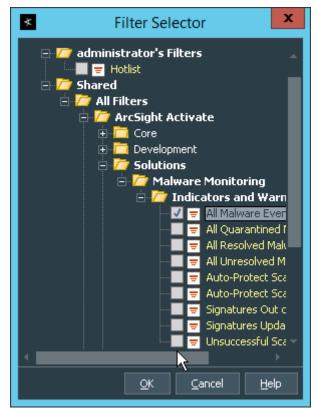
- 1. Click File > New > Rule > Standard Rule.
- 2. Enter a name for the rule.

le Edit View Window Tools System Help			
. <mark>▷ 🖉 🖩 18 № 18 ♦ 11 №</mark>		1	
avigator	d'? ×	Inspect/Edit	ď
esources Packages Use Cases		😤 Destination:Administrator 🚺 Rule Editor	
🗲 Rules	Ctrl+Alt+L 🔻	Attributes Conditions Aggregation Actions Local Variables Notes	
		E Rule	
hortcuts		Name Malware alert     Rule Type Standard Rule	
To Rules		External ID	
Shared		Alias (Display Name)	
🗄 🗁 All Rules		Description Version ID	
🕀 🧮 ArcSight Activate		Deprecated	
ArcSight Administration		Assign	
🕀 🧰 ArcSight Foundation 🕀 🫅 ArcSight Solutions		Owner	
ArcSight System		Notification Groups	
🕀 🚞 Downloads			
🕢 🧱 Personal			
🗃 🧰 Public 🖃 🧮 Real-time Rules			
Cardina Racis			
		External ID	
		Enter an external identifier	
		✓ Test <u>OK</u> <u>Cancel</u>	Apply Help

3. Click the **Conditions** tab.

👔 🗁 🖫 🚦 🕌 🕷 🔍 हे।स स्ट 🂵	🕩 🖬     🛃 🖷	🔍 🗉 🖉 🔚 👻	12 🧐 📫 🔍 🗥 🖕 🕌 I	🍭 🛃 📑 🕒 🚺 🕴 🔍	
lavigator		Inspect/Edit			
Resources Packages Use Cases		Destination:Administrator	F Rule Editor		
✓ Rules	Ctrl+Alt+L 🔻	Attributes Conditions Aggre		es Notes	
- Tuics			sets 🕵 Vulnerabilities 🌄 Acti		
hortcuts		Edit Summary	*		
		# Event conditions			
Rules		event1			
- 🦰 administrator's Rules					
🗄 🗁 All Rules					
🗉 🧮 ArcSight Activate			▶		
Image: Second State S					
ArcSight Solutions					
🕀 🥅 ArcSight System					
Downloads     Personal					
🕀 🧮 Public 🕀 🧮 Real-time Rules					
💿 🧮 Real-time Rules		Common Conditions Editor	-		🔝 +/- Global Variable.
		Common Conditions Editor	▼ Op	Condition	
💿 🧮 Real-time Rules		Name Event		Condition	A3 (
🚊 🧮 Real-time Rules		Name Event Aggregated Event Count		Condition	A.8 (2
🗉 🧮 Real-time Rules		Name Event		Condition	∧a ( 
🚊 🧮 Real-time Rules		Name Event Aggregated Event Count Application Protocol Bytes In Bytes Out		Condition	
🚊 🧮 Real-time Rules		Name Event Aggregated Event Count Application Protocol Bytes In Bytes Out Correlated Event Count		Condition	
💿 🧮 Real-time Rules		Name Event Aggregated Event Count Application Protocol Bytes In Bytes Sout Correlated Event Count Customer		Condition	
🗉 🧰 Real-time Rules		Name Event Aggregated Event Count Application Protocol Bytes In Bytes Out Correlated Event Count		Condition	
💿 🧮 Real-time Rules		Name Event Aggregated Event Count Application Protocol Bytes In Bytes Out Correlated Event Count Customer Domain			
🗉 🧰 Real-time Rules		Ame Fuent Aggregated Event Count Aggregated Protocol Bytes In Bytes Out Correlated Event Count Customer Domain Domain External ID		Condition	+/- Global Variable.     A         A         A         A      A
💿 🧮 Real-time Rules		Ame Fyent Aggregated Event Count Aggregated Event Count Correlated Event Count Controllented Event Count Coustomer Domain Domain External ID Domain D			

4. Either create a custom condition for the rule or click the **Filters** button to select a preconfigured Filter. (Ensure you check the box next to desired filters if you choose to select a preconfigured filter.)



- 5. If you selected a filter, click OK.
- 6. Click the Actions tab.

ile Edit View Window Tools System Help		
[- 122 團    [ H № № ペ    [ [ H ↔ II ]] [ D >> >>>    [ ==	🖷	
lavigator d' ?	× Inspect/Edit	
tesources Packages Use Cases	影 Destination:Administrator 🚺 Rule Editor	
S Rules Ctrl+Alt+L		
hortcuts	Adi 🖉 Adi 🗶 Edit 💥 Remove 🔺 Move Up 🔻 Move Down 🍃 Hide Empty Triggers	
Rules       ■ Stand       ■ All Rules       ■ ArcSight Admestration       ■ ArcSight Admestration       ■ ArcSight Admestration       ■ ArcSight Routes       ■ Personal       ■ Point       ■ Routes       ■ ArcSight Routes       ■ ArcSight Routes	• Con First Event (Active)     Con First Event (Active)     Con First Event (     Con First Treahold     Con First Treahold     Con First Treahold     Con Time United     Con Time United     Con Time United     Con Time Window Expration - Cumulative Rule Chain Is Off     Con Time Window Expration - Cumulative Rule Chain Is Off     Con Time United     Con Tim	

- 7. Select the trigger for the notification, and click **Add > Send Notification**.
- 8. Select the **Destination Group** in which the desired destinations reside.

× 4	Add "Send Notification" Acti	ion 🔽
When: On First Eve	nt	
Send Notification —		
Destination Group:	ArcSight Administrators 🔹	🗾 Ack Required
Message:		
L		
		<u>C</u> ancel <u>H</u> elp

9. Click OK.

# 2.9 Tripwire Enterprise

### Notes:

This installation requires MSSQL to be installed on a remote server and configured according to the instructions in the *Tripwire Enterprise 8.6.2 Installation and Maintenance Guide.* 

## 2.9.1 Install Tripwire Enterprise

- 1. Ensure that you have a current version of Oracle Java. You must install both the Java Runtime Environment (JRE) and the Java Cryptography Extension (JCE).
- 2. Download and run the JRE installer.

Java Setup - Welcome	-		x			
Welcome to Java						
Java provides access to a world of amazing content. From business solutions to helpful utilities and entertainment, Java makes your Internet experience come to life.						
Note: No personal information is gathered as part of our install process. <u>Click here</u> for more inf what we do collect.	ormat	ion c	on			
Click Install to accept the license agreement and install Java now.						
Change destination folder	Ins	tall >				

- 3. Click Install.
- 4. Download the JCE, and extract the files.

Name	Date modified	Туре	Size
local_policy	12/20/2013 1:54 PM	JAR File	3 KB
README	12/20/2013 1:54 PM	Text Document	8 KB
US_export_policy	12/20/2013 1:54 PM	JAR File	3 KB

- 5. Copy the **local\_policy.jar** and **US\_export\_policy.jar** files to */lib/security/Unlimited/* and */lib/security/Limited* in the Java installation directory.
- 6. Run install-server-windows-amd64.
- 7. Select the Java runtime that was just installed.

te	JVM Selection	_ D X				
	Please select the Java(tm) Runtime to use					
Uracle/Sun 1.8.0 d	Oracle/Sun 1.8.0 64-bit C:/Program Files/Java/jre1.8.0_181/bin/java.ϵ ♥					
	OK Cancel					

8. Click **OK.** 

te	Tripwire Enterprise Console Installer	- 🗆 X
TRIPMIC ENTERPRISE 8.7	Welcome to the Tripwire Enterprise Console installa This wizard will install and configure Tripwire Enterp Before continuing, please review the installation do ensure that you are in compliance with all installatio Failure to meet all requirements may cause the insta	prise Console. cumentation to on requirements.
	< Back Next >	Cancel
Click Next. Select I accept the		
	agreement. Tripwire Enterprise Console Installer	_ <b>D</b> X
Select I accept the	Tripwire Enterprise Console Installer	
Select I accept the	t wing License Agreement. You must accept the terms	pwire: LAKE CONTROL.
Select I accept the License Agreement Please read the follo before continuing w IMPORTANT INFORM TRIPWIRE SOFTWAR SUBJECT TO LICEN AGREEMENT BEFORE COMPLETE AND UNC SET FORTH IN THI	t t wing License Agreement. You must accept the terms with the installation.	of this agreement
Select I accept the License Agreement Please read the follo before continuing w IMPORTANT INFORM TRIPWIRE SOFTWAR SUBJECT TO LICEN AGREEMENT BEFORE COMPLETE AND UNC SET FORTH IN THI	t t t t t t t t t t t t t t	of this agreement
Select I accept the License Agreement Please read the follo before continuing w IMPORTANT INFORM TRIPWIRE SOFTWAR SUBJECT TO LICEN AGREEMENT BEFORE COMPLETE AND UNC SET FORTH IN THI ORDER TERMS AND	Tripwire Enterprise Console Installer t wing License Agreement. You must accept the terms ith the installation. IATION RE IS LICENSED, NOT SOLD. USE OF THIS SOF ISE RESTRICTIONS. CAREFULLY READ THIS LIC USING THE SOFTWARE. USE OF SOFTWARE IND CONDITIONAL ACCEPTANCE OF THE TERMS AND C IS AGREEMENT. ANY ADDITIONAL OR DIFFERENT CONDITIONS SHALL NOT APPLY.	of this agreement

Tripwire Enterprise Cons	ole Installer 📃 🗖 🗙			
Installation Directory	tripwire: TAKE CONTROL.			
Please specify the directory where all Tripwire Enterprise components will be installed.				
Installation Directory C:\Program Files\Tripwire\TE	<b>2</b>			
InstallBuilder				
<	Back Next > Cancel			

13. The installer should automatically detect the hostname of the system on which Tripwire Enterprise (TE) is being installed. If it does not, enter the hostname here.

te	Tripwire Enterprise Co	nsole Installer	_ 🗆 X		
Tripwire Enterprise	Console Configuration Part 1	of 4	r <mark>ipwire:</mark> Control.		
Please provide the hostname of the system where Tripwire Enterprise Console will be installed.					
TE Server Hostname	TRIPWIRE-E				
InstallBuilder					
	L	< Back Ne	kt > Cancel		

- 14. Click Next.
- 15. Enter the port numbers to use for each of the HTTPS Web Services port, HTTP EMS Integration Port, and Tripwire Enterprise RMI port. The Remote Method Invocation (RMI) port is used for inbound communication from Tripwire agents to the server, so ensure that it is allowed through the firewall.

te Tripw	ire Enterprise Console Installer
Tripwire Enterprise Console C	Configuration Part 2 of 4
Specify the ports that Tripwire	Enterprise Console uses to communicate.
This port is used for user-initiat	ted Web console sessions.
HTTPS Web Services port	443
This port is used for external in	tegrations (such as plugins).
HTTP EMS Integration Port	8080
This port is used for Console/A	gent Java communications.
Tripwire Enterprise RMI Port	9898
InstallBuilder	
	< Back Next > Cancel

17. Enter a passphrase to use.

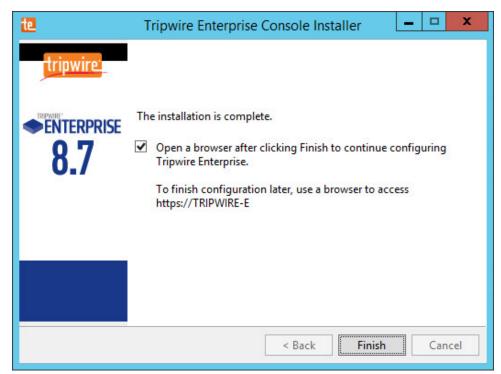
te	Tripwire Enter	orise Console Inst	aller	>	ĸ
Tripwire Enterpris	se Console Configurati	on Part 3 of 4	tripv	vire take	DL.
The services passpl	hrase is used to secure	Tripwire Enterprise co	mmunication	15.	
double-quote ("), l	t be between 19 and 64 ess-than (<), greater-th ved. See the Installatio	an (>), or backslash (	) characters,	most other	
Services Passphrase	e				
Confirm Passphras	e				
InstallBuilder		< Back	Next >	Cancel	
lick <b>Next.</b>					
te	Tripwire Ent	erprise Console	Installer	_ 0	
	Tripwire Ent	14 29 Sch 100 March 10	Installer	ripwire	TAKE
Tripwire Enterp	*******	ration Part 4 of 4	ţ	ripwire	TAKE
Tripwire Enterpr	rise Console Configu	ration Part 4 of 4 or Tripwire Enterpris	e Console.	ripwire	TAKE
Tripwire Enterpr Please review the The following set Installation Direct Available Disk Spa Hostname: TRIPV	rise Console Configur installation settings f tings are configured f cory: C:\Program Files ace: 184716 MB VIRE-E	ration Part 4 of 4 or Tripwire Enterpris for Tripwire Enterpris	e Console.	ripwire	TAKE
Tripwire Enterpr Please review the The following set Installation Direct Available Disk Spa Hostname: TRIPV IP Address(Listen HTTPS Web Servi	ise Console Configur installation settings f tings are configured f tory: C:\Program Files ace: 184716 MB VIRE-E ing): 0.0.0.0 ces Port: 443	ration Part 4 of 4 or Tripwire Enterpris for Tripwire Enterpris	e Console.	ripwire	TAKE
Tripwire Enterpr Please review the The following set Installation Direct Available Disk Spa Hostname: TRIPV IP Address(Listen HTTPS Web Servi HTTP EMS Integr	ise Console Configur installation settings f tings are configured f tory: C:\Program Files ace: 184716 MB VIRE-E ing): 0.0.0.0 ces Port: 443 ation Port: 8080	ration Part 4 of 4 or Tripwire Enterpris for Tripwire Enterpris	e Console.	r <mark>ipwire</mark>	TAKE
Tripwire Enterpro Please review the The following set Installation Direct Available Disk Spa Hostname: TRIPV IP Address(Listen HTTPS Web Servi HTTP EMS Integra TE Services (RMI)	ise Console Configur installation settings f tings are configured f tory: C:\Program Files ace: 184716 MB VIRE-E ing): 0.0.0.0 ces Port: 443 ation Port: 8080	ration Part 4 of 4 or Tripwire Enterpris for Tripwire Enterpris	e Console.	ripwire	TAKE
Tripwire Enterpr Please review the The following set Installation Direct Available Disk Spa Hostname: TRIPV IP Address(Listen HTTPS Web Servi HTTP EMS Integra TE Services (RMI)	ise Console Configur installation settings f tings are configured f tory: C:\Program Files ace: 184716 MB VIRE-E ing): 0.0.0.0 ces Port: 443 ation Port: 8080 Port: 9898	ration Part 4 of 4 or Tripwire Enterpris for Tripwire Enterpris	e Console.	ripwire	TAKE

- 19. Click Next.
- 20. Check the box next to Install Real-time Monitoring.
- 21. Enter 1169 for Real-time Port.

te	Tripwire Enterprise	Console Insta	aller 🔄	• <b>x</b>
Tripwire Enterpri	se Agent Configuration		tripwi	re control.
enable monitoring	e Agent software is installed o of that system. Do you wan t? The Real-time Monitoring	t to install Real-ti	me Monitoring	functionality
🖌 Install Real-t	ime Monitoring			
Please specify the	e local port to be used by the	Real-time subsy	stem.	
Real-time Port	1169			
InstallBuilder ——				
		< Back	Next >	Cancel

te	Tripwire Enterprise Console Installer	_ 🗆 🗙
Ready to Install	t	ripwire: TAKE CONTROL.
The installer is ready t	to begin installing Tripwire Enterprise Console.	
	stalling Tripwire Enterprise. ny changes before you begin the installation.	
InstallBuilder	< Back Nex	t > Cancel

- 23. Click Next.
- 24. Check the box next to **Open a browser after clicking Finish to continue configuring Tripwire** Enterprise.



#### 25. Click Finish.

26. Once at the web address, enter the **Services passphrase** chosen earlier.

Inpwire Enterprise Post-Install Computation	
Tripwire Enterprise needs additional configuration. To finish installing, please enter your Services Passphrase for authentication. The Services Passphrase was created when you installed Tripwire Enterprise. Services Passphrase: Login	
	Tripwire Enterprise needs additional configuration. To finish installing, please enter your Services Passphrase for authentication. The Services Passphrase was created when you installed Tripwire Enterprise. Services Passphrase:

27. Click Login.

Database Configuration Sett	ings
These settings control how the TE Co any necessary changes in the fields b	sole connects to a remote database that stores data for all TE operations. You can check the current configuration here, and make slow.
Remote Database Type: Microsoft SQL Server ▼ Microsoft SQL Server	Remote Database Type: The type of remote database used by TE.
Oracle Oracle RAC MySQL	

- 28. Select Microsoft SQL Server for Remote Database Type.
- 29. Select SQL Server for Authentication Type.
- 30. Enter login details for the account created during the MSSQL setup.
- 31. Enter the **hostname** or **IP** of the database server.

- 32. Enter the **port** on which the database is operating.
- 33. Enter the **name** of the database to be used for TE.
- 34. Select the appropriate setting for **SSL** according to your organization's needs.

	Authentication Type:		
	SQL Server	Authentication Type: Specifies whether the database login should authenticate using a W the format domain/user), or an SQL Server account (an account defined only in SQL Serve authentication type, NTLMv2 should be used, as it is cryptographically superior to the first NTLMv2 is configured in the operating system, not in the database or application, TE can b compatibility.	r). With the Windows rersion of NTLM. However, as
	Look News		
	Login Name: twadmin	Login Name: The login name that TE will use to authenticate with the database.	
	Password:	Password: The password that TE will use to authenticate with the database.	
		Password. The password that TE will use to admenticate with the database.	
	Database Host:		
	192.168.78.125	Database Host: The fully qualified domain name, hostname or IP address of the system w	nere the database is installed.
	Port (default 1433):		
	1433	Port: The TCP port that the database is listening on. If an Instance Name is specified here	
		will use UDP 1434 to connect to the SQL Server Browser Service, and this Port field will be Browser service listens for incoming connections to a named instance and provides the clie	
		corresponds to that named instance.	in the ror portnumber that
	Database Name:	Database Name: The name of the database that TE should use when connecting to the re	moto databaco. Noto that the
	TE_DB	login name in SQL Server should have this database set as the default, and the login name	
		database.	
	Instance Name (Optional):		
		Instance Name (Optional): The location/name of the database instance on the server. As	: your DBA if a non-default
		instance should be used for TE.	
	SSL:		
	Off •	SSL (Secure Sockets Layer): Specifies whether the database connection should request,	require or authenticate SSL.
		<ul> <li>Request - SSL will be used if available.</li> </ul>	
		<ul> <li>Require - SSL will always be used, and an error will occur if SSL is not available for</li> <li>Authenticate - SSL will always be used, and an error will occur if SSL is not available</li> </ul>	
		the certificate chain of the database server's public key will be authenticated using T	
		<ul> <li>chain does not originate from a trusted source, an error will occur.</li> <li>Off - SSL will never be used. This setting is not recommended.</li> </ul>	Activate Windows
			Go to System in Control P
	Test Database Login		
25	Click Test Database Les	in to oncure the connection is functional	
55.	CIICK Test Database Logi	in to ensure the connection is functional.	

Activate Windows
Go to System in Control P
Save Configuration and Restart Console Logout

- 36. Click Save Configuration and Restart Console.
- 37. After the reboot, enter a new administrator password.

	nfiguration Steps Needed:
	Tripwire administrator account password needs to be changed from the default.
С	eate Administrator Password Passwords must: Be between 8 and 128 characters in length Contain at least 1 uppercase character Contain at least 1 uppercase character Contain at least 1 non-alphanumeric character Supported characters: `-(@#\$%^&`()_==+{([)})\!;:"<>/? Confirm Ad Continue
S	pport Information         Still having problems with your installation?         Contact Tripwire Support.         Information about your system and this installation. Attach the support bundle file to you web ticket or email. What is a Support Bundle?         Or open a Support ticket: <a href="https://secure.tripwire.com/customers/">https://secure.tripwire.com/customers/</a>
Trip	ire Enterprise 8 7.0 b8.7.0 r20180606173604-e215728 b40
	k Confirm and Continue.
Inp	wire Enterprise Fast Track
	Welcome to Tripwire Enterprise Fast Track!
	TRIPWIRE ENTERPRISE Fast Track
	TRIPWIRE ENTERPRISE ENTERPRISE FAST Track will help you to configure Tripwire Enterprise for Change Auditing. Policy Management, or an integrated Security Configuration Management (SCM) solution. It only takes a few minutes to complete the setup questionnaire. After you do, Fast Track will use your
	<image/> <text><text><text><text></text></text></text></text>
	<image/>
	<image/> <section-header><text><text><text><text><text></text></text></text></text></text></section-header>

Step 1: Add your Tripwire Enterprise license (\*.cert)
Choose File No file chosen

- 40. Click **Choose File**, and select the TE license file, which should be a *.cert* file.
- 41. Check the box next to Change Auditing and Policy Management.

Step 2: Configure Cha	nge Auditing and/or Policy Management
Monitoring Solutions	<ul> <li>☑ Change Auditing</li> <li>☑ Policy Management</li> </ul>
Available Policies	CIS PCI DISA NIST 800-53 (FISMA)

### 42. Select any available policies desired.

Operating System	× Microsoft Windows Server 2008 R2	
Microsoft Windows Server 2008 R2	× Microsoft Windows Server 2012 R2 × Oracle Solaris 10	
Microsoft Windows Server 2012 R2	× Oracle Solaris 11	
✓ Oracle Solaris 10	× Red Hat Enterprise Linux 6 × Red Hat Enterprise Linux 7	
Oracle Solaris 11	× VMware ESXi 5.5 Server	
Red Hat Enterprise Linux 6		
Red Hat Enterprise Linux 7		
Virtual Infrastructure		
VMware ESXi 5.5 Server		

#### 43. Select all the operating systems that you wish to monitor with TE.

Checks	Reports
How frequently would you like to run checks on your assets?	How frequently would you like to run reports on your assets?
Daily	Daily
	Run the reports at 4:00  AM
Run the checks at 1:00  AM  Olicy Scheduling Checks	Run the reports at 4.00 • AM •
olicy Scheduling Checks How frequently would you like to run checks on	Reports How frequently would you like to run reports on
olicy Scheduling Checks How frequently would you like to run checks on your assets?	Reports How frequently would you like to run reports on your assets?
olicy Scheduling Checks How frequently would you like to run checks on your assets?	Reports How frequently would you like to run reports on your assets?

44. Set up a schedule for running checks and reports according to your organization's needs. Leave the box next to **Enable Checks and Reports** unchecked for now.



Passwords must: Be between 8 and 128 characters in length Contain at least 1 numeric character Contain at least 1 oppercase character Contain at least 1 non-alphanumeric character Supported characters: `~I@#\$%^&*()=+{[[]]W ,:'*<,>./?	User Name:	
	admin	1
	Password:	
		~
	Confirm Password:	
		1
	Email Address:	

46. Enter a username and password for a new administrator account for TE Console.

Preview Configuration Ctive te Volance OW

### 47. Click Preview Configuration.

FORCY TAILOS - VINIMATE LOAT 5.5 GETVEN		
These tasks will be applied to your configuration Critical Change Audit Check - RHEL 6 Critical Change Audit Check - RHEL 7 Critical Change Audit Check - Solaris 10 Critical Change Audit Check - Solaris 11 Critical Change Audit Check - Solaris 11 Critical Change Audit Check - Windows Policy Check - RHEL 7 Policy Check - RHEL 7 Policy Check - Solaris 11 Policy Check - Solaris 11 Policy Check - Windows Report Task - Solaris 11 Policy Check - Windows Report Task - Daily File System Changes by Node Report Task - Daily File System Changes by Nude Report Task - Daily File System Changes by Nude Report Task - Test Result Summary - Ked Hat - PCI v3.1 Report Task - Test Result Summary - Vindows - PCI v3.1 Report Task - Test Result Summary - Vindows - PCI v3.1 Report Task - Test Result Summary - Vindows - PCI v3.1 Report Task - Test Results by Node - Solaris - PCI v3.1 Report Task - Test Results by Node - Solaris - PCI v3.1 Report Task - Test Results by Node - Solaris - PCI v3.1 Report Task - Test Results by Node - Solaris - PCI v3.1 Report Task - Test Results by Node - Solaris - PCI v3.1 Report Task - Test Results by Node - Solaris - PCI v3.1 Report Task - Test Results by Node - Solaris - PCI v3.1 Report Task - Test Results by Node - Solaris - PCI v3.1 Report Task - Waivers - Windows - PCI v3.1 Report Task - Waivers - Waivers - Solaris - PCI v3.1 Report Task - Waivers - Mindows - PCI v3.1 Report Task - Waivers - Mindows - PCI v3.1 Report Task - Waivers - Waivers - RepI v3.1 Report Task - Waivers - Waivers - Sola		
Customer Center Home Page PCI Overview - Red Hat PCI Overview - Solaris PCI Overview - VMware ESX PCI Overview - Windows Tripwire Enterprise Administrator		
	Apply Configuration	Edit Configuration CUN ate Volance OWs

48. Click Apply Configuration.

Configuring Tripwire Enterprise Tripwire Enterprise Best Practice for the selected platforms	
PCI for Microsoft Windows Server 2008 R2	Configuring 120 Rules
Change Audit for Microsoft Windows Server 2008 R2	
PCI for Microsoft Windows Server 2012 R2	
Change Audit for Microsoft Windows Server 2012 R2	
PCI for Oracle Solaris 10	
Change Audit for Oracle Solaris 10	
PCI for Oracle Solaris 11	
Change Audit for Oracle Solaris 11	
PCI for Red Hat Enterprise Linux 6	
Change Audit for Red Hat Enterprise Linux 6	
PCI for Red Hat Enterprise Linux 7	
Change Audit for Red Hat Enterprise Linux 7	
PCI for VMware ESXi 5.5 Server	
Finalize Policy Management configuration for the selected platform	ms
Finalize Change Auditing configuration for the selected platforms	
	Continue d ThipWatenYchistow

49. Click **Continue to Tripwire Enterprise** when the installation finishes.

# 2.9.2 Install the Axon Bridge

- 1. Ensure that TCP traffic on port 5670 is allowed through the firewall.
- 2. Navigate to the TE Console installation directory, to the */server/data/config* folder. Copy *bridge\_sample.properties* to *bridge\_properties*.
- 3. In the bridge.properties file, find the line that says: #tw.cap.bridge.registrationPreSharedKey= Remove the # character. After the = character, enter a password. The password has some restrictions, so ensure that it meets the requirements if the connection fails later.
- 4. Restart the TE console by running the following command from an administrator command prompt, where *<te\_root>* is the TE installation directory:
  - > <te\_root>/server/bin/twserver restart

# 2.9.3 Install the Axon Agent (Windows)

- Download the Axon Agent .zip file from the Tripwire customer website (<u>https://tripwireinc.force.com/customers</u>), under the **Product Downloads** tab.
- 2. Unzip the file.
- 3. To begin the installation, double-click the *.msi* file in the extracted folder. Note: No installation wizard will appear; the installation happens automatically.
- 4. After the Axon Agent is installed, navigate to C:\ProgramData\Tripwire\agent\config, and copy twagent\_sample.conf to twagent.conf.

#	
# H	OST based agent configuration:
#	Instead of using a DNS SRV record, the agent may be configured
#	to talk to a specific host, or list of hosts. Lists use a comma separator and
#	can optionally specify a port. The default of port 5670 will be used if a port
#	is not specified.
#	
#	Example: host1, host2:5900, 10.123.0.15, [feac:ba80:6fff:93fe]:7582
#	
#	The agent may be configured to connect to hosts in a randomized or textual order
#	(default: true)
#	
bri	dge.host=192.168.1.136
#br	idge.port=5670
#br	idge.randomize.hosts=true
#	

- 5. Open *twagent.conf*, and find the line that says bridge.host. Remove the # character, and enter the hostname or IP address of the Axon Bridge server.
- 6. In a file called *registration\_pre\_shared\_key*, enter the value of the pre-shared key that was set in the Axon Bridge.
- 7. Restart the Axon Agent Service by opening a command prompt and running the following commands:

🔤 Administrator: Command Prompt	_7	×
icrosoft Windows [Version 10.0.17134.228] c) 2018 Microsoft Corporation. All rights reserved.		
:\Users\Administrator>net stop TripwireAxonAgent he Tripwire Axon Agent service is stopping he Tripwire Axon Agent service was stopped successfully.		
:\Users\Administrator>net start TripwireAxonAgent he Tripwire Axon Agent service is starting. he Tripwire Axon Agent service was started successfully.		
:\Users\Administrator>_		

## 2.9.4 Install the Axon Agent (Linux)

- Download the Axon Agent .tgz file from the Tripwire customer website (<u>https://tripwireinc.force.com/customers</u>), under the **Product Downloads** tab.
- 2. To install the software, run the following commands: Red Hat Enterprise Linux (RHEL) or CentOS: > rpm -ivh <installer\_file> Debian or Ubuntu: > dpkg -i <installer\_file>
- 3. Navigate to /etc/tripwire/ and copy twagent\_sample.conf to twagent.conf.
- 4. Open *twagent.conf*, and find the line that says bridge.host. Remove the # character, and enter the hostname or IP address of the Axon Bridge server.

- 5. In a file called *registration\_pre\_shared\_key.txt*, enter the value of the pre-shared key that was set in the Axon Bridge.
- 6. Restart the Axon Agent Service by opening a command prompt and running the following commands:

```
RHEL or CentOS:
> /sbin/service tripwire-axon-agent stop
> /sbin/service tripwire-axon-agent start
```

```
Debian or Ubuntu:
```

- > /usr/sbin/service tripwire-axon-agent stop
- > /usr/sbin/service tripwire-axon-agent start

## 2.9.5 Configure Tripwire Enterprise

### 2.9.5.1 *Terminology*

**Node:** A monitored system, such as a file system, directory, network device, database, or virtual infrastructure component.

**Element:** A monitored object, which is a component or property of a node being audited by TE.

**Element Version:** A record of an element's state at specific points in time. Multiple element versions create a historical archive of changes made to the element.

**<u>Rule:</u>** A rule identifies one or more elements to the TE Console.

<u>Action</u>: An object that initiates a response to either changes detected by TE or by failures generated from policy tests.

Task: A TE operation that runs on a scheduled or manual basis.

**<u>TE Policy</u>**: A measurement of the degree to which elements comply with a policy.

**Policy Test:** A determination of whether elements comply with the requirements of a policy.

**Baseline:** The act of creating an element that reflects the current state of a monitored object (also called the **current baseline.** When a node's baseline is promoted, TE saves the former baseline as a **historic baseline.** 

**Version Check:** A check on monitored objects/elements. It is a comparison of the current state of the element against its already recorded baseline for changes.

### 2.9.5.2 Tags

In TE, tags can be used to label and target specific nodes. Tags are not required but allow for targeting nodes more granularly than by the operating system. This section will describe how to create and assign tags.

- 1. Navigate to the TE Console in your browser.
- 2. Click Asset View.

Tripwire Web Console × Survey	× +				j.	- 0	×
← → C' ŵ (() & https://t	ripwire-e/console/app.showApp	p.cmd		🖸 🕁		lii\ @	) ≡
SENTERPRISE HOME NODES RULES ACTIONS	TASKS   POLICIES   LOG   REPO	ORTS SETTINGS					
Nodes Asset View Node Search Element Se	earch Version Search				🔂 Refresh 🔟 H	elp 🕅 L	ogout
Filter Assets Manage Tagging	All   None	9 of 9	ABC 🛋	Selected: 0   Clear			
Filter assets by keyword Q	192.168.78.126 192.168.78.126			Getting Started with Asset View			
Clear all   Save current filter	ad-dns.di.ipdr 192.168.1.12		-0	Manage Tagging Create Tags, Tagging Profiles, and Saved Filters.			
	EXCHANGE 192.168.1.134			Filter Assets Tag your assets.			
<ul> <li>System Tag Sets</li> <li>Database Server</li> </ul>	HYPERV.DI.IPDR 192.168.78.105		-0	Filter by keyword and tags			

- 3. Click the Manage Tagging tab.
- 4. Enter the name of a tag set or use one of the four existing ones (Location, Owner, Platform Family, Primary Function). Click Add if adding your own tag set.

SENTERPRISE HOME NODES RULES ACTIONS	TASKS   POLICIES   LOG   REPORTS   SETTINGS		
Nodes Asset View Node Search Element Se	arch Version Search		😔 Refresh 🔯 Help 🕅 Logout
Fliter Assets Manage Tagging	Create and Edit Tag Sets		
Tag Sets	Tutorial Add		Tag Sets
Tagging Profiles	× Location	(Add tags)	Tags and Tag Sets are limited to 50 characters in length and may not contain the following characters:
Saved Filters	Add a new tag Add		Tags are descriptors that you can create and assign to your assets. You can assign as many tags to an asset as you like and
	×  Vowner Add a new tag Add	(1 teg)	you can always rename or delete the tags later. Tags are organized using tag sets, which group a set of related tags.
	× DI Testing		For example, a tag set named Location could include the tags Portland, Chicago, and New York. These tags would be represented in TE as Location: Portland, Location: Chicago, and Location: New York.

5. Under the tag set you wish to add a tag to, enter the name of the tag.

uu	a non lay ool			1
×	Location		(Add tags)	-
	Add a new tag	Add		
×	▼ Owner		(1 tag)	
	Add a new tag	Add		
	× DI Testing			
×	▼ Platform Family		(4 tags)	
	Add a new tag	Add		
	× Red Hat			Ξ
	× Solaris × VMware ESX			
	× Windows			
×	<ul> <li>Primary Function</li> </ul>		(1 tag)	
	Add a new tag	Add		
	× Domain Controller			
×	Tutorial		(Add tags)	
	Tutorial tag	Add		

### 6. Click Add.

- 7. Navigate to **Nodes > Asset View > Filter Assets.**
- 8. Check the boxes next to the nodes to which you wish to add this tag.

Nodes Asset View Node Search Element Se	earch Version Search				😣 Refresh 🗇 Help 🕅 Logout
Filter Assets Manage Tagging	All   None	9 of 9	ABC 🛋	Selected: 3   Clear	
Filter assets by keyword Q	192.168.78.126 192.168.78.126		-	Edit Tags Health Check 🔻	
Clear all   Save current filter	ad-dns.di.ipdr 192.168.1.12		-	WINDOWS10-1.DLIPDR     WINDOWS10-2.DLIPDR     WINDOWS10-3.DLIPDR	
System Tag Sets     Database Server     Directory Server	HYPERV.DI.IPDR 192.168.78.105				
Network Device     Operating System     Status     Virtual Infrastructure	MSSQL 192.168.1.141		-8		
▼ Tag Sets ▶ Location	■ 192.168.1.136 ■ WINDOW S10-1.DI.IPDR 192.168.1.138	8			
Owner     Platform Family     Primary Function	WINDOW S10-2.DI.IPDR 192.168.78.118		-		
Tutorial     Saved Filters	WINDOW \$10-3.DI.IPDR 192.168.78.119	2	-8		
Windows 2008 R2 Domain Controllers Windows 2012 R2 Domain Controllers					
Operational Tag Sets					
▶ Health				Activate Wind	ows

#### 9. Click Edit Tags.

#### 10. Check the boxes next to any tags you wish to add to these nodes.

SENTERPRISE HOME NODES RULES ACTIONS		2	↔ Refresh 团 Help 🖟 Logout
Nodes Asset View Node Search Element	BACKWARD COMPANY OF THE OWNER OF	S	** Refresh @ Help @ Logout
	Edit Tags		
Filter assets by keyword Q	For: 3 Assets		Edit Tags Health Check
Clear all [ Save current filter	Tag Sets	and the second se	WINDOWS10-1.DLIPDR
	Location	(0 tags)	WINDOWS10-2 DLIPDR WINDOWS10-3 DLIPDR
	▼ Owner	(1 tag)	WINDOWS 10-3 DLIPDR
	DI Testing		
▼ System Tag Sets	Platform Family	(4 tags)	
Database Server Directory Server Network Device > Operating System > Status	Red Hat  Solaris  VMware ESX  Windows  Primary Function	(1 teg)	
Virtual Infrastructure	Domain Controller	(1 (40)	
▼ Tag Sets			
Location     Owner     Platform Family     Primary Function     Tutorial	▼ Tutorial ☑ Tutorial tag	(1 tag)	
▼ Saved Filters			
Windows 2008 R2 Domain Controllers Windows 2012 R2 Domain Controllers			
Operational Tag Sets			
▶ Health	-	Close	
Node Manager			Last Axon Agent config: 16 hours ago (Oct 12, 2018 12:00:17 AM)   User: admin

11. Click Close.

## 2.9.5.3 *Rules*

This section will describe how to create a rule.

1. Click Rules.

ENTERPRISE HOME NODES RULES ACTIONS TASKS POLICIES LOG REPORTS SETTINGS

2. Select or create a rule group in which to put the new rule.

🛛 Hefresh 🔟 Help 🕼 Log

Rules Rule Search	NODES   RULES   ACTIONS   TASKS   POLICIES   LOG   REPORTS   SETTINGS	😔 Refresh 🔟 Help 🖟 Logout
🖺 💁 New Group 🚺 Nev	v Rule 🖓 Import 🕼 Export 🔄 Duplicate 🗙 Delete 🏡 Link 🚳 Unlink 🕼 Move	
- Tripwire	Rules	Tutorial
Root Rule Group     Linux OS Rule Grou		
Solaris OS Rule Gr	oup 1	
Ulfware Virtual In	rastru Group	
🕞 🦳 Critical Change		
Policy Rules     Testing		
Co Uninked		
520		
23		

- 3. Click New Rule.
- 4. Select the type of rule. For monitoring Windows filesystems, we choose **Windows File System Rule.**



- 5. Click **OK.**
- 6. Enter a name and description for the rule.

🛈 🔒 https://	New Windows File System Rule Wizard - tripwire-e/console/app.showWizard.cmd?wizardName	
New Windov	rs File System Rule Wizard	2 Help
Name:	and description for the rule. tutorial rule a rule specifically for tutorial documentation	
🗹 Enable Tra	cking Identifier	
	1	< Back Next > Finish Cancel
ck Next.		

7.

۵	New Windows File System Rule Wizard - Mozilla Firefox
🛈 陷 https	s://tripwire-e/console/app.showWizard.cmd?wizardName=si.web.specifierRule 🖤 😎 😭 🗄
New Wind	ows File System Rule Wizard
New Start	Point Point Browse X Delete
🛓 Path	Type Default Severity Criteria Set Recurse Level Archive Content
	< Back   Next >   Finish   Cancel

- 8. Click New Start Point.
- 9. For Path, enter a directory that represents the scope of the scan. It can be limited to the documents folder or be wide enough to encompass all the files on a system. Note that the latter will take much longer to scan.
- 10. Check the box next to **Recurse directory** if you also wish to scan all subfolders.

New Start Point Wizard			? He
Archive element content	_ 💘	ettings.	

#### 11. Click Next.

#### 12. Select Windows Content and Permissions.

<b>)</b>	New Start Point Wizard - Mozilla Firefox
🛈 👠 https://tripwire-e/	onsole/app.showWizard.cmd?wizardName=si.web.startPointWiz 🚥 😒 😭 🗄
New Start Point Wiza	d 🛛 Help
🛐 New Criteria Set 🚺 Ne	/ From Selected
🛓 Name	Description
🖲 🎬 Windows - Conten	and Permissions
🔿 🎬 Windows - Conten	Dnly
🔿 🎬 Windows - Permiss	ons Only
	< Back Next > Finish Cancel
	ricu

#### 13. Click Finish.

- 14. Click New Stop Point.
- 15. Enter the path of any folders or files that should not be included in the scan, and indicate whether they should end the recursion.

<b>)</b>	New Stop Point Wizard - Mozilla Firefox	- 0	x
1 🔒	https://tripwire-e/console/app.showWizard.cmd?wiz •••		≡
New S	Stop Point Wizard	? H	elp
Specif setting Path:	C:\Users\DI2\Desktop\Tutorial docs\Tutorial3 ✓ Stop recursion	sociate	

- 16. Click Finish.
- 17. Click Next.
- 18. Click Next.
- 19. Click Finish.

### 2.9.5.4 *Tasks*

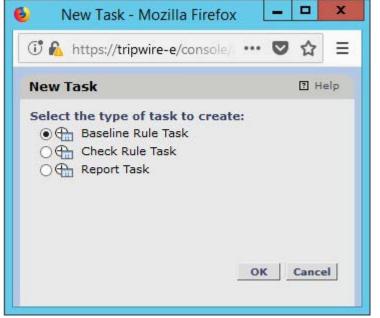
This section will describe how to create a task.

