

DRAFT NISTIR 8183A
Volume 2

Cybersecurity Framework Manufacturing Profile
Low Security Level Example
Implementations Guide:
Volume 2 – Process-based Manufacturing System Use Case

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Jeffrey Cichonski
Neeraj Shah
Wesley Downard

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8183A-2-draft>

DRAFT NISTIR 8183A
Volume 2

Cybersecurity Framework Manufacturing Profile
Low Security Level Example
Implementations Guide:
Volume 2 – Process-based Manufacturing System Use Case

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Intelligent Systems Division
Engineering Laboratory

Neeraj Shah
Strativia, LLC
Largo, Maryland

Jeffrey Cichonski
Applied Cybersecurity Division
Information Technology Laboratory

Wesley Downard
G2, Inc.
Annapolis Junction, Maryland

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8183A-2-draft>

May 2019



U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

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

National Institute of Standards and Technology Internal Report 8183A, Volume 2
401 pages (May 2019)

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8183A-2-draft>

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

Public comment period: *May 28, 2019* through *July 8, 2019*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: CSF_Manufacturing_Profile_Implementation@nist.gov

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

Abstract

This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented in process-based manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile [4] Low Security Level. The example proof-of-concept solutions include measured network, device, and operational performance impacts observed during the implementation. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they may voluntarily implement. The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to compliment but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

Keywords

Computer security; Cybersecurity Framework (CSF); distributed control systems (DCS); industrial control systems (ICS); information security; manufacturing; network security; programmable logic controllers (PLC); risk management; security controls; supervisory control and data acquisition (SCADA) systems.

Supplemental Content

Additional volumes of this publication include:

Draft NISTIR 8183A Volume 1, *Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 1 – General Implementation Guidance*. <https://doi.org/10.6028/NIST.IR.8183A-1-draft>

Draft NISTIR 8183A Volume 3, *Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case*. <https://doi.org/10.6028/NIST.IR.8183A-3-draft>

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication. A special acknowledgement to the members of the ISA99, Industrial Automation and Control Systems Security Committee and the Department of Homeland Security Industrial Control System Joint Working Group (ICSJWG) for their exceptional contributions to this publication.

Note to Reviewers

This 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 [CSF Manufacturing Profile Implementation@nist.gov](mailto:CSF_Manufacturing_Profile_Implementation@nist.gov).

130

Call for Patent Claims

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

137

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

140

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

143

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

147

148 i) under reasonable terms and conditions that are demonstrably free of any unfair
149 discrimination; or

150

151 ii) without compensation and under reasonable terms and conditions that are
152 demonstrably free of any unfair discrimination.

153

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

159

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

162

163 Such statements should be addressed to: CSF_Manufacturing_Profile_Implementation@nist.gov

Table of Contents

164			
165			
166	Executive Summary	vii	
167	1. Introduction	1	
168	1.1 Purpose and Scope	1	
169	1.2 Audience	2	
170	1.3 Document Structure	2	
171	2. Process-based Manufacturing System Low Security Level Use Case	3	
172	2.1 Introduction	3	
173	2.2 Process-based Low Security Level Use Case	3	
174	3. Policy and Procedure Implementations	8	
175	3.1 Security Program Document Example	8	
176	3.2 Security Policy Document Example	20	
177	3.3 Standard Operating Procedures Document Example	35	
178	3.4 Risk Management Document Example	65	
179	3.5 Incident Response Plan Document Example	75	
180	3.6 Incident Recovery Plan Document Example	85	
181	4. Technical Solution Implementations	100	
182	4.1 Introduction	100	
183	4.2 Open-Audit	102	
184	4.3 CSET	118	
185	4.4 GRASSMARLIN	125	
186	4.5 Wireshark	135	
187	4.6 Veeam Backup and Replication	143	
188	4.7 Security Onion	159	
189	4.8 Cisco AnyConnect VPN	174	
190	4.9 Microsoft Active Directory	207	
191	4.10 Symantec Endpoint Protection	247	
192	4.11 Tenable Nessus	262	
193	4.12 NamicSoft	272	
194	4.13 The Hive Project	282	
195	4.14 Microsoft EFS	291	
196	4.15 GTB Inspector	303	
197	4.16 Graylog	322	
198	4.17 DBAN	340	
199	4.18 Network Segmentation and Segregation	344	
200	4.19 Network Boundary Protection	348	
201	4.20 Managed Network Interfaces	362	
202	4.21 Time Synchronization	370	
203	4.22 System Use Monitoring	374	
204	4.23 Ports and Services Lockdown	379	

205	4.24 Media Protection	384
206		
207	Appendix A - Acronyms and Abbreviations	387
208	Appendix B - Glossary.....	388
209	Appendix C - References.....	392
210		

Executive Summary

This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented in process-based manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile [4] Low Security Level. The example proof-of-concept solutions include measured network, device, and operational performance impacts observed during the implementation. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they may voluntarily implement.

