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 publication 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 https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond.





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	Practio	ce Guide Structure	1
1.2	Build (Overview	2
1.3	Туроді	raphical Conventions	3
Pro	duct li	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
	Intro 1.1 1.2 1.3 Proo 2.1 2.2 2.3 2.4 2.5 2.6	Introduct 1.1 Praction 1.2 Build O 1.3 Typog Product I 2.1 2.1 Active 2.1.1 2.1.2 2.1.3 2.1.4 2.1.5 2.1.6 2.2 Micros 2.3 Windo 2.3 Windo 2.4 MS SO 2.4.1 2.4.2 2.4.3 SO 2.5 Micros 2.5.1 2.5.1 2.5.2 Sempter 2.6.1 2.6.2 2.6.3 2.6.4	Introduction 1.1 Practice Guide Structure 1.2 Build Overview 1.3 Typographical Conventions. Product Installation Guides

	2.6.5	Configu	e Email Alerts with Semperis DSP	118
2.7	Glassw	vall FileT	rust [™] 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	299
2.14	Symant	ec Analytics	302
	2.14.1	Initial Setup	302
	2.14.2	Capturing Data	308
2.15	Symant	ec Information Centric Analytics	309
	2.15.1	Installing MS SQL 2017	309
	2.15.2	Install Windows Services	317
	2.15.3	Installing Symantec ICA	325
	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	
	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	
	2.21.2	Select Logs for Forwarding	
2.22	Integra	ation: Micro Focus ArcSight and Semperis DSP	
	2.22.1	Configure Semperis DSP to Forward Logs	
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	441

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 File > Edit .
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	 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. 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.

- 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		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	 Select a virtual hard disk 		
Server Roles	Server Pool			
Features	Filter:			
Results	Name	IP Address	Operating System	
	AD-DNS	192.168.78.4	Microsoft Windows Server 2012 R2 Standard	
	1 Computer(s) four This page shows se	id ivers that are running Wir and in Server Manager. O	ndows Server 2012, and that have been added by using	
	Add Servers comm			

Select server rol	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	 Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Application Server DHCP Server 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 	 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 permittee resources anywhere on the netwo through a single logon process.

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 Cartificate Services	Active Directory Domain Services
Server Roles	Active Directory Domain Services	(AD DS) stores information about
Features	Active Directory Federation Services	this information available to user
AD DS	Active Directory Lightweight Directory Services	and network administrators. AD I
Confirmation	Active Directory Rights Management Services	network users access to permitte
	Application Server	resources anywhere on the netwo
	DHCP Server	through a single logon process.
	DNS Server	
	Fax Server	
	Ille and Storage Services (1 of 12 installed)	
	In Network Policy and Access Services	
	Print and Document Services	
	Remote Access	
	Remote Desktop Services	
		•

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	AD-D
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 their select between the selected automatically.	have to cl
Features	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.

L	Active Directory Domain Servic	es Configuration Wizard	_ D 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 Add a <u>d</u>omain controller to an e Add a new domain to an <u>e</u>xistin Add a new <u>forest</u> Specify the domain information for <u>R</u> oot domain name: More about deployment configurat	ions	
		< Previous Next N	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.

a ,	Active Directory Domain Services	Configuration Wizard	_ D X
Domain Controlle	r Options		TARGET SERVER AD-DNS
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new fores Forest functional level: Domain functional level: Specify domain controller capabilities Image: Domain Name System (DNS) serve Image: Domain Controller (ROD) Read only domain controller (ROD) Type the Directory Services Restore Ma Passwor <u>d</u> : Confirm password:	st and root domain Windows Server 2012 R2 Windows Server 2012 R2 r r c) ode (DSRM) password •••••••	v
	More about domain controller options	2revious <u>N</u> exty	Install
4. Click Next.		, , , , , , , , , , , , , , , , , , ,	
a	Active Directory Domain Services	Configuration Wizard	_ _ ×
DNS Options Deployment Configuration Domain Controller Options	Specify DNS delegation options		TARGET SERVER AD-DNS
Additional Options Paths Review Options Prerequisites Check Installation Results			
	More about DNS delegation		

26. Verify the domain name.

b	Active Directory Domain Service	es Configuration Wizard	_ D 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	b the domain and change it if necessary	
	More about additional options		
		<u>Previous</u>	Cancel
27. Click Next.		an an an an an a	
	Active Directory Domain Service	s Configuration Wizard	
Paths			TARGET SERVER AD-DNS
Deployment Configuration	Specify the location of the AD DS dat	abase, log files, and SYSVOL	
Domain Controller Options DNS Options	Database folder:	C:\Windows\NTDS	
Additional Options	Log files folder:	C:\Windows\NTDS	
Paths Review Options Prerequisites Check Installation Results	STRACT LODGEL:	C: (VIRGOWS (STSVUL	
	More about Active Directory paths		
	<	Previous Nyst > Insta	ll Cancel

Period Review Options Deployment Configuration Configure this server as the first Active Directory domain controller in a new forest. DNS Options The new domain name is "DUPDR". This is also the name of the new forest. The new domain name is "DUPDR". This is also the name of the new forest. The new domain name is "DUPDR". This is also the name of the new forest. The new domain name is "DUPDR". This is also the name of the new forest. The NetBIOS name of the domain: DU Prerequisites Check Installation Results Obsolutional Controller options: Obsolutional Options: Global catalog: Yes DNS Server: Yes Create DNS Delegation: No These settings can be exported to a Windows PowerShell script to automate additional installation: Were about installation options: Ontain Controller option: Options: Options: </th <th></th> <th>Active Directory Domain Services Configuration Wizard</th> <th></th>		Active Directory Domain Services Configuration Wizard	
Deployment Configuration Review your selections: DNS Options Dis Options Parts Review Options Prerequisities Check The new domain name is "DUPDR". This is also the name of the new forest. The New domain name is "DUPDR". This is also the name of the new forest. The NextBIOS name of the domain: DI Prerequisities Check 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 Wree about installation services Configuration Wizard View script More about installations Wine wore the view of the security setting name of the security setting name of halows PowerShell script to automate additional installations Deployment Configuration More about installation options Citck Next. Incerequisites checks Prerequisites checks Prerequisites checks passed successfully. Click Install to begin installation. Show mare Dis Options Altiver Directory Domain Services Configuration Wizard Windows Server 2012 R2 domain controllers have a default for the security setting name of halows options wake scriptings phy algorithms compatitis with Windows SI 40 ⁴ that preventis wake	Review Options		TARGET SER AD-E
Previous (nstall Click Next. Active Directory Domain Services Configuration Wizard (nstall Concell Active Directory Domain Services Configuration Wizard TARGET SERV Prerequisites Check TARGET SERV Ad-D Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites check Prerequisites check Installation Results View results View results Minite additional options Paths Results View results View results Minite addition Results View results This computer has at least one physical network adapter that does not have static IP addiress(e) assigned to biot IPV4 and IPV6 are enabled for a network adapter, both IPV4 and IPV6 are enabled for a network adapter so the IPV4 and IPV6 are enabled for a network adapter so the IPV4 and IPV6 are enabled for a network adapter soth IPV4 and IPV6 are enableater for reliable Domain Nam	Deployment Configuratio Domain Controller Option DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Review your selections: 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 automatiadditional installations	w forest.
Installation Results Additional Options Prerequisites Check Installation 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.microsoft.com/fwlink/?Linkld=104751). Installation Results Installa		< <u>Previous</u>	nstall Cancel
Image: Prerequisites Check TARGET SERV AD-D Image: Prerequisite checks passed successfully. Click 'Install' to begin installation. Show more Deployment Configuration Domain Controller Options DNS Options Prerequisites need to be validated before Active Directory Domain Services is installed on this computer Review Options Prerequisites check Prerequisites Check ✓ Yiew results Installation Results ✓ Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms when establishing security channel sessions. For more information about this setting, see Knowledge Base article 942564 (http:// go.microsoft.com/fwlink/?Linkld=104751). Installation 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 adapters for reliable Domain Name System Image: Prove Circle Install, the server automatically reboots at the end of the promotion operation.	lial: Nout		
All prerequisite checks passed successfully. Click 'Install' to begin installation. Show more Prerequisites checks Domain Controller Options DNS Options Prerequisites need to be validated before Active Directory Domain Services is installed on this computer DNS Options Additional Options Rerule prerequisites check Prerequisites Check View results View results Installation Results Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms when establishing security channel sessions. 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 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 If you click Install, the server automa	lick Next.	Active Directory Domain Services Configuration Wizard	
More about prerequisites	lick Next.	Active Directory Domain Services Configuration Wizard	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	r Manager		-	
ခြော Server Ma	anager • Dashbo	bard			•@ r	Manage Tools View	w Help
Dashboard	WELCOME TO SERVER	MANAGER					
Local Server All Servers AD DS DNS	QUICK START	1 Conf	igure this local server				
File and Storage Services D	WHATS NEW	2 <u>Ac</u> 3 Ac	Id roles angle teatures Id other servers to manage				
		4 Cr	eate a server group				Hide
	ROLES AND SERVER G	ROUPS					
	Roles I Server groups	Servers tota	a DNS	1 File and Storage Services	Local Server	1	
	Manageability Events Services		Manageability Events Services	Manageability Events Services	Manageability Events Services		
	Performance BPA results		Performance BPA results	Performance BPA results	Performance BPA results		
	Services Performance BPA results	1	Services Performance BPA results	Services Performance BPA results	Services Performance BPA results 11/6/2017 3/01 f	1944.	
	 Manageability 						

2. Click Add roles and features.

2	Add Roles and Features Wizard	_		x
Before you begin		DESTINATION AD-DNS	SERVER DI.IPDR	
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 shorting 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 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.	roles, role serv aring documer	ices, or its, or	
	Skip this page by default			
	< Previous Ins	tall Ca	incel	
ick Next. elect Role-based or	feature-based installation.			
2	Add Roles and Features Wizard	_		x
Select installation t	ype	DESTINATION AD-DNS	SERVER .DI.IPDR	
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	 Select the installation type. You can install roles and features on a running physicil machine, or on an offline virtual hard disk (VHD). Role-based or feature-based installation Configure a single server by adding roles, role services, and features. Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a or session-based desktop deployment. 	al computer or virtual machin	virtual e-base	:d

3. 4.

5. Click Next.

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

< Previous Next

Cancel

Install

6. Select Select a server from the server pool.

7. Select the intended Active Directory server.

Select destination server Select destination server Select a server or a virtual hard disk on which to install roles and features. Server Selection Server Selection Server Pool Select a server from the server pool Select a virtual hard disk Server Selection Results AD-DNSDLIPDR 192.166.78.4 Merocoft Windows Server 2012 R2 Standard Computer(s) found This page shows servers that are running Windows Server 2012, and that have been added by us Add Servers command in Server Manager. Offline servers and newly-added servers from which d collection is still incomplete are not shown. Click Next. Select server roles Select one or more roles to install on the selected server. Roles Server Roles Active Directory Centificate Service Active Directory Centificate Service Active Directory Centificate Service Active Directory Roletain Services Active Directory Roletain Services Active Directory Roletain Services Active Directory Roletain Services Confirmation Results Server Note The Server DHCP Server Services (2 of 12 installed) Confirmation Results DHCP Server DHCP Server Services (2 of 12 installed) Confirmation Results DHCP Server Services (2 of 12 installed) Confirmation DHCP Server DHCP Server DHCP Server DHCP Server DHCP Server Services (2 of 12 installed) Confirma		Add Roles and Features Wizard	
Before You Begin Installation Type Select a server or a virtual hard disk on which to install roles and features. Server Selection Select a server from the server pool Server Roles Features Confirmation Results Name IP Address Operating System AD-DNS.DLIPDK 10 computer(s) found This page shows servers that are running Windows Server 2012, and that have been added by us Add Servers command in Server Manager. Offline servers and newly-added servers from which d collection is still incomplete are not shown. Click Next. Image: Select one or more roles to install on the selected server. Before You Begin Select one or more roles to install on the selected server. Roles Metro Directory Certificate Services Pactures Confirmation Confirmation Results Select server roles Select one or more roles to install on the selected server. Roles Description Active Directory Certificate Services C(D) is used to create certification services Results Active Directory Rights Management Services C(D) is used to create certification services Papplication Server DHCP Server DHCP Server DHCP Server DHCP Server DHCP Server	Select destination	server	DESTINATION SERVER AD-DNS.DI.IPDR
1 Computer(s) found This page shows servers that are running Windows Server 2012, and that have been added by us Add Servers command in Server Manager. Offline servers and newly-added servers from which d collection is still incomplete are not shown. Image: Click Next.	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 feature Image: Select a server from the server pool Select a virtual hard disk Server Pool Filter: Name IP Address AD-DNS.DI.IPDR 192.168.78.4 Microsoft Windows Server	ver 2012 R2 Standard
Click Next. Click Next. Click Next. Confirmation Results ConfirmatioRefi		1 Computer(s) found This page shows servers that are running Windows Server 2012, and tha Add Servers command in Server Manager. Offline servers and newly-add collection is still incomplete are not shown.	it have been added by using th ded servers from which data
Click Next. Image: Confirmation Results Add Roles and Features Wizard Select server roles DESTINATION 3 AD-DNSI Before You Begin Installation Type Server Selection Select one or more roles to install on the selected server. Roles Description Active Directory Certificate Services Active Directory Certificate Services Active Directory Relearation Services Active Directory Services Active Directory Rights Management Services Applications. DHCP Server DNS Server (Installed) File and Storage Services (2 of 12 installed) File and Storage Services (2 of 12 installed) File and Storage Services (2 of 12 installed)		Tenon Territ	instan
Add Koles and Peatures Wizard Destination : AD-DNS: Before You Begin Installation Type Server Selection Select one or more roles to install on the selected server. Roles Description Active Directory Certificate Services Confirmation Results Description Active Directory Lightweight Directory Services Active Directory Rights Management Services Active Directory Rights Management Services Description DHCP Server DNS Server (Installed) Features Features Active Directory Rights Management Services Description Active Directory Rights Management Services Active Directory Services Active Offication Server Image: Active Directory Rights Management Services Image: Active Offication Server DHCP Server DNS Server (Installed) Fax Server Image: Active Directory Services (2 of 12 installed) Image: Active Directory Services (2 of 12 installed)	ck Next.	And Delse and Freduce Milered	
Features □ Active Directory Federation Services Confirmation □ Active Directory Federation Services role services that allow you to and manage certificates used in variety of applications. Results □ Active Directory Rights Management Services □ Active Directory Rights Management Services □ and manage certificates used in variety of applications. □ DHCP Server □ DHCP Server □ □ DNS Server (Installed) □ Fax Server □ □ □ File and Storage Services (2 of 12 installed) □	Select server roles Before You Begin Installation Type	Select one or more roles to install on the selected server. Roles	DESTINATION SERVER AD-DNS.DLIPDR ription e Directory Certificate Services :S) is used to create
Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services V	Server Selection Server Roles	A stive Directory Domain Convices (Installed)	ication authorities and related

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 Veb 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	AD CS Configuration	_
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 >>	Configure Cancel

23. Select Enterprise CA.




27. Select Create a new private key.

a	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	 Use existing private key Use this option to ensure continuity with previously issued certificates when reinstalling a CA. Select a certificate and use its associated private key 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. Select an existing private key on this computer Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
	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.

Cryptography for CA Credentials Role Services Select a gyptography for rolder Example Private Kay CA Type Private Kay Caname Validity Period Certificate Database Confirmation Progress Results Specify the name of the CA Role Services Select Role Database Configuration Credentials Role Services Specify the name of the CA Role Services Specify the name of the CA Role Services Select Role Database Confirmation Progress Results Control Con		AD CS Configuration	_ _ ×
Credentials Specify the cryptographic options Role Services Select a gyptographic provider: Kgy length: Cryptography Select a gyptographic provider: Kgy length: Cryptography Select begal algorithm for signing certificates issued by this CA: Select a gyptography Select begal algorithm for signing certificates issued by this CA: Cryptography Select begal algorithm for signing certificates issued by this CA: Select Big algorithm for signing certificates issued by the CA: Select begal algorithm for signing certificates issued by the CA: Select Big algorithm for signing certificates issued by the CA: Select begal algorithm for signing certificates issued by the CA: More about Cryptography More about Cryptography Configure Cancel Click Next: AD CS Configuration DESTINATION SERVE AD-DNS.DLIPD Credentials Specify the name of the CA Specify the name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix: Cryptography Diabouse Diabouse Diabouse Validity Period Diabouse Diabouse Diabouse Cryptography Diabouse Diabouse Diabouse Diabouse Validity Period <th>Cryptography fo</th> <th>or CA</th> <th>DESTINATION SERVER AD-DNS.DI.IPDR</th>	Cryptography fo	or CA	DESTINATION SERVER AD-DNS.DI.IPDR
More about Cryptography Image: Configure Cancel Cick Next. Image: Configure	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	Key length: 2048 At de by the CA.
Image: AD CS Configuration Image: AD CS Configuration CA Name DESTINATION SERVE AD-DNS.DI.IPD Credentials Specify the name of the CA Role Services Steup Type CA Type Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but ca be modified. Private Key Common name for this CA: Cryptography DI-AD-DNS-CA Validity Period Distinguished name suffix: Confirmation Dregiress Progress Results More about CA Name More about CA Name		More about Cryptography	
CA Name Specify the name of the CA Credentials Specify the name of the CA Role Services Type Setup Type CA Type Private Key Type or common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but cate modified. Validity Period Common name for this CA: Cryptography Di-AD-DNS-CA Progress Distinguished name: Results Nore about CA Name	lick Next.	< Fuerions Wet 2 >	<u>C</u> onfigure Cancel
Credentials Specify the name of the CA Role Services Type Setup Type Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but cate be modified. Private Key Common name for this CA: Cryptography DI-AD-DNS-CA Validity Period Distinguished name suffix: Confirmation DC=DI,DC=IPDR Progress CN=DI-AD-DNS-CA,DC=DI,DC=IPDR Results More about CA Name	lick Next.	<u>ح ب</u> revious <u>معرج ک</u> AD CS Configuration	Configure Cancel
	lick Next.	AD CS Configuration	Configure Cancel
	Lick Next. CA Name Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	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 ar 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	Cancel

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

a	AD CS Configuration	_ _ ×
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 the certificates it will issue.	ation authority (CA): he validity period for the
	More about Validity Period	<u>C</u> onfigure Cancel
35. Click Next.		
B	AD CS Configuration	_ _ ×
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 <u>C</u> ertificate database log location: C:\Windows\system32\CertLog	
	< Previous Nixt >	Configure Cancel

	AD CS Cor	nfiguration	_ _ ×
Confirmation			DESTINATION SERVER AD-DNS.DI.IPDR
Credentials	To configure the following roles	s, role services, or features, click Configure.	
Role Services	 Active Directory Certification 	te Services	
Setup Type	Certification Authority		
CA Type	СА Туре:	Enterprise Root	
Private Key	Cryptographic provider:	RSA#Microsoft Software Key Storage Prov	ider
Cryptography	Hash Algorithm:	SHA512	
CA Name	Key Length:	2048	
Validity Period	Allow Administrator Interaction	: Disabled	
Certificate Database	Certificate Validity Period:	11/6/2022 3:19:00 PM	
Confirmation	Distinguished Name:	CN=DI-AD-DNS-CA,DC=DI,DC=IPDR	
Departure	Certificate Database Location:	C:\Windows\system32\CertLog	
Progress	Certificate Database Log Location:	C:\Windows\system32\CertLog	
		< Previous Next > Cor	Gure Cancel
			Ŋ
Click Configure.			
Click Configure.	AD CS Co	nfiguration	_ 0
Click Configure.	AD CS Co	nfiguration	
Results	AD CS Co	nfiguration	
Click Configure.	AD CS Co	nfiguration	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co	nfiguration	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service	nfiguration es, or features were configured:	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service	nfiguration es, or features were configured: ate Services	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service	nfiguration es, or features were configured: ate Services	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service Active Directory Certification Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service Active Directory Certification Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	DESTINATION SERVER AD-DNS.DI.IPDF
Click Configure.	AD CS Co The following roles, role service Active Directory Certification Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service Active Directory Certification Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service Active Directory Certification Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service Active Directory Certificat Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service Active Directory Certificat Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service Active Directory Certification Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	DESTINATION SERVER AD-DNS.DI.IPDR
Click Configure.	AD CS Co The following roles, role service Active Directory Certificat Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	DESTINATION SERVER AD-DNS.DLIPDR
Click Configure.	AD CS Co The following roles, role service Active Directory Certificat Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	eeded
Click Configure.	AD CS Co The following roles, role service Active Directory Certificat Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	eeded
Click Configure.	AD CS Co The following roles, role service Active Directory Certificat Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	eeded
Click Configure.	AD CS Co The following roles, role service Active Directory Certificat Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	eeded
Click Configure.	AD CS Co The following roles, role service Active Directory Certificat Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	eeded
Click Configure.	AD CS Co The following roles, role service • Active Directory Certifica Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	eeded
Click Configure.	AD CS Co The following roles, role service Active Directory Certificat Certification Authority More about CA Configuration	nfiguration es, or features were configured: ate Services Configuration succ	eeded

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 ~ dsa.msc	
L	Windows			dsa	
Server Manager	PowerShell				
	e				
Control Panel	Internet Explorer				
Desktop					
۲					

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

le Action View Help				
🔿 🖄 📅 🤾 🗎 🗙 🛛	1 🖪 🔒 🛛 🖬	1 🙎 🐮 🛯	7 🗾 🗽	
Active Directory Users and Com Saved Queries DI.IPDR Suiltin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour	Name Administrator Allowed RO Cert Publish Cloneable D Denied ROD DisAdmins DisUpdateP Domain Ad Domain Go Domain Go Domain Go Domain Go Domain Gos Domain Guses Enterprise A	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description Built-in account for ad Members in this group c Members of this group Members of this group t Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users Designated administrato	
	 Enterprise R Group Polic Guest Protected Us RAS and IAS Read-only D Schema Ad Schema Ad 	Security Group Security Group User Security Group Security Group Security Group	Members of this group Members in this group c Built-in account for gue Members of this group Servers in this group can Members of this group Designated administrato	

4. Click Delegate Control.

Delegation of Control Wizard

×

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	x
Users or Groups Select one or more users or groups to whom you want to delegate control.	
Selected users and groups:	
Add Remove	

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

Users, Groups, or Built-in s	ecurity principals		Object Types
From this location:			
DI.IPDR			Locations
Enter the object names to a	select (examples):		
Domain Admins			Check Names
Advanced		ОК	Cancel

8. Click **OK.**

Delegation of Control Wizard	x
Users or Groups Select one or more users or groups to whom you want to delegate control.	2
Selected users and groups:	
Add Remove	
< Back Nert > Cancel Help	

10. Choose Create a custom task to delegate.

Delegate n select common tasks or customize your own.	(A)
and an one of the second and the second and the second and the second second second second second second second	K
egate 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 k ✓	
III >	
ate a custom task to delegate	
< Back Sext > Cancel	Help
	egate 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 > ate a custom task to delegate

- 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: This folder, existing objects in this folder, and creation of new objects in this folder Only the following objects in the folder: 	
 account objects aCSResourceLimits objects applicationVersion objects bootableDevice objects certificationAuthority objects Computer 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**.

Select the permission	s you want to delegate.	P
Show these permissio	ins:	
General		
Property-specific		
Creation/deletion	of specific child objects	
Permissions:		
Receive as		~
Read and write a	account restrictions	
Read and write p	personal information	
Read and write p	public information	=
✓ Validated write to	o DNS host name	
Validated write to	o service principal name	~
Click Next.		
Click Next.	Delegation of Control Wizard Completing the Delegation of Control Wizard	of
Click Next.	Delegation of Control Wizard Completing the Delegation of Control Wizard You have successfully completed the Delegation of wizard.	• f Control
Click Next.	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 in the following Active Directory folder:	of Control
Click Next.	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 in the following Active Directory folder: DI.IPDR/Users	of Control
Click Next.	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 in the following Active Directory folder: DI.IPDR/Users The groups, users, or computers to which you have given control are:	of Control
Click Next.	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 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)	of Control
Click Next.	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 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)	of Control
Click Next.	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 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) They have the following permissions:	of Control
Click Next.	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 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) They have the following permissions: To close this wizard, click Finish.	of 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.

-	. tetti ente ente enterning een			68 - 18 A.
🍥 – 🛧 🔩 🕨 Control P	Panel Network and Internet Network and Sharing Cente	r v C	Search Control Panel	
Control Panel Home	View your basic network information and	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 connect	ion; or set up a router or acces	is point.	
	Troubleshoot problems	et troubleshooting information		
	biogrose and repair network problems, or ge	the activity mornator	8	
See also				
See also Internet Options				

3. Click the name of the internet adapter.

1			
ction			
4 Connectivit	y:		Internet
6 Connectivity	y:	No Inte	ernet access
dia State:			Enabled
ration:			02:16:05
eed:			1.0 Gbps
Details			
	Sent —	-	Received
es:	3,043,324		2,073,372
roperties	😚 Disable	Diagnose	
			F
	ection 4 Connectivit 6 Connectivit 6 Connectivit dia State: ration: eed: Details y	ection 4 Connectivity: 6 Connectivity: dia State: ration: eed: Details y Sent — ees: 3,043,324 Properties Disable	ection 4 Connectivity: No Inte 6 Connectivity: No Inte dia State: ration: eed: Details y Sent — Sent — res: 3,043,324 bioperties Disable Diagnose

	olgabit Helwork connects	on
		Configure
his connection uses t	he following items:	
Client for Micro	soft Networks	
File and Printe	r Sharing for Microsoft Net	works
QoS Packet S	cheduler	
A Microsoft Netw	ork Adapter Multipleyor P	Innotan
	on Audpter multiplexor	1010001
🗹 🛶 Link-Layer Top	ology Discovery Mapper	I/O Driver
🗹 🔺 Link-Layer Top 🗹 🔺 Link-Layer Top	oology Discovery Mapper bology Discovery Respor	IVO Driver Ider
 Link-Layer Top Link-Layer Top Internet Protoc 	oology Discovery Mapper oology Discovery Respor ol Version 6 (TCP/IPv6)	I/O Driver Ider
 Link-Layer Top Link-Layer Top Link-Layer Top Internet Protoc Internet Protoc 	oology Discovery Mappel bology Discovery Respor ol Version 6 (TCP/IPv6) ol Version 4 (TCP/IPv4)	I/O Driver ider
Link-Layer Top Link-Layer Top Link-Layer Top Link-Layer Top Internet Protoc Internet Protoc Install	oology Discovery Mapped oology Discovery Respon of Version 6 (TCP/IPv6) of Version 4 (TCP/IPv4) Uninstall	VO Driver Ider Properties
Link-Layer Top Link-Layer Top Link-Layer Top Internet Protoc Internet Protoc Install Description	ology Discovery Mapped pology Discovery Mapped ol Version 6 (TCP/IPv6) ol Version 4 (TCP/IPv4) Uninstall	Properties
Link-Layer Top Link-Layer Top Link-Layer Top Link-Layer Top Internet Protoc Internet Protoc Install Description Transmission Contr	ol Vaspter Malpheter Mappet poology Discovery Mapper ol Version 6 (TCP/IPv6) ol Version 4 (TCP/IPv4) Uninstall ol Protocol/Internet Protoc	I/O Driver I/O Driver Ider Properties
 ✓ Link-Layer Top ✓ Link-Layer Top ✓ Internet Protoc ✓ Internet Protoc<!--</td--><td>oology Discovery Mapper bology Discovery Respor ol Version 6 (TCP/IPv6) ol Version 4 (TCP/IPv4) Uninstall Ol Protocol/Internet Protoc col that provides communi</td><td>I/O Driver ider Properties</td>	oology Discovery Mapper bology Discovery Respor ol Version 6 (TCP/IPv6) ol Version 4 (TCP/IPv4) Uninstall Ol Protocol/Internet Protoc col that provides communi	I/O Driver ider 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	Alternate Configuration					
You ca suppor admini	n get IP settings assigned a ts this capability. Otherwise strator for the appropriate	automatica 2, you nee IP setting:	ally if ed to a s,	your r ask yo	etwork ur netw	ork
	btain an IP address automa	atically				
OU	se the following IP address	-				
IP a	ddress:			*		
Sub	net mask:			+	34	
Defa	ault gateway:		4	6	-	
0 0 • U	btain DNS server address a se the following DNS server	automatica r address	ally es			
Pref	ferred DNS server:	192	2.16	8.7	8.4	
Alte	rnate DNS server:			*		
	/alidate settings upon exit				Adv	anced
			-	OK		Can

9. Click OK.

Connection -		
IPv4 Connect	tivity:	Intern
IPv6 Connect	tivity:	No Internet acce
Media State:		Enable
Duration:		02:30:0
Speed:		1.0 Gb
Details		
Details	1	
Details	Sent —	Receive
Details Activity Bytes:	Sent — 3,043,845	Receive 2,074,11

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



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

e,			System	
	🕥 – 🛧 🍓 🕨 Control P	anel System and Security System	tem	✓ C Search Control Panel
	Control Panel Home	View basic information	about your computer	
-	Device Manager	Windows edition		
V	Remote settings	Windows Server 2012 R2 S	tandard	
¥	Advanced system settings	© 2013 Microsoft Corpora	tion. All rights reserved.	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.

		System I	Propert	ies	
Computer Nam	Hardware	Advanced	Remote	•	
W th	/indows uses t e network.	he following i	nformatio	n to identify y	our computer o
Computer de	scription:	-			
		For example Server".	e: "IIS Pro	duction Serv	er" or "Account
Full compute	r name:	REMOTED	ESKTOP	1	
Workgroup:		WORKGRO	UP		
To rename th workgroup, c	nis computer o lick Change.	r change its o	domain or		Change
lick Char	nge.	C	K	Cancel	Apj
elect Doi nter the	main. domain				
С	omputer	Name	/Dom	ain Cha	inges
You can ch Changes m	ange the na ight affect a	me and th ccess to n	e memb etwork r	ership of t esources.	his compute
Computer n	ame:				
REMOTED	ESKTOP1	5			
Full comput	er name:				
REMOTED	ESKTOP1				
					More
					Morea
Membero)f				
Dom	ain:				
DLIF	UK				
Work	kgroup:				
WO	RKGROUP				
L					
				L.	0

- 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.
	DI\Administrator
	OK Cancel
.9.	Click OK.
	Computer Name/Domain Changes
	You must restart your computer to apply these changes Before restarting, save any open files and close all programs.
	ОК

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.

a	Local Security Policy	_ _ ×
File Action View Help Image: Constraint of the second seco		
 Security Settings Account Policies Local Policies Local Policies Local Policy Lise Rights Assignment Security Options Windows Firewall with Advanced Security Optices Public Key Policies Software Restriction Policies Software Restriction Policies Software Advanced Audit Policy Configuration 	Policy Audit account logon events Audit account logon events Audit directory service access Audit logon events Audit object access Audit policy change Audit provess tracking Audit process tracking 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.

	Audit	accoun	t manage	ment	Properti	es ?	
Local Sec	urity Setting	Explain					
	Audit accou	unt manag	jement				
Aud	t these attem	pts:					
V 9	ouccess						
A	This setting r override cate For more info	night not b egory leve rmation, s	be enforced if I audit policy. ee <u>Audit acco</u>	other product man	olicy is confi	igured to Q921468	()

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
R	everse Lookup Zone Name 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. Network ID: 192 .168 .192 .168 The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order. If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa. Reverse lookup zone name: 1.168.192.in-addr.arpa
Click	< Back Next > Cancel
	New Zone Wizard
D	ynamic Update You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
	Dynamic updates enable DNS dient computers to register and dynamically update their resource records with a DNS server whenever changes occur.
	 Select the type of dynamic updates you want to allow: Allow only secure dynamic updates (recommended for Active Directory) This option is available only for Active Directory-integrated zones. Allow both nonsecure and secure dynamic updates Dynamic updates of resource records are accepted from any client. This option is a significant security vulnerability because updates can be accepted from untrusted sources. Do not allow dynamic updates Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

10. Click Next.

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		DNS Manager		_ D X
File Action View Help				
🗢 🄿 🙍 🖬 🖬 🖉 🖌	? 🖬 🗎 🗐 🛱			
🚊 DNS	Name	Туре	Data	Timestamp
△ AD-DNS.DI.IPDR	same as parent folder)	Start of Authority (SOA)	[1], ad-dns.di.ipdr., hostm	static
Forward Lookup Zones	🔲 (same as parent folder)	Name Server (NS)	ad-dns.di.ipdr.	static
1.168.192.in-addr.arp				
Trust Points	N			
Conditional Forwarders	4			
Global Logs				
< 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 X
Γ	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
	¢}
L	OK Cancel
~1	ick OK.
-1	
	DNS Manager
ار گ F	DNS Manager ile Action View Help

å		DNS Manager		_ □ ×
File Action View Help				
🗢 🄿 📶 🛅 🖾 🚺 👔				
 DNS A -DNS.DI.IPDR Converse Lookup Zones Reverse Lookup Zones 1.168.192.in-addr.arp Trust Points Conditional Forwarders M Global Logs 	Name (same as parent folder) (same as parent folder) 192.168.1.12	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 Directory	For Extracted Files	
C:\Program Files	\Microsoft\Exchan	ige Server
		-

3. Click OK.

Application Tools	Exchar	nge Server		-
: View Manage				~
ocal Disk (C:) Program Files Microsoft Exe	change Server 🕨	~ ¢	Search Exchange Server)
Name	Date modified	Туре	Size	
si s	8/14/2017 10:22 AM	File folder		
	8/14/2017 10:22 AM	File folder		
SW SW	8/14/2017 10:22 AM	File folder		
ta ta	8/14/2017 10:22 AM	File folder		
te te	8/14/2017 10:22 AM	File folder		
li th	8/14/2017 10:22 AM	File folder		
📕 tr	8/14/2017 10:22 AM	File folder		
📕 uk	8/14/2017 10:22 AM	File folder		
🍱 ur	8/14/2017 10:22 AM	File folder		
👪 vi	8/14/2017 10:22 AM	File folder		
퉬 zh-hans	8/14/2017 10:22 AM	File folder		
🔰 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	
microsoft.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.acquirelangua	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	
microsoft.exchange.setup.signverfwrapp	9/20/2015 4:41 AM	Application extens	83 KB	
setup N	9/20/2015 4:41 AM	Application	31 KB	
	Application Tools * View Manage ocal Disk (C:) > Program Files > Microsoft > Ex Name * >> >> >>	Application Tools Exchange view Manage ocal Disk (C:) > Program Files > Microsoft > Exchange Server > Name Date modified 91 91 91 91 92 8/14/2017 10:22 AM 93 8/14/2017 10:22 AM 94 8/14/2017 10:22 AM 95 8/14/2017 10:22 AM 94 10:22 AM 95 8/14/2017 10:22 AM 96 11:02 AM 97 8/14/2017 10:22 AM 96 11:02 AM 97 11:02 AM 96 11:02 AM 97 11:02 AM 97	Application Tools Exchange Server view Manage ocal Disk (C:) > Program Files > Microsoft > Exchange Server > v © Name Date modified Type view 8/14/2017 10:22 AM File folder sv 8/14/2017 10:22 AM File folder sv 8/14/2017 10:22 AM File folder sv 8/14/2017 10:22 AM File folder ta 8/14/2017 10:22 AM File folder uk 8/14/2017 10:22 AM File folder wi 8/14/2017 10:22 AM File folder autorun 9/20/2015 4:41 AM Setup Information ge microsoft.exchange.cabutility.dll 9/20/2015 4:41 AM Ap	Application Tools Exchange Server 2 View Manage ocal Disk (C:) > Program Files > Microsoft > Exchange Server > ✓ C Search Exchange Server Name Date modified Type Size Sr-cyrl 8/14/2017 10:22 AM File folder Sw 8/14/2017 10:22 AM File folder Sw 8/14/2017 10:22 AM File folder It a 8/14/2017 10:22 AM File folder

- 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	
En 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		
E S 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: DI		
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 th for the management of Exchange and Active Directory among different groups of people. Applying this security model ability for Exchange servers and administrators to create Active Directory objects such as users, groups, and contacts. Th 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. Click information.	e responsibi emoves the e ability to '?' for more	lity
E 28 Exchange	<u>n</u> ext	

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

М	CROSOFT EXCHANGE SERVER 2016 SETUP	?
Ν	Ialware Protection Settings	
Ma tur	lware scanning helps protect your messaging environment by detecting messages that may contain viruses or spyw 1ed off, replaced, or paired with other premium services for layered protection.	vare. It can be
Ma	lware scanning is enabled by default. However, you can disable it if you're using another product for malware scann vose to disable malware scanning now, you can enable it at any point after you've installed Exchange.	ning. If you
Dis	able malware scanning.	
0	<u>Y</u> es	
0	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	Add Roles and Features Wizard	_ 0	x
Before you begin	DESTI WIN-MR2BO	NATION SEF 7CRMO1.DI.	RVER TEST
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.	ole service ocuments,	s, or
	< Previous Install	Cano	:el

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

Select installation	on type Destination ser WIN-MR2807CRM01.DL
Before You Begin	Select the installation type. You can install roles and features on a running physical computer or vir machine, or on an offline virtual hard disk (VHD).
Server Selection Server Roles	Role-based or feature-based installation Configure a single server by adding roles, role services, and features. Pamoto Decktop Services installation
Features Confirmation Results	Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-l or session-based desktop deployment.
	< Previous Netwo Install Can
Click Next. On the Select dest	Fination conver page, collect a conver from the conver pool
Click Next. On the Select dest	tination server page, select a server from the server pool.
Click Next. On the Select dest Page: Contemporation Contemporation Provide Pro	tination server page, select a server from the server pool. Add Roles and Features Wizard
Click Next. On the Select dest Select destination	tination server page, select a server from the server pool. Add Roles and Features Wizard
Click Next. On the Select dest E Select destination	Add Roles and Features Wizard On Server
Click Next. On the Select dest Res Select destination Before You Begin	tination server page, select a server from the server pool. Add Roles and Features Wizard On Server Select a server or a virtual hard disk on which to install roles and features.
Click Next. On the Select dest Belect destination Before You Begin Installation Type	Lination server page, select a server from the server pool. Add Roles and Features Wizard On Server Select a server or a virtual hard disk on which to install roles and features. © Select a server from the server pool
Click Next. On the Select dest Select destination Before You Begin Installation Type Server Selection	Lination server page, select a server from the server pool. Add Roles and Features Wizard OD SERVER OD SERVER Select a server or a virtual hard disk on which to install roles and features. Image: Select a server from the server pool Image: Select a virtual hard disk
Click Next. On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles	Lination server page, select a server from the server pool. Add Roles and Features Wizard ON SERVER Select a server or a virtual hard disk on which to install roles and features. Image: Select a server from the server pool Select a virtual hard disk Server Pool
Click Next. On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation	Add Roles and Features Wizard Add Roles and Features Wizard DESTINATION SERV 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:
Click Next. On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	tination server page, select a server from the server pool. Add Roles and Features Wizard DESTINATION SERV 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: Name
Click Next. On the Select dest E Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	tination server page, select a server from the server pool. Add Roles and Features Wizard DESTINATION SERV DESTINATION SERV 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: IP Address Operating System WIN MEREORCEMOI DI 102 168 50 50 Mircereft Windows Server 2012 R2 Standard
Click Next. On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and Features Wizard Add Roles and Features Wizard DESTINATION SERV WIN-MR2BO7CRMO1.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 Server Pool Filter: Name IP Address Operating System WIN-MR2B07CRM01.DL 192.168.50.50 Microsoft Windows Server 2012 R2 Standard
Click Next. On the Select dest E Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	tination server page, select a server from the server pool. Add Roles and Features Wizard DESTINATION SERV 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: Name IP Address WIN-MR2B07CRMO1.DL 192.168.50.50 Microsoft Windows Server 2012 R2 Standard 1/Conserver@l found
Click Next. On the Select dest Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and Features Wizard DESTINATION SERV OD 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: Name IP Address Operating System WIN-MR2B07CRMO1.DL. 1 Computer(s) found This page shows servers that are running Windows Server 2012, and that have been added by using Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

- 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.