1. Click Tasks.

		S ACTIONS TASKS POLICIES LOG REPORTS SETTINGS
2.	Select a folder fo	or a new task or create one.
	Tasks Task Search	
	📃 Manage 🖣 🎦 New Group 🎦	New Task 🗿 Import 🕼 Export 🔁 Duplicate 🗴 Delete 🛸 Link 🎄 Unlink 🕵 Move Control 🖣 Run 🖳 Baseline 🚱 Stop 🔂 Disable 🔂 Enable
	<ul> <li>Tripwire</li> <li>2 Root Task Group</li> </ul>	Tasks
	Check Tasks	Anme Type Status Last Start Last Duration Timeout Next Start Description
	Change Audit Report	
	Configuratio     Configuratio     Configuratio     Configuratio	
	Tutorial Tasking	
	Unlinked	

3. Click New Task.

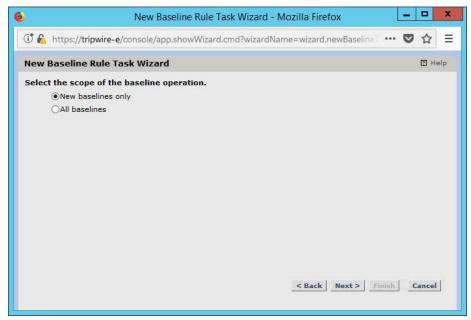
4. Select **Baseline Rule Task** or **Check Rule Task** (Note: Both are needed: baseline creates the initial state of the monitored object, and check updates the state and reports any changes).



- 5. Click OK.
- 6. Enter a name and description for the task.

6	New Baseline Rule Task Wizard - Mozilla Firefox 📃 🗖 🗙
🛈 🚯 https://	/tripwire-e/console/app.showWizard.cmd?wizardName=wizard.newBaseline 🛛 🚥 😒 🏠 🗏
New Baselin	e Rule Task Wizard
Enter the tas	k name and description.
Name:	Tutorial Task
Description:	Task for tutorial documentation
Run as user:	admin v
Use time	hour(s) 3 minute(s)
	< Back Next > Finish Cancel

- 7. Click Next.
- 8. Select whether you want all baselines to be updated or to only create new baselines.

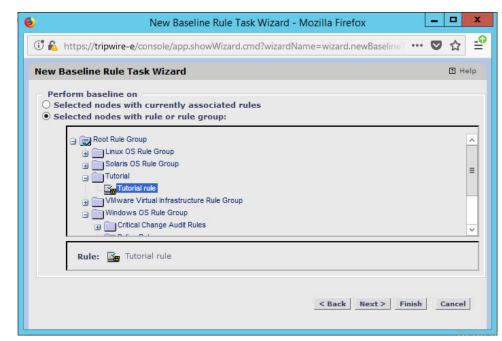


#### 9. Click Next.

10. Select the systems to be included in the task. You can use tags or select by operating system (or other defaults).

New Baseline Rule Task Wizard - Mozilla Firefox	_		x
🕕 🚯 https://tripwire-e/console/app.showWizard.cmd?wizardName=wizard.newBaseline	🔊	☆	- <b>0</b>
New Baseline Rule Task Wizard		Рн	elp
Work House Groups         Smart Node Groups         Operational Tag Sets         Saved Filters         System Tag Sets         Tag Sets         Owner         O I Testing         Platform Family         Primary Function         Tutorial         WINDOWS10-1.DLIPDR         WINDOWS10-2.DLIPDR         WINDOWS10-3.DLIPDR			< III >
Selection: 😌 Tutorial tag			
< Back Next > Finis	sh (	Cancel	Ĩ

- 11. Click Next.
- 12. Select the rule created earlier.



#### 13. Click Next.

14. Set the schedule of this task according to your organization's needs.

N	tee Bele Teels Minered		
New Base	line Rule Task Wizard		7 He
Specify wh	en you want this task to run.		
Interval:	Manually		
	Hourly		
The task w	Daily Y-		
	Weekly		
	Monthly		
	Monthly by Day		
	Once		
	Interval		
	Periodic		
	Manually		
0.3			

15. Click Finish.

# 2.10 Tripwire Log Center

### 2.10.1 Install Tripwire Log Center Manager

See the *Tripwire Log Center 7.3.1 Installation Guide* that should accompany the installation media for instructions on how to install **Tripwire Log Center.** Use the **Tripwire Log Center Manager** installer.

#### Notes:

- a. It is recommended that you install **Tripwire Log Center** on a separate system from **Tripwire Enterprise.**
- b. You will need to install **JRE8** and the **Crypto** library. Instructions are also in the *Tripwire Log Center 7.3.1 Installation Guide*.
- c. .NET Framework 3.5 is required for this installation; install this from the Server Manager.
- d. You may need to unblock port **9898** on your firewall for the TE agents.
- e. Do not install PostgreSQL if you wish to use a database on another system; this guide will use a local PostgreSQL database, however.
- f. When it finishes installing, there should be a configuration wizard (see below for configuration steps).

# 2.10.2 Configure Tripwire Log Center Manager

1. The configuration wizard should start after the installation is complete.

*	Configuration Wizard 🗙
	Welcome to the Tripwire Log Center Manager Configuration Wizard
	To begin the configuration process, click Start. For further guidance, see the Tripwire Log Center Installation Guide.
	Start 📎

2. Click Start.



- 3. Click New Install.
- 4. Enter the registration details for your **Tripwire Log Center** license.

6		Tripwire Log Center
	7	Register Tripwire Log Center To continue you must register your copy of Tripwire Log Center.
		Name
		Serial Number
		Email Address
Get Help		Register Cancel

- 5. Click Register.
- 6. Enter details about the database that Tripwire Log Center should use.

				Database	
Database		ts. Following inst		nvironment, an Event-Manager nay add other databases to ma	
Connec	tivity —		S	ecurity	
Databa	se software	MS SQL	~	Encrypt data with SSL	
Host IP	address	192.168.1.141			
Host po	ort	1433			
Use Wi	ndows authe	ntication 🗸			
assigne	ed to the Trip	Windows creder wire Log Center N o an MS SQL inst	Manager	R	
Userna	me				
Passwo	ord				
		[	Test Conn	ectivity	
		L.		Next 📎	Exit

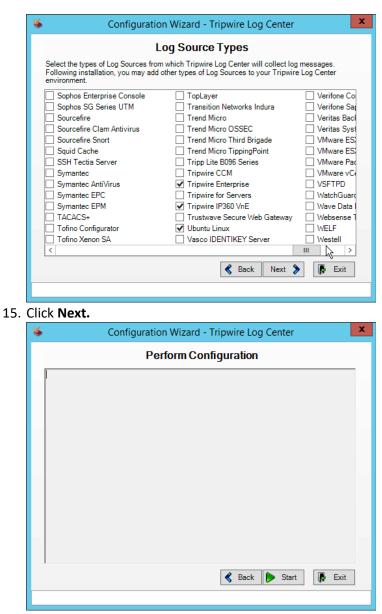
- 7. Click Next.
- 8. Select a directory to store log messages in, such as C:\Program Files\Tripwire\Tripwire Log Center Manager\Logs\AUDIT.

Sconfiguration Wizard - Tripwire Log Center	x
Audit Logger Settings	
The Audit Logger is the log-management tool in Tripwire Log Center. Collected log messages are stored in the Audit Logger File Store.	
Root directory for the Audit Logger File Store C:\Program Files\Tripwire\Tripwire Log Center M 💓 Browse	
R	
х 	
🔇 Back Next 📎 🚺 Exit	

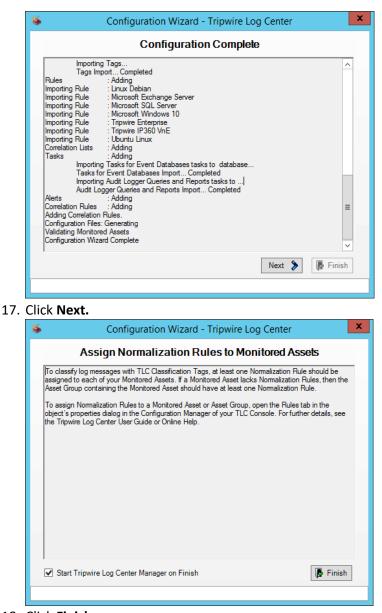
- 9. Click Next.
- 10. Enter a **password** and an **email**.
- 11. Change the IP to a hostname, if preferred.

*	Configuration Wizard -	Tripwire Log Center	x
	Primary Mana	ger Settings	
Additiona	ame of your choosing for the Primary Man Ily, enter and confirm a password for the o password to log in to Tripwire Log Center	default Administrator user account.	
	Primary Manager		
	Manager name	Primary Manager	
	Manager IP/hostname	arcsight-cons.di.ipdr	
	Enable Auto-Discovery 2		
	Administrator Settings Administrator password	0	
	Administrator password (confirm)	•••••••	
	Email address	administrator@di.ipdr	
N		again instator Campail	
R			
		Back Next 📎	Exit
			<b>_</b>
2. Click Nex	kt.		
*	Configuration Wizard -	Tripwire Log Center	x
	Manager Servic	e Credentials	
Specify th	ne user account with which Tripwire Log C	Center will authenticate with other he	osts.
	Authenticate with:		
	The local Windows Syste O Domain user account	m user account	
	Username:		
	Password:		
	Password (confirm):		
			4
	Apply Apply	Settings	v
		🔇 Back Next 📎	Exit

- 13. Click Next.
- 14. Select any log sources that you expect to collect with **Tripwire Log Center**. Examples: **Tripwire Enterprise**, **Microsoft Windows 10**, **Tripwire IP360 VnE**, **Linux Debian**, **Ubuntu Linux**, **Microsoft Exchange**, **Microsoft SQL Server**.



16. Click Start.



18. Click Finish.

# 2.10.3 Install Tripwire Log Center Console

Chapter 4 of the *Tripwire Log Center 7.3.1 Installation Guide* details the installation of the **Tripwire Log Center Console.** Use the **Tripwire Log Center Console** installer.

You can install this on the same machine as the Tripwire Log Center Manager, if desired.

# 2.11 Cisco Identity Services Engine

This section will detail the installation and some configurations for the Cisco Identity Services Engine (ISE). It assumes the use of the ISE virtual machine.

## 2.11.1 Initial Setup

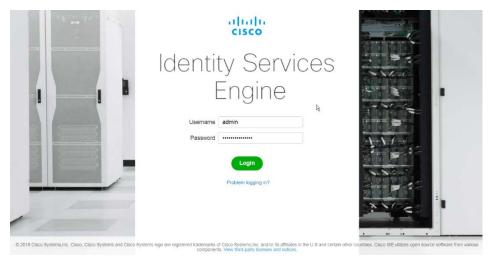
- 1. When prompted to log in for the first time, enter **setup**. (You can use the command **reset**-config to change these values later.)
- 2. Enter the desired **hostname** for the machine.
- 3. Enter the desired **IP address** for the machine. (Ensure that the specified hostname is associated with this IP address in your DNS.)
- 4. Enter the **netmask** for the machine.
- 5. Enter the **default gateway.**
- 6. Enter the **default DNS domain** (the name of your domain).
- 7. Enter the primary nameserver (the IP address of your DNS).
- 8. Enter a second nameserver if desired.
- 9. Enter an **NTP time server.**
- 10. Enter the **timezone.**
- 11. Enter Y for SSH service.
- 12. Enter an administrator **username** for the machine.
- 13. Enter a **password** twice.

### 2.11.2 Inventory: Configure SNMP on Routers/Network Devices

See the corresponding vendor documentation for the correct way to enable SNMP on your network device. Ensure that the community string you choose is considered sensitive, like a password.

### 2.11.3 Inventory: Configure Device Detection

1. Log in to the web client by visiting https://hostname/admin, but replace **hostname** with the hostname of the ISE machine.



2. On the top right, use the small play button to select Visibility Setup.

PassiveID	Setup							
Visibility Se	etup		lizard					
Wireless S	etup (B	ETA)	120110					
Click Next								
cisco Identity Service	s Engine	Home → Cont	ext Visibility	rations ►Policy ►A	Iministration + Wo	rk Centers	License Warning 🔺 🤇	
Welcome 1 Endpoint     Get to know the				re   ✓ Summary	I context with th	is setup wizard.		•
								•
	devices and	l users' detai	ls of your netwo	rk. Gain visibility and	I context with th	is setup wizard. Group Name Cisco.com/Network Configuration Ope	rators	•
	devices and	l users' detai Domain	ls of your netwo	rk. Gain visibility and IP Address 10.56.53.76 10.56.53.77	8	Group Name		
	devices and	l users' detai Domain Cisco.com	DC Host DC1.Clace.com DC2.Clace.com DC3.Clace.com	rk. Gain visibility and IP Address 10.56.53.76 10.56.53.77 10.56.53.78	0 0 0	Group Name Cisco.com/Network Configuration Ope Cisco.com/Performance Monitor Users Cisco.com/Performance Log Users		
	devices and	d users' detai Domain Cisco.com Cisco.com	DC Host DC1.Cisco.com DC2.Cisco.com DC3.Cisco.com DC3.Cisco.com	rk. Gain visibility and		Group Name Cisco.com/Network Configuration Ope Cisco.com/Performance Monitor Users Cisco.com/Performance Log Users Cisco.com/Distributed COM Users		-
	devices and	Domain Cisco.com Cisco.com	DC Host DC Host DC2, Cisco.com DC3, Cisco.com DC4, Cisco.com DC4, Cisco.com	rk. Gain visibility and IP Address 10.56.53.76 10.56.53.77 10.56.53.78	0 0 0	Group Name Cisco.com/Network Configuration Ope Cisco.com/Performance Log Users Cisco.com/Performance Log Users Cisco.com/Disvibuted COM Users Cisco.com/Disvibuted COM Users		
	devices and	Domain Cisco.com Cisco.com Cisco.com Cisco.com Cisco.com	DC Host DC1.Cisco.com DC2.Cisco.com DC3.Cisco.com DC3.Cisco.com	rk. Gain visibility and IP Address 10.56.53.76 10.56.53.78 10.56.53.79 10.56.53.80	0 0 0 0 0	Group Name Cisco.com/Network Configuration Ope Cisco.com/Performance Monitor Users Cisco.com/Performance Log Users Cisco.com/Distributed COM Users		C Ext Wear

- 4. Enter the range of IP addresses to add to ISE's inventory.
- 5. Ensure that **Active Scanning** is checked.

ngine Home	Context Visibility	Operations	+ Policy	<ul> <li>Administration</li> </ul>	Work Centers	License Warning 🔺	$Q_{\rm eff}$	0	•	•
endpoints using the	IP range(s) below.									
192.163.0.0/16									Delete	
e.g. 10.10.10.0/24				14					Delete	6
8 0										
										_
						240		ack	No	KE.
	endpoints using the	endpoints using the IP range(s) below. 192 103 0.0/10 e.g. 10.10.10.0/24	endpoints using the IP range(s) below. 192 103 0.0/10 e.g. 10.10.10.0/24	endpoints using the IP range(s) below. 1922-103-0.0/10 e.g. 10.10.10.0/24	endpoints using the IP rangels) below. 192 163 0.0/10 eg 10 10 10 00/24 Bg	endpoints using the IP range(s) below. 192 103 0.0/10 eg. 10.10.10.0/24 Bg	endpoints using the IP range(s) below.	endpoints using the IP rangels) below.	endpoints using the IP range(s) below.	endpoints using the IP range(s) below. 192.108.0.010 e.g. 10.10.024 Dg @ •

- 6. Click Next.
- 7. Click the Add Device Manually link.
- 8. Enter a name.
- 9. Enter the IP address of the network device you configured for SNMP.
- 10. Select 1 for SNMP version.
- 11. Enter the **community string** you created.

Cisco contrady and the contract of the	Context Visionity	ions + Policy + Administration + Work Genters		/ Genie Warning 🔺 🔍 🔍 🔿 🔗
ISE VISIBILITY SETUP WIZARD	Add Network Dev	ice	×	G• Exit Wicard
Network Device Discovery	Name *	GATEWAYROUTER		
Total Added (0) Failed (0)	IP Address *	192.168.1.1		
Q, Scan 🔶 Add 📓 fermine 4	Location			Y Filter •
Name IP Address You have not added any retrievely access de	Device Type			
	Description			Back
	SNMP Settings	ţ\$		
	SNMP Version *	1		
	RO Community *		Show	

12. Click OK.

Identity Services E	Engine Home   Context Visibility   Operations   Policy   Administration   Work (	Centers Licen	se Warning 🔺 🔍 🎯 🔿 👘
ISE VISIBILITY SETUR			🕒 Exit Wiza
H mineante - anapara	• Contract • Contract		
Network Device Discovery	1		
Total Added (1)	Failed (0)		
Q Scan + Ad	id 🖀 Remove 🗛 Add Location		¥ Filter 🛩
Name	IP Address Device Type Location Description	Action	
GATEWAYR	OUT 192.168.1.1	Edit	
			4
			Back
			Server Response
			Network Devices created successfully
Click Next.			
Enter a <b>disp</b>	ilay name.		
Enter the de	omain name.		
Enter the <b>h</b>	ostname of Cisco ISE.		
	rname and password.		
	-		
	onnection to ensure that this works.		
cisco Identity Services E	Engine Home Context Visibility Operations Policy Administration Work Co aury (Acr)	enters License	Warning 🔺 🤍 📵 O 🗘
Connect Active Directory se	erver to get user identity information. You can add one or more Active Directories.		
Display Name *	ADDNS.		
and a second second			
Domain FQDN *	DLIPDR		
Domain FQDN *			
	DI IPDR cisco-ise di ipdr		
Domain FQDN *			
Domain FQDN * ISE Node *	cisco-ise di jpdr		
Domain FQDN * ISE Node * Username * Password *	cisco-ise di ipdr Administrator		
Domain FQDN * ISE Node * Username *	cisco-ise di ipdr Administrator	R	
Domain FQDN * ISE Node * Username * Password *	cisco-ise di ipdr Administrator	Ę	

19. Click Next.

Add another Active Directory server

- 20. Enter a username and password.
- 21. Check the box next to Enable Endpoint Logging.
- 22. Check the box next to Include Range.

Skip Back Next

ISE VISIBILITY SETUP	WIZARD									
A Welcome 1 Endpoints		3 Active Directory	4 Posture	✓ Summary					G	• Exit
Posture Discovery										
Discover posture on endpoints	s using common admini	strative account and sar	me IP range(s) fr	om step 1						
Username *	Administrator									
Password *										
Enable Endpoint Logging	~ •									
	100 100 0 010									
IP Address Range *	192.168.0.0/16									
Include Range	2 O									
									₽¢.	
								Skp	Back	
Click <b>Next.</b>								Skp	Back	
Click Next.	gine Hame	→ Context Visibility	Operations	Policy	Administration	→ Work Centers	License Warning			
		<ul> <li>Context Visibility</li> </ul>	+ Operations	▶ Policy	Administration	Work Centers	License Warning			
dentity Services En		Context Visibility	Operations	<ul> <li>Policy</li> </ul>	► Administration	Work Centers	License Warning			
Active Scanning	true <b>O</b>	Context Visibility	Operations	▶ Policy	<ul> <li>Administration</li> </ul>	Work Centers	License Warning			
Active Scanning	true <b>O</b>	Context Visibility	➤ Operations	▶ Policy	<ul> <li>Administration</li> </ul>	Work Centers	License Warning			
Active Scanning Active Scanning Network Device Discovery Total Devices Added	true O	Context Visibility	➤ Operations	▶ Policy	<ul> <li>Administration</li> </ul>	➤ Work Centers	License Warning			
Identity Services En Active Scanning Network Device Discovery Total Devices Added Active Directory Information Display Name Domain FQDN	true	Context Visibility	➤ Operations	▶ Policy	⊁ Administration	➤ Work Centers	License Warning			
Identity Services En     Active Scanning     Network Device Discovery     Total Devices Added     Active Directory Information     Display Name     Domain FQON     ISE Node	true  1 ADDNS	Context Visibility	➤ Operations	► Policy	► Administration	Work Centers	License Warring			
Identity Services En Active Scanning Network Device Discovery Total Devices Added Active Directory Information Display Name Domain FQDN	true	Context Visibility	> Operations	> Policy	<ul> <li>Administration</li> </ul>	➤ Work Centers	License Warning			

- 24. Verify the settings, and click **Done.** (This should begin importing endpoints connected to the network device, and they will be visible on the ISE dashboard.)
- 2.11.4 Policy Enforcement: Configure Active Directory Integration
  - 1. Navigate to Administration > Identity Management > External Identity Sources > Active Directory.

GEdit

De

Posture Discovery

IP Scanning Range

192 168 0 0/16

Included true 0

	Context Visibility      Operations      Policy      Administration      Work Centers	License Warning 🛕	۹,
System      Identity Management     Network R     Identities Groups External Identity Sources	esources	ireless setup and visibility setup D	o not s
External Identity Sources	Active Directory		
Click <b>Add.</b> Enter a <b>name.</b>			

- 2.
- 3.
- 4. Enter the **domain.**

	sources		Threat Cen     Click here to do wireless setup and visib	ility setup Do not s
External Identity Sources	Connection * Join Point Name * Active Directory Domain B Submit Cancel	AD-DNS di.ipdr		

-1[-1]-- Identity Services Engine Home + Context Visibility + Operations + Policy Administration + Work Centers License Warning A Q

5. Click Submit.

Identitive Identity Services Engine Home     System      Identity Management     identities Groups External identity	Context Visibility     Operatio Would you like to Join all ISE Nodes to		ation Viork Centers	License Warning 🔺 🔍
External Identity Sources	* Join Point Name	AD-DNS	No Yes	Advanced Settings
Centricate Authentication Profile     Active Directory     Active Directory     AD-DNS     LDAP     DOBC	* Active Directory Domain	di.lpdr ser 🙆 Dagnostic Tool 😪 Refi	resh Table	£
RADIUS Token RSA Securit Social Login Social Login	ISE Node	ISE Node Role STANDALONE	Status Domain (	Controller Site

- 6. Click Yes.
- 7. Enter a **username** and **password** to join ISE to the domain.

External Identity Sources       Coreaction       Writelisted Domains       PasswelD       Groups       Attributes       Advanced Settings            • Contracta Automitization Profile           • Jon Point Name         AD/DNS           · Jon Point Name         AD/DNS           //            // <th></th> <th></th>		
Join Point Name AD-ONS     Advec Drectory     Advec Drectory	External Identity Sources	Connection Whitelisted Domains PassiveID Groups Attributes Advanced Settings
AD-DNS Join Domain × Please specify the credentials required to Join ISE node(s) to the Active Directory Domain. AD User Name () DI/Administrator * AD User Name () DI/Administrator * Password * Password Social Login Store Credentials ()		Join Point Name AD-DNS
RADIUS Token     'Password     'Password     RSA Securit     Social Login     Social Login     Store Credentials ()	AD-DNS	Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.
Social Login Store Credentials ()	RADIUS Token	
Enter Cancel	SAML Id Providers	
	Social Login	Cancel

8. Click **OK.** 

	Home Context Visibility Network Resources Device 1 y Sources Identity Source Seque	Portal Management pxGrid Serv		Threat Cen     Click here to do v	License Warning 🔺 🔍 🤇
External Identity Sources	Join Operation Status Status Summary: Successful ISE Node cisco-ise di lipdr	Node Status     Z Completed.	Dg	X er R	Advanced Settings Site Default-First-Site-Na

9. Click **Close** when the join is finished.

# 2.11.5 Policy Enforcement: Enable Passive Identity with AD

This configuration allows users to use Active Directory usernames/passwords as authentication for the portal. The web portal will allow clients to download profiling software to ensure that clients have up to date software and can be trusted on the network.

- 1. Navigate to Administration > System > Deployment.
- 2. Check the box next to ISE.

riterite Identity Services Engine Home + (	Context Visibility → Operations → Policy	nk Centers License Warning 🛕 🔍 🛛 o
	ources	
Deployment Licensing + Certificates + Logging	Maintenance Upgrade      Backup & Restore      Admin Access      S	Settings
Deployment	Deployment Nodes	
φ•Ε• ∰•		Selected 1   Total 1 🛞 🤤
Deployment     PAN Fallover	🖌 Edit 🔯 Register 🧕 Syncup 💆 Deregister	Show All
M PAN Palover	Hostname A Personas	Role(s) Services Node Status
	Cisco-ise Administration, Monitoring, Policy Service	STANDALONE IDENTITY MAPPING, SESSION, PROFILER
Click <b>Edit.</b>		

4. Check the box next to Enable Passive Identity Service.

o Identity Services Engine Home (	Context Visibility	License Warning 📣	Q	0	•
System + Identity Management + Network Res	surces				
ployment Licensing + Certificates + Loggin	Maintenance Upgrade      Backup & Restore      Admin Access      Settings				
	Role STANDALONE Make Primary				
	G Administration				
	✓ ▼ Monitoring				
	Role PRIMARY *				
	Other Manitoring Node				
	Policy Service				
	✓ Fnable Session Services ()				
	Include Node in Node Group None 👘 👔				
	Enable Profiling Service (j)				
	Enable Threat Centric NAC Service (j)				
	■ Finable SXP Service (i)				
	Enable Device Admin Service (i)				
	Enable Passive Identity Service (1)				
	pxGrid @				
	Save Reset				

- 5. Click Save.
- 6. Navigate to Administration > Identity Management > External Identity Sources > Active Directory.
- 7. Click the name of the Active Directory machine.
- 8. Check the box next to the join point you just created.

dentity Services Engine Home	Context Visibility     Operations     Policy     Administration     Work Centers	License Warning 🛕	Q,	0	0	0
System      Identity Management     Network	Resources					
Identities Groups External Identity Sources	Identity Source Sequences					
External Identity Sources	Active Directory ▲ Gat					

- 9. Click Edit.
- 10. Click the **PassiveID** tab.
- 11. Click Add DCs if there are no domain controllers listed.

cisco Identity Services Engine	Home Context Visibility	+ Opennoiss - + Policy	*Administration		Liceme Wanning A	9. <b>0 0</b> 4
Eystem     Identities     Groups     Extended					×	
External Identity Source	Add Domain Controllers					
• E Centrate Automoa		Domain	DC Host	Site		
- Adve Dremory	0	di.ipdr	ad-dns-supp.di.ipdr			
CDAP		DLIPDR	AD-DNS.DLIPDR	Default-First-Site-Name		
RADIUS Token	0	di.ipdr	ad-dns08.di.ipdr		14	
SAAL IS Providers				Cancel	ок	

- 12. Select the Active Directory domain controller.
- 13. Click OK.
- 14. Check the box next to the selected domain controller.
- 15. Click Edit.
- 16. Enter credentials for an administrator account.

Adentifiaes Groups Exte				
External Identity Source	Edit Domain Controller			
0.* <u>*</u> *	Host FQDN	AD-DNS DLIPDR		
Cectical Automotiv     Cectical Automotiv     Cectical Active Directory     Active Directory     Active Directory     Active Directory     Active Directory     Active Directory	Description			Co. 1 Total Rows
DOBC RADIUS Tokes	User Name *	administrator		
RISA Securito	Password	Show Password		Monito
SALAL Id Providers				Sweller /
	Protocol	WMI * Configure Test	53	
			Cancel Save	

- 17. Click Save.
- 18. Click Config WMI.
- 19. Click OK.

entities Groups External Identity Sources	Identity Source Sequences	Settings			
xternal Identity Sources	Connection V	Attelisted Domains PassiveID Groups Atte	nbutes Advanced S	stings	
	PassiveID Domain		ows/Page 1 *	1 /1 Go	1 Total Rows
ADDNS LDAP COBC	C Refresh & E	Config WMI in process	MI Add Agent		
RADIUS Token	Domain     Configuration of WMI has begun and will take some tim		IP Address	Monit	
RSA SecuriD SAML Id Providers Social Login	DIPDR	Status will be shown on completion. Run in background? $\begin{tabular}{c} \begin{tabular}{c} tabula$	t-First-Site-Name	192 168 1 12	WM
	-			_	

- 20. Click **OK** when this configuration finishes.
- 21. Navigate to Administration > System > Settings > Client Provisioning.
- 22. Set Enable Automatic Download to Enable.

cisco Identity Services Engine	Home   Context Visibility  Operations	Policy     Administration     Work Centers	License Warning 🛕	R 6	0	•
System      Identity Management	Network Resources	pxGrid Service   Feed Service   Threat Centric NAC				
Deployment Licensing + Certificates	Logging      Maintenance Upgrade      Bac	kup & Restore + Admin Access - Settings				
0						
Client Provisioning	Client Provisioning					
FIPS Mode	chere i rousioning					
Security Settings	* Enable Provisioning	Enable *				
Alarm Settings	* Enable Automatic Download	Enable - T				
▶ Posture	" Update Feed URL	https://www.cisco.com/web/secure/spa/provisioning-upda	D			
Profiling	* Native Supplicant Provisioning Policy Unavailable	Apply Defined Authorization Policy *				
Protocols						
Proxy	Save Reset	5				
SMTP Server		10				
SMS Gateway						
System Time						
ERS Settings						
Smart Call Home						
DHCP & DNS Services						
Max Sessions						

- 23. Click Save.
- 24. Navigate to Administration > Identity Management > External Identity Sources > Active Directory.
- 25. Click the **Groups** tab.
- 26. Click Add > Select Groups from Directory.
- 27. Click **Retrieve Groups.** (This should populate the window with the groups from Active Directory.)
- 28. Select them all.

System	Select Directory Groups This dialog is used to select g					×
<ul> <li>Identities</li> </ul>	Domain di.ipdr			*		
	Name Filter *	SID Filter		Type ALL	*	
¢ .	Retrieve Groups	68 Groups Retrieved.		1 mar		
	Name Name		Group SID		Group Type	
on Profile	DI.IPDR/Builtin/Access	Control Assistance Operators	di.ipdr/S-1-5-32-579		BUILTIN, DOMAIN LOCAL	
	DI IPDR/Builtin/Account	t Operators	di.ipdr/S-1-5-32-548		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Adminis	trators	di.ipdr/S-1-5-32-544		BUILTIN, DOMAIN LOCAL	
	DI IPDR/Builtin/Backup	Operators	di.ipdr/S-1-5-32-551		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Certifica	ate Service DCOM Access	di.ipdr/S-1-5-32-574		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Cryptog	raphic Operators	di.ipdr/S-1-5-32-569		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Distribu	ted COM Users	di.ipdr/S-1-5-32-562		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Event L	og Readers	di.ipdr/S-1-5-32-573		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Guests		di.ipdr/S-1-5-32-546		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Hyper-	/ Administrators	di.ipdr/S-1-5-32-578		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/IIS_IUS	RS	di.ipdr/S-1-5-32-568		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Incomin	g Forest Trust Builders	di.ipdr/S-1-5-32-557		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Network	Configuration Operators	di.ipdr/S-1-5-32-556		BUILTIN, DOMAIN LOCAL	
	DLIPDR/Builtin/Perform	ance Log Users	di.ipdr/S-1-5-32-559		BUILTIN, DOMAIN LOCAL	

- 29. Click **OK**. (If you add more groups to Active Directory, they can be imported in the same way in the future.)
- 30. Click the **Attributes** tab.
- 31. Click Add > Select Attributes from Directory.
- 32. Enter a username.
- 33. Click **Retrieve Attributes.** (This will populate the window with Active Directory's available attributes, so they can be used for policy in Cisco ISE.)
- 34. Click OK.
- 35. Select any desired attributes.

<ul> <li>System</li> </ul>	Onit	ectory Attributes y attributes selected below will be		y conditions in po	licy rules.			×
<ul> <li>Identities</li> </ul>	* Si	Imple User or Machine Account	ciscoiseadmin Retrieve Attributes	Ð				
		Name	<ul> <li>Туре</li> </ul>		Example Va			
rces.		logonHours	OCTET_STRING		(Binary Valu	ie)		
	1	mDBUseDefaults	STRING		TRUE			L R
ication Profile		memberOf	STRING			zation Management,O	J=Microsoft Exchange Security Group	L R
		msExchDumpsterQuota	STRING		31457280			
		msExchDumpsterWarningQuota	STRING		20971520			
		msExchHomeServerName	STRING		(Non-Displa	yable or XSS data)		
		msExchUserAccountControl	STRING		0			
		name	STRING		ciscoiseadn	nin		R
		objectCategory	STRING		CN=Person	CN=Schema,CN=Cor	figuration,DC=DI,DC=IPDR	~
		objectClass	STRING		top			
		objectGUID	STRING		887223A09	96062468648D3C3B8	65A0C7	
		objectSid	STRING		S-1-5-21-28	893925980-384658434	3-2419738538-1268	
		primaryGroupID	STRING		513			
		protocolSettings	OCTET_STRING		(Binary Valu	ue)		
		pwdLastSet	STRING		131889436	495884672		
		sAMAccountName	STRING		ciscoiseadn	nin		
		sAMArcountType	STRING		805306368			-
	4							
								OK Cancel

#### 36. Click OK.

#### 37. Click Save.

## 2.11.6 Policy Enforcement: Developing Policy Conditions

- 1. Navigate to Policy > Policy Elements > Conditions > Posture.
- 2. Expand the **Posture** section. This will reveal a list of categories for conditions. (Note: these conditions allow you to select or define requirements that endpoints should meet. In typical enterprises these conditions can be used as requirements to gain network access; however, this strongly depends on the capabilities of your network device. Furthermore, the network device
- 3. As an example, we will require that Cisco AMP be installed on all Windows devices. If you are using a different anti-malware software, locate that instead. Click **Anti-Malware Condition.**

Identity Services Engine	Home	Context Visibility	Operations		Administration	Work Centers		License W	aming
Policy Sets Profiling Posture	Client Prov	Policy Elements					Click here to do wireles	s setup and vi	isibility :
e brary Conditions mart Conditions	Ant	i-Malware Conditions							
me and Date	1	Edit +Add Duplicate		ription				Show	All
Posture		ANY_am_win_inst ANY_am_win_def	0.00	AM installation AM definition ch					
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition		ANY_am_mac_inst ANY_am_mac_def Cisce-AMP	Any /	AM installation AM definition cl irres Cisco AMP					
Disk Encryption Condition File Condition Firewall Condition			R						
Patch Management Condition Registry Condition Service Condition									
USB Condition Hardware Attributes Condition									

- 4. Click Add.
- 5. Enter a name.
- 6. Enter a **description** if desired.
- 7. Select Windows All for Operating System.
- 8. Select Cisco Systems, Inc. for Vendor.
- 9. Under **Products for Selected Vendor,** check the box next to **Cisco Advanced Malware Protection,** with the version number you have installed.

← → C ▲ Not secure	https://cisco-ise.di.ipdr/a	admin/#policy/p	oncy_contents	1			☆ <b>0</b>
Identity Services Engine	Home + Context \	visibility → Ope	erations 💌 Pe	licy Administration	Work Centers     ■	🕘 L	icense Warning 🔺
Policy Sets Profiling Posture	Client Provisioning  Pol	licy Elements				Click here to do wireless s	atup and visibility a
Dictionaries Conditions Re						Click liele to do wireless s	etup and visionity s
dubrary Conditions	Anti-Malware Conditio		Malware Condit	ion			
Smart Conditions	* Name	CiscoAMP					
Time and Date	Description	Check for cisco	AMP	1			
	<b>A 1 1 1 1</b>	, d u es later (7)					
	Compliance Module	4 A UI Id/CI					
Posture			4				
Anti-Malware Condition	* Operating System	Windows All	\$				
Anti-Malware Condition Anti-Spyware Condition	* Operating System Vendor	Windows All Cisco Systems, In	nc.	9			
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition	* Operating System Vendor	Windows All	nc.				
Anti-Malware Condition Anti-Spyware Condition	* Operating System Vendor Check Type	Windows All Cisco Systems, In Installation	nc.	2			
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition	* Operating System Vendor Check Type * Products for So	Windows All Cisco Systems, Ii Installation elected Vendor	Definition				
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition	* Operating System Vendor Check Type • Products for Si Product Name	Windows All Cisco Systems, Ii Installation elected Vendor	Definition     Version	Remediation Support	Definition Check	Latest Definition Date	Latest Defin
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition	* Operating System Vendor Check Type * Products for St Product Name ANY	Windows All Cisco Systems, In Installation elected Vendor	Definition     Version     ANY	Remediation Support N/A	YES		
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition	* Operating System Vendor Check Type • Products for S Product Name ANY Cisco Advance	Windows All Cisco Systems, Ii Cisco Systems, Ii Installation elected Vendor	Version     ANY     5.x	Remediation Support. N/A NO	YES YES	02/19/2019	7.79603
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition File Condition Firewall Condition	* Operating System Vendor Check Type • Products for S Product Name ANY Cisco Advance	Windows All Cisco Systems, In Installation elected Vendor	Version     ANY     5.x	Remediation Support N/A	YES		
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition File Condition Firewall Condition Patch Management Condition	* Operating System Vendor Check Type • Products for S Product Name ANY Cisco Advance	Windows All Cisco Systems, Ii Cisco Systems, Ii Installation elected Vendor	Version     ANY     5.x	Remediation Support. N/A NO	YES YES	02/19/2019	7.79603
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition File Condition File Condition Patch Management Condition Registry Condition	* Operating System Vendor Check Type • Products for S Product Name ANY Cisco Advance	Windows All Cisco Systems, Ii Cisco Systems, Ii Installation elected Vendor	Version     ANY     5.x	Remediation Support. N/A NO	YES YES	02/19/2019	7.79603
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition File Condition Firewall Condition Patch Management Condition	* Operating System Vendor Check Type • Products for S Product Name ANY Cisco Advance	Windows All Cisco Systems, Ii Cisco Systems, Ii Installation elected Vendor	Version     ANY     5.x	Remediation Support. N/A NO	YES YES	02/19/2019	7.79603

10. Click Submit.

## 2.11.7 Policy Enforcement: Developing Policy Results

- 1. Navigate to Policy > Policy Elements > Results > Posture > Requirements.
- 2. Click one of the black arrows next to the Edit link, and select Insert New Requirement.
- 3. Enter a name.
- 4. Select Windows All for Operating Systems.
- 5. Select **4.x or later** for **Compliance Module.**
- 6. Select Temporal Agent for Posture.
- 7. Select **User Defined Conditions > Anti-Malware Condition > Cisco AMP** (substitute "Cisco AMP" with the name of the condition you just created).
- Select Message Text Only for the Remediation Action. (Other remediation actions can be defined by going to Policy > Policy Elements > Results > Posture > Remediation Actions, but there is no option for Cisco AMP to be installed, so we leave the default for now.)
- 9. Enter a Message to show to the user to inform them that they must install Cisco AMP.

Identity Services Engine × ← → C ▲ Not secure   https://dentity.com//den	• cisco-ise.di.ipdr/admin/#policy/policy_elements/policy_elem	ants parmissions/posture pa	armissions/nosture requirements nolicy 🔹	<b>☆ ⊖</b>
		fministration + Work Centers		Q. (
Policy Sets Profiling Posture Clien	rovisioning    Policy Elements		Click here to do wireless setup and visibility set	un Do pot ci
Dictionaries + Conditions - Results			Click here to do wretess setup and visionity set	ip bonot si
0	ANY_av_win_inst then Message Text Only			
Authentication	Any_AV_Definition_Win for Windows All	using 3 x or earlier	using AnyConnect	Smet #
	ANY_av_win_def then AnyAVDefRemediationWi			
Authorization	Any AS Installation Win for Windows All	using 3 x or earlier	using AnyConnect	met if
Profiling	ANY_as_win_inst then Message Text Only			
• Posture	Any_AS_Definition_Win for Windows All ANY_as_win_def theo AnyASDefRemediationWin n	using 3.x or earlier	using AnyConnect	metif
* Remediation Actions	AMP_CHECK for Windows All 🔷 us	ing 4.x or later	using Temporal Agent	met if
Requirements	Cisco-AMP 💠 then Message 💠			*** 000000
Client Provisioning	Any_AV_Installation_Mac for Mac OSX ANY_av_mac_inst then Message Text Only	using 3 x or earlier	using AnyConnect	met if
	Any_AV_Definition_Mac for Mac OSX ANY_av_mac_def then AnyAVDefRemediationMa	using 3 x or earlier	using AnyConnect	mot it
	c Any_AS_Installation_Mac for Mac OSX ANY_as_mac_inst then Message Text Only	using 3 x or earlier	using AnyConnect	met if
	Any_AS_Definition_Mac for Mac OSX ANY_as_mac_def then AnyASDefRemediationMa	using 3 x or earlier	using AnyConnect	met if
	c Any_AM_Installation_Win for Windows All ANY_am_win_inst then Message Text Only	using 4 x or later	using AnyConnect	met if
	Any_AM_Definition_Win for Windows All ANY am win def then AnyAMDefRemediationWi	using 4.x or later	using AnyConnect	met if

10. Click Save.

## 2.11.8 Policy Enforcement: Enforcing a Requirement in Policy

- 1. Navigate to **Policy > Posture.**
- 2. Click one of the black arrows next to the Edit link and select Insert New Policy.
- 3. Enter a name.
- 4. Select Windows All for Operating Systems.
- 5. Select 4.x or later for Compliance Module.
- 6. Select Temporal Agent for Posture Type.
- 7. Select Cisco AMP (substitute "Cisco AMP" with the name of the requirement you just created).