The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to compliment but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

The CSF Manufacturing Profile focuses on desired cybersecurity outcomes and can be used as a roadmap to identify opportunities for improving the current cybersecurity posture of the manufacturing system. The Manufacturing Profile provides a prioritization of security activities to meet specific business/mission goals. Relevant and actionable security practices that can be implemented to support key business/mission goals are then identified.

While the proof-of-concept solutions in this guide used a suite of commercial products, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Each organization's information security experts should identify the products that will best integrate with their existing tools and manufacturing system infrastructure. Organizations may voluntarily adopt these solutions or one that adheres to these guidelines in whole, or can use this guide as a starting point for tailoring and implementing parts of a solution. This guide does not describe regulations or mandatory practices, nor does it carry any statutory authority.

1. Introduction

The Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” [1] directed the development of the voluntary Cybersecurity Framework that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk [1] for those processes, information, and systems directly involved in the delivery of critical infrastructure services.

The Cybersecurity Framework is a voluntary risk-based assemblage of industry standards and best practices designed to help organizations manage cybersecurity risks [2]. The Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without imposing additional regulatory requirements.

To address the needs of manufacturers, a Manufacturing Profile [4] of the Cybersecurity Framework was developed, through collaboration between government and the private sector, to be an actionable approach for implementing cybersecurity controls into a manufacturing system and its environment. The Profile defines specific cybersecurity activities and outcomes for the protection of the manufacturing system, its components, facility, and environment. Through use of the Profile, the manufacturer can align cybersecurity activities with business requirements, risk tolerances, and resources. The Profile provides a manufacturing sector-specific approach to cybersecurity from standards, guidelines, and industry best practices.

1.1 Purpose and Scope

Many small and medium sized manufacturers have expressed that they are challenged in implementing a standards-based cybersecurity program. This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are available today can be implemented in manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile Low Security Level. Example proof-of-concept solutions with measured network, device, and operational performance impacts for a process-based manufacturing environment (Volume 2) and a discrete-based manufacturing environment (Volume 3) are included in the guide. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they may voluntarily implement. The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

While the proof-of-concept solutions in this guide used a suite of commercial products, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Each organization’s information security experts should identify the products that will best integrate with their existing tools and manufacturing system

infrastructure. Organizations may voluntarily adopt these solutions or one that adheres to these guidelines in whole, or can use this guide as a starting point for tailoring and implementing parts of a solution. This guide does not describe regulations or mandatory practices, nor does it carry any statutory authority.

This project is guided by the following assumptions: The solutions were developed in a lab environment. The environment is based on a typical small manufacturer. The environment does not reflect the complexity of a production environment. An organization can access the skills and resources required to implement a manufacturing cybersecurity solution.

1.2 Audience

This document covers details specific to manufacturing systems. Readers of this document should be acquainted with operational technology, general computer security concepts, and communication protocols such as those used in networking. The intended audience is varied and includes the following:

- Control engineers, integrators, and architects who design or implement secure manufacturing systems.
- System administrators, engineers, and other information technology (IT) professionals who administer, patch, or secure manufacturing systems.
- Managers who are responsible for manufacturing systems.
- Senior management who are trying to understand implications and consequences as they justify and implement a manufacturing systems cybersecurity program to help mitigate impacts to business functionality.
- Researchers, academic institutions and analysts who are trying to understand the unique security needs of manufacturing systems.

1.3 Document Structure

Volume 2 is divided into the following major sections:

- Section 2 provides an overview of the process-based manufacturing system use case.
- Section 3 provides the detailed policy and procedure documents developed for the process-based manufacturing system use case.
- Section 4 provides the detailed technical capability implementations and associated performance measurements for the process-based manufacturing system use case.
- Appendix A provides a list of acronyms and abbreviations used in this document.
- Appendix B provides a glossary of terms used in this document.
- Appendix C provides a list of references used in the development of this document.

2. Process-based Manufacturing System Low Security Level Use Case

2.1 Introduction

This use case is a proof-of-concept solution demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented in a manufacturing environment to satisfy the requirements in the CSF Manufacturing Profile Low Security Level. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of proof-of-concept solution they may voluntarily implement.

2.2 Process-based Low Security Level Use Case

The fictional company, Westman Chemical (i.e. Westman), is a chemical manufacturer producing commercial grade chemical products for use in the transportation, building and construction, and other industrial products. It is headquartered in Westland, a city with population of about 100,000 people.

Westman operates its manufacturing facility 24 hours per day, 7 days per week (24/7), with the exception of a schedule maintenance shutdown for about 2 weeks every year, typically scheduled at the end of December.

To increase industrial competitiveness, Westman has introduced process automation equipment to improve the production efficiency and to lower production costs. Industrial automation equipment like programmable logic controllers (PLC), human-machine-interfaces (HMI), and data historians are deployed in the factory to monitor and control the production operation.

2.2.1 Mission

To supply high quality chemical products for industrial application.

2.2.2 Facility

Westman facility is a single building about 50,000 square foot, with about 35,000 square foot of manufacturing space which includes the production space, a distribution facility, and several above ground chemical storage tanks. The remainder of the facility contains the administrative and engineering office space.