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	 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. Things to note: Before you install this role, you should identify which network connections on this server you wan use for setting up virtual switches. After you install Hyper-V, you can use Hyper-V Manager to create and configure your virtual machines.
lick Next. In the Create Virtu	More information about Hyper-V
lick Next. On the Create Virtu	More information about Hyper-V < Previous
lick Next. On the Create Virtu Create Virtual Sv	More information about Hyper-V < Previous Install Cance Install Cance

Next >

Cancel

Install

< <u>P</u>revious

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

Installation Type Server Selection Server Roles Features Hyper-V Virtual Switches Migration Default Stores Confirmation Results	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 migration, use Hyper-V settings after you install the Allow this server to send and receive live migrations of virtual machines Authentication protocol Select the protocol you want to use to authenticate live migrations.
--	--

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

Default Stores	DESTIN WIN-MR2B07	IATION SERV CRMO1.DI.TE
Before You Begin Installation Type Server Selection Server Roles Features	Hyper-V uses default locations to store virtual hard disk files and virtual machine configur unless you specify different locations when you create the files. You can change these def now, or you can change them later by modifying Hyper-V settings. Default location for virtual hard disk files: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks	ation files, ault locatio Brows
Hyper-V	Default location for virtual machine configuration files:	
Virtual Switches	C:\ProgramData\Microsoft\Windows\Hyper-V	Brows
Migration		
Default Stores		
Confirmation		
	< Previous Net > Install	Cance

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

2	Add Roles and Features Wizard	_ D 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 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 Specify an alternate source path	DESTINATION SERVER WIN-MR2807CRM01.DLTEST on selected server, click Install. ired
	< <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.

1	SQL Server Installation Center
Planning Installation Maintenance Tools Resources Advanced Options	 New SQL Server stand-alone installation or add features to an existing installation Launch a wizard to install SQL Server 2014 in a non-clustered environment or to add features to an existing SQL Server 2014 instance. New SQL Server failover cluster installation Launch a wizard to install a single-node SQL Server 2014 failover cluster. Add node to a SQL Server failover cluster Launch a wizard to add a node to an existing SQL Server 2014 failover cluster. Upgrade from SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012 Launch a wizard to upgrade SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012 to SQL Server 2014.
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 Serve 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	SQL Server 2014 Setup ar 2014 to install. Validate this instance of SQL Server 2014 by entering the 25-character key from the Microso certificate of authenticity or product packaging. You can also specify a free edition of SQL Server features, as documente Server Books Online, and is activated with a 180-day expiration. To upgrade from one editio another, run the Edition Upgrade Wizard. Specify a free edition: Evaluation Specify a free edition: Evaluation Specify a free edition: Second S	ft erver, d in S	such	×	
Complete	< Back	0	ancel	~	

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

5	SQL Server 2014 Setup	
License Terms To install SQL Server 2014, y Product Key License Terms Global Rules Product Updates Install Setup Files Install Rules Setup Role	ou 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 yo 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 Micross undates	u ;, oft
Feature Selection Feature Rules Feature Configuration Rules Ready to Install Installation Progress Complete	updates, supplements,	e Pri
	* Microsoft SQL Server 2014 also includes a Visual Studio component that will have CEIP settings turn off by default. If Visual Studio is installed, this component will use the CEIP settings for Visual Studio. < <u>Back</u> <u>Next > </u> Canc	ied

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	d before Setup			
Product Key License Terms Global Rules Product Updates Install Setup Files	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 Fusion Active Template Library (ATL) Previous releases of SQL Server 2008 Business Intelligence Devel Consistency validation for SQL Server registry keys Computer domain controller Microsoft .NET Application Security Windows Firewall Block install when Microsoft SQL Server 2014 CTP1 is present.	Status Passed Passed Passed Passed Warning Passed			
	< <u>B</u> ack <u>Next</u>	Cancel	ŀ	lelp	

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	 SQL Server Feature Installation Install SQL Server Database Engine Services, Analysis Services, Reporting Services, Integration Services, and other features. 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. Add SQL Server Database Relational Engine Services to this installation. All Features With Defaults Install all features using default values for the service accounts.
	< <u>B</u> ack Next > 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

	SQL Serve	r 2014 Setup	
Feature Selection Select the Enterprise features to	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	Instance Features Database Engine Services SQL Server Replication Full-Text and Semantic Data Quality Services Reporting Services - Nativ Shared Features Reporting Services Add-in Data Quality Client Client Tools Connectivity Integration Services	Extractions for Sea ≡ e Point for SharePoint Proc	The configuration and operation of each instance feature of a SQL Server instances is isolated from other SQL Server instances. SQl Server instances can operate side-by-side on Prerequisites for selected features: Already installed:
Feature Configuration Rules	< III	>	
Ready to Install	Select <u>A</u> ll <u>U</u> nselect All		
Complete	Instance <u>r</u> oot directory:	C:\Program Files\Mic	rosoft SQL Server\
	Shared feature directory:	C:\Program Files\Mic	rosoft SQL Server\
	Shared feature directory (v06)	C\Program Files (x86	\\Microsoft SOL Server\

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

1		SQL Server 2014	Setup		_ 🗆 X
Instance Configuration Specify the name and instance	ID for the instance of S	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	Instance <u>I</u> D:	MSSQLSERVER			
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	
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	
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.

Specify Database Engine authority	entication security mode, a	administrators 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 Specify the authenti Authentication Moc Windows authen Mixed Mode (SQ Specify the password: Enter password: Confirm password: Specify SQL Server a	Data Directories FILESTREAM ication mode and administrators for the Databa de tication mode L Server authentication and Windows authentic dfor the SQL Server system administrator (sa) a e e dministrators	se Engine. ation) ccount.
	Add Current User	O1\Administrator (Administrator) Add Remove	SQL Server administrator 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 featur	es 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 Ready to Install Installation Progress Complete	Ready to install SQL Server 2014: Summary Edition: Enterprise Action: Install (Product Update) Prerequisites Already installed: Already installed: Already installed: Already installed: To be installed from media: Microsoft Visual Studio 2010 Redistributables Microsoft Visual Studio 2010 Redistributables Microsoft Visual Studio 2010 Shell General Configuration Features Client Tools Connectivity Client Tools SDK Macanement Tools + Racie CityProgram Files\Microsoft SQL Server\120\Setup Bootstrap\Log\20170814_070653\ConfigurationFile.	⇒ N

21. Wait for the install to finish.

5	SQL Server 2014 Setu	ıp 💶 🗖	X
Complete Your SQL Server 2014 install	ation completed successfully with product updates.		
Product Key	Information about the Setup operation or possi	ible next steps:	
Clobal Pulsa	Feature	Status	1
Global Rules	Management Tools - Complete	Succeeded	
Product Updates	Client Tools Connectivity	Succeeded	Ξ
Install Setup Files	Client Tools SDK	Succeeded	
Install Rules	Client Tools Backwards Compatibility	Succeeded	
Setup Role	Management Tools - Basic	Succeeded	-
Feature Selection	Matabase Engine Services	Succeeded	
Feature Rules			
Instance Configuration	Details:		
Server Configuration	Viewing Product Documentation for SQ	I Server	Τ,
Database Engine Configuration	Viewing Product Documentation for 54		Ē
Feature Configuration Rules	Only the components that you use to view	and manage the documentation for SQL Server have	1
Ready to Install	been installed. By default, the Help Viewer	component uses the online library. After installing	
	SQL Server, you can use the Help Library in	vanager component to download documentation to	
Installation Progress	(<http: ?linkid="29</td" fwlink="" go.microsoft.com=""><td>39578>).</td><td>-</td></http:>	39578>).	-
Complete	<u></u>		1
	Summary log file has been saved to the followin	ng location:	
	<u>C:\Program Files\Microsoft SQL Server\120\Set</u> <u>MR2B07CRM01_20170814_070653.txt</u>	up Bootstrap\Log\20170814_070653\Summary_WIN-	
		Close Help	

22. Click Close.

2.4.2 Open Port on Firewall

1. Open Windows Firewall with Advanced Security.



2. Click Inbound Rules.

for the same second second	Windows	Firewall with Advanced S	ecurity			
ile <u>A</u> ction <u>V</u> iew <u>H</u> elp						
• 🔿 🙍 📰 🗟 🚺 🖬						
Windows Firewall with Advance	Inbound Rules					Actions
🔣 Inbound Rules	Name	Group	Profile	Enabled	A ^	Inbound Rules
Cutbound Rules	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	No	A	Man Parlo
Connection Security Rules	BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Cach	All	No	A	New Kulling
Monitoring	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All	No	A	Filter by Profile
	OM+ Network Access (DCOM-In)	COM+ Network Access	All	Yes	A	Filter by State
	COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati	All	No	A≡	Filter by Group
	Ore Networking - Destination Unreacha	Core Networking	All	Yes	A	15
	Ore Networking - Destination Unreacha	Core Networking	All	Yes	A	View
	Ocore Networking - Dynamic Host Config	Core Networking	All	Yes	A	a Refresh
	Ore Networking - Dynamic Host Config	Core Networking	All	Yes	A	Export List
	🖉 Core Networking - Internet Group Mana	Core Networking	All	Yes	A	2 Hala
	Ocore Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	A	M Help
	Ore Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	A	
	Ore Networking - Multicast Listener Do	Core Networking	All	Yes	A	
	Ore Networking - Multicast Listener Qu	Core Networking	All	Yes	A	
	🖉 Core Networking - Multicast Listener Rep	Core Networking	All	Yes	A	
	🖉 Core Networking - Multicast Listener Rep	Core Networking	All	Yes	A	
	Ocore Networking - Neighbor Discovery A	Core Networking	All	Yes	A	
	Ocore Networking - Neighbor Discovery S	Core Networking	All	Yes	A	
	🕑 Core Networking - Packet Too Big (ICMP	Core Networking	All	Yes	A	
	Ocore Networking - Parameter Problem (I	Core Networking	All	Yes	A	AL 10
	Ore Networking - Router Advertisement	Core Networking	All	Yes	A	
	Ocore Networking - Router Solicitation (IC	Core Networking	All	Yes	A	
	Ocore Networking - Teredo (UDP-In)	Core Networking	All	Yes	A	
	Ore Networking - Time Exceeded (ICMP	Core Networking	All	Yes	A	
	O Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo	All	Yes	A	
	O Distributed Transaction Coordinator (RP	Distributed Transaction Coo	All	Yes	A	
	O Distributed Transaction Coordinator (TC	Distributed Transaction Coo	All	Yes	A	
	File and Printer Sharing (Echo Request - I	File and Printer Sharing	All	No	A	
	File and Printer Sharing (Echo Request - I	File and Printer Sharing	All	No	A	
	File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No	A	
	File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	No	A	
	File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	No	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 Wiz	zard	X
Protocol and Ports Specify the protocols and ports	o which this rule applies.		
Specify the protocols and ports Steps: Rule Type Protocol and Ports Action Profile Name	 o which this rule applys. Does this rule apply to TCP or UDP? ICP UDP Does this rule apply to all local ports or specifi All local ports Specific local ports: 1433 Example 	ic local ports? 2: 80, 443, 5000-5010	
		< Back Nert > Cancel	

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

	New mooding Nate wizard
Action Specify the action to be taken w	hen a connection matches the conditions specified in the rule.
Steps: Protocol and Ports	What action should be taken when a connection matches the specified conditions?
Action Profile Name	This includes connections that are protected with IPsec as well as those are not. 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 Rule node.
	Customize
	< <u>B</u> ack <u>N</u> ext > Cancel

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

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

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

<i>🖌</i>	New Inbound Rule Wizard	
Name Specify the name and description of	of this rule.	
Steps:		
Rule TypeProtocol and Ports		
Action Profile	Name:	
 Name 	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		olor 342. Server management studio (Manimistrator)				
• 🔄 • 😅 🚽 🔔 New Query 👍 🔂 🔂 🖓 🖓 🗛 🕰 🖄 🕫	· [· [] · [] · [] ·] ·			· · · · · · · · · · · · · · · · · · ·		
ct Explorer + 0 ×						
ned. 2 2 1 7 0 5						
	<u> 198</u>	Connect to Server				
	Microsoft	SQL Server 2014				
		Provide State Stat				
	Server type:	Database Engine				
	Server name:	WOLMR2002040401	· ·			
	Authentication:	Windows Authentication	*			
	Over nome	WIN-MR280/7CRM01-Admini	rator v			
	Passent					
		Remember passions				
	Con	nerg Cancel Help	Options >>			

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

	Microsoft SQL S	Server Managemer	rt Studio (Administrator)		- 0 x
e Edit View Debug Tools Window Help					
🗊 * 🔄 - 😅 🚽 🔮 New Query 📑 🔂 🔂 🔂	11日 4・4・11・11日 日	-	3	· 2399.	
bject Epslover + 0 × 1 innest+ 2 2 2 = 7 2 3 ⊗ W44-M2000CSMOI (SQL Serve 122) ⊗ W45-M2000CSMOI (SQL Serve 122) ⊗ W45-M2000CSMOI (SQL Serve 122) ⊗ Substances ⇒ Subs					
August Cryptographic Providers Build August Supervariant Specifications Supervariant Specifications Build Server Objects Replication una Objection					
Management Management Management Management Monagement Monagement Magement M					
and a second sec					

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

- R WALLARDONTOPLANT JON Comments	音	Loois	New	- D X		
* Databases	Select a page	Sout + D Hep		Land Land		
E Cogins Server Roles Credentials Construction Resident	Server Roles User Mapping Securaties	Login game:	douter1	Spech		
a Garante Construction		SQL Server authentication Pressured				
Server Objects Beolication		Confirm password	[
R 🔄 AlwaysOn High Availability		Cit assessed				
Integration Services Catalogs SQL Server Agent (Agent XPs disabl		Enforce password polo	r Minn			
		V User must change password at next login				
		 Mapped to cetticate Mapped to asymmetric key 				
	Connection	Bap to Credential		* <u>8</u> H	64	
	Server WIN-MR2B07CRM01	Mapped Credentials	Gredential Provider			
	Connection: WIN-MR2807CRIM01VAdministrat					
	Ven corrector propeties					
	Progress			Familys		
	O reedy	Default gistabase: Default language:	cdelaulto	~		
			0	K, Cancel		
			10000	8		

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.

a	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
	< Previous Next > Install Cancel

3. Click Next.

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

C 1	. DESTINATION SER
Select installatio	оп туре мssqLdu
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	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 destinat	ion server			DESTINATION SERVER MSSQL.DI.IPDR
Before You Begin Installation Type Server Selection Server Roles Features	Select a server or a v Select a server fro Select a virtual he Server Pool Filter:	irtual hard disk on which om the server pool ırd disk	to install roles and features.	
Confirmation Results	Name	IP Address	Operating System	
	1 Computer(s) found This page shows sen Add Servers comman	192.168.78.103 rers that are running Wind	Microsoft Windows Server 2012 dows Server 2012, and that have b line servers and newly-added serv	een added by using the
	collection is still inco	mplete are not shown.	vious Next > Ir	Istall Cancel

7. Click Next.

elect server roles	5	DESTINATION SERV MSSQLDI.IF
Before You Begin Installation Type	Select one or more roles to install on the selected server.	Description
Server Selection		Web Course (IIC) and idea a selicity
Server Roles	Application Server	manageable, and scalable Web application infrastructure
Features	DNS Server	appreciation initiation detailed
Confirmation	Fax Server	

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

Select server ro	Add Roles and Features Wizard		DESTINATION SERVE
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add features that are required for Web Serv The following tools are required to manage this feature, have to be installed on the same server. Web Server (IIS) Management Tools [Tools] IIS Management Console	er (IIS)? but do not	tion ver (IIS) provides a reliable able, and scalable Web on infrastructure.
	✓ Include management tools (if applicable) Add Features	Cancel	
	< Previous	Next >	Install Cancel
lick Add Features.			
	Add Roles and Features Wizard		
Select server role	Add Roles and Features Wizard		
Select server role Before You Begin Installation Type	Add Roles and Features Wizard	ver.	DESTINATION SERV MSSQLDLIP
Select server role Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Add Roles and Features Wizard Select one or more roles to install on the selected ser Roles Application Server DHCP Server DNS Server Fax Server Image: File and Storage Services (1 of 12 installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Windows Deployment Services Windows Server Update Services Windows Server Update Services	лет.	DESTINATION SERV MSSQLDLIP Description Web Server (IIS) provides a reliabl manageable, and scalable Web application infrastructure.

11. Ensure that all desired features are selected.

È	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	Features Image: State Sta	Description .NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
	Group Policy Management IIS Hostable Web Core Ink and Handwriting Services V	
	< Previous Next >	Install Cancel
lick Next.	Add Roles and Features Wizard	Install Cancel
lick Next.	< Previous Next > Add Roles and Features Wizard (S) Web servers are computers that let you share information over the	Install Cancel
Veb Server Role	Add Roles and Features Wizard 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 Servic diagnostic and administration, a unified Web platform that integral Communication Foundation.	DESTINATION SERVER MSSQLDLIPDR Internet, or through intranets and tes (IIS) 8.5, ASP.NET, and Windows
Lick Next. Web Server Role Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS)	Add Roles and Features Wizard 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 Servic diagnostic and administration, a unified Web platform that integral Communication Foundation. Things to note: • Using Windows System Resource Manager (WSRM) can help ensister traffic, especially when there are multiple roles on this context of the server traffic.	Install Cancel DESTINATION SERVER MSSQLDLIPDR Internet, or through intranets and is (IIS) 8.5 with enhanced security, tes IIS 8.5, ASP.NET, and Windows sure equitable servicing of Web mputer.
Lick Next. Web Server Role Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	 < Previous Next > 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 Servic diagnostic and administration, a unified Web platform that integral Communication Foundation. Things to note: Using Windows System Resource Manager (WSRM) can help ensister traffic, especially when there are multiple roles on this cort. The default installation for the Web Server (IIS) role includes the enable you to serve static content, make minor customizations (serrors), monitor and log server activity, and configure static content.	Install Cancel DESTINATION SERVER MSQLDIJPDF Internet, or through intranets and ses (IIS) 8.5 with enhanced security, tes IIS 8.5, ASP.NET, and Windows sure equitable servicing of Web mputer. installation of role services that such as default documents and HTT sent compression.
Lick Next. Web Server Role Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	 < Previous Next > Add Roles and Features Wizard (IIS) Web servers are computers that let you share information over the extranets. The Web Server role includes Internet Information Servic diagnostic and administration, a unified Web platform that integral Communication Foundation. Things to note: Using Windows System Resource Manager (WSRM) can help ensister traffic, especially when there are multiple roles on this context reading server traffic, especially when there are multiple roles on this context reading you to serve static content, make minor customizations (servors), monitor and log server activity, and configure static context matching and log server activity. 	Install Cancel DESTINATION SERVER MSSQLDUPPR Internet, or through intranets and tes (IIS) 8.5 with enhanced security, tes IIS 8.5, ASP.NET, and Windows sure equitable servicing of Web mputer. installation of role services that such as default documents and HTTI ient compression.

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 Image: Common HTTP Features Image: Custom Logging Image: Custom Logging <th>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.</th>	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.
	S FIEVIOUS HEAT	instan Cancer
Click Next.	Add Roles and Features Wizard	DESTINATION SERVE
Click Next. Confirm installat Before You Begin Installation Type Server Selection Server Roles Features	Add Roles and Features Wizard tion selections 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 displa been selected automatically. If you do not want to install these their check boxes.	DESTINATION SERVE MSSQL.DI.PDI ed server, click Install. yed on this page because they have optional features, click Previous to clea
Click Next.	Add Roles and Features Wizard tion selections To install the following roles, role services, or features on selected Restart the destination server automatically if required Optional features (such as administration tools) might be displateen selected automatically. If you do not want to install these their check boxes. Web Server (IIS) Management Tools IIS Management Console Web Server Common HTTP Features Default Document Directory Browsing HTTP Errors Static Content Health and Diagnostics	DESTINATION SERVE MSSQL.DIJPDI ed server, click Install. yed on this page because they have optional features, click Previous to clear r

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	
	i Feature installation	
	Installation succeeded on MSSQLDI.IPDR.	
	Web Server (IIS)	
	Management Tools	
	IIS Management Console	
Confirmation	Common HTTP Features	
Results	Default Document	
	Directory Browsing	
	HTTP Errors	
	Static Content	
	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.	· 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	isk (C:)		
File Home Shar	e View Manage				~ ()
۰ 🕁 🐑 🛞 🛞	This PC 🕨 Local Disk (C:)		~ ¢	Search Local Disk (C:)	,p
🖌 Favorites	Name	Date modified	Туре	Size	
Desktop	퉲 inetpub	1/26/2018 1:52 PM	File folder		
\rm 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		
🖳 This PC	Users	11/9/2017 6:27 PM	File folder		
🙀 Network	🎍 Windows	1/26/2018 1:52 PM	File folder		
6 items					::: .

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

🚣 l 💽 🚺 🗢 l		Local Disk (C:)			□ ×
File Home Share	View				~ ()
🔄 🎯 👻 🕆 👗 🕨 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.

)		Internet Informa	ation Services (IIS) Manager	X
🔪 🕨 Start Page				<u>₩</u> ≥ \$
File View Help				
Connections 📑 🖄 🥵 Start Page	Morrosoft Internet Info Application Server Mar	ormation Se	ervices 8	
MSSQL (MSSQL\Administrate	Recent connections	5	Connection tasks	Online resources
	Name MIMSSQL < III	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
	IIS News	click the Enable IIS Nev	is link to get the most recent online news.	Enable IIS News
III >				
eady				

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

		Internet Inf	formation Services (IIS)	Manager	
€ 10 € MSSQL + Site	в				90 10 li 🖗
File View Help					Management
Connections .• 🗔 🖄 🚱	Sites				Actions Add Website
Start Page	Filter	+ 🌾 Go - 🕁 Show A	All Group by: No Grouping		Set Website Defaults
Application Pools	Name *	ID Status	Binding	Path	😧 Help
m >	c Features View a	Content View	18		

7. Click Add Website....

		Add Website	e			?	
Site name:		Application pool:			Select		
Content Directory					Jelect		
Physical path:							
Pass-through authen	tication						
Connector	Test Cattings						
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						
 Start Website immed 	latery						
 Start Website immed 	inately						

8. Enter the desired site name.

	Add We	bsite	?
Site name:	Application	pool:	
MISSQLSITE	MSSQLSITE		belect
Content Directory			
Physical path:			
Pass-through authe	ntication	100	
Connector	Total California		
Connect as	rest settings		
Binding			
Туре:	IP address:	Port:	
http	All Unassigned	✓ 80	
Host name:			
Example: www.cont	oso com or marketing contoso	com	
Example: www.com	osolcom of marketing.comoso.	com	
 Start Website imme 	diately		
		OK	Carro

9. Click ... under Physical path:.

Cita nama	Application peak
MSSQLSITE	MSSQLSITE Select
Content Directory Physical path:	
	Browse For Folder
Connect as Test Settings	Select a directory for the application.
Binding Type: IP address: http Host name: Example: www.contoso.com or ma	Image: Second system Image: Second system Image: Second
Start Website immediately	Make New Folder OK Cancel

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

	Add Website	ſ
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		
✓ Start Website immediately		
	ОК	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 Sele	ect
Content Directory		
Physical path:		
C:\www		
Pass-through authentication	n	
Connect as Test Se	ttings	
Binding		
Type: IP ad	ldress: Port:	
http v 192.	168.81.107 🗸 80	
Hert name		
MSSOL di indr		
Example: www.contoso.com	n or marketing.contoso.com	
Start Website immediately		
Start Website immediately		

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		- 🗆 X
File Action View Help				
🗢 🔿 🙇 📰 🤾 📋 🗙 🗉	0 🕒 🚺 🖬 % 🕷 🗑 🏹	°₽.		
 Active Directory Users and Com Saved Queries BUIIPOR Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Microsoft Exchange Security Users 	Name Abraham Administrator Allowed RODC Password Replication Cett Publishers Cloneable Domain Controllers Denied RODC Password Replication DiscoverySearchMailbox (D919BA05 DrsAdmins DnsUpdateProxy Domain Admins	Last Name Leptoceratops MsExchDiscoveryMailbox D919BA05-46A6-41	Type User User Security Group Security Group Security Group User Security Group Security Group	Description User Account Built-in account Members in this Members of this Members of this Members in this DNS Administra DNS clients who Designated adm
Ŗ	Domain Computers Domain Controllers Domain Guests Domain Users Enterprise Admins Enterprise Read-only Domain Contro Exchange Online-ApplicationAccount EvertedEmail.4c1f4d8b-8179-4148	FederatedEmail.4c1f4d8b-8179-4148-93bf-00a	Security Group Security Group Security Group Security Group Security Group User User	All workstations All domain cont All domain gues All domain user Designated adm Members of this
	 Franklin Group Policy Creator Owners Guest Harry John Lyndon 	Delano Raptorvelt S Triceratops Quincy Ankylosaurus Brontosaurus Johnson	User Security Group User User User User	User Account Members in this Built-in account User Account User Account User Account
< III >				>

- 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			
DI.IPDR/Users			
DSP Initials:			
Service			
DSP Service			
@DI.IPDR ¥			
-Windows 2000):			
dspservice			
< Back Next > Canc	el		
	New Object - User DI.IPDR/Users DSP Initials: Service DSP Service @DI.IPDR V -Windows 2000): dspservice		

- 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 Mana	gement Editor		_ 🗆 X
File Action View Help File Action View Help File Action View Help File Action View Help File Action Prefault Domain Controllers Poli Computer Configuration P Policies File Action View Help File Action Controllers Poli Policies File Action View Help File Action Controllers Poli Policies File Action View Help File Action Controllers Poli Policies File Action Policies File Action Policies File Policies File Policies	Group Policy Mana Default Domain Controller Select an item to view its description.	gement Editor rs Policy [AD-DNS.DI.IPDR] Name Mage Computer Configuration	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 | |
| , i i i i i i i i i i i i i i i i i i i | |
| | |
| 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	x
Policy Explain	
Audit Directory Service Changes	
□ Configure the following audit events:	
<u>F</u> ailure	
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	<u>.</u>	Group Policy Management Editor	_ D ×
 Windows Firewall with Admonstrate and the second sec	File Action View Help		
Image: Subcategory Audit Events Image: Subcategory Audit Directory Service Replication Image: Subcategory Audit Directory Service Changes Image: Subcategory Audit Directory Service Replication Image: Subcategory Image: Subcategory Image: Subcategory Audit Directory Service Replication Image: Subcategory Image: Subcategory Image: Subcategory Image: Subcategory Image: Subcategory Image: Subcategory Image: Subcategory Image: Subcategory Image: Subcategory Image: Subca	🗢 🄿 🔁 💽 🗟 🖬		
 ▷ interpretation ▷ interpretation ▷ interpretation ▷ interpretation ▷ interpretation ▷ interpretation ○ interpretation ○ interpretation ○ interpretation ○ interpretation ○ interpretation ○ interpretation 	Windows Firewall with Ad Windows Firewall with Ad Wireless Network List Manager Pol Wireless Network (IEEE 80 Wireless Network (IEE 80 Wireless Network (Subcategory Audit Detailed Directory Service Replication Audit Directory Service Access Audit Directory Service Changes Audit Directory Service Replication	Audit Events Not Configured Not Configured Success Not Configured
	 ↓ Logon/Logoff ↓ Object Access ↓ Privilege Use ↓ Privilege Use ↓ Object Access ↓ Object Access ↓ Privilege Use ↓ Object Access ↓ Preferences ↓ User Configuration ∨ 	₿ I	

- 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	DO) :				
DI							
Descript	tion:						
Domain	functional leve	l:					
Window	s Server 2008						
Forest fo	unctional level:						
Window	is Server 2008						
] [
	ОК		Cancel	Apply		He	elp

24. Click the Security tab.

Group or user names:				
Everyone				
Man SELF				
	F			
& Organization Manage	ement	(DI\Organi	zation Manage	ment)
			Add	Remove
Permissions for Everyone			Allow	Deny
Full control				
Read				
Write				
Create all child objects				
Delete all child objects				
For special permissions or	advan	ced settin	ns click	
Advanced.	Gavan	ood ooting	go, onore	Advanced
				.0

25. Click Advanced.

Owner:	Administrators (DI\Administr	ators) Change		
Permission	s Auditing Effective A	ccess		
For addition	al information, double-click a per	mission entry. To modify	permission entry sele	ect the entry and click Edit (if avail
	antinomiation, double crick a per		permission energy, ser	
Type	Principal	Access	Inherited from	Applies to
Allow	Exchange Windows Permissi	Change password	None	Special
🔏 Allow	Exchange Windows Permissi	Reset password	None	Special
🖲 Allow	Exchange Servers (DI\Exchan	Special	None	Descendant InetOrgPerson
😣 Allow	Exchange Servers (DI\Exchan	Special	None	Descendant User objects
😣 Allow	Pre-Windows 2000 Compatib	Special	None	Descendant InetOrgPerson
😫 Allow	Pre-Windows 2000 Compatib	Special	None	Descendant Group objects
👫 Allow	Pre-Windows 2000 Compatib	Special	None	Descendant User objects
👫 Allow	Authenticated Users	Enable per user reversi	None	This object only
🛃 Allow	ENTERPRISE DOMAIN CONT	Replicating Directory	None	This object only
🛃 Allow	Authenticated Users	Unexpire password	None	This object only
🚨 Allow	Authenticated Users	Update password not r	None	This object only
All		Deulisetian Diserten.	News	This shirest each.
Add	Remove View			Restore de
Add	Remove View			Restore

- 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

Per For a	missions	Auditing Effective Ac	cess dit entry. To modify an a	udit entry, select the entr	y and click Edit (if available).
Aud	Type Succ	ries: Principal Everyone	Access	Inherited from None	Applies to Special
28 <u>8</u> 52	Succ	Everyone Domain Users (DI\Domain Us	All extended rights	None	Special This object only
82	Succ	Administrators (DI\Administr	All extended rights	None	This object only
<u>88</u>	Succ	Everyone	Special	None	This object only
	Add	Remove			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.

1			Auditing Entry for DI	-		x
	Type:	Success 🗸				^
						⊨
	Applies to:	This object and all descendant objects V				43
	Permissions	8				
		Full control	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			-
Ľ					Cance	-
			U.V.		canee	

	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	VICE		
Section Market M	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

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 I	icense			
O Active	Directory Forest Recove	ery		
Active	Directory State Manage	ement		
O Full License				
Bro	owse			
a în			\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		
Enter the use the Semperis	rname and password Management Server	t to use for the ADSM service accord to communicate with the ADSM a	unt. The Service account is use agents.	ed by
Forest Name:		Service account:	Password:	
emperis			?	() ()
k the > but	tton.			
k the > but	tton. dd the Servic	e Account to the autho	rization group	x
ck the > but A A A t it	tton. dd the Servic lick OK to add the ccounts" group. does not exist.	e Account to the autho e Service Account to the "Ser The group will be created in t	mperis ADSM Service	×

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.

	AGREEMENT	LICENSE	CONFIGURATION	IN STALLATION	X
				.	•
	Select installa Create a new Create a new Use an exist Use an existin Install SQL Use Microsoft	tion type w database database on an existin ting database g database on an exis Express locally SQL Express 2014 run	ng SQL server Si sting SQL server Ni nning locally U	rovide connection details erver: ort: Windows Authentication sername: assword:	?
	Semperis			(*	
14. Cl	lick the > butto	on.	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.

6	ADSM AGENT	MANAGEMENT				ڻ ف
		TANAGENENT			JOE	STATUS
- ALL C	DOMAINS - • DOW	NLOAD AGENT INSTAL	LER	Deploy	Latest Velson + RUN	ACTION
	NAME *	DOMAIN + *	STATUS + +	VERSION + •	OS VERSION + +	ACTION
	AD-DNS	DUPDR	No agent	0.0 0.0	3.40	20
	AD-DNS08	DI. IPDR	No agent	0.0.0.0	12 L	30

- 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.

all -	Semperis		Domain: DLIPDR •	I 💿 Aamin	istrator 🔅 SETTINGS	🕐 LOGOUT
Current Do DI IPDR	main:					
N	DASHBOARD	> Agents (DI.IPDR)				
-	CHANGED	> Database				
2	ITEMS	> Email Alerts				
×	DELETED	> Group Policy				
	CONFIGURATION	> Data Collection				
	PARTITION	Y Audit				
	DNS	Audit Configuration Wizard				Run
	GPO	Define audit settings and manage Audit A	gents and Audit Collectors.			
		Audit Agent			Downloa	id Agent
Ø	REPORTS	Audit Collector			Download 0	Collector
	BOL	> General		G		
	STRIUS	> Operation Log			Activate Windows	
20	ROLE-BASED ACCESS CONTROL				Go to System in Control	Panel 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.

dir.	Semperis						Domain: DLIP	DR 🔹 I	Administrator	SETTINGS (9 LOC
Current Do DLIPDR	imain:	2	C	HAN	GED ITEMS				Live		
N	DASHBOARD	AUG 9	AUG	10	AUG 11	AUG 12		Â	UG 13 Aug 13,	SEA1	ксні
3	CHANGED		UND	<u>6</u>	ECTED				FILTER RESULTS	۵ 💩	Ľ
×	DELETED	▼ Sh	owing	results	1 - 9 of 9 📴 9 ung	ouped results NEXT >	LAST »	20 • Go to	Gro	up results by opera	tion (
a	CONFIGURATION PARTITION	0	OP	CLASS	DN	ATTRIBUTE	OLD VALUE	NEW VALUE	TIME	CHANGED BY	
			0	1	Administrator	lastLogonT	2018-08-03	2018-08-13	08/13/2018, 3:50:37 PM	ć - s	0
	DNS		Ø	2	HealthMailboxf3	lastLogonT	2018-08-03	2018-08-13	08/13/2018, 3:39:09 PM	-	Θ
-			Ø	1	HealthMailboxff	lastLogonT	2018-08-03	2018-08-13	08/13/2018, 3:36:26 PN	C et	0
	GPO		1		WINDOWS10-1	dBCSPwd	<not set=""></not>	<not set=""></not>	08/13/2018, 1:19:54 PM	17.1	Θ
20			0	-	WINDOW510-1	unicodePwd	<secret></secret>	<secret></secret>	08/13/2018, 1:19:54 PM	10 A	Θ
_				-	WINDOWS10-1	ntPwoHisto	1 <secret></secret>	2018-08-13	08/13/2018, 1:19:54 PM		0
Q	REPORTS		-	2	WINDOWSID-1	supplement	2010-07-14	2016-06-15	08/13/2018, 1:19:54 PM		0
			0		WINDOWS10-1	ImPwdHisto	<secret>,</secret>	<secret>,</secret>	08/13/2018, 1:19:54 PM		Θ
1.	JOB	-									
		TSN	owing	results	1 - a or a 📴 a undi	ouped results		-			

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	۲ ()	Administrator	SETTINGS	U LOGOUT
Current Di DI IPDR	omain	Your evaluation	of Semperis AD	5M expired on	Sep 8, 2018.		
N	DASHBOARD						
\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					Vate windows System in Control	i 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.

- atle	Semperis		Domaini	DLIPDR •	1 ① Ao	ministrator	SETTINGS	🕑 госопт
Current Do DI.IPDR	main		Your evaluation of Sem	perts ADSM exp	ired on Sep 8, 20	18,		
N	DASHBOARD							
2	CHANGED	Agents (DI.IPDR)						
×	DELETED ITEMS	> Database Email Alerts 						
-	CONFIGURATION	Authentication Requirements	Anonymous:					Cancel
	PARTITION	Settings required to send notifications and alerts	Enable SSL:					
	DNS		Server:		EXCHANG	E.DI.IPDR		
	GPD		Port:		25			
_			Username:		USERNAM	ιE		
Ø	REPORTS		Password:		PASSWOR	D		
	JOB STATUS		Mail from:		semperis@	idi.ipdr		
	BOUE BASED				SAVD.	Acti	vate Window	
20	ACCESS CONTROL	Alert Recipients						

5. Click Save.

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

Semperis		Domain DLIPDR •	1 (Administrator 	SETTINGS	C LDGOUT
Current Domain Dr. IPDR		Your evaluation of Samparis ADSM au	pined on Sep	8, 2018.		
Снамого птень	> Agents (DI.IPDR)					
DELETED ITEMS	Validate SMTP settings					
	Enter an email address to test successfully, it automatically t administrator@di.ipdr	and validate SMTP settings. If settings v e saved.	alidated			Cancel
DHS DHS				:		
G				CLOSE		
NEPCHTS		Username	USE	RNAME		
		Mail from: -	semp	veris@di.ipdr		
STATUS			54	VE.		