Policy Sets Pro	dian		8	Context Visibility	• Орг	ratio	rs • Policy	Administra	ition	Work Centers		0	License Warning 🔺		٩,	
			visio	ing Policy Element							Click here	to do wi	reless setup and visibility se	etup 0	io not	sh
Any	and	Mac OSX	and	4 x or later	1	nd	Temporal Agent		and			1000	ac_temporal			Ē
lny	and	Windows All	and	4 x or later	3	nd .	AnyConnect		and			theo	Any_AM_Installation_W			L
liny	and	Windows All	and	4 x or later	a	nd.	Temporal Agent		and			then	Cisco AMP			l
Any 💠		Windows All 💠		4.x or later	•		Temporal Agent	•		(Optional) Dictionar	\$		Cisco AMP 🔶		Ľ	l
Any	and (	Mac OSX	and	4 x or later	a	nd .	AnyConnect		and			then	Default_AppVis_Requir ement_Mac		1	
kny i	and	Mac OSX	and	4.x or later	- 2	nd .	Temporal Agent		and			then	Default_AppVis_Requir ement_Mac_temporal			
Any a	and	Windows All	and	4.x or later	3	nd .	AnyConnect		and			then	Default_AppVis_Requir ement_Win			
Any	and	Windows All	and	4 x or later	.0	bn	Temporal Agent		and			then	Default_AppVis_Requir ement Win temporal			
Lones	md	Mar Oev	201	A user Inter		1	AnuCananat		and			flaces	Defails Freedal Based		. '	r.
											1	5			1	1

- 8. Click Done.
- 9. Ensure that the green checkboxes next to the rules you wish to apply are the only checkboxes enabled, as anything enabled will be enforced.

# 2.11.9 Policy Enforcement: Configuring a Web Portal

- 1. Navigate to Administration > Device Portal Management > Client Provisioning.
- 2. Select the Client Provisioning Portal (default).

cisco	dentity Serv	ices Engine	Home	<ul> <li>Context Vis</li> </ul>	ibility > Operations	► Policy	<ul> <li>Administration</li> </ul>	) → Wo	ork Centers	License Warning 🔺	٩	.0	0
+ Syst	em + Ident	ity Management	<ul> <li>Network</li> </ul>	k Resources	Device Portal Manageme	nt pxGrid Se	rvices Feed	Service	Threat Centric NAC				
Blackle	st BYOD	Certificate Prov	isioning	Client Provisioning	Mobile Device Manag	ement My D	evices Custom	Portal Files	s • Settings				
Clie	nt Provisio	ning Portals											
You	can edit and c	ustomize the defi	ault Client Pr	rovisioning portal	and create additional ones								
G	eate Edg	Duplicate	Delete										
Dentis	6	( the second											
	Client Prov	isioning Portal	(default)										
	Default port	al and user exper	fience used	to install the postu	re agents and verify comp	liance on user's	devices						

3. Click Edit.

- 4. Under **Portal Settings**, go to **Configure authorized groups**, and select the groups that should require a Cisco ISE client.
- 5. Enter a domain name for **FQDN**, and add it to your DNS.

System      Identity Management     Network Resources     Pevice Portial Management     pxQrid Service     Pevice Portial Management     pxQrid Service     Pevice Portial Management     My Devices     Custom Portal Files     Settings     Custome Portal Files     Settings     Custome Certificates     System Certificates     System Certificates     Authentication method     Configure authorized groups     Configure authorized groups     Configure authorized groups     Certificate Sequence >     Configure authorized groups     Certificates Sequence >     Configure authorized Groups     Configure	elin Identity Services Engine Home	is   Policy  Administration  Work Centers	License Warning 🗛 🔍 💿
Configure contributes at: Administration > System Certificates > System Certificates: Authentication method: * Configure authorization method: * Config	System + Identity Management + Network Resources	ement pxGrid Services + Feed Service + Threat Centric NAC	
Administration > System > Certificates > Configure authonication method: * Certificate, Request, Sequence * Candigure authonication method: act Administration > Sequences Configure authonication methods act Administration > Sequences Configure authonication methods act Administration > Sequences Configure authonication methods act Advantable Configure authonication Configure Config	lacklist BYOD Certificate Provisioning Client Provisioning Mobile Device Mar	nagement My Devices Custom Portal Files + Settings	
Cher account with Super admin privilege of DRS admin privilege will have access to the portal  Available  ADDNS:DLIPDR/Microsoft Exchange Securit AL_ACCOUNTS (default)  ADDNS:DLIPDR/Microsoft Exchange Securit ADDNS:DLIPDR/Microsoft Exchange Secu	Administration > System > Certificates System Certificates Authentication method: * Certificate_Request_Sequence * Configure authentocate methods at Administration > Identity Manual Identity Source Sequences		Suco
AL_ACCOUNTS (default) ADDNS:0LIPPQ/Microsoft Exchange Securit ADDNS:0LIPPQ/Microsoft Exchange Securit ADDNS:0LIPPQ/Microsoft Partial Server Lio GROUP.ACCOUNTS (default)	User account with Super admin privilege or ER Available		
ADDNS:DLIPDR/Builtin/IIIS_JUSRS ADDNS:DLIPDR/Builtin/IIIS_JUSRS ADDNS:DLIPDR/Builtin/RDNS Authorizat ADDNS:DLIPDR/Builtin/RDNS Remote Access		ALL_ACCOUNTS (default) ADDMS:DLIPDR/Merser/Bornane Securit ADDMS:DLIPDR/Merser/Bornane Controllers ADDMS:DLIPDR/Users/Domain Controllers ADDMS:DLIPDR/Users/Domain Controllers ADDMS:DLIPDR/Users/Semperis Audit Colle ADDMS:DLIPDR/Users/Semperis Audit Colle ADDMS:DLIPDR/Users/Semperis Audit Colle ADDMS:DLIPDR/Users/Semperis Audit Colle ADDMS:DLIPDR/Users/Demied RODC Passw ADDMS:DLIPDR/Users/Demied RODC Passw	ş
Clear all      Fully qualified domain name (FQDN)		× Clear all	

6. Click Save.

### 2.11.10 Configuring RADIUS with your Network Device

Cisco ISE requires a Remote Authentication Dial-In User Service (RADIUS) session for posture to function. Posture refers to ISE's ability to check that a machine complies with a specified policy, which may be based on the OS and may contain requirements such as the installation of certain security applications or the presence of configuration files. Machines that are not in compliance can be kept separated from the network. The process for setting this up varies widely between machines, but the overall requirements have commonalities between systems.

- 1. The Network Device (i.e. the router or switch) must support RADIUS functions, specifically Authentication, Authorization, and Accounting. Furthermore, it must also support CoA, which is Change of Authorization.
  - a. To configure this, you must configure your network device to use Cisco ISE as a Radius Server. What this means is that your network device will forward authentication requests to Cisco ISE, and Cisco ISE will respond with an "accept" or "reject."
- The Network Device must support some form of 802.1x. Note that this is not supported on certain routers, even if RADIUS is supported. 802.1x is a mechanism for authenticating the end workstation to the network device, potentially over wireless or through ethernet.
  - a. This can take various forms, such as a captive web portal, Media Access Control (MAC) address authentication, or user authentication. A captive web portal, if the device supports it, may be ideal for configuration without the correct hardware.

- b. There are also many switches that provide direct 802.1x username/password authentication. Note that if you choose to use this mechanism, a client is still required, and it will not be in the web browser. Windows has a built-in 802.1x client that can be configured on Network adapters under the Authentication tab. To enable it, you must first start the service Wired AutoConfig, and then the Authentication tab will become available for configuration.
- c. Whichever form of **802.1x** is chosen, the request for authentication must be forwarded to Cisco ISE. Cisco ISE will process the request for authentication.
- 3. The two steps above detail the **authentication** phase. Once authenticated, the network device must redirect the user to the client provisioning portal (or to a guest portal), depending on the setup. The URL for this can be acquired from the active **Authorization Profile** in ISE.
- 4. The user will then authenticate to the **Guest Portal** or **Client Provisioning Portal** (depending on your setup). The portal will prompt the user to download an executable, which will run posture.
- 5. The executable will *first* check for the existence of a RADIUS session in Cisco ISE for the user who downloaded the executable. It will primarily check the MAC address that visited the ISE web portal against the MAC addresses of existing sessions. *If and only if a session exists,* it will run posture based on the policy you set up. You can verify that a session exists by navigating to **Operations > RADIUS > Live Sessions.**

## 2.11.11 Configuring an Authentication Policy

- 1. Navigate to **Policy > Policy Elements > Results > Authentication > Allowed Protocols.**
- 2. Select the **Default Network Access** protocol, or create your own.
- 3. Ensure any protocols that need to be supported for your network setup are allowed. In particular, if using **802.1x**, you should likely check the box next to **Allow MS-CHAPv2**.

dentity Services Engine	Home > Co	ontext Visibility	Operations	* Policy	Administration	Work Centers		License Warning 🛕	Q.	
Policy Sets Profiling Posture C	Client Provisioning	▼ Policy Elements					Click have to do wirely	ess setup and visibility si	atus Do	ant et
Dictionaries + Conditions + Resul	Its						CICK INTE ID GO MIER	cas actup and nationly a	sup ou	
0		ols Services List > D	efault Network	Access						
Authentication	Allowed Pro									
Authorization	Name	Default Network A	coess							
Profiling	Description	Default Allowed Pr	otocol Service							
Posture	<ul> <li>Allowed Pr</li> </ul>	otocols			4					
Client Provisioning	Auth	entication Bypass								
		Process Host Looku	p (I)							
	Auth	entication Protocol	Is							
		Allow PAP/ASCII								
		Allow CHAP								
	•	Allow MS-CHAPv1			R					
		Allow MS-CHAPv2								
	<b>V</b>	Allow EAP-MD5								
	- 🗹	Allow EAP-TLS								
		Allow Authent	tication of expired	l certificates	to allow certificate ren	ewal in Authorization	n Policy ④			
		Enable State	less Session Res	ume						

- 4. Click Save.
- 5. Navigate to **Policy > Policy Sets.**
- 6. Select the default policy.
- 7. Ensure that the **Allowed Protocol** selection matches the allowed protocol you just created/edited.
- 8. Expand the **Authentication Policy** section, and select the ID stores from which to authenticate users. For example, if you set up an Active Directory integration, it may be desirable to authenticate users from there.

Identity Services Engine	B Home D Context Visit	iity > Operations -	Policy Administration	Work Centers	•	License Warning 🔺	
Policy Sets Profiling Posture	Client Provisioning   Policy	Elements		Clic	k here to do wirek	ess setup and visibility setup	Do not
Policy Sets → Default							R
Status Policy Set Na	ame Descriptio	n Cor	nditions			Allowed Protocols / Ser	ver Se
Search							
O Default	Default polic	y set				Default Network Access	: a <b>r</b>
Authentication Policy (1)     H Status Rule Name	Condition	15			Use		
Search							
			+				
/ 🕢 Default					AD-DNS		*
					> Optio	ns	
Authorization Policy - Local	Exceptions						
Authorization Ballay, Local	Exceptions				> Optio	ns	

9. Click Save.

# 2.11.12 Configuring an Authorization Policy

- The Authorization Profile is likely dependent on your network device, but it is possible that the Cisco\_Temporal\_Onboard profile will work even for non-Cisco devices. You can edit the authorization policy by navigating to Policy > Policy Elements > Results > Authorization > Authorization Profiles.
- 2. The temporal onboard profile will attempt to redirect the user to a client provisioning portalthis redirection will most likely only happen automatically on compatible Cisco network devices. If another device is used, the device may need to manually redirect the user to the client provisioning portal after authentication. (We accomplished this in PFSense for our build using a "Post-authentication redirection" feature in the Captive Portal.)
- 3. Once you are finished configuring the **Authorization Profile**, navigate to **Policy > Policy Sets**.
- 4. Select the default policy.
- 5. Expand the Authorization Policy section.
- Note that you can configure this for as many groups and conditions as desired, potentially specifying different authorization profiles for various user groups or levels of authentication, including unauthenticated access. Under **Results > Profiles**, you can select the authorization profiles you configured.

Policy Sets         Profiling         Posture         Client Provisioning         Policy Elements           Authentication Policy (1)         Authorization Policy - Local Exceptions         Authorization Policy - Global Exceptions           Authorization Policy - Global Exceptions         Authorization Policy (2)         Authorization Policy (2)	Clic	ck here to do wireless setup	and visibility setup Dr	o not
Authorization Policy - Local Exceptions     Authorization Policy - Global Exceptions				
Authorization Policy - Global Exceptions				
✓ Authorization Policy (2)				
· · · · · · · · · · · · · · · · · · ·				
(+) Results				
Status Rule Name Conditions Profiles		Security Groups		
Search				
Basic_Authenticated_Access interview in the second interview interview in the second interview inter	hboard	+ Guests	** +	
Default     Visco_Temporal_O	Onboard	+ Unknown	× +	

7. Click Save.

# 2.12 Cisco Advanced Malware Protection

This section assumes the use of the Cisco Advanced Malware Protection (AMP) Console, a cloud-based server that connects to clients on individual machines. There is some configuration to be done on this cloud-based server, which may impact the installation. Cisco provides best practices guides online for AMP configuration. Here is a link to one such guide:

https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/213681-best-practices-foramp-for-endpoint-excl.html.

# 2.12.1 Dashboard Configuration

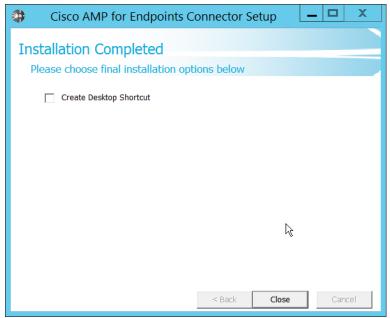
- 1. From the Cisco AMP dashboard, located at <u>https://console.amp.cisco.com/dashboard</u>, click **Set Up Windows Connector.**
- 2. The configuration of this will be different for each enterprise, so consult your Cisco representative for the proper way to set this up. For the purposes of this build, we accepted the default values.

# 2.12.2 Installing the Connector on a Windows Server

- 1. On the Cisco AMP dashboard, navigate to Management > Download Connector.
- 2. Select the AMP group in which to put the machine. For example, when installing on an Active Directory machine, we chose **Domain Controller.**

- 3. Find the correct OS version of the installer, and click **Download.**
- 4. Run the downloaded executable (for example, Domain\_Controller\_FireAMPSetup.exe).

	🗱 Cisco AMP for Endpoints Connector Setup 📘 🗖 👗
	Choose Install Location
	Choose the folder in which to install Cisco AMP for Endpoints Connector.
	Setup will install Cisco AMP for Endpoints Connector in the following folder. To install in a different folder, dick Browse and select another folder. Click Install to start the installation.
	Destination Folder C \Program Files\Cisco\AMP Browse
	Space required: 105 MB Space available: 64 GB
	By dicking 'Install' below, you verify that you have read and Accept the Subscription Agreement
	et aller a freeze servit too veritt and too have read and Mechanic Topperbaat Hall content
	[Install] Cancel
ا 5. (	Click Install.
J. [	Cisco AMP for Endpoints Connector Setup
	Installation Complete
	Setup was completed successfully.
	Cisco AMP for Endpoints Connector has completed
	Show <u>d</u> etails
	Snow <u>d</u> etails
	R. C.
	< Back Cancel



7. Click Close.

# 2.12.3 Installing the Connector on a Windows 10 Machine

- 1. On the Cisco AMP dashboard, navigate to **Management > Download Connector.**
- 2. Select the AMP group in which to put the machine. For this installation we chose Protect.
- 3. Find the correct OS version of the installer, and click Download.
- 4. Run the downloaded executable (for example, Protect\_FireAMPSetup.exe).

Cisco AMP for Endpoints Connector Setup		×
Choose Install Location		
Choose the folder in which to install Cisco AMP for Endpoints Con	nector.	
Setup will install Cisco AMP for Endpoints Connector in the following folder. To ir different folder, click Browse and select another folder. Click Install to start the		
Destination Folder		
C:\Program Files\Cisco\AMP Browse		
Space required: 105 MB		
Space available: 3 GB		
By dicking 'Install' below, you verify that you have read and accept the Subscri	ption Agreer	<u>nent</u>
	Cano	el

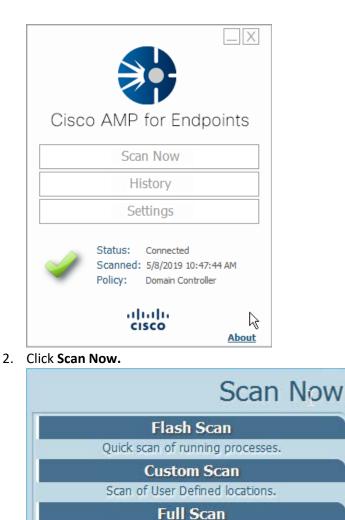
### 5. Click Install.

			_		
Cisco AMP for Endpoints Connector Setup	1				
Installation Complete					
Installation Complete					
Setup was completed successfully.					
Cisco AMP for Endpoints Connector has completed	1				
Show <u>d</u> etails					
			Γ	6	
			V	5	
	< <u>B</u> ack	Ne	xt >	Car	icel
Click Novt	< <u>B</u> ack	Ne	xt >	Car	icel
Click Next.		Ne	xt>		icel
Click Next.		Ne	xt >	Car	icel
Cisco AMP for Endpoints Connector Setup		Ne	xt >		ncel
Cisco AMP for Endpoints Connector Setup Installation Completed		Ne	xt >		icel
Cisco AMP for Endpoints Connector Setup		Ne	-		
Cisco AMP for Endpoints Connector Setup Installation Completed		Ne	xt >		
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options		Ne	-		
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options		Ne	-		icel (
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options		Ne	xt>		
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options		Ne	xt>		
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options			-		
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options	below		xt>		
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options	below		xt>		
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options	below		xt>		
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options	below		xt >		
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options	below		xt>		
Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options	below		xt>		

### 7. Click Close.

# 2.12.4 Scanning using AMP

1. If the AMP software does not run automatically, open it from the **start** menu.



This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-26.

- 3. Click Full Scan.
- 4. A scan should begin.

# 2.12.5 Configure AMP Policy

1. On the web console, navigate to Management > Policies.

Scan of entire computer. Rootkit Scan Scan system for running rootkits.

Cancel

Select a policy to edit; for this example, we choose Domain Controllers. (To edit which policies map to which groups, select Management > Groups, and click Edit on the group for which you wish to select a policy. You can select a policy for each Operating System (OS) in that group.)
 Policies
 O View All Changes

earch	Q		+ New Policy
All Products Windows Android	Mac Linux iOS		
Audit This policy puts the AM	/P for Endpoints Connector in a mode t	nat will only detect malicious files but not	quarantine them 😵 1 🛛 🖵 0
🕀 📲 Audit Mode Policy-This is for r	monitoring and visibility only. NO BLOC	KING This policy puts the AMP for Endpo	oints Connector in 🔮 1 🛛 🖵 0
🕀 📲 Blocking Policy. All detections	are set to BLOCK. This is the standard	policy for the AMP for Endpoints Connec	tor that will quara 曫 1 🛛 🖵 0
🖯 📲 Domain Controller This is a l	ightweight policy for use on Active Dire	tory Domain Controllers.	🚰 1 🛛 🖵 2
Modes and Engines	Exclusions	Proxy	Groups
Files Audit Network Disabled Malicious Activity Prote Disabled System Process Protection Protect	<ul> <li>Altiris by Symantec</li> <li>AVAST</li> <li>Avira</li> <li>Diebold Warsaw</li> </ul>	Not Configured	Domain Controller 📮 2
Outbreak Control			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
File Blacklist	Not Configured	Execution Blacklist Blocked File Whitelist Allowed	
O View Changes Modified 2019-	05-20 14:56:48 UTC Serial Number	54 🕹 Download XML	🕰 Duplicate 🕼 Edit 🗎 Delete
Protect This is the standard	policy for the AMP for Endpoints Conne	tor that will quarantine malicious files ar	nd block malicious 皆 1 🛛 🖵 0
🗄 📕 Server This is a lightweight p	policy for high availability computers an	d servers that require maximum perform	ance and uptime. 🏾 🚰 1 🛛 🖵 0
1 - 8 of 8 total records	25 ^ / page 🖌 1	of 1 🔿	

- 3. Click Edit.
- 4. In the **Modes and Engines** tab, "Conviction Modes" refers to the *response* taken to various detected suspicious activity or files.
  - Audit is a detection/logging approach that does not take any action other than logging the activity.
  - Quarantine involves the move of the offending file to its own folder, where it is monitored and deleted after a certain amount of time. Quarantining can also be applied to processes, in which the process is monitored and prevented from affecting system operations.
  - **Block** involves the deletion of the file or the stopping of the process or network traffic.
- 5. "Detection Engines" refer to the actual detection of the suspicious activity.
  - **TETRA** is intended to be an anti-malware engine and recommends that it not be used when other antimalware software is in use.
  - **Exploit Prevention** refers to an engine that defends endpoints against memory injection attacks.

Name	Domain Controller				
Description	This is a lightweight	policy for use o	n Active Directory	Domain Controllers.	li
Modes and Engines	Conviction I	Modes			Recommended Settings
Exclusions 20 exclusion sets	These settings con files and network a		or Endpoints respo	nds to suspicious	Workstation Files: Quarantine
Proxy	Files Quarantine	Audit			Network: Block Malicious Activity Protection: Quarantin System Process Protection: Protect
Outbreak Control	Network Block	Audit	Disabled		<b>Server</b> Files: Quarantine
Product Updates	Malicious Activity P	rotection			Network: Disabled Malicious Activity Protection: Disabled
Advanced Settings	Quarantine System Process Pro	Block	Audit	Disabled	System Process Protection: Disabled
	Protect	Audit	Disabled		
	Detection E	ngines			
	TETRA ()	•			
	Exploit Preventi	on U			
					L3
					Cancel Sav

6. Click Save.

# 2.13 Cisco Stealthwatch

This section will describe the setup and configuration of Cisco Stealthwatch, a network monitoring solution. This guide assumes the use of the Stealthwatch virtual machines.

# 2.13.1 Configure Stealthwatch Flow Collector, Stealthwatch Management Console, Stealthwatch UDP Director and Stealthwatch Flow Sensor

- 1. Log in to the console of Stealthwatch Flow UDP Director.
- 2. Navigate the menu to highlight Management and Select.

Select one:	System Configuration	
Tamagement Password TrustedHosts Advanced	Change the Management Port Network Change the password for the current user Change the Trusted Hosts Advanced Operations	
	(Select) < Exit >	

- 3. Press Enter.
- 4. Enter an IP Address for this machine.
- 5. Highlight OK.

192.168.1.55		
<mark>&lt; ОК &gt;</mark>	<cancel></cancel>	

- 6. Press Enter.
- 7. Enter a **network mask** for the IP Address.
- 8. Highlight OK.

Enter the FlowR	<mark>System Con</mark> eplicator Administr	nfiguration rative IP Netmask	
255.255.255.0			
	K OK >	<cancel></cancel>	

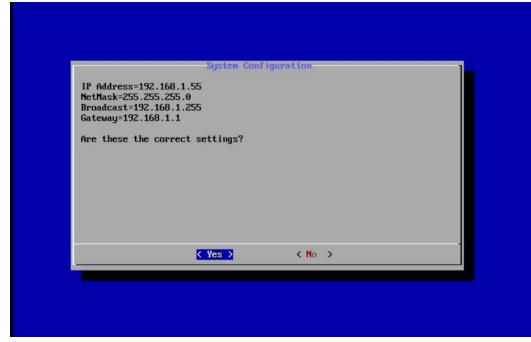
- 9. Press Enter.
- 10. Enter the network gateway.
- 11. Highlight OK.

Enter the Flow	<mark>System Co</mark> Replicator Administ	onfiguration trative IP Gateway Address	1
192.168.1.1_			
	< ок >	<cancel></cancel>	

- 12. Press Enter.
- 13. Enter the network broadcast address.
- 14. Highlight OK.

	en Configuration ministrative IP Broadcast Address	
192.168.1.255_		
<mark>&lt; ОК &gt;</mark>	<cancel></cancel>	

- 15. Press Enter.
- 16. Highlight Yes.



- 17. Press Enter.
- 18. Highlight OK.

	System Configuration ters have been modified. I for the primary network i	
etwork access to this	system which will require ll now be restarted to imp	console access to
	K OK >	

19. Press Enter.

20. Repeat steps 1-19 for each of the **Stealthwatch Management Console, Stealthwatch UDP Director, Stealthwatch Flow Sensor,** and **Stealthwatch Flow Collector.** 

# 2.13.2 Change Default Stealthwatch Console Passwords

1. In the System Configuration menu, highlight Password and Select.

Select one:	System Configur	ation	
Hanagement Password TrustedHosts Advanced	Change the passwo	ment Port Network ord for the current us ad Hosts ms	ser
	Select>	< Exit >	

- 2. Press Enter.
- 3. Enter the original password.

	System Configuration 1
Select one:	
Management Password Trustedilos Advanced	Change the password for the current user
	(Select) < Exit >
At the prompt type in your curr	ent password. Then type your new password at the next two prompts.
Changing password for sysadmin. (current) UNIX password:	

- 4. Press Enter.
- 5. Enter the new password, and confirm it.

Rassword       Change the password for the current user         TrustedHosts       Change the Trusted Hosts         Advanced       Advanced Operations	Sele	System Configuration ct one: Management Change the Management Port Network
<pre>     Select&gt; &lt; Exit &gt; </pre>		Password Change the password for the current user TrustedHosts Change the Trusted Hosts
		<pre></pre>
	nnging password urrent) UNIX pa u password: type new passwo	

- 6. Press Enter.
- 7. In the System Configuration menu, highlight Advanced and Select.
- 8. Press Enter.
- 9. Highlight RootShell and Select.



- 10. Press Enter.
- 11. Log in using the original root shell password.



12. Enter the command root.

### 13. Type the new password, and confirm it.

Type the root password at the prompt to open a root shell.

Password: smc-01:<sup>°</sup># passwd root New password: Retype new password: passwd: password updated successfully smc-01:<sup>°°</sup>#

### 14. Press Enter.

15. Repeat steps 1-14 for each console.

# 2.13.3 Configure the Stealthwatch Management Console Web Interface

1. Change the default password by filling in the fields for **Current Password, New Password,** and **Confirm New Password.** 

Step 1: Change Default Password	Change Default	Passwords		
Step 2: Management Network Interface	Password Format (Ca	use Sensitive) 8 and 30 characters.		
Step 3: Host Name and Domains		from the previous password by at least	4 characters.	
Step 4: DNS Settings	Note: You must cha	ange the password for all th © ADMIN	e users before cor	tinuing.
Step 5: NTP Settings	Current Password:		Required	
Review: Review Your Settings	New Password:		Required	
	Confirm New Password:			

### 2. Click Next.

3. Fill in the fields for **IP Address, Subnet Mask, Default Gateway** and **Broadcast Address** according to your network topology.

Step 1: Change Default Password	Management N	etwork Inte	rface	
Step 2: Management Network Interface			I the network. Default network er with your network administra	settings for this appliance appear ator.
Step 3: Host Name and Domains			ne, or network domain name, If ficate, save the certificate and ;	ne appliance identity certificate is private key before you change
Step 4: DNS Settings	Interface Name:	eth0	Interface MAC Address:	00:50:56:b2:64:52
Step 5: NTP Settings		IPv4		IPv6
Review: Review Your Settings	IP Address:			
	Subnet Mask:			
	Default Gateway:			
	Broadcast Address:			

- 4. Click Next.
- 5. Enter a host name.
- 6. Enter the network domain that Stealthwatch is in for Network Domain.
- 7. Enter the network domain that Stealthwatch will be monitoring for **Stealthwatch Domain**.

Build: 2018.12.12.1645-0			
Step 1: Change Default Password	Host Name and	Domains	
Step 2: Management Network Interface			where it is installed.
Step 3: Host Name and Domains		our IP address, host name, or network domair you have a custom certificate, save the certifi ose data.	
Step 4: DNS Settings	Host Name:	smc-01	
Step 5: NTP Settings	Network Domain:	di, ipdr	
Review:	Identify your organization's	domain and the IP addresses that Stealthwa	tch will be monitoring.
Review Your Settings	Stealthwatch Domain:	di.ipdr	
	IP Address Ranges:	10.0.0.0/8 192.168.0.0/16	
	Here Back	172.16.0.0/12 fc00::/7	Next →
			le .

#### 9. Enter a DNS Server.

Step 1: Change Default Password	DNS Set	tings	
Step 2: Management Network Interface		address(es) of your domain name server(s). To inding checkbox, and then click the - button.	add a server, click the + button. To delete a server, select
Step 3: Host Name and Domains	Delete	DNS Server 192.168.1.12	
Step 4: DNS Settings			
Step 5: NTP Settings			
Review: Review Your Settings			
			• •
	+ Back		Next →

### 10. Click Next.

11. Configure the Network Time Protocol (NTP) server according to your network topology.

Step 1: Change Default Password	N	TP Set	tings	
Step 2: Management Network Interface				col server(s). Choose the same NTP h FlowCollector for NetFlow. To add a ser , and then click the - button.
Step 3: Host Name and Domains		Delete	NTP Server	
Step 4: DNS Settings		-		
Step 5: NTP Settings				
Review: Review Your Settings				
		<b>H</b> Back		Next 🔿

- 12. Click Next.
- 13. Select Restart.

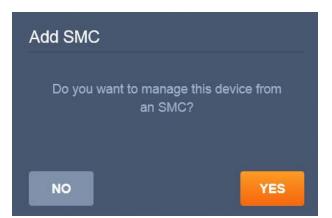
<b>1</b>	Step 1. Change Default Password	R	teview Your S	Settings			
	Step 2 Management Network Interlace		Management Networ	k Interface	Host Name and Doma	ains	• Kon
	Step 3: Host Name and Domaina		Name: MAC Address: IP Address: Subnet Masic Default Gateway: Broadcast Address: IPv6 Address:	eth0 00.50:56.b2.64.52 192.168.1.52 255.255.255.0 192.168.1.1 192.168.1.255	Hont Name: Network Domain:	amc-01 dilipdr	
3	Step 4 DNS Settings		IPv6 Address: IPv6 Prefix Length: IPv6 Gateway:				
	Step 5		DNS Settings		NTP Settings		*(Edi)
	NTP Settings					10 97 74 8	
~	Review. Review Your Settings				Finalize	• Restart	Shut Do
			<b>←</b> Васк			Apply -	2

# <text><text><text><text><text><text>

15. After the restart, click Next.

# 2.13.4 Configure the Stealthwatch UDP Director, Stealthwatch Flow Collector and Stealthwatch Flow Sensor Web Interfaces

1. Repeat steps 1-12 from Configure the Stealthwatch Management Console Web Interface.



- 2. When prompted to manage this device from an SMC, click Yes.
- 3. Enter the IP Address of the Stealthwatch Management Console.

🥦 Step 1:	Central Management Settings
Change Default Password	Central Management Settings
Step 2: Management Network Interface	
	Note: By default, this will be the IP address of your SMC. If you have SMCs in a failover pair, enter the IP address of your primary SMC. Also, your security events will be sent to the SMC you enter here.
Step 3: Host Name and Domains	IP Address
Step 4:	
Step 4: DNS Settings	The second se
Step 5:	
NTP Settings	
Step 6: Central Management	
Complete	

- 4. Click Save.
- 5. Verify the certificate.

### Add Trust Certificate

We found an SMC Trust Certificate named:

SHA-256 Fingerprint=D0:FE:04:CB:95:4E:E8: 89:B9:0B:A6:F0:48:78:E5:CF:3E:DB:AA:B1:8 2:BB:A7:9F:0C:ED:69:DC:E0:E8:9A:88

**Do you trust this certificate?** A trusted certificate is required to communicate with the SMC and complete setup



- 6. Click Yes.
- 7. Enter the User ID and Password for the Stealthwatch Management Console.

Please enter your administration credentials below.	
In order to be added for management you your SMC administration credentials below	
User ID:	
Password:	
Cancel	Next →

- 8. Click Next.
- 9. Repeat steps 1-8 for the Flow Collector *first* and *then* for the Flow Sensor. The Flow Sensor cannot be added to the Management Console until after the Flow Collector is successfully added.

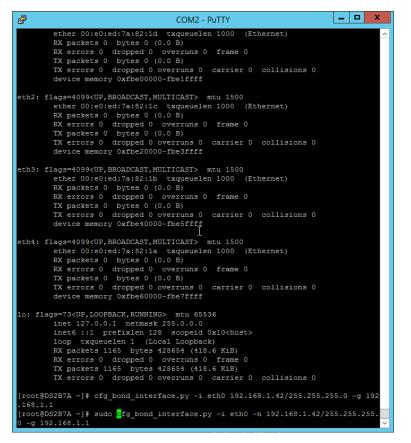
# 2.14 Symantec Analytics

This section details the installation and configuration of Symantec Analytics, a network analysis tool. This guide assumes that Symantec Analytics is connected via serial to a terminal.

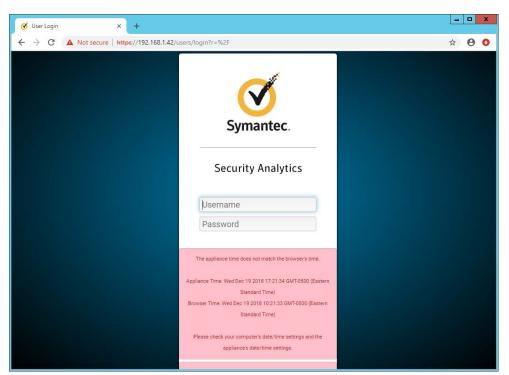
# 2.14.1 Initial Setup

- 1. Log in to the Symantec Analytics command line.
- 2. Enter the following command to configure the IP for the interface:

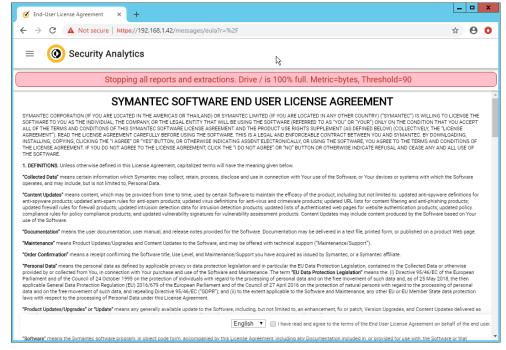
sudo cfg\_bond\_interface.py -i eth0 -n 192.168.1.42/255.255.255.0 -g 192.168.1.1



### 3. Navigate to the IP you assigned in a browser.



- 4. Enter the username and password to log in. The default is (Admin/Solera).
- 5. Check the box next to I have read and agreed to the terms of the End User License Agreement on behalf of the end user.



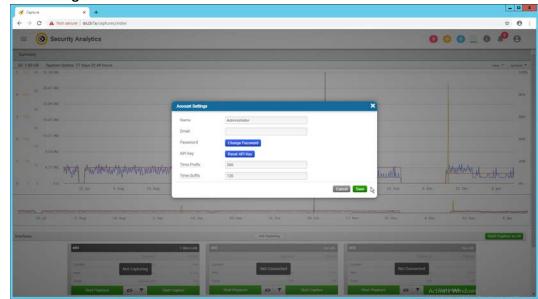
- 6. Click Next.
- 7. Enter the license key.
- 8. If you do not have internet connectivity, follow the instructions under **Upload License File.** Otherwise, click **Send Request.**

🧭 System Message 🛛 🗙	+	-	
← → C ▲ Not secure http	ps://192.168.1.42/messages/control_center#LicenseDialog	☆	00
😑 🔞 Security Analy	ytics 🕒 🕒 🖢 🔔 🖲	<b>P</b> (	9
Change	License Details		
Stopp	Retrieve License		
	This appliance is not licensed. Please license it below.		
	Use this section if your appliance has access to the internet. Type your license key in the space provided and		
	click Update. After the license is retrieved, the appliance will be rebooted automatically.		
	License Key Send Request		
	Upload License File		
	Use this section if your appliance does not have access to the Internet. Click <b>Download DS Seed</b> and save dsseed tgz to your workstation. Go to <i>license soleranetworks.com</i> and follow the instructions. Return to this		
	page, click Browse to retrieve license.tgz, and then click Update. After the license is uploaded, the appliance will		
	be rebooted automatically. Download DS Seed		
	License File Browse		
	Seventeer ne Liumote		
	Update		

- 9. Click **Update.** The device will reboot.
- 10. Log in to the web page again.
- 11. Click the silhouette in the top right corner and click **Account Settings.**

E 💽 Sec	urity Analytics										◎ ◎ _	Account Ser	tingi 1
E 1 00 GB System	Uptime: 27 days 22-4	Phours										Risk and Vir Encoder/De Log Out	
53 28.61 Mb													
23.84 Mb 40 18.07 Mb													
30 14.31 Mb											-		
20											1		
9.54 Mb		philosoft physionell	M.WWWW	World Wo	www.texp.Duv	or Malicany Summary Street	ndrada jinaduan	MW/WUUU	Mumhu		MAMMAN	rther	ł
9,54 Mb	My Awal	s has	19 Aug	2. Srp	MMMMM UM	20.540 14.000 MALANNARANALAN	28 Oct	MW/W ULU	MuuMu 25. Nov	9. Dec	25 Dec	rthr 1910	H
9.54.96 10 4.77.96 1 5 0.0	My MWM	terliter the property of the second	19 Aug	2. Sep	and the Day	and the second for		11. Nov	25, Nov	5 Dec	I IM		H
9.54.96 10 4.77.96	My MWM	M JW MMW 5. Aug 19. Aug	19. Aug 2. Sep	2. Sep 14. Sep	and the Day	and the second for			25, Nov	S Dec 9. Dec	I IM	14. 5 jan 6 jan	H
9.54 Mb 52 17 4.77 Mb 1 5 0 b 22 Jd	MAN HWM				16.5ep	30. Sep 14. Der	28 Oct	11. Nov	25. Nov		21. Dec		H
9.54 Mb 52 17 4.77 Mb 1 5 0 0 22.34	MAN HWM		2. Sag	16. Sep TGN/LINK	16.5ep	30.54p K. Oct M. Oct Mr. Capturing	28. Oct.	11. Nov	25. Nov	9. Čet	23. Dec 23. Dec 23. Dec		H
9.54 Mb 50 10 4.77 Mb 1 5 0.0 22. Jul	5. Aug			16. Sep	16. Sep 10. Sep	33.5ep 14.0ct M. Oct Mat Ceptong Captroni	28 Oct	11. Yev 11. Yev	25. Nov 25. Nov 25. Nov	9. Det	23. Dec 23. Dec 23. Oec		
9.54 MD 50 10 4.77 MD	5. Aug 8. Aug		3. Say	16. Sep 1 Gb/s Link Three	16.5ep	30.54p K. Oct M. Oct Mr. Capturing	28. Oct.	11. Nov 11. Nov	25. Nov 25. Nov 25. Nov	9. Čet	23. Dec 23. Dec 23. Dec		

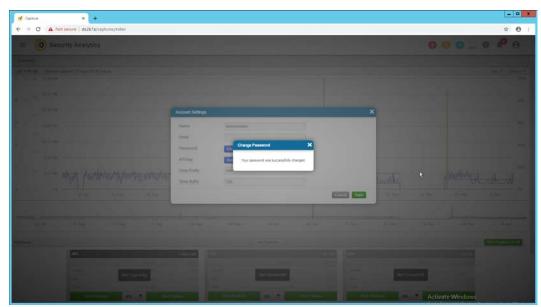
### 12. Click Change Password.



13. Enter a new password. Click Save.

Security Analytics Security Analytics Securi	• × +			- 0
Distance	C A Not secure   ds2b7a/captures/index			<b>☆ 0</b>
Al 1002 Refer Libror 27 Sep 27 Shors on one of 100 M Sep 10 Sep 27 Shors on one of 100 M Sep 10 Sep 27 Shors on one of 100 M Sep 10 Sep 27 Shors on one of 100 M Sep 10 Sep 27 Shors on one of 100 M Sep 10 Sep 27 Shors on one of 100 M Sep 10 Sep 20	Security Analytics		0	00_00
				Unit * Accord
	21.01.10			
I REF THE I RE		Account Settings	×	
I E I M <sup>2</sup> S S M <sup>2</sup> S S M <sup>2</sup> S S M <sup>2</sup> S M <sup></sup>		Current Password	De .	
	Contraction of the second s			
				1
22. pl         5. kmj         15. kmj         15. kmj         23. pl         5. kmj         5. km	and the family and the mail of the second		Luchhe	photomythat
22 ja S. Ang S. Ang S. Sang S.		Canol Sav	15 bus B Dec.	Zi Der & Jan
22 / 2 3 Aug 15 Aug 15 Aug 16 Aug 18 Aug 18 Aug 16 Aug 18 Aug 16 Aug 18				
et Touria de Sula de Sula de Sula	in pa to have the host of the second se	14 Nap 10 Nap 14 Or 28 OF 11 Nam	n na i Dec	23 Dat 6 jar
et Touris de suis de s				
Not Cast And	ant .			
Not Casturing Connected Not Connected Not Connected		The Party of State		and a second sec
	Not Capturing	Not Connected	No: Connected	
Ten				

14. The screen should reflect that the password has been changed. Close out of both windows and return to the main web console.