The perimeter of the facility is fenced, and the main entrance has gate that is open during business hours and is locked after hours. There are two entrances to the main building. One is for employee's access and is protected by a badge access system. Employees must swipe their assigned badge to enter the building. The other entrance is located at the front lobby, staffed by a receptionist during normal business hours. Guests and visitors are required to sign in and receive proper identification before entering the building or facility. The Westman facility does not have any contracted security guards at the gate or entrances.

2.2.3 Employees

Westman Chemical has 200 full-time employees, with most of the employees working on the manufacturing floor. A small team of full-time manufacturing/control engineers responsible for the manufacturing, control and automation equipment controlling manufacturing process. Their mission is to ensure the safe and efficient operation of the production system.

Westman also has a small team of full-time IT personnel responsible for the enterprise IT systems.

Westman Management position and responsibility:

Westman Management	Major Responsibility
CEO/General Manager	Oversight of the company
Director of Operations	Oversight of manufacturing operations. Management of the manufacturing staff and control engineers. Reports to the CEO/General Manager.
Director of Product Development	Oversight of product development. Management of the on-site chemists. Reports to the CEO/General Manager.
Director of Marketing	Oversight of marketing and sales. Reports to the CEO/General Manager.
Controller/Finances	Manager of finance staff. Reports to the CEO/General Manager.
General Counsel	Handles all legal matters. Reports to the CEO/General Manager.
IT Manager	Manager of IT staff. Reports to the CEO/General Manager.
HR Manager	Manager of human resources staff. Reports to the CEO/General Manager.

2.2.4 Supply Chain

Raw materials are utilized continuously to support the continuous operation of the manufacturing process. Raw materials are typically supplied through a long-term contract established with suppliers and are transported to the facility on a regular basis.

The end products are typically sold to customers in large quantity. Delivery is sub-contracted to several logistics companies which will handle the transportation from the Westman facility to the end customers. Westman's products are typically used as raw materials or additives in chemical processes performed by other industrial manufacturers.

2.2.5 Supporting Services

The supporting services required by Westman are electricity, natural gas, water, and Internet. The broadband Internet connection is a business class service provided by a large national provider with business class service level agreement.

2.2.6 Legal and Regulatory Requirements

As a chemical manufacturer, Westman and its employees are required to comply with all federal and state legal and regulatory requirements for chemical and hazardous materials. Westman is also required to comply with all legal, regulatory and safety requirements.

2.2.7 Critical Infrastructure

The chemical sector is considered as a critical infrastructure under the Presidential Policy Directive 21 (PPD-21).

2.2.8 Manufacturing Process

The manufacturing system consists of five major chemical processing components: a reactor, a product condenser, a vapor-liquid separator, a recycle compressor, and a product stripper to separate the end products. The manufacturing system has 12 valves for controlling the flow of chemicals through the system, and 41 sensor measurements for monitoring the chemical process. All valves and sensors are connected to the automation equipment (PLCs) through a DeviceNet communications bus. Valves are equipped with manual overrides, enabling workers to override the automation equipment during an emergency.

Raw materials are fed to the reactor where the materials are mixed and the main reaction takes place. Output from the reactor flows downstream to the product condenser and the vapor-liquid separator. Any output from the reactor still in the gaseous form is recycled through a compressor and fed back into the main reactor. All condensed components continuously flow to the product stripper separate the components into the final products. Quality assurance samples are taken at various stage of the process to validate the product quality and process efficiency.

2.2.9 Systems

The administrative office is supported by a small team of IT personnel mainly using general enterprise IT applications (e.g., email, web applications, and enterprise planning applications).

The IT personnel maintains a central file storage that is used to store source code, chemical formulas, drawings, procedures, and diagrams, and is backed up regularly. The product development staff and the manufacturing engineers are authorized to access this storage.

The IT personnel also installed and configured a Historian database on the manufacturing floor to record manufacturing process data. IT personnel is responsible for regular data backup of the Historian, and the manufacturing engineers are responsible for the configuration and operation of the Historian.

2.2.10 Data

Data transferred over, or stored within the company network include:

- PLC program code
- Chemical formulas and calculations
- Workflow and operating manuals and documentation
- Electrical diagrams
- Network diagrams
- Quality Assurance procedures
- Historical production data

NOTE: All data listed above are considered to be proprietary, trade secrets, and/or confidential.

2.2.11 Network

The IT systems within the administrative offices are connected to the corporate network, which is managed by the IT team. The manufacturing floor has a separate network for automation equipment and is managed by the manufacturing engineers.

The manufacturing network consists of a typical Ethernet based TCP/IP network and other industrial protocols, e.g., DeviceNet.

Some of the production equipment vendors required Westman to provide remote access to the equipment. The remote access allows the authorized vendors to connect to the manufacturing equipment to provide maintenance and support.