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

د الله	emperis		Domain: DLIPDR 🔻	l 💿 Admini	itrator 🔅 SETTINGS	O LOGOUT
Current Dom	əin		Port:	25		
i .			Username	-		
\sim	DASHBOARD		Password:	-		
	CHANGED ITEMS		Mail from:	semperis@di.ip	dr	
×	DELETED	Alert Recipients				
	CONFIGURATION PARTITION	Add a recipient administrator@di.ipdi	ADD			
	DNS	EMAIL ADDRESS • •	No alert recipients for	und		
	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		
	ine.	Repeating Error Notification Threshold	Threshold:	60 minutes		Edit
2.1	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[™] 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.

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

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

	Add F	Roles and Features V	Wizard		_		x	
Select destinati	on server			DESTI GLA	NATION	I SERV	'ER DR	
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	Select a server from the server pool						
Server Selection	O Select a virtual ha	O Select a virtual hard disk						
Server Roles	Server Pool	Server Pool						
Features								
	Filter:							
	Name	IP Address	Operating System					
	GLASSWALLDLIPDR	192.168.1.133	Microsoft Windows Serve	er 2012 R2 Stan	dard			
	1 Computer(s) found							
	This page shows serv Add Servers comman collection is still incor	ers that are running Wir d in Server Manager. Of nplete are not shown.	ndows Server 2012, and that fiftine servers and newly-adde	have been adde ed servers from t	ed by u which	using data	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.

퉬 ⊋ 📗 🗢 Visual	C++ RunTi	Application Tools		_ D X
File Home Sha	re View	Manage		~
🔄 💿 🔻 🚺 «	Std ► Visual	C ∀ Ċ	Search Visual C++	RunTime 🔎
🔶 Eavorites	Name	*	Da	te modified
Desktop	/ vcredist	tx64 ⊾	1/3	30/2018 12:00 PM
📜 Downloads		- 6		
📃 Recent places				
💶 This PC				
Desktop				
Documents				
〕 Downloads				
Music				
Pictures				
Videos				
DVD Drive (D:) SO	2			
575 Bille (5) 56				
📬 Network				
	<			
1 item 1 item selected	13.8 MB			
back the box p	ovt to Log	roo to tho	liconco torm	s and car
P Microsoft Visual C	++ 2015 Redi	stributable (x64) - 14[^
A A Micro	oft Vieu		15	
🔹 🛡 Redist	ributable	e (x64) - 1	4.0.23026	
MICROSOFT SOFTWA	RE LICENSE TE	RMS		^
and C++ REDISTRIBU	TUDIO 2015 A	DD-ONs, VISUAL	STUDIO SHELLS	
These license terms or	e an agreemen	t between Micros	oft Corporation (or	
Intrese incense territis di	e an agreeillell	C Dermeen Million	on corporation (or	

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.

ø	Glasswall Hub Setup 📃 🗖 🗙
ALL	Welcome to the Glasswall Hub Setup Wizard
ASSW st every	The Setup Wizard will install Glasswall Hub on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
ant GL/	k}
	Back Next Cancel

2. Click Next.



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

4. Click Next.

閿	Glasswall Hub Setup		
Custom Select t	Setup ne way you want features to be installed		
Click the	icons in the tree below to change the way features will be installed		
	✓ Management Service ✓ File Release Request Service ✓ Database ✓ This feature will be installed on the local hard drive		
L _s			
Back Next 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	Glasswall Hub Setup			
Database Installation Specify the Installation S	Database Installation Settings Specify the Installation Setting for the Glasswall Database			
Database Administrate Configure the credentials	or Credentials : that will be used to create the database (all fields required)			
Authentication Method User name Password	Windows Authentication			
Database Installation Location of the database Installation Log File	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.

閿	Glasswall Hub Setup	_		x
Re	ady to install Glasswall Hub			=
C	Click Install to begin the installation. Click Back to review or change any of nstallation settings. Click Cancel to exit the wizard.	your		
	k₃			
	Back Install		Cano	el

14. Click Install.



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

谩	Glasswall Integration Service Setup		
ALL	Welcome to the Glasswall Integration Service Setup Wizard		
ASSW Ist 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	=
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").	ipany Place, g the alf 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	.VING I BY :T AS O BE HAVE ~
☑ 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			
	Notifications Smtp Username			_	
	Notifications Smtp Password				
		Pack Novt		Cano	
		Dack		Cano	<u> </u>
10.	Click Next.				
	😥 Glass	wall Integration Service Setup	-		x
	Ready to install Glasswall Integration Service				
	Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.				
			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
ALL	Welcome to the Glasswall Administrator Console Setup Wizard
ST EVERV 1	The Setup Wizard will install Glasswall Administrator Console on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	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		
End-User Please re	License Agreement and the following license agreement carefully		
	END USER LICENCE AGREEMENT (EULA)		
This lice number London, software individua	Ince 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 and also, where applicable, the organisation on whose behalf the al is acting) ("You" "Your" "Customer").		
IMPORT/ THE SO COMPAN YOUR A BOUND	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 accep	ot 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.

뤙	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	es snap-in		
This snap-in will always mana	ge certificates for:			
O My user account				
 Service account 				
 Computer account 				
			<u>⊳</u>	
			· \\	
		< Back	Next >	Cancel

- 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:	
Local computer: (the computer this console is running on) Another computer: Browner:	wse
Allow the selected computer to be changed when launching from the command lin only applies if you save the compose.	e. This
< <u>B</u> ack Finish	Cancel

8. Click Finish.

nan-in	Vendor		Con	sole Root	Edit Extensions
ActiveX Control	Microsoft Cor	-		Certificates (Local Computer)	Luit Extensions.
Authorization Manager	Microsoft Cor			er ancares (cocur computer)	Remove
Certificates	Microsoft Cor	=			
Component Services	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 nie you want to import.
File name:
C:\Users\Administrator.DI\Desktop\gw\nist.pfx Browse
Note: Man the an or "Code on to should be since for in 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 V 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.

 Ertificate Import Wizard
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.	
h.	_
Next Cano	el

20. Click Next.

21. Select the same certificate.

 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: 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 Certil 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.

Pr	ivate 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.
	<i>₽</i>
	Next Can
	Certificate Import Wizard
E S	Certificate Import Wizard rtificate Store Certificate stores are system areas where certificates are kept.
CR 110	Certificate Import Wizard rtificate Store Certificate stores are system areas where certificates are kept.
CR 196	Certificate Import Wizard rtificate 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.
) <i>5</i> (e	Certificate Import Wizard rtificate 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 rtificate 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 in the following store Place all certificates in the following store
C	Certificate Import Wizard rtificate 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:
Ce	Certificate Import Wizard rtificate 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 Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Bgowse
Ce	Certificate Import Wizard rtificate 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
Ce	Certificate Import Wizard rtificate 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
Ce	Certificate Import Wizard rtificate 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 Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse
C (e	Certificate Import Wizard rtificate 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 Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse
Ce	Certificate Import Wizard rtificate 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 certificate store based on the type of certificate Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse
Ce	EXT. 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 Place all certificates in the following store: Certificate store: Trusted Root Certification Authorities Browse
) <i>5</i>	Certificate Import Wizard rtificate 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 Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse

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

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

	<u> </u>
🕤 🍠 Certificate Import Wizard	
· ·	
Welcome to the Certificate Import Wizard	
lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identit and contains information used to protect data or to establish secure network	y
connections. A certificate store is the system area where certificates are kept.	
Store Location	
○ Current User	
Local Machine	
To continue, click Next.	
Ν	
Net	ncol
	incer

29. Click Next.

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

-	Open						x
🔄 🍥 👻 🕆 🌗 🕨 Th	is PC → Desktop → gw → NIST	~ ¢	Search NI	ST			Q
Organize 👻 New folder					==	•	0
쑦 Favorites	Name	Date mod	lified	Туре			Size
Desktop	📮 GlasswallLicenceValidation	1/26/2018	3:04 PM	Security	y Cer	tificate	
Downloads Recent places							
in the second process							
🜉 This PC							
Network							
T							
							>
File na	me: GlasswallLicenceValidation	~	X.509 Cer	tificate (*.cer;	*.crt)	¥
			Оре	n		Cancel	
lick Onon				<u></u>			
Certificate Import	wizard ant to import. or.DI\Desktop\gw\NIST\GlasswallLicenceValid2 certificate can be stored in a single file in the following	wyse					
Personal Information	on Exchange- PKCS #12 (.PFX,.P12)						
Cryptographic Mes	sage Syntax Standard- PKCS #7 Certificates (.P7B)						
Microsoft Serialized	I Certificate Store (.SST)						
	L3						

32. Click Next.

Certificate Store	
Certificate stores are system are	eas where certificates are kept.
Windows can automatically selec the certificate.	t a certificate store, or you can specify a location for
○ A <u>u</u> tomatically select the ce	ertificate store based on the type of certificate
elace all certificates in the	following store
Certificate store:	
Personal	B <u>r</u> owse
	N
	14

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	ttings:
Certificate Store Selected by Use	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.

N	Internet Information Services (IIS) Manager									
🔰 👌 Start Page			📴 🛛 🟠 🔞 🗸							
<u>File V</u> iew <u>H</u> elp										
Connections	Monosoft	ices 8								
Start Dage	Application Server Manager									
GLASSWALL (DI\Administrate	Recent connections	Connection tasks	Online resources							
	Name Server GLASSWALL localhost ∠ Ш Ш HIS News HIS News lin	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							
< III >										
Ready										

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

8]	Internet Information Services (IIS) Manager	_ D X
GLASSWALL > Site	; > Default Web Site >	📴 🛛 🟠 🔞 -
File View Help		
Connections	Default Web Site Home Filter: • • •	Actions Explore Edit Permissions Edit Site Bindings Basic Settings View Applications View Virtual Directories Manage Website Start Start Browse %80 (http) Advanced Settings
2	Authentic Compression Default Directory Error Pages Handler HTTP Document Browsing Error Pages Company Respon	Configure Limits
Ready		• <u>1</u> .:

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

			Site	Bindings	? ×
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	 ,				
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 ? X					
Type https	Host Name	Port 443	IP Address *	Binding Informa	<u>A</u> dd <u>E</u> dit <u>R</u> emove <u>B</u> rowse
			Ŕ		
					<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 Inb	ound SMTP Analysis Agent Setup 📃 🗖 🗙					
ALL	Welcome to the Glasswall Inbound SMTP Analysis Agent Setup Wizard					
ASSW 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.					
	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 VIEW I accept the terms in the License Agreement
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.

뻻		Applicatio	on Settings	– – X
	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.pdr/GlasswallManagementServi exchange.dl.pdr:25	Logging Settings Logging directory Log level Performance logging enabled Advanced Settings Scanning interval (ms) Event upload interval (ms) Mail relay interval (ms) Mai 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								
	Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.									
		L _o								
		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.								
		L ₃								
		Back Finish 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*.

🏭 l ⊋ 🛄 = l		NIST		_	D X
File Home Share	View				× 🕐
🔄 🍥 🔻 🕇 퉬 🕨 Thi	is PC → Desktop → gw → NIST		✓ C Search NIS	Т	Q
🗼 Downloads 🗠	Name	Date modified	Type S	ize	
🖳 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					
bownloads	\searrow				
Pictures =					
Videos					
🏭 Local Disk (C:)					
DVD Drive (D:) SC					
Network					
2 items 1 item selected 1	.60 KB				:==

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

🎉 l ⊋ 🕕 = l		Mar	agementService		-	D X
File Home Sha	are View					~ ?
🗲 💿 🔻 🚹 🕷	Program Files 🕨 Gl	asswall 🕨 Managem	entService 🕨	✓ C Search N	/lanagementServi	ce 🔎
☆ Favorites	^ Name	*	Date modified	Туре	Size	
Desktop	🐌 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	📑 Web	N	7/24/2018 6:34 PM	XML Configuratio	7 KB	
膧 Desktop	=	43				
Documents						
鷆 Downloads						
🔰 Music						
📔 Pictures						
📔 Videos						
🚢 Local Disk (C:)						
💹 DVD Drive (D:) SC						
	~					
5 items						:== E

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

↓ 1 1 2 = 1	InboundSmtpAna	alysisAgent		_	
E Home Share H S € ⊚ ▼ ↑ 🎉 « Pi	rogram Files → Glasswall → InboundSmtpAnalysis.	Agent 🕨	✓ ♂ Search Ir	nboundSmtpAn	ې 🗸 م alysis ک
☆ Favorites	Name	Date modified	Туре	Size	^
Desktop	퉬 Licenses	7/25/2018 5:04 PM	File folder		
🚺 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	
📔 Desktop 🗏	OiscUtils.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	
🐌 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:) SC	🚳 Glasswall.SecuritySolution.Domain.dll	7/6/2018 4:05 PM	Application extens	684 KB	
51 items 1 item selected	Glasswall.SecuritvSolution.FileAnalvsisCo 1 1.60 KB	7/6/2018 4:05 PM	Application	46 KB	

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

↓ 1 2 = 1	bin			_	D X
E Home Share	e View				~ e
🔄 💿 🔻 🚺 « P	rogram Files 🕨 Glasswall 🕨 AdministratorConsole	e ▶ bin	✓ C Search b	in	Q
☆ 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	
Pesktop ≡	🚳 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	=
DVD Drive (D:) SC	S WebActivatorEx.dll	10/5/2016 1:11 PM	Application extens	12 KB	
v	NebGrease.dll	1/23/2014 12:57 PM	Application extens	1,245 KB	\sim
61 items 1 item selected	1.60 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.

Processes Performance	Users	Details	Services			
Vame	F	ND	Description	Status	Group 📤	
🔍 InboundSmtpAnalysisA	gent		Glasswall Inbound SMTP Analysi	Starting		
🥋 wmiApSrv			WMI Performance Adapter	Stopped		
🔍 VSS			Volume Shadow Copy	Stopped		
🔍 vmvss			VMware Snapshot Provider	Stopped		
C VMTools	1	416	VMware Tools	Running		
🔍 VGAuthService	1	388	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	1	272	SQL Server VSS Writer	Running		
SQLSERVERAGENT			SQL Server Agent (MSSQLSERVER)	Stopped		
🔍 SQLBrowser			SQL Server Browser	Stopped		
🔍 sppsvc			Software Protection	Stopped		
🔍 Spooler	1	044	Print Spooler	Running		
SNMPTRAP			SNMP Trap	Stopped		
🔍 SamSs	5	528	Security Accounts Manager	Running		
🔍 RSoPProv			Resultant Set of Policy Provider	Stopped		
🔍 RpcLocator			Remote Procedure Call (RPC) Lo	Stopped		
🔆 PerfHost			Performance Counter DLL Host	Stopped		
🔍 NetTcpPortSharing			Net.Tcp Port Sharing Service	Stopped		
Netlogon	5	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.

LASSWALL	Supported File Types			Other File Types	
Administrator Console	Files 0	Sanitised / Remediated 0		Files 0	
Transaction Log	Outbound Emails				
File Release Requests 💿	Total Emails O	Total Files 0			
Inbound SMTP Policy	Supported File Types			Other File Types	
Outbound SMTP Policy	Files 0	Sanitised / Remediated 0		Files 0	
Configuration	Inbound SMTP Age	nt Status			
Accounts	Active 1	Inactive 0	Inbound Queues 0	Scan Queues 0	Inspection Queues 0
	Outbound Queues 0	Reporting Queues	Failed Queues 0	Unprocessable Queues 0	
Logout	Outbound SMTP Ag	jent Status			
	Active 0	Inactive 0	Inbound Queues 0	Scan Queues 0 Activa	Inspection Queues
	Outbound Queues	Reporting Queues	Failed Queues	Unprocessable Queues	ntem in Control Panel to activate Wi

7. On the left sidebar, click Accounts.

GLASSWALL	redrafterConsele/Acces	ori D * B X O glasswall dripdi	×				
THOST EVENY FILE	Accoun	its					
Administrator Console		Name	En	nail		Security Group	Account Locked
Transaction Log	0	Administrator	admin@glassw	allsolutions.com	Pri	ncipal Administrator	
File Release Requests 💿			() Add	J Edit	Unlock 👔	Delete	
Inbound SMTP Policy	Security	y Groups					
Outbound SMTP Policy		Name				Security Roles	
Reporting					View I Edit I Request Pub	Inbound Policy Catalogue nbound Policy Catalogue lish of Inbound Policy Catalog	we
Configuration					Approve Pub View C	lish of Inbound Policy Catalog Subound Policy Catalogue	ue
Accounts					Edit O Request Publi	utbound Policy Catalogue ish of Outbound Policy Catalo	aue.
Your Account	0	Principal Admin	istrator		Approve Publi Ar	ish of Outbound Policy Catalo ccount Administration Export Retained File Delete Retained File	gue
Logout					Appro F Vie Edi	ver ne resease Réquest Request File Release w System Configuration t System Configuration Create Reports	
	0	Standard U	ser			Activate Windows	
			0	2		Go to System in Control	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 🛛 🕅	(=)
GLASSWALL	Create Account	
Administrator Console	Name	
Transaction Log	Administrator	
File Release Requests (***)	Email	
Internet SMTP Police	Administrator@di.pdr	
and carrier takey	Security Group	
Outbound SMTP Policy	Principal Administrator	
Reporting	\otimes	
Configuration	Le.	
Accounts		
Your Account		
Logout		
		Activate Windows
		Go to System in Control Panel to activate Windows

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

GLASSWALL	-	Come	nts X				
TRUST EVERY FILE			User Admi	nistrator@dupdr.o	reated success	stully.	
Administrator Console	Accounts						
Transaction Log	2. <u></u>	Name	Ema			Security Group	Account Locked
File Release Requests 💿	0	Administrator	admin@glasswall	solutions.com		Principal Administrator	
Inbound SMTP Policy	○ ▲	Administrator	Administrato	r@di.ipdr		Principal Administrator	
Outbound SMTP Policy	R		Add	Edit	Unlock	Doleto	
Reporting	Security	Groups					
Configuration		Name				Security Roles	
Accounts					V	iew Inbound Policy Catalogue dit Inbound Policy Catalogue	
					Request	Publish of Inbound Policy Catalogue	
Your Account					Approve	Publish of Inbound Policy Catalogue	
					E	dit Outbound Policy Catalogue	
					Request	Publish of Outbound Policy Catalogue	
) Logout	0	Principal Admini	strator		Approve I	Publish of Outbound Policy Catalogue Account Administration	
						Export Retained File	
						Delete Retained File	
					A	pprove File Release Request	
						Request File Release	
						View System Configuration 10005	
						Edit System Configuration	

12. The new administrator account should be created.

= Mail						-	ſ
earch Mail and Peop	e P	😧 New 👻 🧯 Delete Archi	ive Junk Sweep	Move to Y Categor	ries 🗸 🚥		2
Favorites.		Inbox	All 🗸	Your acco	ount has been created		
Inbox	168	Today	~	_			
Sent Items Drafts		Administrator@DI.IPDR	8.23 PM	AD Admin	histrator@DI.IPDR istrator; ¥	39 Rept Wed 7/25/20	y all 118 8
Administrator		Account Graned Your account has been o	Printed, Pie				
Inbox	368	Mik Un hev hev lookie	3:37 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 asdfasdfadifasdf	Tue 11:23 PM Fro		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 concers in mailable	Tue 11:22 PM				
		Mik Un	1			Activate Windows	

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

GNO			_ 0
🔆 🕑 🗿 https://glasswall.dk/pde/Admir	vistratorConsole/Account D + 🗟 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.

TRUST EVERY FILE	Accour	nts					
Administrator Console		Name	En	ail		Security Group	Account Locked
Transaction Log	•	Administrator	admin@glasswi	allsolutions.com		Principal Administrator	
File Release Requests 💿	0	Administrator	Administra	or@di.ipdr		Principal Administrator	
Inbound SMTP Policy	Securit	V Groups	🕀 Add	🖍 Edit	Unlock		
Outbound SMTP Policy		y Groups Name				Security Poles	
Reporting	-					View Inbound Policy Catalogue	
Configuration					Reque	Edit Inbound Policy Catalogue st Publish of Inbound Policy Catalog e Publish of Inbound Policy Catalog	ue
Accounts						Edit Outbound Policy Catalogue	
Your Account	0	Principal Admir	nistrator		Reques	t Publish of Outbound Policy Catalog Publish of Outbound Policy Catalog Account Administration Export Retained File	jue jue
Logout						Delete Retained File Approve File Release Request Request File Release View System Configuration Edit System Configuration	
						Create Reports	

17. Click Delete.

GLASSWALL	Administrator 0	Console / Accounts			
			User admin@glasswallsolu	tions com deleted successfully	
Administrator Console	Account	ts			
Transaction Log		Name	Email	Security Group	Account Locked
File Release Requests 💿	0	Administrator	Administrator@di.ipdr	Principal Administrator	
Inbound SMTP Policy			🕀 Add 🛛 🥒 Edit	Unlock 💼 Delete	
Outbound SMTP Policy	Security	Groups			
Reporting		Name		Security Roles	
Continuation				View Inbound Policy Catalogu Edit Inbound Policy Catalogue Request Publish of Inbound Policy Ca	e stalogue
Accounts				Approve Publish of Inbound Policy Ca View Outbound Policy Catalogs	atalogue
Your Account	0	Principal Admini	strator	Edit Outbound Policy Catalogu Request Publish of Outbound Policy C Approve Publish of Outbound Policy C	c atalogue atalogue
) Logout				Export Retained File Delete Retained File	
				Approve hier revealable Request Request File Release View System Configuration Edit System Configuration Create Reports	ows
	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://glasswail.dkipdr/AdministratorConsole/Centrgu 🔎 + 🗎 C 🔤 Mail - Administrator - Outlook 🛛 🗐 Glasswall Centiguration	*
	Subject Line The subject of the email used to release a file. Your the has been released by Classwalt. Email Body The content of the email used to release a file.
Inbound SMTP Policy Outbound SMTP Policy Mail Footer Text The text inserted at the bottom of processed emails.	The attached file(s) have been checked and released in accordance with organisation policy. %ReleaseDetails% Please contact IT support for more information.
Configuration This mail has been protected by Glasswall.	Subject Line The subject of the email used to notify user of a file release denial. $b_{g}^{\rm c}$ Your the release request has been denied.
Logoul	Email Body The content of the email used to deny a tile release. The following fle(c) have been denied for release in accordance with organisation policy. WiteteaseDetails%
vit 802.8	Please contact IT support for more information Archivate Windows

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).

The second secon	Configuration X Mail - Administrator - Outlook Casswall Configuration X		UU.
GLASSWALL Proc	essing Mode		
TRUST EVERY FILE Config	ure Glasswall Inbound SMTP Agent Processing Mode		
Administrator Console Analy	is and Protect		
Transaction Log File I	Release Service Hostname		
File Release Requests	ostname to be used for File Release service		
https://	/ dasswall di lodr /GlasswallFileReleaseRequestService		
Inbound SMTP Policy			
File I	Preview Mode		
Outbound SMTP Policy			
Disab	ed - File Preview is not generated		
Reporting Passi	Generate and attach to emails enails		
Configuration			
Accounts File I	Preview Timeout		
A CONTRACTOR OF	Ch Devise secondar for the seconds		
Tour Account Maxim	ium Hie Preview processing time in seconds	2	
300		*	
Logout Allow	ved Domains		
Dama	ins that the Inhound SMTP Agent is allowed to relay mail to (separate with semicolog)		
Doma	the even are encoured owner. Afters to encource to ready finds to (separate with sectionally		
d.ipdr			
		A LOCAL AND A REPORT OF A REPORT OF	
		Go to System in Control Rabel to activate We	-
+5.00.2.5			Save
Do you want Aut	oComplete to remember web form entries? Learn about AutoComplete	Yes No ×	

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
🕖 💮 https://glassus?.dLipdr/Admia	natustorConsols/Inbound 🖓 + 🔒 C 🔤 Mail - Administrator	- Outlook 👩 Gasswall Policy Catalogue 🛛 🛛	
GLASSWALL"	Administrator Console / Inbound SMTP Policy	1	
TRUST EVERY PILE	Inbound SMTP Policy Cat	alogues	
Administrator Console		Published	Published By
Transaction Lon	Current Policy Catalogue	7/25/2018 1:33:50 AM	Admin
manageaunitary	нç	Updated	Updated By
File Release Requests 0	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?	ann shout AutoComplete	Ves No

3. Under Receiver Groups, click Add.

-		- 0
🕘 🧭 https://glasseall.dLipde/Admin	astrator Console/Inbound D + 🔒 C 🔯 Mail - Administrator - Outlook 🧔 Glasswall Draft Inbound S., 🛪	n -
GLASSWALL TRUST EVERY FILE	Al Senders V Al Receivers V Organisation Content Main	agement Policy
Administrator Console	ThreatCensor Policy Set Organisation ThreatCensor Policy Bet	
File Release Requests		
Inbound SMTP Policy	Sender Groups There are no Sender Groups in this Policy Catalogue.	⊕ Add
Reporting	Receiver Groups	⊕ Add
Configuration	There are no Receiver Groups in this Policy Catalogue.	0
Your Account	Content Management Policies	⊕ Add
	Name	
b Logout	Organisation Content Management Policy	Details
	ThreatCensor Policy Sets	⊕ Add
	Name	Activate Windows
	Organisation ThreatCensor Policy Set	Details

4. Under User Defined Mailboxes, click Edit.

🕘 💿 🖉 https://glasswalk.dk.ipde/Adv	ninistrator Conscie/Inbound D = 🔒 C 🔤 Mail - Administrator - Outlook 🧔 Glasswall Receiver	Sroups X	- 0
GLASSWALL	Administrator Console / Inbound SMTP Policy / Policy Catalogue / Receiv	er Group Details	
	New Receiver Group 2		
Administrator Console			🖍 Edit
Transaction Log	LDAP Synchronisation Settings		
File Release Requests 💿			🖌 Edit
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))		
	Mailbox Attribute Name		
	mai	R	
) Logout			Ø
	User Defined Mailboxes		
	There are currently no user-defined mailboxes for this receiver group		Activate Windows
v6.00.2.5			Professional and an other statements

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

			- 0 ×
🗲 🛞 🗿 https://glassnail.dlipde/Admini	thato-Console/Inbound D = 🔒 C 🚘 Mail - Administrator - Outlook 🛛 🧔 Glasswal	I Receiver Group	n * 0
GLASSWALL	- an an and a set of the set of t	 memory coup county - construction ontogy management 	
	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	De .	
Outbound SMTP Policy	There are currently no user-defined mailboxes for this receiver group		
Reporting			
Configuration			
Accounts			
Your Account			
		Activate Windows Go to Swarm in Control Pane	
+6.00.2.5			

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

				- 0
🔵 😰 https://glasseall.dk.ipde/Admi	nistratorConsole/Inbound D + 🖶 X 🔤 Mail - Administrator - Outlook 🔿 Waiting for glasswalldsipdr - X			0
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	Descine Course			(A) Ad
Outbound SMTP Policy	Name			.
Reporting	New Receiver Group-4		Details	+ Undo
Configuration	allowed to receive encryption		Details	Delete
Accounts				
Your Account	Content Management Policies	R		⊕ Ad
	Name			
յ Logout	Organisation Content Management Policy		Details.	
	ThreatCensor Policy Sets			(+) Ad
	Name		Pariel to activa	te Windows.
	Organisation ThreatCensor Policy Set		Details	

2.7.3.5 Create a ThreatCensor Policy Set

1. Under ThreatCensor Policy Sets, click Add.

🕥 🥑 https://glasswall.dkipde/Admi	nistratorConsole/Inbound P + 🔒 C 🔤	Mail - Administrator - Ou	×	- 0
GLASSWALL			was a wing wasana	
TRUST EVERY FILE	New ThreatCenso	or Policy Se		1
Administrator Console	Explicit ThreatConco	r Policion		
Transaction Log	There are no Explicit ThreatCer	nsor Policies in the F		,
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		
			Activate Win	
			Go to System in	Control Panel to activate Windows.

2. Under Explicit ThreatCensor Policies, click Edit.

🗲 🕤 💋 https://glasswall.di.jpdr/Adminis	stratorConsole/Inbound 🔎 👻 🚔 🖒 🔛 Ma	il - Administrator - Outlook 🧧 Glass	wall Edit Explicit Thre ×		_ 0 × 0 ∩ ★ 0
GLASSWALL TRUST EVERY FILE	Administrator Console / Inbound	d SMTP Policy / Policy Catalogu tCensor Policies	e / ThreatCensor Set Policy Details / Edi	Explicit ThreatCensor Policies	
Administrator Console	Add Explicit ThreatCe	nsor Policy			
File 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 ThreatCens	Policies or Policies in the Policy Catalogu	e		
Your Account					
() 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 💮 🧭 https://glasswall.di.ipde/Admini P [dit View Fgvorites Jools Help	stratorConsole/Inbound D + 🔒 C 🖾 Mail - Au	Sministrator - Outlook 🦉 Glasswo	ill Draft Inbound S	×		ń *
GLASSWALL	Sender Group	Receiver Group		Mail Delivery	Action	
TROST EVENT FILE	All Senders	All Receivers	~	Blacklist		Add
Administrator Console						
Transaction Log						
File Release Requests 💿	Processing Rules Sender Group	Receiver Group	Content Mana	gement Policy	ThreatCensor Policy Set	
Inbound SMTP Policy	All Senders	All Receivers	Organisatio	on Content ent Policy	Organisation ThreatCenso Policy Set	r
Outbound SMTP Policy			manageri	cial only	1, out ; out	
Reporting	Sender Group	Receiver Group		Content Mans	gement Policy	
Configuration	All Senders	allowed to receive encrypt	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 Co	Iows ontrol Panel to activate Wi 🕀 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
ALL	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 V
☑ <u>accept</u> 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	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.jpdr/GlasswallIntegrationServ
Integration Service Username	Administrator
Integration Service Password	
Ignore Integration Service Certificate	False ¥
Use Proxy?	False
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
ick Next.	
g 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.		
	Ъ _р		
	Back Install Cancel		
l			

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.
	 Yes, I want to transfer the settings No, I do not want to transfer the settings
	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
	 Run console in default mode Run console in FIPS mode
	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.							
	 Use direct connection. Use proxy server. 							
	k k							
	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.
	 Password Based Authentication Password Based and SSL Client Based Authentication Password Based or SSL Client Based Authentication SSL Client Only Authentication
	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	of its affiliates.
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></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		<u>A</u>	_		×
À ArcSight	What would you like to do?	-0			
Configure					
R					
		Add a Connector			
		Set Global Parameters			
		< 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	 ✓ Security log ✓ System log 	
K.	Application log ForwardedEvents log	
5	Source hosts for all forwarded events	
	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						
K.	Manager Hostname	arcsight-esm				
	Manager Port	8443				
$ \lambda \lambda $	User	administrator				
	Password	•••••				
	AUP Master Destination	false			\sim	
	Filter Out All Events	false			~	
	Enable Demo CA	false			~	
MICRO						
L-FOCUS				\searrow		
			< Previous	Next >	Can	icel

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

Connector Setup				_		×
À ArcSight	Enter the connec	ctor details				
Configure						
K.						
	Name Location	Windows 10-1				
	DeviceLocation Comment	Windows10-1 Client				
		Ş				
			< Previous	Next >	Cance	ł

- 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
 Introduction Choose Install Folder Choose Install Set Pick Shortcut Folder Pre-Install Summary Installing Upgrade System Restart Install Complete 	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 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.			
	 Add a Connector Set Global Parameters 		
	< <u>P</u> revious <u>N</u> ext > <u>C</u> ancel		

- 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	realtime	-
	Action Upon Reaching EOF	None	-
	The Extension in Rename Action	processeu	
OFOCUS	(
	< <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.

ArcSight	Enter the destination parameters		
Configure			
	Manager Hostname	arcsight-esm	
	Manager Port	8443	
	User administrator Password ······		
	AUP Master Destination	false	-
	Filter Out All Events	false	-
	Enable Demo CA	false	-
		< Previous Next >	<u>C</u> ancel

- 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.

😣 🗖 🗊 Connector	Setup
À ArcSight	Add connector Summary Following are the added connector details: Connector Name [Ubuntu Client], Connector Type [syslog_file]
Configure	
	< Previous Next > Cancel

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>Next</u> > <u>C</u> ancel
Click Next	

- 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
 Introduction Choose Install Folder Choose Install Set Pick Shortcut Folder Pre-Install Summary Installing Upgrade System Restart Install Complete 	Where would you like to create product icons? In a new Program Group: ArcSight SmartConnectors In the Start Menu On the Desktop In the Quick Launch Bar Other: Don't create icons
	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	x
文 ArcSight	Select the connector to configure	
Configure		
	Type Microsoft Windows Event Log - Native	
	ß	
	< Previous Next > Ca	incel

- 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	
	\Box Do not use any source for Windows OS version	-
$P \rightarrow 0 / - c$	\Box Use Active Directory for OS version	
	Use file for OS version	
	Parameters to add hosts for event collection	
	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.