15. In the top left corner of the web console, click the menu button. (It shows as three horizontal bars).

🕑 Aler	ts	× +	_ <b>_</b> X
$\leftrightarrow$ $\rightarrow$	C A Not secure	https://192.168.1.42	☆ 🖯 🔾
6	Capture	lytics 🛛 🔍 🔍 🗖	<b>P</b> 0
	Statistics	bing all reports and extractions. Drive / is 100% full. Metric=bytes, Threshold=90	
\$	Settings	Little data in the second state	
	<ul> <li>Authentication</li> </ul>		
	• Central Management	)	
	Communication		
	• Data Enrichment		
	• Date/Time		
	Geolocation		
	• Metadata	There are no alerts to display.	
	• Network		
	· Security	Set Up Rules for Alerts Go to Summary Page	
	• System		
	• Upgrade		
4	• Users and Groups	• Activate Wind	ows

16. Navigate to **Settings > Data Enrichment.** 

$- \rightarrow C$ A Not s	secure https://	192.168.1.42/integration_providers/index	A 0
= 🔞 Secur	ity Analytic	cs 0 0 📃 🛈	<b>P</b> 0
		all reports and extractions. Drive / is 100% full. Metric=bytes, Threshold=90	
Data Enrichment			
Symantec Intelligence Services	;		
Name	Licensed	Data Enrichment Filters	Actions
Symantec Web Reputation Service	Yes	-118-	<b>↔ 0</b>
Symantec File Reputation Servi	ce Yes	Archives, Binarles, Debian Packages, Office Documents, Programs and Librarles, JAR Archives, Adobe PDF	<b>♀</b> <b>/ → 0</b>
Data Enrichment Profiles			
	), analysis, and data e	enrichment to enable and then click 'Save'.	
Select the amount of indexing Profile	), analysis, and data (		
Select the amount of indexing Profile	), analysis, and data e		Actions
Select the amount of indexing Profile Symantec Analysis Providers	g, analysis, and data <del>(</del>	Full Data Enrichment (No Anomaly Detection) •	Actions
Select the amount of indexing Profile Symantec Analysis Providers Name ICAP	), analysis, and data 4	Full Data Enrichment (No Anomaly Detection)   Data Enrichment Filters	
Select the amount of indexing Profile Symantec Analysis Providers Name ICAP Malware Analysis Appliance	4. 14 Set	Full Data Enrichment (No Anomaly Detection)  Data Enrichment Filters Default filters	<b>♀ / 0</b>
Select the amount of indexing Profile Symantec Analysis Providers Name	4. 14 Set	Full Data Enrichment (No Anomaly Detection)  Data Enrichment Filters Default filters	<b>♀ / 0</b>

17. Click the red upside-down power symbols next to **Symantec Web Reputation Service** and **Symantec File Reputation Service** to turn them on.

~			
🗏 🔘 Securi	ity Analytic	cs 0 0 0 📃	0 4 0
	Stopping	all reports and extractions. Drive / is 100% full. Metric=bytes, Threshold=90	
Data Enrichment			
Symantec Intelligence Services			
Name	Licensed	Data Enrichment Filters	Actions
Symantec Web Reputation Service	Yes	-na-	0+0
			ڻ ٺ
Symantec File Rep <mark>utation Servic</mark>	e Yes	Archives, Binaries, Debian Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDF	/ + 0
Data Enrichment Profiles			/*0
Data Enrichment Profiles		Archives, Binaries, Debian Packages, Office Documents, Programs and Ubraries, JAR Archives, Adobe PDP enrichment to enable and then click Save.	/ → 0
Data Enrichment Profiles Select the amount of indexing,		enrichment to enable and then click Save.	/*0
Data Enrichment Profiles Select the amount of indexing, Profile		enrichment to enable and then click Save.	∕ ★ O Actions
Data Enrichment Profiles Select the amount of indexing, Profile Symantec Analysis Providers		enrichment to enable and then click Save. Full Data Enrichment with Anomaly Detection. •	
Data Enrichment Profiles Select the amount of indexing, <u>Profile</u> Symantec Analysis Providers Name		enrichment to enable and then click 'Save'. Full Data Enrichment with Anomaly Detection.   Data Enrichment Filters.	Actions
Data Enrichment Profiles Select the amount of indexing, Profile Symantec Analysis Providers Name ICAP	analysis, and data (	enrichment to enable and then click 'Save'. Full Data Enrichment with Anomaly Detection   Data Enrichment Filters Default filters	Actions $\phi  e 3$
Data Errichment Profiles Select the amount of indexing, Profile Symantec Analysis Providers Name ICAP Malware Analysis Appliance	analysis, and data (	enrichment to enable and then click 'Save'. Full Data Enrichment with Anomaly Detection   Data Enrichment Filters Default filters	Actions $\phi  e 3$

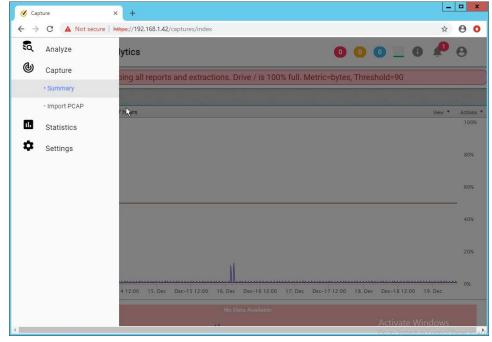
18. Select Full Data Enrichment (with Anomaly Protection) for the profile under Data Enrichment Profiles.

	192.168.1.42/integration_providers/index	щ
	os 🛛 🔍 🔍 🚺 🚺	<b>P</b> (
Stopping	all reports and extractions. Drive / is 100% full. Metric=bytes, Threshold=90	
<ul> <li>Office Documents</li> </ul>	Programs and Libraries	
Login Correlation Service		
Login Correlation Service Download Version 1.1.2 of the Login Correlation Se	rrvice Installation File	
Web Reputation Service		
Web Reputation Service Version	Web Reputation Service has never been updated.	
Initiate Web Reputation Service Update	Update	
Update Interval in Seconds	300	
Enable Custom Update Location		
YARA File Manager		
YARA File Manager Download the current YARA file	Download	
	Download Upload	

19. Click Save.

# 2.14.2 Capturing Data

1. Navigate to **Capture > Summary** in the menu.



2. Begin capturing data on any desired interfaces by clicking Start Capture.

≡ (	💿 Security Analy	tics			000	0 🔑 🤅
	Stoppi	ng all reports and extra	actions. Drive / is 1	00% full. Metric	=bytes, Threshold=90	0
			No Data Availabl	E		
14	. Dec Dec-14 12:00 1	5. Dec Dec-15 12:00 1	6. Dec Dec-16 12:00	17. Dec Dec-1	7 12:00 18. Dec Dec	:-18 12:00 19. Dec
faces			Not Capturing			Start Capture on A
	eth1		No Link eth2	_		No Link
		Captured	Filtered		Captured	Filtered
	Current	Not Connected	Curr	ent	Not Connected	
			0 b/s Max		(8	0 b/s
	Max	/s				
	Total	OB	0 B Tota		0 B	0 B
						0 B
	Total		0 B Tota			0 B
	Total Start Playback		0 B Tota			0 B Capture
	Total Start Playback	💋 Y Start C	0 B Tota Capture No Link eth4	Start Playback	💋 Y Start	0 B Capture No Link

# 2.15 Symantec Information Centric Analytics

This section describes the installation and configuration of Symantec Information Centric Analytics (ICA).

# 2.15.1 Installing MS SQL 2017

1. Launch the SQL Setup Wizard.



### 2. Click Installation.

5	SQL Server Installation Center	x
Planning Installation	New SQL Server stand-alone installation or add features to an existing installation Launch a wizard to install SQL Server 2017 in a non-clustered environment or to add features to an existing SQL Server 2017 instance.	1
Maintenance Tools Resources	Install SQL Server Reporting Services Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.	
Advanced Options	Install SQL Server Management Tools     Launch a download page that provides a link to install SQL Server Management     Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell     provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is     required to install these tools.	
	Install SQL Server Data Tools Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.	
	New SQL Server failover cluster installation Launch a wizard to install a single-node SQL Server 2017 failover cluster.	
	Add node to a SQL Server failover cluster Launch a wizard to add a node to an existing SQL Server 2017 failover cluster.	
	Upgrade from a previous version of SQL Server Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2017.	
Microsoft SQL Server 2017	New Machine Learning Server (Standalone) installation Launch a wizard to install Machine Learning Server (Standalone) on a Windows machine. This is twoically used by data scientists as a standalone analysis server or as a	

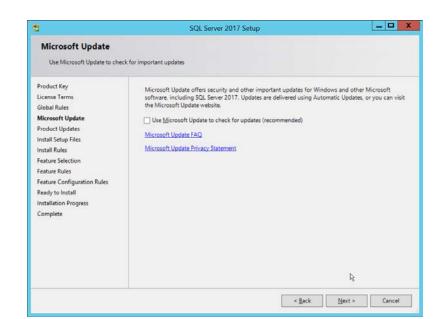
- 3. Click New SQL Server stand-alone installation or add features to an existing installation.
- 4. Enter a product key.

5	SQL Server 2017 Setup	
Product Key Specify the edition of SQL Se Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Setup Files Install Rules Feature Selection Feature Rules Feature Configuration Rules Peadure Lot		Le Microsoft certificate dition of SQL Server. Developer, features, as documented in SQL Server r edition does not have an expiration, non-production database application
Ready to Install Installation Progress Complete	< Bac	:k Next > Cancel

### 6. Check the box next to I accept the license terms.

To install SQL Server 2017,	you must accept the Microsoft Software License Terms.			
Product Key <b>License Terms</b> Global Rules Microsoft Update Product Updates Install Sclup Files Install Rules Feature Releation Feature Rules Feature Configuration Rules Ready to Install Installation Progress Complete	MICROSOFT SOFTWARE LICENSE TERMS MICROSOFT SQL SERVER 2017 ENTERPRISE These license terms are an agreement between Microsoft Corpor you live, one of its affiliates) and you. Please read them. They app above, which includes the media on which you received it, if any, any Microsoft • updates. • updates. • supplements. • Internet-based services, and ✓ I accept the licefse terms. SQL Server 2017 transmits information about your installation experience, <i>i</i> , performance data, to Microsoft to help improve the product. To learn more processing and privacy controls, please see the <u>Privacy Statement</u> .	ly to the soft The terms als as well as other	ware name o apply to <u>Copy</u> usage and	ed Prir

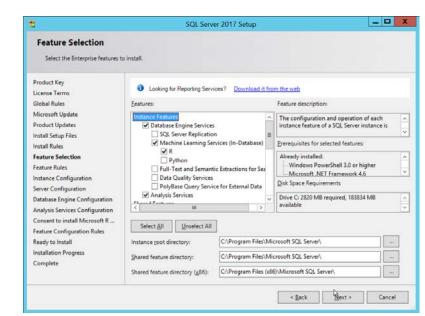
### 7. Click Next.



5	SQL Server 2017 Setup	
Install Rules Setup rules identify potential can continue.	problems that might occur while running Setup. Failures must b	e corrected before Setup
Product Key License Terms Global Rules Microsoft Update Product Updates	Operation completed. Passed: 3. Failed 0. Warning 1. Skip Hide details_<< <u>View detailed report</u>	ped 0. <u>B</u> e-run
Install Setup Files Install Rules Feature Selection Feature Configuration Rules Ready to Install Installation Progress Complete	Rule       Image: Second S	Status Passed Passed Passed Warning
		R < Back Next > Cancel

### 9. Click Next.

10. Ensure that box next to **R** and the box next to **Analysis Services** is checked.



- 11. Click Next.
- 12. Select Named instance.
- 13. Specify a name for the instance.

3		SQL Server 201	, betap		
Instance Configuratio		SQL Server. Instance	ID becomes part of 1	the installation path.	
Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Feature Selection Feature Rules Instance Configuration Severe Configuration	<u>D</u> efault instance     Named instance	ICA			
	Instance [D:	ICA			
	SQL Server directory: C\Program Files\Microsoft SQL Server\MSSQL14.ICA Analysis Services directory: C\Program Files\Microsoft SQL Server\MSAS14.ICA Installed instances:				
Database Engine Configuration	Instance Name	Instance ID	Features	Edition	Version
Analysis Services Configuration Consent to install Microsoft R Feature Configuration Rules Ready to Install Installation Progress Complete					
				< <u>B</u> ack <u>N</u> ex	t> Cancel

1	SQL Server 2	2017 Setup			
Server Configuration					
Specify the service accounts an	d collation configuration.				
Product Key	Service Accounts Collation				
License Terms Global Rules	Microsoft recommends that you	use a separate account for each	SQL Server serv	ice.	
Microsoft Update	Service	Account Name	Password	Startup Type	
Product Updates	SQL Server Agent	NT Service\SQLAgentSICA		Manual	¥
Install Setup Files	SQL Server Database Engine	NT Service\MSSQLSICA		Automatic	-
Install Rules	SQL Server Analysis Services	NT Service\MSOLAPSICA		Automatic	Y
Feature Selection Feature Rules Instance Configuration Database Engine Configuration Analysis Services Configuration Consent to install Microsoft R Feature Configuration Rules Ready to Install Installation Progress Complete	SQL Server Launchpad	NT Service\MSSQLLaun		Automatic	
	SQL Server Browser	NT AUTHORITY\LOCAL		Automatic	Y
	This privilege enables instant	nance Task privilege to SQL Sen file initialization by avoiding zerr llowing deleted content to be ac llowing deleted content to be ac	oing of data pag	-	I
		< Bac	k Nex	t> Can	-

- 15. Click Next.
- 16. Select Mixed Mode (SQL Server authentication and Windows authentication).
- 17. Enter a password.
- 18. Add any users who should be administrators of the SQL database.

Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Feature Selection Feature Rules Instance Configuration Oatabase Engine Configuration Database Engine Configuration Consent to install Microsoft R Feature Configuration Rules Ready to Install Installation Progress Complete	Authentication Mod	ication mode and administrators for de trication mode II. Server authentication and Windov rd for the SQL Server system adminis	r the Database Engine.	2 2 
	DIVAdministrator (A DIVAdministrator2 ( Add <u>C</u> urrent User		1	QL Server administrators have unrestricted access o the Database Engine.

- 19. Click Next.
- 20. Select Multidimensional and Data Mining Mode.
- 21. Add any users who should be administrators of the Analysis Services.

Analysis Services Confi Specify Analysis Services server	iguration modes, administrators, and data directories.			
Global Rules Microsoft Update Product Updates Install Kules Install Kules Installation Type Product Key License Terms Feature Rules Instance Configuration Server Configuration Database Engine Configuration Analysis Services Configuration Consent to install Microsoft R Feature Configuration Rules Ready to Install	Server Configuration         Data Directories           Server Mode: Multidimensional and Data Mining Mode Dabular Mode BeowerPivot Mode            Specify which users have administrative permissions for Analysis Services. Data Services.			
	DIAdministrator (Administrator) DIAdministrator2 (Admin2)	Analysis Services administrators have unrestricted access Analysis Services.		
Installation Progress Complete	Add <u>C</u> urrent User <u>A</u> dd <u>R</u> emove			

Download and install necessary	pre-requisite.
Product Key License Terms Global Rules Microsoft Update	Microsoft R Open is an enhanced distribution of R made available by Microsoft under the GNU General Public License v2.
Product Updates Install Setup Files Install Rules Feature Rules Instance Configuration Server Configuration Database Engine Configuration Analysis Services Configuration Consent to Install Microsoft R Feature Configuration Rules Ready to Install	R is © the R Foundation for Statistical Computing. For more information on R-related products and servi visit http://r-project.org. By clicking "Accept" you are choosing to download Microsoft R Open and install it on your machine, and agreeing to accept patches and updates to this software according to your SQL Server update preference
Installation Progress Complete	Accept

### 23. Click Accept.

Consent to install Mic	rosoft R Open
Download and install necessary	y pre-requisite.
Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files	Microsoft R Open is an enhanced distribution of R made available by Microsoft under the GNU General Public License v2. R is © the R Foundation for Statistical Computing. For more information on R-related products and service with http://r-project.org.
Install Rules Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Analysis Services Configuration Consent to Install Microsoft R Feature Configuration Rules Ready to Install	By clicking "Accept" you are choosing to download Microsoft R Open and install it on your machine, and agreeing to accept patches and updates to this software according to your SQL Server update preferences.
Installation Progress Complete	Accept

5	SQL Server 2017 Setup	
Ready to Install Verify the SQL Server 2017 fee	tures to be installed.	
Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Analysis Services Configuration Consent to install Microsoft R Feature Configuration Rules <b>Ready to Install</b>	Ready to install SQL Server 2017: Summary - Edition: Enterprise - Action: Install (Product Update) - Prerequisites - Already installed: - Windows PowerShell 3.0 or higher - Microsoft NRT Framework 4.6 - To be installed from media: - Microsoft MPLv7 - General Configuration - Restures - Database Engine Services - Database Engine Services - Rachine Learning Services (In-Database) - Rachine Learning Services (In-Database) - Rachine Learning Services (In-Database) - Rachine Learning Services (In-Database)	8
Complete	Configuration file path: C\/Program Files\Microsoft SQL Server\140\Setup Bootstrap\Log\20190806_060849\Configuration	File.ini
	< Back Install (	Cancel

# 25. Click Install.

1	SQL Server 2017 Setup		
Complete Your SQL Server 2017 installat	ion completed successfully with product updates.		
Product Key	Information about the Setup operation or possible	le next steps:	
License Terms Global Rules	Feature	Status	
	🖉 R	Succeeded	
Microsoft Update	Machine Learning Services (In-Database)	Succeeded	
Product Updates	Oatabase Engine Services	Succeeded	
Install Setup Files	Analysis Services	Succeeded	
Install Rules	SQL Browser	Succeeded	
Feature Selection	SOL Writer	Succeeded	
Feature Rules			
	200		
Instance Configuration	Details:		
Server Configuration	Install successful.		
Database Engine Configuration			
Analysis Services Configuration			
Consent to install Microsoft B			
Feature Configuration Rules			
Ready to Install			
Installation Progress	Summary log file has been saved to the following	location:	
Complete	C\Program Files\Microsoft SQL Server\140\Setup ica 20190806_060849.bt	p.Bootstrap\Log\20190806_060849\Sum	mary symant
			Close

26. Click Close.

# 2.15.2 Install Windows Services

1. Open Server Manager.

• <ol> <li>I Manage Iools View Het</li> <li>this local server</li> </ol>
this local server
this local server
and features
servers to manage
erver group
his server to cloud services
Hide

2. Click Add Roles and Features.



Select destination	on server		DESTINATION symantec-ic
Before You Begin	Select a server or a virtual hard disk on which to in	stall roles and features.	
Installation Type Server Selection	<ul> <li>Select a server from the server pool</li> <li>Select a virtual hard disk</li> </ul>		
Server Roles	Server Pool		
Features Confirmation	Filter:		
	Name IP Address C	Operating System	
	symantec-ica.DLIPDR 192.168.1.83 N	Aicrosoft Windows Server 2012	2 R2 Standard
	1 Computer(s) found This page shows servers that are running Window Add Servers command in Server Manager. Offline collection is still incomplete are not shown.		
	conection is still incomplete are not shown.	kr	
	< Breviou	is Next >	nstall
	Add Roles and Features Wiz	ard	_
ick Next. Select server rc			
Select server rc Before You Begin Installation Type	les		DESTINATIO symantec-io
Select server ro Before You Begin Installation Type Server Selection Server Roles Features Confirmation	Select one or more roles to install on the selected Roles  Application Server DHCP Server Fax Server Fax Server	server. Description Web Server (I application ini	symantec-ii IIS) provides a i and scalable W
Select server ro Before You Begin Installation Type Server Selection Server Roles Features	Select one or more roles to install on the selected Roles Application Server DHCP Server DNS Server DNS Server	server. Description Web Server (I application ini	symantec-i IIS) provides a and scalable V

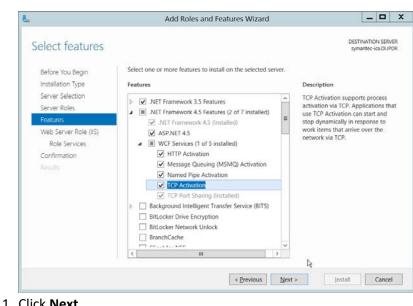
6. Select Web Server (IIS).



7. Click Add Features.

Before You Begin	Select one or more roles to install on the selected server.	symantec-ica.DLIP
Installation Type	Roles	Description
Server Selection Server Roles Features Web Services Role Services Confirmation Results	Application Server     DHCP Server     DHCP Server     Fax Server     Fax Server     Fax Server     Fax Server     Faint and Document Services     Print and Document Services     Remote Activation Services     Volume Activation Services     Volume Activation Services     Windows Deployment Services     Windows Server Essentials Experience     Windows Server Update Services     Windows Server Update Services     Windows Server Update Services     Vindows Server Update Services     Vindows Server Update Services     Vindows Server Update Services	Web Server (IIS) provides a reliable manageable, and scalable Web application infrastructure.

- 8. Click Next.
- 9. Select all services under .NET Framework 3.5 Features.
- 10. Select all services under .NET Framework 4.5 Features.



Web Server Rol	e (IIS)	DESTINATION SERVEI symantec-ica.DUPD
Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS)	Web servers are computers that let you share information ove extranets. The Web Server role includes internet information S diagnostic and administration, a unified Web platform that int Communication Foundation. Things to note: • Using Windows System Resource Manager (WSRM) can hel server traffic, especially when there are multiple roles on thi	ervices (IIS) 8.5 with enhanced security, legrates IIS 8.5, ASP.NET, and Windows p ensure equitable servicing of Web
Role Services Confirmation Results	<ul> <li>The default installation for the Web Server (IIS) role include: enable you to serve static content, make minor customizati errors), monitor and log server activity, and configure static</li> </ul>	ons (such as default documents and HTT
	More information about Web Server IIS	

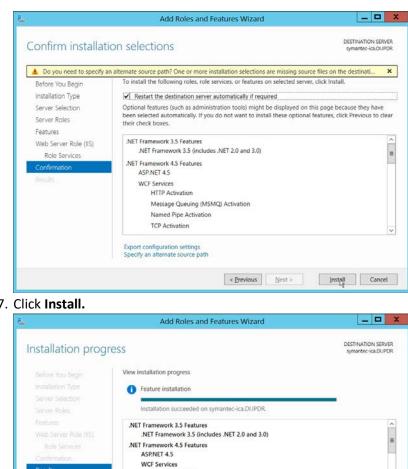
#### 12. Click Next.

- 13. Ensure that the following **Role Services** are selected:
  - a. Common HTTP Features
    - i. Default Document
    - ii. Directory Browsing
    - iii. HTTP Redirection
  - b. Health and Diagnostics
    - i. HTTP Logging
  - c. Performance

- i. Static Content Compression
- d. Security
  - i. Windows Authentication
- e. Application Development
  - i. .NET Extensibility 4.5
  - ii. ASP.NET 4.5
  - iii. ISAPI Extensions
  - iv. ISAPI Filters

Select role service		DESTINATION SERVEI symantec-ica.DLIPDI
Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Select the role services to install for Web Server (IIS) Role services Web Server Web Server Default Document Directory Browsing HTTP Features Static Content HTTP Redirection WebDAV Publishing WebDAV Publishing WebDAV Publishing Custom Logging Cu	Description Application Development provides infrastructure for developing and hosting Web applications. Use thes features to create Web content or extend the functionality of IIS. These technologies typically provide a way to perform dynamic operations that result in the creation of HTML output, which IIS then sends to fulfi client requests.

- 14. Click Next.
- 15. If necessary, specify a path to **/Sources/SxS**, which is found in the Windows Installation Media.
- 16. Check the box next to **Restart the destination server automatically if required.**



#### 17. Click Install.

Installation prog	ress	DESTINATION SERVE symantec-ica.DLIPD
	View installation progress	
	Feature installation	
	Installation succeeded on symantec-ica.DLIPDR.	
	.NET Framework 3.5 Features	
	.NET Framework 3.5 (includes .NET 2.0 and 3.0)	
	.NET Framework 4.5 Features ASP.NET 4.5	1
	ASP.NET 4.5 WCF Services	
Results	HTTP Activation	
	Message Queuing (MSMQ) Activation	
	Named Pipe Activation	
	TCP Activation	
	Message Queuing	
	Messane Queuling Services	
	You can close this wizard without interrupting running tasks. View task prograpage again by clicking Notifications in the command bar, and then Task Deta	
	Export configuration settings	

- 18. Click **Close** when the installation finishes.
- 19. Open Internet Information Services Manager.

<u>File</u> <u>View</u> <u>H</u> elp		
Connections Connections Star Rage SYNANTEC-ICA (DI\Administ Application Pools b- Stes	Filter:          •          •          •	and View Sites
	IS Authentic Compression Default Document Browsing Data Directory Decument Browsing Directory Dir	nd

- 20. Navigate to SERVER-NAME > Sites.
- 21. Right-click the Default Web Site, and select Bindings.
- 22. Change the port for http to 8080.

Type	Host Name	Port	IP Address	Binding Informa	Add
net.tcp net.m				808:* localhost	Edit
msm net.pi				localhost *	Remove
http		8080	*		Browse
				N	
				Le .	

23. Click Close.

			Internet In	formation Services (IIS) Manag	ler	_ <b>D</b> X
SYMANTEC-ICA	Sites +					<u>0</u> ≈ ∰ (0 ·
File View Help						
Connections	Sites					Alerts
8- 🗟 😥						(i) This sit
Start Page	Filter:	• 2	Go - Chow A	II   Group by: No Grouping +		bindings
SYMANTEC-ICA (DI\Administ	Name	ID	Status	Binding	Path	Actions
▷ - ● Sites	Default Web Site			%SystemDrive%\inetpub\wwwroot	Add Website Set Website Defaults	
						Edit Site Bindings Basic Settings
						<ul> <li>Explore</li> <li>Edit Permissions</li> <li>Remove</li> <li>Rename</li> </ul>
						View Applications View Virtual Directories
	٢			- 10		Manage Website  Compared Restart Compared Stop Browse Website
	Features View	Content View				Browse *:8080 (http)

24. Click Restart under Manage Website.

# 2.15.3 Installing Symantec ICA

- 1. In Task Manager, verify that the SQL Server Agent service is running.
- 2. Copy the installation media SymanteclCASoftware\_65.zip onto the server.
- 3. Extract the installation media.

1 2	Syman	tecICASoftware_65			>
E Home Share	View				v
💿 💿 – 🕆 📕 🖡	This PC + Downloads + SymanteclCASoftware_65			~ C	Search SymanteclCASoftware A
+ Favorites	Name	Date modified	Туре	Size	
Desktop	ADConnector.msi	4/19/2018 12:24 PM	Windows Installer	2.010 K	8
🐌 Downloads	BayDynamics.RiskFabric.IntegrationPack	6/29/2016 6:50 AM	Compressed (zipp.)	4.8	8
Sk Recent places	BayDynamics.RiskFabric.IntegrationPack	11/20/2017 9:20 A_	Compressed (zipp	6 K	B
	BayDynamics.RiskFabric.IntegrationPack	10/24/2016 9:26 A_	Compressed (zipp	7 K	B
👫 This PC	SymanteclCAInstaller.exe	7/27/2018 10:26 A	Application	270,048 K	B
		R			
		~			
5 items					

4. Run SymanteclCAInstaller.exe.

Risk F	abric Installation Wizard		X
Risk Fabric <sup>®</sup>	owered by Predictive Security Intelligence	(PSI™) En	igine
Welcome to the Risk Fabric Installer. This utili the Risk Fabric Database and Website. Please	y will guide you through the process of installing select an option below to get started.	g or upgrad	ing
Full Install	Database Utilities		
Select this to install Risk Fabric. You will also ha option to install the database utilities.	ve the Select this if Risk Fabric is already installed need to install the database utilities to the If you are not installing this on the server h	SQL Server.	
L <sup>4</sup>	Server, ensure you have access to a share the server.	d drive on	
Start	Start		
License Activation	Uninstall		
Select this to install a license generated offline.	Select this to uninstall Risk Fabric.		
Start	Start		1.1.1

- 5. Under Full Install, click Start.
- 6. Scroll down and check the box next to I have read, understood, and agree with the terms of the license agreement.

	Risk Fabric Installation Wizard
Risk Fabric <sup>®</sup>	Powered by Predictive Security Intelligence (PSI™) Engine
Terms and Conditions Prerequisites Website Notifications Data Sources Database Utilities Integration Warnings License Activation Install	<ul> <li>8.2 Disclosure and Use. For so long as Owner's Confidential Information remains Confidential Information, the Recipient Will (i) not disclose such Confidential Information; (ii) not use any of the Confidential Information other than in connection with its performance hereunder; (iii) protect the servecy of the Confidential Information, using the same measures that Recipient takes to protect its own Confidential Information.</li> <li>8.3 Obligations on Termination. On termination of the applicable Subscriptions, each party will discontinue its use of the other party's Confidential Information.</li> <li>8.3 Obligations on Termination. On termination of the applicable Subscriptions, each party will discontinue its use of the other party's Confidential Information.</li> <li>9.3 In extirctions. Bay Dynamics will take reasonable steps to protect the Security Data from unauthorized disclosure.</li> <li>9.4 Regregated Data. Bay Oynamics will take reasonable steps to protect the Security Data from unauthorized disclosure.</li> <li>9.4 Regregated Data. Bay Oynamics will take reasonable steps to protect the Security Data from unauthorized disclosure.</li> <li>9.4 Regregated Data. Bay Oynamics will not disclose any aggregated Security Data that could identify new cyber-attack vectors. Bay Dynamics will not disclose any aggregated Security Data that could identify client.</li> <li>10.6 Governing Law. These T&amp;C are governed by the laws of the State of New York without regard to its choice-of-laws provisions or the application of the Uniform Computer Information ramactions Act or the WOrk without regard to its choice-of-laws provisions or the application of the defail or state courts serving New York County, New York with a the secures.</li> <li>10.4 Suprement. A party may not assign or otherwise transfer its rights or obligations under a Subscription without the prior written consent of the other party except that Bay Dynamics may assign Subscriptions in will be via addivery. Counce, express 6400407, or cansults anu</li></ul>
	✓ I have read, understood, and agree with the terms of the license agreement.
	Next

5	Risk Fabric Installation Wizard		
Risk Fabric <sup>®</sup> Bay Dynamics	Powered by Predictive Securi	ty Intelligence (PSI™	1) Engi
Terms and Conditions	System Prerequisites The following features are required for the in	stallation of Risk Fabric.	
Prerequisites Website	IIS .NET Framework Extensibility base and v4.5 enabled for Application Development Features	Auto Install On	
Notifications Data Sources	IIS HTTP Activation enabled for Windows Communication Foundation (WCF)	Auto Install On	
Database Utilities Integration Warnings	Microsoft Microsoft .NET Framework 4.7.1	Already Installed	
License Activation Install	Runtime Visual C++ Redistributable Packages for Visual Studio 2013 (x64) https://www.microsoft.com/en-us/download/details.aspx? id=40784. Will require restarting the installer after this has been installed.	Already Installed	
	Authorization User is Local Admin	Already Installed	
	IIS ASP.NET v4.5	Already Installed	
	IIS ISAPI Extensions enabled for Application Development Features	Already Installed	
	IIS ISAPI Filters enabled for Application Development Features	Already Installed	
	llS		

9. Enter a username and password with privileges on the domain.

		Risk Fabric	Installation Wizard		
Risk Fabric <sup>®</sup> Bay Dynamics		Powe	red by Predictive Security Intelligenc	e (PSI™) Engi	
	upgrade.				
Terms and Conditions	Website Name	RiskFabric		•	
Prerequisites					
Website	Port	80	Check Port		
Notifications	Website URL	http://symar	ntec-ica.DI.IPDR:80/RiskFabric		
Data Sources	Installation Directo	rv Select a bas	e directory for the Risk Fabric server on the local n	machine A sub	
Database Utilities		ll be automatic	ally created in the base directory. It is the physical		
Integration Warnings		<b></b>			
License Activation	Path	C:\Program Files\Bay Dynamics\Risk Fabric Server Web Browse			
Install			count that will be used as the identity of the Risk F		
		count will also	will be granted sysadmin server role on the Risk Fa require elevated permissions to other systems su Server.	abric SQL Server	
	automatically. The ac	count will also	require elevated permissions to other systems su Server.	abric SQL Server	
	automatically. The ac administrator access	count will also to an Analysis	require elevated permissions to other systems su Server.	abric SQL Server	
	automatically. The ac administrator access Domain\Username	count will also to an Analysis	require elevated permissions to other systems su Server.	abric SQL Server	
	automatically. The ac administrator access Domain\Username Password	DIVAdministr	require elevated permissions to other systems su Server.	abric SQL Server ich as	
	automatically. The ac administrator access Domain\Username Password Administrator Acco	DIVAdministr	require elevated permissions to other systems su Server. rator •••••• indows Domain User name that will be granted ad	abric SQL Server ich as	
	automatically. The ac administrator access Domain\Username Password Administrator Acco on the Risk Fabric Po	DIVAdministr UVAdministr	require elevated permissions to other systems su Server. rator •••••• indows Domain User name that will be granted ad	abric SQL Server ich as	

- 10. Click Next.
- 11. Configure any alert settings desired; these can be changed later.

Risk Fabric	Pov	vered by Predictive Security Intellig	tence (PSI™) Eng
Terms and Conditions Prerequisites Website		s below so that email notifications can be sent. T	
Notifications Data Sources	SMTP Port	0	
Database Utilities	From Email Address		
Integration Warnings	Enable SSL		
License Activation	Send Test Email To	Send	Test Email
Install	Vulnerability Summary Vulnera It defaults to the main email add		ail address.
	Override From Email Addres	s	
	defaults to the main email addre	ls	ess. It
	Override From Email Addres	5	
		ilse positive emails will be sent sing the addres	

- 12. Click Next.
- 13. Enter the name of the SQL Server you created in the format **<SERVER-DOMAIN-NAME>\<SQL-SERVER-NAME>.**
- 14. Click **Connect**, and verify that there are no connection issues.
- 15. Enter the name of the SQL Analysis Services server you created in the format **<SERVER-DOMAIN-NAME>** (It may be the same as the SQL Server).
- 16. Click **Connect**, and verify that there are no connection issues.

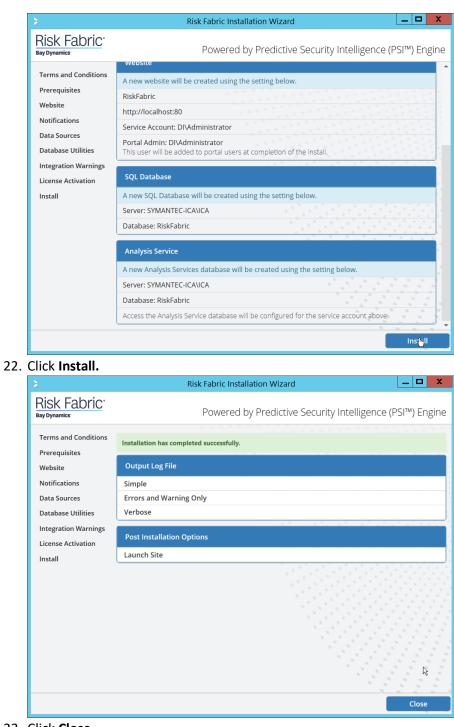
7		Risk Fabric Installation Wizard	
Risk Fabric <sup>.</sup> Bay Dynamics <sup>.</sup>	,	Powered by Predictive Security I	ntelligence (PSI™) Eng
Terms and Conditions	SQL Server Configu	ration	
Prerequisites		SYMANTEC-ICA\ICA	Connec
Website	Database	RiskFabric	-
Notifications			
Data Sources	Analysis Services Co		
Database Utilities	Server	SYMANTEC-ICA\ICA	Connec
Integration Warnings	Database	RiskFabric	-
License Activation	Default Domain D	omain to be used in case an integration provides an a	account name without a dom
Install		DI	
			Ą
			Next
lick <b>Next.</b>		Pick Fabric Installation Wizard	
>		Risk Fabric Installation Wizard	
Click <b>Next.</b> Risk Fabric <sup>®</sup> Bay Dynamics		Risk Fabric Installation Wizard Powered by Predictive Security In	
Risk Fabric	on the same server		ntelligence (PSI™) Eng ase note, this directory must
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website	on the same server	Powered by Predictive Security In ease select a directory for the database utility files. Pie r as the Risk Fabric SQL Server. If you do not have acc restart this installer.	ntelligence (PSI™) Eng ase note, this directory must
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website Notifications	on the same server administrator and	Powered by Predictive Security In ease select a directory for the database utility files. Pie r as the Risk Fabric SQL Server. If you do not have acc restart this installer.	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syste
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources	on the same server administrator and Install Databas	Powered by Predictive Security In ease select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now?	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syst
Risk Fabric Bay Dynamics Prerequisites Website Notifications Data Sources Database Utilities	on the same server administrator and Install Databas	Powered by Predictive Security In ease select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now?	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syste
Risk Fabric: Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Database Utilities Integration Warnings	on the same server administrator and Install Databas	Powered by Predictive Security In ease select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now?	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syste
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Data Sources Database Utilities Integration Warnings License Activation	on the same server administrator and Install Databas	Powered by Predictive Security In ease select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now?	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syste
Risk Fabric: Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Database Utilities Integration Warnings	on the same server administrator and Install Databas	Powered by Predictive Security In ease select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now?	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syste
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Data Sources Database Utilities Integration Warnings License Activation	on the same server administrator and Install Databas	Powered by Predictive Security In ease select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now?	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syste
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Data Sources Database Utilities Integration Warnings License Activation	on the same server administrator and Install Databas	Powered by Predictive Security In tase select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now? c:\Program Files\Bay Dynamics\Database U	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syste
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Data Sources Database Utilities Integration Warnings License Activation	on the same server administrator and Install Databas	Powered by Predictive Security In ease select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now?	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syste
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Data Sources Database Utilities Integration Warnings License Activation	on the same server administrator and Install Databas	Powered by Predictive Security In tase select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now? c:\Program Files\Bay Dynamics\Database U	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syste
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Data Sources Database Utilities Integration Warnings License Activation	on the same server administrator and Install Databas	Powered by Predictive Security In tase select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now? c:\Program Files\Bay Dynamics\Database U	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syst
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Data Sources Database Utilities Integration Warnings License Activation	on the same server administrator and Install Databas	Powered by Predictive Security In tase select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now? c:\Program Files\Bay Dynamics\Database U	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syst
Risk Fabric Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Data Sources Database Utilities Integration Warnings License Activation	on the same server administrator and Install Databas	Powered by Predictive Security In tase select a directory for the database utility files. Ple r as the Risk Fabric SQL Server. If you do not have acc restart this installer. se Utilities Now? c:\Program Files\Bay Dynamics\Database U	ntelligence (PSI™) Eng ase note, this directory must ess, please contact your syst



Risk Fabric <sup>®</sup> Bay Dynamics <sup>®</sup>		Powered b	y Predictive Security Inte	lligence (PSI™) En{
Terms and Conditions Prerequisites Website			s that might require actions outs he log file if you click the save but	
Notifications				Copy warning
Data Sources	Integration	Warnings		
Data Sources	No Warnings	No Warnings		
Integration Warnings License Activation Install				N

#### 20. Check the box next to Activate Offline.

Risk Fabric <sup>®</sup> Bay Dynamics <sup>®</sup>		Powered by Predictive Security Intelligenc	e (PSI™) Er
Terms and Conditions Prerequisites	License Activation		
Website Notifications Data Sources Database Utilities Integration Warnings License Activation Install	✓ Activate Offline		ß
			Next





# 2.15.4 Configuring Symantec ICA for Analysis

This section will contain instructions for navigating some aspects of the ICA admin console and dashboards, though this largely depends on the specific data your organization has identified and is trying to analyze.

# 2.15.4.1 Installing Integration Packs

- 1. Download the relevant integration packs to someone on the local system. These are typically provided by Symantec, in a zip file. The zip file should be titled in the format of *BayDynamics.RiskFabric.IntegrationPack.productName>.*
- 2. Log in to the Risk Fabric web interface.
- 3. Navigate to Admin > Integration.

=	Risk Fa	lbric®				S	earch	् 🗍 🗩	DMdministrator 🙆	🗂 Drait (
<u>_</u>	Assets	•								
3	Recently Viewed		Integration Pack	s Data	a Sources	Data Integrations	Job Status			
۰	Admin	-	2 Refresh	1 Import	<ul> <li>Move Up</li> </ul>	<ul> <li>Move Down</li> </ul>				
-	Settings	-	Integration Pack						Created Date	
	General		Risk Fabric Symantee	Data At Rest In	ntegration Pack				8/3/2016	٠
	Data In Motion									
	Policy									
	Queues									
	Web Activity									
	Vulnerability Manage	.								
	Residual Risk									
	Datails Grid Configur.	.								
	Entity Actions									
	Notifications									
	Organizations & Regi.									
	Operating Systems									
Privile	<b>3</b> 05									
Integra	ition									
Dashb	oards									
Risk M	lodels									
Risk V	octors									
Event	Scenarios									
Scan	Exclusions									
Entity	Collections								Activate Windows	
0	Help	•							Go to System in Control Panel to activate Windo	VW5.
	65.2									

- 4. Click Import.
- 5. Find the zip file for the integration pack that you downloaded earlier.