426 **2.2.12 Mission Objectives**

427 **Maintain Personnel Safety**

428 Westman commits to safe operation of the manufacturing system and to always put personnel
429 safety as its highest priority. All manufacturing process, protocols, automation process and
430 equipment, operating procedures and guidelines are designed to ensure personnel safety.

431

432 **Maintain Environmental Safety**

433 Westman complies to all applicable regulations regarding environment safety. Westman is
434 committed to ensuring environmentally-friendly operation of its manufacturing process and
435 working to reduce its environment footprint. Environmental impact caused by the manufacturing
436 process is measured and reviewed on a quarterly basis.

437

438 **Maintain Quality of Product**

439 Westman has a world-class manufacturing facility and process. It has employed state of the art
440 automation, equipment, and techniques to ensure the high quality of its product. It has developed
441 a quality assurance program using automation equipment, including PLCs, Historian, and high
442 precision sensors operating on a high-speed control network to monitor product quality.

443

444 **Maintain Production Goals**

445 Meeting the monthly production goals is an important objective for Westman, and ensures the
446 supply of products to its customers in a timely fashion. It also maintains financial stability for
447 Westman.

448 Constant 24/7 production enables Westman to plan its manufacturing operation to meet its
449 production goals and customer demand. The investment in automation equipment and skilled
450 professional assists Westman to maintain the monthly production goals.

451

452 **Protect Trade Secrets**

453 Westman is committed to protecting its trade secrets, including product development,
454 manufacturing processes, product quality, and supply chain management.

3. Policy and Procedure Implementations

This section includes example policy and procedure documents and statements that were developed for the fictional company Westman. Each organization's information security experts should identify the policy and procedure documents and statements that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

3.1 Security Program Document Example

Security Program for Westman

Document Owner:	Director of Operations, Westman
------------------------	---------------------------------

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO		4-22-2018
	Legal Counsel		4-23-2018

3.1.1 Purpose

The Information Security Program establishes guidelines and principles for initiating, implementing, maintaining, and improving cybersecurity management for Westman.

This program is designed to:

- Ensure the security and confidentiality of employees and business information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to Westman, its partners, customers, or any member.

In addition, the Director of Operations oversees the development, implementation, and maintenance of the information security program.

3.1.2 Who Should use this Document?

This document is intended to be used by the CEO/General Manager, IT Manager, Director of Operations and any other members as deemed appropriate by the management. It supports an agencies responsibility for implementing a cybersecurity program.

3.1.3 Commitment from Management

Westman's leadership team is committed to the development of this Information Security Program. It fully supports and owns the ultimate responsibility of this program. This commitment involves allocating necessary funding to information security work and responding without delay to new situations. The leadership team will participate in any information security related event as organized.

3.1.4 Organization Overview

Role in the Industrial sector

Westman is a chemical manufacturer producing commercial grade chemical products for use in the transportation, building and construction, and other industrial products.

Westman operates its manufacturing facility 24 hours per day and 365 days per year. To increase competitiveness, Westman has introduced process automation equipment to improve the production efficiency and to lower cost. Industrial automation equipment like Programmable Logic Controller (PLC), Human-Machine-Interface (HMI), and Data Historian are deployed in the factory to control and monitor the production operation.

The chemical sector is considered as a **Critical infrastructure** under the Presidential Policy Directive 21 (PPD-21).

510 **Mission Objectives**

511 **1. Maintain Personnel Safety**

512 Westman commits to safe operation of the manufacturing system and to always put
513 personnel safety as its highest priority. All manufacturing process, protocols, automation
514 process and equipment, operating procedures and guidelines are designed to ensure
515 personnel safety.
516

517 **2. Maintain Environmental Safety**

518 Westman complies to all applicable regulations regarding environment safety. Westman
519 is committed to ensuring environmentally-friendly operation of its manufacturing process
520 and working to reduce its environment footprint. Environmental impact caused by the
521 manufacturing process is measured and reviewed on a quarterly basis.
522

523 **3. Maintain Quality of Product**

524 Westman has a world-class manufacturing facility and process. It has employed state of
525 the art automation, equipment, and techniques to ensure the high quality of its product. It
526 has developed a quality assurance program using automation equipment, including PLCs,
527 Historian, and high precision sensors operating on a high-speed control network to
528 monitor product quality.
529

530 **4. Maintain Production Goals**

531 Meeting the monthly production goals is an important objective for Westman, and
532 ensures the supply of products to its customers in a timely fashion. It also maintains
533 financial stability for Westman. Constant 24/7 production enables Westman to plan its
534 manufacturing operation to meet its production goals and customer demand. The
535 investment in automation equipment and skilled professional assists Westman to maintain
536 the monthly production goals.
537

538 **5. Protect Trade Secrets**

539 Westman is committed to protecting its trade secrets, including product development,
540 manufacturing processes, product quality, and supply chain management.

541 **Role in the Supply chain**

542 Raw materials are supplied through a long-term contract established with suppliers and are
543 transported to the facility on a regular basis.