*	Connector Se	tup 📃 🗖 🗙
Configure	Enter the parameter details	
	Domain Name	DI
2	Domain User Name	arcsight_admin
	Domain User Password	•••••
	Active Directory Domain	DI.IPDR
	Active Directory User Name	arcsight_admin
	Active Directory User Password	•••••
	Active Directory Server	ad-dns.di.ipdr
	Active Directory Filter	(&(cn=*)(operatingsystem=*)(whencreated=*))
	Active Directory Protocol	non_ssl 🗸
	Use Active Directory host results for	Replace Hosts V
	G	
		< 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	b							-		x
ArcSight	Enter t	he device details														
Xucaigin	~	Host Name	Do	Use	Pas	Win	Is	Sec	Sys	Appl	For	Cus	Filter	Locale	Enc	
Configuro	~	EXCHANGE.DI.IPDR			•••••	Wind		✓	~	✓			*	en_US	UIF-8	
conligure	✓	REMOTEDESKTOP3.DI			****	Wind		✓	~	✓			*	en_US	UTF-8	
	~	WINDOWS10-1.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	1
	~	WINDOWS10-2.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	1
	~	HYPERV.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	Н
L.	~	MSSQL.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	1
	~	WINDOWS10-3.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	1
	~	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
	v	AD-DNS08.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	1
	v	BACKUP-STORAGE.DI.I			****	Wind			~				*	en_US	UTF-8	
	✓	BACKUPSERV.DI.IPDR			****	Wind		•	~	~			*	en_US	UTF-8	11
	~	GLASSWALL.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	1
	✓	SEMPERIS-DSP.DI.IPDR			****	Wind		~	~	~			*	en_US	UTF-8	-
		1			Ad	bb	Import	Ex	port	1		1				
						R				< Pre	evious	N	ext >		Cancel	

*	Connector Setup	_		x
À ArcSight	Will use Active Directory at: ad-dns.di.ipdr			
Configure	whenesser withows 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	_ D X	
À ArcSight	Enter the type of destination			
Configure				
		ArcSicht Mannacz (angewated)		
12		 ArcSight Logger SmartMessage (encrypted) 		
		ArcSight Logger SmartMessage Pool (encrypted)		
1. A. A.		○ CEF File		
19		○ Event Broker		
		CEF Syslog		
		CEF Encrypted Syslog (UDP)		
		O CSV File		
		() Raw Syslog		
O FOCUS				
	A			_
		< Previous Next >	Cancel	1

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

*		Connector Setup	_ D X
À ArcSight	Enter the destination para	meters	
Configure			
14	Manager Hostname	arcsight-esm	
1 S S S	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 I
ArcSight	Enter the connect	tor details				
	Name Location DeviceLocation Comment	Windows Connector Server				
			14			
				< Previous Next >	Car	ncel

- 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	_ □	>
À ArcSight	Would you like to continue or exit?		
Configure			
	○ Continue		
	• Exit		
	ha an		
OFICES			
	- Drasky pr	Cano	el
	< PTEVIOUS INEXL >		-



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 Network	Host	Application	Data Entity	System Health	Threat Intelligence	Malware
Start with the activate base! Download			S	ecurity Products 8	& Connectors			
Track Execution							Devices	• (3
② Business Challenges	•	② Associated Packages	•	⑦ Status •	② Attack Vector So	lutions	E	apand All 🔍
Valware Monitoring		L1 - Malware Monitoring - Indicators and	d Warnings					

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				-
	 Continuously evaluate time parameters (like \$Now) Evaluate time parameters once at attach time 				
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				
	-			
Navigator 🗗	? X	Inspect/Edit		ð
Resources Packages Use Cases		🐉 Destination Editor		
✓ Rules Ctrl+Alt+L	-	Attributes Notes		
		Destination		
Shortcuts		Name	Administrator	
		# Start Time	12:00:00 AM	
7 To Dulas		🗰 End Time	11:59:59 PM	
- Kules		Destination Type	Email Address	
Shared		# Email Address	administrator@di.ipdr	
All Rules		User/Group	/All Users/Administrators/administrator	
ArcSight Activate				
+ 🧰 ArcSight Administration		= Common		
ArcSight Foundation		External ID		
🛓 🧰 ArcSight Solutions		Alids (Display Name)		
🗄 🥅 ArcSight System		Version ID		
🗉 🧮 Downloads		Deprecated		
🗈 📴 Personal		- Assign		
🕀 🦲 Public		Owner		
🛨 🧰 Real-time Rules		Notification Groups		
		(Name) (Sesorption)		
				Apply <u>H</u> e

- 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.

e Edit View Window Tools System Help	-		
- 🙋 🖩 📲 🖄 📲 🖷 🗶 🔍 📑 Het 4 👖 🚺		• _ [♥] = 2 = - [♥] 2 2 2 2 2 2 2 0 0 1 [♥] 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
avigator	d' ? ¥	Inspect/Edit	ď
esources Packages Use Cases		😴 Destination:Administrator 🚺 Rule Editor	
5 Rules	Ctrl+Alt+L 🔻	Attributes Conditions Aggregation Actions Local Variables Notes	
		Rule Mourse shot	
hortcuts		Name Maiware aiert	
C Rules		External ID	
Shared		Alias (Display Name)	
- 7 All Rules		Description	
🗊 🧰 ArcSight Activate		Deprecated	
ArcSight Administration		Assign	
🖃 🧰 ArcSight Foundation		Owner	
Arcsight Solutions		Notification Groups	
T Downloads			
🗈 🦳 Personal			
🕀 🧰 Public			
🕀 🛄 Real-time Rules			
		External ID	
		V Test OK Cancel	Apoly Hel

3. Click the **Conditions** tab.

lavigator	с ^л ? х	Inspect/Edit			
tesources Packages Use Cases		🗱 Destination:Administrator	🗲 Rule Editor		
✓ Rules	Ctrl+Alt+L 🔻	Attributes Conditions Aggree	ation Actions Local Variab	les Notes	
		🚯 🐍 🚺 💻 🗣 Filters 👺 As	sets 😻 Vulnerabilities 📑 Act	ive Lists ≿ Joins	
hortcuts		Edit Summary			
		🔅 Event conditions			
C Rules		i event1			
= 7 Shared					
🖻 🗁 All Rules					
🗄 🧮 ArcSight Activate			R R R R R R R R R R R R R R R R R R R		
ArcSight Administration					
H Clight Foundation					
🕂 🧮 ArcSight System					
🗈 🧰 Downloads					
e Personal					
Real-time Rules		Common Conditions Editor	~		📠 +/- Global Variable.
H Linassigned		Name		Condition	A0 (
		Event			
		Event Aggregated Event Count			
		Event Aggregated Event Count Application Protocol Bytes In			✓ ✓ ✓
		Event Aggregated Event Count Application Protocol Bytes In Bytes Out			2 2 2 2 2 2 2 2 2
		Event Aggregated Event Count Application Protocol Bytes In Bytes Out Correlated Event Count			2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
		Event Aggregated Event Count Application Protocol Bytes In Bytes Out Correlated Event Count Customer			
		Event Aggregated Event Count Application Protocol Bytes In Bytes Out Correlated Event Count Customer Domain Evternal ID			
		Event Aggregated Event Count Application Protocol Bytes In Bytes Out Correlated Event Count Customer Domain Domain External ID Domain ID			
		Event Aggregated Event Count Application Protocol Bytes In Bytes Out Correlated Event Count Correlated Event Count Coustance Domain Domain External ID Domain ID Q. Search for:			
		Event Agregated Event Count Application Protocol Bytes In Bytes Out Correlated Event Count Custome Domain Domain Eternal ID Domain ID C., Search for:			

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	Attributes Conditions Aggregation Actions Local Variables Notes	
hostrute	📕 Adi 💉 Edit 🗱 Remove 🔺 Move Up 🔻 Move Down 🖹 Hide Empty Triggers	
Rules ■ Stand ■ All Rules ■ All Scipht Admestration ■ ArcSight Admestration ■ ArcSight Admestration ■ ArcSight Solutions ■ Personal ■ Poundat ■ Real-time Rules ■ Linassigned	Image: Second	

- 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	on 💌
When: On First Eve	nt	
Send Notification —		
Destination Group:	ArcSight Administrators 🔹	🗾 Ack Required
Message:		
L		
		<u>Cancel 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 uti entertainment, Java makes your Internet experience come to life.	ities and	
Note: No personal information is gathered as part of our install process. <u>Click here</u> for more in what we do collect.	formation on	
Click Install to accept the license agreement and install Java now.		
Change destination folder	Install >	

- 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 Sele	ction	_ 🗆 X				
Pleas	e select the Java(ti	m) Runtime to (Jse				
Oracle/Sun 1.8.0 64	Oracle/Sun 1.8.0 64-bit C:/Program Files/Java/jre1.8.0_181/bin/java.∉ ♥						
	ОК	Cancel					

8. Click **OK.**

	Tripwire Enterprise Console Installer	– – X
tripwire Enterprise 8.7	Welcome to the Tripwire Enterprise Console installat This wizard will install and configure Tripwire Enterp Before continuing, please review the installation doc ensure that you are in compliance with all installation Failure to meet all requirements may cause the instal	tion wizard. rise Console. cumentation to n requirements. llation to fail.
	< Back Next >	Cancel
Click Next. Select I accept the a	agreement.	
Click Next. Select I accept the a	agreement. Tripwire Enterprise Console Installer	_ 0 X
Click Next. Select I accept the a te License Agreement	agreement. Tripwire Enterprise Console Installer	
Click Next. Select I accept the a te License Agreement Please read the follow before continuing with	agreement. Tripwire Enterprise Console Installer figure wing License Agreement. You must accept the terms of th the installation.	WIRE TAKE CONTROL.
Click Next. Select I accept the a License Agreement Please read the follow before continuing with IMPORTANT INFORMAT TRIPWIRE SOFTWARM SUBJECT TO LICENS AGREEMENT BEFORE COMPLETE AND UNCO SET FORTH IN THIS ORDER TERMS AND O	agreement. Tripwire Enterprise Console Installer	TWARE IS ENSE ICATES DUDITIONS PURCHASE
Click Next. Select I accept the a License Agreement Please read the follow before continuing with IMPORTANT INFORMAT SUBJECT TO LICENS AGREEMENT BEFORE COMPLETE AND UNCO SET FORTH IN THIS ORDER TERMS AND CON	agreement. Tripwire Enterprise Console Installer wing License Agreement. You must accept the terms of th the installation. ATION E IS LICENSED, NOT SOLD. USE OF THIS SOFT SE RESTRICTIONS. CAREFULLY READ THIS LICE USING THE SOFTWARE. USE OF SOFTWARE INDI ONDITIONAL ACCEPTANCE OF THE TERMS AND CO S AGREEMENT. ANY ADDITIONAL OR DIFFERENT CONDITIONS SHALL NOT APPLY. I accept the agreement O I do not accept the agreement	TWARE IS ENSE ICATES DNDITIONS PURCHASE

Tripwire Enterprise C	onsole Installer
Installation Directory	tripwire
Please specify the directory where all Tripwire Ente	erprise components will be installed.
Installation Directory C:\Program Files\Tripwire	TE 🔊
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 Cons	ole Installer	_ 🗆 X
Tripwire Enterprise	Console Configuration Part 1 of	ia tri	pwire Inke
Please provide the ho installed.	ostname of the system where Trip	owire Enterprise Co	nsole will be
TE Server Hostname	TRIPWIRE-E		
InstallBuilder			
		Back Next	> 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 Enterp	orise Console Inst	aller		x
Tripwire Enterpris	e Console Configuratio	on Part 3 of 4	tripv	vire TAKE	0L.
The services passph	nrase is used to secure 1	Tripwire Enterprise co	mmunication	s.	
This password mus double-quote ("), le characters are allow	t be between 19 and 64 ess-than (<), greater-th red. See the Installation	characters, and cann an (>), or backslash (n and Maintenance G	ot contain sir \) characters, uide for more	ngle-quote ('), most other details.	,
Services Passphrase	•••••				
Confirm Passphrase	••••••				
InstallBuilder ——		< Back	Next >	Cancel	
ilick Next .					
te	Tripwire Ente	erprise Console	Installer	_ !	
te Tripwire Enterpr	Tripwire Ent	erprise Console ration Part 4 of 4	Installer	ripwire	TAKE
Tripwire Enterpr Please review the	Tripwire Enter ise Console Configur	erprise Console ation Part 4 of 4 or Tripwire Enterpris	Installer	ripwire	TAKE
Tripwire Enterpr Please review the The following sett	Tripwire Enter ise Console Configur installation settings for tings are configured f	erprise Console ation Part 4 of 4 or Tripwire Enterpris or Tripwire Enterpris	Installer ti e Console. se Console:	ripwire	TAKE
Tripwire Enterpr Please review the The following sett Installation Direct Available Disk Spa Hostname: TRIPW	Tripwire Entr ise Console Configur installation settings for tings are configured f ory: C:\Program Files' icce: 184716 MB //RE-E	erprise Console ration Part 4 of 4 or Tripwire Enterpris or Tripwire Enterpris	e Console.	r <mark>ipwire</mark>	TAKE
Tripwire Enterpr Please review the The following sett Installation Direct Available Disk Spa Hostname: TRIPW IP Address(Listeni HTTPS Web Servio	Tripwire Entr ise Console Configur installation settings for tings are configured f ory: C:\Program Files' icce: 184716 MB //RE-E ng): 0.0.0.0 ces Port: 443	erprise Console ration Part 4 of 4 or Tripwire Enterpris or Tripwire Enterpris	e Console.	ripwire	
Tripwire Enterpr Please review the The following sett Installation Direct Available Disk Spa Hostname: TRIPW IP Address(Listeni HTTPS Web Servio HTTP EMS Integra TE Services (RMI)	Tripwire Enter ise Console Configur installation settings for tings are configured f ory: C:\Program Files' toe: 184716 MB /IRE-E ng): 0.0.0.0 ces Port: 443 ation Port: 8080 Port: 9898	erprise Console ration Part 4 of 4 or Tripwire Enterpris or Tripwire Enterpris	e Console.	r <mark>ipwire</mark>	TAKE
Tripwire Enterpr Please review the The following sett Installation Direct Available Disk Spa Hostname: TRIPW IP Address(Listeni HTTPS Web Servie HTTP EMS Integra TE Services (RMI) TEConsoleInstalle	Tripwire Enter ise Console Configur installation settings for tings are configured f ory: C:\Program Files' oce: 184716 MB /IRE-E ng): 0.0.0.0 ces Port: 443 ation Port: 8080 Port: 9898 r: Java Version detect	erprise Console ration Part 4 of 4 or Tripwire Enterpris or Tripwire Enterpris \Tripwire\TE ed: 1.8.0_181 64	Installer to e Console. :e Console:	r <mark>ipwire</mark>	TAKE
Tripwire Enterpr Please review the The following sett Installation Direct Available Disk Spa Hostname: TRIPW IP Address(Listeni HTTPS Web Servic HTTP EMS Integra TE Services (RMI) TEConsoleInstalle	Tripwire Enter ise Console Configur installation settings for tings are configured f ory: C:\Program Files' tee: 184716 MB /IRE-E ng): 0.0.0.0 ces Port: 443 ation Port: 8080 Port: 9898 r: Java Version detect	erprise Console ration Part 4 of 4 or Tripwire Enterpris or Tripwire Enterpris \Tripwire\TE ed: 1.8.0_181 64	Installer tr e Console. se Console:	ripwire	

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

te	Tripwire Enterprise Con	sole Installer	_ 🗆 X
Tripwire Enterpr	ise Agent Configuration	tri	pwire Inke
Tripwire Enterprise enable monitoring for this local Agen	e Agent software is installed on the g of that system. Do you want to in: it? The Real-time Monitoring featur	Tripwire Enterprise stall Real-time Moni re can also be install	Console system to itoring functionality ed later.
🖌 🖌 Install Real-f	time Monitoring		
Please specify th	e local port to be used by the Real-	time subsystem.	
Real-time Port	1169		
InstallBuilder			
		< Back Next	> Cancel

te	Tripwire Enterprise Console Installer	_ D X
Ready to Install	t	ripwire: TAKE CONTROL.
The installer is ready t	to begin installing Tripwire Enterprise Console.	
Click Next to begin in Click Back to make ar	istalling 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.

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

27. Click Login.

Database Configuration Sett	ngs
These settings control how the TE Cor any necessary changes in the fields be	sole connects to a remote database that stores data for all TE operations. You can check the current configuration here, and make low.
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 domainuser), 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.	indows account (typically of r). With the Windows ersion of NTLM. However, as e used with NTLM to ensure
	Lock 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 authenticate with the database.	
	Database Host:		
	192.168.78.125	Database Host: The fully qualified domain name, hostname or IP address of the system w	here the database is installed.
	Port (dofault 1433)-		
	1433	Port: The TCP port that the database is listening on. If an Instance Name is specified here,	then the database connection
		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	disabled. The SQL Server at the TCP port number that
		corresponds to that named instance.	
	B. Materia M ²⁰¹⁹²		
	Database Name:	Database Name: The name of the database that TE should use when connecting to the re	mote database. Note that the
	12_00	login name in SQL Server should have this database set as the default, and the login name	should be mapped to this
		uatabase.	
	Instance Name (Optional):		
		Instance Name (Optional): The location/name of the database instance on the server. As	your DBA if a non-default
	SSL:		
	Off •	SSL (Secure Sockets Layer): Specifies whether the database connection should request,	require or authenticate SSL.
		Request - SSL will be used if available. Scl will be used if available.	No. databasa
		 Require - SSL will always be used, and an error will occur if SSL is not available for Authenticate - SSL will always be used, and an error will occur if SSL is not available 	e for the database. In addition,
		the certificate chain of the database server's public key will be authenticated using T chain does not originate from a trusted source, an error will occur	E's trust store. If the certificate
		 Off - SSL will never be used. This setting is not recommended. 	Activate Windows
	Test Database Login		
25	Click Test Database Logi	in to ensure the connection is functional	
55.	CIICK TEST Database LUg		

Test Database Login	
Fest Results: Connection Succeeded.	
	Activate Windows
	Go to System in Control
pwire Enterprise 8.7.0.b8.7.0.r20180606173604-e215728.b40	Save Configuration and Restart Console Logo

- 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.
C	Passwords must: Be between 8 and 128 characters in length Contain at least 1 numeric character Contain at least 1 numeric character Contain at least 1 non-alphanumeric character Supported characters: "-1@#\$%-&"()=+{[]]\\ ;."<>./?
S	pport Information Still having problems with your installation? Contact Tripwire Support. Itips://secure.tripwire.com/customers/contact-support.cfm Or open a Support ticket: https://secure.tripwire.com/customers/
Trip	re Enterprise 8.7.0.b8.7.0.120180606173604-e215728.b40
Clic	Confirm and Continue.
Inp	vire Enterprise Fast Track
	Welcome to Tripwire Enterprise Fast Track!
	TRIPWIRE* ENTERPRISE Fast Track
	TRIPWIRE ENTERPRISE FAST Track
	<text></text>
	<text><image/><text><text></text></text></text>
	<text><image/><text><text><text><text></text></text></text></text></text>
	<text><image/><text><text><text><list-item><list-item><list-item><text></text></list-item></list-item></list-item></text></text></text></text>
	<text><image/><text><text><list-item><list-item><list-item><text></text></list-item></list-item></list-item></text></text></text>

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	 ☑ Change Auditing ☑ Policy Management
Available Policies	CIS PCI DISA NIST 800-53 (FISMA)

42. Select any available policies desired.

⁹ Microsoft Windows Server 2008 R2 ⁹ Microsoft Windows Server 2012 R2	× Microsoft Windows Server 2012 R2 × Oracle Solaris 10 v Oracle Solaris 11	
Microsoft Windows Server 2012 R2	v Oracle Solaris 11	
	X Oracio Oblaria II	
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		
irtual Infrastructure		
VMware ESXi 5.5 Server		
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 checks at 1:00 • AM •	Run the reports at 4:00 V AM V	
How frequently would you like to run checks on your assets?	How frequently would you like to run reports on your assets?	
your assets?	your assets?	
Weekly • on Sundays •	Weekly on Sundays	

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: `~!@#\$%^&"()=+{[[]]\\ ;;"'<,>./?	User Name:		
	admin	~	
	Password:		
		~	
	Confirm Password:		
		~	
	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.

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 - Windows Policy Check - RHEL 7 Policy Check - RHEL 7 Policy Check - Solaris 11 Policy Check - July File System Changes by Node Report Task - Daily File System Changes by Rule Report Task - Daily File System Changes by Rule Report Task - Test Result Summary - Solaris - PCI v3.1 Report Task - Test Result Summary - Solaris - PCI v3.1 Report Task - Test Result Summary - Solaris - PCI v3.1 Report Task - Test Result Summary - Windows - PCI v3.1 Report Task - Test Result Summary - Windows - PCI v3.1 Report Task - Test Result Summary - Windows - PCI v3.1 Report Task - Test Result Summary - Windows - PCI v3.1 Report Task - Test Result Summary - Windows - PCI v3.1 Report Task - Test Result Summary - Windows - PCI v3.1 Report Task - Test Result Summary - Windows - PCI v3.1 Report Task - Test Results by Node - Koldnis - PCI v3.1 Report Task - Test Results by Node - Windows - PCI v3.1 Report Task - Test Results by Node - Windows - PCI v3.1 Report Task - Waivers - Red Hat - PCI v3.1 Report Task - Waivers - Solaris - PCI v3.1 Report Task - Waivers - Solaris - PCI v3.1 Report Task - Waivers - Videow With Daily Changes Report Task - Waivers - Solaris - PCI v3.1 Report Task - Waivers - Waivers - Red Hat - PCI v3.1 Report Task - Waivers - Waivers - Red Hat - PCI v3.1 Report Task - Waivers - Videow With Daily Changes Report Task - Waivers - Videow VIdeow - PCI v3.1 Report Task - Waivers - Videow VIdeow - Not v3.1 Report Task - Waivers - Videow - PCI v3.1 Report Task - Waivers - Videow - PCI v3.1 Report Task - Waivers - Videow - PCI v3.1 Report Task - Waivers - Videow - VIdeow - PCI v3.1 Report Task - Waivers - Videow - PCI v3.1 Report Task - Waivers - Vid			
These home pages will be applied to your configuration Change Audit Customer Center Home Page PCI Overview - Red Hat PCI Overview - Solaris PCI Overview - ViMware ESX PCI Overview - Windows Tripwire Enterprise Administrator			
	Apply Configuration	Edit Configuration Ctil a te Voar	Relow

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 to ThipWild EnVerbried |

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	_1	×
licrosoft 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 X Firefox Survey 	× +				L=	6
← → C* ŵ ① & https://t	ripwire-e/console/app.showApp.cn	md		🛡 ☆	lii1\	
ENTERPRISE HOME NODES RULES ACTIONS	TASKS POLICIES LOG REPORTS	S SETTINGS				
Nodes Asset View Node Search Element Se	earch Version Search				🕀 Refresh 🔟 Help	D Logou
Filter Assets Manage Tagging	Ali 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			Manage Tagging Create Tags, Tagging Profiles, and Saved Filters.		
	EXCHANGE 192.168.1.134			Filter Assets		
System Tag Sets Database Server	HYPERV.DI.IPDR 192.168.78.105		-	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	ASKS POLICIES LOG REPORTS SETTINGS	
Nodes Asset View Node Search Element Se	arch Version Search	🔂 Refresh 🔟 Help 🕅 Logout
Filter Assets Manage Tagging	Create and Edit Tag Sets	
Tag Sets	Tutorial	Tag Sets
Tagging Profiles	× Location	(Add tags) Tags and Tag Sets are limited to 50 characters in length and may
Saved Filters	Add a new tag	not contain the following characters: ,,''\ 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
	× ▼ Owner Add a new tag Add × DI Testing	(1 tep) you can always rename or delete the tags tater. Tags are organized using tag sets, which group a set of related tags. For example, a tag set named Location could include the tags Portland, Chicago, and New York. These tags would be represented

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)	1
	Add a new tag	Add		
	× DI Testing			
×	Platform Family		(4 tags)	
	Add a new tag	Add		
	× Red Hat			Ξ
	× Solaris × VMware ESX			
	× Windows			
×	 Primary Function 		(1 tag)	
	Add a new tag	Add		
	× Domain Controller			
×	Tutorial		(Add tags)	
	Tutorial tag	bba		

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	arch 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	-	Edit Tags Health Check 🔻	
Clear all Save current filter	ad-dns.di.jpdr 192.168.1.12		XWINDOWS10-1.DLIPDR XWINDOWS10-2.DLIPDR XWINDOWS10-3.DLIPDR	
System Tag Sets Database Server	HYPERV.DI.IPDR 192.168.78.105	-		
Operating System Status	MSSQL 192.168.1.141	-	-	
Virtual Infrastructure	192.168.1.136		• •	
Tag Sets Location	WINDOWS10-1.DI.IPDR 192.168.1.138	-		
Platform Family Primary Function	WINDOWS10-2.DI.IPDR 192.168.78.118	-	R.	
Tutorial Saved Filters	WINDOW S10-3.DI.IPDR 192.168.78.119	-	i l	
Windows 2008 R2 Domain Controllers Windows 2012 R2 Domain Controllers				
Operational Tag Sets				
▶ Health			Activate Window	WS

9. Click Edit Tags.

10. Check the boxes next to any tags you wish to add to these nodes.

VENTERPRISE HOME NODES RULES ACTIONS	TASKS POLICIES LOG REPORTS SETTINGS	2 	
Nodes Asset View Node Search Element	Search Version Search		Refresh [] Help () Logout
Hiter Assets Manage Tagging	Edit Tags	Se	rected 5 Crear
Filter assets by keyword Q	For: 3 Assets	_ <u>E</u>	dit Tags Health Check
Clear all Save current filter	Tag Sets	×	WINDOWS10-1.DI.IPDR
	Location	(0 tags)	WINDOWS10-2.DLIPDR
	▼ Owner	(1 tag)	WINDOWSTU-J.D.IPDR
	DI Testing		
▼ System Tag Sets	▼ Platform Family	(4 tags)	
Database Server Directory Server Network Device > Operating System > Status	Red Hat Solaris VMware ESX Windows Windows	(1 text)	
Virtual Infrastructure	Damaia Castrollar	(1.00)	
▼ Tag Sets	Domain Controller		
Location Owner Platform Family Primary Function Tutorial	▼ Tutorial tag	(1166)	
▼ 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		🔂 Refresh 🔟 Help 🖟 Logout
🖺 🎦 New Group 🚺 New	Rule 🗿 Import 🕼 Export 🔤 Duplicate 🗙 Delete 🔽 Link 🚳 Unlink 🕼 Move	
- Tripwire	Rules	Tutorial
∃ ∐ Linux OS Rule Grou	A Name Type Description	
Solaris OS Rule Gro	JP	
UMware Virtual Infr	sstru irour	
Critical Change	udt	
Testing		
Testing		

- 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.

🛈 <u> h</u> ttps://	/tripwire-e/console/app.showWizard.cmd?wizardName=si.web.specifierR	luleV ••• 💟	1 ☆ =
New Windov	vs File System Rule Wizard		🛛 Help
Enter a name Name: Description:	a and description for the rule. tutorial rule a rule specifically for tutorial documentation		
	< Back Next >	Finish	Cancel
ck Next.			
	New Windows File System Rule Wizard - Mozilla Fin	efox	

7.

	New \	Windows File Syst	em Rule Wizard	Mozilla Firefox	_	
🛈 陷 http	s://tripwire-e/cons	ole/app.showWizar	d.cmd?wizardNam	e=si.web.specifierR	uleV 🚥 💟	• ☆
New Wind	ows File Syster	m Rule Wizard				? Help
New Start	Point New Sto	p Point Brows	e X Delete			
🗌 🛓 Path	Type Default Se	verity Criteria Se	t 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				? Hel
Specify the monitored obj Path: C:\Users\D12\Deskt Default Severity: 1000 Archive element conter Recurse directory Limit depth to 0	ect for the start point, op\Tutorial docs (0-10,000, 0 = no nt (0-100, 0 = no limit)	, and enter asso	aiated settings.	

11. Click Next.

12. Select Windows Content and Permissions.

b	New Start Point Wizard - Mozilla Firefox
🛈 陷 https://tripwire-e/consc	ole/app.showWizard.cmd?wizardName=si.web.startPointWie 🚥 😒 🏠
New Start Point Wizard	I He
New Criteria Set Mew Fro	m Selected
🛓 Name	Description
Windows - Content and F	Permissions
🔿 🎬 Windows - Content Only	
🔿 🛅 Windows - Permissions O	Dnly
	<pre></pre>
	C

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.

	New Stop Point Wizard - Mozilla Firefox		x
1 🖍	https://tripwire-e/console/app.showWizard.cmd?wiz 🚥 💟	☆	Ξ
New S	Stop Point Wizard	? H	elp
Specif setting Path:	y the monitored object for the stop point, and enter asso gs. C:\Users\DI2\Desktop\Tutorial docs\Tutorial3 Stop recursion	ciate	d
	< Back Next > Finish C	ancel	

- 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
	Tripwire Proof Task Group	Tasks
	Check Tasks	Aname Type Status Last Start Last Duration Timeout Next Start Description
	Change Audit Report	
	😠 🥶 Security 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	-		x
🛈 🚯 https://	/tripwire-e/console/app.showWizard.cmd?wizardName=wizard.newBaselineT ••••	◙	☆	≡
New Baselin	e Rule Task Wizard		<u>р</u> н	≥lp
Enter the tas	k name and description.			
Name:	Tutorial Task			
Description:	Task for tutorial documentation			
Run as user:	admin v			
	hour(s) 3 minute(s)			
	< Back Next > Finish	С	ancel	J

- 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).

6 New Baseline Rule Task Wizard - Mozilla Firefox	-		x
🛈 🚯 https://tripwire-e/console/app.showWizard.cmd?wizardName=wizard.newBaseline	🛡	☆	- 0
New Baseline Rule Task Wizard		РН	elp
 Kout Node Group Smart Node Groups Operational Tag Sets System Tag Sets Tag Sets O I Testing Platform Family Primary Function Tutorial Tutorial VINDOWS10-1.DLIPDR WINDOWS10-3.DLIPDR 			× III ×
Selection: 💡 Tutorial tag			
< Back Next > Fini	ish	Cancel	ľ

- 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.

	line Bule Tack Wizard		
New Base			Шпе
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		

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	X
	1	Register Tripwire Log Center To continue you must register your copy of Tripwire Log Center.	
		Name Organization	
		Serial Number .	
		Email Address	
0.111			
Get rielp		Register Ca	ncel

- 5. Click Register.
- 6. Enter details about the database that Tripwire Log Center should use.

		Defaul	tEventD	atabase	
An option Database Tripwire	al componen stores Even Log Center da	t of your Tripwire I ts. Following insta ata.	Log Center en Ilation, you m	vironment, an Event-Manage ay add other databases to ma	ment anage your
Conne	ctivity		Se	curity	
Databa	se software	MS SQL	~	Encrypt data with SSL	
Host IF	address	192.168.1.141			
Host p	ort	1433			
Use W	indows authe	ntication 🗸			
This op assign Service	otion uses the ed to the Trip e to connect t	Windows credent wire Log Center M to an MS SQL insta	tials lanager ance.	R	
Userna	me				
Passw	ord				
		8	Test Conne	ectivity	
				Next S	Evit

- 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	
ks (
Back Next 📎 🕞 Exit	

- 9. Click Next.
- 10. Enter a **password** and an **email**.
- 11. Change the IP to a hostname, if preferred.

۵.	Configuration Wizard -	Tripwire Log Center	×
	Primary Mana	ger Settings	
Enter a n Additiona need this	ame of your choosing for the Primary Man ally, enter and confirm a password for the o password to log in to Tripwire Log Center	ager, as well as the Manager's l default Administrator user accou r.	Paddress. nt. You will
	Primary Manager		
	Manager name	Primary Manager	
	Manager IF/nostname	arcsignt-cons.di.ipdr	
	Administrator Settings		0
	Administrator password (confirm)		•
	Email address	administrator@di.ipdr	
N			
K			
		💰 Back 🛛 Next 📎	📕 Exit
	•		
2. CIICK Ne	xt.		×
	Configuration Wizard -	Tripwire Log Center	<u> </u>
	Manager Servic	e Credentials	
Specify t	he user account with which Tripwire Log 0	Center will authenticate with othe	er hosts.
	Authoritopto with:		
	The local Windows System	em user account	
	C Domain user account		
	Isername:		
	oborname.		
	Password:		
	Password: Password (confirm):		
	Password: Password (confirm):	Settings	L.
	Password: Password (confirm):	Settings	Ŀ,
	Password: Password (confirm):	Settings	ß
	Password:	Settings	l≩
	Password:	Settings	k∂ I 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 S	Setup							
Visibility Set	tup		izard					
Wireless Se	tup (Bl	ETA)						
Click Next.								
cisco Identity Services	Engine H	ome ▶ Cont	ext Visibility ► Ope	rations ♦ Policy ♦ A	Iministration + Wo	ork Centers License	Warning 🔺 🔍	0 0
Get to know the d	2 Network D	evices 3 Activ	ve Directory 4 Postu	re 🖌 Summary	I context with th	iis setup wizard.		
★ Welcome 1 Endpoint Get to know the d	evices and	evices 3 Activ users' detai Domain	e Directory 4 Postu Is of your netwo DC Host	re 🖌 Summary rk. Gain visibility and	I context with th	iis setup wizard. Grue Name		
★ Welcome 1 Endpoint Get to know the d	evices and	evices 3 Activ users' detai Domain Cisco.com	Postu Is of your netwo DC Host DC1.Cisco.com	re Summary rk. Gain visibility and IP Address 10.56.53.76	I context with th	iis setup wizard. Group Name Cscc.com/Network Configuration Operators		C Los H
Welcome 1 Endpoint	evices and t	avices 3 Activ users' detai Domain Cisco.com Cisco.com	A Postu S of your netwo DC Host DC1.Cisco.com DC2.Cisco.com	rk. Gain visibility and IP Address 10.56.53.76 10.56.53.77	d context with th	is setup wizard. Group Name Cisco.com/Network Configuration Operators Cisco.com/Renformance Monitor Users		
Welcome 1 Endpoint	evices and	vices 3 Activ users' detai Domain Cisco.com Cisco.com	Is of your network DC Host DC Host DC Clisco.com DC2.Clisco.com DC3.Clisco.com	P → Summary rk. Gain visibility and IP Address 10.56.53.76 10.56.53.76 10.56.53.76	i context with th	is setup wizard. Group Name Cacc.com/Network Configuration Operators Cacc.com/Performance Monitor Users Cisco.com/Performance Log Users		
Welcome 1 Endpointe	evices and	vices 3 Activ users' detai Domain Cisco.com Cisco.com Cisco.com Cisco.com	DC Host DC Host DC Lisco.com DC2 Clisco.com DC3 Clisco.com DC4 Clisco.com	P ✓ Summary rk. Gain visibility and IP Address 10.56.53.76 10.56.53.79 10.56.53.79 10.56.53.79 10.56.53.79	I context with th	Group Name Group Name Casc.com/Network Configuration Operators Cisco.com/Performance Monitor Users Cisco.com/Performance Log Users Cisco.com/Disributed COM Users		
Welcom 1 Endpoint	 2 Network D evices and i i<td>Users' detai Domain Cisco.com Cisco.com Cisco.com Cisco.com</td><td>DC Host DC Host DC Lost DC: Cisco.com DC: Cisco.com DC: Cisco.com DC: Cisco.com DC: Cisco.com</td><td>P ✓ Summary rk. Gain visibility and IP Address 10.56.53.76 10.56.53.77 10.56.53.78 10.56.53.78 10.56.53.78 10.56.53.80 10.56.53.81</td><td>I context with th</td><td>Group Name Group Name Cace.com/Network Configuration Operators Cace.com/Performance Monitor Users Cace.com/Distributed COM Users Cace.com/Distributed COM Users</td><td></td><td>C Carro</td>	Users' detai Domain Cisco.com Cisco.com Cisco.com Cisco.com	DC Host DC Host DC Lost DC: Cisco.com DC: Cisco.com DC: Cisco.com DC: Cisco.com DC: Cisco.com	P ✓ Summary rk. Gain visibility and IP Address 10.56.53.76 10.56.53.77 10.56.53.78 10.56.53.78 10.56.53.78 10.56.53.80 10.56.53.81	I context with th	Group Name Group Name Cace.com/Network Configuration Operators Cace.com/Performance Monitor Users Cace.com/Distributed COM Users Cace.com/Distributed COM Users		C Carro
Welcom 1 Endpoint	 2 Network D evices and a a<td>Domain Cisco.com Cisco.com Cisco.com Cisco.com Cisco.com Cisco.com Cisco.com</td><td>DC Host DC Host DC Host DC: Clico.com DC2: Clico.com DC3: Clico.com DC4: Clico.com DC4: Clico.com DC4: Clico.com</td><td>P Address 10.56.53.76 10.56.53.76 10.56.53.78 10.56.53.80 10.56.53.81</td><td>I context with th</td><td>is setup wizard. Group Name Caco.com/Network Configuration Operators Caco.com/Performance Monitor Users Caco.com/Derformance Log Users Caco.com/Deformance Log Users Caco.com/Deformance Log Users Caco.com/Deformance Log Users Caco.com/Deformance</td><td></td><td>C Carro</td>	Domain Cisco.com Cisco.com Cisco.com Cisco.com Cisco.com Cisco.com Cisco.com	DC Host DC Host DC Host DC: Clico.com DC2: Clico.com DC3: Clico.com DC4: Clico.com DC4: Clico.com DC4: Clico.com	P Address 10.56.53.76 10.56.53.76 10.56.53.78 10.56.53.80 10.56.53.81	I context with th	is setup wizard. Group Name Caco.com/Network Configuration Operators Caco.com/Performance Monitor Users Caco.com/Derformance Log Users Caco.com/Deformance Log Users Caco.com/Deformance Log Users Caco.com/Deformance Log Users Caco.com/Deformance		C Carro

- 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	 Administration 	Work Centers	License Warning 🔺	0,	0	•	(0)
endpoints using the I	IP range(s) below.									
192,163.0.0/10									Delete	
e.g. 10.10.10.0/24				14					Delete	10
3 O										
										_
						54		ack	No	XE
	ngine Home	ngine Hore Contrast Valabity endpoints using the IP range(s) before 192.193.0.0/10 eg.10.10.10.0/24 @	ngine Home Context Visibility Operations endpoints using the IP range(s) below. 192 193 0.0/10 e.g. 10.19.10.0/24 @ •	ngine Hone) Context Visibility) Operations) Policy endpoints using the IP range(s) below. 192:193:0.0/10 e.g. 10:10:10.0/24 @ •	ngine Home + Context Visibility + Operations + Pokcy + Administration rendpoints using the IP range(s) below. 192: 103:0:0/16 eg: 10:10:10:0/24 ©	ngine Hone + Contrast Visibility + Operations + Pokey + Administration + Work Centers. endpoints using the IP range(s) below. 192.103.0.0/10 e.g. 10.10.10.0/24 © ©	ngine Hone i Context Vabelty i Operations i Poley i Administration i Work Centers. License Wamnig A rendports using the IP range(s) below. 192.103.0.010 ag 10.10.10.024 b ⊗ ●	ngine Hone) Control Valbety) Operations) Policy) Administration) Work Centure Livense Warming A Q endpoints using the IP range(s) before. 192.103.0.016 e.g. 10.10.10.024 ©	ngine Home + Context Valokity + Operations + Policy + Administration + Work Centers Levene Warning A Q @ endpoints using the (P rangels) below: 192: 103:0:0/16 e.g: 10:10:10:0/24 & © Sap Back:	ngine Home + Context Vability + Operations + Policy + Administration + Work Centers License Warning A Q @ Q endpoints using the IP rangels) below. 192.103.0.0/16 e.g. 10.10.10.0/24 & O Sig Back Net

- 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 Internet condition Figure 1	Context Visibility + Operat	sons + Policy + Administration + Work Centers		Deense Warning 🐽 📉 🔍 🔍 O 🖓
ISE VISIBILITY SETUP WIZARD	Add Network Dev	ice	×	Q. Exit Wicard
Network Device Discovery	Name *	GATEWAYROUTER		
Total Added (0) Failed (0)	IP Address *	192.168.1.1		
Q, Scan + Add @ Firming	Location			¥ Filar •
Name IP Address You have not added any relieve a access de	Device Type			
	Description			
	SNMP Settings	P.		
	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	P WIZARD		🕒 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	DUT 192.168.1.1	Edit	
			4
			Back
			Server Response
			Network Devices created successfully
CIICK Next.			
Enter a disp	ilay name.		
Enter the de	omain name.		
Enter the h	ostname of Cisco ISE.		
Entor a uso	rname and nassword		
Click Test C	onnection to ensure that this works.		
cisco Identity Services E	Engline Home Context Visibility Operations Policy Administration Work Category	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 *	DLIPDR		
Domain FQDN *	DI IPDR cisco-ise di ipdr		
Domain FQDN * ISE Node * Username *	DLIPDR cisco-ise di jadr Administrator		
Domain FQDN * ISE Node * Username * Password *	Di IPDR cisco-ise di jodr Administrator		
Domain FQDN * ISE Node * Username * Password *	Di IPDR cisco-ise di ipdr Administrator		
Domain FQDN * ISE Node * Username * Password * Organization Unit	D IPDR Disco-ise di ipdr Administrator e.g. CN=COMPUTERS.DC=CISCO.DC=COM	R	
Domain FQDN * ISE Node * Username * Password * Organization Unit	DLIPDR Cisco-ise dLipdr Administrator e.g. CN=COMPUTERS.DC=CISCO.DC=COM Test Connection	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	2 Network Devices	3 Active Directory	4 Posture	✓ Summary					œ	Exi
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	× 0									
IP Address Range *	192.168.0.0/16									
Include Range	2 0									
									₽\$	
								Skip B	ack	
Click Next.								Skp B	ack	
Click Next.	g ine Hame	 Context Visibility 	→ Operations	Policy	Administration	→ Work Centers	License Warning	Skip (B	ack	
Click Next.	gine Hame true ●	 Context Visibility 	Operations	• Робсу	Administration	→ Work Centers	License Warning	Skip B	ack Ø	
Click Next. "Interference and active Scanning Network Device Discovery	gine Home true O	Context Visibility	+ Operations	→ Policy	Administration	• Work Centers	License Warning	Skp B	ack Ø	
Click Next. dentify Services En Active Scanning Network Device Discovery Total Devices Added	jine Home true O	 Context Visibility 	► Operations	▶ Policy	Administration	Work Centers	License Warning	5xp (B	Ø	
Click Next. dentity Services Eng Active Scanning Network Device Discovery Total Devices Added Active Directory Information	g ine Home true O	Context Visibility	➤ Operations	⊁ Policy	Administration	• Work Centers	License Warning	Skip B	Ø	
Click Next. Identity Services Eng Active Scanning Network Device Discovery Total Devices Added Active Directory Information Display Name	tue O	Context Visibility	➤ Operations	▶ Policy	Administration	• Work Centers	License Warning	Skip B	Ø	
Click Next. Services End Active Scanning Network Device Discovery Total Devices Added Active Directory Information Display Name Domain FQDN	jine Home true O 1 ADDNS DIJPDR	 Context Visibility 	Operations	Policy	▶ Administration	• Work Centers	License Warning	Skep B	e e e e e e e e e e e e e e e e e e e	
Click Next. Services Eng Active Scanning Network Device Discovery Total Devices Added Active Directory Information Display Name Domain FQON ISE Node	Internet Home true • 1 ADDNS DUPDR cisco-ase dupdr	 Context Visibility 	Operations	Policy	Administration	→ Work Centers	License Warning	Sxop (B	0	
Click Next. Services Eng Active Scanning Network Device Discovery Total Devices Added Active Directory Information Display Name Domain FQDN ISE Node Username	pine Home true • 1 ADDNS DLIPDR cisco-ise duipdr	 Context Visibility 	➤ Operations	Policy	Administration	Work Centers	License Warning	Sxp B	e e	

- 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

Home Home	Context Visibility Operations Policy Administration Work Centers	License Warning 🛕	٩
System Identity Management Network Identities Groups External Identity Sources	Resources Device Portal Management pxGrid Services Feed Service Threat Cen Click here to do wirel Identity Source Sequences Settings	ess setup and visibility setup	Do not s
External Identity Sources	Active Directory Edit <u>A</u> dd <u>Delete</u> <u>Node View</u> <u>Advanced Tools</u> <u>Scope Mode Join Point Name <u>Active Directory Domain <u>No data available </u></u></u>		
Click Add.			
Enter a name.			