	Open		
🖻 💿 🔻 🕇 <u></u> 🕨 This	s PC + Downloads + SymanteclCASoftware_65 +	V 🖒 Search Syn	nanteclCASoftware 🔎
Organize 👻 New folder			)= <b>-</b> 🔟 (
☆ Favorites	Name	Date modified	Туре
Desktop	🛃 ADConnector	4/19/2018 12:24 PM	Windows Installer .
Downloads	BayDynamics.RiskFabric.IntegrationPack.MicrosoftActiveDirectory	6/29/2016 6:50 AM	Compressed (zipp.
📃 Recent places	BayDynamics.RiskFabric.IntegrationPack.SymantecDataLossPrevention	11/20/2017 9:20 AM	M Compressed (zipp.
	BayDynamics.RiskFabric.IntegrationPack.SymantecEndpointProtection	10/24/2016 9:26 AM	M Compressed (zipp.
🌉 This PC	𝗭 SymanteclCAInstaller	7/27/2018 10:26 AM	M Application
🖵 C on MM246942-PC			
朣 Desktop			
Documents			
🗼 Downloads			
🔰 Music			
📔 Pictures			
Videos			
🊢 Local Disk (C:)			
📬 Network			
	< III		
File nar	me: BayDynamics.RiskFabric.IntegrationPack.SymantecDataLossPrevention	✓ All Files	

# 6. Select the file and click **Open.**

=	Risk Fabric <sup>®</sup>				Search	् 🔺 🗩	DIAdministrator	🗂 Draft (0)
<u>_</u>	Assets 🕨							
9	Recently Viewed	Integration Packs	Data Sources	Data Integrations	Job Status			
•	Admin 🔫	2 Refresh	🛓 Import 🔺 Mov	e Up 🔹 Move Down				
0	Settings 👻	Integration Pack					Created Date	
	General	Risk Fabric Symantec D	Data At Rest Integration Pa	ck			8/3/2016	•
	Data In Motion	Risk Fabric Symantec D	Data Loss Prevention Integ	ration Pack			11/20/2017	•
	Policy							
	Queues							
	Web Activity							
	Vulnerability Manage							
	Residual Risk							
	Details Grid Conligur							
	Entity Actions							
	Notifications							
	Organizations & Regi							
	Operating Systems							
Privi	lagas							
Integ	ration							
Dast	boards							
Risk	Madata							
Risk	Vectors							
Ever	it Scenarios							
Scar	Exclusions							
Entit	y Collections						Windows em in Control Panel to activate Windo	
0	Help 🕨							

# 2.15.4.2 Create a View

1. Navigate to Analyzer > New View.

=	Risk	Fabric	Ф	Search	۹ 🖡	•	DfAdministrator 🙆 🗎 Draft (0)
	Risk		Views w Filter w Soft w Details w Char	ts 👻		3	Field List >
Le .	Dashboards	•					Search
	Analyzer	-	Add Measures from the Field List.				Measures
-			to view data from this cube.				AD Group
Now	View						AD Group First Detected Date     AD Group Last Detected Date
Oper	1 View						AD Organizational Unit
-	Action Plans						AD Organizational Unit First Detected Date
_							AD Organizational Unit Last Detected Date     Action Plan
۰.	Events	•					Action Plan Assigned To Portal User
Ð	Vulnerabilities	•					Action Plan Closed By Portal User
							Action Plan Closed Date     Action Plan Committed Completion Date
	Identities	,					Action Plan Committee Competion Date
묘	Assets	•					Action Plan Expected Completion Date
~	Recently View	- 4					<ul> <li>Action Plan Requested Completion Date</li> </ul>
3	Postaney views	aa					Action Plan SLA End Date     Action Plan SLA Start Date
۰	Admin	•					Action Plan SLA Start Late     Action Plan Status
	Help						Application
v	nep	· · ·					<ul> <li>E Application Assignment Environment</li> </ul>
							Application Assignment Tier
							Application Category     Application Centect Role
							Application Contact Hole     Application Contact User
							Application Contact Usin     Application Owner
							Authentication Event Application Direction
							Authentication Event Characteristic Ground Speed
							Authentication Event Classification
							Authentication Event Classification Date
							Authentication Event Classified By Portal User     Authentication Event Code
							Authentication Event Code     Authentication Event Computer Endpoint Behavior
							Authentication Event Computer Endpoint Behavior     Authentication Event Computer Endpoint Direction
							Authentication Event Computer Endpoint Director     Authentication Event Computer Endpoint Director
							Authentication Event Date
			View Configuration				*
Γ.			Measures	Rom	Columns	Piters Activate	Details

- 2. In the field list on the right, manually select or search for the data fields desired.
- 3. The fields can be added either by dragging the field onto the screen or by right-clicking on the field and selecting where it should be added. Ultimately, which views to select depends on the needs and preferences of your organization.
- 4. When finished, click Save.
- 5. Enter a name for the View Name.
- 6. Select the type of View for **Type.**
- 7. Check the box next to **This view is accessible by all Users (Public)** only if you wish for this view to be visible by anyone logged in.

Create new View	O Overw	rite existing View
View Name:	Testing	
Туре:	Analyzer View	v
Existing View Name:		

8. Click Save.

### 2.15.4.3 *Open an Existing View*

1. Navigate to Analyzer > Open View.

Views Manager						×
🖨 Delete 📝 R	ename 🛛 🕼 Edit Pro	operties	🛓 Import 🖾 Expo	ert		
Search Cube Views	1		Q Cube V	÷		
View Name	Туре	Accessibil	Owner	Date Created	Modified By	Date Modified
Insider Threats   Dat	Widget Definition	Public	(RiskFabric System)	09/06/2019 05:5	(RiskFabric System)	09/06/2019 05:5
Endpoint Protection	Metric Definition	Public	(RiskFabric System)	09/06/2019 05.5	(RiskFabric System)	09/06/2019 05.5
Failed Authentication	Risk Vector Definition	Public	(RiskFabric System)	09/06/2019 05:5	(RiskFabric System)	09/06/2019 05:5
Low Severity Cloud I	Metric Definition	Public	(RiskFabric System)	09/06/2019 05:5	(RiskFabric System)	09/06/2019 05:5
Unmitigated EP Eve	Metric Definition	Public	(RiskFabric System)	09/06/2019 05.5	(RiskFabric System)	09/06/2019 05:5
New High Severity In	Event Scenario Set	Public	(RiskFabric System)	09/06/2019 05:5	(RiskFabric System)	09/06/2019 05:5
Remediation   Data I	Widget Definition	Public	(RiskFabric System)	09/06/2019 05.5	(RiskFabric System)	09/06/2019 05 5
Medium Severity Tag	Metric Definition	Public	(RiskFabric System)	09/06/2019 05:5	(RiskFabric System)	09/06/2019 05:5
EP Events to Compr	Risk Vector Definition	Public	(RiskFabric System)	09/06/2019 05:5	(RiskFabric System)	09/06/2019 05:5
Users with SEP Eve	Metric Definition	Public	(RiskFabric System)	09/06/2019 05:5	(RiskFabric System)	09/06/2019 05 5
« < Page	1 of 12 > 2	) C				Displaying 1 - 25 of 285

- 2. Begin to search for the view you want by typing a search term into **Search Cube Views.** (Note: if you created a view, it will also be present in this list).
- 3. Click the **Search** icon.
- 4. Select a view.

O Delete 🕼 R	ename 🕼 Edit Pr	operties 👤 土	Import 🛓 Expo	ort			
Dar			Q Cube V	New Types		*	
View Name	Туре	Accessibility	Owner	Date Created	Modified By	Date Modified	
DAR Incident Details	Analyzer Vlew	Private	(DIVAdministrator)	09/06/2019 08 2	(DI\Administrator)	09/06/2019 08:2	

5. Click Open.

#### 2.15.4.4 Viewing Detailed Analyzer Data

1. The desired field data can be exported to either a *.csv* or *Microsoft Excel* format, by clicking on the **Export** button in the details tab.

=	Risk Fal	oric®			Search		Q	<b>*</b> •			DMAdministrator 🦲 🗂 Dr	sili (0)
	Risk	Vieus 🕶 🛛	Filter 🕶 Sort 🕶 Details								Field List	· F
		DAR Incident Sta	atus New	Total								
2	Dashboards			DAR Incident Match Count DAR Inciden							Search	_
	Analyzer	2-7 Days Ago	64			324					Measures	
v	nagen	61-90 Days Ago			43	195					AD Oroup	
New	View	Total	107	520	107	520					AD Group First Detected Date	
Oper			Bar Chart	0 = 2 ×	Details (1)				0 = 2 ×		AD Group Last Detected Date     AD Organizational Unit	
8	Action Plans	•							📥 Export 💌		AD Organizational Unit First Detected Date     AD Organizational Unit Last Detected Date	
			\$								Action Plan	
*	Events	•	2-7 Deye Ago		DAR Incident Date	DAR Incident Status	DAR Incident Sour	DAR File Docume	DAR File Folde		Action Plan Assigned To Portal User	
Ð	Vulnerabilities		2		2-7 Days Ago	New	101				Action Plan Closed By Portal User	
· ·			1		T-I Data HRo	Topo	101				Action Plan Clased Date	
	Identities	•	81-40 Days App		2-7 Dava Ago	New	102				Action Plan Committed Completion Date	
_			-								Action Plan Due Date     Action Plan Expected Completion Date	
-	Assets		40	an an 70	2-7 Days Ago	New	103				Action Plan Expected Competion Date     Action Plan Requested Completion Date	
ອ	Recently Viewed			DAR Incident Count							Action Plan Requested Companion Date     Action Plan SLA End Date	
					2-7 Days Ago	New	104				Action Plan SLA Start Date	
۰	Admin	•			-						Action Plan Status	
0	Help				« < Page	1 012 > >	) a	Paroute 1	- 100   Total: 107		Application	
	nep				Sec. 1 also	1 000 7 7					Application Assignment Environment	
											Application Assignment Tier	
											Application Category	
											Application Centact Role	
											Application Centact User	
											Application Owner	
											Authentication Event Application Direction	
											Authentication Event Characteristic Ground	speed
											<ul> <li>Authentication Event Classification</li> </ul>	
											Authentication Event Classification Date	
											Authentication Event Classified By Portal Us	ēf
											Authentication Event Code	
											Authentication Event Computer Endpoint Be	
											Authentication Event Computer Endpoint Dir	
											Authentication Event Computer Endpoint Ov	ned B
		🔄 Bar Chart	Detaits (1)								Authentication Event Date	
		View Config	uration: DAR Incident Deta	alls (Analyzer View)								٣
		Measures		Rows		Columns		Fiters			Details	
		DAR Incident Co	ount	DAR Incident Date Range		DAR Incident Status				Activate	DAH Incident Source ID	
		DAR Incident Ma								Go to Syste	DAR File Document Type	
											DAR File Folder	
												-

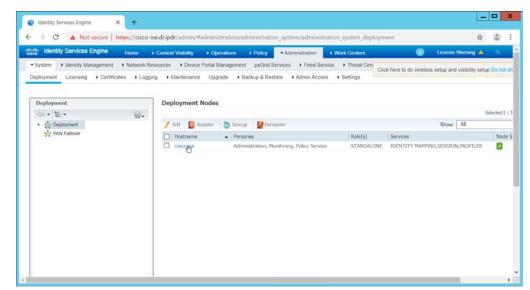
- 2. Charts can be added or removed using the **Charts** dropdown menu near the top of the analyzer.
- 3. Any data in the **Field List** on the right side can be added to or removed from the view and will be automatically incorporated into its relevant rows or columns.
- 4. The entire view format can be exported as a *.json* file from the **Open View** option.

# 2.16 Integration: Cisco Identity Services Engine and Cisco Stealthwatch

This section will detail an integration between Cisco Identity Services Engine (ISE) and Cisco Stealthwatch, allowing Stealthwatch to apply certain policies to hosts in ISE. Stealthwatch acts as a network monitoring solution and can be integrated with ISE to enable mitigation capabilities in response to events. Please see *Deploying Cisco Stealthwatch 7.0 with Cisco ISE 2.4 using pxGrid* for details and other potential uses of the integration.

# 2.16.1 Configuring Certificates for pxGrid

- 1. Log in to the Cisco ISE web console in a browser.
- 2. Navigate to Administration > System > Deployment.



- 3. Click the hostname of the Cisco ISE machine.
- 4. Check the box next to **pxGrid.**

In Identity Services Engine Home + Co	di.ipdr/admin/#administration/ad	Policy      Administration	Work Centers	0	License Warning 🔺 🔍
System + Identity Management + Network Resource eployment Licensing + Certificates + Logging	arces		ice  Threat Cen		setup and visibility setup Do n
	Role Other Monitoring Node	PRIMARY *			
5	<ul> <li>✓ Policy Service</li> <li>✓ Enable Session Service</li> <li>Include Node in</li> </ul>	noes () Node Group None	• w		
	Enable Profiling Serv     Enable Threat Centre	c NAC Service (j)			
	Enable SXP Service     Enable Device Admi     Enable Passive Iden	n Service (į)			
	Dec pxGrid (7)	La			

- 5. Click Save.
- 6. Navigate to Administration > pxGrid Services.

System      Identity Managem	Home      Context Visibility ent      Network Resources      Devi	Operations      Policy     Portal Management pxGrid Se	Administration     Work Centers  rvices     Feed Service     Threat Centers	Click here to do wireless setup	se Warning 🔺 🔍
the second s	Capabilities Live Log Settings	U			
Client Name	Ve 😝 Group 👎 Decline 😵 beles	<ul> <li>Refresh Total Pending Ap Capabilities</li> </ul>	proval(0) +	Client Group(s)	Auth Method
Cileric ricorne	Calche Description	Capacinities	No data available	Cilclic Group(s)	MultiPictiou
					_

- 7. Click Certificates.
- 8. Select Download Root Certificate Chain for I want to.
- 9. Select the hostname of the Cisco ISE server for Host Names.
- 10. Select Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PLCS8 PEM format (including certificate chain) for Certificate Download Format.

In Identity Services Engine Hor	ne	Operations	Policy     Administrate	on  Vork Centers	0	License Warning 🔺	۹,
System + Identity Management + Net	work Resources	e Portal Management	pxGrid Services Fe	ed Service + Threat Cen	Click here to do wireles	ss setup and visibility setu	p Do n
All Clients Web Clients Capabilities	Live Log Settings	Certificates Perm	nissions				
Generate pxGrid Certificates							
I want to *	Download Root Certificate	Chain			*		
Host Names *	> cisco-ise						
Certificate Download Format *	Certificate in Privacy Enh	anced Electronic Mall (P	'EM) format, key in PKCS8	PEM format (including certi	ficate chair • 0		
				Reset	Create		
inected to pxGrid cisco-ise di ipdr							

- 11. Click **Create.** This will download a zip file containing the certificate.
- 12. Extract the zip file—it may contain several files—the one we are interested in is the Root CA.
- 13. Log in to the **Stealthwatch Management Console** through the browser.

diado cisco	Stealthwatc	h Monitor	Analyze	Jobs	Configure	Deploy		9 0	Global Settin	ktop Client
	y Insight Dashbo	oard   Inside	e Hosts						UDP Directo	igenernt izer Configura r Configuration kup Configura
Concern (		Recon	csc ()	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Po User Manag	ement ()
Top Al	arming Hosts No data to di		- /	Alarms by Type	3	-	7 Toda	ay's Alarms		- /

14. In the top right corner of the console, hover over the **gear icon** and select **Central Management** from the submenu.

Identity Services Engine	X Security Insight D	and the second sec	Inventory   Central Management	× +			
→ C ▲ Not secu	re   https://192.168.1.52/cen	tral-mgmt/#!/invento	ory/				\$ ٢
stealthwa	tch Central Mana	agement	Appliance Manager	Update M	lanager	App Manager	C
Appliances found							
Q Filter Appliance Inv	entory Table						
APPLIANCE STATUS	LICENSE STATUS	△ HOST NAME		~	IP ADDRESS	^ ACTIONS	
Up	60 Days or Less	smc-01	SMC SMCVE-VMware- 4232d9abe1b32e14 e810b21f42a1f570		192.168.1.52	R	
Up	90 Days or Less	fcnf-01	Flow Collector FCNFVE-VMware- 4232dbf162c01ea4 f1b1edb64da9166b		192.168.1.54	Θ	
Up	90 Days or Less	fr-01	UDP Director UDVE-VMware- 4232cfa73db93cb3 472570289f7a4dea	2	192.168.1.55	$\odot$	
Up	90 Days or Less	fsae-01	Flow Sensor		192.168.1.53		

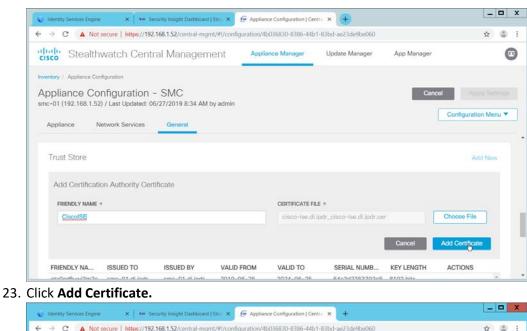
15. In the table, find the row with the Stealthwatch Management Console (likely labeled as SMC). Click the **ellipses button** in the **Actions** column.

ldentity Services Eng	gine 🗙 🛛 🐝 Security Insight [	ashboard   Stea 🗙 😥	Inventory   Central Management 🗙	+		
- > C 🔺 N	Not secure   https://192.168.1.52/cer	ntral-mgmt/#!/inventor	y/			☆ 🍵
Appliances found	Ithwatch Central Man	agement	Appliance Manager Upd	ate Manager App Manag	er	0
Q Filter Applia	ance Inventory Table	○ HOST NAME	∧ түре	Edit Appliance Configuration	CTIONS	
Up	60 Days or Less	smc-01	SMC SMCVE-VMware- 4232d8dbe1b32e14- e810b21f42e1f570	Manage Licenses Support	$\odot$	
Up	90 Days or Less	fcnf-01	Flow Collector FCNFVE-VMware- 4232dbf162c01ea4- 11b1edb64da9166b	Reboot Appliance Shut Down Appliance	O	
Up	90 Days or Less	fr-01	UDP Director UDVE-VMware- 4232cfa73db93cb3- 472570289f7a4dea	Remove This Appliance	œ	
Up	90 Days or Less	fsae-01	Flow Sensor	192.168.1.53		

- 16. This will open a submenu. Select Edit Appliance Configurations.
- 17. Click the **General** tab.
- 18. Scroll down to the **Trust Store** section.

Identity Services Engine	× w Sp	curity Insight Dashboard	Ster 🗙 ਓ Appliar	nce Configuration   Cent	m × +		_ 0
→ C ▲ Nots	ecure   https://192	168.1.52/central-mgm	nt/#!/configuration/4	b036830-8386-44b1	-83bd-ae23de9be060		* 4
Stealthy	watch Centr	al Managem	ent Appli	ance Manager	Update Manager	App Manager	(
ventary ( Appliance Cont Appliance Cor mc-01 (192.168.1.52) Appliance Ne Trust Store FRIENDLY NA	nfiguration -		y admin	VALID TO	SERIAL NUMB	Canc	el Apply Setting Configuration Menu V Add New Actions
otaOndfiywi2m2e wzjhmntkxotdmzd mzmjm5ntrknza tq2ywmxzdc1ngu 5mtcznja0ymeznji wodwmndhhyw==- cert		smc-01.di.ipdr	2019-06-25 07:50:35	2024-06-25 07:50:35	64c2d2753702e5 538e85593013b1 28332c2b41e8	8192 bits Delete	
fr-01.di.ipdr	fr-01.di.ipdr	fr-01.di.ipdr	2019-06-18 05:51:57	2024-06-18 05:51:57	633aa308a37cba2 3e511c486d1f2c9 8b6e1b93bd	8192 bits	

- 19. Click Add New.
- 20. Enter a name.
- 21. Click Choose File.
- 22. Select the Cisco ISE Root certificate from the files downloaded earlier.



#### → C A Not secure | https://192.168.1.52/central-mgmt/#1/configuration/4b036830-8386-44b1-83bd-ae23de9be060 x 3 : ~ cisco Stealthwatch Central Management Appliance Manager Update Manager App Manager 0 ry / Appliance Config Appliance Configuration - SMC ic-01 (192.168.1.52) / Last Updated: 06/27/2019 8:34 AM by admin n Menu V Appliance Network Services General Trust Store Modified Add New FRIENDLY NA ... ISSUED BY VALID FROM VALID TO SERIAL NUMB .... KEY LENGTH ISSUED TO ACTIONS e5t8t9692t9 Delete 2019-06-26 2024-06-26 201a1158dd248d 8192 bits fsae-01.di.ipdr fsae-01.di.ipdr fsae-01.di.ipdr 13:02:19 13:02:19 dbfa1c0d3cee2 74403d0ca66 Delete CiscolSE cisco-ise.di.ipdr cisco-ise.di.ipdr 2019-04-09 2021-04-08 5cacf13c000000 2048 bits 12:23:40 12:23:40 0df37c2085c187c d0 Delete

24. Click Apply Settings.

→ C A Not	secure   https://19	2.168.1.52/central-mom	t/#!/configuration/4	b036830-8386-44b1-4	83bd-ae23de9be060		1	0.0
	watch C Ar	ply Configuration C	Changes to Appli	iance		x		
	nfigurati	ile the system applies juired, the appliance w			al modifications. If a re ad.	boot is		
	The Ge	e following configuration neral: Trust Store	ons have changed:					
					1	4		
					Cancel Apply C	Changes IN		

- 25. Click **Apply Changes** if prompted to confirm the changes.
- 26. When that finishes, navigate back to the **Appliance Configurations** section.
- 27. In the table, find the row with the Stealthwatch Management Console (likely labeled as SMC). Click the **ellipses button** in the **Actions** column.
- 28. This will open a submenu. Select Edit Appliance Configurations.

Stealthwatch Central Management	Appliance Manager	Update Manager	App Manager	C
entery / Appliance Configuration ppliance Configuration - SMC ne-01 (192.168.1.52) / Last Updated: 06/27/2019 9:36 AM by admin Appliance Network Services General			Cancel	Apply Settings
Additional SSL/TLS Client Identities				AddWew
A Improperty modifying your Certificates can break your Stealth	watch System.			
	watch System.	SERIAL NUMB	KEY LENGTH	ACTIONS

- 29. Click Add New under Additional SSL/TLS Client Identities.
- 30. Select 2048 for RSA Key Length.
- 31. Enter your organization's information.

Stealthwatch Central Manager	THENE Appliance Manager Update Manager App Manager	
Inventory / Appliance Configuration Appliance Configuration - SMC sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:55 A Appliance Network Services General	M by admin Cancel Apply 3 Configuration N	Sami
Generate a CSR		
RSA KEY LENGTH *	COMMON NAME	
2048 bits    4096 bits    8192 bits	sw-smc.di.lpdr	
	ORGANIZATIONAL UNIT	
DI	IPDR	
LOCALITY OR CITY	STATE OR PROVINCE	
Rockville	MD	
COUNTRY CODE	EMAIL ADDRESS	
Click Generate CSR.	administrator@di.jpdr Cancel Generate CSR	
	d   Stee X @ Appliance Configuration   Centre X +	-
Click Generate CSR.	Cancel Generate CSR d Ste: X @ Appliance Configuration   Centre X + guration/b4915dc2-2979-45fc-b907-42dc19ce70b6 \$	- 1
Click Generate CSR.	Cancel Generate CSR d Ste: X @ Appliance Configuration   Centre X + guration/b4915dc2-2979-45fc-b907-42dc19ce70b6 \$	- 1
Click Generate CSR. w Identity Services Engine ★ ■ Security Insight Dashboar ★ → C ▲ Not secure   sw-smc/central-mgmt/#l/config ticsco Stealthwatch Central Managen Inventory / Appliance Configuration Appliance Configuration - SMC	Cancel Generate CSR d15tc: X @ Appliance Configuration   Centre X + guration/b4915dc2-2979-45fc-b907-42dc19ce70b6 \$ Ment Appliance Manager Update Manager App Manager Cancel Apply 3	- I X Setti
Click Generate CSR.	Cancel Generate CSR d15tc: X @ Appliance Configuration   Centre X + guration/b4915dc2-2979-45fc-b907-42dc19ce70b6 \$ Ment Appliance Manager Update Manager App Manager Cancel Apply 3	Setti
Click Generate CSR. w Identity Services Engine ★ ■ Security Insight Dashboar ★ → C ▲ Not secure   sw-smc/central-mgmt/#l/config ticsco Stealthwatch Central Managen Inventory / Appliance Configuration Appliance Configuration - SMC	Cancel Generate CSR ad JSte: X @ Appliance Configuration   Centre X + guration/b4915dc2-2979-45fc-b907-42dc19ce70b6 Ment Appliance Manager Update Manager App Manager M by admin	Setti
Click Generate CSR. ♦ Identity Services Engine ★ I ** Security Insight Dashboar ♦ → C ▲ Not secure I sw-smc/central-mgmt/#I/config *Cisco Stealthwatch Central Manager Inventory / Appliance Configuration Appliance Configuration – SMC sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:31 A	Cancel Generate CSR ad JSte: X @ Appliance Configuration   Centre X + guration/b4915dc2-2979-45fc-b907-42dc19ce70b6 Ment Appliance Manager Update Manager App Manager M by admin	Senti Menu
Click Generate CSR.	Cancel Generate CSR d15te: X @ Appliance Configuration   Centr: X + guration/b4915dc2-2979-45fc-b907-42dc19ce70b6 Ment Appliance Manager Update Manager App Manager M by admin Configuration M Configuration M	Senti
Click Generate CSR.	Cancel Generate CSR d Stee X @ Appliance Configuration   Centre X + guration/b4915dc2-2979-45fc-b907-42dc19ce70b6 Ment Appliance Manager Update Manager App Manager Cancel Apply 3 Configuration M	Senti
Click Generate CSR.	Cancel Generate CSR d15te: X @ Appliance Configuration   Centr: X + guration/b4915dc2-2979-45fc-b907-42dc19ce70b6 Ment Appliance Manager Update Manager App Manager M by admin Configuration M Configuration M Configuration M Configuration M	Setti
Click Generate CSR.  Click Generate CSR.  Click Generate CSR.  Click Generate CSR.  Click Generate Configuration  Click Generate Structure Structure Structure Configuration  Click Generate Configuration  Appliance Configuration - SMC  Swr-amc (192.168.1.150) / Last Updated: 08/08/2019 6:31 A  Appliance Network Services Generat  Add SSL/TLS Client Identity  FRIENDLY NAME =	Cancel Generate CSR d15te: X @ Appliance Configuration   Centr: X + guration/b4915dc2-2979-45fc-b907-42dc19ce70b6 Ment Appliance Manager Update Manager App Manager M by admin Configuration M Configuration M Configuration M	Setti

- 33. When this finishes, click **Download CSR.**
- 34. Open the Certificate Signing Request (CSR) in a text file, and copy all the contents.
- 35. On the ISE web console, navigate to Administration > pxGrid Services > Certificates > Generate pxGrid Certificates.

- 36. Select Generate a single certificate (with certificate signing request) for I want to.
- 37. Paste the copied text into the Certificate Signing Request Details.
- 38. Enter a description such as SMC for the Description.
- 39. Select IP Address for Subject Alternative Name (SAN).
- 40. Enter the IP Address of the Stealthwatch Management Console.
- 41. Select PKCS12 format (including certificate chain; one file for both the certificate chain and key) for Certificate Download Format.
- 42. Enter a password, and confirm the password.

	ne   Context Visibility  Operations  Policy  Administration  Work Centers	1 License Warni
System Identity Management Ne	work Resources	vireless setup and visibi
All Clients Web Clients Capabilities	Live Log Settings Certificates Permissions	
Generate pxGrid Certificates		
I want to *	Generate a single certificate (with certificate signing request)	
Certificate Signing Request Details	NIGVIS-204KCom040708HoRa8taKELaNwk=	
Description	smc-csr	
Certificate Template	PxGrid_Certificate_Template	
Subject Alternative Name (SAN)	IP address 🔹 192.168.1.150 🚥 🐇	
Certificate Download Format *	PKCS12 format (including certificate chain; one file for both the certificate chain and key)	D
Certificate Password *		D
Confirm Password *		

- 43. Click Create.
- 44. This will download a zip file. Unzip the file.
- 45. On the Stealthwatch Management Console (SMC) web console, under Additional SSL/TLS Client Identities (where you downloaded the CSR), click Choose File.
- 46. Upload the certificate file from the zip file that has the hostname of the SMC in it; the file extension should be *.p12*.
- 47. Enter a name for Friendly Name.
- 48. Enter the password used in ISE when generating the certificate.

Stealthwatch Central Management	Appliance Manager	Update Manager	App Manager	
nventory / Appliance Configuration				
Appliance Configuration - SMC			Cancel	
sw-smc (192.168.1.150) / Last Updated: 08/08/2019 7:34 AM by admin			Configura	ation Menu 1
Appliance Network Services General				
r tannonan oobr i bo' onora raonanoo 🦕				
Add SSL/TLS Client Identity			Download C	CSR
FRIENDLY NAME *	CERTIFICATE FILE *			
SMC_PKCS12	sw-smc.di.lpdr_1	192.168.1.150.p12	Choose Fi	ile
BUNDLE PASSWORD *	CONFIRM PASSWORD	D *		
			_	
		Cancel	Add Client Iden	ntity

VALID TO

CEDIAL MILINA

VALID EDOM

# 49. Click Add Client Identity.

sco Stealt	hwatch Cei	ntral Manager	nent 🦯	Appliance Manager	Update Manag	ger App M	lanager
antory / Appliance C	onfiguration						
	Onfiguration 150) / Last Update	n - SMC ed: 08/08/2019 6:55 A	M by admin			Cance	Configuration Men
Appliance	Network Services	General					Configuration Men
Additional SSI	L/TLS Client Id	entities 👩 🛛 🤇 Mod	fied				Add New
		entities <b>Moo</b> ertificates can break y ISSUED BY		System. VALID TO	SERIAL NUM	KEY LENGTH	Add New
	v modifying your C	ertificates can break y	our Stealthwatch		SERIAL NUM 55e8a9bc77484 06f9d07c429641 e5b05	KEY LENGTH 2048 bits	

- 50. Click Apply Settings.
- 51. Navigate back to the SMC web console home screen.

cisco		althwatc							0	Desk	top Client	~
	Da	ashboards	Monitor	Analyze	Jobs	Configure	e Depj	6y				
Securit	v Insi	ght Dashbo	ard Linsid	e Hosts			Cisco*	ISE Configuration	m			
boount	y mon	grit Duoribe	and Thiold					Directory				
Alarmin	ng Hos	sts 🕲					Stealth	watch Cloud			-	1
Concern	Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly	
0		0	0	0	0	0	0	0	0	0	0	
Top Al	arming	g Hosts	-	- AI	arms by Typ	be	-	и то	day's Alarm:	s	-	2
		No data to dis	play									

#### 52. Navigate to **Deploy > Cisco ISE Configuration.**

V Identity Services Engine	🗙 🐨 Cisco 🖲 IS	E Configuration   Steal: ×	w Inventory   Central	Management ×   +	
← → C 🔺 Not secure	e   sw-smc/lc-landing	g-page/smc.html#/setting:	s/pxgrid		☆ <b>(</b> \$
CISCO Dashboards	tch <sub>Monitor</sub>	Analyze Jobs	Configure	Deploy	Q Desktop Client
Cisco® ISE Configura	ation				
Cisco ISE Configuration	0				
	- Old Add				Add new configuration
No Cisco ISE configuration	s. Click Add new co	infiguration to begin.			

- 53. Click Add New Configuration.
- 54. Enter a Cisco ISE cluster name.
- 55. Select the certificate you just uploaded for Certificate.
- 56. Enter the IP Address of Cisco ISE for Primary pxGrid Node.

#### 57. Enter a **username** for the SMC to use.

😰 Identity Services Engine 🛛 🗙 😰 Cisco® ISE Configuration   Steal: 🗙 🐝 In	wentory   Central Management × +
- → C A Not secure   sw-smc/lc-landing-page/smc.html#/settings/pxg	
Cisco ISE Configuration ()	Add new configuration
Cisco ISE Configuration Setup	
CLUSTER NAME:	
cisco-ise	
CERTIFICATE:	
SMC_PKCS12 V	
PRIMARY PXGRID NODE: *	SECONDARY PXGRID NODE:
192.168.1.61	ex. 10.10.10.10
USER NAME: 0 *	
SMC	
Integration options ()	
Adaptive Network Control 🚳	
Static SGT Classifications	
User sessions 🔞	
	Cancel Save the

#### 58. Click Save.

59. On the Cisco ISE web portal, navigate to Administration > pxGrid Services > All Clients.

All Clients Web Clients Capabilities Live Log Settings Certificates Permissions          I Client Name       Client Description       Capabilities CPUB 0 Subb       Status       Client Group(s)         Client Name       Client Description       Capabilities (0 Pub, 0 Sub)       Online (XMPP)       Internal         Isse-admin-cisco-ise       Capabilities (0 Pub, 0 Sub)       Online (XMPP)       Internal         Isse-admin-cisco-ise       Capabilities (0 Pub, 0 Sub)       Online (XMPP)       Internal         Isse-admin-cisco-ise       Capabilities (0 Pub, 0 Sub)       Online (XMPP)       Internal         Isse-admin-cisco-ise       Capabilities (0 Pub, 0 Sub)       Online (XMPP)       Internal         Isse-admin-cisco-ise       Capabilities (0 Pub, 1 Sub)       Online (XMPP)       Internal         Isse-bidge-cisco-ise       Capabilities (0 Pub, 1 Sub)       Online (XMPP)       Internal         Isse-mint-cisco-ise       Capabilities (0 Pub, 0 Sub)       Online (XMPP)       Internal         Isse-mint-cisco-ise       Capabilities (0 Pub, 0 Sub)       Online (XMPP)       Internal         Isse-mint-cisco-ise       Capabilities (0 Pub, 0 Sub)       Online (XMPP)       Internal         Isse-mint-cisco-ise       Capabilities (0 Pub, 0 Sub)       Online (XMPP)       Internal	Charles     Obselve     Oppose     Group     Declnet     Oppose     Refresh     Total Pending Approval(0) +     1 selected item 1 - 6 of 6     Show       Client Name     Client Description     Capabilities     Status     Client Group(s)       b ise-fanout cisco-ise     Capabilities(0 Pub, 0 Sub)     Online (XMPP)     Internal       b ise-damout cisco-ise     Capabilities(0 Pub, 0 Sub)     Online (XMPP)     Internal       c ise-submit-cisco-ise     Capabilities(0 Pub, 0 Sub)     Online (XMPP)     Internal       b ise-infrage-cisco-ise     Capabilities(0 Pub, 0 Sub)     Online (XMPP)     Internal       c ise-infrage-cisco-ise     Capabilities(2 Pub, 4 Sub)     Online (XMPP)     Internal       c ise-infrage-cisco-ise     Capabilities(2 Pub, 1 Sub)     Online (XMPP)     Internal		em 🕨 Identity	Management	<ul> <li>Network</li> </ul>	k Resources	<ul> <li>Device F</li> </ul>	Portal Manager	pxGrid Services	Feed Service	Threat Cen	Click here to do wi	reless setup	and visibil
Client Name         Client Description         Capabilities         Status         Client Group(s) <ul> <li>ise-fanout cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (2MPP)</li> <li>Internal</li> <li>ise-schmin-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (2MPP)</li> <li>Internal</li> <li>ise-indige-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (2MPP)</li> <li>Internal</li> <li>ise-indige-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (2MPP)</li> <li>Internal</li> <li>ise-indige-cisco-ise</li> <li>Capabilities(2 Pub, 1 Sub)</li> <li>Online (2MPP)</li> <li>Internal</li> </ul>	Client Name         Client Description         Capabilities         Status         Client Group(s) <ul> <li>ise-fanout cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (2MPP)</li> <li>Internal</li> <li>ise-schmin-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (2MPP)</li> <li>Internal</li> <li>ise-indige-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (2MPP)</li> <li>Internal</li> <li>ise-indige-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (2MPP)</li> <li>Internal</li> <li>ise-indige-cisco-ise</li> <li>Capabilities(2 Pub, 1 Sub)</li> <li>Online (2MPP)</li> <li>Internal</li> </ul>	All Clie	ents Web Cl	ents Capa	bilities	Live Log	Settings 0	Certificates	Permissions					
<ul> <li>ise-fanout cisco-ise</li> <li>capabilities(0 Pub, 0 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-admin-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-bitoud-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-indime-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-indime-cisco-ise</li> <li>Capabilities(0 Pub, 4 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-indime-cisco-ise</li> <li>Capabilities(2 Pub, 1 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-indime-cisco-ise</li> <li>ise-indime-cisco-ise</li> <li>ise-indime-cisco-ise</li> <li>ise-indime-cisco-ise</li> <li>ise-indime-cisco-ise</li> <li>ise-indim</li></ul>	<ul> <li>ise-fanout cisco-ise</li> <li>capabilities(0 Pub, 0 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-admin-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-bitoud-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-indime-cisco-ise</li> <li>Capabilities(0 Pub, 0 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-indime-cisco-ise</li> <li>Capabilities(0 Pub, 4 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-indime-cisco-ise</li> <li>Capabilities(2 Pub, 1 Sub)</li> <li>Online (XMPP)</li> <li>Internal</li> <li>ise-indime-cisco-ise</li> <li>ise-indime-cisco-ise</li> <li>ise-indime-cisco-ise</li> <li>ise-indime-cisco-ise</li> <li>ise-indime-cisco-ise</li> <li>ise-indim</li></ul>	🖌 Enabi	e 🕖 Disable	O Approve	Group	P Decline	😧 Delete 👻	😵 Refresh	Total Pending Approval(0)	*		1 selected item	1 - 6 of 6	Show
> ise-admin-cisco-ise     Capabilities(4 Pub, 2 Sub)     Online (XMPP)     Internal       > ise-pubsub-cisco-ise     Capabilities(0 Pub, 0 Sub)     Online (XMPP)     Internal       > ise-bridge-cisco-ise     Capabilities(0 Pub, 4 Sub)     Online (XMPP)     Internal       > ise-mat-cisco-ise     Capabilities(2 Pub, 1 Sub)     Online (XMPP)     Internal	> ise-admin-cisco-ise     Capabilities(4 Pub, 2 Sub)     Online (XMPP)     Internal       > ise-pubsub-cisco-ise     Capabilities(0 Pub, 0 Sub)     Online (XMPP)     Internal       > ise-bridge-cisco-ise     Capabilities(0 Pub, 4 Sub)     Online (XMPP)     Internal       > ise-mat-cisco-ise     Capabilities(2 Pub, 1 Sub)     Online (XMPP)     Internal		Client Name	12	Clier	t Description		Capabilit	ies	Status		Client Group(	s)	
> ise pubsub cisco-ise         Capabilities(0 Pub, 0 Sub)         Online (04/PP)         Internal           > ise-bridge-cisco-ise         Capabilities(0 Pub, 4 Sub)         Online (04/PP)         Internal           > ise-bridge-cisco-ise         Capabilities(2 Pub, 1 Sub)         Online (04/PP)         Internal           > ise-mnt-cisco-ise         Capabilities(2 Pub, 1 Sub)         Online (04/PP)         Internal	> ise pubsub cisco-ise         Capabilities(0 Pub, 0 Sub)         Online (04/PP)         Internal           > ise-bridge-cisco-ise         Capabilities(0 Pub, 4 Sub)         Online (04/PP)         Internal           > ise-bridge-cisco-ise         Capabilities(2 Pub, 1 Sub)         Online (04/PP)         Internal           > ise-mnt-cisco-ise         Capabilities(2 Pub, 1 Sub)         Online (04/PP)         Internal	•	ise-fanout-cisco	ise				Capabili	ies(0 Pub, 0 Sub)	Online (XMPP)		Internal		
Image: Size-Bindge-cisco-ise         Capabilities(0 Pub, 4 Sub)         Online (0MPP)         Internal           Image: Image: Provide Public P	Image: Size-Bindge-cisco-ise         Capabilities(0 Pub, 4 Sub)         Online (0MPP)         Internal           Image: Image: Provide Public P	100000000						Capabili	ies(4 Pub, 2 Sub)	Online (XMPP)		Internal		
Capabilities(2 Pub, 1 Sub) Online (XMPP) Internal	Capabilities(2 Pub, 1 Sub) Online (XMPP) Internal													
Capabilities(0 Pub, 0 Sub) Online (OMPP)	Capabilities(0 Pub, 0 Sub) Online (OMPP)											Internal		
4		4												

60. If the SMC client you just created says **Pending**, check the box next to it and click **Approve**.

Dashbo	hWatch <sub>Dards Monitor</sub>	Analyze Jobs	Configure	Deploy	9	• • •	Desktop Client
Cisco® ISE Con	figuration						
Cisco ISE Config	uration					_	
				•		-	ew configuration
Cluster Name	Primary pxGrid Node 192.168.1.61 •	+ Secondar	ry pxGrid Node	+ Use SMC	r Name	Status	Actions
							<u> </u>

61. The SMC Cisco ISE Configuration page will have a green status icon if it can successfully authenticate to ISE.

# 2.16.2 Configuring Stealthwatch to Quarantine through ISE

#### 1. Navigate to **Operations > Adaptive Network Control > Policy List.**

cisco Identity Services Engine H	fome  F Context Visibility	Operations     Policy	<ul> <li>Administration</li> </ul>	Work Centers	0	License Warning 🔺	S 🕘
RADIUS Threat-Centric NAC Live Logs Policy Lis: Endpoint Assignment	s + TACACS + Troubleshoot	<ul> <li>Adaptive Network Control</li> </ul>	Reports		Click here to do wirele	ess setup and visibility setup	Do not show the
List							
C Refresh + Add Trash - C	5 Edit						19
Policy Name	ANC A	ctions					
No data found.							