544 The end products are typically sold to customers on a large quantity. Delivery is sub-contracted
545 to several logistics companies which will handle the transportation from the Westman facility to
546 the end customers. Westman's products are typically being used as raw materials or additive for
547 other industrial manufacturers

548

549 **Communication to Organization**

550 All critical and operational aspects of the Manufacturing system, key resources should be
551 documented in network diagrams, manuals or other artifacts. The documentation will be
552 reviewed on a yearly basis by the Director of Operations with assistance from the IT Manager.
553 This information will be shared with all employees, contractors depending on their role in the
554 Company.

555

556 Critical Manufacturing System Components:

557

558 The following are a list of critical Manufacturing system components:

- 559 • Engineering workstation
- 560 • Supervisory PLC
- 561 • HMI Server
- 562 • OPC and Controller Server
- 563 • Historian Database Server
- 564 • Network devices

565 Supporting Services:

566

567 The supporting services required by Westman are broadband Internet
568 connection, electricity, natural gas, and water supply. The broadband Internet connection is a
569 business class service provided by a large national provider with business class service level
570 agreement

571

572 **3.1.5 Information Security Policy**

573 The purpose of this Information Security Policy is to provide an overview of the policies,
574 standards, procedures and Technical controls that make up Westman's Information Security
575 Program. This policy is developed and executed by the Director of Operations, and has
576 expectations set for protecting Westman's IT and OT assets.

577 **3.1.6 Applicable Laws and Regulations**

578 As a chemical manufacturer, Westman is required to comply with all federal and state legal or
579 regulatory requirements for chemical and hazardous materials. Westman is also required to
580 comply with all legal, regulatory and safety requirements being an employer.

581

582 **3.1.7 Security Organization and Governance**

583 Information security is an inherent part of governance and consists of the leadership,
 584 organizational structures and processes that safeguard Westman's information, its operations, its
 585 market position, and its reputation.

Organizational Role	Security Responsibilities
CEO/General Manager	<ul style="list-style-type: none"> • Reviewing and approving the information security program and supporting policies, at least annually. • Assigning the Director of Operations responsibility for organization's policies and procedures for use of any IT/OT assets, implementation, documentation and for meeting its compliance obligations. • Serve as Point of Escalation for any incidents. • Responsible for data breaches. • Comply with Westman security policy
Controller / Finances	<ul style="list-style-type: none"> • Comply with Westman security policy • Report any security incident and/or concerns to the Director of Operations
Control Engineers	<ul style="list-style-type: none"> • Report any security incident and/or concerns to the Director of Operations. • Help with the security requirements for their specific area. • Comply with Westman security policy • Assist in remediating vulnerabilities if asked by the Director.
Director of Marketing	<ul style="list-style-type: none"> • Comply with Westman security policy • Report any security incident and/or concerns to the Director of Operations
Director of Product Development	<ul style="list-style-type: none"> • Comply with Westman security policy • Report any security incident and/or concerns to the Director of Operations
Director of Operations	<ul style="list-style-type: none"> • Responsible for overall security of all IT/OT assets. • Responsible for remediating vulnerabilities and/or mitigating any risks. • Develop, implement and maintain the Security Program and Security Policy documents. • Act as a liaison between operators, vendors, and management on matters relating to information security. Acting as a liaison between plant operators, vendors and management on matters relating to information security. • Reports to the CEO about the status of the Security Program and security related risks or incidents.

IT Manager and IT Team	<ul style="list-style-type: none"> • Remediate vulnerabilities as directed by the Director of Operations. • Report any security incident and/or concerns to the Director of Operations. • Help with the security requirements for their specific business unit and area of expertise. • Comply with the Security Policy.
Legal Counsel	<ul style="list-style-type: none"> • Handling of any legal questions/issues relating to security incidents. • Handling of any external communications related to security incidents. • Report any security incident and/or concerns to the Director of Operations
HR Manager	<ul style="list-style-type: none"> • Handling of any personnel and disciplinary issues relating to security incidents. • Report any security incident and/or concerns to the Director of Operations

586

587 All employees, contractors and vendors are responsible for ensuring the security, confidentiality,
588 and integrity of information by complying with all corporate policies and procedures

589 **3.1.8 Privacy of Personal Information**

590 Employees should not assume any degree of privacy to information they create or store
591 on Westman's systems. Westman is a private organization and any information stored on its
592 information systems may be subject to disclosure under state law. Westman will disclose
593 information about individuals only to comply with applicable laws, regulations or valid legal
594 requests.

595 **3.1.9 Operational Security**

596 Risk Management:

597 The Organization's Risk Management Strategy can be found in section 3.4 Risk Management
598 Document. The Director of Operations shall conduct yearly risk assessments to identify potential
599 internal and external risks to the security, confidentiality and integrity of Westman.

600 Risk assessment involves evaluating risks and their likelihood along with selecting and
601 implementing controls to reduce risks to an acceptable level. Each risk assessment documents
602 major findings and risk mitigation recommendations.