- 2.
- 3.
- 4. Enter the **domain.**

System Identity Management Network Re Identities Groups External Identity Sources	Identity Source Sequences S	ement pxGrid Services + Feed Service + ettings	Threat Cen Click here to do wireless setup and visibility setup I	Do not sl
External Identity Sources	Connection * Join Point Name * Active Directory Domain & Submit Cancel	AD-DNS diupdr		

-1[-1]-- Identity Services Engine Home + Context Visibility + Operations + Policy Administration + Work Centers License Warning A Q

5. Click Submit.

Identitiv Identity Services Engine Home System Identity Management identities Groups External identity	Context Visibility Operatio Would you like to Join all ISE Nodes to	o this Active Directory Domain?	ation Viork Centers	License Warning 🔺 🔍
External Identity Sources	* Join Point Name		No Yes	Advanced Settings
Centricate Authentication Profile Active Directory Ap-DNS LDAP DDBC	* Active Directory Domain	di.lpdr ser 🙆 Diagnostic Tool 😪 Refi	resh Table	Ф.
RADIUS Token RSA Securit Social Login Social Login	ISE Node	ISE Node Role STANDALONE	Status Doman (Controller Site

- 6. Click Yes.
- 7. Enter a **username** and **password** to join ISE to the domain.

External Identity Sources Connection Whitelisted Domains PassvelD Groups Attributes Advanced Settings * Los Point Name AD-ONS * * Advec Directory * * Advec Directory * * Advec Directory * . . . * Advec Directory * Advec Directory * Advec Directory * Advec Directory Domain. * BassvelD * Advec Directory Domain. * BassvelD <t< th=""><th>Identities Groups External Identity Sc</th><th>ources Identity So</th><th>ource Sequences + S</th><th>Settings</th><th></th><th></th><th></th><th></th></t<>	Identities Groups External Identity Sc	ources Identity So	ource Sequences + S	Settings				
	External Identity Sources		ionnection W	hitelisted Domains	PassiveID	Groups	Attributes	Advanced Settings
Active Directory AD-DNS AD-DNS Doin Domain Please specify the credentials required to Join ISE node(s) to the Active Directory Domain. AD-User Name ① DI/Administrator * AD User Name ① DI/Administrator * Password * Password * Security Specify Organizational Unit ② Social Login Social Login		- (i)-	* Join Point Name	AD-DNS			a.	
	AD-DNS COBC OBC RADUIS Token RSA SecuriD SAML Providers Social Login	Please specify	the credentials required * AD User Name () * Password Organizational Unit () Store Credentials ()	to Join ISE node(s) t DI\Administrator	to the Active Directory D	omain.	Controller	Site

8. Click **OK.**

System Identity Services Engine System Identity Management Identities Groups External Identit	Home Context Visibility Natwork Resources Device P y Sources Identity Source Seque	Operations Policy ortal Management pxGrid Servic nces Settings	Administration Mo Keed Service	• Threat Cen Click here to do wi	License Warning A R
External Identity Sources	Join Operation Status Status Summary: Successful ISE Node cisco-ise di ipdr	Node Status Completed	k	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.

tiletter Identity Ser	vices Engine H	ome 🕨	Context Visibility	+ Oper	ations	Policy A	dministration	• Work C	enters		License \	Naming 🔺	9.	0	•	•
System Ident	tity Management + Ne	etwork Reso	ources + Device F	Portal Mar	agement	pxGrid Services	Feed Service	ce + Thr	eat Centric NA	C						
Deployment Licer	nsing + Certificates	 Logging 	Maintenance	Upgrad	le Baci	kup & Restore	 Admin Access 	 Settin 	gs							
Deployment			Deployment N	odes												
中•臣•		- 										5	elected 1	Total 1		
Deployment Deployment	¢		/ Edit 🔯 Re	pster	Syncup	Deregister					Show	All		14	+ 15	8
The second	e		Hostname		 Persons 	35		1	Role(s)	Services			Node	e Status		
			Cisco-ise		Adminis	stration, Monitoring	g, Policy Service		STANDALONE	IDENTITY N	APPING, SESSIO	ON, PROFILER				
							56									
lick Edit																

4. Check the box next to Enable Passive Identity Service.

o Identity Services Engine Home	Context Visibility	License Warning 📣	9	0 0	
System Identity Management Network Res	urces				
ployment Licensing Certificates Logging	Maintenance Upgrade Backup & Restore Admin Access Settings				
	Role STANDALONE Make Primary				
	Administration				
	✓ ▼ Monitoring				
	Role PRIMARY *				
	Other Manifester Made				
	Uther Manitoring Node				
	Policy Service				
	Enable Session Services (i)				
	Include Node in Node Group None (1)				
	Enable Profiling Service (j)				
	Enable Threat Centric NAC Service (1)				
	Finable SXP Service (1)				
	Enable Device Admin Service (i)				
	Enable Passive Identity Service (1)				
	C word @				
	bave 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.

cisco Identity Services Engine Home	Context Visibility Operations	Policy Administration W	fork Centers	License Warning 🔺	Q,	0	•	ø
System Identity Management Network F	Resources + Device Portal Management	pxGrid Services + Feed Service	Threat Centric NAC					
Identities Groups External Identity Sources	Identity Source Sequences							
External Identity Sources	Active Directory	iede View Advanced Tools - Scop	e Mode Domain					

- 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	+ Opennions + Policy	*Ammistration		License Warning	9. 0 0 4
Eystem Identities Groups Extended					×	
External Identity Source	Add Domain Controllers					
• En Centruste Authentica		Domain	DC Host	Site		
 Active Descory Actions 	0	di ipdr	ad-dns-supp.di.ipdr			
EL LOAP		DLIPDR	AD-DNS.DLIPDR	Default-First-Site-Name		
RADIUS Teken	•	di.ipdr	ad-dns08 di ipdr		14	
SAAL IS Provides				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.

External Identity Source	Edit Domain Controller		
	Host FQDN	AD-DNS DLIPDR	
Centricals Authentical Centricals Authentical Active Directory Active Directory Active Directory Active Directory Centricals	Description		Con 1 Tatal Ross
ODEC	User Name *	administrator	
RSA Securito	Password	Show Password	Address - Addres
Secial Login	Protocol	WMI * Configure Test	6
			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	Controllers	ows/Page 1 *	1 /1 Go	1 Total Rows
LDAP	C Refresh & E	Config WMI in process	MI Add Agent		
RADIUS Token	🗷 Domain	Configuration of WMI has begun and will take some time.		IP Address	Monif
SAAL id Providens 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	Policy Administration Work Centers	License Warning 🛕	8	0	•
System Identity Management	Network Resources	pxGrid Service Feed Service Threat Centric NAC				
Deployment Licensing + Certificate	s + Logging + Maintenance Upgrade + Bac	kup & Restore + Admin Access + Settings				
0						
Client Provisioning	Client Provisioning					
FIPS Mode	chenerrorisioning					
Security Settings	* Enable Provisioning	Enable *				
Alarm Settings	* Enable Automatic Download	Enable + 0				
▶ Posture	" Update Feed URL	https://www.cisco.com/web/secure/spa/provisioning-upda				
Profiling	* Native Supplicant Provisioning Policy Unavailable	Apply Defined Authorization Policy *				
Protocols						
Proxy	Save Reset	N				
SMTP Server		4				
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 groups from the Directory	nny ⊁Operanions ⊭Poucy	Administration	Work Geners	×
 Identities 	Domain di.ipdr		•	1	
	Name Filter * SID	Filter *	Type ALL	*	
ces	Retrieve Groups 68 Groups Retrieved.	in a state of the	T mus		
	☑ Name	Group SID		Group Type	<u>^</u>
ation Profile	DI.IPDR/Builtin/Access Control Assistance Oper-	ators di.ipdr/S-1-5-32-579		BUILTIN, DOMAIN LOCAL	
	DLIPDR/Builtin/Account Operators	di.ipdr/S-1-5-32-548		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Administrators	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/Certificate Service DCOM Acces	s di.ipdr/S-1-5-32-574		BUILTIN, DOMAIN LOCAL	
	DI IPDR/Builtin/Cryptographic Operators	di.ipdr/S-1-5-32-569		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Distributed COM Users	di.ipdr/S-1-5-32-562		BUILTIN, DOMAIN LOCAL	
	DI IPDR/Builtin/Event Log 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-V Administrators	di.ipdr/S-1-5-32-578		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/IIS_IUSRS	di.ipdr/S-1-5-32-568		BUILTIN, DOMAIN LOCAL	
	DI.IPDR/Builtin/Incoming 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	
	DI. IPDR/Builtin/Performance Log Users	di.ipdr/S-1-5-32-559		BUILTIN, DOMAIN LOCAL	
					Cancel

- 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.

System	Directory Attributes Only attributes selected below will t	be available for use as polic	cy conditions in polic	cy rules.			×
 Identities 	* Sample User or Machine Account	ciscoiseadmin Retrieve Attributes	Ð				1 8
	Name IogonHours	Type OCIET STRING		Example Val (Binary Valu	lue e)		
05	mDBUseDefaults	STRING		TRUE			
	memberOf	STRING		CN=Organiz	ation Management,O	J=Microsoft Exchange Security Grou	
cation Profile	msExchDumpsterQuota	STRING		31457280			
	msExchDumpsterWarningQu	ota STRING		20971520			
	msExchHomeServerName	STRING		(Non-Display	vable or XSS data)		
	msExchUserAccountControl	STRING		0			
	name	STRING		ciscoiseadm	in		N
	objectCategory	STRING		CN=Person,	CN=Schema,CN=Cor	figuration,DC=DI,DC=IPDR	16
	objectClass	STRING	1	top			
	objectGUID	STRING		887223A099	6062468648D3C3B8	55A0C7	
	objectSid	STRING)	S-1-5-21-28	93925980-384658434	3-2419738538-1268	
	primaryGroupID	STRING	1	513			
	protocolSettings	OCTET_STRING		(Binary Valu	e)		
	pwdLastSet	STRING		1318894364	95884672		
	sAMAccountName	STRING		ciscoiseadm	in		
		STRING		805306368			Ŧ
							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	▼ Policy	Administration	Work Centers		License W	aming
Policy Sets Profiling Posture	Client Provi ults	Policy Elements					Click here to do wireles	s setup and v	isibility :
trary Conditions mart Conditions	Anti	-Malware Conditions							
me and Date	/ E	dit 🕂 Add 🖓 Duplicate Name	X Delete Descript	ion				Show	All
Posture		ANY_am_win_inst ANY_am_win_def	Any AM Any AM	installation of definition ch	heck on Win eck on Wind				
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition File Condition		ANY_am_mac_Inst ANY_am_mac_def Cisco-AMP	Any AM Any AM Require	installation d definition ch s Cisco AMP	heck on Mac				
Firewall Condition Patch Management 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.

A Not secure	https://cisco-ise.di.ipdr/a	cumuly "poncy/pc	Jucy_counterie				H O
Identity Services Engine	Home → Context V	/isibility → Ope	rations 👻 F	olicy Administration	Work Centers ■	🕚 Li	cense Warning 🔺
Policy Sets Profiling Posture	Client Provisioning Poli	icy Elements				Click bare to do wirelast se	tup and visibility e
Dictionaries Conditions Re-	sults					Shek here to do where sa ac	sup and reading a
Jbrary Conditions	Anti-Malware Condition	ns List > New Anti-	Malware Cond	tion			
Smart Conditions	Anti-Malware Cor	ndition		_			
Time and Date	* Name	CiscoAMP					
Profilina	Description	Check for cisco A	MP				
Protect	Compliance Module	4.x or later (i)					
" Posture							
	Consisting System	Windows All	A.]				
Anti-Malware Condition	* Operating System	Windows All	\$				
Anti-Malware Condition Anti-Spyware Condition	* Operating System Vendor	Windows All Cisco Systems, In	ф к.	0			
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition	* Operating System Vendor Check Type	Windows All Cisco Systems, In Installation (↓ ↓ ↓ Definition 	0			
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition	* Operating System Vendor Check Type	Windows All Cisco Systems, In Installation (Definition 	0			
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition	* Operating System Vendor Check Type * Products for Se	Windows All Cisco Systems, In Installation (elected Vendor	C. C. Definition	0			
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition	* Operating System Vendor Check Type * Products for So Product Name	Windows All Cisco Systems, In Installation (elected Vendor	C. Definition Version	Remediation Support	Definition Check	Latest Definition Date	Latest Defin
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition File Condition	* Operating System Vendor Check Type • Products for So Product Name ANY	Windows All Cisco Systems, In Installation (elected Vendor	C. Definition Version ANY	Remediation Support N/A	Definition Check YES	Latest Definition Date	Latest Defin
Anti-Malware Condition Anti-Syyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition File Condition	* Operating System Vendor Check Type • Products for So Product Name ANY Cisco Advanced	Windows All Cisco Systems, In () Installation () elected Vendor d Malware Protec.	C. Definition Version ANY 5.x	Remediation Support N/A NO	Definition Check YES YES	Latest Definition Date 02/19/2019	Latest Defin 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 Sc Product Name ANY Cisco Advanced V Cisco Advanced	Windows All Cisco Systems, In Cisco Systems, In Installation Cisco Vendor Cisco Ven	 Definition Version ANY 5.x 6.x 	Remediation Support N/A NO NO	Definition Check YES YES YES	Latest Definition Date 02/19/2019 02/19/2019	Latest Defin 7.79603 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 Sc Product Name ANY Cisco Advanced	Windows All Cisco Systems, In Cisco Systems, In Installation Clected Vendor d Malware Protec. d Malware Protec.	C. Definition Version ANY 5.x 6.x	Remediation Support N/A NO NO	Definition Check YES YES YES	Latest Definition Date 02/19/2019 02/19/2019	Latest Defin 7.79603 7.79603
Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition File Condition File Condition Firewall Condition Patch Management Condition Registry Condition	* Operating System Vendor Check Type • Products for Se Product Name ANY Cisco Advanced	Windows All Cisco Systems, In Installation (elected Vendor d Malware Protec. d Malware Protec.	 Version ANY 5.x 6.x 	Remediation Support N/A N/O N/O	Definition Check YES YES YES	Latest Definition Date 02/19/2019 02/19/2019	Latest Defin 7.79603 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 Service Condition	* Operating System Vendor Check Type • Products for Se Product Name ANY Cisco Advanced Cisco Advanced	Windows All Cisco Systems, In	c. Definition Version ANY 5x 6x	Remediation Support N/A NO NO	Definition Check YES YES YES	Latest Definition Date 02/19/2019 02/19/2019	Latest Defin 7.79603 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.

Induentity Services Engine	forme Context Visibility	Operations Policy	Administration Work Centers	🚯 License Warning 🔺	Q	6
Policy Sets Profiling Posture Client	Provisioning Policy Elements					
Dictionaries + Conditions - Results				Click here to do wireless setup and visibility se	rup Do no	x sno
0	ANY_av_win_inst then	Message Text Only				1.5
Authentication	Any_AV_Definition_Win	for Windows All	using 3 x or earlier	using AnyConnect	met	10
Authorization	ANY_av_win_def then	AnyAVDefRemediationWi n				- 24
Addionzation	Any_AS_Installation_Win	for Windows All	using 3 x or earlier	using AnyConnect	met	8
Profiling	ANY_as_win_inst then	Message Text Only				1
Posture	Any_AS_Definition_Win ANY_as_win_def theo	for Windows All AnyASDefRemediationWin	using 3 x or earlier	using AnyConnect	- met	30) (1
* Remediation Actions	AMP_CHECK	for Windows All	using 4.x or later	using Temporal Agent	• me	n if
Requirements	Cisco-AMP 💠 then Me	ssage 💠				E
Client Provisioning	Any_AV_Installation_Mac ANY_av_mac_inst then	for Mac OSX Message Text Only	using 3 x or earlier	using AnyConnect	met	1
	Any_AV_Definition_Mac ANY_av_mac_def then	for Mac OSX AnyAVDefRemediationMa c	using 3 x or earlier	using AnyConnect	met	.st
	Any_AS_Installation_Mac ANY_as_mac_inst then	for Mac OSX Message Text Only	using 3.x or earlier	using AnyConnect	mat	it j
	Any_AS_Definition_Mac ANY_as_mac_def then	lor Mac OSX AnyASDefRemediationMa c	using 3 x or earlier	using AnyConnect	met	
	Any_AM_Installation_Win ANY_am_win_inst then	for Windows All Message Text Only	using 4 x or later	using AnyConnect	met	(f)
	and the second sec	Concerning the second second				100

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).

cisco Ident	tity Servi	ces Engine	Home	Context V	/isibility ►C	perati	ions Policy	+ Administrat	ion	Work Centers		6	License Warning 🔺		.	0
Policy Sets	Profiling	Posture	Client Provisio	ning + Pol	licy Elements					C	lick here	o do w	ireless setup and visibility s	etup D	o not :	show
uny	and	Mac OSX	and	4 x or later		and	Temporal Agent		and			1997	ac_temporal		Т	
ny	and	Windows All	and	4 x or later		and	AnyConnect		and			hen	Any_AM_Installation_W			
uny	and	Windows All	and	4 x or later		and	Temporal Agent		and			hen	Cisco AMP		1	
Any <	> and	Windows All	\$	4.x or lat	ter •		Temporal Agent			(Optional) Dictionar	\$		Cisco AMP 🔶		Ľ	
iny	and	Mac OSX	and	4 x or later		and	AnyConnect		and :			hen	Default_AppVis_Requir ement_Mac		1	
ny	and	Mac OSX	and	4.x or later		and	Temporal Agent		and			hen	Default_AppVis_Requir ement_Mac_temporal			
liny	and	Windows All	and	4.x or later		and	AnyConnect		and			hen	Default_AppVis_Requir ement_Win			
ny	and	Windows All	and	4 x or later		and	Temporal Agent		and			hen	Default_AppVis_Requir ement_Win_temporal			
Later-	ord	Har DEV	200	A su per l'alore	5	and a	AniConnet		and			hen	Defect Econoli Deniel		. *	
											R	ş				

- 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 Idei	ntity Servi	ces Engine	Home	 Context Vis 	ability > Operations	► Policy	 Administration 	→ Wo	rk Centers	License Warning 🔺	٩,	0	0
+ System	+ Identi	y Management	 Network 	k Resources	Device Portal Management	nt pxGrid S	Services + Feed	Service	Threat Centric NAC				
Blacklist	BYOD	Certificate Prov	risioning	Client Provisioning	Mobile Device Manage	ment My I	Devices Custom	Portal Files	s > Settings				
Client	Provisio	ning Portals											
You can	edit and cu	stomize the def	ault Client Pr	ovisioning portal	and create additional ones								
Creat	te Edit	Duplicate	Delete										
Descining a	0	Second	and the second second										
c	lient Prov	isioning Porta	(default)										
D	Vefault porta	I and user expe	rience used	to install the post.	are agents and verify compl	iance 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.

Here Identity Services Engine H	ome	Policy Administration Work Centers	License Warning 🔺 🧠 😝
System Identity Management N	Vetwork Resources	ent pxGrid Services + Feed Service + Threat Centric NAC	
llacklist BYOD Certificate Provisionin	g Client Provisioning Mobile Device Manag	ement My Devices Custom Portal Files + Settings	
Authenticatio	Configure confidence at Administration > System Certific System Certificates Certificates, Request, Sequence - Configure administration - Identity Manager Identity Source Sequences	rates >	Succ
	User account with Super admin privilege or ERS a Available	dmin privilege will have access to the portal Chosen	
		ADDNS:DLIPDQ/Mkrosoft Exchange Securit = ALLACCOUNTS (default) ADDNS:DLIPDQ/Mkrosoft Exchange Securit ADDNS:DLIPDQ/Mkrosoft Exchange Securit ADDNS:DLIPDQ/UkrsyNDTModes ADDNS:DLIPDQ/UkrsyNDTModes ADDNS:DLIPDQ/UkrsyNDTmodeS ADDNS:DLIPDQ/UkrsyNDTmodeS ADDNS:DLIPDQ/UkrsyNDTmode ADDNS:DLIPDQ/UkrsyNDTModes ADDNS:DLIPDQ/UkrsyNDTmode ADDNS:DLIPDQ/UkrsyNDTModes ADDNS:DLIPDQ/UkrsyNDTmode ADDNS:DLIPDQ/UkrsyNDTmode ADDNS:DLIPDQ/UkrsyNDTmode ADDNS:DLIPDQ/UkrsyNDTmode ADDNS:DLIPDQ/UkrsyNDTmode ADDNS:DLIPDQ/UkrsyNDTmode ADDNS:DLIPDQ/UkrsyNDTmode ADDNS:DLIPDQ/UkrsyNDTmode ADDNS:DLIPDQ/UkrsyNDTm	D ₂
		× 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**.

cisco Identity Services Engine	Home > Co	mtext Visibility	Operations	▼ Policy	Administration	Work Centers		License Warning 🔺	Q,	
Policy Sets Profiling Posture C	lient Provisioning	→ Policy Elements					Click have to do wirely	are ratio and visibility a	the Da	
Dictionaries + Conditions + Resul	ts						CACK HERE TO DO WITCH	ess serup and visionity s	nup bu i	104.5
0	Allowed Dealers	als Consistent Links D	afault Natural	Access						
Authentication	Allowed Proto	otocols	CIAUL NELWORK	AUUCSS :						
Authorization	Name	Default Network A	coess							
	Description	Default Allowed Pr	otocol Service		1					
Profiling										
Posture	 Allowed Pr 	otocols								
Client Provisioning	Auth	antiantion Bunner								
		Process Host Looku	p (7)							
	Auth	entication Protocol	Is							
		Allow PAP/ASCII								
		Allow CHAP								
	•	Allow MS-CHAPv1			R					
		Allow MS-CHAPv2								
		Allow EAP-MD5								
	- 🗹	Allow EAP-TLS								
		Allow Authors	tination of avaira	d cortificator	to allow continents rore	aual in Authorization	n Bolieu (7)			
			inclusion of expire	o constituites	o anon continuate rei		ar only the			

- 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 E	Engine Home I	Context Visibility	Operations Policy	Administration	• Work Centers		License Warning 🔺	
Policy Sets Profiling P	osture Client Provisionir	ng Policy Elements				Click here to do wirele	ess setup and visibility setup	Do not
Policy Sets → Defau	It							R
Status Policy	Set Name	Description	Conditions				Allowed Protocols / Se	rver Se
Search								
Default		Default policy set					Default Network Access	: 28
+ Status Rule	Name	Conditions				Use		
Search				27.24.5				
				+		AD-DNS	,	-
/ 🥑 Defau	1					> Optio	ns	
	Local Exceptions							

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.

			Context v	soury F Operations	• Policy	 Administration 	• work Geneers		•	License warning	•	- - -
Policy Sets	Profil	ing Posture Client Provisionin	ng 🕨 Poli	cy Elements				Click he	re to do wirele	ss setup and visibility	setup	Do no
> Authen	ntication	Policy (1)										
> Authori	ization F	Policy - Local Exceptions										
> Author	ization F	Policy - Global Exceptions										
✓ Author	ization F	Policy (2)										
+						Results						
	Status	Rule Name	Condit	lons		Profiles			Security G	roups		
Search								12.000				_
	0	Basic_Authenticated_Access		machineuserauth		× Cisco_Temp	oral_Onboard	+	Guests		• •	+
	0	Default				× Cisco_Temp	oral_Onboard	+	Unknown			+
								-				_
												0

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, click Browse and select another folder. Click Install to start the installation.
	Destination Folder
	Space required: 105 MB Space available: 64 GB
	By dicking 'Install' below, you verify that you have read and Scent the Subscription Agreement
	et aller a freeze and the relation of the reading Machanic Topper haut we control
	[Install] Cancel
ا 5 ر	lick Install
J. [Cisco AMP for Endpoints Connector Setup
	Installation Complete
	Setup was completed successfully.
	Cisco AMP for Endpoints Connector has completed
	Chaw datails
	Snow <u>d</u> etails
	R
	< 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 in different folder, click Browse and select another folder. Click Install to start the	istall in a installation.	
Destination Folder		
C:\Program Files\Cisco\AMP Browse		
Space required: 105 MB		
Space available: 3 GB		
By dicking ' <u>I</u> nstall' below, you verify that you have read and accept the <u>Subscri</u> j	otion Agree	<u>ment</u>
[Vistal]	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	<u>\</u>	
			μ	5	
	< <u>B</u> ack	Ne	xt >	Car	icel
Click Novt	< <u>B</u> ack	Ne	xt >	Car	icel
Click Next.	< <u>B</u> ack	Ne	xt>	Car	icel
Click Next.	< <u>B</u> ack	Ne	xt >	Car	icel
Click Next. Clicc AMP for Endpoints Connector Setup	< <u>B</u> ack	Ne	xt >	Car	ncel
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed	< <u>B</u> ack	Ne	xt >	Car	icel
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options	< <u>B</u> ack	Ne	-	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< <u>Back</u>	Ne	xt >	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< <u>B</u> ack	Ne	-	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< <u>B</u> ack	Ne	-	Car	icel (
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< <u>B</u> ack	Ne	xt>	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< <u>Back</u>	Ne	xt>	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< Back		-	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< Back		xt>	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< Back		xt>	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< Back		xt>	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< Back		xt >	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< Back		xt>	Car	
Click Next. Cisco AMP for Endpoints Connector Setup Installation Completed Please choose final installation options Create Desktop Shortcut	< Back		xt>	Car	

7. Click Close.

2.12.4 Scanning using AMP

1. If the AMP software does not run automatically, open it from the **start** menu.



- 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

285

2. 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

earcn	4		+ New Policy
All Products Windows Android	Mac Linux iOS		- Henrong
Audit This policy puts the AM	/P for Endpoints Connector in a mode t	hat 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	ints Connector in 🔮 1 🛛 📮 0
🗄 📲 Blocking Policy. All detections	are set to BLOCK. This is the standard	policy for the AMP for Endpoints Connect	tor that will quara 🖀 1 🛛 🖵 0
🖯 📲 Domain Controller This is a l	ightweight policy for use on Active Dire	ctory Domain Controllers.	i 1 📮 2
Modes and Engines	Exclusions	Proxy	Groups
Files Audit Network Disabled Malicious Activity Prote Disabled System Process Protection Protect	 Altiris by Symantec AVAST Avira Diebold Warsaw 	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	Not Configured
O View Changes Modified 2019-	05-20 14:56:48 UTC Serial Number	54 🕹 Download XML	C Duplicate C Edit 🖻 Delete
Protect This is the standard	policy for the AMP for Endpoints Conne	ctor that will quarantine malicious files an	id block malicious 🕍 1 🛛 🖵 0
🗄 📲 Server This is a lightweight p	policy for high availability computers an	d servers that require maximum performa	ance and uptime. 🏼 🖉 1 🛛 🖵 0
1 - 8 of 8 total records	25 A / page 4 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.	
Modes and Engines	Conviction I	Modes			Recommended Settings
Exclusions 20 exclusion sets	These settings con files and network a	trol how AMP fo ctivity.	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		Server Files: Quarantine
Product Updates	Malicious Activity P	rotection			Network: Disabled Malicious Activity Protection: Disabled
Advanced Settings	Quarantine	Block	Audit	Disabled	System Process Protection: Disabled
	Protect	Audit	Disabled		
	Detection E	ngines			
	🗹 TETRA 🚯				
	🖉 Exploit Preventi	on 🕚			
					Ŕ
					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:		
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>< ОК ></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.

Enter the FlowReplicator f	dministrative IP Bro	adcast Address	1
192.168.1.255_			
		`	

- 15. Press Enter.
- 16. Highlight Yes.



- 17. Press Enter.
- 18. Highlight OK.

rimary network parame	ters have been modified. I	lease note that
etwork access to this epair. This system wi	system which will require Il now be restarted to imp	console access to lement these changes.
	< 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 Manage Change the passuo Change the Truste Advanced Operatio	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:	
Hanager Passuo Truste Advance	hent Change the Management Port Network rd Change the password for the current user Hosts Change the Trusted Hosts Advanced Operations
	<pre></pre>
At the prompt type in your of	current password. Then type your new password at the next two prompts.
Changing password for sysad (current) UNIX password:	nin.

- 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	ct one: Management Change the Management Port Network
<pre> Select> < Exit > </pre>		PasswordChange the password for the current userTrustedHostsChange the Trusted HostsAdvancedAdvanced Operations
		<pre></pre>
	anging password urrent) UNIX pa µ password: type new passwo	for sysadmin. ssword: rd:

- 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:[°]# passwd root New password: Retype new password: passwd: password updated successfully smc-01:^{°°}#

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	ise Sensitive)		
Step 3: Host Name and Domains	Must be different	from the previous password by at least	4 characters.	
Step 4: DNS Settings	Note: You must cha	ange the password for all th	e users before continuin	g.
Step 5: NTP Settings	Current Bossword	T ADMIN		
Aeview:	Current Password:		Required	
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	Enable communication be below. Before changing an	tween this appliance and iy of these settings, conf	t the network. Default network fer with your network administra	settings for this appliance appear ator.
Step 3: Host Name and Domains	Warning! If you change y replaced automatically. If these fields so you don't l	our IP address, host nan you have a custom certi lose data.	ne, or network domain name, th 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	Warning! If you change yo replaced automatically. If these fields so you don't lo	our IP address, host name, or network domair you have a custom certificate, save the certifi ose data.	name, the appliance identity certificate is cate and private key before you change
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	
	- 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	Enter the IP the correspo	address(es) of your domain name server(s). To and then click the - builton.	add a server, click the + button. To delete a server, select
Step 3: Host Name and Domains	Delete	DNS Server	
Step 4: DNS Settings			
L 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		Select or en server(s) us click the + b	ter the IP address(es) or n ed for other devices that fe utton. To delete a server, s	ame(s) of your network time proto ed information to the StealthWatc elect the corresponding checkbox	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					
					•
		H Back			Next 🔿

- 12. Click Next.
- 13. Select Restart.

1	Step 1. Change Default Password	R	teview Your S	Settings			
	Step 2		Management Networ	k Interface	Host Name and Doma	lins	- EGH
50	Step 3: Nost Name and Domains		Nome: MAC Address: IP Address: Subnet Mask: Default Gateway: Froadcast Address:	eth0 00:50:56:b2:64:52 192:168:1.52 255:255:255:0 192:168:1.1 192:168:1:255	Host Name: Network Domain:	senc-01 di.ipdr	
A	Step 4: DNS Settings		IPv6 Address: IPv6 Prefix Length: IPv6 Gateway:				
			DNS Settings		NTP Settings		e Edit
	NTP Settings					10.97.74.8	
~	Review. Review Your Settings				Finalize	O Restart	Shut Do
			- Back			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:	Control Management Settings
Change Default Password	Central Management Settings
Step 2:	
	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
Sten 4 [.]	
DNS Settings	
Step 5:	
VIP Settings	
Step 6: Central Management	
1 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	must enter /.
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		0 0
😑 🔞 Security Analy	ytics 🕒 🕒 🕘 🕘 📃 🛈	P (Э
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 Request		
	Upload License File		
	Use this section if your appliance does not have access to the Internet. Click Download DS Seed and save dsseed taz to your workstation. Go to <i>license soleranetworks.com</i> and follow the instructions. Return to this		
	page, click Browse to retrieve <i>license.tgz</i> , and then click Update. After the license is uploaded, the appliance will		
	be rebooted automatically.		
	License Elle Browne		
	LIVE IV		
	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.**

12. 10.0 ml hybers: 12. 00 ml hybers: 12. 00 ml hybers: 12. 00 ml hybers: 13. 00 ml hyber	ummary												Account Set	Elingi
and bit bit <th>E 1.00 G8 System (50 60 33 35 Ho</th> <th>Uptime: 27 days 22-4</th> <th>Phours</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>Risk and Vis Encoder/De Log Out</th> <th>code</th>	E 1.00 G8 System (50 60 33 35 Ho	Uptime: 27 days 22-4	Phours										Risk and Vis Encoder/De Log Out	code
2 2 2 100 3 3 3 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	51 25.61 Mb													-
30 11.31 M0 30 12.34 M0 31.31 M0 32 3.54 M0 32 3.54 M0 34 10.400 35.4 M0 10.400 35.4 M0 10.400 32.34 3.440 34 10.400 35.4 M0 10.400 35.	45 45 13.07 Mb													
No. No. <td>14.31 Mb</td> <td></td>	14.31 Mb													
B B	20 9 54 10											1		
22 Jul S. Aug 18 Aug 3. Sag 16 Aug 19 Sag M. Out 28 Out 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 25 Nov 9 Out 21 Dat 6 MAC Out 00 11 Nov 12 Dat 6 MAC Out 00	9,54 Mb 9,54 Mb	My MWM	Million Million	M.WWWWW	Working the	WWW WWW	an a	waterstern	MWMMUU	Muumhu		MAMMAN	rthr	+
22 July 5 Aug 19 Aug 1 Sup 16 Sup 16 Sup 16 Sup 16 Aug 18 Sup 6 Sup 18 Sup <th1< td=""><td>20 9.54 Mb 10 4.77 Mb 1 0 0 b</td><td>MAN AWA</td><td>Miller Mythewet 5. Aug</td><td>M.WWWWWW</td><td>2 5mp</td><td>16.500</td><td>00.500 14.000 14.000</td><td>Wid Wide 28 Oct</td><td>MW/WUUU 11. You</td><td>MuuMu 25. Nov</td><td>5. Dec</td><td>NAMANA M</td><td>rthrd 6 jan</td><td>ł</td></th1<>	20 9.54 Mb 10 4.77 Mb 1 0 0 b	MAN AWA	Miller Mythewet 5. Aug	M.WWWWWW	2 5mp	16.500	00.500 14.000 14.000	Wid Wide 28 Oct	MW/WUUU 11. You	MuuMu 25. Nov	5. Dec	NAMANA M	rthrd 6 jan	ł
lose (NaCaylung) Sel Cayl All Cognet	9,54 Mb 9,54 Mb 11 4.77 Mb	MAN AWM	MMW MMWM	M.W.W.W.M.M.	WWWWWWWW 2. Sno	16. Sep	ч <mark>үү-үүүүүүүүүүүү</mark> үүү 39.549 14.00	and the funder	MAN'W ULUU	MuuMu 25. Nov	5 Dec	25. Dec	1411 6 jun	H
Info National Info National Nation differee National	24 9.54 Mb 52 17 4.77 Mb 1 5 0.0 22 Jul	M/W/ /W/W 22 Jul 5. Aug	5. Aug 19. Aug	79 Aug 2. Sep	2. Sep 14. Sep	10 Sep	(ชีพูศัพท์)เหล่ายไม่ได้ 22.569 14.0a 14.0a	28. Oct	11. New	25. Nov 25. Nov 25. Nov	9. Dec 9. Cec	25. Dec 23. Dec	nth-nt 6 jan 96 ja	ł
Option These Captured Preset States These	22 3.54 Mb 25 10 4.77 Mb 1 5 0.0 22 Jul 2008	5. Aug	S Aug 19 Aug	2. Sap	2. Sep 4. 14. Sep	16.5ep 30 [°] Sep	20.549 14.00 10.549 14.00 14.04	28.0ct	11 Nov	25. hov 25. hov	9. Dec 9. Cec	ZE. Dec 23. Dec	E jan 6 jan 6 jan 6 jan	21
Current 2 - 11.4 Current Current Current Current	22 9.54 MD 32 13 4.77 MD 1 3 0.0 32 Jd 3000	5. Arg	M W WWW 5 Aug 19 Aug	75. Xug 75. Xug 3. Sep	2. Sep 2. Sep 14. Sep 1 Gave Linek	10.500 10.500	от _{МР} ПолуП _О ЛУМИ(МУ) 30. 5на 14. Ост 14. Ост Мот Сараница	28. Oct. 28. Oct.	11. Nov	25. hov 25. hov 26. how	9. Dec 9. Cex	25 Dec 25 Dec 25 Dec 25 Dec	Alfred 6 jan 6 jan 6 jan 8 jan	21
	9 9,54 Mb 9 19 4.77 Mb 1 0 0 0 12 Jul 100	S. Ang S. Ang Current Mass	N due normalise	Thinking	2. 5ep 4 16. 5ep 16. 5ep	16.5sp 30.5sp etc Current Mar	NAT A STATE AND	28 Oct 28 Oct	11. Nov 13. Nov	25. hey 25. hey 25. hey 26. hey Not C	9. Dec 9. Cet Concest	25. Dec 23. Dec 23. Dec 23. Dec 23. Dec 23. Dec 23. Dec 23. Dec	6 jan 6 jan 6 jar 8 jar	

12. Click Change Password.



13. Enter a new password. Click Save.

Capture	× +											
-> C A Not	secure ds2b7a/ca	aptures/index										☆ 0
= 💿 Secu	rity Analytics									0	00_	0 A 0
energy .												
1.00 G8 System Lz	stime 27 days 72 51	hours										Udu * Amon 10
10 21.01.00												
21.94.90			1	Account Settings					×			
19,07349				Current Par	seword .				R			
14.11-04				New Pasov	vord	41						
- 10				Confirm Pa	anword	-1						
							Curco					
4.37300 1	and in hamage	wanter Manual Manual And	WWWWWW	Time Suffa	120				human		King Marker	that
	TL Jul	5 Aug	19 440				G	ancel Save	85. bus	S.Dec.	23 Der	5.341
				1								
22 [°] ju	5.04	18 Aug	Lier	18 tap	bit Sap		23.04	it. Name	TT These	a Dec	IS Dec	8. jar
												_
	-				PT1			-			Concepter State	BBAY Capture on A
	401	_		T GO/H LAN			THE LOCK				The second	
		Not Capture				Not Connected			Notice	omected		
			_									

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	× +	_ _ X
\leftrightarrow \rightarrow	C A Not secure	https://192.168.1.42	☆ 🖯 🔾
6	Capture	lytics 🛛 🔍 🔍 🗖	P 0
	Statistics	bing all reports and extractions. Drive / is 100% full. Metric=bytes, Threshold=90	
\$	Settings	Little data in the second state	
	 Authentication 	and the second	
	• Central Management)	
	Communication		
	• Data Enrichment		
	• Date/Time		
	Geolocation		
	• Metadata	There are no alerts to display.	
	• Network		
	· Security	Set Up kulles for Alerts Go to Summary Page	
	• System		
	• Upgrade		
4	• Users and Groups	• Activate Wind	ows

16. Navigate to **Settings > Data Enrichment.**

> C A Not	secure https://	192.168.1.42/integration_providers/index	÷ A
= 🛞 Secu	rity Analytic	s 0 0 _ 1	P 0
	Stopping	all reports and extractions. Drive / is 100% full. Metric=bytes, Threshold=90	
Data Enrichment			
Symantec Intelligence Service	IS		
Name	Licensed	Data Enrichment Filters	Actions
symantec Web Reputation Service	Yes	-na-	↔ 0
lymantec File Reputation Serv	<mark>vi</mark> ce Yes	Archives, Binaries, Deblan Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDF	° ∕ → 0
Data Enrichment Profiles	a applysic and data o	prickmonette graphic and then all di 'Sturd'	
Data Enrichment Profiles Select the amount of indexing Profile	ıg, analysis, and data e	enrichment to enable and then click Save. Full Data Enrichment (No Anomaly Detection)	
Data Enrichment Profiles Select the amount of indexing Profile Symantec Analysis Providers	ıg, analysis, and data e	enrichment to enable and then click Save. Full Data Enrichment (No Anomaly Detection) *	
Data Enrichment Profiles Select the amount of indexiny <u>Profile</u> Symantec Analysis Providers Name	g, analysis, and data e	enrichment to enable and then click Save. Full Data Enrichment (No Anomaly Detection) Data Enrichment Filters	Actions
Data Enrichment Profiles Select the amount of indexin <u>Profile</u> Symantec Analysis Providers Name	ıg, analysis, and data e	enrichment to enable and then click Save. Full Data Enrichment (No Anomaly Detection) Data Enrichment Filters Default filters	Actions ho i 0
Data Enrichment Profiles Select the amount of indexing <u>Profile</u> Symantec Analysis Providers Name CAP Talware Analysis Appliance	ig, analysis, and data e	enrichment to enable and then click 'Save'. Full Data Enrichment (No Anomaly Detection) Data Enrichment Filters Default filters Archives, Debian Packages, Office Documents, Programs and Libraries, Adobe PDF	Actions • • • • • • • • •
Data Enrichment Profiles Select the amount of indexing <u>Profile</u> Symantec Analysis Providers Name CAP Talware Analysis Appliance Symantec On Demand Provide	g, analysis, and data e	enrichment to enable and then click Save'. Full Data Enrichment (No Anomaly Detection) Data Enrichment Filters Default filters Archives, Debian Packages, Office Documents, Programs and Libraries, Adobe PDF	Actions () / () () / ()
Data Einfolment Profiles Select the amount of indexing <u>Profile</u> Symantee Analysis Providers Name CAP Alware Analysis Appliance Symantee On-Demand Provide Name	g, analysis, and data e	enrichment to enable and then click 'Save'. Full Data Enrichment (No Anomaly Detection) Data Enrichment Filters Default filters Archives, Debian Packages, Office Documents, Programs and Libraries, Adobe PDF Data Enrichment Filters	Actions Q 2 3 Q 2 3 Actions

17. Click the red upside-down power symbols next to **Symantec Web Reputation Service** and **Symantec File Reputation Service** to turn them on.