- 2. Click Add.
- 3. Enter a name for a quarantine action.

AddIUS Threat-Centric NAC Live Logs + TACACS + Troublestoot + Adaptive Network Control Reports      Click here to do wireless setup and visibility setup Do not show this a      Policy List      Form     CUARANTINE      CUMPONTINE      SHUT_DOWN     PORT_BOUNCE      COMPONTINE      COMPONTINE      SHUT_DOWN	Identity Service	is Engine Home	➤ Context Visibility	• Operations	+ Policy	Administration	Work Centers		License Warning	<u>a</u> q		
Acton* CULARANTINE Acton* CULARANTINE CULARANTINE SHUT_DOWN			ACACS + Troubleshoot	<ul> <li>Adaptive</li> </ul>	Network Control	Reports		Click here to do w	reless setup and visibility	setup Do n	x show t	his ag
Action* CULARANTINE CULARANTINE SHUT_DOWN	put fields marked with an a											
SHUT_DOWN												
PORT_BOUNCE			0									
		PORT_BOUNCE										

4. Select **QUARANTINE** for the **Action**.

🔮 Identity Services Eng	× Cisco Identity 5	Servici 🗙 🛛 😂 Cisco Id	lentity Service 3	c   six Invent	ory   Central N= ×	sw Flow Search ( 5	itealiii 🗙 🛛 🚮 ptSeni	seBorder.di2 · ×   +	e.	-	•
← → C ▲ No	ot secure   cisco-ise.di.	ipdr/admin/#monitor/a	anc/anc_polici	es_listpage						\$	4
cisco Identity Service	is Engine Home	Context Visibility	◆ Operations	+ Policy	Administration	Work Centers	0	License Warning 🔺	Q,		•
RADIUS Threat-Cer     Policy List Endpoint A	ntric NAC Live Logs • T asignment	ACACS > Troubleshoot	t •Adaptive	Network Control	Reports		Click here to do wirele	ss setup and visibility set	up Do no	t show t	his aga
List > New Input fields marked with an o	asterisk (*) are required.										
name	ANC_QUARANTINE										
Action *	- QUARANTINE										
			Cancel	Submit	R						

- 5. Click Submit.
- 6. Navigate to **Policy > Policy Sets.**

Status Policy Set Name Description Conditions Allowed Protocols / Server Sequence Hits Actions Viewarch	cisco ident	ity Services Engine	Home + C	ontext Visibility	► Operations	* Policy	<ul> <li>Administration</li> </ul>	Work Centers		Lio	ense Warning	4	R 🕘	
Status Policy Set Name Description Conditions Allowed Protocols / Server Sequence Hits Actions Vicesrch	Policy Sets	Profiling Posture	Client Provisioning	Policy Element	ts				Click here to do w	reless set	up and visibilit	y setup D	o not show t	his aga
earch	licy Sets												Reset	Sav
Default Default policy set     Default Network Access **      Of	+ Status	Policy Set Name	Des	cription	Co	nditions			Allowed Protocols	/ Server :	Sequence	Hits	Actions	Vie
🕗 Default Default policy set Default Network Access *** + 84 🗘	earch						-							
- 6							+							
Result Sav	Ø	Default	Def	ult policy set					Default Network Acc	ess	•• +	94	¢	3
													Reset	5.14

- 7. Click the > arrow next to the default policy set.
- 8. Expand the Authorization Policy Global Exceptions section.
- 9. Click the + plus sign to add a new policy.
- 10. Click the + plus sign under **Conditions.**
- 11. Select the field **Session ANCPolicy.**
- 12. Select the quarantine action you just created for the Attribute value.

	uly Services Engine Hume + Ce	UNICAL VALUES	<ul> <li>Operato</li> </ul>	The second s	* Address	Work Centers	License Warring 🔺		0 ×	
Library			Editor							
Sear	ch by Name			Session ANG	Policy				0.	
•		🛛 ଧ 🕈	ĥ	Equals	•	ANC_QUARANTINE	-	ш		
8	AD_Domain_Admin	Ø		Set to 'is not'			Duplicate	Sav		
	BYOD_is_Registered	0								
	Catalyst_Switch_Local_Web_Authenticat	0				+ (New (AND OR				
	Compliance_Unknown_Devices	Ø								
8	Compliant_Devices	Ø								
	Domain Admins	0							1	

- 13. Click Use.
- 14. Select the **Deny Access** profile; the profile selected here will be applied to the machine when the machine is added to the quarantine group.
- 15. Select Quarantined\_Systems for Security Groups.

Policy Set	entity Services Engine Home s Profiling Posture Client Prov		Administration     Work Centers	License Warning A     Click here to do wireless setup and visibility setu	P. O	_
* Authoriza	tion Policy - Global Exceptions (1)					
+			Results			
	atus Rule Name	Conditions	Profiles	Security Groups	Hits	Action
Search						
1 0	Quarantine	E Session ANCPolicy EQUALS ANC_QUARA	TINE Cisco_Temporal_Onboard	Quarantined_Systems * *	+	0
Authoriza	tion Policy (2)					
					Reset	Sa

- 16. Click Save.
- 17. In the SMC web console, click **Monitor > Users.**

Dashboards Monitor	Analyze Job	s Config	ure	Deploy				80	0 De	sktop Clien
Jsers (1)										
Current Filters	Users									
inside Hosts	Sorted by overall sev	verity 📵								
Clear All	Cuser Name	Sessions	¢ CI	\$п	‡ RC	\$ C&C	¢ EP	≎ DS	≎ DT	‡ DH
Filter Results By:	Administrator	1/34								
	0									
RFC 1918 (1) Select Multiple	Previous 1	Next								

18. Select a user to quarantine.

→ C ▲ Not secure   192.168.	1.150/lc-landing-page/smc.ht	ml#/userentity/Administra	tor			\$	9.4
7 days		ت ط					
Command & Control							
7 days	Devices & Ses						
Exploitation	Host	50:56:b2:8c:ad Name Group	Location	Count	Device Type: Micro Start	End	
7 days	192868.8.102 (	· Catch /	AI .8. RFC 1918	34	8/8/19 9:25 AM	* Current	
DDoS Source							
7 days							
DDoS Target							
7 days							

## 19. Click a host to quarantine.

	/Servic: X   🗰 Inventory   Central III X 😥 Host Report   Stealth X 💆 ptSenseBorder.di2 X   🕂	- 0	1
Loadion: RFC 1918 First Seen: Last Seen: Policies: Inside MAC Address: 00:50:56:152:8c:ad (V/Aware, Inc.) ISE ANC Policy: Ege Top Security Events for 192.168.8.102 No events were found. If you are sure this result is incorrect. Users & Sessions MAC Address: MAC Vendor: Device Type: 05:05:60:23:8c:ad VV/Ware, Inc. Microsoft-	1#/host/192.168.8.102	0.4	5
No events were found. If you are sure this result is incorrect, Users & Sessions MAC Address: MAC Vendor: Device Type: 00:50:56:b2:8c:ad VMware, Inc. Microsoft-	192.168.8.102		
MAC Address: MAC Vendor: Device Type: 00:50:56:b2:8c:ad VMware, Inc. Microsoft-	ct your Stealthwatch administrator.	i)	
	plication Traffic External External	ы ::	
User Start End Administrator 8/8/19 9:25 AM ★ Current	splication Total % Sent Ratio Received 7-day Trend 24-hour Trend ere are no application traffic details to display		

- 20. Click Edit next to ISE ANC Policy.
- 21. From the drop down, select the quarantine action you created earlier.

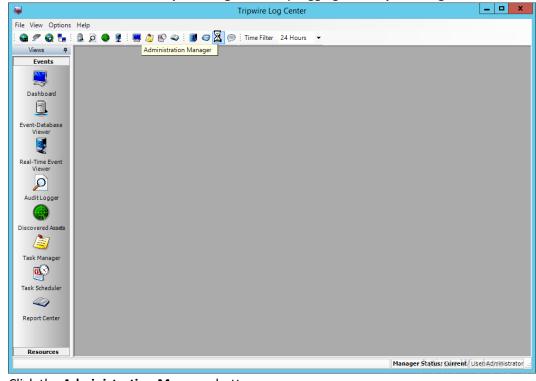
<ul> <li>Sector Sciences (Sector)</li> </ul>	on of the second second second second	eren an		sw_inventory Central M_×	🧐 Host Report   Stealth 🗙	ptSenseBorder.di2	×   +			
	g ANC polic		page/smc.html#/host/192	× 192.168.8.102				Ŕ	•	1
		ISE cluster for this host	: 192.168.8.102							
ISE	Username	MAC	ANC Policy							
cisco-ise	Administrator	00:50:56:B2:8C:AE	ANC_QUARAN $\lor$							
				atch administrator.		Sourc	e (0)	Target (0)		
				ic			nternai	External		
				I % Sent	Ratio Received	7-day Trend	24-hou	r Trend		
		Close	Save	ution traffic details to	display					

#### 22. Click Save.

23. This will apply the quarantine action to the machine.

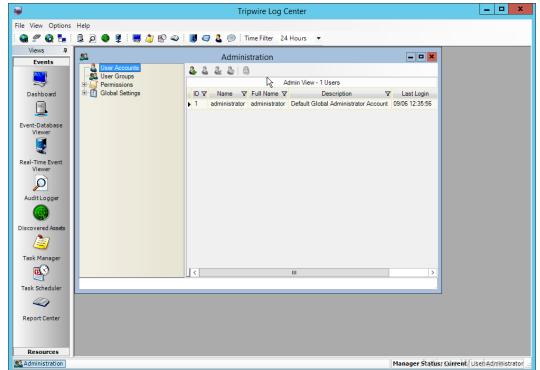
# 2.17 Integration: Tripwire Log Center and Tripwire Enterprise

1. Create a user account in **Tripwire Log Center** by logging into **Tripwire Log Center Console.** 



2. Click the Administration Manager button.

3. Click User Accounts.



- 4. Click the **Add** button.
- 5. Enter the details of the user.

🕹 Ado	d New User
Username	tweuser
Settings	
Full name	
Description	
Authentication method	Tripwire Log Center
Password	
Password Verify	
	Add Cancel

- 6. Click Add.
- 7. Double-click the user account.

P	Manager Permiss	ions	🛃 Audit	Logger Permission	ns
	🚨 User Groups		n 🥃 Permissions	s 🧻 Database F	Permissio
Full name					
Description Email					
Phone			✓	$\searrow$	
Phone Authentication	n		¥		
Valid IP's					
Auth method	d Tripwire Lo	g Center 🔍 🗸			
External Us	er				
Account is	Disabled 🗌				

8. Click the **Permissions** tab.

2	I	Edit User - twe	euser	
🙎 User I	lame tweuser			
P	Manager Permissions	Q	Audit Logger Permissions	
📰 General	🚨 User Groups 🚯	Information	Permissions 📑 Database Pe	rmission
S S				
Name		Descrip	tion	
			R	
			.0	
ОК	Cancel			

- 9. Click Edit list of permissions.
- 10. Select Databases.

5	Permissions for: twe	user 📃 🗖 🗙
Permissions Admin Admin Admin Admin Admin Admin Audit Logger Scheduler Scheduler Report Center Amic Ticket Center RealTime Event Viewer API Discovered Assets	Enabled Name View System Databas	Description Allows the user to view the System Database dat
OK Cancel		

11. Check the box next to View System Database.

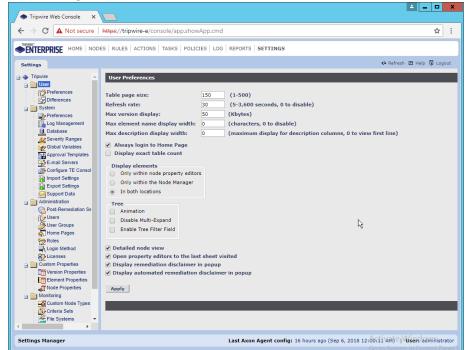
#### 12. Select API.

5	P	ermissions for: tweu	iser 📃 🗖 🗙
Permissions Admin Admin Admin Admin Admin Resource Addit Logger Task Manager Constant Scheduler Constant Misc Constant Resource Addit Logger Constant	Enabled	Name	Description Allows the user to connect using the REST API.
OK Cancel			

13. Check the box next to Allow REST API Logon.

2	Edit User - tweuser
User Name tweus	er
Manager Per	
🧱 General 🧏 User Gr	roups 🚯 Information 🚽 Permissions 🗐 Database Permissions
🈼 🍒	
Name	Description
View System Database	Allows the user to view the System Database data.
Allow REST API Logon	Allows the user to connect using the REST API.
	L3
OK Cano	cel

- 14. Click OK.
- 15. Click OK.
- 16. Log in to the Tripwire Enterprise web console.
- 17. Click Settings.

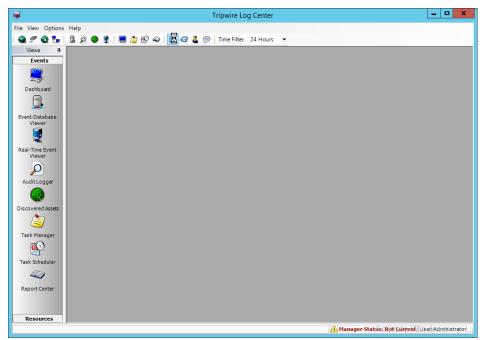


18. Go to System > Log Management.

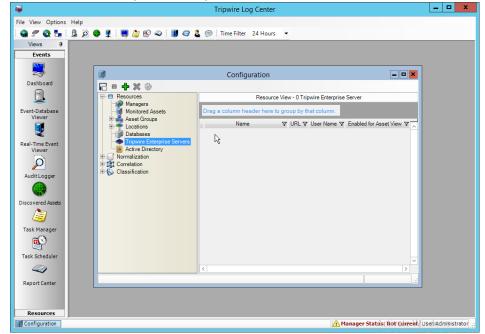
- 19. Check the box next to Forward TE log messages to syslog.
- 20. Enter the hostname and port of the Tripwire Log Center server. The default port is 1468.
- 21. Check the box next to Allow TE to use information from Tripwire Log Center.
- 22. Enter the **service address** like this: https://arcsight-cons.di.ipdr:8091/tlc, replacing the **hostname** with the hostname of your **Tripwire Log Center** server.
- 23. Enter the account information of the account just created for Tripwire Log Center.
- 24. You can use **Test Connection** to verify that the connection is working.

← → C ▲ Not secure	https://tripwire-e/console/app.showApp.cmd	☆
	S   RULES   ACTIONS   TASKS   POLICIES   LOG   REPORTS   SETTINGS	
Settings		🔂 Refresh 🖸 Help 🕅 Logo
<ul> <li>Tripwire</li> <li>User</li> <li>Differences</li> <li>Differences</li> <li>Differences</li> <li>System</li> <li>Dratasse</li> <li>Goutasse</li> <li>Goutas</li></ul>	Log Hanagement Preferences   Porward TE log messages to syslog  Transport protocol: CC  Host: arcsight-cons.dl.ipdr Port: 1468  Test Connection   Apply    Log Hanagement Preferences  Test Connection  Test Connection  Test Connection	
Settings Manager	Last Axon Agent config: 16 hours ago (Sep 6, 2018 12:00	

- 25. Click **Apply** when finished.
- 26. Go back to the Tripwire Log Center Console.



- 27. Click Configuration Manager.
- 28. Click Resources > Tripwire Enterprise Servers.



- 29. Click Add.
- 30. Enter a name for the server.
- 31. Enter the URL of the TE server.

32. Enter the **name** of a user account on the TE server. The account must have the following permissions: create, delete, link, load, update, view.

•	Tripwire Enterprise X
Name	Tripwire
Base URL	https://tripwire-e.di.ipdr
Username	tlcadmin
Passphrase	
Use this ser	ver for Asset View
Cryptograp	phic Protocols
SSL 3	TLS 1.0 TLS 1.1 TLS 1.2
	✓ Tripwire Enterprise Server connection successful.
	Test Connection Save Cancel

33. Click Save.

# 2.18 Integration: Symantec ICA and ArcSight ESM

This section describes the integration of Symantec ICA and ArcSight ESM, to import data from ArcSight into ICA for analysis. For the purposes of this build, we did not use ArcSight Logger, a tool which provides a web Application Programming Interface (API) for other applications. Because of this, the standard integration between ICA and ESM was unavailable. However, it is still possible to import Comma-Separated Values (CSV) files exported from ArcSight into ICA, and we will detail the process below. There are a few things to note when doing this import:

- On the version of Symantec ICA we are using, it is required to replace empty fields in the CSV with NULL. This may be unnecessary in future updates.
- The CSV file should be in a location accessible to the ICA server. You can replace this file with a new CSV file on a daily basis, and Symantec ICA has the capability to import the new data.
- The following integration details how to do it for a subset of fields on Active Directory logging events, but the process can be expanded for your organization's needs.

# 2.18.1 Export the CSV File from ArcSight Console

- 1. In ArcSight Console, find a connector which you wish to import events from. Right-click it, and select **Create Channel with Filter.**
- 2. In the channel, apply any filters desired.

Navigator d' ? ×	Viewer							đ
Decourses and the set of the set	Untitled Active Channel 1							
Resources Packages Use Cases								
🖉 Connectors Ctrl+Alt+E 🔻	Active Channel:						Total Events: 528	8
		08:32:25 POT				Very High	: 0	
Shortcuts 🗆		windows-ad"				Medium		
	Inline Filter: No Filter					Low	: 487	
🗄 🌅 Connectors	Verified Rules: No Rule					Very Low		
🗄 🦾 Shared	Radar							
All Connectors								
ArcSight Administration     Site Connectors								
AMP Connectors								
CEF collector(numing)	0							
- Cisco AMP(running)	Manager Receipt Time 1 1	1End Time ©	Name 🗢	Attacker Address	Target Address 🖨	Priority C	Device Vendor ©	
🔗 FileZila Logs(running)	25 Oct 2019 10:31:19 PDT	25 Oct 2019 10:31:13 PDT	An account was looged off.		172.23.122.229	1	Microsoft	
- 🤣 Glasswall Connector(down)	25 Oct 2019 10:31:15 PD1		Software Protection Platform Service			3	Microsoft	
- 🤣 Glasswall Inbound SMTP Analy		25 Oct 2019 10:31:08 PDT	Software Protection Platform Service			3	Microsoft	
🧭 Glasswall Inbound SMTP(down	ENOLUTION IN THE PLAN		25 Oct 2019 10:31:08 PDT Im Service				Microsoft	
- 🕺 Glasswall Logging Connector(c	25 Oct 2019 10:31:04 PDT	25 Oct 2019 10:31:01 PDT	Device connection down		192.168.81.56		ArcSight	
Glasswall Logging Connector( Classwall Logs(down)	25 Oct 2019 10:31:04 PDT 25 Oct 2019 10:30:43 PDT 25 Oct 2019 10:30:43 PDT	25 Oct 2019 10:31:01 PDT 25 Oct 2019 10:30:38 PDT	Device connection down Software Protection Platform Service		192. 168. 81. 56	3	ArcSight Microsoft	
Gasswall Logging Connector(o     Gasswall Logs(down)     Gasswall Management Service	25 Oct 2019 10:31:04 PDT 25 Oct 2019 10:30:43 PDT 25 Oct 2019 10:30:43 PDT 25 Oct 2019 10:30:43 PDT	25 Oct 2019 10:31:01 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:30:38 PDT	Device connection down Software Protection Platform Service Software Protection Platform Service		192.168.81.56	1	ArcSight Microsoft Microsoft	
Gasswal Logging Connector( Classwal Logs(down) Gasswal Management Service Gasswal MultiConnector(dow	25 Oct 2019 10:31:04 P07 25 Oct 2019 10:30:43 P07 25 Oct 2019 10:30:43 P07 25 Oct 2019 10:30:43 P07 25 Oct 2019 10:30:43 P07	25 Oct 2019 10:31:01 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:30:38 PDT	Device connection down Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service		192.168.81.56	3	ArcSight Microsoft Microsoft Microsoft	
Gasswall Logging Connector(u     Gasswall Loggidown)     Gasswall Mangement Service     Gasswall MatioConnector(down     Gasswall Service Logs(down)	25 Oct 2019 10:31:04 POT 25 Oct 2019 10:30:43 POT	25 Oct 2019 10:31:01 PDT 25 Oct 2019 10:30:38 PDT	Device connection down Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service		192.168.81.56	3 3 3	ArcSight Microsoft Microsoft Microsoft Microsoft	
Gasowal Logging Connector(     Gasowal Log(down)     Gasowal Log(down)     Gasowal MubiConnector(dow     Gasowal Service Log(down)     Clasowal Service Log(down)     FLC-Systap-Deemon(numing)	25 Oct 2019 10:31:04 PDT 25 Oct 2019 10:30:43 PDT 25 Oct 2019 10:30:23 PDT	25 Oct 2019 10:31:01 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:30:20 PDT	Device connection down Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Connector Raw Event Statistics			3 3 3 3 2 3 3 3 3 3 3 3	ArcSight Microsoft Microsoft Microsoft Microsoft ArcSight	
Gasswall Logging Connector(u     Gasswall Loggidown)     Gasswall Mangement Service     Gasswall MatioConnector(down     Gasswall Service Logs(down)	25 Oct 2019 10:31:04 POT 25 Oct 2019 10:30:43 POT 25 Oct 2019 10:30:23 POT 25 Oct 2019 10:30:23 POT 25 Oct 2019 10:30:25 POT	25 Oct 2019 10:31:01 PDT 25 Oct 2019 10:30:38 POT 25 Oct 2019 10:39:15 POT	Device connection down Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Connector Raw Event Statistics A logen was attempted using exploit c.		192. 168.81.50	1 3 3 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3	ArcSight Microsoft Microsoft Microsoft Microsoft ArcSight Microsoft	
Gasonal Logaing Connector( Gasonal Analysis of the Gasonal MultiConnector (dwo Gasonal MultiConnector (dwo Gasonal Service Logaidown) TLC-Systap-Deamor(nurning) Liburbu Canet(dwon)	25 Oct 2019 10:31:04PDT 25 Oct 2019 10:30:43PDT 25 Oct 2019 10:30:57PDT 25 Oct 2019 10:30:57PDT 25 Oct 2019 10:39:57PDT	25 Oct 2019 10:31:01 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:39:21 FPDT 25 Oct 2019 10:29:15 PDT 25 Oct 2019 10:29:15 PDT	Device connection down Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Connector Raw Event Statistics			3 3 3 3 2 3 3 3 3 3 3 3	ArcSight Microsoft Microsoft Microsoft Microsoft ArcSight	
Gasonal Loging Connectory     Gasonal Loging Connectory     Gasonal Management Service     Gasonal Management Service     Gasonal Management Service     Gasonal Management Connectory     Connectory     Connectory     Connectory     Connectory     Worknows Connectors Service     Windows Connectors Service     Windows Connectors Service	25 Oct. 2019 10:31:04 PDT 25 Oct. 2019 10:30:43 PDT 25 Oct. 2019 10:30:43 PDT 25 Oct. 2019 10:30:43 PDT 25 Oct. 2019 10:30:43 PDT 25 Oct. 2019 10:30:23 PDT 25 Oct. 2019 10:30:25 PDT 25 Oct. 2019 10:30:53 PDT 25 Oct. 2019 10:29:53 PDT	25 Oct 2019 10:31:01 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:39:21 FPDT 25 Oct 2019 10:29:15 PDT 25 Oct 2019 10:29:15 PDT	Device connection down Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Connector Rew Yeard Statistics A logon was attempted using explicit c. Special privileges assigned to new logon Characteria twis stresset of a groupe for		192. 168.81.50 172.23.122.229	3 3 2 3 3 1 3 3 3 3 1 3 3 3 3 3 3 3 3 3	ArcSight Microsoft Microsoft Microsoft ArcSight Microsoft Microsoft Microsoft	
Gesonal Loging Corrector     Gasonal Loging Corrector     Gasonal MultiCondent     Gasonal MultiCondentor (down     Gasonal MultiCondentor (down     Corrector (down)     Corrector (down)     Gutor Connector (down)     Windows Connector Server (d     Windows UP systematics     Windows UP systematics     Windows UP systematics	25 Oct 2019 10:31:04 PD 25 Oct 2019 10:30:43 PD 25 Oct 2019 10:30:23 PD 25 Oct 2019 10:30:23 PD 25 Oct 2019 10:30:35 PD 25 Oct 2019 10:25:31 PD 25 Oct 2019 10:25:31 PD 25 Oct 2019 10:25:31 PD	25 Oct 2019 10:31:01 POT 25 Oct 2019 10:30:38 POT 25 Oct 2019 10:30:38 POT 25 Oct 2019 10:30:38 POT 25 Oct 2019 10:30:38 POT 25 Oct 2019 10:30:39 POT 25 Oct 2019 10:30:29 POT 25 Oct 2019 10:39:15 POT 25 Oct 2019 10:39:15 POT	Texte connection down Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Connection Platform Service Software Protection Platform Service Software Protection Platform Service Connection Rew Fernt Statistics A logon was attempted using explicit. A sopont was attempted using explicit. A account was to topped off.		192, 168, 81, 50 172, 23, 122, 229		ArcSight Microsoft Microsoft Microsoft ArcSight Microsoft Microsoft Microsoft	
Gasonal Logring Connectory     Gasonal Logring Connectory     Gasonal Management Service     Gasonal Management Service     Gasonal Management Service     Gasonal Management Connectory     Guto Conneco	25 Oct. 2019 10:31:04 PDT 25 Oct. 2019 10:34:04 PDT 25 Oct. 2019 10:30:43 PDT 25 Oct. 2019 10:30:45 PDT	25 Oct 2019 10:31:01 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:30:38 PDT 25 Oct 2019 10:30:30 PDT 25 Oct 2019 10:30:29 PDT 25 Oct 2019 10:29:15 PDT	Texas connection durin Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Connector Rew Event Statistics A logon was attempted unargeoptier c. Sobela privileges assigned to new logon Annecent texasersed by dogod chi An account was logged off. Device connection up		192. 158. 81. 50 172. 23. 122. 229 1228 412 422 423 192. 158. 81. 56		ArcSight Microsoft Microsoft Microsoft ArcSight Microsoft Microsoft Microsoft Microsoft	
Gesonal Loging Corrector     Gasonal Loging Corrector     Gasonal MultiCondent     Gasonal MultiCondentor (down     Gasonal MultiCondentor (down     Corrector (down)     Corrector (down)     Gutor Connector (down)     Windows Connector Server (d     Windows UP systematics     Windows UP systematics     Windows UP systematics	25 CH 2019 20:31:04 FDT           25 CH 2019 20:31:04 FDT           25 CH 2019 20:30:44 FDT           25 CH 2019 20:30:45 FDT           25 CH 2019 20:30:45 FDT           25 CH 2019 20:30:40 FDT           25 CH 2019 20:30:40 FDT           25 CH 2019 10:30:31:47 FDT           25 CH 2019 10:30:31:37 FDT           25 CH 2019 10:30:33 FDT	25 04 2019 10.3160 P07 26 04 2019 10.3063 P07 26 04 2019 10.3063 P07 25 04 2019 10.3063 P07 25 04 2019 10.3063 P07 25 04 2019 10.3063 P07 26 04 2019 10.2013 P07 26 04 2019 10.2015 P07 26 04 2019 10.2015 P07 25 04 2019 P07 25 04 2019 P07 25 04 2019 P07 25 04 2019 P07 25 04 2015 P07 25 04 2015 P07 25 04	Device connection dwim Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Connection Rew Event Statistics A logon was attempted using exploit c. Soppal privleges assigned to new logon An account was logged off. Device connection up An account was logged off.		192. 158. 81. 50 172. 23. 122. 229 17. 24. 12. 25. 25 192. 158. 81. 56 192. 158. 81. 56		ArcSight Microsoft Microsoft Microsoft ArcSight Microsoft Microsoft ArcSight ArcSight Microsoft ArcSight Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	
Gasonal Logring Connectory     Gasonal Logring Connectory     Gasonal Management Service     Gasonal Management Service     Gasonal Management Service     Gasonal Management Connectory     Guto Conneco	25 Oct 2019 10:31:04 PO 25 Oct 2019 10:33:04 PO 25 Oct 2019 10:33:44 PO 25 Oct 2019 10:33:44 PO 25 Oct 2019 10:33:44 PO 25 Oct 2019 10:33:44 PO 25 Oct 2019 10:32:45 PO	15 od. 2019         10.5.1.0.1           15 od. 2019         10.5.1.0.1           15 od. 2019         10.5.0.3.8           15 od. 2019         10.5.0.3           15 od. 2019         10.5.0.3           15 od. 2019         10.5.2.1           15 od. 2019         10.2.2.1           15 od. 2019         10.2.2.3           15 od. 2019         10.2.2.3	Device connection dwim Software Protection Platform Service Software Protection Platform Service Special privleyers assigned to new logon Intercent private assigned to new logon An account was successfully logard on: An account was successfully logard on:	192, 168, 2, 122	192, 158, 81, 50 172, 23, 122, 229 172, 23, 125, 225 192, 168, 81, 56 192, 168, 81, 56 192, 168, 81, 56 192, 168, 81, 56		ArcSynt Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft ArcSynt Microsoft ArcSynt Microsoft Microsoft Microsoft	
Gasonal Logring Connectory     Gasonal Logring Connectory     Gasonal Management Service     Gasonal Management Service     Gasonal Management Service     Gasonal Management Connectory     Guto Conneco	32         0.02, 2013         0.03, 10, 4100           25         0.02, 2013         0.03, 1431         0.03           26         0.02, 2013         0.03, 1431         0.03           26         0.02, 2013         0.03, 1431         0.03           26         0.02, 2013         0.03, 1431         0.03           26         0.02, 2013         0.03, 1431         0.03           26         0.02, 2013         0.03, 1431         0.03           26         0.02, 2013         0.03, 1431         0.03           26         0.02, 2013         0.03, 1431         0.03           26         0.02, 2013         0.03, 1431         0.03         0.03           26         0.02, 2013         0.03, 1431         0.03         0.0	15         0.12         0.13         0.01         0	Device connection dwim Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Software Protection Platform Service Connection Rew Event Statistics A logon was attempted using exploit c. Soppal privleges assigned to new logon An account was logged off. Device connection up An account was logged off.	192, 168, 2, 122	192, 168, 81, 50 172, 23, 122, 229 192, 168, 81, 56 192, 168, 81, 56 192, 168, 81, 56		ArcSight Microsoft Microsoft Microsoft ArcSight Microsoft Microsoft ArcSight ArcSight Microsoft ArcSight Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	

- 3. When finished, right-click any of the events in the channel, and select **Export > Events in Channel....**
- 4. Enter a name for the CSV file for File name:.
- 5. Select All in Channel for Rows:.
- 6. For **Columns:** either select a custom field-set to determine the output columns or leave the default selected.

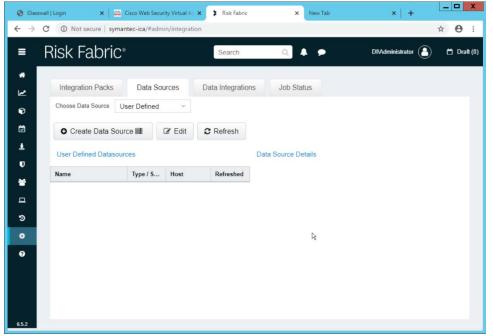
*	Export Events	x
Save in:	🛾 Desktop 🔹 📦 📂 🎞 -	
Adminis Adminis This PC This PC This PC This PC Screens screens export aca-arcs File <u>n</u> ame: Files of type	s k hots ight ight-noextra ad-events-export	OK
Export Data (	Intions	
Rows:	All in channel     Selected rows only	
Columns:	exporterset	
Destination:	Local CSV File	-
		Help

7. Click OK.

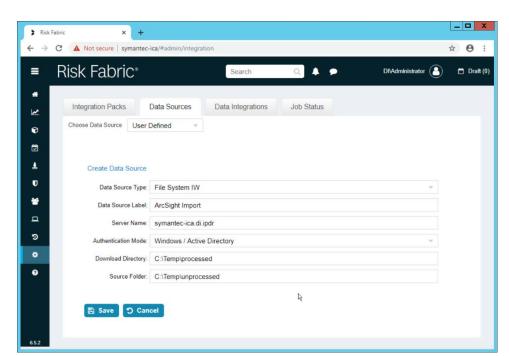
8. Move the file to the desired location for ICA to collect. (Ensure that if required for your version of Symantec ICA, all empty fields are replaced with "NULL") For the purposes of this demonstration, we moved it to *C:\Temp\unprocessed* on the Symantec ICA server.

## 2.18.2 Import the CSV File to Symantec ICA

- 1. On the Symantec ICA web console, navigate to Gear Icon > Integration.
- 2. Click the Data Sources tab.

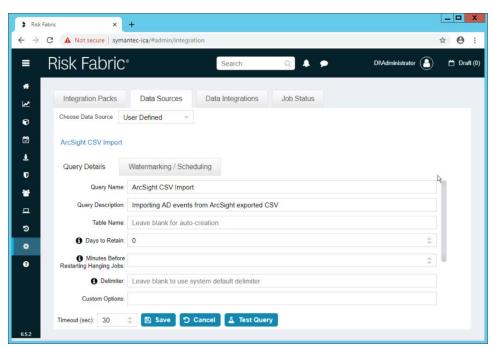


- 3. Select User Defined for Choose Data Source.
- 4. Click Create Data Source.
- 5. Select File System IW for the Data Source Type.
- 6. Enter a name for the data source for Data Source Label.
- 7. Enter the hostname of the Symantec ICA server for Server Name.
- 8. Select Windows/Active Directory for the Authentication Mode.
- 9. Enter the location for the downloaded CSV file for **Download Directory** (relative to the Symantec ICA server).
- 10. Enter the location for the CSV file to be downloaded from for **Source Folder** (relative to the Symantec ICA server).



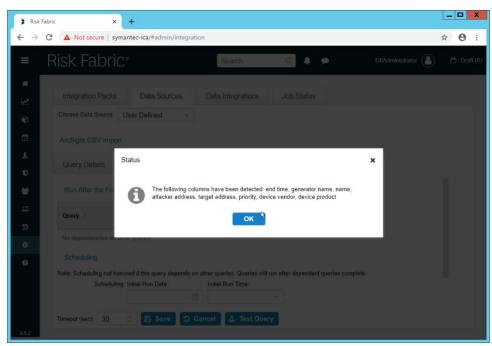
Risk Fabric <sup>®</sup>			Search	۹.	P DI	Administrator	٥
Integration Packs	Data Sourc	ces C	Data Integratio	ns Job Status			
Choose Data Source	ser Defined						
Create Data Sour	ce 🗃 🛛 🖉	Edit	C Refresh				
User Defined Datasour	ces			Data Source Details			
Name	Type / S	Host	Refreshed	Data Source Label:			
ArcSight Import	1.1	symantec-i		Server Name: Authentication Mode: Username:	symantec-ica.di.ipdr Windows		
	Edit D	ata Source 🗃 Query 🗃		Password: Download Directory:			
		5		Download Directory.	C. tremp processed		

- 12. Right-click the newly created data source and select Create Query.
- 13. Enter a Query Name and Query Description.



- 14. If you specified the **Source Folder** correctly, you will see the CSV file listed.
- 15. Check the box next to any CSVs to import.

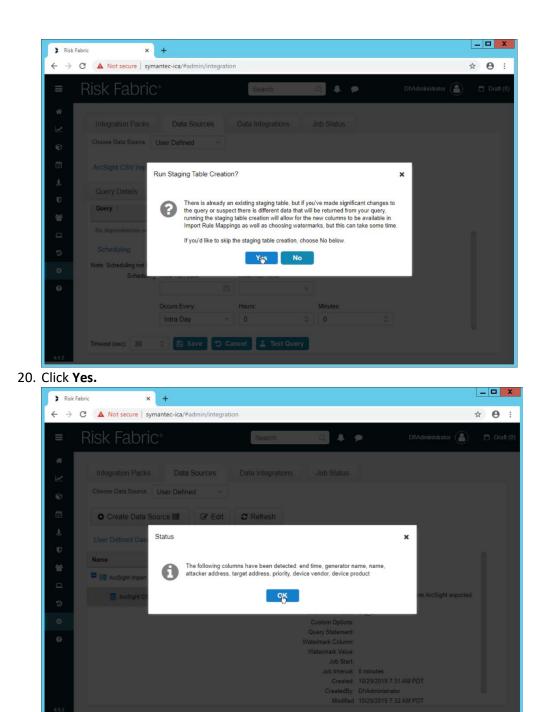
	Risk Fabric		Search Q 🌲 🗩	DI\Administrator	🗎 Di
*	Integration Packs		Pata Sources Data Integrations Job Status		
•	Choose Data Source	lser [	efined 👻		
Ċ	ArcSight CSV Import				
Ŧ		18/-4			
U	Query Details	vvat	rmarking / Scheduling		
*	Minutes Before Restarting Hanging Jobs:			\$	
-	O Delimiter:	Lea	ve blank to use system default delimiter		
ອ	Custom Options:				
•		Selec	which files to import into the table:		
0		Ø	Path	Modified Date	
		V	C:\Temp\unprocessed\export_withnulls.csv	10/28/2019 8:27 AM	
			Note: The destination table will be completely replaced with the latest spreadsheet da		
			Note: The destination table will be completely replaced with the latest spreadsheet da	la	200



## 17. Click OK.

18. If desired, set a schedule for this import.

∎ F	Risk Fabric		Search	(	2 🔺 🗩		DIVAdministrator	) 🖻	) (
*	Integration Packs	Data Sources	Data Integration		ob Status				
~		User Defined	Data Integration	13 01	ob Oldius				
ଚ ଅ									
<b>7</b>	ArcSight CSV Import								
U	Query Details	Watermarking / Scheo	duling						
	Query 1		D						
<b>-</b>	No dependencies on oth	er queries						1	
ອ	Scheduling								
•	and the second se	ored if this query depends or Initial Run Date:	Initial Run Time:	s will run atte	er dependent quer	ies complete.			
?		Ê	1	Ŧ					
		Occurs Every:	Hours:		Minutes:				
		Intra Day	0	\$	0	÷			



21. Click **OK.** 

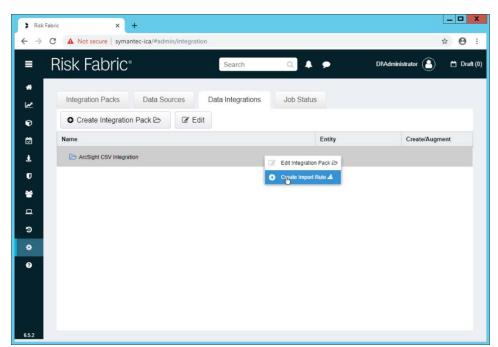
# 2.18.3 Create a Mapping between ArcSight events and Symantec ICA

1. Navigate to the **Data Integrations** tab.

#### \_ 🗆 X Risk Fabric × + → C ③ Not secure | symantec-ica/#admin/integration ☆ **0** : ÷ **Risk Fabric**\* DIVAdministrator Search . . 🗂 Draft (0) \* Integration Packs Data Sources Data Integrations Job Status M Create Integration Pack 🗷 Edit Ø Entity Create/Augment ً Name 1 U e Э ٠ ?

- 2. Click Create Integration Pack.
- 3. Enter a Name and Description.

🕽 Risk Fa	abric	× +			_ <b>_ X</b>
$\leftrightarrow$ $\rightarrow$	C A Not secure	symantec-ica/#admin/integra	tion		☆ <b>0</b> :
	Risk Fab	ric®	Search	o. 🔺 🗩	DIAdministrator 🦲 📋 Draft (0
*	Integration Par	cks Data Sources	Data Integrations	Job Status	
0	Create Integr	ation Pack			
€	Name:	ArcSight CSV Integration			
U	Description:	Arcsight CSV Import			
*					
₽					
ত					
•					
Ø					
6.5.2					Save Cancel



- 5. Right-click the newly created Integration Pack, and select Create Import Rule.
- 6. Enter a Name and Description.

Risk I	Fabric	× +			
$\leftarrow \   \rightarrow$	C A Not secure	symantec-ica/#admin/integr	ation		± 0 :
=	Risk Fab	oric"	Search	۹ 🔺 🗩	DIVAdministrator 🙆 🛱 Draft (0)
*	Integration Pa	acks Data Sources	Data Integrations	Job Status	
₽ 2	Create Impo	ort Rule			
L.	Name:	ArcSight AD Event Import	Rule		
Ū	Description:	For importing AD login ev	ents		
, and the second					
ອ					
۰					
0					
6.5.2					Sales Cancel

- 7. Click Save.
- 8. Right-click the newly created Import Rule and select Create Import Rule Mapping.
- 9. Enter a Name for the mapping.

- 10. Enter a **Description**.
- 11. Select the **Data Source** created earlier.
- 12. Select the Query created earlier.
- 13. Select **EP Events** for the **Entity Type** (or explore other Entity Types that may better match the events you are importing).