603 All employees are encouraged to report any potential or existing risks to the Director of
604 Operations. Once the Director of Operations has identified or acknowledged the risks, the next
605 course of action will be determined (e.g., accept the risk, seek assistance from the IT Team,
606 contact a vendor to remediate the risk). Similarly, a vendor or contractor can also notify the

607 Director of Operations if they identify any threats or risks to their equipment. A
608 detailed description of risk notification process can be found in Section 3.4 Risk Management
609 Document.

610 Physical Security:

611 The perimeter of the facility is fenced, and the main entrance has a gate that is open during
612 business hours and locked after hours. There are two entrances to the main building. One is for
613 Employees only which is normally locked, employees need to swipe their personal
614 badges to enter the building. The other entrance located at the front lobby staffed by
615 a receptionist during normal business hours. Guests and visitors are required to sign in with
616 proper identification. Additional details about Physical security requirements are mentioned in
617 the Physical Security Section of the Security Policy document.

618 Personnel security is addressed through pre-employment screenings, adequate position
619 descriptions, terms of employment, and security education and training.

620 Access Control:

621 User access to IT and OT systems is based on the principle of least privilege depending on the
622 user's role in the organization. Proper authorization and approval by the Director of
623 Operations is required prior to granting access or operating any manufacturing system
624 equipment. Sets of controls are in place to restrict access through authentication methods and
625 other technical means. Passwords are managed through a formal process and secure log-on
626 procedures. Sensitive systems are explicitly identified and audited regularly.

627 Appropriate authentication controls are used for external connections and remote users. Physical
628 and logical access to critical infrastructure is controlled. Duties are separated to protect systems
629 and data. Access rights are audited at regular intervals

630 **3.1.10 Security Awareness Training**

631 Security awareness information is provided to new employees at the time of hire. Online
632 resources are provided to educate employees on best practices and the importance of reporting
633 security incidents. Additionally, the Director of Operations will ensure the employee understands
634 their role and responsibilities in Westman's information security program.

635 Any information about potential or existing cyber threats to Westman's systems may be
636 exchanged routinely between the Director of Operations and external vendors. Likewise, any
637 news about email scams, phishing attempts and other malicious actions are posted to inform
638 users of possible threats.

639 **Training for Users and Managers**

640 Employees must perform online computer-based training or classroom-based training per
641 management approval. Below is a list of training options. Trade organization subscriptions to
642 newsletters and magazines will offer more industry specific training classes.

Computer Based Training

- ICS-CERT VLP (Virtual Learning Portal)
<https://ics-cert-training.inl.gov>
- DHS Recommended Training
<https://www.dhs.gov/chemical-sector-training>
- SCADAhacker
<https://scadahacker.com/training.html>
- In Person Training
Sans Industrial Control Systems Training
<https://ics.sans.org/training/courses>

Training for Privileged Users**Privileged Users in the Organizational Use case:**

- **Director of Operations**
 - This user has complete control of the manufacturing process within Westman.
- **IT Manager**
 - This user has complete control of the manufacturing process within Westman.

Responsibilities:

- Any privileged user within manufacturing environment will have two accounts. A primary account used for normal activities, and a privileged “administrator” account for performing privileged functions.
 - Primary accounts are used for normal daily operations.
 - Primary accounts will have same rights as a standard Westman user account (e.g., email access, Internet access).
 - Privileged accounts will have administrative privileges, and must only be used when performing administrative functions within manufacturing system (e.g., system updates of firmware or software, system reconfigurations, device restarts).

Privileged users will adhere to securely using Administrative account when performing duties within manufacturing system. If a privilege account becomes compromised this could have a damaging impact on the manufacturing process.

Training:

- Training for privileged users will include training for regular users. Advance training will be provided from industry trade group specializing in automation process, or other specialty training organization focusing on manufacturing security for ICS environments.

Examples:

- International Society of Automation (ISA) <https://www.isa.org>
- SANS (Information Security Training) <https://www.sans.org>

Training for Third Party contractors

- There are many different training options available. Training can be completed in person at a training facility, or online in a virtual classroom environment. In person training at a facility will have a cost associated and it not always appropriate depending on the level of training required. Online training can also have a cost depending on the level required, but there are also options that are free and provide a good understanding of the difference between a traditional Information Technology (IT) environment and Operations Technology (OT) environment.
- Payed Training Options.
 - <https://www.sans.org/course/ics-scada-cyber-security-essentials> (Offers hands on training with experienced instructors).
- Free Online Training Options.
 - <https://ics-cert-training.inl.gov/learn> (Offers virtual classroom environment at no cost).

3.1.11 Third Party Responsibilities and Requirements

- Third party contractors and vendors are required to be aware of the sensitive information within Westman facility and the steps to ensure propriety information is kept secret.
- Third party contractors and vendors will be re-evaluated yearly from the date of completion of first security compliance check. During this re-certification all objectives listed in the Security Awareness Training section above will be reviewed again to ensure security compliance with original plan.
- Remote connections from third party providers will be conducted using a VPN Connection. All third-party remote connections will be monitored and audited.
- All software and hardware tools used within Westman network will be approved first before service provider can proceed.
- No data shall leave Westman's network without written approval from President.
- Network accounts will be limited to only enabled when needed. Accounts used by service for remote access will require approval before being allowed to connect during normal business hours. Refer to Remote Maintenance Approval process in the Security Policy document for additional details.