= 🔞 Securit	ty Analytic	cs 🛛 0 0 🛄 🚺	🥐 ө
	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	-18-	0 + 0
			C
Symantec File Reputation Service	e Yes	Archives, Binaries, Debian Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDF	/ + 6
Symantec File Reputation Service	Yes	Archives, Binanes, Debian Packages, Office Documents, Programs and Libranes, JAR Archives, Adobe PDP	/*0
Symantec File Reputation Service Data Enrichment Profiles Select the amount of indexing, a Profile	Yes analysis, and data e	Archives, Binaries, Debian Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDF enrichment to enable and then click 'Save'. Full Data Enrichment with Anomaly Detection *	/ + 0
Symantec File Reputation Service Data Enrichment Profiles Select the amount of indexing, a <u>Profile</u> Symantec Analysis Providers	e Yes analysis, and data e	Archives, Binaries, Debian Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDF enrichment to enable and then click 'Save'. Full Data Enrichment with Anomaly Detection *	/ * 6
Symantec File Reputation Service Data Enrichment Profiles Select the amount of Indexing, a <u>Profile</u> Symantec Analysis Providers Name	e Yes	Archives, Binaries, Debian Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDF enrichment to enable and then click Save: Full Data Enrichment with Anomaly Detection Data Enrichment Filters	/ → C Actions
Symantec File Reputation Service Data Enrichment Profiles Select the amount of indexing, a <u>Profile</u> Symantec Analysis Providers Name CAP	e Yes	Archives, Binaries, Debian Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDP enrichment to enable and then click 'Save'. Full Data Enrichment with Anomaly Detection Data Enrichment Filters Default filters	/ → € Actions ♀ / €
Symantec File Reputation Service Data Enrichment Profiles Select the amount of Indexing, a Profile Symantec Analysis Providers Name CAP Malware Analysis Appliance	e Yes	Archives, Binaries, Debian Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDF enrichment to enable and then click 'Save'. Full Data Enrichment with Anomaly Detection Data Enrichment Filters Default filters Archives, Debian Packages, Office Documents, Programs and Libraries, Adobe PDF	/ → 0 Actions
symantec File Reputation Service Data Enrichment Profiles Select the amount of Indexing, a <u>Profile</u> Symantec Analysis Providers Name CAP Melware Analysis Appliance Symantec On Demand Providers	 Yes 	Archives, Binaries, Debian Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDF enrichment to enable and then click 'Save'. Full Dala Enrichment with Anomaly Detection Data Enrichment Filters Default filters Archives, Debian Packages, Office Documents, Programs and Libraries, Adobe PDF	/ → € Actions
Symantec File Reputation Service Data Enrichment Profiles Select the amount of Indexing, a Profile Symantec Analysis Providers Name CAP Malware Analysis Appliance Symantec On Demand Providers Name	 Yes analysis, and data e 	Archives, Binaries, Debian Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDF enrichment to enable and then click 'Save'. Full Data Enrichment with Anomaly Detection Data Enrichment Filters Default filters Archives, Debian Packages, Office Documents, Programs and Libraries, Adobe PDF Data Enrichment Filters	/ → € Actions

18. Select Full Data Enrichment (with Anomaly Protection) for the profile under Data Enrichment Profiles.

	192.108.1.42/integration_providers/index	ж
Security Analytic	cs 📀 📀 💽 🚺	P (
Stopping	all reports and extractions. Drive / is 100% full. Metric=bytes, Threshold=90	
C Office Documents		
Lonin Completion Service		
Download Version 1.1.2 of the Login Correlation Se	ervice 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		
Enable Custom Update Location		
Enable Custom Update Location YARA File Manager Download the current YARA file	UT Download	
Enable Custom Update Location VARA File Manager Download the current YARA file Upload a local YARA file	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	rtics			00	0 🖊 (
	Stoppi	ing all reports and extr	actions. Drive	e / is 100% full. Me	tric=bytes, Threshold=90	0
			No Data A	vailable		
14. [Dec Dec-14 12:00 1	5. Dec Dec-15 12:00 1	6. Dec Dec-16	512:00 17. Dec E	ec-17 12:00 18. Dec Dec	-18 12:00 19. Dec
aces			Not Captu	ring		Start Capture on
	eth1		No Link	eth2		No Link
		Captured	Filtered		Captured	Filtered
	Current	Not Connected		Current	Not Connected	
	Current	Not Connected	0 b/s	Current	Not Connected	0 b/s
	Current Max Total	Not Connected /s	0 b/s 0 B	Current Max Total	Not Connected	0 b/s 0 B
	Current Max Total Start Playback	Not Connected	0 b/s 0 B Capture	Current Max Total Start Playback	Not Connected	0 b/s 0 B Capture
	Current Max Total Start Playback eth3	Not Connected	0 b/s 0 B Capture No Link	Current Max Total Start Playback etb4	Not Connected	0 b/s 0 B Capture No Link
	Current Max Total Start Playback eth3	Not Connected 0 B Start C Captured	0 b/s 0 B Capture No Link Filtered	Current Max Total Start Playback eth4	Not Connected 0 B Start Captured	0 b/s 0 B Capture No Link Filtered
	Current Max Total Start Playback eth3 Current	Not Connected	0 b/s 0 B Capture No Link Filtered	Current Max Total Start Playback eth4 Current	Not Connected	0 b/s 0 B Capture No Link Filtered

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	Wew SQL Server stand-alone installation or add features to an existing installation	^
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.	
Maintenance	The second secon	
Tools	Install SQL Server Reporting Services	
Resources	An internet connection is required to install SSRS.	
Advanced	Install SQL Server Management Tools	
Options	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.	ļ
	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 SOL Server 2017	New Machine Learning Server (Standalone) installation	
ind oboit one offer con	Launch a wizard to install Machine Learning Server (Standalone) on a Windows machine. This is twinically 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 Rules Feature Rules Feature Rules Feature Configuration Rules	Validate this instant. Validate this instance of SQL Server 2017 by entering the 25-charac of authenticity or product packaging. You can also specify a free et Evaluation, or Express. Evaluation has the largest set of SQL Server Books Online, and is activated with a 160-day expiration. Developer has the same set of features found in Evaluation, but is licensed for development only. To upgrade from one installed edition to anothe Specify a free edition: Evaluation © Enter the product key:	ter key from the Microsoft certificate intion of SQL Server: Developer, features, as documented in SQL Server redition does not have an expiration, non-production database application ar, run the Edition Upgrade Wizard.
Ready to Install Installation Progress Complete		

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 License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Feature Relection 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 Corporating you live, one of its affiliates) and you. Please read them. They apply above, which includes the media on which you received it, if any. The any Microsoft • updates. • supplements. • Internet-based services, and I accept the licetize terms. SQL Server 2017 transmits information about your installation experience, as a proformance data, to Microsoft to leps improve the product. To learn more at processing and privacy controls, please see the <u>Privacy Statement</u> .	on (or base to the soft e terms also well as other bout SQL Ser	d on whe ware nam o apply to cap Sopy usage and wer 2017 o	ere led o

7. Click Next.



can continue.	incorens uner might occu	a while forming setup, railores most be t	conected denote setup				
Product Key License Terms Global Rules	Operation completed. Passed: 3. Failed 0. Warning 1. Skipped 0.						
Product Updates Install Setup Files	View detailed report			Dentil			
Install Rules	Rule	Rule		Status			
Feature Selection	Fusion Active Ter	Fusion Active Template Library (ATL)		Passed			
Feature Rules	Consistency valid	Consistency validation for SQL Server registry keys		Passed			
Feature Configuration Rules	Computer domai	Computer domain controller		Passed			
Ready to Install	🗘 Windows Firewall		Warning				
Complete			De .				

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.

Instance Configuratio	n e ID for the instance of	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 Server 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 Instal]ed 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	
Specify the service accounts an	nd collation configuration.					
---	--	---	--	------------------------------------	---	
Product Key License Terms Global Rules	Service Accounts Collation	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	~	
Feature Selection	SQL Server Launchpad	NT Service\MSSQLLaun		Automatic		
Feature Rules Instance Configuration Server Configuration Database Engine Configuration Analysis Services Configuration Consent to install Microsoft R Feature Configuration Rules Ready to Install Installation Progress Complete	SQL Server Browser	NT AUTHORITY\LOCAL		Automatic	Y	
	Grant Perform Volume Mainte This privilege enables instant to information disclosure by a <u>Click here for details</u>	nance Task privilege to SQL Sen file initialization by avoiding zerc llowing deleted content to be ac	ver Database En bing of data pag cessed.	gine Service ges. This may lead	ł	

- 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 Slobal Rules Microsoft Update Product Updates nstall Setup Files nstall Rules Feature Selection Feature Rules nstance Configuration Database Engine Configuration	Server Configuration Specify the authent Authentication Moo Windows authen Mixed Mode (SQ Specify the password: Enter password: Cgnfirm password: Specify SQL Server a	Data Directories TempDB FILEST ication mode and administrators for de tication mode IL Server authentication and Window rd for the SQL Server system administ executions	REAM the Database Engine s authentication) trator (sa) account.	5
Analysis Services Configuration Consent to install Microsoft R Feature Configuration Rules Ready to Install Installation Progress Complete	DIVAdministrator (A DIVAdministrator2 (Add <u>C</u> urrent User	Administrator) (Admin2) (Add		SQL Server administrators have unrestricted access to 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 Setup Files Install Rules Installation Type Product Key	Server Configuration Data Directories Server Mode:	is Services.
Installation Type Product Key License Terms Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Database Engine Configuration Consent to install Microsoft R Feature Configuration Rules	(D/Administrator (Administrator) D/Administrator2 (Admin2)	Analysis Services administrators have unrestricted access Analysis Services.
Installation Progress	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.

Download and install necessary	y pre-requisite.		
Product Key	Microsoft R Open is an enhanced distribution of R made available by Microsoft under the GNU General		
License Terms	Public License v2.		
Global Rules			
Microsoft Update			
Product Updates	R is © the R Foundation for Statistical Computing. For more information on R-related products and service		
Install Setup Files	visit http://r-project.org.		
Install Rules			
Feature Selection	By clicking "Accept" you are choosing to download Microsoft P Open and install it on your machine, and		
Feature Rules	agreeing to accept patches and updates to this software according to your SQL Server update preferences.		
Instance Configuration			
Server Configuration			
B			
Database Engine Configuration			
Analysis Services Configuration			
Analysis Services Configuration Consent to install Microsoft R			
Database Engine Configuration Analysis Services Configuration Consent to install Microsoft R Feature Configuration Rules			
Database Engine Configuration Analysis Services Configuration Consent to install Microsoft R Feature Configuration Rules Ready to Install			
Database Engine Configuration Analysis Services Configuration Consent to install Microsoft R Feature Configuration Rules Ready to Install Installation Progress			

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

en anticipation de la companya de la		
Ready to Install		
Verify the SQL Server 2017 fea	tures to be installed.	
Product Key	Bandy to Jactoll 501 Concer 2017	
Inducting 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	Neady to Initial Sci. Server EV11	
Consent to install Microsoft R Feature Configuration Rules	 - R - Analysis Services - Machine Learning Server (Standalone) 	
Ready to Install	<	>
Installation Progress	Configuration file path:	
Complete	C/(Brogram Eiler) Microsoft SOI, Senier) 14/1 Setup Bootstrap) Loo) 20190906 060940 Configuratio	onFile ini
		ALL US ALL
		Course .

25. Click Install.

	SQL Server 2017 Setup		
Complete Your SQL Server 2017 installar	ion completed successfully with product updates.		
Product Key	Information about the Setup operation or possible	e next steps:	
License Terms	Feature	Status	
Global Rules	🖉 R	Succeeded	
Microsoft Update	Machine Learning Services (In-Database)	Succeeded	
Product Updates	Database Engine Services	Succeeded	
Install Setup Files	Analysis Services	Succeeded	
Install Rules	SQL Browser	Succeeded	
	SOL Writer	Succeeded	
Feature Selection			
Feature Rules		N	
Instance Configuration	Details:	24	
Server Configuration	Install successful.		
Database Engine Configuration			
Analysis Services Configuration			
Concept to install Missoroft P			
Consent to install Microsoft K			
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\Setus	Bootstrap\Log\20190806_060849\Summ	ary symant
	ica 20190806 060849.txt		2.2
			-
			Close

26. Click Close.

2.15.2 Install Windows Services

1. Open Server Manager.

er • Dashboard	• ② 🏴 Manage Tools y	/iew <u>H</u> elp
COME TO SERVER MAN	IGER	
1		
	Configure this local server	
K START	2 Add roles and features	
	Add other servers to manage	
T'S NEW	4 Create a server group	
	5 Connect this server to cloud services	
N MORE		Hide
	V MORE	Add roles and features Add other servers to manage Add other servers to manage Create a server group Source this server to cloud services Add server groups Source server group Sou

2. Click Add Roles and Features.



Select destination	on server	DESTINATIO symantec-
Refore Vou Begin	Select a server or a virtual hard disk on which to install roles and fe	atures.
Installation Type Server Selection	Select a server from the server pool Select a virtual hard disk	
Server Roles	Server Pool	
Features Confirmation	Filter	
	Name IP Address Operating System	
	symantec-ica.DLIPDR 192.168.1.83 Microsoft Window	s Server 2012 R2 Standard
	1 Computer(s) found This page shows servers that are running Windows Server 2012, an Add Servers command in Server Manager. Offline servers and newly collection is still incomplete are not shown.	d that have been added by y-added servers from which
	conection is a un incomprete are not shown.	Q
	< <u>Previous</u> <u>Next</u> >	nstall
ICK INEXL.	Add Roles and Features Wizard	_
Select server ro	Add Roles and Features Wizard	DESTINATIC
Select server ro Before You Begin Installation Type	Add Roles and Features Wizard	DESTINATION Symantec
Select server ro Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and Features Wizard Select one or more roles to install on the selected server. Roles Application Server DHCP Server DNS Server Fax Server M File and Storage Services (1 of 12 installed)	Description Web Server (IIS) provides a manageable and scalable to application infrastructure.
Select server ro Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and Features Wizard Select one or more roles to install on the selected server. Roles Application Server DHCP Server DHS Server Fax Server Image: File and Storage Services (1 of 12 installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services	DESTINATIC symantec- Description Web Server (IIS) provides a manageable, and scalable V application infrastructure.

6. Select Web Server (IIS).

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



7. Click Add Features.

Before You Begin Installation Type	Select one or more roles to install on the selected server. Roles	Description
Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Application Server DHCP Server DHCP Server Fax Server Fax Server Fax Server Fax Server Fain and Storage Services (1 of 12 installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Access Volume Activation Services Volume Activation Services Vindows Deployment Services Windows Server Essentials Experience 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.DI.IPDI
Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS)	Web servers are computers that let you share information ow extranets. The Web Server role includes Internet Information : diagnostic and administration, a unified Web platform that in Communication Foundation. Things to note: • Using Windows System Resource Manager (WSRM) can he server traffic, especially when there are multiple roles on th	er the Internet, or through intranets and Services (IIS) 8.5 with enhanced security, tegrates IIS 8.5, ASP.NET, and Windows IIp ensure equitable servicing of Web is computer.
Role Services Confirmation Results	 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 	es the installation of role services that ions (such as default documents and HTT c ontent compression.
	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 servic	Ces Select the role services to install for Web Server (IIS)	DESTINATION SERVE symantec-ica.DUPDI
berore rou begin Installation Type Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Role services	Description Application Development provides infrastructure for developing and hosting Web applications. Use these 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 s	ISTINATION SERVEI symantec-ica.DI.IPDI
	View installation progress	
	1 Feature installation	
	Installation succeeded on symantec-ica.DLIPDR.	
	.NET Framework 3.5 Features	1
	.NET Framework 3.5 (includes .NET 2.0 and 3.0)	
	.NET Framework 4.5 Features	
	ASPNET 4.5	
Results	HTTP Activation	
	Message Queuing (MSMQ) Activation	
	Named Pipe Activation	
	TCP Activation	
	Message Queuing	
	You can close this wizard without interrupting running tasks. View task progree gas again by clicking Notifications in the command bar, and then Task Detail Export configuration settings	ss or open this 5.

- 18. Click **Close** when the installation finishes.
- 19. Open Internet Information Services Manager.

<u>File</u> <u>View</u> <u>H</u> elp		
Connections Star Bage Star Page SYMANTEC-ICA (DI\Administ Application Pools b-	Filter: • • •	Actions Manage Server Restart Start Start Stop View Application Pools View Stes Change .NET Framework Version Get New Web Platform Components
	IIS Authentic Compression Default Document Browsing ISAPI Filters Logging MIME Types Modules MIME Types Modules MIME Types Modules MIME Types MIME Types MIM	nd v

- 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
				k	

23. Click Close.

9			Internet In	formation Services (IIS) Manag	er		- 5	x t
SYMANTEC-ICA	Sites						100 100 (*	a 10
File View Help								
Connections	Sites					Al	erts	
3 .• 🗟 2 8 ,	Sites					0	This site has multiple	
Start Page	Filter:	• 🔻 Go	- 🕞 Show A	II Group by: No Grouping •			bindings	-
Application Pools	Name *	ID	Status	Binding	Path	A	ctions	
D Sites	Default Web Site	1	Unknown (808:* (net.tcp), localhost (net.ms	%SystemDrive%\inetpub\wwwroot	•	Add Website Set Website Defaults	
							Edit Site Bindings Basic Settings	
						×	Explore Edit Permissions Remove Rename	
							View Applications View Virtual Directorie	es
						M 2 ->	anage Website Restart Start Do Stop	•
	N			m	,		Browse Website	
< 111 >	Features View	Content View					Browse *:8080 (http)	
Ready								6-

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.

9 (9) = A 💽 🖬	This PC Downloads SymanteclCASoftware_65			~ C	Search SymanteclCASoftware_
+ Favorites	Name	Date modified	Туре	Size	
Desktop	ADConnector.msi	4/19/2018 12:24 PM	Windows Installer	2,010 K	в
🐌 Downloads	BayDynamics.RiskFabric.IntegrationPack	6/29/2016 6:50 AM	Compressed (zipp	4 K	8
🐉 Recent places	BayDynamics.RiskFabric.IntegrationPack	11/20/2017 9:20 A	Compressed (zipp	6 K	в
	BayDynamics.RiskFabric.IntegrationPack	10/24/2016 9:26 A	Compressed (zipp	7 K	B
Mar This PC	SymanteclCAInstaller.exe	7/27/2018 10:26 A	Application	270,048 K	В
		R			

4. Run SymanteclCAInstaller.exe.

Risk	Fabric Installation Wizard		X
Risk Fabric [®]	Powered by Predictive Security Intelligen	ce <mark>(</mark> PSI™) En	igine
Welcome to the Risk Fabric Installer. This util the Risk Fabric Database and Website. Please	ity will guide you through the process of installi e select an option below to get started.	ng or upgrad	ing
Full Install	Database Utilities		
Select this to install Risk Fabric. You will also h option to install the database utilities.	ave the Select this if Risk Fabric is already install need to install the database utilities to t If you are not installing this on the serve	ed and you he SQL Server. er hosting SQL	
Lą.	Server, ensure you have access to a sha the server.	red drive on	
Start	Start		
License Activation	Uninstall		
Select this to install a license generated offline	e. Select this to uninstall Risk Fabric.		
Start	Start		1111

- 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	_ 🗆 X
Powered by Predictive Security Intelligence (P	'SI™) Engine
 8.2 Dickosure and Use. For so long as Owner's Confidential Information remains Confidential Information will (i) not disclose such Confidential Information (iii) not use any of the Confidential Information, using measures that Recipient takes to protect its own Confidential Information; and (iv) notify Owner Immediat Recipient discovers any unauthorized disclosure of such Confidential Information. 8.3 Obligations on Termination. On termination of the applicable Subscriptions, each party will disconting the other party's Confidential Information in Its possession and return or discroy, on the Owner's requiring last and copies of the other party's Confidential Information and return or discroy, on the Owner's requiring last and copies of the other party's Confidential Information and return or discroy, on the Owner's requiring last. 9.1 Restrictions. Bay Dynamics will take reasonable steps to protect the Security Data from unauthorized 9.2 Aggregated Data. Bay Dynamics may use, store and distribute the results of its analysis of the Security Data. 10 General. 10 General. 10 Goneral. 11 Gordentian Sale of Goods. The parties consent to personal purisdiction in the state of New York with regard to its clipate singulation of the Uniform Computer Information Transactions Act or the UN Convention the the Informational Sale of Goods. The parties consent on the analy prices with a subscripting and to the secure or any subscriptions in comection transfer of all or substantially all of Bay Dynamics assets. 10 Assignment. A party may not assign or otherwise transfer its rights or obligations under a Subscripting in complexis assets. 10 Asset Banee	, the Recipient in in it the same ely if le its use of uest, all disclosure. Data in an yber-attack holce-of-laws on Contracts on Contracts on Contracts on the sect to any on without the with a via hand y. No waiver sion. If a roid but all
$\boxed{\mathbf{V}}$ I have read, understood, and agree with the terms of the license agreement.	Print
	Next
	Risk Fabric Installation Wizard POWERED by Predictive Security Intelligence (P a.2 Disclosure and Use. For so long as Owner's Confidential Information remains Confidential Information will (i) not disclose such Confidential Information; (ii) not use any of the Confidential Information, other will (i) not disclose such Confidential Information; (iii) not use any of the Confidential Information, other measures that Recipient takes to protect its own Confidential Information; and (iv) notify Owner Immediat Recipient discovers any unauthorized disclosure of such Confidential Information. 8.3 Obligations on Termination. On termination of the applicable Subscriptions, each party will discontinu the other party's Confidential Information and certify that destruction. 9.3 Destingations. Buy Dynamics mill take reasonable steps to protect the Security Data from unauthorized 9.1 Restrictions. 9.1 Restrictions. Buy Dynamics will take reasonable steps to protect the Security Data from unauthorized 9.2 Aggregated Data. Bay Dynamics may use, store and distribute the results of its analysis of the Security 10.3 Governing Law. These T&C are governed by the laws of the State of New York without regard to its cl provisions of the application of the Uniform Compatter Information Transactions. Act or the UN Convextion 10.3 Governing Law. These T&C are governed by the laws of the State of New York without regard to its cl provisions or the application of the Uniform Compatter Information Transactions. Act or the UN Convextion 10.4 Susteinuol. Sile of Goods. The parties consent to previous professional Services. 10.3 Miscellancous. All notices hereunder must be in writing to the other party at its designated address disputes aring out of or related to these T&C, any Subscription. and/or any Professional Services. 10.3 Miscellancous. All notices hereunder must be in writing to the other party at its designated address delivery. Course, express delivery, or fascinille addeemed given the next busines day aft

5	Risk Fabric Installation Wizard		
Risk Fabric [®] 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	N	

9. Enter a username and password with privileges on the domain.

≥ .		Risk Fabric Installation Wizard				
Risk Fabric [®] Bay Dynamics [®]		Powe	ered by Predictive Security Intelligenc	e (PSI™) Engine		
	upgrade.					
Terms and Conditions	Website Name	RiskFabric		•		
Prerequisites						
Website	Port	80	Check Port			
Notifications	Website URL	Website URL http://symantec-ica.DI.IPDR:80/RiskFabric				
Data Sources	Installation Directo	rv Select a bas	se directory for the Risk Fabric server on the local r	machine A sub		
Database Utilities	folder 'RiskFabric' wil content of the Risk Fa	l be automatic abric Server ap	ally created in the base directory. It is the physical oplication in IIS.	path to the		
Integration warnings	Path	C:\Program	Files\Bay Dynamics\Risk Fabric Server Web	Browse		
	application pool in IIS automatically. The ac	S. The account count will also	will be granted sysadmin server role on the Risk F require elevated permissions to other systems su	abric SQL Server ich as		
	Domain\Username	DI\Administ	rator			
	Password		•••••			
	Fassword					
	Administrator Acco	unt Enter a W	indows Domain User name that will be granted ad	ministrator rights		
	Administrator Acco on the Risk Fabric Po Domain\Username	unt Enter a W irtal. DI\Administ	indows Domain User name that will be granted ad	ministrator rights		
	Administrator Acco on the Risk Fabric Po Domain\Username	unt Enter a W irtal. DI\Administ	indows Domain User name that will be granted ad	ministrator rights		

- 10. Click Next.
- 11. Configure any alert settings desired; these can be changed later.

Risk Fabric	Pov	vered by Predictive Security In	telligence (PSI™) Eng
Terms and Conditions Prerequisites Website	Notifications Configure setting Email Address' should be an em Enable Emails	below so that email notifications can be all address that is monitored.	sent. The 'From
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 Vulner It defaults to the main email add	ability summary emails will be sent from t ress entered above. ary Emails	his email address.
	Override From Email Addres	s	
	Scan Exclusions Scan exclusion defaults to the main email addre Enable Scan Exclusion Ema	related emails will be sent from this ema ess entered above. Is	Il address. It
	Override From Email Addres	5	
	Global False Positives Global fa	ilse positive emails will be sent using the	address in the

- 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.

ř.		Risk Fabric Installation Wizard		
Risk Fabric [.] Bay Dynamics		Powered by Predictive	e Security Intelligence	e (PSI™) Eng
Terms and Conditions	SQL Server Configu	ration		
Prerequisites	Server	SYMANTEC-ICA\ICA		Connec
Website	Database	RiskFabric	•	
Notifications		Niski done		
Data Sources	Analysis Services Co	onfiguration		
Database Utilities	Server	SYMANTEC-ICA\ICA		Connec
Integration Warnings	Database	RiskFabric	•	
License Activation				
Install	Default Domain D	omain to be used in case an integratio	in provides an account name	without a dom
	Domain			
			Ŀ\$	
			· · · ·	1.1.1
				Next
lick Next				Next
lick Next.		Rick Fabric Installation Wizard		Next
Click Next.		Risk Fabric Installation Wizard		Next
Click Next. ≥ <u>Risk Fabric</u> _{Bay Dynamics}		Risk Fabric Installation Wizard Powered by Predictive	e Security Intelligence	Next
Click Next. Risk Fabric: Bay Dynamics Terms and Conditions	Database Files Pie	Risk Fabric Installation Wizard Powered by Predictive ase select a directory for the database	e Security Intelligence utility files. Please note, this o	Next (PSI [™]) En directory must
Click Next. Risk Fabric: Bay Dynamics Terms and Conditions Prerequisites	Database Files Piles on the same server administrator and	Risk Fabric Installation Wizard Powered by Predictive Powered by Predictive ras the Risk Fabric SQL Server, If you d restart this Installer.	e Security Intelligence utility files. Please note, this io not have access, please cor	P (PSI [™]) Eng directory must ntact your syst
Click Next. Risk Fabric: Bay Dynamics Terms and Conditions Prerequisites Website	Database Files Pile on the same server administrator and I	Risk Fabric Installation Wizard Powered by Predictive ase select a directory for the database r as the Risk Fabric SQL Server, If you d restart this installer. we Utilities Now?	e Security Intelligence utility files. Please note, this to not have access, please cor	e (PSI™) Eng directory must ntact your syst
Click Next. Risk Fabric: Bay Dynamics Terms and Conditions Prerequisites Website Notifications	Database Files Ple on the same server administrator and i ✓ Install Databas	Risk Fabric Installation Wizard Powered by Predictive ase select a directory for the database as the Risk Fabric SQL Server. If you d restart this installer. we Utilities Now?	e Security Intelligence utility files. Please note, this o to not have access, please cor	e (PSI™) Eng directory must
Click Next. Risk Fabric: Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources	Database Files Ple on the same server administrator and i ✓ Install Databas	Risk Fabric Installation Wizard Powered by Predictive ase select a directory for the database as the Risk Fabric SQL Server. If you d restart this installer. as Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this o to not have access, please cor cs\Database Utilities\	e (PSI TM) Eng directory must ntact your syst
Click Next. Risk Fabric: Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Database Utilities	Database Files Ple on the same server administrator and I ✓ Install Databas	Risk Fabric Installation Wizard Powered by Predictive ase select a directory for the database as the Risk Fabric SQL Server. If you d restart this installer. the Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this o to not have access, please cor cs\Database Utilities\	e (PSI TM) Eng directory must ntact your syst
Click Next. Click Next. Risk Fabric: Bay Dynamics Terms and Conditions Prerequisites Website Notifications Data Sources Database Utilities Integration Warnings	Database Files Ple on the same server administrator and r Install Databas	Risk Fabric Installation Wizard Powered by Predictive asse select a directory for the database as the Risk Fabric SQL Server. If you d restart this installer. We Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this o to not have access, please cor cs\Database Utilities\	e (PSI TM) Eng directory must ntact your syst
Click Next. Click Next. Risk Fabric: Bay Dynamics Terms and Conditions Prerequisites Vebsite Notifications Data Sources Database Utilities Integration Warnings License Activation	Database Files Ple on the same server administrator and r ✓ Install Databas	Risk Fabric Installation Wizard Powered by Predictive asse select a directory for the database as the Risk Fabric SQL Server. If you d restart this installer. ie Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this o to not have access, please cor ccs\Database Utilities\	e (PSI™) Eng directory must ntact your syst
Click Next. Click Next. Risk Fabric: Bay Dynamics Prerequisites Vebsite Notifications Data Sources Database Utilities Integration Warnings License Activation Install	Database Files Ple on the same server administrator and r ✓ Install Databas	Risk Fabric Installation Wizard Powered by Predictive asseselect a directory for the database as the Risk Fabric SQL Server. If you d restart this installer. ie Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this o to not have access, please cor ccs\Database Utilities\	e (PSI™) En{ directory must ntact your syst
Click Next. Risk Fabric: Bay Dynamics Prerequisites Vebsite Notifications Data Sources Database Utilities Integration Warnings License Activation Install	Database Files Ple on the same server administrator and i ☑ Install Databas	Risk Fabric Installation Wizard Powered by Predictive asseselect a directory for the database as the Risk Fabric SQL Server. If you d restart this installer. ie Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this o to not have access, please cor ccs\Database Utilities\	e (PSI™) En{ directory must ntact your syst
Click Next. Risk Fabric: Bay Dynamics Prerequisites Vebsite Notifications Data Sources Database Utilities Integration Warnings License Activation Install	Database Files Ple on the same server administrator and i ✓ Install Databas	Risk Fabric Installation Wizard Powered by Predictive asseselect a directory for the database as the Risk Fabric SQL Server. If you d restart this installer. ie Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this o to not have access, please cor ccs\Database Utilities\	e (PSI TM) Eng directory must ntact your syste Browse
Click Next.	Database Files Ple on the same server administrator and i ☑ Install Databas	Risk Fabric Installation Wizard Powered by Predictive asseselect a directory for the database as the Risk Fabric SQL Server. If you d restart this installer. ie Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this o to not have access, please cor	e (PSI TM) Eng directory must ntact your syste Browse
Click Next.	Database Files Ple on the same server administrator and i ✓ Install Databas	Risk Fabric Installation Wizard Powered by Predictive tase select a directory for the database r as the Risk Fabric SQL Server. If you d restart this installer. ie Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this of o not have access, please cor ccs\Database Utilities\	e (PSI™) Eng directory must ttact your syste
Click Next.	Database Files Ple on the same server administrator and i ✓ Install Databas	Risk Fabric Installation Wizard Powered by Predictive tase select a directory for the database r as the Risk Fabric SQL Server, If you d restart this installer. ise Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this of to not have access, please cor ccs\Database Utilities\	e (PSI™) Eng directory must ntact your syst
Click Next.	Database Files Ple on the same server administrator and i ✓ Install Databas \\SYMANTEC-ICA\	Risk Fabric Installation Wizard Powered by Predictive uses select a directory for the database r as the Risk Fabric SQL Server, If you d restart this installer. use Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this of o not have access, please cor ccs\Database Utilities\	e (PSI™) En directory must ntact your syst
Click Next.	Database Files Ple on the same server administrator and ✓ Install Databas \\SYMANTEC-ICA\	Risk Fabric Installation Wizard Powered by Predictive asse select a directory for the database r as the Risk Fabric SQL Server, If you d restart this installer. are Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this of o not have access, please cor ccs\Database Utilities\	e (PSI™) En directory must ntact your syst
Click Next.	Database Files Ple on the same server administrator and ✓ Install Databas \\SYMANTEC-ICA\	Risk Fabric Installation Wizard Powered by Predictive asse select a directory for the database r as the Risk Fabric SQL Server. If you d restart this installer. e Utilities Now? c:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this of io not have access, please cor ccs\Database Utilities\	e (PSI TM) Eng directory must ntact your syst
Click Next.	Database Files Ple on the same server administrator and ✓ Install Databas \\SYMANTEC-ICA\	Risk Fabric Installation Wizard Powered by Predictive asse select a directory for the database as the Risk Fabric SQL Server. If you d restart this installer. We Utilities Now? C:\Program Files\Bay Dynami	e Security Intelligence utility files. Please note, this o io not have access, please cor ics\Database Utilities\	e (PSI ^M) Eng directory must ntact your syste Browse



Dick Eabric				
RISK FADITC Bay Dynamics		Powered b	y Predictive Security Inte	lligence (PSI™) En
Terms and Conditions	This section shows	intogration warning	s that might require actions outs	do tho installor. Those
Prerequisites	integration warnin	igs will be saved to th	e log file if you click the save but	on at the end of the
Website	installer process.			
				Copy Warning
Notifications	Integration	Warnings		
Data Sources	No Warnings	No Warnings		
Database Utilities				
Integration Warnings				
License Activation				
Install				
				R

20. Check the box next to Activate Offline.

Dick Eabric		
NISK FOULD Bay Dynamics		Powered by Predictive Security Intelligence (PSI™) Engi
Terms and Conditions	License Activation	
Prerequisites		
Website	Activate Offline	
Notifications	_	
Data Sources		
Database Utilities		
Integration Warnings		
License Activation		
Install		
		R
		Next

21. Click 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	iearch	Q 🜲 🗭	DMdministrator 🙆	🗂 Drait (
a	Assets	•								
3	Recently Viewed		Integration Pack	s Data	Sources	Data Integrations	Job Status			
۰	Admin	-	2 Refresh	1 Import	 Move Up 	 Move Down 				
-	Settings	-	Integration Pack						Created Date	
	General		Risk Fabric Symantee	Data At Rest In	tegration 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	ges									
Integra	ation									
Dashb	oards									
Risk N	lodels									
Risk V	lectors									
Event	Scenarios									
Scan	Exclusions									
Entity	Collections								Activate Windows	
3	Help	•							Go to System in Control Panel to activate Windo	
	65.2									

- 4. Click Import.
- 5. Find the zip file for the integration pack that you downloaded earlier.