> Risk	Fabric × +				_ <b>D</b> X
<b>←</b> →	C A Not secure   symantec-ica/#admin	/integration		07	☆ <b>0</b> :
=	Risk Fabric®	Search	Q 🔺 🗩	DIVAdministrator	苗 Draft (0)
*	Integration Packs Data Sour	ces Data Integrations	Job Status		
Ð	Edit Import Rule Mapping: ArcSight Al	D Event Import Rule Mapping			
٢	Mapping Name:	ArcSight AD Event Import Rule	Mapping		
Ł	Description:	AD events			
U	Data Source:	ArcSight Import	*		
*	Query:	ArcSight CSV Import			
묘	Risk Fabric Processing Watermark:				
ອ	Run Intra-Day:	No	*		
٠	Run Order:	0	÷		
0	Entity Type:	EP Events	*		
	Update Pre-Process Table:	Yes	·*:		
	• Create Entities:	Yes	- 195		
	Save Cancel				
6.5.2					

- 14. Below, the **Entity Column** refers to the target field in ICA to which a field is being mapped. Map event fields from the CSV to fields in the Entity Column.
- 15. For example, **EventDate** in ICA corresponds directly to the **End Time** in ArcSight, so we select that value directly as a **Source Column** for the mapping.

	C A Not secure   symantec	ice - uoniniprincipliation		07 1	\$ <b>0</b>
=	Risk Fabric <sup>®</sup>	Search	a 🔺 🗩	DIVAdministrator	📋 Dra
*	Integration Packs	Data Sources Data Integr	ations Job Status		
•	Edit Import Rule Mapping:	ArcSight AD Event Import Rule Ma	apping		
2					
Ł	Required Fields				
U	Entity Column	Туре	Value	Default Value	
<b>*</b>	EventDate datetime	Source Column v	End Time 👻		
ือ	SourceEventID nvarchar(50)	Formula	Convert unique 5 🕼 🕷 👻		
¢ 9	Optional Fields				
	Search:				
			Value	Default Value	

- 16. Formulas can be used to transform columns in the CSV to something more specific in ICA. Because we did not export an event ID to our CSV file, we use a formula to create a hash of the End Time and use that as the ID.
- 17. All **Required Fields** must be mapped, and you will likely also want to map some optional fields to make useful data.

Risk Fabric®	Search		DI\Administrator ( 🔒	🗂 Draft
NISK LADITC	Jean			
Integration Packs Da	ta Sources Data Integr	ations Job Status		
Create Import Rule Mapping				
EventObjectTypeName 2 nvarchar(254)	Source Column 🖤		*	
Create and Associate Event Ac	tivity Type			
Entity Column	Туре	Value	Default Value	
EventActivityTypeName 2	Source Column *		*	
nvarchar(254)				
Create and Associate Event Ru	ıle			
Entity Column	Туре	Value	Default Value	
EventRuleName 🖾	Source Column		-	-

#### 18. Click **Save** when finished.

19. Navigate to the Job Status tab.

isk Fabric			×	+				
> C	A 1	lot sec	<mark>cure</mark>   syman	tec-ica/#admin/ii	ntegration			야 ☆
Ri	sk	Fa	abric⁼		Search	Q. 🔺	🗩 DI	NAdministrator 😩 🛱
					11			
-	Integ	Iration	Packs	Data Source	es Data Integra	ations Job Status		
		5 <sub>n</sub>		· -				A
				atus				View Details
		N	Enabled	Status	Last Run Outcome	Last Run	Last Run Duration	Next Run
	۲	R	yes	Not running	O Failed	10/29/2019 7:57:00 AM	00:00:01	10/29/2019 11:00:00 AM
	¥	R	yes	Not running	Succeeded	10/29/2019 7:57:00 AM	00:10:44	10/30/2019 12:15:00 AM
	<b>e</b>	R	yes	Not running	Succeeded	10/29/2019 7:57:00 AM	00:00:05	
	_							
	-							
	~	<	Page	1 of 1 )	» C			Displaying records 1 - 3 of 3

20. Select all the jobs and click **Start.** This is to force a refresh of the ICA processing, allowing the data from the CSV to be imported immediately.

## 2.18.4 View ArcSight Events in the Analyzer

1. Once the processing jobs are finished, navigate to the Analyzer.

>	C A Not secur	e   symantec-ica/#/analyzer/\	view/8879870D-672D-4	FFD-9859-A8F2E0E28	A9B	☆ <b>0</b> :
=	Risk Fat	oric	Search	Q	Diva	udministrator 😩 🛱 Draft (
*	Views  Filter Filter Filter Filter Views Ago		harts 💌		۵	Field List  Search
€ 101	Total	Details		Þ	¢ ⊒ 2 ×	Measures     AD Group     AD Group     AD Group First Detected
Ł		EP Event Date Ra	Action Taken	EP Event Date	EP Event Count	AD Group Last Detecte     AD Organizational Unit     AD Organizational Unit
U 2		2-7 Days Ago 2-7 Days Ago	A logon was attemp An account failed to		2	AD Organizational Unit     Action Plan     Action Plan Assigned To
ม จ •		<pre></pre>	1 of 1 >	≫ D Rec	ords: 1 - 15   Total: 15	Action Plan Closed By     Action Plan Closed Dal     Action Plan Closed Dal     Action Plan Committed     Action Plan Due Date     Action Plan Expected 0
0	Details					Action Plan Requested
	View Configuration	n: arcsight (Analyzer View)				
	Measures	Rows	Columns		Fitters	Details
	EP Event Count	EP Event Date Range	()			Action Taken EP Event Date

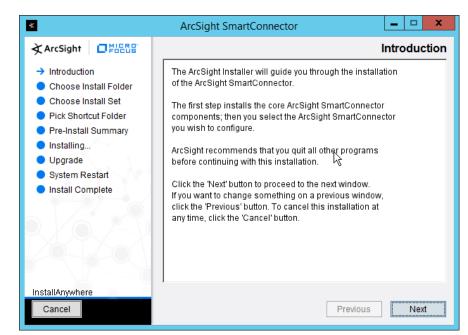
2. Drag mapped columns (from the import rule mapping you created) from the list on the right to view them in the analyzer.

# 2.19 Integration: Micro Focus ArcSight and Tripwire

This section will detail the forwarding of logs from **Tripwire Log Center** to **Micro Focus ArcSight**. This will forward **Tripwire IP360** and **Tripwire Enterprise** logs to **ArcSight**, assuming those logs are being collected by **Tripwire Log Center**.

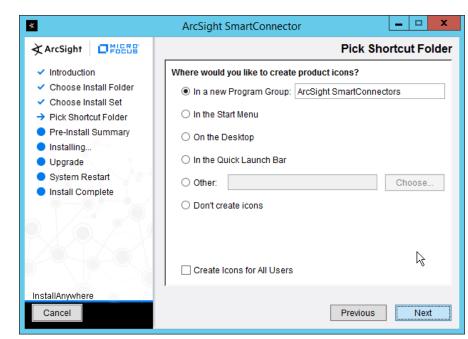
## 2.19.1 Install Micro Focus ArcSight

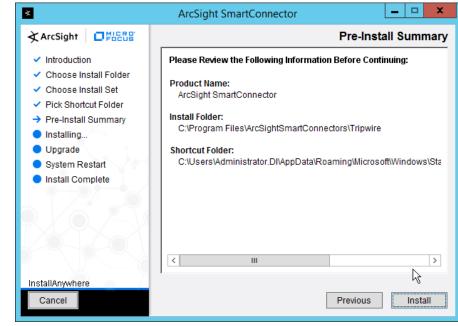
1. Run ArcSight-7.9.0.8084.0-Connector-Win64.exe on any server except the one running Tripwire Log Center.



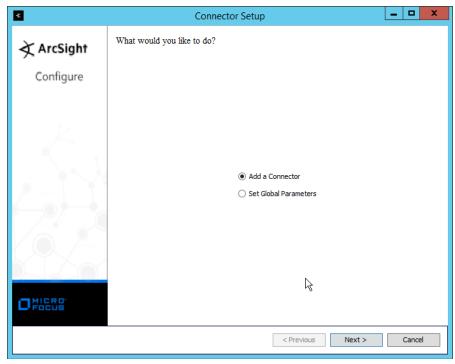
*	ArcSight SmartConnector
ArcSight	Choose Install Folder
<ul> <li>Introduction</li> <li>Choose Install Folder</li> <li>Choose Install Set</li> <li>Pick Shortcut Folder</li> <li>Pre-Install Summary</li> <li>Installing</li> <li>Upgrade</li> <li>System Restart</li> <li>Install Complete</li> </ul>	Please choose the installation folder. It is recommended that you choose the folder name according to the device that you want to connect to, for example /ciscoids or /checkpointng. If you are upgrading from a previous version, please select the folder where the ArcSight SmartConnector is currently installed.         Where Would You Like to Install?         C:\Program Files\ArcSightSmartConnectors\Tripwire         Restore Default Folder       Choose
InstallAnywhere Cancel	Previous Next

3. Enter C:\Program Files\ArcSightSmartConnectors\Tripwire.





- 5. Click Install.
- 6. Select Add a Connector.



- 7. Click Next.
- 8. Select Syslog Daemon.

*	Connector Setup	
ArcSight	Select the connector to configure	
Configure		
	Type Eyslog Daemon	<b>v</b>
	R	
	< Previous Next >	Cancel

- 10. Enter a port for the daemon to run on.
- 11. Select Raw TCP for Protocol.

*	Connector Setup	X
ArcSight	Enter the parameter details	
Configure		
	Network Port     514       IP Address     (ALL)       Protocol     Raw TCP       Forwarder     false	
		;
	< Previous Next > Ca	incel

- 12. Click Next.
- 13. Select ArcSight Manager (encrypted).

×	Connector Setup	- 🗆 X
ArcSight	Enter the type of destination	
Configure		
	<ul> <li>ArcSight Manager (encrypted)</li> </ul>	
k.	ArcSight Logger SmartMessage (encrypted)	
	<ul> <li>ArcSight Logger SmartMessage Pool (encrypted)</li> </ul>	
	O CEF File	
	O Event Broker	
	◯ CEF Syslog	
	CEF Encrypted Syslog (UDP)	
	○ CSV File	
	◯ Raw Syslog	
		$\searrow$
MICRO		
FOCUS		
	< Previous Next >	Cancel

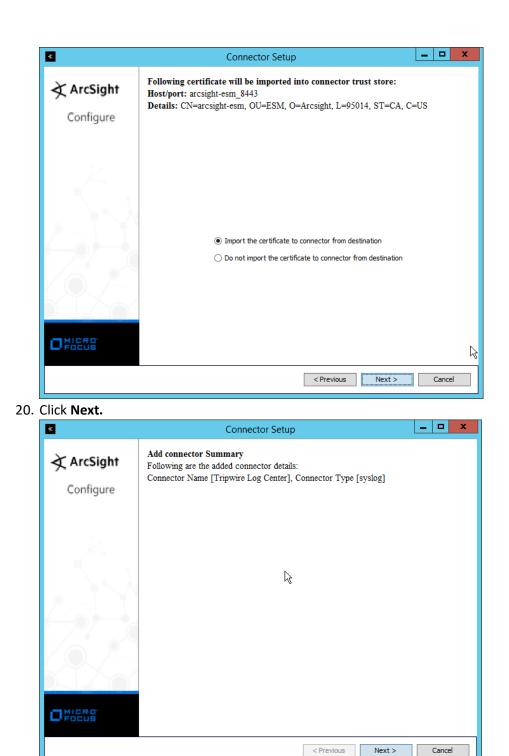
- 14. Click Next.
- 15. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.

*	Co	nnector Setup			-		x
<b>∢ ArcSight</b> Configure	Enter the destination para	meters					
	Manager Hostname Manager Port User Password AUP Master Destination Filter Out All Events Enable Demo CA	arcsight-esm 8443 administrator false false false			 		
			< Previous	Next >		Cancel	I

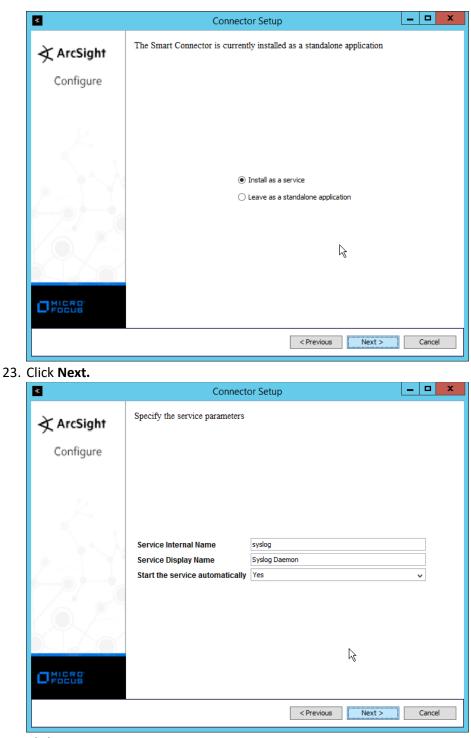
- 16. Click Next.
- 17. Enter identifying details about the system (only **Name** is required).

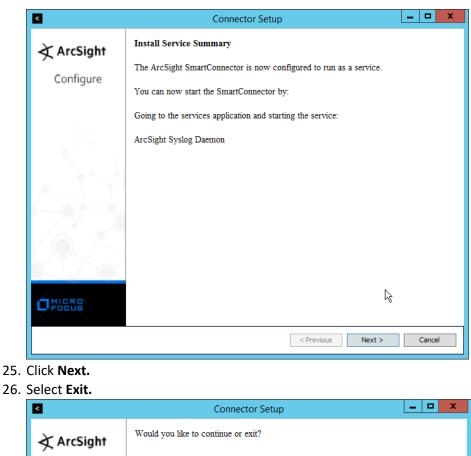
*		Connector Setup		_	
ArcSight	Enter the connec	tor details			
Configure					
	Name Location DeviceLocation Comment	Tripwire Log Center			
				L <sub>2</sub>	
			< Previous	Next > (	Cancel

- 18. Click Next.
- 19. Select Import the certificate to connector from destination.

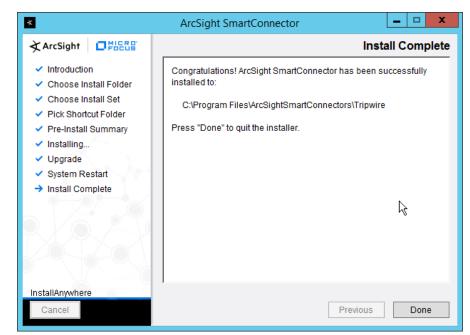


- 21. Click Next.
- 22. Select Install as a service.





Connector Setup	
Would you like to continue or exit?	
• Exit	
k	
< Previous Next > Cancel	
	(⊂ Continue

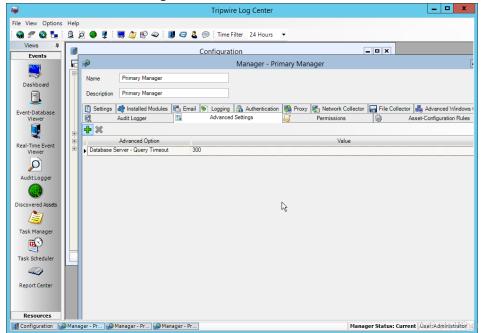


- 28. Click Done.
- 29. Open the Tripwire Log Center Console.
- 30. Go to the Configuration Manager.

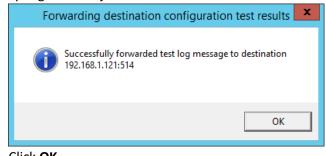
. 😽		Tripwire Log Center	_ <b>□</b> ×
File View Options Help			
ି 🍓 🖉 🧕 💺 🚊 🍳	\varTheta 💈 🗒 🖄 🚱 🥥 🗄	🥪 🚨 🍥 🗄 Time Filter 24 Hours 🔻	
Views 4		Configuration	- <b>x</b>
Events			
	Resources	Resource View - 1 Managers	
Dashboard	Managers Monitored Assets	Drag a column header here to group by that column.	
	Asset Groups	ID V Name V IP V Status V Description	Y
Event-Database	Locations     Databases	1 Primary Manager arcsight-cons.di.ipdr Current Primary Manager	¥ ^
Viewer	Tripwire Enterprise Servers		
12-+1 2	Vormalization		
Real-Time Event	Correlation Classification		
Viewer	512551102101		
$\mathbf{P}$			
AuditLogger			
Discovered Assets			
Task Manager			
<b>6</b> 3		<	×
Task Scheduler			
		<u>"</u>	
~			
Report Center			
Resources			
Configuration		Mana	ger Status: Current Öser: Administrator

- 31. Select Resources > Managers.
- 32. Double-click the Primary Manager.

33. Click the Advanced Settings tab.



- 34. Click the **Add** button.
- 35. In the Advanced Option box select Log Message Forwarding Destinations.
- 36. In the **Value** box next to it, type *<ip\_address>:<port>:tcp* with the **IP address** and **port** of the syslog daemon just created.



37. Click **OK**.

Views #			Configura	tion			x		
Events	<b>F P</b>			Manager - Pri	mary Mar	nager			- <b>-</b> ×
Dashboard	Database :			d Settings	Proxy	Permissions Value	tor 🕞 File Colle	ctor 🛃 Advanced Window Asset-Configuration Rule	
covered Assets					ß				
		<u>О</u> К	<u>C</u> ancel						

- 38. Click OK.
- 39. Restart the Tripwire Log Center Manager.

## 2.20 Integration: Micro Focus ArcSight and Cisco AMP

This section will detail the collection of logs from Cisco AMP's REST APIs using Micro Focus ArcSight.

## 2.20.1 Create API Credentials for ArcSight to access AMP

1. On the Cisco AMP web console, log in and navigate to Accounts > API Credentials.

ashboard Analysis V Outbreak Control V Management V Accounts V	Search	Q
PI Credentials	O View API	Documentatio
A Delete	+ New API Credential	
□ ⊞ ← ArcSight	Last used: 2019-06-17 15	:17:04 UTC
□		

- 2. Click New API Credential.
- 3. Enter a name for the credential.
- 4. Select Read-only.

Application name	ArcSight Connector	
Scope	Read-only	
	Read & Write	

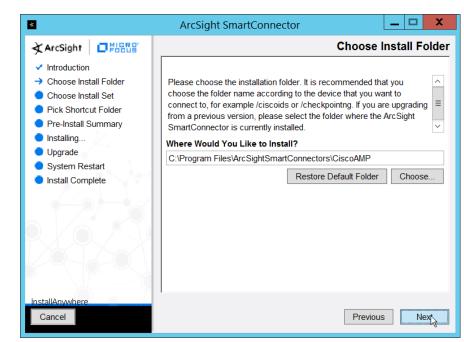
- 5. Click Create.
- 6. This will direct you to a page with an **ID** and **API Key.** Keep track of these, as you will need them in the setup for the ArcSight Connector, and Cisco AMP may not let you view them again.

# 2.20.2 Install Micro Focus ArcSight

1. Run ArcSight-7.9.0.8084.0-Connector-Win64.exe on any server.

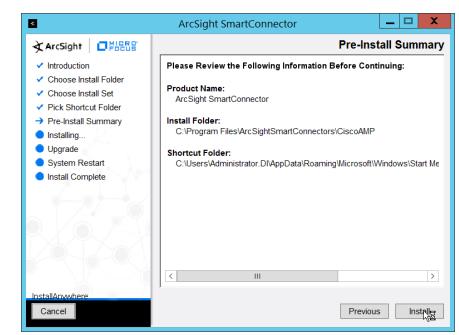
*	ArcSight SmartConnector
ArcSight	Introduction
<ul> <li>Introduction</li> <li>Choose Install Folder</li> <li>Choose Install Set</li> <li>Pick Shortcut Folder</li> <li>Pre-Install Summary</li> <li>Installing</li> <li>Upgrade</li> <li>System Restart</li> <li>Install Complete</li> </ul>	<ul> <li>The ArcSight Installer will guide you through the installation of the ArcSight SmartConnector.</li> <li>The first step installs the core ArcSight SmartConnector components; then you select the ArcSight SmartConnector you wish to configure.</li> <li>ArcSight recommends that you quit all other programs before continuing with this installation.</li> <li>Click the 'Next' button to proceed to the next window. If you want to change something on a previous window, click the 'Previous' button. To cancel this installation at any time, click the 'Cancel' button.</li> </ul>
InstallAnywhere Cancel	Previous Next

- 2. Click Next.
- 3. Enter C:\Program Files\ArcSightSmartConnectors\CiscoAMP.



X	ArcSight SmartConnector
¢ArcSight □₩₩₽₽₽	Pick Shortcut Folder
<ul> <li>Introduction</li> <li>Choose Install Folder</li> <li>Choose Install Set</li> <li>Pick Shortcut Folder</li> <li>Pre-Install Summary</li> <li>Installing</li> <li>Upgrade</li> <li>System Restart</li> <li>Install Complete</li> </ul>	Where would you like to create product icons? <ul> <li>In a new Program Group: ArcSight SmartConnectors</li> <li>In the Start Menu</li> <li>On the Desktop</li> <li>In the Quick Launch Bar</li> <li>Other:</li> <li>Choose</li> <li>Don't create icons</li> </ul> Create Icons for All Users
Cancel	Previous

5. Click Next.



- 6. Click Install.
- 7. Select Add a Connector.

*	Connector Setup	-		x
र्रे ArcSight	What would you like to do?			
Configure				
	<ul> <li>Add a Connector</li> <li>Set Global Parameters</li> </ul>			
O MICRO'				
	< Previous Next >		Cance	

- 8. Click Next.
- 9. Select ArcSight FlexConnector REST.

*	Connector Setup 📃 🗖	X
ArcSight	Select the connector to configure	
Configure		
	Type ArcSight FlexConnector REST	
	< Previous Next Cance	el

- 10. Click Next.
- 11. Enter Cisco\_AMP for the Configuration File.
- 12. Enter https://api.amp.cisco.com/v1/events?start\_date=\$START\_AT\_TIME for the **Events URL.** (Note: You can see the Cisco AMP REST API documentation for more information on how to formulate this URL for things other than events.)
- 13. Enter the username and password from the credential generated on Cisco AMP in <u>Section</u> 2.20.1.

×	Connec	tor Setup	_ 🗆 X
ArcSight	Enter the parameter details		
	Proxy Host Proxy Port Proxy User Name Proxy Password Configuration File Events URL Authentication Type User Name Password OAuth2 Client Properties File Refresh Token	Cisco_AMP https://api.amp.cisco.com/v1/events? Basic	start_date=\$START
			₽ ₽
		< Previous	Next > Cancel

- 14. Click Next.
- 15. Select ArcSight Manager (encrypted).

*	Connector Setup	- 0	x
À ArcSight	Enter the type of destination		
Configure			
	<ul> <li>ArcSight Manager (encrypted)</li> <li>ArcSight Logger SmartMessage (encrypted)</li> <li>ArcSight Logger SmartMessage Pool (encrypted)</li> <li>CEF File</li> <li>Event Broker</li> <li>CEF Syslog</li> <li>CEF Encrypted Syslog (UDP)</li> <li>CSV File</li> <li>Raw Syslog</li> </ul>		
	k,		
	< Previous Next >	Cano	el

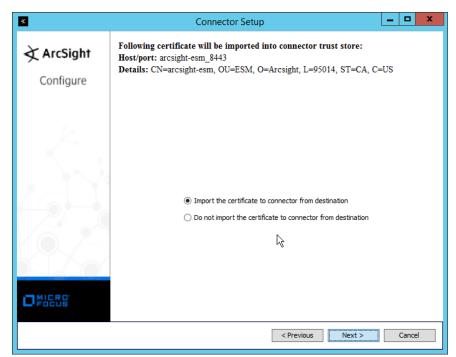
- 16. Click Next.
- 17. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.

*	Со	nnector Setup			-		x
ArcSight Configure	Enter the destination para	meters					
	Manager Hostname Manager Port User Password AUP Master Destination Filter Out All Events Enable Demo CA	arcsight-esm 8443 administrator false false false				-	
			< Previous	Next >		Cancel	I

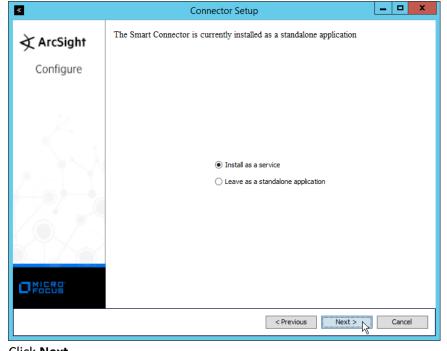
- 18. Click Next.
- 19. Enter identifying details about the system (only Name is required).

8		Connector Setu	р	
ArcSight Configure	Enter the connec	ctor details		
	Name Location DeviceLocation Comment			
			< Previous Next	> Cancel

- 20. Click Next.
- 21. Select Import the certificate to connector from destination.



- 22. Click Next.
- 23. Click Next.
- 24. Select Install as a service.

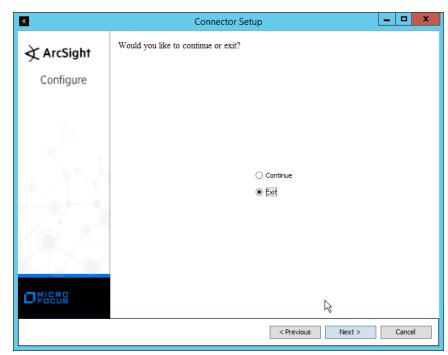


25. Click Next.

26. Enter a service name and display name.

*	Connector Setup	
✓ ArcSight Configure	Specify the service parameters	
	Service Internal Name         sdkrest           Service Display Name         ArcSight FlexConnector REST           Start the service automatically         Yes	v
	k	
	< Previous Next >	Cancel
Click Next.		
*	Connector Setup	
ArcSight	Install Service Summary The ArcSight SmartConnector is now configured to run as a service.	
Configure	You can now start the SmartConnector by:	
Configure	You can now start the SmartConnector by: Going to the services application and starting the service: ArcSight ArcSight FlexConnector REST	
Configure	Going to the services application and starting the service:	
Configure	Going to the services application and starting the service:	
Contigure	Going to the services application and starting the service:	Cancel

29. Select Exit.



#### 30. Click Next.

*	ArcSight SmartConnector
ArcSight	Install Complete
<ul> <li>Introduction</li> <li>Choose Install Folder</li> <li>Choose Install Set</li> <li>Pick Shortcut Folder</li> <li>Pre-Install Summary</li> <li>Installing</li> <li>Upgrade</li> <li>System Restart</li> <li>Install Complete</li> </ul>	Congratulations! ArcSight SmartConnector has been successfully installed to: C:\Program Files\ArcSightSmartConnectors\WindowsUDP Press "Done" to quit the installer.
Cancel	Previous Done

31. Click Done.

### 2.20.3 Create a Parser for Cisco AMP REST events

1. Ensure that the ArcSight connector service is not running.

- Create a text file located at <ARCSIGHT\_HOME>/current/user/agent/flexagent/Cisco\_AMP.jsonparser.properties. (Note: Replace Cisco\_AMP with the name used for "Configuration File" during setup.)
- 3. Use the following text to parse some basic information such as the IP, the type of event, and links to Cisco AMP's more detailed descriptions of the event.

```
trigger.node.location=/data
token.count=6
token[0].name=id
token[0].type=String
token[0].location=id
token[1].name=timestamp
token[1].type=String
token[1].location=date
token[2].name=event_type
token[2].type=String
token[2].location=event_type
token[3].name=hostname
token[3].type=String
token[3].location=computer/hostname
token[4].name=external_ip
token[4].type=IPAddress
token[4].location=computer/external_ip
token[5].name=links
token[5].type=String
token[5].location=links
event.deviceReceiptTime=__createOptionalTimeStampFromString(timestamp,"y
yyy-MM-dd'T'HH:mm:ssX")
event.destinationAddress=external_ip
event.destinationHostName=hostname
event.name=event_type
event.message=links
event.deviceCustomString1=id
event.deviceCustomString1Label=__stringConstant("AMP Event ID")
```

4. This parser will allow for details of Cisco AMP events to be shown in ArcSight. Custom parsers are a functionality of ArcSight. For more information on the creation of custom parsers, please see the *ArcSight FlexConnector Developer's Guide* as well as the *FlexConnector REST Developer's Guide*. You can start the service for these changes to take effect.

#### 2.21 Integration: Micro Focus ArcSight and Cisco ISE

This integration will briefly detail how to send logs to an ArcSight syslog collector from Cisco ISE. Please see <u>Section 2.18</u> (under integrating Tripwire & ArcSight) for instructions for setting up an ArcSight syslog

collector. If a server is already configured, you do not need to install a new one—use the address of that server to which to forward logs.

## 2.21.1 Configure Cisco ISE to Forward Logs

 In the Cisco ISE web client, navigate to Administration > System > Logging > Remote Logging Targets.

duale Identity Services Engine	Home Context Visibility	Operations + Po	icy • Adminis	stration Vork Centers	🕦 License Warning 🛕 🤇	
System Identity Management	Network Resources     Device Por	tal Management px	Grid Services	Feed Service + Threat Cen	lick here to do wireless setup and visibility setup Do	not st
Deployment Licensing + Certificat	and the second se	Upgrade + Backup	& Restore + Ad	Imin Access + Settings		
.ocal Log Settings	Remote Logging Targets					
Remote Logging Targets					Selecte	d 0   To
Logging Categories	/ Edit - Co Duplicate	X Delete			Show All	
Vessage Catalog	Name	<ul> <li>IP Address</li> </ul>	Port	Туре	Description	Sta
Debug Log Configuration	O LogCollector	127.0.0.1	20514	UDP SysLog	Syslog Target for Log Collector	8
	O ProfilerRadiusProbe	127.0.0.1	30514	Profiler SysLog	Syslog Target for Profiler RADIUS Probe	-
Collection Filters	O SecureSyslogCollector O TCPLogCollector	127.0.0.1	6514 1468	Secure SysLog TCP SysLog	Secure Syslog Collector TCP SysLog collector	0

- 2. Click Add.
- 3. Enter a name for Name.
- 4. Enter the hostname of the ArcSight syslog collector server for Host/IP Address.
- 5. Select **TCP SysLog** for Target Type. (Ensure that your syslog collector server is configured to use TCP).
- 6. Enter **514** or the port used on the syslog server.
- 7. Enter 8192 or a custom message size limit for Maximum Length.
- 8. Ensure that Status is set to Enabled.

the Identity Services Engine		
		Varning 🔺
	Network Resources      Device Portal Management pxGrid Services     Feed Service     Threat Cen Click here to do wireless setup and v	visibility setup (
Deployment Licensing Certifica	es -Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings	
Local Log Settings	Remote Logging Targets List > New Logging Target	
Remote Logging Targets	Logging Target	
Logging Categories	* Name ArcSight Target Type TCP SysLog *	
Message Catalog	Description Status 🛃 Enabled 👻	
Debug Log Configuration	* Host / IP Address backupserv.di.ipdr	
Collection Filters	* Port 514 (Valid Range 1 to 65535)	
	Facility Code LOCAL6	
	* Maximum Length 8192 (Valid Range 200 to 8192)	
	Include Alarms For this Target	
	Buffer Messages When Server Down	
	Enable Server Identity Check	
	Buffer Size (MB) 100 (Valid Range 10 to 100)	
	Reconnect Timeout (Sec) 30 (Valid Range 30 to 120)	
	Cancel	
lick Submit.		
lick <b>Submit.</b>		-
🚭 Identity Services Engine 🛛 🗙		
<ul> <li>§ Identity Services Engine</li> <li>X</li> <li>↔ O</li> <li>▲ Not secure   h</li> </ul>	tps://cisco-ise.di.jpdr/admin/#administration/administration_system/administration_system_logging/remote_log	¢
Ventity Services Engine X ★ → C. ▲ Not secure   h A Not secure   h A Not secure   h	tps://cisco-ise.di.ipdr/admin/#administration/administration_system_logging/remote_log           Home         Context Visibility         Operations         Policy         Administration         > Work Centers         ()         License V	
Solution     Identity Services Engine     X     A     C     A     Not secure     h     A     Not secure     h     Aentity Services Engine     System     Hentity Management	tps://cisco-ise.dl.ipdr/admin/#administration/administration_system_logging/remote_log           Home         Context Visibility         Operations         > Policy         > Mont Centers         It knows of the second seco	☆ Varning ▲
Ventity Services Engine X ★ → C. ▲ Not secure   h A Not secure   h A Not secure   h	tps://cisco-ise.dl.ipdr/admin/#administration/administration_system_logging/remote_log           Home         Context Visibility         Operations         > Policy         > Mont Centers         It knows of the second seco	☆ Varning ▲
<ul> <li>Identity Services Engine</li> <li>×</li> <li>→ C. ▲ Not secure   Model</li> <li>Identity Services Engine</li> <li>• System</li> <li>Identity Management</li> <li>Deployment</li> <li>Licensing</li> <li>• Certifica</li> </ul>	tps://cisco-ise.di.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log         Home       Context Visibility       Operations       > Poley       > Administration       > Work Centers       I License V         * N       *	☆ Varning ▲
Solution     Identity Services Engine     X     A     C     A     Not secure     h     A     Not secure     h     Aentity Services Engine     System     Hentity Management	tps://cisco-ise.dl.ipdr/admin/#administration/administration_system_logging/remote_log           Home         Context Visibility         Operations         > Policy         > Mont Centers         It knows of the second seco	☆ Varning ▲
Kentity Services Engine     ×	type://cisco-ise.di.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log tome  Context Visibility  Operations  Policy  Administration  Work Centers  License V  Context Visibility  You have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  No  Kes  N	☆ Varning ▲
<ul> <li>Identity Services Engine</li> <li>A Not secure</li> <li>Not secure</li> <li>N</li></ul>	tps://cisco-ise.di.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log         Home       Context Visibility       Operations       > Poley       > Administration       > Work Centers       I License V         * N       *	☆ Varning ▲
Identity Services Engine     X     A Not secure     Not secur	type://cisco-ise.di.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log tome  Context Visibility  Operations  Policy  Administration  Work Centers  License V  Context Visibility  You have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  No  Kes  N	☆ Varning ▲
<ul> <li>Stentity Services Engine</li> <li>→ C</li> <li>▲ Not secure</li> <li>♦ Not secure</li> <li>♥ Not secure</li> <li>♥</li></ul>	tps://cisco-ise.dl.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log tome  Context Visibility  Operations  Policy  Administration  Work Centers  License V  Context Visibility  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  No  Cest Cest Cest Cest Cest Cest Cest Ces	☆ Varning ▲
<ul> <li>♦ Identity Services Engine</li> <li>×</li> <li>→</li> <li>C</li> <li>▲ Not secure</li> <li>♦ Not secure</li> <li>♥ Output</li> <li>♥</li></ul>	type://cisco-ise.dl.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log tome Context Visibility Operations Policy Administration Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Ces No Ces Description Status Enabled  Host / IP Address Enabled	☆ Varning ▲
<ul> <li>♦ Identity Services Engine</li> <li>×</li> <li>→</li> <li>C</li> <li>▲ Not secure</li> <li>♦ Not secure</li> <li>♥ Output</li> <li>♥</li></ul>	type://cisco-ise.dl.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log tome  Context Visibility Operations Context Visibility	☆ Varning ▲
<ul> <li>♦ Identity Services Engine</li> <li>×</li> <li>→</li> <li>C</li> <li>▲ Not secure</li> <li>♦ Not secure</li> <li>♥ Output</li> <li>♥</li></ul>	tex://cisco-ise.dl.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log tome  Context Visibility Operations Folicy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou hav	☆ Varning ▲
<ul> <li>♦ Identity Services Engine</li> <li>×</li> <li>→</li> <li>C</li> <li>▲ Not secure</li> <li>♦ Not secure</li> <li>♥ Output</li> <li>♥</li></ul>	type://cisco-ise.dl.ipdfr/admin/#administration_system/administration_system_logging/remote_log tome  Context Visbility Operations Place Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connecti	☆ Varning ▲
<ul> <li>♦ Identity Services Engine</li> <li>×</li> <li>→</li> <li>C</li> <li>▲ Not secure</li> <li>♦ Not secure</li> <li>♥ Output</li> <li>♥</li></ul>	tex://cisco-ise.dl.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log tome  Context Visibility Operations Folicy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Vou hav	☆ Varning ▲
<ul> <li>♦ Identity Services Engine</li> <li>×</li> <li>→</li> <li>C</li> <li>▲ Not secure</li> <li>♦ Not secure</li> <li>♥ Output</li> <li>♥</li></ul>	type://cisco-ise.dl.ipdfr/admin/#administration_system/administration_system_logging/remote_log tome  Context Visbility Operations Place Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connecti	☆ Varning ▲
<ul> <li>♦ Identity Services Engine</li> <li>×</li> <li>→</li> <li>C</li> <li>▲ Not secure</li> <li>♦ Not secure</li> <li>♥ Output</li> <li>♥</li></ul>	tes://cisco-ise.dl.ipdfr/admin/#administration_system/administration_system_logging/remote_log tome  Context Visbility Operations Place Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Note: Address backupserv.dl.ipdr  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Note: Address backupser	☆ Varning ▲
<ul> <li>♦ Identity Services Engine</li> <li>×</li> <li>→</li> <li>C</li> <li>▲ Not secure</li> <li>♦ Not secure</li> <li>♥ Output</li> <li>♥</li></ul>	type://cisco-ise.dl.ipdfr/admin/#administration_system/administration_system_logging/remote_log tome  Context Visbility Operations Place Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Note: A term to the server server is a term to the server is a term to the server is a term to term t	☆ Varning ▲
<ul> <li>♦ Identity Services Engine</li> <li>×</li> <li>→</li> <li>C</li> <li>▲ Not secure</li> <li>♦ Not secure</li> <li>♥ Output</li> <li>♥</li></ul>	type://cisco-ise.dl.ipdfr/administration/administration_system/administration_system_logging/remote_log  tome  Context Visbility Operations Play Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?  Note: Status  Enabled  Vou have chosen to create an unsecure (TCP/UDP)  Note: Status  Enabled  En	☆ Varning ▲

10. Click Yes.

# 2.21.2 Select Logs for Forwarding

1. Navigate to System > Logging > Logging Categories.

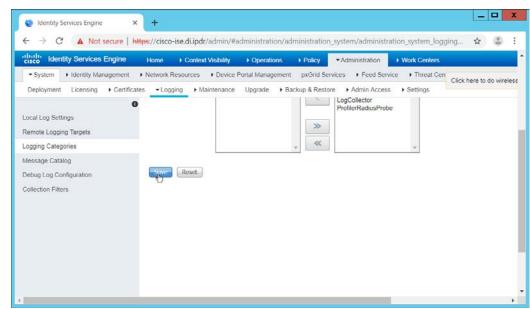
← → C ▲ Not secure   http	s://cisco-ise.di.ipdr/admin/	#administration/administration_system/admin	iistration_system_logging 😭 👶
dentity Services Engine	Home	Operations      Policy      Administration	Work Centers
▼System → Identity Management →	Network Resources + Devic	e Portal Management pxGrid Services + Feed	Service  Threat Cen Click here to do wirele
Deployment Licensing + Certificates	s → Logging → Maintenanc	e Upgrade 🕨 Backup & Restore 🕨 Admin Ac	
0	O AAA Audit	AAA Audit	LogCollector
Local Log Settings	0	Failed Attempts	LogCollector,ProfilerRadius
and a state of the second s	0	Passed Authentications	LogCollector, Profiler Radius
Remote Logging Targets	O AAA Diagnostics	AAA Diagnostics	LogCollector
Logging Categories	0	Administrator Authentication	and Authorization ArcSight
Message Catalog	0	Authentication Flow Diagnos	dics
Debug Log Configuration	0	Identity Stores Diagnostics	
	0	Policy Diagnostics	
Collection Filters	0	RADIUS Diagnostics	LogCollector
	0	Guest	LogCollector
	0	MyDevices	LogCollector
	0	AD Connector	LogCollector
	0	TACACS Diagnostics	LogCollector
	O Accounting	Accounting	LogCollector
	•	RADIUS Accounting	cryptonite,cryptonite2,Log0
	0	TACACS Accounting	LogCollector
	O Administrative and Oper	ational Audit Administrative and Operation	nal Audit LogCollector

2. Select a log file to forward to ArcSight.

#### 3. Click Edit.

cisco Identity Services Engine	Home	Visibility	Policy	Administration	Work Centers	
System      Identity Management Deployment Licensing     Certificate		Device Portal Management intenance Upgrade      Back	pxGrid Servic		<ul> <li>Threat Cen</li> <li>Settings</li> </ul>	Click here to do wirele
Local Log Settings Remote Logging Targets Logging Categories Message Catalog Debug Log Configuration Collection Filters	Logging Categor Name Log Severity Level Local Logging Targets	TY RADIUS Accounting INFO (Log level can not be changed. Available:		elected		
		SecureSyslogCollector	> c < 1	ArcSight cryptonite cryptonite2 LogCollector ProfilerRadiusProbe	*	

4. Move the ArcSight logging target you just created to the **Selected** box.



- 5. Click Save.
- 6. Repeat steps 1-5 for any log files you wish to forward to ArcSight.

## 2.22 Integration: Micro Focus ArcSight and Semperis DSP

This integration will briefly detail how to send logs to an ArcSight syslog collector from Semperis DSP. Please see <u>Section 2.18</u> (under integrating Tripwire & ArcSight) for instructions for setting up an ArcSight syslog collector. If a server is already configured, you do not need to install a new one—use the address of that server to which to forward logs.

Note: This integration requires Semperis DSP version 2.6.