3.1.12 Fire and Safety Regulations

- Fire Protection Systems will compile with Local, State, and Federal laws. This is to include Fire Protection Systems specially designed for manufacturing process. Fire Protection System will place emphasis on human safety first and for most, before concern for

manufacturing system. Fire Protection Systems will be checked minimum once per year unless shorter intervals are required from superseding regulations.

- Only Industry approved Environmental Controls will be used within manufacturing systems, to included compliance with all Local, State, Federal laws. Environmental Control will be implemented to place human/community safety first before manufacturing systems.
- Fire protection for a manufacturing environment should be designed to safeguard electrical equipment. Fire Protection should be designed and implemented to protect human life first and equipment second. Installed fire protection systems will be certified compliant with existing/new environment by a licensed and accredited vendor. Check industry standards for any required baselines.

3.1.13 Emergency Power

A short-term uninterruptible power supply (UPS) to facilitate both an orderly shutdown and transition of the organization to a long-term alternate power in the event of a major power loss.

3.1.14 Incident Management

Westman's Incident Response and Recovery Plan describe the detection, analysis, containment, eradication, recovery and review of security incidents. The process for responding to security incident is designated in Incident Response Plan, while the procedures for incident recovery and resilience requirements are defined in the Incident Recovery Plan. Security incidents are managed by the Director of Operations who ensures that security incidents are promptly reported, investigated, documented and resolved in a manner that restores operation quickly and, if required, maintains evidence for further disciplinary, legal, or law enforcement actions. The Incident Response Plan and Recovery Plans are reviewed annually and updated as needed.

Lessons learned from cybersecurity events will be used to revise and improve device detection ability while increasing protection for the organization and manufacturing system.

3.1.15 Information Sharing Plan

Information sharing with outside entities like trade organizations and local, state, and federal agencies can help strengthen cybersecurity. Information sharing, especially when receiving information from other outside entities, will improve Westman's situational awareness, and result in a more secure manufacturing system.

Trade Organizations:

Relationships will be established with trade organizations. These relationships will be used to share information regarding cybersecurity incidents detected within the manufacturing facility. Information shared with trade organizations regarding cybersecurity incidents must have all proprietary information and trade secrets removed. This information will be listed as unclassified. Information regarding a cybersecurity incident containing information relating to

proprietary, customer, or trade secret process will require a Non-Disclosure Agreement before data is transmitted; this would be considered classified information requiring approval from executive management before being sent.

Local Government:

Relationships with any local government organization whose purpose is to share cybersecurity incident data should be established.

State Government:

Relationships with any state government organization whose purpose is to share cybersecurity incident data should be established. Trade organizations should be able to provide contact information for state government incident sharing organizations, if they exist.

Federal Government:

Relationships with federal government agencies whose purpose is to share cybersecurity incident data should be established. Some federal government agencies are listed below.

DHS (CISA) Agency for reporting incidents of Phishing, Malware, Vulnerabilities.

<https://www.us-cert.gov/report>

DHS (NCCIC) Agency for reporting cybersecurity incidents relating to Industrial Control Systems.

<https://ics-cert.us-cert.gov/Report-Incident>

3.1.16 Periodic Reevaluation of the Program

The Security Program document will be continuously updated to reflect changes made to manufacturing system and to improve cybersecurity. Lessons learned will be incorporated to help improve this document in the event a cybersecurity incident occurs.

The Director of Operations shall reevaluate and modify the Program from time to time as deemed appropriate. The Director of Operations shall base such reevaluation and modification on the following:

- The results of the risk assessment and monitoring efforts
- Any material changes to the Westman's operations, business or infrastructure components
- Any cybersecurity incident
- Any other circumstances that the Director of Operations knows or is informed of by the CEO

3.1.17 References

1. Implementing Effective Information Security Program by SANS Resources
<https://www.sans.org/reading-room/whitepapers/hsoffice/designing-implementing-effective-information-security-program-protecting-data-assets-of-1398>
2. InfoSec Program Plan by University of Tennessee Knoxville <https://oit.utk.edu/wp-content/uploads/2015-11-11-utk-sec-prog-plan.pdf>
3. GCADA Sample Information Security Procedure
[http://www.gcada.org/pdf/Sample%20Information%20Security%20Procedure%20\(safeguard%20policy\).pdf](http://www.gcada.org/pdf/Sample%20Information%20Security%20Procedure%20(safeguard%20policy).pdf)
4. IT Security Program by Old Dominion University
<https://www.odu.edu/content/dam/odu/offices/occs/docs/odu-it-security-program.pdf>

3.2 Security Policy Document Example

<p style="text-align: center;">Security Policy for Westman Chemicals</p>

Document Owner:	Director of Operations, Westman
------------------------	---------------------------------

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

3.2.1 Purpose

This Security Policy document defines the security requirements for the proper and secure use of IT and OT services in the organization. The goal of the policies defined within is to protect the organization and its users to the maximum extent possible against cybersecurity threats that could jeopardize their integrity, privacy, reputation, and business outcomes.