	- Fri		
😌 🍥 👻 🕈 <u></u> 🕨 Thi	s PC → Downloads → SymanteclCASoftware_65 →	V 🖒 Search Syma	nteclCASoftware 🔎
Organize 🔻 New folder)= • 🔟 (
☆ Favorites	Name	Date modified	Туре
 ★ Favorites ■ Desktop ▶ Downloads > Recent places Phis PC ♀ C on MM246942-PC ▶ Desktop ▶ Desktop ▶ Decuments 	得 ADConnector	4/19/2018 12:24 PM	Windows Installer .
Favorites Contestance	BayDynamics.RiskFabric.IntegrationPack.MicrosoftActiveDirectory	6/29/2016 6:50 AM	Compressed (zipp.
📃 Recent places	BayDynamics.RiskFabric.IntegrationPack.SymantecDataLossPrevention	11/20/2017 9:20 AM	Compressed (zipp.
Controp Control Cont	BayDynamics.RiskFabric.IntegrationPack.SymantecEndpointProtection	10/24/2016 9:26 AM	Compressed (zipp.
This PC C on MM246942-PC Desktop Desktop Documents Documents Music Pictures Videos Local Disk (C:) Network	SymanteclCAInstaller	7/27/2018 10:26 AM	Application
File na	III BayDynamics.RiskFabric.IntegrationPack.SymantecDataLossPrevention	V All Files	Cancel

6. Select the file and click **Open.**

=	Risk Fabric*			Search	۹ 🔺 🗩	DIAdministrator 🕚	🗂 Draft (0
<u>_</u>	Assets 🕨						
9	Recently Viewed	Integration Packs	Data Sources	Data Integrations Job Status			
•	Admin 🔫	2 Refresh	L Import A Move	• Up • Move Down			
0	Settings 👻	Integration Pack				Created Date	
	General	Risk Fabric Symantec D)ata At Rest Integration Pac	×		8/3/2016	•
	Data In Motion	Risk Fabric Symantec D	Data Loss Prevention Integra	ation Pack		11/20/2017	•
	Palicy						
	Queues						
	Web Activity						
	Vulnerability Manage						
	Residual Risk						
	Details Grid Centigur						
	Entity Actions						
	Notifications						
	Organizations & Regi						
	Operating Systems						
Privi	lagos						
Integ	pation						
Dast	hboerds						
Risk	Models						
Risk	Vectors						
Ever	nt Scenarios						
Scar	n Exclusions						
Entit	y Collections					Activate Windows Go to System in Control Panel to activate Winde	
0	Help 🕨						

2.15.4.2 Create a View

1. Navigate to Analyzer > New View.

_							
=	Risk	Fabric	<i>•</i>	Search	۹ 🖡	•	DfAdministrator 🕚 🗎 Draft (0)
	Risk		Views w Filter w Soft w Details w Char	ts 👻		3	Field List >
Le .	Dashboards	•					Search
	Applymer	-	Add Measures from the Field List.				Measures
v	манудет		to view data from this cube.				> III AD Group
Now	Victor						AD Group First Detected Date
Oper	1 View						AD Group List Deleted Date AD Organizational Unit
-	Action Direct						AD Organizational Unit First Detected Date
	Activitinians						AD Organizational Unit Last Detected Date
	Events	•					Action Plan Assigned To Portal User
Ð	Vulnerabilities	•					Action Plan Closed By Portal User
							Action Plan Closed Date
	Identifies	•					Action Plan Committee Competion Late
묘	Assets	•					Action Plan Expected Completion Date
~	December Marrie	- 4					Action Plan Requested Completion Date
3	Postaney views	aa					Action Plan SLA End Date
۰	Admin	•					Action Plan SLA Start Date
	Hele						II Application
v	nep						Application Assignment Environment
							Application Assignment Tier
							Application Category
							Application Centact Role
							Application Central User
							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 Computer Endpoint Behavior
							Authentication Event Computer Endpoint Direction
							Authentication Event Computer Endpoint Dwned B Authentication Event Data
			View Configuration				*
			Measures	Rous	Columns	Fitars	Details
						Activate	

- 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						×
🖨 Delote 📝 R	tename 🛛 🖉 Edit Pro	operties	Import 🛓 Expo	rt		
Search Gube View	5		Cube V	ïew Types		÷
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 > 3	> 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		Ψ.
View Name	Туре	Accessibility	Owner	Date Created	Modified By	Date Modified
DAR Incident Details	Analyzer Vlew	Private	(DI\Administrator)	09/06/2019 08.2	(DI\Administrator)	09/06/2019 08:2
« < Page	1 of 1 > >	0				Displaying 1 - 1 of 1

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 Fat	oric®			Search		Q	* •			DNAdministrator 💧 🛍 D	braft (0)
	Risk	Vieus v Filter	▼ Sot ▼ Details	▼ Chats ▼							Field List	- F
		DAR Incident Status	New	Totel								
2	Dashboards	DAR Incident Date R	lange DAR Incident Count	DAR Incident Match Count DAR Inciden	t Count DAR Incident Match C	sunt					Search	_
0		2-7 Days Ago	64	324	64	324					Measures	
v	rutarjan	61-90 Days Ago	43	195	43	195					AD Group	
New	View	Total	107	520	107	520					 AD Group First Detected Date 	
Open		F	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 First Detected Date	1
			ę.								Action Plan	
*	Events	•	8 2-7 Days App -		DAR Incident Date	DAR Incident Status	DAR Incident Sour	DAR File Docume	DAR File Folde		Action Plan Assigned To Portal User	
D	Vulnerabilities	•	ę.		2-7 Dava App	New	101				Action Plan Closed By Portal User	
-			1								Action Plan Clased Date	
	Identities	•	81-40 Days App		2-7 Days Ago	New	102				 Action Plan Committed Completion Date 	
_			-								Action Plan Due Date	
-	Acides		40	80 80 70	2-7 Days Ago	Neur	103				Action Plan Expected Competion Date	
э	Recently Viewed			DAR Incident Count							Action Plan St A End Date	
					2-7 Days Ago	New	104				Action Plan SLA Start Date	
•	Admin	•									Action Plan Status	
	Help				« < Page	1 0[2 > 2	0	Records: 1	- 100 Total: 107		Application	
											Application Assignment Environment	
											 Application Assignment Tier 	
											Application Category	
											Application Centact Role	
											Application Centact User	
											Application Owner	
											Authentication Event Characteristic Genuer	1 Snaed
											Authentication Event Classification	,
											Authentication Event Classification Date	
											Authentication Event Classified By Portal U	Joer
											Authentication Event Code	
											 Authentication Event Computer Endpoint B 	lehavior
											Authentication Event Computer Endpoint D	Rection
										_	Authentication Event Computer Endpoint C	Avned B
		Bar Chart	Details (1)								 Authentication Event Date 	
		View Configurat	tion: DAR Incident Deta	ils (Analyzer View)								×
		Measures		Rows		Columns		Filters			Details	
_		DAR Incident Count		DAR Incident Date Range		DAR Incident Status				Activate	DAR Incident Source ID	
_		DAR Incident Match	Count								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					
System + Identity Management + Network Resource eployment Licensing + Certificates + Logging	intext Visibility Coperations inces Device Portal Management Maintenance Upgrade Ba Same provide the second	pxGrid Services	ice Threat Centers	Click here to do wireless	setup and visibility setup Do n
	Role Other Monitoring Node	PRIMARY *			
5	 ✓ Policy Service ✓ Enable Session Service Include Node in 	noes () Node Group None	• w		
	Enable Profiling Serv Enable Threat Centre	ice () c NAC Service ()			
	Enable SXP Service Enable Device Admi Enable Passive Iden	1) n Service (1) tity Service (1)			
	DxGrid (7)	N			

- 5. Click Save.
- 6. Navigate to Administration > pxGrid Services.

		milest) area incompany							
sco Iden	tity Services Engine	Home Context	Visibility Operations	Policy	- Administration	Work Centers	0	License Warning 4) 9
 System 	 Identity Management 	 Network Resources 	Device Portal Manageme	ent pxGrid Ser	vices Feed Servi	ce	Click here to do wireles	ss setup and visibility s	etup Do r
All Clients	Web Clients Cap	abilities Live Log S	ettings Certifiqges F	Permissions					
Enable	Oisable OApprove	😝 Group 📫 Decline	🔂 Delete 👻 🤣 Refresh	Total Pending App	oroval(0) +				
] Clier	nt Name	Client Description	Capabilitie	es	Status		Client Group(s)	Au	th Metho
					INO Ga	ua avanaulit			

- 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.

a mentry berances Lighter Hot	ne	 Operations 	Policy Administ	ration • Work C	enters	0	License Warning 4	<u>8</u>	
System Identity Management Ne	work Resources	ce Portal Management	pxGrid Services	Feed Service + T	Click here to	do wireles	s setup and visibility se	tup Do n	10
All Clients Web Clients Capabilities	Live Log Settings	Certificates Perr	missions						
Generate pxGrid Certificates									
I want to *	Download Root Certificate	e Chain							
Host Names *	> cisco-ise								
Certificate Download Format *	Certificate in Privacy Enh	anced Electronic Mall (F	PEM) format, key in PKC	S8 PEM format (inclu	ding certificate chair 🔹	0			
					Reset Create	2			
nected 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.

linihi isco	Stealthwate	Monitor	Analyze	Jobs	Configure	Deploy		00	Global Settin	sktop Client
ecurity Alarmir	/ Insight Dashb g Hosts @	oard Inside	e Hosts						Central Man Packet Anal UDP Directo	agenernt yzer Configura. r Configuration
Concern	Index Target Index	Recon	csc ()	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exhitration P	User Manag	ement
Top Ala	arming Hosts		-2	Alarms by Type	8	-	7 Toda	ıy'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 Engli	ne 🗙 🛛 🗰 Security Insight	Dashboard Ster ×	🕞 Inventory Central Management	× +		_ D X
← → C ▲ No	ot secure https://192.168.1.52/c	entral-mgmt/#!/invent	ory/			☆ 🍮 1
cisco Stealt	hwatch Central Mar	nagement	Appliance Manager	Update Manager	App Manager	0
4 Appliances found						
Q Filter Appliar	nce Inventory Table					
APPLIANCE STA	TUS 🗠 LICENSE STATUS	HOST NAME		IP ADDRESS	ACTIONS	
Up	60 Days or Less	smc-01	SMC SMCVE-VMware- 4232d9dbe1b32e14 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- 4232cta73db93cb3- 472570289f7a4dea	192.168.1.55	œ	
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.

Identity Services Engine	× Security Insight I	Dashboard Stee 🗙 💈	🦻 Inventory Central Management 🗙	+	_	
→ C ▲ Not	secure https://192.168.1.52/cer	ntral-mgmt/#!/invento	ory/		\$	
tulu Stealth	watch Central Man	agement	Appliance Manager Upc	date Manager App Manag	er	(
Appliances found						
Q Filter Applianc	us A LICENSE STATUS	△ HOST NAME	Түре	Edit Appliance Configuration	CTIONS	
Up	60 Days or Less	smc-01	SMC SMCVE-VMware- 4232d8dbe1b32e14- e810b21f42a1f570	Manage Licenses Support	\odot	
Up	90 Days or Less	fcnf-01	Flow Collector FCNFVE-VMware- 4232dbf162c01ea4- f1b1edb64da9166b	Reboot Appliance Shut Down Appliance		
Up	90 Days or Less	fr-01	UDP Director UDVE-VMware- 4232cfa73db93cb3- 472570289f7a4dea	Remove This Appliance	\odot	
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	× *** 50	curity Insight Dashboard	Stec 🗙 😥 Applia	nce Configuration Cent	tra × +		_ 0
→ C ▲ Nots	ecure https://192.	168.1.52/central-mgm	it/#!/configuration/	4b036830-8386-44b1	1-83bd-ae23de9be060		☆ 4
sco Stealthv	watch Centr	al Managem	ent App	iance Manager	Update Manager	App Manager	
entory Appliance Conf ppliance Cor nc-01 (192.168.1.52) Appliance Ne Trust Store	iguration - ifiguration - / Last Updated: 06 twork Services	- SMC //27/2019 8:34 AM E General	iy admin			Canc	el Apply Setter Configuration Menu Add New
FRIENDLY NA ota0ndfiywi2m2e wzjhrnntkxotdmzd mzmjm5ntrknza tq2ywmxzdc1ngu 5mtcznja0ymeznji wodwmdhhyw==- cert	ISSUED TO smc-01.di.lpdr	ISSUED BY smc-01.di.ipdr	VALID FROM 2019-06-25 07:50:35	VALID TO 2024-06-25 07:50:35	SERIAL NUMB 64c2d2753702e5 538e85593013b1 28332c2b41e8	KEY LENGTH 8192 bits Delete	ACTIONS
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 🔻 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.

A Note	noura https://107	169 1 52 (central mam	t/#1/configuration/A	LANK 3959 0593504	27bd-aa22da0ba060		A
7 C A 16013	secure mips//15c	. 100. 1.32/ central-ingin	g #g conniguration y 4	0030030-0300-4401-			н
	App App	oly Configuration C	Changes to Appli	iance		×	
	nfigurati	le the system applies uired, the appliance w	boot is				
	The	following configuration	ons have changed:				
	Ger	eral:					
		Trust Store			1	8	
					Cancel Apply C	Changes (14	

- 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.

sco Stealu Watch Central Management	Appliance Manager	Update Manager	App Manager	
entery / Appliance Configuration ppliance Configuration - SMC nc-01 (192.168.1.52) / Last Updated: 06/27/2019 9:36 AM by admin Appliance Network Services General			Cancel	Apply Satings
Additional SSL/TLS Client Identities	vatch System.			AddNew
Improperly modifying your Certificates can break your Stealthy				
Improperly modifying your Certificates can break your Stealthy FRIENDLY NA ISSUED TO ISSUED BY VALID	FROM VALID TO	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 Manageme	ent Appliance Manager Update Manager App Manager	
Invertory / Appliance Configuration Appliance Configuration - SMC sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:55 AM Appliance Network Services General	by admin Configuration	on Menu
Generate a CSR		
DCA VEV I ENGTLI *	COMBION NAME	
O 2048 bits ○ 4096 bits ○ 8192 bits	sw-smc.di.ipdr	
DI	IPDR	
LOCALITY OR CITY	STATE OR PROVINCE	
Rockville	MD	
COUNTRY CODE	EMAIL ADDRESS	
Click Generate CSR.	administrator@di.ipdr Cancel Generate CS	R
US Click Generate CSR. Identity Services Engine × ** Security Insight Dashboard [1] $\leftrightarrow \rightarrow \mathbb{C}$ A Not secure sw-smc/central-mgmt/#l/configur	administrator@di.ipdr Cancel Generate CS Ste: X @ Appliance Configuration Centre X + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6	R
US Click Generate CSR. ↓ Identity Services Engine × I ** Security Insight Dashboard [1 ← → C ▲ Not secure sw-smc/central-mgmt/#l/configur Clich: Stealthwatch Central Management	administrator@di.ipdr Cancel Cenerate CS Ster X @ Appliance Configuration Centre X + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6 ent Appliance Manager Update Manager App Manager	R
US Click Generate CSR. ↓ identity Services Engine × i ** Security Insight Dashboard [] ← → C ▲ Not secure sw-smc/central-mgmt/#l/configur * Cisco Stealthwatch Central Management Inventory / Appliance Configuration	administrator@di.ipdr Cancel Generate CS Size X @ Appliance Configuration Centro X + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6 Cnt Appliance Manager Update Manager App Manager	R _ 1
US Click Generate CSR. ↓ Interference in the second of the second o	administrator@di.ipdr Cancel Cenerate CS Ster × ☞ Appliance Configuration Centre × + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6 Cancel Appliance Manager Update Manager App Manager Cancel Appliance Manager App Manager	x ×
US Click Generate CSR. Menthy Services Engine × ■ Security Insight Dashboard [: ← → C ▲ Not secure sw-smc/central-mgmt/#l/configur cisco Stealthwatch Central Management Inventory / Appliance Configuration Appliance Configuration - SMC sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:31 AM	administrator@di.ipdr Cancel Generate CS Stee X @ Appliance Configuration Centre X + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6 ent Appliance Manager Update Manager App Manager by admin Configuration	sR A
US Click Generate CSR. identity Services Engine × security Insight Dashboard [] ← → C ▲ Not secure sw-smc/central-mgmt/#l/configur 'clicch' Stealthwatch Central Manageme inventory / Appliance Configuration Appliance Configuration - SMC sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:31 AM Appliance Network Services General	administrator@di.ipdr Cancel Generate CS Sec. X @ Appliance Configuration Centro X + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6 ent Appliance Manager Update Manager App Manager by admin by admin	x ★
US Click Generate CSR. ↓ Identity Services Engine × security Insight Dashboard [1 ↓ → C ▲ Not secure sw-smc/central-mgmt/#l/configur ↓ firstly: Stealthwatch Central Management ↓ Stealthwatch Central Management ↓ Appliance Configuration - SMC sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:31 AM Appliance Network Services General Add SSL/TLS Client Identity	administrator@di.ipdr Cancel Generate CS Ster X @ Appliance Configuration Centro X + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6 ent Appliance Manager Update Manager App Manager by admin Cancel Acc	R A A A A A A A A A A A A A
US Click Generate CSR. ↓ Identity Services Engine ★ I == Security Insight Dashboard [] ↓ → C ▲ Not secure sw-smc/central-mgmt/#l/configur +listly: Stealthwatch Central Management inventory / Appliance Configuration Appliance Configuration - SMC sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:31 AM Appliance Network Services General Add SSL/TLS Client Identity FRIENDLY NAME =	administrator@di.ipdr Cancel Generate CS Sec. X @ Appliance Configuration Centre X + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6 ent Appliance Manager Update Manager App Manager by admin Configuratic Con	R A A A A A A A A A A A A A
US Click Generate CSR. ↓ Identity Services Engine × I == Security Insight Dashboard [1 ← → C ▲ Not secure sw-smc/central-mgmt/#l/configur ·[f_ct_b' Stealthwatch Central Management inventory / Appliance Configuration Appliance Configuration – SMC sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:31 AM Appliance Network Services General Add SSL/TLS Client Identity FRIENDLY NAME =	administrator@di.ipdr Cancel Generate CS Stel X @ Appliance Configuration Centre X + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6 ent Appliance Manager Update Manager App Manager by admin Centel Acc Configuratio Configur	R x cly Settle R R
US Click Generate CSR. identity Services Engine ★ security insight Dashboard [] if → C ▲ Not secure sw-smc/central-mgmt/#l/configur if_csch Stealthwatch Central Management inventory / Appliance Configuration Appliance Configuration - SMC sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:31 AM Appliance Network Services General Add SSL/TLS Client Identity FRIENDLY NAME =	administrator@di.ipdr Cancel Generate CS Sec. X @ Appliance Configuration Centro X + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6 ent Appliance Manager Update Manager App Manager by admin Cancel App Configuration CentreficAte File * Choose File Concol App Concol App Concol App Concol Concol Concol	R ¢
US	administrator@di.ipdr Cancel Generate CS Sec. X @ Appliance Configuration Centro X + ration/b4915dc2-2979-45fc-b907-42dc19ce70b6 ent Appliance Manager Update Manager App Manager by admin Cancel Appliance Configuration Centre File * Choose File Cancel Act Clent Idente v. Improperty modifying your certificates can break your Stealthwatch system. Follow th	xR ★ ply Senti xR xR xR xR xR xR xR xR xR xR

- 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 Warnin
System Identity Management Net	twork Resources	vireless setup and visibili
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	NI3WB+204KCmr040708H0Ra8taKFLuNwk=	
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)	0
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			Configurat	tion Menu 1
Appliance Network Services General				
Houtonal Coll Leo caona donardo 🖉				
Add SSL/TLS Client Identity			Download C	SR
EDIENTY V NAME +	CEPTIEICATE EN E *		3.1	
SMC_PKCS12	sw-smc.di.lpdr_1	192.168.1.150.p12	Choose Fil	e
BUNDLE PASSWORD *	CONFIRM PASSWORE	D *		
		Cancel	Add Client Iden	tity

VALID TO

CEDIAL MILINA

VALID EDOM

49. Click Add Client Identity.

ICCLIED TO

Stealt	hwatch Ce	ntral Manager	ment	Appliance Manager	Update Mana	ger App M	lanager
ntory / Appliance C	Configuration		_				
opliance Co -smc (192.168.1.	onfiguration 150) / Last Update	n - SMC ad: 08/08/2019 6:55 A	M by admin			Cance	Configuration Mer
Appliance	Network Services	General					
Additional SSI	L/TLS Client Id	entities 👩 🛛 🤇 Moo	lifiod				Add New
Additional SSI	L/TLS Client Id	entities o Mo c	iñed) System.			Add New
Additional SSI	L/TLS Client Id y modifying your C	entities o Moo Vertificates can break y	ified	ı System.			Add New
Additional SSI	L/TLS Client Id y modifying your C ISSUED TO	entities Moo Pertificates can break y ISSUED BY	Kñed our Stealthwatch VALID FROM	n System. VALID TO	SERIAL NUM	KEY LENGTH	Add New
Additional SSI	L/TLS Client Id y modifying your C ISSUED TO DI	entities Moo iertificates can break y ISSUED BY Certificate Services Endpoint Sub CA - cisco-ise	valid FROM 2019-08-07 07:02:34	1 System. VALID TO 2021-08-07 07:02:34	SERIAL NUM 55e8a9bc77484 06f9d07c429641 e5b05	KEY LENGTH 2048 bits	Add New ACTIONS Delete

- 50. Click Apply Settings.
- 51. Navigate back to the SMC web console home screen.

ICCLIED BY

ili.ili. cisco	Ste	ealthwatc	h						0	Desk	top Client	~
	Da	ashboards	Monitor	Analyze	Jobs	Configure	e Dep	6y				
Securit	v Insi	aht Dashbo	ard Linsid	e Hosts			Cisco*	ISE Configuratio	n			
Joodine	y mor	grit Duoribe	and Thiold				Active	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	-	Al	arms by Typ	be	-	и то	day's Alarm:	s	-	2
		No data to dis	play									

52. Navigate to **Deploy > Cisco ISE Configuration.**

😧 Identity Services Engine	× 💿 Cisco 🖲 ISE Conf	guration Steal 🗙	w Inventory Central	Management × +	
← → C ▲ Not secure	sw-smc/lc-landing-pag	e/smc.html#/settings	/pxgrid		☆
Stealthwa	tch Monitor Ana	lyze Jobs	Configure	Deploy	Q (1) (2) Desktop Client
Cisco® ISE Configura	tion				
Cisco ISE Configuration	0				Add any and much
No Disso ICE conferention	o Oliok Add ony configu	ation to bools			And new configuratio
No Gisco ISE configuration	s. Click Add new configu	ation 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	rid 🛧 🗳 i
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 (b)

58. Click Save.

59. On the Cisco ISE web portal, navigate to **Administration > pxGrid Services > All Clients.**

 System I dentify Management I Network Resources I Device Portal Management pxGrd Service I Freed Service I Threat Cent Cick here to do wireless setup and visible All Cients Capabilities Live Log Settings Certificates Permissions Clent Name C Clent Description Capabilities CPU, 0 Sub Online (XMPP) Internal Ise-dandit-cisco-ise Capabilities Capabilities	2130		and a state of the state		TIONING	P Contra	At VISIDILITY	P Operadoria	- Tolicy		TOTA OCIMETS			
All Clients Web Clients Capabilities Live Log Settings Certificate Permissions Client Name Concernation Capabilities Permissions Client Name Client Description Capabilities Client Croup(s) Internal I is e-admin-cisco-ise Capabilities Capabilities Capabilities Client Croup(s) Internal I is e-bridge-cisco-ise Capabilities Capabilit	• Sy:	stem)	Identity Mar	agement	 Network 	k Resources	 Device F 	Portal Manager	nent pxGrid Servi	Feed Service	 Threat Cen 	Click here to do win	eless setup	and visibil
Image: Control of Contro	All C	lients	Web Clients	Capa	bilities	Live Log	Settings	Certificates	Permissions					
Clent Name Clent Description Capabilities Status Clent foroug(s) ise-fanoat-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal ise-admin-cisco-ise Capabilities(0 Pub, 2 Sub) Online (XMPP) Internal ise-admin-cisco-ise Capabilities(0 Pub, 2 Sub) Online (XMPP) Internal ise-admin-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal ise-bridge-cisco-ise Capabilities(0 Pub, 4 Sub) Online (XMPP) Internal ise-sermit-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal	🖌 En	able 🥝	Disable 🥑	Approve	e Group	Decine	Delete -	🛞 Refresh	Total Pending Appro	oval(0) 👻		1 coloring item	1 0 4 0	Chaus
• ise-fanout-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal • ise-admin-cisco-ise Capabilities(4 Pub, 2 Sub) Online (XMPP) Internal • ise-bridge-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal • ise-bridge-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal • ise-bridge-cisco-ise Capabilities(0 Pub, 1 Sub) Online (XMPP) Internal • ise-indict-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal • ise-indict-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal • ise-indict-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal • ise-indict-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal • ism: capabilities(0 Pub, 0 Sub) Online (XMPP) Internal		Client I	lame	h	Clier	nt Descriptio	1	Capabilit	ties	Status		Client Group(s	1-0010	Snow
▶ Isse-admin-cisco-Ise Capabilities(4 Pub, 2 Sub) Online (XMPP) Internal ▶ Isse-publub Cisco-Ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal ▶ Isse-Intridge-Cisco-Ise Capabilities(0 Pub, 1 Sub) Online (XMPP) Internal ▶ Isse-met-Cisco-Ise Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal ✔ ▶ smc Capabilities(0 Pub, 0 Sub) Online (XMPP) Internal		ise-fan	out-cisco-ise					Capabili	ties(0 Pub, 0 Sub)	Online (XMPP)		Internal	1.S	
▶ 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-mnt-cisco-ise Capabilities(2 Pub, 1 Sub) Online (XMPP) Internal ✓ * smc Capabilities(0 Pub, 0 Sub) Online (XMPP)		ise-adr	nin-cisco-ise					Capabilit	ties(4 Pub, 2 Sub)	Online (XMPP)		Internal		
Image: bit ise-bridge-cisco-ise Capabilities(0 Pub, 4 Sub) Online (XMPP) Internal Image: bit ise-bridge-cisco-ise Capabilities(2 Pub, 1 Sub) Online (XMPP) Internal Image: bit ise-bridge-cisco-ise Capabilities(0 Pub, 0 Sub) Online (XMPP)		ise-put	sub cisco iso					Capabilit	ties(0 Pub, 0 Sub)	Online (XMPP)		Internal		
▶ ise-mnt-osco-ise Capabilities(2 Pub, 1 Sub) Online (XMPP) Internal ▶ smc Capabilities(0 Pub, 0 Sub) Online (XMPP)	•	ise-brid	lge-cisco-ise					Capabili	ties(0 Pub, 4 Sub)	Online (XMPP)		Internal		
Capabilities(0 Pub, 0 Sub) Online (XMPP)	•	ise-mn	t-cisco-ise					Capabilit	ties(2 Pub, 1 Sub)	Online (XMPP)		Internal		
		smc						Capabilit	ties(0 Pub, 0 Sub)	Online (XMPP)				

60. If the SMC client you just created says **Pending**, check the box next to it and click **Approve**.

sco	nwaten	1759-5 175 9-5			9	00	Desktop Client
Dashbo	ards Monitor Ana	alyze Jobs	Configure	Deploy			
sco® ISE Con	iguration						
ilsco i SE Contigi	Iration U					Add n	new configuration
Cluster Name	Primary pxGrid Node	Secondar	y pxGrid Node		🗘 User Name	Status	Actions
cisco-ise	192.168.1.61 💮				SMC	00	0

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	Home + Context Visibility	Operations Policy	 Administration 	Work Centers	0	License Warning 📥	S 0
RADIUS Threat-Centric NAC Live Logs Policy List Endpoint Assignment	s + TACACS + Troubleshoot	Adaptive Network Control	Reports		Click here to do wirele	ess setup and visibility setup	Do not show the
List							
C Refresh + Add Trash - C	i Ear)0
Policy Name	ANC A	ctions					
No data lound.							
No data Kound.							
wo data round							
NO SIST RUNG							

- 2. Click Add.
- 3. Enter a name for a quarantine action.

RADIUS Threat-Centric NAC Live Logs + TACACS + Troubleshoot + Adaptive Network Control Reports Click here to do wireless setup and visibility setup Do not show this a Policy Lat Endpoint Assignment St > New put fields marked with an asterisk (*) are required. Action* QUARANTINE GUARANTINE SHUT_DOWN PORT_BOUNCE	ilisiti Identity Service	is Engine Home	➤ Context Visibility	* Operations	+ Policy	Administration	➤ Work Centers		License Warning	<u>a</u> q		
st > New put fields marked with an asterisk (*) are required. Action *	RADIUS Threat-Cer Policy List Endpoint A	ntric NAC Live Logs 🔹 🕨	TACACS Troubleshoot	Adaptive I	Network Control	Reports		Click here to do w	reless setup and visibility	setup Do n	x show t	his ag
Acton* CUARANTINE Acton* CUARANTINE SHUT_DOWN PORT_BOUNCE	st > New put fields marked with an o	asterisk (*) are required.										
CUMRINITINE SHUT_DOWN PORT_BOUNCE	name Action *	QUARANTINE										
PORT_BOUNCE		QUARANTINE SHUT_DOWN	0									
		PORT_BOUNCE										

4. Select **QUARANTINE** for the **Action**.

🚭 Identity Services Eng	× Cisco Identity 5	Servici 🗙 🛛 😂 Cisco Id	entity Service 3	K siw Invent	ory Central N= ×	sw Flow Search (5	Stealth 🗙 📔 💁 ptSenseBo	rder.di2 × +	e.	-	
← → C ▲ No	ot secure cisco-ise.di.	ipdr/admin/#monitor/a	anc/anc_polici	es_listpage						\$	4
cisco Identity Service	es Engine Home	Context Visibility	• Operations	+ Policy	Administration	Work Centers	(1)	cense Warning 📣	Q,		•
RADIUS Threat-Cer Policy List Endpoint A	ntric NAC Live Logs + T assignment	ACACS + Troubleshoot	 Adaptive 	Network Control	Reports		Click here to do wireless se	rtup and visibility set	up Do no	t show t	his aga
List > New Input fields marked with an a	asterisk (*) are required.										
name	ANC_QUARANTINE										
Action *	- QUARANTINE										
			Cancel	Submit	R						

- 5. Click Submit.
- 6. Navigate to **Policy > Policy Sets.**
| Policy Sets | Profiling Posture C | Ilent Provisioning | 5 | | Click here to do wireless | s setup and visibilit | y setup [| o not show t | his à |
|-------------|---------------------|--------------------|------------|---|---------------------------|-----------------------|-----------|--------------|-------|
| cy Sets | | | | | | | | | |
| | | | | | | | | Reset | Si |
| Statu | s Policy Set Name | Description | Conditions | | Allowed Protocols / Ser | ver Sequence | Hits | Actions | V |
| rch | | | | | | | | | |
| | | | | + | | | | | |
| 0 | Default | Default policy set | | | Default Network Access | •• + | 94 | ٥ | + |
| | | | | | | | | Reset | 5 |
| | | | | | | | | | |

- 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.

0	differen Obudia	onlisit Vsobiity	 Operation 	no (** Policy)	 Administration 	Work Centers	License Warning - 🛎 -		a y
Librar	y		Editor					23	9.5
Sea	rch by Name			Session ANG	Policy				•
•		© է 🕈	ĥ	Equals	•	ANC_QUARANTINE			
	AD_Domain_Admin	0		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	0							
11	Domain Admins	0							
8	Compliant_Devices	0							

- 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	ts Profiling Posture Client Prov	Context visibility Operations Policy Elements	Padministration Provincial Centers	Click here to do wireless setup and visibility setu	up Do not sho	w this aga
* Authoriza	ation Policy - Global Exceptions (1)				
			Results			
St	atus Rule Name	Conditions	Profiles	Security Groups	Hits	Action
Search						
1 0	Quarantine	E Session ANCPolicy EQUALS ANC_QUAR	ANTINE Cisco_Temporal_Onboard	Quarantined_Systems * *	+	0
Authoriza	ation Policy (2)					
					Reset	Sa

- 16. Click Save.
- 17. In the SMC web console, click **Monitor > Users.**

Stealthwatch 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.

V C A Not secure 152.100.	riswic-analog-pagersine.	and they does not style of the lost and				н	
7 days		ت - مله					
Command & Control							
7 days	Devices & Se	essions					
Exploitation	MAC Address: 00 Host	0:50:56:b2:8c:ad Name Group	MAC Vendor: Location	Count	Device Type: Micros Start	soft-Workstation End	
7 days	192/068.8.102	Catch Al	-8- RFC 1918	34	6/8/19 9:25 AM	* Current	
DDoS Source							
7 days							
DDoS Target							
7 days							

19. Click a host to quarantine.

dentity Services E	🐑 🗙 📔 🐑 Cisco Identity Service	🗴 🕼 Cisco Identity Servicii 🗴 🕴 Inventory Central IV 🗙 🚱 Host Report Stealthi 🗴 🚮 pfSenseBorder.di2 - 🗴	+ -
→ C 🔺	Not secure 192.168.1.150/lc-	-landing-page/smc.html#/host/192.168.8.102	\$
Host Groups: Location: First Seen: Last Seen: Policies: MAC Address: ISE ANC Policy:	Catch All RFC 1918 Inside 00:50:56:b2:8c:ad (VMwar Egit	192.168.8.102 re, Inc.)	
op Security o events were	Events for 192.168.8.1	102 Source (0) will is incorrect, contact your Stealthwatch administrator.	Target (0)
Users & Sess	sions	Application Traffic	nal External
Users & Sess MAC Address: 00:50:56:b2:8c:a	MAC Vendor: Device Id VMware, Inc. Micros Workst Start End	Application Traffic Internation Application Total % Sent Ratio Received 7-day Trend tation There are no application traffic details to display	24-hour Trend

- 20. Click Edit next to ISE ANC Policy.
- 21. From the drop down, select the quarantine action you created earlier.

Con Identity S	ienvices Eng: 🗙 🌚 Ca	sco Identity Service ×	Eisco Identity Service 🛪	sw Inventory Central M 🗙	🚱 Host Report Stealth 🗙	ptSenseBorder.di2	× +	-		
Applyin	g ANC polic	92.168.1.150/ic-landing-	page/smc.html#/host/19/	× 192.168.8.102				ਸ	Ĵ	:
Select the Al	NC Policy to apply to	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.		Source	2 (0)	Target (0)		
				ic			itemal	External		
				I % Sent	Ratio Received	7-day Trend	24-hou	r Trend		
		Close	Save	ation 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 Permis	sions		Audit L	ogger	Permissions
General	🚨 User Group	s 📵 Info	ormation	Permissions		Database Permissio
Full name						
Email						
Phone				~		\searrow
Phone Authentication	n			V		
Valid IP's						
Auth method	d Tripwire L	og Center	\checkmark			
External Us	er					
Account is	Disabled 🗌					

8. Click the **Permissions** tab.

2	l	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	
			2	
			.0	
ОК	Cancel			

- 9. Click Edit list of permissions.
- 10. Select Databases.

5	Permissions for: twe	user 📃 🗖 🗙
Permissions Admin Adm	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	Finabled	Name Allow REST API Logon	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 🕅	veuser
Manage	r Permissions Audit Logger Permissions
📰 General 🚨 Use	er Groups 🚺 Information 💐 Permissions 🗾 Database Permissions
🈼 🍒 🕹	
Name	Description
View System Datab	ase Allows the user to view the System Database data.
Allow REST API Log	gon Allows the user to connect using the REST API.
	Ĺ₹
	Cancel

- 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	\$
	ES RULES ACTIONS TASKS POLICIES LOG REPORTS SETTINGS	
Settings	*	Refresh 🖸 Help 🕅 Logr
Tripwire Tripwire Strip User Strip Preferences	Log Management Preferences	
Differences	Forward TE log messages to syslog Transport protocol: TCP	
Preferences Log Management Database Sourcity Dappeop	Host: arceight-cons.dl.jpdr Port: 1469 Test Connection	
Colobal Variables Approval Templates E-mail Servers Configure TE Consol Import Settings Export Settings Administration	Allow TE to use information from Tripwire Log Center Service address: https://arcsight-cons.di.ipdr:8091/tic User name: tweuser Password: Confirm: Text Connection	
C Post-Remediation Se W Users User Groups C Home Pages	Apply	
Roles		
Custom Node Types		
File Systems		

- 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	ĸ
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.	5
	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.