## 2.22.1 Configure Semperis DSP to Forward Logs

- 1. In Semperis DSP, navigate to **Settings** > **SIEM Integration.**
- 2. Check the box next to Enable SysLog.
- 3. Under Syslog Server, enter the hostname for the ArcSight syslog collector, as well as the port.
- 4. Select TCP.
- 5. Enter a value for **Change Event Polling Frequency** based on the needs of your organization; this is how often it will poll for new logs to forward.
- 6. Under Change Event Filtering, select AD Changed Items, and Send Operation Log to SysLog. Ensure that All is selected for Partitions.
- 7. You can also select any specific **operations**, **classes**, and **attributes** to be forwarded or leave it as **All**.

6	de	Semperis				Domain: DI.IPG	R • I	Aoministrator	C LOGOUT
	Current Do DLIPDR		GENERAL	DS PROTECTOR AGENTS	PERMISSIONS	SIEM INTEGRATION			
		CHANGED	AUDIT AGENTS	AUDIT. COLLECTORS	AUDIT				
	3	ITEMS	🛃 Enable SysLog						
		DELETED ITEMS	Syslog Server						
	~		Primary Syslog Serve	er: backupserv.di.ipc	r Primary 5	vslog Port: 514	TCP O U	DP	
		CONFIGURATION PARTITION	C TLS						
	-		③ Secondary Sysio	g Server: SERVER	Sec	ondary Syslog Port 514		ICP 🚫 UDP	
		DNS	TLS						
	-		Change Event Pollin	g Frequency: 10	minutes				
	9	6PO	Change Event Filteri	ng	R				
						Include these events			
	0	REPORTS	Operations :	All (O items sele	(ted) •	AD Changed items			
			Object Classes	All (O items sele	ted) ·	Partitions	All	•	
		801	Attributes :	All (O items sele	• Det	DNS			
	245	STATUS	minutes :	No to terro see		Send Operations L	og to SysLog		
		OPERATION LOG	SAVE						
	•	SETTINGS							
ick <b>Sav</b> e	1000								
💽 S	UCC	ess							
<u> </u>									
SvsLoo	conf	iouration ha	əs been səv	ed.					
2,29									
								CL	OSE

9. Click Close.

## 2.23 Integration: Micro Focus ArcSight and Symantec Analytics

This section will first detail the forwarding of logs from **Symantec Analytics** to **Micro Focus ArcSight**. Please see <u>Section 2.18</u> (under integrating Tripwire & ArcSight) for instructions for setting up an ArcSight syslog collector. If a server is already configured, you do not need to install a new one; use the address of that server to which to forward logs.

The second part of this section will detail a further integration for ArcSight that allows ArcSight to better analyze network packets received from Symantec Analytics.

#### 2.23.1 Configure Symantec Analytics to Forward Logs

1. Log in to the Symantec Analytics web console.

= 🧿 Security Analytics		000_00
lerts		24
ashboard Summary List		
Update		
Time Range		
From: 06/27/2019 15:39:19 • To: 07/01/2019 15:39:19		
Filter by IP	0	
No Data Found	There are no alerts	
Advanced Filter		
(AND) 94 🗣 🖻	Set Up Rules for Alerts	Go to Summary Page
( <u>OR</u> ) $\nabla_{\Phi} \boxtimes_{\Phi} \boxtimes_{\star} \times$		
Add a Filter		
Apply one or more filters		
to the displayed results:		
for example, indicator~1918		

- 2. Click the **menu** icon in the top left.
- 3. Navigate to Settings > Communication.
- 4. Scroll down to the Syslog Settings section.
- 5. Select SysLog for Syslog Facility.
- 6. Enter the hostname or IP of the ArcSight syslog collector server under Server.
- 7. Enter **514** for the port.
- 8. Select **TCP** for the protocol.

Trap Servers					
Server	Port		Community	Enable Authenti	cation
	162			) •	×
add a new host					
Enable Authtrap	8				
nilog Settings					
Enable Coalescing:					
Syslog Facility:	SysLog •				
Syslog Servers:					
Servet		Port		Protocol	
backupserv.di.ipdr		514		ТСР 🔹	×
add a new host					

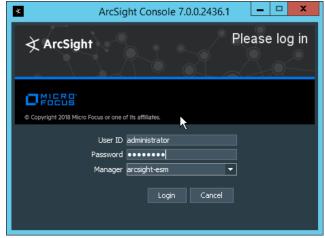
- 9. Click Save.
- 10. Click the **Advanced** tab.
- 11. Select the box under **Remote Syslog** column for any events that you wish to forward to ArcSight, for example, **System Events**, **Unclassified Events**, **Alert Events**, **Rule Events**, **Anomaly Events**.

enote Noteicacioneg				
	Local	Email	SNMP	Remote Syslog
Miscellaneous	2			
System Events	8		8	×
User Events	2	0		
Playback Events	8	0	0	
Capture Events	2			
Report Events	8			
Hardware Events	8			
Unclassified	8	0	0	2
Alert Events	8	0		×
Indexing Events	2			11 De
Enrichment Events	2			
Indicator Events	×			0
Rule Events	8		0	
Anomaly Events	2	8		

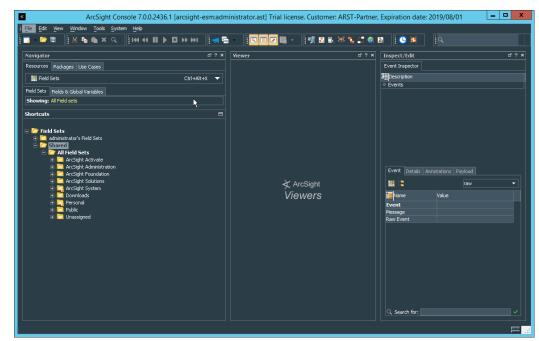
12. Click Save.

#### 2.23.2 Install Symantec Analytics Package for ArcSight

- Navigate to the ArcSight marketplace. Look for the "Blue Coat Security Analytics" package for ArcSight. It may be available here: <u>https://marketplace.microfocus.com/arcsight/content/bluecoat-security-analytics-platform</u> but not please contact your ArcSight representative to get the package. The package should be called **Blue\_Coat\_SA\_HP\_ArcSight-3.0.arb**.
- 2. Place this package on a system with ArcSight ESM Console installed.



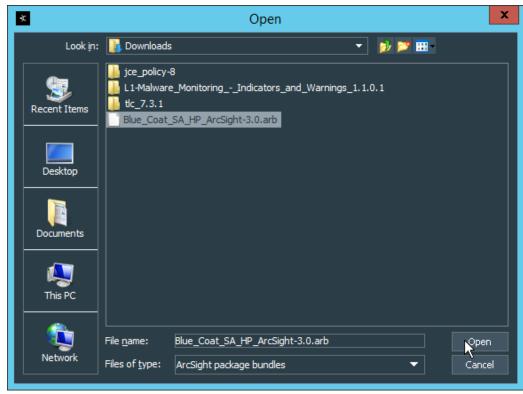
3. Log in to the ArcSight ESM Console with a user that has the privileges to install packages.



4. In the **Navigator** pane, click the **Packages** tab.

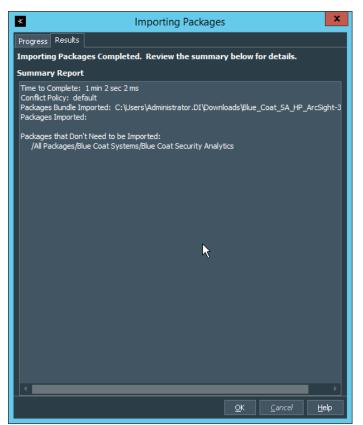
File Edit Yiew Window Tools System Help 雪 🎦 🗮 👔 🙀 🐿 🏫 🛪 🔍 🎚 [44 4 🔢 🕨 🕪 )> 1	i 🛹 🖷	I - I - I - I - I - I - I - I - I - I -	8 i 🕒 🛤 i 9
Navigator	≓?×	Viewer 6?×	Inspect/Edit e
Resources Packag		≹ ArcSight Viewers	Event Inspector  Event Details Annotations Payload  Event Control Details Annotations Payload  Event Value V

- 5. Click Import.
- 6. In the window that it opens, find and select the package you downloaded.

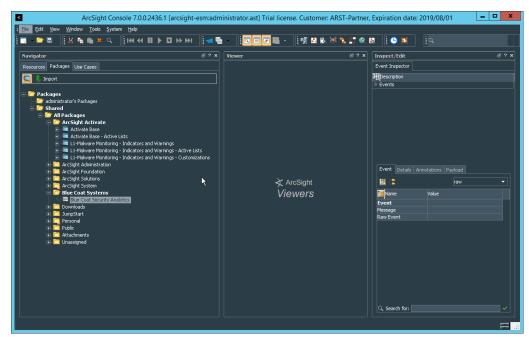


7. Click **Open.** 

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-26.



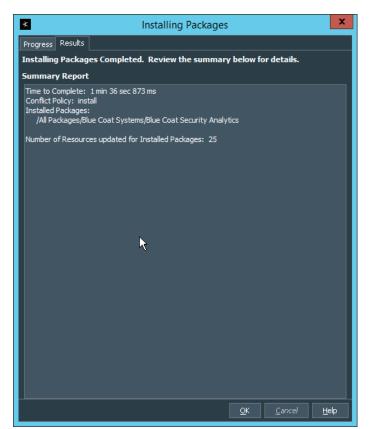
- 8. Click **OK** when the import finishes.
- 9. Under the Packages tab in the Navigator pane, navigate to Packages > Shared > All Packages > Blue Coat Systems > Blue Coat Security Analytics.



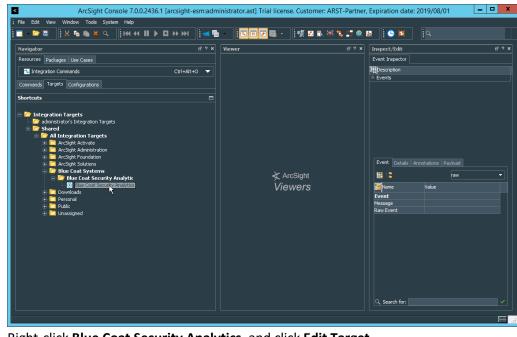
10. Right-click Blue Coat Security Analytics, and select Install Package.

All Packages/Blue	Coat Systems/Blue Coat Security Analytics
dditional requi	ired packages:
he following pack	ages will also be installed.
ackages	

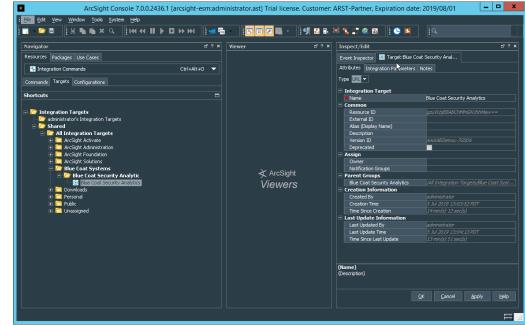
11. Click OK.



- 12. Click OK.
- 13. When this completes, you can verify that the installation was successful by the existence of a Blue Coat Systems folder when you navigate to Resources > Integration Commands > Commands > Shared > All Integration Commands.
- 14. In the **Resources** tab of the **Navigation** pane, under **Integration Commands**, select the **Targets** tab.
- 15. Navigate to Integration Targets > Shared > All Integration Targets > Blue Coat Systems > Blue Coat Security Analytic > Blue Coat Security Analytics.



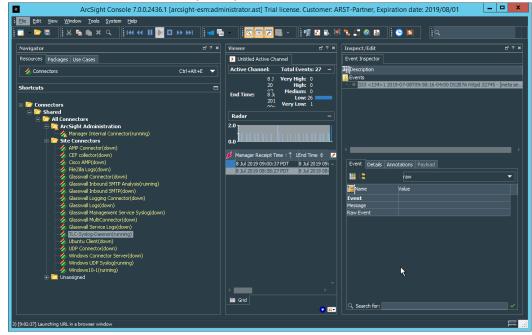
#### 16. Right-click Blue Coat Security Analytics, and click Edit Target.



- 17. Click the Integration Parameters tab.
- 18. Replace the SAHost value with the IP address of Symantec Analytics.

je Edit View Window Tools System Help					
डू <mark>// स</mark>	. 🤜 💼	🔄 🔲 🖉 🖳 👻 👯 👪 🕵	🔆 🔩 📮 🚳 📓		
Navigator	₫?×	Viewer ♂?×	Inspect/Edit		ď
Resources Packages Use Cases			Event Inspector	Target:Blue Coat Secu	rity Anal
Lintegration Commands Ctrl+Alt+C	) <b>–</b>		Attributes Integral	ion Parameters Notes	
Commands Targets Configurations			🕂 Add 🗙 Remove		
			Parameter	Туре	Value
ihortcuts			SAHost SATimeZone	text text	192.168.2.42
			SAMinutee	text	
Integration Targets           Image: Comparison of the second seco			SAStartTime	text	
Administrator's Integration Targets     Shared			SAEndTime	text	
🔄 🚝 All Integration Targets					
ArcSight Activate					
E C ArcSight Administration					
ArcSight Foundation					
🖶 🥅 ArcSight Solutions 🖹 🌽 Blue Coat Systems					
Due Coat Systems Due Coat Security Analytic		🔾 ArcSight			
Blue Coat Security Analytics		Viewers			
🗉 🥅 Downloads		VIEWEIS			
🗉 🛅 Personal					
🕀 🧮 Public					
🗈 🧰 Unassigned					
				<u>о</u> к	Cancel Apply Help

- 19. Click OK.
- 20. To verify the functionality, right-click an event in any channel, and select **Integration Commands > Blue Coat Security Analytics.**



21. Select Security Analytics Investigation.



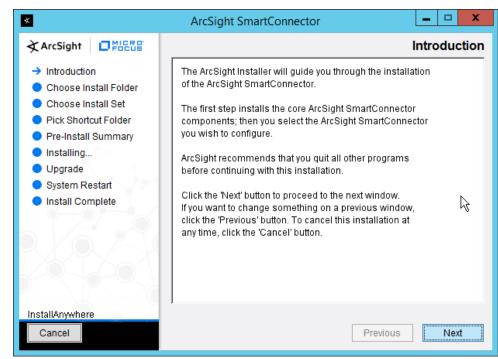
22. Click **OK.** This will open Security Analytics in the browser and perform a packet search based on the event parameters.

## 2.24 Integration: Micro Focus ArcSight and Glasswall FileTrust

**Glasswall FileTrust for Email** stores its logs in *C*:\*Logging*, on the server running the **Glasswall** services.

#### 2.24.1 Install Micro Focus ArcSight

1. Run ArcSight-7.9.0.8084.0-Connector-Win64.exe on the same server as Glasswall FileTrust.

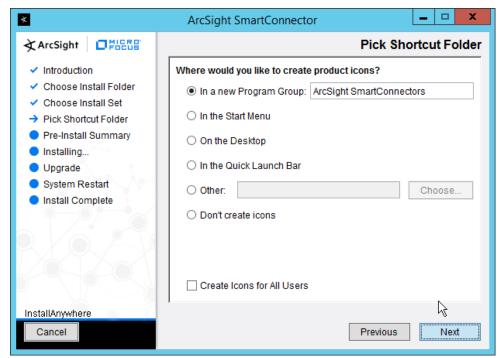


#### 2. Click Next.

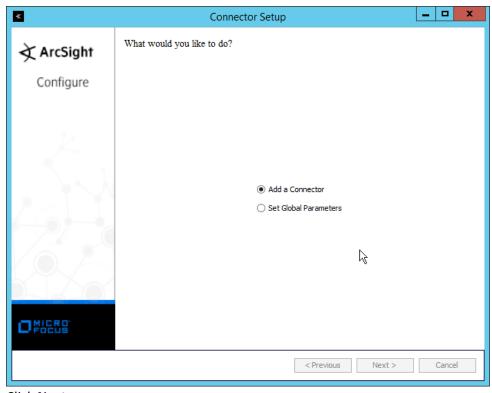
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.

*	ArcSight SmartConnector
ArcSight	Choose Install Folder
<ul> <li>Introduction</li> <li>Choose Install Folder</li> <li>Choose Install Set</li> <li>Pick Shortcut Folder</li> <li>Pre-Install Summary</li> <li>Installing</li> <li>Upgrade</li> <li>System Restart</li> <li>Install Complete</li> </ul>	Please choose the installation folder. It is recommended that you choose the folder name according to the device that you want to connect to, for example /ciscoids or /checkpointng. If you are upgrading from a previous version, please select the folder where the ArcSight SmartConnector is currently installed.         Where Would You Like to Install?         C:\Program Files\ArcSightSmartConnectors\Windows         Restore Default Folder         Choose
InstallAnywhere Cancel	Previous Next

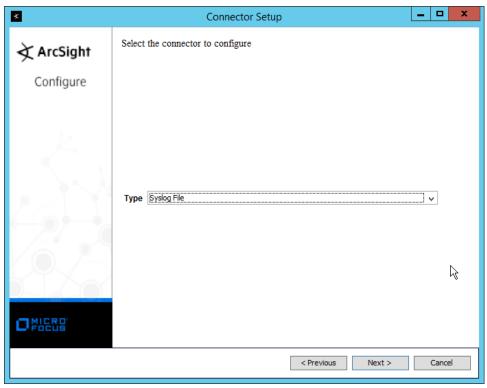
4. Click Next.



- 5. Click Next.
- 6. Click Install.
- 7. Select Add a Connector.



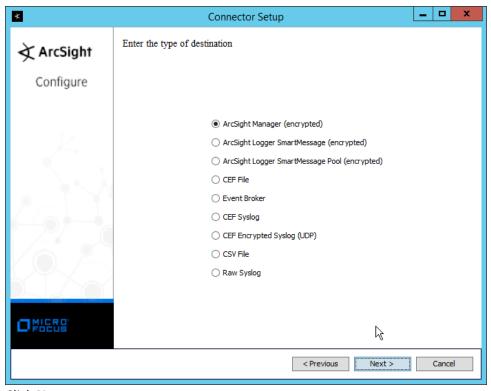
- 8. Click Next.
- 9. Select Syslog File.



- 10. Click Next.
- 11. Enter C:\Logging\gw-inbound-smtp-analysis-agent.current.log for File Absolute Path Name.

*	Connector S	etup	_ <b>D</b> X
ArcSight Configure	Enter the parameter details		
	File Absolute Path Name Reading Events Real Time or Batch Action Upon Reaching EOF File Extension If Rename Action	ig\gw-inbound-smtp-analysis-agent.curr realtime None processed	ent.log
		ķ	
		< Previous Next >	Cancel

- 12. Click Next.
- 13. Select ArcSight Manager (encrypted).



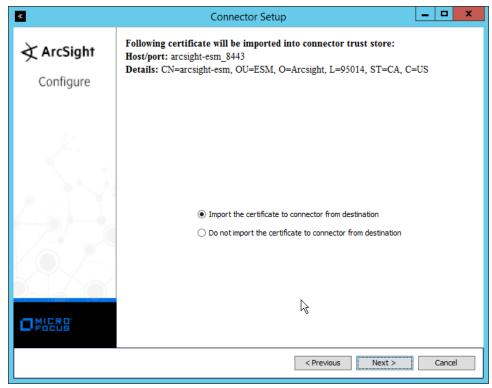
- 14. Click Next.
- 15. Enter the hostname, port, username, and password for the ArcSight ESM server.

*	Со	nnector Setup	_ <b>D</b> X
ArcSight	Enter the destination para	meters	
Configure			
K.	Manager Hostname	arcsight-esm	
	Manager Port	8443	
	User	administrator	
	Password	•••••	
	AUP Master Destination		~
	Filter Out All Events	false	~
	Enable Demo CA	false	~
D MICRO'			
	Real Provide P		
		< Previous Next >	Cancel

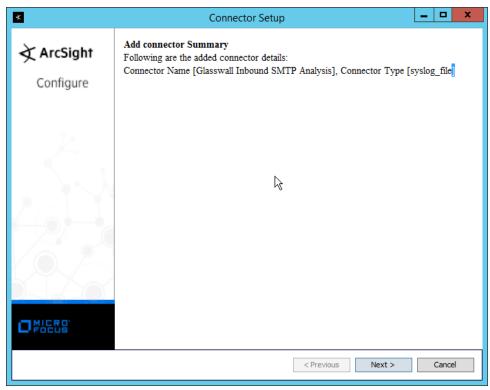
- 16. Click Next.
- 17. Enter identifying details about the system (only **Name** is required).

*		Connector Setup		_ <b>□</b> X
ArcSight	Enter the connec	tor details		
Configure				
K.	Name	Glasswall Inbound SMTP Ana	lysis	
4	Location DeviceLocation Comment			
			< Previous	lext > Cancel

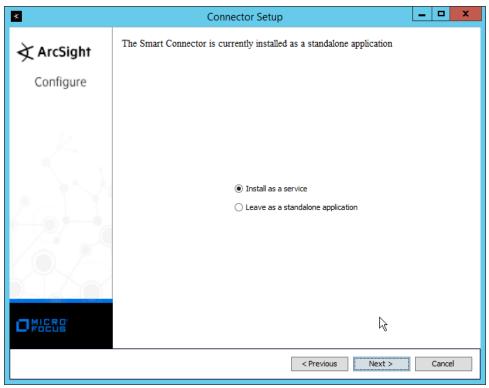
- 18. Click Next.
- 19. Select Import the certificate to connector from destination.



20. Click Next.



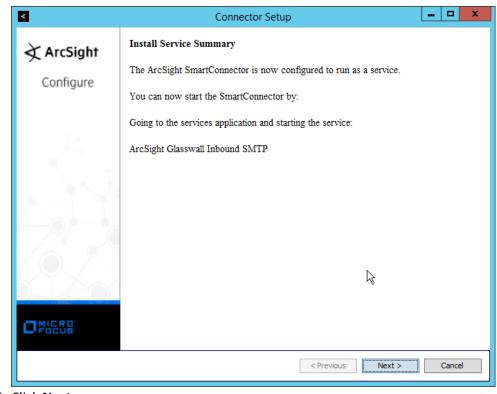
- 21. Click Next.
- 22. Select Install as a service.



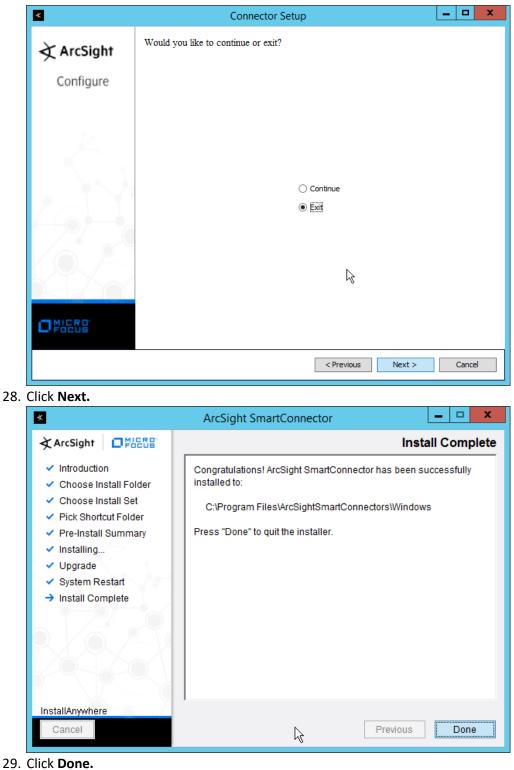
- 23. Click Next.
- 24. Change the service parameters to more appropriate names, because multiple connectors need to be installed on this server.

*	Connecto	or Setup	_ <b>D</b> X
ArcSight Configure	Specify the service parameters		
	Service Internal Name Service Display Name Start the service automatically	glasswall_inbound_smtp Glasswall[Inbound SMTP Yes	
	Start the Service automaticany	10	V
	k		
		< Previous Next >	Cancel

25. Click Next.



- 26. Click Next.
- 27. Select Exit.





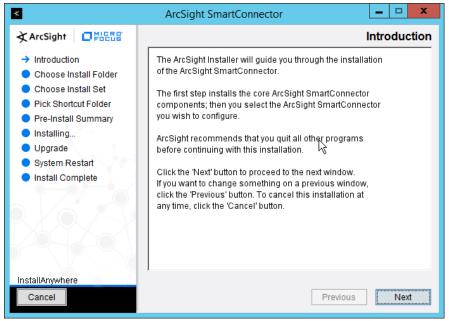
- 30. Repeat steps 1 to 29 for the other three "current" log files in *C*:\*Logging,* with the following caveats:
  - a. Replace C:\Program Files\ArcSightSmartConnectors\Windows with a different folder name for each connector.
  - b. Replace *C*:\*Logging*\*gw-inbound-smtp-analysis-agent.current.log* with the appropriate log file.
    - i. C:\Logging\gw-management-service.current.log
    - ii. C:\Logging\gw-file-analysis-process-InboundSMTPAgent-0.current.log
    - iii. C:\Logging\gw-administration-console.current.log
  - c. Replace the **Name** of the connector in its identifying details.
  - d. Replace the **service parameters** with different names so that the services do not conflict.

# 2.25 Integration: Micro Focus ArcSight and Cisco Stealthwatch

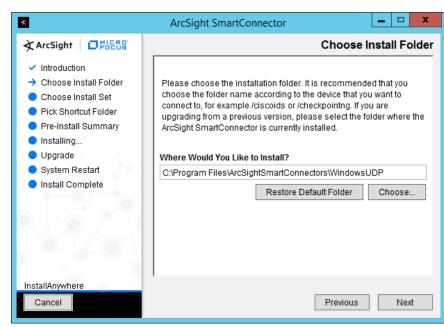
This section will detail the forwarding of logs from Cisco Stealthwatch to Micro Focus ArcSight.

## 2.25.1 Install Micro Focus ArcSight

1. Run ArcSight-7.9.0.8084.0-Connector-Win64.exe on any server except the one running Cisco Stealthwatch.



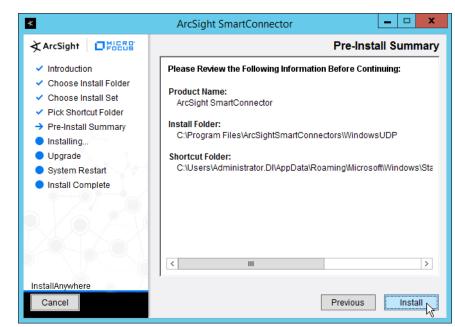
- 2. Click Next.
- 3. Enter C:\Program Files\ArcSightSmartConnectors\WindowsUDP.



4. Click Next.

*	ArcSight SmartConnector
ArcSight	Pick Shortcut Folder
<ul> <li>Introduction</li> <li>Choose Install Folder</li> <li>Choose Install Set</li> <li>Pick Shortcut Folder</li> <li>Pre-Install Summary</li> <li>Installing</li> <li>Upgrade</li> <li>System Restart</li> <li>Install Complete</li> </ul>	Where would you like to create product icons? <ul> <li>In a new Program Group: ArcSight SmartConnectors</li> <li>In the Start Menu</li> <li>On the Desktop</li> <li>In the Quick Launch Bar</li> <li>Other:</li> <li>Don't create icons</li> </ul> Create Icons for All Users
InstallAnywhere Cancel	Previous Next

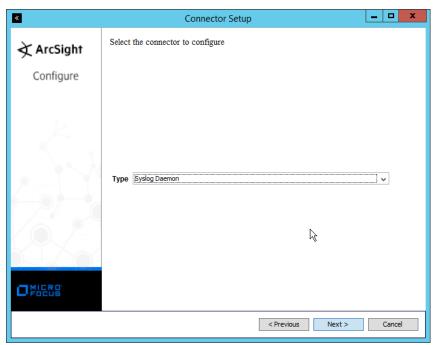
5. Click Next.



- 6. Click Install.
- 7. Select Add a Connector.

×	Connector Setup	- 0	x
À ArcSight	What would you like to do?		
Configure			
K.			
	Add a Connector		
	Add a Connector Set Global Parameters		
O FOCUS			
	< Previous Next >	Can	cel

- 8. Click Next.
- 9. Select Syslog Daemon.



- 10. Click Next.
- 11. Enter an unused port for the daemon to run on. (Ensure that this port is allowed through the firewall.)
- 12. Select UDP for Protocol.

×		Connect	tor Setup			
ArcSight	Enter the paran	neter details				
	Network Port IP Address Protocol Forwarder	6514 (ALL) UDP false				>
				L <sub>8</sub>		
				< Previous Next 2	>	Cancel

NIST SP 1800-26C: Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events

### 14. Select ArcSight Manager (encrypted).

×	Connector Setup	-		x
À ArcSight	Enter the type of destination			
Configure				
	ArcSight Manager (encrypted)     ArcSight Logger SmartMessage (encrypted)     ArcSight Logger SmartMessage Pool (encrypted)     CEF File     Event Broker     CEF Syslog     CEF Encrypted Syslog (UDP)     CSV File     Raw Syslog			
	< Previous Next >		Cancel	

### 15. Click Next.

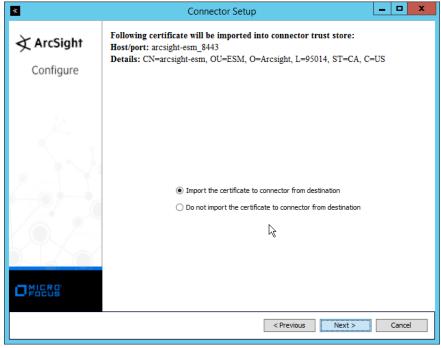
16. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.

*	Со	nnector Setup			
文 ArcSight	Enter the destination para	meters			
Configure					
7.4					
100	Manager Hostname	arcsight-esm			
	Manager Port	8443			
$\sim \lambda$	User	administrator			
	Password	•••••			
	AUP Master Destination	false			~
	Filter Out All Events	false			~
	Enable Demo CA	false			~
			< Previous	Next >	Cano

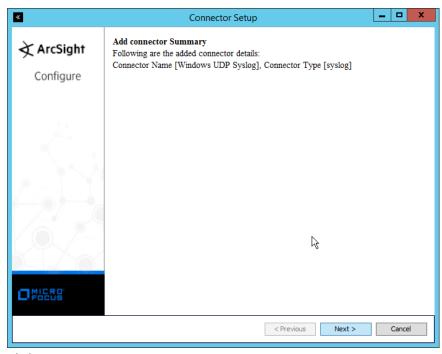
18. Enter identifying details about the system (only Name is required).

×		Connector Setup		_ <b>□</b> ×
文 ArcSight	Enter the connec	tor details		
Configure				
	Name Location DeviceLocation Comment	Windows UDP Syslog		
			< Previous N	ext > Cancel

- 19. Click Next.
- 20. Select Import the certificate to connector from destination.



21. Click Next.



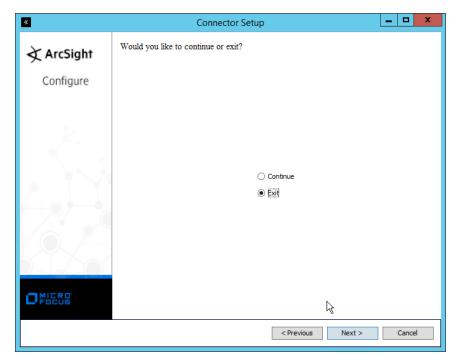
- 22. Click Next.
- 23. Select Install as a service.

*	Connector Setup	_		x
À ArcSight	The Smart Connector is currently installed as a standalone application			
Configure				
	<ul> <li>Install as a service</li> <li>Leave as a standalone application</li> </ul>			
	< Previous Next >		Cance	

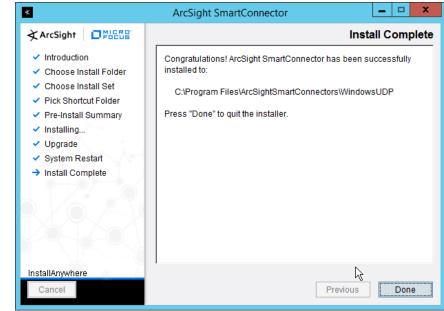
- 24. Click Next.
- 25. Enter a service name and display name.

	Connect	or Setup	_ <b>_</b> ×
À ArcSight	Specify the service parameters		
Configure			
- K			
	Service Internal Name Service Display Name	arc_syslog_udp Syslog UDP Daemon	
<u> </u>	Start the service automatically	Yes	~
		< Previous	Next > Cancel
Click Next.			
*	Connect	or Setup	_ <b>_</b> ×
À ArcSight	Install Service Summary		
ArcSight Configure	The ArcSight SmartConnector i		ervice.
	The ArcSight SmartConnector i You can now start the SmartCo	nnector by:	ervice.
	The ArcSight SmartConnector i	nnector by:	ervice.
	The ArcSight SmartConnector i You can now start the SmartCo Going to the services application	nnector by:	ervice.
	The ArcSight SmartConnector i You can now start the SmartCo Going to the services application	nnector by:	ervice.
	The ArcSight SmartConnector i You can now start the SmartCo Going to the services application	nnector by:	ervice.
	The ArcSight SmartConnector i You can now start the SmartCo Going to the services application	nnector by:	ervice.
Configure	The ArcSight SmartConnector i You can now start the SmartCo Going to the services application	nnector by:	ervice.
	The ArcSight SmartConnector i You can now start the SmartCo Going to the services application	nnector by:	ervice.

- 28. Select Exit.



### 29. Click Next.



30. Click Done.

# 2.25.2 Configure Cisco Stealthwatch

- Log in to the Cisco Stealthwatch Management Console desktop interface. (This can be downloaded from the web interface and run using javaws.exe. You may need to add the site to your Java exceptions in Control Panel > Java.)
- 2. Click Configuration > Response Management.

Rules	Name 🔺 1	Type 💠	Enabled 💠	Description 💠
Actions Syslog Formats	FlowCollector System Alarm	FlowCollector System Alarm	~	This rule will send an email message to users populated within the "Send email" action. To send additional alarm types, edit this rule to add/remove alarm types.
	SMC System Alarms	StealthWatch Management Console System Alarm	~	This rule will send an email message to users populated within the "Send email" action. To send additional alarm types, edit this rule to add/remove alarm types.
	StealthWatch Host Alarms - Inside Hosts as the Source of alarm	Host Alarm	~	This rule will send an email message to users populated within the "Send email" action.

3. Click Actions.

2	Re	sponse Ma	nagement		X
	Actions				1
Rules Actions Syslog Formats	Name 1 Send email	Type 🔷	Enabled 🗢	Description Send email message Edit to add recipients within the "To:" field	Used by Rules \$
					<u> </u>
		Add	Remove	Duplicate	Edit
Help					Close

- 4. Click Add.
- 5. Select ArcSight Common Event Format (CEF).

2	Action	Types		X
Email QualysGuard SNMP Trap	on Event Format (CEF) ppliance Syslog Message (Legac	y)		
Help		[	OK	Cancel

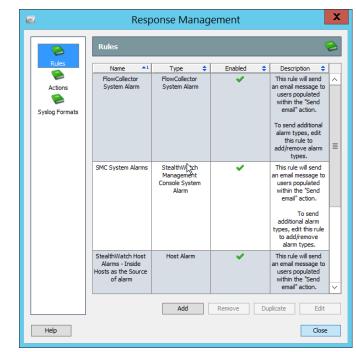
- 6. Click OK.
- 7. Enter a **name** for the **Action**.
- 8. Enter a description.
- 9. Enter the **IP address** of the server with the User Datagram Protocol (UDP) ArcSight Connector that you just created.
- 10. Enter the **port** used in the UDP ArcSight Connector that you just created.
- 11. (Optional) Click **Test** to send a test message to ArcSight, and verify that ArcSight receives the message.

🖾 Add Arc	:Sight Common Event Format (CEF) Acti 💌
Action	
Name:	ArcSight CEF
Description:	Send to ArcSight.
E Made	
Enabled:	▼
Destination —	
IP Address:	192. 168. 1. 121
Port:	6514
	Test
Help	OK

- 12. Click OK.
- 13. Verify that the action was created properly.

2	Re	sponse Ma	nagement		X	
	Actions					
Rules Actions	Name 1 ArcSight CEF	Type ArcSight Common Event Format (CEF) Email	Enabled 💠	Description Send to ArcSight.	Used by Rules \$	
Syslog Formats	Send email	Email	•	Edit to add recipients within the "To:" field	4	
		Add	Remove	Duplicate	Edit	
Help					Close	

14. Click Rules.



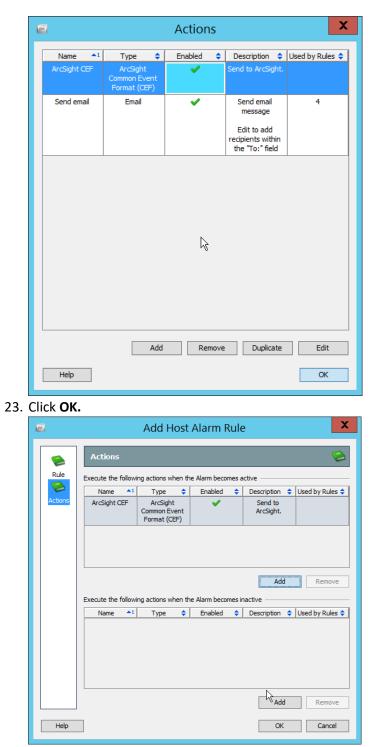
- 15. Click Add.
- 16. Select Host Alarm.

2	Rule Types	5
Please select a rule type		
StealthWatch Manager	nt Console System Alarm	
FlowCollector System A	rm	
Exporter or Interface A	arm	
Host Alarm		
Host Group Relationship	Alarm	
Help		OK Cancel
	1 Contraction of the second se	

- 17. Click OK.
- 18. Enter a **name.**
- 19. Enter a **description.**

	e	Add Host Alarm Rule
	Rule Notions	Rule       Image: sends host alarm to ArcSight         Description:       This rule sends host alarms to ArcSight.         Image: I
20.	Help Click Act	tions.
	Rule Actions	Actions         Execute the following actions when the Alarm becomes active         Name ^1       Type \$ Enabled \$ Description \$ Used by Rules \$         Add       Remove         Execute the following actions when the Alarm becomes inactive         Name ^1       Type \$ Enabled \$ Description \$ Used by Rules \$         Name ^1       Type \$ Enabled \$ Description \$ Used by Rules \$         Name ^1       Type \$ Enabled \$ Description \$ Used by Rules \$
	Help	Add Remove OK Cancel

- 21. Click the Add button for the top section; this adds an action when the alarm becomes active.
- 22. Select the ArcSight CEF rule you just created.



24. Click the **Add** button for the bottom section; this adds an action when the alarm becomes inactive.

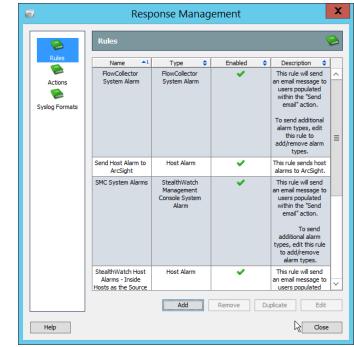
### 25. Select the ArcSight CEF rule you just created.

ē.		Actions		X
Name 1 ArcSight CEF	Type 💠 ArcSight Common Event	Enabled 🔶	Description 💠 Send to ArcSight.	Used by Rules 💠
Send email	Format (CEF) Email	~	Send email message	4
			Edit to add recipients within the "To:" field	
		$\searrow$		
	Add	Remove	e Duplicate	Edit
Help				ОК

### 26. Click OK.

		Add Host	Alarm F	tule	2	
	Actions					Sec. 1
Rule	Execute the followi	ing actions when th	e Alarm beco	nes a	ctive	
	Name 🔺	Type 💠	Enabled	\$	Description 🗢	Used by Rules
Actions	ArcSight CEF	ArcSight Common Event Format (CEF)	~		Send to ArcSight.	
	Everyte the followi	ing actions when th	e Alarm beco	nes ir	Add	Remove
	Execute the followi	-			active	
		ng actions when th Type ArcSight Common Event Format (CEF)	e Alarm becor Enabled	mes ir ¢	active	
	Name 🔺	Type 💠 ArcSight Common Event			Description 💠	Used by Rules
	Name 🔺	Type 💠 ArcSight Common Event			Add	Remove

#### 27. Click OK.



28. Click Close.

# Appendix A List of Acronyms

AD	Active Directory
AMP	Advanced Malware Protection
ΑΡΙ	Application Programming Interface
CEF	Common Event Format
CSR	Certificate Signing Request
CSV	Comma-Separated Values
DNS	Domain Name System
DSP	Directory Services Protector
ESM	Enterprise Security Manager
ICA	Information Centric Analytics
IIS	Internet Information Services
ISAPI	Internet Server Application Programming Interface
ISE	Identity Services Engine
п	Information Technology
JCE	Java Cryptography Extension
JRE	Java Runtime Environment
MAC	Media Access Control
ММС	Microsoft Management Console
MSSQL	Microsoft Structured Query Language
МХ	Mail Exchange

NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PEM	Privacy Enhanced Mail
RADIUS	Remote Authentication Dial-In User Service
RHEL	Red Hat Enterprise Linux
RMI	Remote Method Invocation
SAN	Subject Alternative Name
SDK	Software Development Kit
SMC	Stealthwatch Management Console
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell
TE	Tripwire Enterprise
UDP	User Datagram Protocol