	Viewer		
ROBERT Darkaner Lies Cares	Intitled Active Channel 1		
	Action Channels		Total Supple: 52
Connectors Ctrl+Alt+E 👻	Shark Times 25 Oct 2010 09:22:25 007		Van High 0
	End Time: 25 Oct 2019 10:32:25 PDT		High: 22
iortcuts	Filter Agent ID = "windows-ad"		Medium: 8
	Inline Filter: No Filter		Low: 487
Connectors	VEHING RUPS: NO RUP		wery tow: 11
- Sharco	Radar		
+ ArcSight Administration			
- Dite Connectors		🖬 ang pang sa sang pang pang sa 📕 🖉 kana sa	
- 🔗 AMP Connector(running)	· · · · · · · · · · · · · · · · · · ·	Real Section Real Property lines. Real Property lines and the section of the sect	
CEF collector(running)			
- Gisco AMP(running)	Manager Receipt Time ↓ 1End Time ↓ Name ↓	Attacker Address 🌣 Target Address 🗢	Priority Device Vendor
FleZila Logs(running)	25 Oct 2019 10:31:19 PDT 25 Oct 2019 10:31:13 PDT An account was lo	gged off. 172.23.122.229	I Microsoft
Glasswall Connector(down)	25 Oct 2019 10:31:15 PDT 25 Oct 2019 10:31:08 PDT Software Protects	on Platform Service	3 Microsoft
Glasswall Inbound SMTP Analy	25 Oct 2019 10:31:15 PDT 25 Oct 2019 10:31:08 PDT 30 Software Protects	on Platform Service	a Microsoft
Garoval Loomo Correctorio	25 Oct 2019 10:31:15 POT 25 Oct 2019 10:31:08 POT 25 Oct 2019 10:31	OU PDT on Service	5 Microsoft
Glasswall Logs(down)	25 Oct 2019 10:31:04 POT 25 Oct 2019 10:31:01 PDT Device connection	00W1 192.108.01.20	Arcsignt
Glasswall Management Service	25 Oct 2019 10:30/43 PDT 25 Oct 2019 10:30:38 PDT Software Protects	on Platform Service	3 Merosoft
🤣 Glasswall MultiConnector(dowr	25 Oct 2019 10:30:43 PDT 25 Oct 2019 10:30:38 PDT Software Protects	an Platform Service	a Microsoft
- 🤣 Glasswall Service Logs(down)	25 Oct 2019 10:30:43 PDT 25 Oct 2019 10:30:38 PDT Software Protects	on Platform Service	2 Microsoft
- 🌮 TLC-Syslog-Daemon(running)	25 Oct 2019 10:30:23 PDT 25 Oct 2019 10:30:20 PDT Connector Raw Ev	rent Statistics	3 ArcSight
🤣 Ubuntu Client(down)	25 Oct 2019 10:29:57 POT 25 Oct 2019 10:29:15 POT A logon was atten	pted using explicit c 192.168.81.50	Mcrosoft
	25 Oct 2019 10:29:33 PDT 25 Oct 2019 10:29:15 PDT Special privileges (assigned to new logon. 172.23.122.229	3 Microsoft
UDP Connector(down)	25 Oct 2019 10:29:33 PDT 25 Oct 2019 10:29:15 PDT An account was a	uccessfully logged on. 172.23.122.229	I Microsoft
UDP Connector(down)	25 Oct 2019 10:29:12 PDT 25 Oct 2019 10:29:06 PDT An account was lo	gged off. 192.168.81.56	3 Microsoft
UDP Connector(down) Windows Connector Server(dc Windows UDP Systogrunning)	25 Oct 2019 10:28:37 PDT 25 Oct 2019 10:28:32 PDT Device connection	up 192.168.81.56	3 ArcSight
 UDP Connector(down) Windows Connector Server(do Windows UDP Systog(running) Windows-ad(running) Windows-ud(running) Windows-ud(running) 			3 Microsoft
UDP Connector(down) Windows Connector Server(do Windows Lee Systal(running) Windows-ad(running) Windows-ad(running) Windows-0-1(running) Windows-0-1(running)	25 Oct 2019 10:28:37 PDT 25 Oct 2019 10:23:04 PDT An account was to	gged off. 192.168.81.56	A Manager II
CUP Connector(down) Windows Connector Sorver(de Windows UCP System/uning) Windows -ul/(uning) Windows:0:10 (running) Windows:0:10 (running)	25 Oct 2019 10:28:37 PDT 25 Oct 2019 10:23:04 PDT An account was lo 25 Oct 2019 10:28:37 PDT 25 Oct 2019 10:28:31 PDT Special privileges /	gged off. 192.168.81.56 assigned to new logon. 192.168.81.56 uccessfield logond on 192.168.2.122 103.168.81.56	3 Microsoft
	25 Oct 2019 10:28:37 PDT 25 Oct 2019 10:23:04 PDT An account was lo 25 Oct 2019 10:28:37 PDT 25 Oct 2019 10:28:31 PDT Special privileges i 25 Oct 2019 10:28:37 PDT 25 Oct 2019 10:28:31 PDT An account was lo 29 Oct 2019 10:28:37 PDT 25 Oct 2019 10:28:31 PDT An account was lo	gged off. 192.168.81.56 sasigned to new logon. 192.168.81.56 uccessfully logged on. 192.168.2.122 192.168.81.56 uccessfully logged on. 192.168.2.122 192.168.81.56	3 Microsoft 3 Microsoft
UP Connector(down) UP Connector(down) Windows Connector Server(dc Windows ULP Systop(running) Windows ULP Systop(running) Windows ULP (running) Windows ULP (running) Windows ULP (running)	25 Oct 2019 10:28:37 POT 25 Oct 2019 10:23:04 POT An account was 25 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:31 POT Special privileges 25 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:31 POT An account was 25 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:32 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:37 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:37 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019 10:28:37 POT Special privileges 5 Oct 2019 10:28:37 POT 25 Oct 2019	gged off. 192, 168, 81, 56 assigned to new logon. 192, 168, 81, 56 arcressfully logged on. 192, 168, 2, 122 192, 168, 81, 56 assigned to new logon. 192, 168, 2, 127 192, 168, 81, 56 192, 168, 31, 56 192, 168, 31, 56	3 Microsoft 3 Microsoft 3 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 <u>i</u> n:	🛾 Desktop 🔹 🍺 📂 🔛 -	
Adminis Adminis This PC This PC Librarier Network screens export ica-arcs ica-arcs ica-arcs	trator m iica-minimal s k hots ight ight-noextra	
Salve II. Desktop Administrator ica-minimal This PC Libraries Ibraries Network screenshots export ica-arcsight ica-arcsight-noextra File name: ad-events-export File name: ad-events-export Ica-arcsight-noextra OK Files of type: Comma separated values (*.csv) Cancel Export Data Options Rows: All in channel Columns: exporterset Destinctions Export late Columns:	ОК	
Files of <u>type</u>	: Comma separated values (*.csv) 🔹	Cancel
Export Data (Options	
Rows:	All in channel Selected rows only	
Columns:	exporterset	-
Destination:	Local CSV File	-
		Help

7. Click OK.

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

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	Ð	Search	Q. 🔺	DI\Administrator	🗂 Draft (f
*	Integration Packs	Data Sources	Data Integrations	Job Status		
Ð	Choose Data Source	Jser Defined 👻				
٢	O Create Data Sou	irce 🗃 🕼 Edit	2 Refresh			
*	User Defined Datasou	rces		Data Source Details		
*	Name	Type / S Host	Refreshed	Data Source Label: Server Name:	ArcSight Import symantec-ica.di.ipdr	
<u>ם</u>	ArcSight Import	File Syst symanted	H	Authentication Mode: Username:	Windows	
9		Ocreate Query ■		Password: Download Directory:	C:\Temp\processed	
•						
Ø						

- 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 🔺 🗩	DIVAdministrator	🗎 Di
#) 1/2	Integration Packs		Data Integrations Job Status		
•	Choose Data Source U	lser [efined 👻		
8	ArcSight CSV Import				
Ł	Query Details	Wat	rmarking / Scheduling		
U	A 11				
*	Restarting Hanging Jobs:			÷	
-	Delimiter:	Lea	ve blank to use system default delimiter		
9	Custom Options:				
•		Selec	which files to import into the table:		
0		Ľ	Path	Modified Date	
			C:\Temp\unprocessed\export_withnulls.csv	10/28/2019 8:27 AM	
			k	ta	
			revis. The destination table will be compretely replaced with the latest spicadsheet da	5.5.4	



17. Click OK.

18. If desired, set a schedule for this import.

≡ F	Risk Fabric		Search		् 🔺 🗩		DIVAdministrator) 🗖
*	Integration Dacks	Data Sources	Data Integration		ob Status			
~	Integration Packs	Data Sources	Data Integration:	5 J	op Status			
9	Choose Data Source	User Defined 👻						
3	ArcSight CSV Import							
!	Query Details	Watermarking / Sched	duling					
U	Query	-	_					
8			0					
	No dependencies on oth	ner queries						1
2	Scheduling							
•	Note: Scheduling not hone	ored if this query depends o	n other queries. Queries	s will run afte	er dependent quer	ies complete.		
*	Scheduling	Initial Run Date:	Initial Run Time:					
3		Î	<u> </u>	Y				
		Occurs Every:	Hours:		Minutes:			
		Intra Day	0	\$	0	۰		



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** : 4 **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.

3 Ri	lisk Fabric	× +			Ĺ	_ 🗆 X
← -	C A Not secure	e symantec-ica/#admin/integra	tion		ц ц	0:
=	Risk Fab	oric®	Search	<u> </u>	DIVAdministrator	苗 Draft (0)
*	Integration Pa	acks Data Sources	Data Integrations	Job Status		
•	Create Inter	gration Pack				
ی ا	Name: Description:	ArcSight CSV Integration				
*						
ອ						
۰						
0						
6.5.2					Save Can	cel



- 5. Right-click the newly created Integration Pack, and select Create Import Rule.
- 6. Enter a Name and Description.

> Risk	Fabric	× +			
$\leftarrow \ \rightarrow$	C A Not secure	symantec-ica/#admin/integr	ation		☆ Θ :
=	Risk Fab	oric [®]	Search	۹ 🔺 🗩	DIVAdministrator 🕒 📋 Draft (0)
*	Integration Pa	acks Data Sources	Data Integrations	Job Status	
¢ ۳	Create Impo	ort Rule			
	Name:	ArcSight AD Event Import	Rule		
s.	Description:	For importing AD login even	ents		
็จ					
•					
3					
652					Salap 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 × +				_ X
← →	C A Not secure symantec-ica/#admin	/integration		07	☆ 0 :
=	Risk Fabric®	Search	۹ 🔺 🗩	DIVAdministrator	🗂 Draft (0)
*	Integration Packs Data Sour	ces Data Integrations	Job Status		
Ð	Edit Import Rule Mapping: ArcSight Al	D Event Import Rule Mapping			
₿	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:	528			
ত	Run Intra-Day:	No			
٠	Run Order:	0	\$		
?	Entity Type:	EP Events	*		
	Update Pre-Process Table:	Yes	197		
	• Create Entities:	Yes			
6.5.2	Save Cancel				

- 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.

		rea - uoniniprincipation			A U
=	Risk Fabric [®]	Search	n Q 🖡 🗩	DI\Administrator	🛱 Dra
* 	Integration Packs	Data Sources Data Integr	ations Job Status		
9	Edit Import Rule Mapping:	ArcSight AD Event Import Rule Ma	apping		
	Required Fields				
!			hearr -	T	
U	Entity Column	Туре	Value	Default Value	
	EventDate datetime	Source Column 🔍	End Time 👻		
ອ	SourceEventID nvarchar(50)	Formula 👻	Convert unique 🗧 🖀 👻		
¢ 0	Optional Fields				
	Search:				

- 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 Fahric	Search		DIVAdministrator	🗂 Drafi
MISIX LADITC	b.		0	
Integration Packs Da	ta Sources Data Integra	ations Job Status		
Create Import Rule Manping				
EventObjectTuneName				
nvarchar(254)	Source Column 👻		r	
6				
Create and Associate Event Ac	tivity Type			
Entity Column	Туре	Value	Default Value	
EventActivityTypeName 🖾	Source Column			
nvarchar(254)				
Create and Associate Event Ru	ıle			
	-			_
E 10 0 1		Value	Default Value	
Entity Column	туре		,	

18. Click **Save** when finished.

19. Navigate to the Job Status tab.

🕻 Risk	k Fabric			×	+				
$\leftrightarrow \rightarrow$	C 4	Not	secur	re syman	tec-ica/#admin/ir	ntegration			• ☆ ⊖ :
=	Ris	k F	al	bric⁼		Search	a 🔍 🖡	, D	NAdministrator 😩 🛗 Draft (0)
*									
M	Ir	itegrat	tion F	Packs	Data Source	s Data Integr	ations Job Status		
Ð	1				1 .				Α.
۲		sÜn	1	Stop Sta	atus				View Details
Ł	6	<u>з</u> и	. 1	Enabled	Status	Last Run Outcome	Last Run	Last Run Duration	Next Run
U	6	Z R	<u>ia</u> 1	yes	Not running	O Failed	10/29/2019 7:57:00 AM	00:00:01	10/29/2019 11:00:00 AM
*	6	R R		yes	Not running	Succeeded	10/29/2019 7:57:00 AM	00:10:44	10/30/2019 12:15:00 AM
▫	6	R R		yes	Not running	Succeeded	10/29/2019 7:57:00 AM	00:00:05	
9									
۰									
0									
		«	<	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.

🕻 Risk	Fabric	× +				_ □ X
\leftrightarrow \rightarrow	C 🔺 Not secure	symantec-ica/#/analyzer/v	iew/8879870D-672D-4F	FD-9859-A8F2E0E28/	A9B	☆ 🛛 :
=	Risk Fabr	'iC∗	Search	۹.	DīvAd	lministrator 😩 🛱 Draft (0)
# 12	Views Views Filter Views EP Event Date Range	Sort - Details - Ch Event Count	arts 💌		3	Field List Search
Ð	Z-r Days Ago Total	Details	÷		0 = 2 ×	Measures AD Group
₽		EP Event Date Ra	Action Taken	EP Event Date	EP Event Count	AD Group First Detected AD Group Last Detected AD Organizational Unit
0 **		2-7 Days Ago	A logon was attemp	2019-10-25	10	AD Organizational Unit F AD Organizational Unit L Action Plan Action Plan
п э		<pre></pre>	1 of 1 > >	C Reci	ords: 1 - 15 Total: 15	Action Plan Assigned to Action Plan Closed By Pr Action Plan Closed Date Action Plan Committed C Action Plan Due Date Action Plan Due Date
?	Details					Action Plan Requested C
	View Configuration: an	rcsight (Analyzer View)				*
	Measures	Rows	Columns		Fitters	Details
652	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.



2. Click Next.

*	ArcSight SmartConnector
ArcSight	Choose Install Folder
 Introduction Choose Install Folder Choose Install Set Pick Shortcut Folder Pre-Install Summary Installing Upgrade System Restart Install Complete 	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.



4. Click Next.



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



- 7. Click Next.
- 8. Select Syslog Daemon.

*	Connector Setup	
À ArcSight	Select the connector to configure	
Configure		
	Type Eyslog Daemon	v
	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	ncel

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

×	Connector Setup	- 🗆 X
À ArcSight	Enter the type of destination	
Configure		
	 ArcSight Manager (encrypted) 	
k.	ArcSight Logger SmartMessage (encrypted)	
	 ArcSight Logger SmartMessage Pool (encrypted) 	
	O CEF File	
	O Event Broker	
	◯ CEF Syslog	
	CEF Encrypted Syslog (UDP)	
	○ CSV File	
	◯ Raw Syslog	
		R
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
∢ 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

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

*		Connector Setup		_	
À ArcSight	Enter the connec	tor details			
Configure					
	Name Location DeviceLocation Comment	Tripwire Log Center			
				L ₂	
			< Previous	Next > (Cancel

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



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



24. Click Next.



*	Connector Setup	^
À ArcSight	Would you like to continue or exit?	
Configure		
	⊖ Contrue	
	ka la	
DFOCUS		
	< Previous Next > Cancel	



- 28. Click Done.
- 29. Open the Tripwire Log Center Console.
- 30. Go to the Configuration Manager.

A	Tripwire Log Center	_ D X
File View Options Help		
- 🚱 🖉 🔕 🐂 - 🖳 🔎 🔷 💆 - 🔜 🖄 🚱 🛷 -	J 🥶 🕹 🥽 Time Filter 24 Hours 🔻	
Views 7		
Events		
	Resource View - 1 Managers	
Dashboard Monitored Assets	Drag a column header here to group by that column	
Asset Groups		
Event-Databases	▶ 1 Printary Manager arcsight-cons.di.ipdr Current Primary Manager	
Viewer Tripwire Enterprise Servers		
Active Directory		
Real-Time Event		
Viewer		
\mathcal{P}		
AuditLogger		
Discovered Assets		
Task Manager		
TA A A A A A A A A A A A A A A A A A A		
Turk Chuddau		
~		
Report Center		
Resources		
Configuration	Manager Status: Curren	User: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**.

iews 🕂		Configuration	
Events	R	Manager - Primary Manager	. . ×
5	P	Name Primary Manager	
ashboard		Description Primary Manager	
		🕅 Settings 🏕 Installed Modules 🕞 Email 💿 Logging 🙈 Authentication 🦓 Procy 🖳 Network Collector 🖵 File Collector 💑 Advanced Windows C	`ollector
t-Database Viewer		Audit Logger Advanced Settings Permissions Asset-Configuration Rules	
I		+ X	
-Time Event		Advanced Option Value	
Viewer		Log Message Forwarding - Destinations 192 163 1.121:514:top	
2			
dit Logger			
overed Assets			
<i>i</i>			
k Manager			
6 3			
k Scheduler		₽ A	
ourt Center			
		Apply QK Cancel	

- 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.

Dashboard Analysis VOutbreak Control V Management V Accounts V	Search	Q		
API Credentials	O View API Documentation			
🔲 🖻 Delete	+ New API Creden	tial 😑 🕀		
□ 🕀 ← ArcSight	Last used: 2019-06-17	Last used: 2019-06-17 15:17:04 UTC		
□ ⊕ ← ArcSight Read/Write				

- 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
 Introduction Choose Install Folder Choose Install Set Pick Shortcut Folder Pre-Install Summary Installing Upgrade System Restart Install Complete 	 The ArcSight Installer will guide you through the installation of the ArcSight SmartConnector. The first step installs the core ArcSight SmartConnector components; then you select the ArcSight SmartConnector you wish to configure. ArcSight recommends that you quit all other programs before continuing with this installation. 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.
InstallAnywhere Cancel	Previous Next

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


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

5. Click Next.



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

×	Connector Setup	_		x
र्दे ArcSight	What would you like to do?			
Configure				
	 Add a Connector Set Global Parameters 			
O FOCUS				
	< Previous Next >		Cance	

- 8. Click Next.
- 9. Select ArcSight FlexConnector REST.

*	Connector Setup	
À ArcSight	Select the connector to configure	
Configure		
	Type ArcSight FlexConnector REST]
	< Previous Next	Cancel

- 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 V
			₽ ₽
		< Previous	Next > Cancel

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

*	Connector Setup	- 0	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 		
	k,		
	< Previous Next >	Cano	el

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

*	Co	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.



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	You can now start the SmartConnector by: Going to the services application and starting the service: ArcSight ArcSight FlexConnector REST	
Configure	You can now start the SmartConnector by: Going to the services application and starting the service: ArcSight ArcSight FlexConnector REST	
Configure	You can now start the SmartConnector by: Going to the services application and starting the service: ArcSight ArcSight FlexConnector REST	

29. Select Exit.



*	ArcSight SmartConnector
ÀrcSight □	Install Complete
 Introduction Choose Install Folder Choose Install Set Pick Shortcut Folder Pre-Install Summary Installing Upgrade System Restart Install Complete 	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.

identity Services Engine	Home	Operations	icy • Admini	istration Vork Centers	① License Warn	ing 🔺 🔍
System Identity Management Deployment Licensing Certificat	Network Resources Device Porta tes Logging Maintenance U	/ Management px0 pgrade + Backup 8	Grid Services I & Restore → Ac	Feed Service Threat Cen dmin Access Settings	Click here to do wireless setup and visibi	lity setup Do not
Cal Log Settings	Remote Logging Targets					Colored A
emote Logging Targets	A Edg _APade De Destante				Show All	Selected o 1
ogging Categories	Cor don d'Erstrone	Coste	D	*	Silow M	1
essage Catalog	Name	IP Address 127.0.0.1	Port	UDD Surface	Description	
ebug Log Configuration	O Drofile/DadusDroha	127.0.0.1	20514	Drofiler Curt on	Systog Target for Drofilar DADI	UC Droka
ollection Filters		127.0.0.1	6514	Secure Syston	Secure System Collector	op river.
And a second state of the second s	O TCPLogCollector	127.0.0.1	1468	TCP SysLog	TCP SysLog collector	

- 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.

ululu Identity Convines Engine		
cisco Identity Services Engine	Home → Context Visibility → Operations → Policy Administration → Work Centers Uperations Uperations → Policy	ning 🔺
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Cen Click here to do wireless setup and visi	bility setup
Deployment Licensing Certifical	es	
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 \$14 (Valid Range 1 to 65535)	
	Facility Code LOCAL6	
	* Maximum Length 8192 (Valid Range 200 to 8192)	
	Include Alarms For this Tarnet	
	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)	
lick Submit .		
lick Submit.		
lick Submit.	+	
IiCk Submit. identity Services Engine × ← → C ▲ Not secure identity Services Engine	+ tps://cisco-ise.di.ipdr/admin/#administration_system/administration_system_logging/remote_log	
Iick Submit. identity Services Engine x → C A Not secure N vester identity Services Engine identity Services identity Services identity Services identity Services identity identy identity identy identy identy	+ tps://disco-ise.dl.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log Home Context Visibility Operations Policy Administration Work Centers D License War	
IiCk Submit. identity Services Engine × x → C ▲ Not secure Not secure Not secure identity Services Engine · system · identity Services identity Management · Centered ·	+ tps://cisco-ise.dlipdr/admin/#administration/administration_system/administration_system_logging/remote_log Home → Context Visibility → Operations → Policy Administration → Work Centers ① License War * R * N * N * You have chosen to create an unsecure (TCP/LIDP) connection to the server. Are you sure you want to proceed?	rting ▲
Iick Submit. Identity Services Engine Identity Services Engine Identity Services Engine Identity Services Engine Identity Management Deployment Loensing + Certifical	+ tps://cisco-ise.dlipdr/admin/#administration_system/administration_system_logging/remote_log Home Context Visibility Operations Policy Administration Work Centers ① License War * N * N * You have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?	x tring A bility setup I
Iick Submit. ♦ Identity Services Engine × ♦ ♦ € ▲ Not secure in ender • System • Identity Management Deployment Licensing • Centificat • Centificat	+ tps://cisco-ise.dlipdr/administration/administration_system/administration_system_logging/remote_log. Home Context Visibly Operations Policy Administration Weak Centers 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?	rting ▲ billity setup I
IICK Submit. Statuty Services Engine × C A Not secure № system + Identity Management Deployment Licensing + Certificat	+ tps://cisco-ise.dlipdr/adminix#administration_system/administration_system_logging/remote_log Home Context Visibity Operations Policy Administration Work Centers Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No	rung ▲
IICK Submit. Statuty Services Engine × C A Not secure № System + Identity Management Deployment Licensing + Certificat Control Logging Targets Logging Targets Logging Targets Logging Targets	+ type://cisco-ise.diupdr/administration/administration_system/administration_system_logging/remote_log Home Context Visibity Operations Policy Administration Work Centers Use Context Visibity Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? No Kes N	rung ▲ bility setup t
Iick Submit. Statuty Services Engine × C A Not secure № System + Identity Management Deployment Licensing + Certificat Local Log Settings Remote Logong Targets Logong Categones Message Catalog	+	÷ ↑ ning A bility setup b
Iick Submit. S Identity Services Engine × C A Not secure № *System + Identity Management Deployment Licensing + Certificat Local Log Settings Remote Logong Targets Logong Categories Message Catalog Debug Log Configuration	+	r ☆ hing A bility setup (
Ilick Submit. ♦ Idently Services Engine × ♦ ♦ C ▲ Not secure w • System + Identity Management Deployment Licensing + Certificat Cocal Log Settings Remote Logging Targets Logging Categories Message Catalog Debug Log Configuration Collection Fitters	+ typs://cisco-ise.di.jpdf/administration/administration_system/administration_system_logging/remote_log Home Context Vability Operations Policy Administration Work Centers Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Name Name	r ning ▲ bility setup (
Ilick Submit. Ilick Submit. Ilick Services Engine	+ type://cisco-ise.di.jpdf/administration/administration_system/administration_system_logging/remote_log tome Context Vability Operations Policy Administration Work Centers Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Name Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Name Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Name Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Name Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Name Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Name Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Name Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Note Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Note Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Note Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Note Piccopia Vou have chosen to create an unsecure (TCP/IDP) connection to the server. Are you sure you want to proceed? Note Piccopia Vou have chosen to create an unsecure (TCP/IDP) Note Piccopia Vou have chosen to create an unsecure (TCP/IDP) Note Piccopia Vou have chosen to create an unsecure (TCP/IDP) Note Piccopia Vou have chosen to create an unsecure (TCP/IDP) Note Piccopia Vou have chose	tung A
Ilick Submit. Ilic	+	tring ▲
Ilick Submit. ♦ Identity Services Engine × ← → C ▲ Not secure N • System + Identity Management Deployment Licensing + Certifica Local Log Settings Remote Logging Targets Logging Categories Message Catalog Debug Log Certificantion Collection Filters	+ type://cisco-ise.di.jpdf/admin/#administration_system/administration_system_logging/remote_log tome Context Vability Operations Policy Administration Work Centers Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Policy Vou have chosen to create an un	r r ning ▲ bility setup (
Ilick Submit. ♦ Identity Services Engine × ← → C ▲ Not secure N • System + Identity Management Deployment Licensing + Certifica Local Log Settings Remote Logging Targets Logging Categories Message Catalog Debug Log Certificantion Collection Filters	+ type://cisco-ise.di.jpdf/admin/#administration_system/administration_system_logging/remote_log tome Context Vability Operations Policy Administration Work Centers Work Centers Vou have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed? Note: Placeting and vesting the server of th	r rang A
Ilick Submit. ♦ Identity Services Engine × ← → C ▲ Not secure w • System + Identity Management Deployment Locasing + Certifica Local Log Settings Remote Logging Targets Logging Categores Message Catalog Debug Log Configuration Collection Filters	+ tex://cisco-ise.dl.ipdf/admin/#administration_system/administration_system_logging/remote_log Home Context Visbility Operations Policy Administration Work Centers 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? Norme Administration Status Policy Batters Policy	rt and a setup for
Ilick Submit. ♦ Identity Services Engine × ← → C ▲ Not secure w • System + Identity Management Deployment Locasing + Certificat Local Log Settings Remote Logging Targets Logging Categories Message Catalog Debidg Log Configuration Collection Filters	terre//disco-ise.di.ipdr/admin/#administration_system/administration_system_logging/remote_log torne Context Visability Operators Policy	the sector of th
Licck Submit.	+ tex://cisco-ise.dl.ipdf/sdmin/#administration_vadministration_vystem/administration_vystem_logging/remote_log terme Context Visibility Operations Policy Administration Work Centers	targ à
Lick Submit.	+ tex://cisco-ise.dlipdr/administration/administration_oystem/administration_oystem_logging/remote_log terme Context Visibility Operations Policy Administration Work Centers 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 chos	targ À bilty setup 1
Lick Submit.	+ tex://cisco-ise.dlipdr/administration/administration_system/administration_system_logging/remote_log tome Context Visibility Operations Policy Administration Work Centers Context Visibility Context Visibility Vou have chosen to create an unsecure (TCP/UDP) connection to the server, Are you sure you want to proceed? No Status Context Visibility Code CodA6 Facility Code Fac	rang À bility setup 1

10. Click Yes.

2.21.2 Select Logs for Forwarding

1. Navigate to System > Logging > Logging Categories.

🍘 Identity Services Engine 🛛 🗙	€		
← → C ▲ Not secure http:	<mark>s://cisco-ise.di.ipdr</mark> /admin/#administration/a	dministration_system/administration_system	n_logging 🟠 👶
dealle Identity Services Engine	lome → Context Visibility → Operations	Policy Administration Work Cent	ers
▼System → Identity Management → N	Network Resources	nt pxGrid Services + Feed Service + Three	at Cen Click here to do wire
Deployment Licensing + Certificates	← Logging	ackup & Restore + Admin Access + Settings	;
0	O AAA Audit	AAA Audit	LogCollector
acal Los Settinas	0	Failed Attempts	LogCollector,ProfilerRadiu
Jocar Eog Octaings	0	Passed Authentications	LogCollector,ProfilerRadiu
Remote Logging Targets	O AAA Diagnostics	AAA Diagnostics	LogCollector
.ogging Categories	0	Administrator Authentication and Authorization	ArcSight
Message Catalog	0	Authentication Flow Diagnostics	
Debug Log Configuration	0	Identity Stores Diagnostics	
coug cog comignation	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
	• k	RADIUS Accounting	cryptonite,cryptonite2,Log
	0	TACACS Accounting	LogCollector
	O Administrative and Operational Audit	Administrative and Operational Audit	LogCollector

2. Select a log file to forward to ArcSight.

3. Click Edit.

cisco Identity Services Engine	Home ► Context	Visibility	s Folicy	 Administration 	Work Centers	
System Identity Management Deployment Licensing Certificat	Network Resources es Logging Ma	Device Portal Managen intenance Upgrade	nent pxGrid Ser Backup & Restor	vices Feed Servi re Admin Access	ce I Threat Cen I Settings	Click here to do wire
Local Log Settings Remote Logging Targets Logging Categories Message Catalog Debug Log Configuration Collection Filters	Logging Categories L Logging Categori Name Log Seventy Level Local Logging Targets	ist > RADIUS Accounting TY RADIUS Accounting INFO (Log level can not be cha Available:	anged.)	Selected		
		SecureSyslogCollector	* >	ArcSight cryptonite cryptonite2 LogCollector	*	

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**.

	de	Semperis				Domain: DI.IPI	DR 🔹 I	Apministrator	C LOGOUT
	Current Do	main:	GENERAL	DS PROTECTOR AGENTS	PERMISSIONS	SIEM INTEGRATION			
	DLIPDR		AUDIT AGENTS	AUDIT. COLLECTORS	AUDIT				
	2	ITEMS	👩 Enable SysLog						
		DELETED	Syslog Server						
			Primary Syslog Serve	er: backupserv di ipo	r Primary S	yslog Port: 514	TCP O I	JDP	
		CONFIGURATION PARTITION	TLS				1		
	-		Secondary Sysio	g Server: SERVER	Sec	condary Syslog Port: 514	۲	TCP 🔿 UDP	
		DNS	TLS						
	-		Change Event Pollin	g Frequency 10	minutes				
	9		Change Event Filter	ng					
			5 13			Include these events:			
	\odot	REPORTS	Operations 1	All (O items sele	(ted) •	AD Changed Item	5		
	-		Object Classes	All (O items sele	tted) •	Partitions	All	•	
		801	Attributes	All (O items sele	tted) •	DNS			
	141	STATUS				Send Operations I	.og to SysLog		
		OPERATION LOG	SAVE						
	•	SETTINGS							
ick Sav	e.								
S	SUCC	ess							
SysLog	conf	iguration ha	əs been səv	ed.					
		-							
								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 💷 0 📌 😖
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	Ì
NO Data FOUND	There are no alerts	to display.
dvanced Filter		
(AND) 🛛 🖓 🕂 🗁	Set Up Rules for Alerts	Go to Summary Page
(OR) 🖓 🗄 🙀 🔁 🗙		
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 Authent	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		TCP •	×
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**.

more Normeanonagy				
	Local	Email	SNMP	Remote Syslog
Miscellaneous	2		8	
System Events	8			×
User Events	2	0		
Playback Events	8	0	0	
Capture Events	8	0		
Report Events	8			
Hardware Events	8			
Unclassified	8	0	0	2
Alert Events	8	0		×
indexing Events	2			
Enrichment Events	2			0
indicator Events	×			0
Rule Events	8	0	0	R
Anomaly Events	2	0		

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.

<u>, </u>	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 Datals Annotations Payload Event Datals Annotations Payload Event Value

- 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.

ArcSight Console 7.0.0.2436.1 [arcsight-e	sm:adm	nistrator.ast] Trial license	. Customer	: ARST-Partner, Ex	piration date:	2019/08/01	_	
e Edit <u>Vi</u> ew <u>Wi</u> ndow <u>T</u> ools <u>S</u> ystem <u>H</u> elp								
▷ 🛱 🐘 🖄 🖬 🛍 🗶 🔍 🚺 🚺 🖡 🖬 🖬 🔛 🕨 树 🗌	. 🛃 🖶	I I I I I I -	i 🦉 👪 🖹	💥 🕵 📑 🚳 📓	i 🕒 🛤	ia,		
avigator	d' ? ¥	Viewer	₫?×	Inspect/Edit				
esources Packages Use Cases				Event Inspector	Target:Blue Coal	Security Anal		
Thegration Commands Ctrl+Alt+C	→			Attributes Integra	tion Parameters	lotes		
ammande Targets Configurations				🕂 Add 🗙 Remove				
ommanos raigeo conriguracions				Parameter	Туре		/alue	
iortcuts				SAHost	text		192.168.2.42	¢ –
				SAMinutee	text			
administrator's Integration Targets				SAStartTime				
- To Shared				SAEndTime	text			
🖹 🚈 All Integration Targets								
🗈 🥅 ArcSight Activate								
ArcSight Foundation								
ArcSight Solutions								
Image: Provide the second s								
Blue Coat Security Analytics		Viewers						
🗉 🥅 Downloads		VIEWEIS						
🔁 🧮 Personal								
						Cancel	0 moly	
							мррну	

- 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.



3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.

*	ArcSight SmartConnector
ArcSight	Choose Install Folder
 Introduction Choose Install Folder Choose Install Set Pick Shortcut Folder Pre-Install Summary Installing Upgrade System Restart Install Complete 	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	_ D 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.curre realtime None processed	nt.log
		₿ 	
		< 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	_ D X
文 ArcSight	Enter the destination para	meters	
Configure			
K.	Manager Hostname	arcsight-esm	
	Manager Port	8443	
	User	administrator	
	Password	•••••	
	AUP Master Destination	false	~
	Filter Out All Events	false	~
	Enable Demo CA	false	~
	k.		
	. 0	< Previous Next >	Cancel

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

*		Connector Setup		_ D X
ArcSight	Enter the connec	tor details		
Configure				
	Name Location DeviceLocation	Glasswall Inbound SMTP Ana	lysis	
	Comment			
			C Dravieura N	test > Concel
			< Previous N	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	_ D X
ArcSight Configure	Specify the service parameters		
	Service Internal Name Service Display Name Start the service automatically	glasswall_inbound_smtp GlasswallInbound SMTP Yes	 v
	<i>k</i> ₀		
	·	< 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
 Introduction Choose Install Folder Choose Install Set Pick Shortcut Folder Pre-Install Summary Installing Upgrade System Restart Install Complete 	Where would you like to create product icons? In a new Program Group: ArcSight SmartConnectors In the Start Menu On the Desktop In the Quick Launch Bar Other: Don't create icons Create Icons for All Users
InstallAnywhere Cancel	Previous Next

5. Click Next.



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

×	Connector Setup	- 0	x
🖈 ArcSight	What would you like to do?		
Configure			
K.			
	Add a Connector Set Clobal Decembers		
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.

×		Connecto	or Setup				
ArcSight	Enter the param	neter details					
	Network Port IP Address Protocol Forwarder	6514 (ALL) UDP false					
				ß			
				< Previous Nex	<t></t>	Cance	el

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					
	Manager Hostname	arcsight-esm			
	Manager Port	8443]
	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		_ D X
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				
	 Install as a service Leave as a standalone application 			
	< Previous Next >		Cance	

- 24. Click Next.
- 25. Enter a service name and display name.

*	Connector Setu	p	_ _ ×
À ArcSight	Specify the service parameters		
Configure			
2			
	Service Internal Name arc_system Service Display Name Syslog U	D ^p Daemon	
	Start the service automatically Yes		~
		< Previous Ne	ext > Cancel
Click Next.			
*	Connector Setu	р	_ D X
À ArcSight	Install Service Summary		
Configure	The ArcSight SmartConnector is now co	onfigured to run as a serv	ice.
	You can now start the SmartConnector	by:	
K.	ArcSight Syslog UDP Daemon	rung me service.	
- K			

- 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:" fold	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
Please select an ArcSight Comm Email QualysGuard SNVP Trap StealthWatch A Syslog Message	action type: n Event Format (CEF) ppliance Syslog Message (Legacy)	
Help	ОК	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 Ard	Sight Common Event Format (CEF) Acti 💌
Action	
Name:	ArcSight CEF
Description:	Send to ArcSight.
Concilia da	
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				1
Rules	Name 1 ArcSight CEF	Type ArcSight Common Event Format (CEF)	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 Material Actions	Rule Image: Provide the set of
20.	Click Act	Cancel Cot Cancel tions. Add Host Alarm Rule
	Rule Actions	Actions Execute the following actions when the Alarm becomes active Name
	Help	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.

2		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	mes ir	Add	Remove
	Execute the followi	ing actions when the Type	e Alarm beco	mes ir	Add	Remove
	Execute the followi Name 1 ArcSight CEF	ng actions when th Type ArcSight Common Event Format (CEF)	e Alarm becor Enabled	mes ir ¢	Add nactive Description Send to ArcSight.	Remove
	Execute the followi	ng actions when the Type \$ ArcSight Common Event Format (CEF)	e Alarm becon Enabled	nes ir	Add Description \$ Send to ArcSight.	Used by Rules
	Execute the follows Name 1 ArcSight CEF	ng actions when th Type \$ ArcSight Common Event Format (CEF)	e Alarm becon Enabled	nes ir	Add Description Send to ArcSight.	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
ΝΤΡ	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