3.2.2 Scope

Any employee, contractor, or individual with access to the organization's systems or data.

3.2.3 Policy Maintenance

The Security Policy must be approved by the Director of Operations in consultation with the IT Manager and CEO/General Manager before it can be disseminated to employees. Any updates to this document will must also be approved by the Director of Operations.

This policy document will be reviewed by the Director of Operations on an annual basis and will notify all employees of any updates made to the policy.

3.2.4 Role-based Security Responsibilities

Security responsibilities vary depending on an individual's role in the company. Each is defined below.

Employees

Organizational Role	Security Responsibilities
CEO/General Manager	<ul style="list-style-type: none"> Serve as Point of Escalation for any incidents. Responsible for data breaches. Comply with Westman security policy
Controller / Finances	<ul style="list-style-type: none"> Comply with Westman security policy Report any security incident and/or concerns to the Director of Operations
Control Engineers	<ul style="list-style-type: none"> Often assume responsibility for intrusion detection in Manufacturing system. Report any security incident and/or concerns to the Director of Operations. Help with the security requirements for their specific area. Comply with Westman security policy Assist in remediating vulnerabilities if asked by the Director.
Director of Marketing	<ul style="list-style-type: none"> Comply with Westman security policy Report any security incident and/or concerns to the Director of Operations
Director of Product Development	<ul style="list-style-type: none"> Comply with Westman security policy Report any security incident and/or concerns to the Director of Operations
Director of Operations	<ul style="list-style-type: none"> Responsible for overall security of all IT/OT assets. Responsible for remediating any detected events and vulnerabilities Implement and maintain Security Policy documents.

	<ul style="list-style-type: none"> • Serve as a SPOC for any security related incident and keeping upper management in the loop.
IT Manager and IT Team	<ul style="list-style-type: none"> • Assist in remediating vulnerabilities if asked by the Director of Operations. • Report any security incidents, anomalies detected and/or concerns to the Director of Operations. • Help with the security requirements for their specific area. • Comply with Westman security policy
Legal Counsel	<ul style="list-style-type: none"> • Handling of any legal questions/issues relating to security incidents. • Handling of any external communications related to security incidents. • Report any security incident and/or concerns to the Director of Operations
HR Manager	<ul style="list-style-type: none"> • Handling of any personnel and disciplinary issues relating to security incidents. • Inform Law Enforcement if security incident involves data breach of sensitive information. • Report any security incident and/or concerns to the Director of Operations

838

839 **External Personnel**

Role	Security Responsibilities
Equipment Vendor	<ul style="list-style-type: none"> • Assist in remediating vulnerabilities, upgrading software or hardware as required. • Comply with Westman security policy if called in.
Visitor	<ul style="list-style-type: none"> • Comply with Westman security policy if called in.

840

841 **3.2.5 Employee requirements**

- 842 1. Employees must complete security awareness training and agree to uphold the acceptable
843 use policy.
- 844 2. Employees must immediately notify the Director of Operations if an un-escorted or
845 unauthorized individual is found in the facility.
- 846 3. Employees must always use a secure password on all systems as per the password policy.
847 These credentials must be unique and must not be used on other external systems or
848 services.

4. Terminated employees must return all company records, in any format.
5. Employees must verify with the Director of Operations that authorizations have been granted before allowing external personnel to connect to the IT or OT network.
6. Employees must report any physical security incidents to the Supervisor.
7. Employees must understand and diligently follow the physical security requirements stated in the next section.

3.2.6 Physical Security

1. Employees must always use and display physical identification (ID) provided by the company.
2. IDs must be designed to enable the immediate visual distinction between employees, external personnel, and visitors.
3. Sharing of IDs for any reason is strictly prohibited.
4. A sign-in sheet will be maintained by the receptionist to record all Visitor visits. These log records will be reviewed periodically by the Director of Operations.
5. Any visitors, contractors and/or maintenance personnel must always be escorted by an employee.
6. Unauthorized removal of any documentation, equipment, or media from any device is restricted, unless authorized. Authorization can be obtained from the Director of Operations.
7. All activities of visitors, contractors, and maintenance personnel will be subject to monitoring while onsite. An employee from the IT team will be assigned to monitor all computer activities if the visitor, contractor, or maintenance personnel is connected to any company network.
8. A supervisor will conduct monthly security status monitoring of the company to check for any physical security incidents.

3.2.7 Information Technology (IT) Assets

1. IT assets must only be used for the business activities they are assigned and authorized to perform.
2. Every employee is responsible for the preservation and proper use of the IT assets they have been assigned.
3. IT assets must not be left unduly exposed.
4. Desktops and laptops must be locked if left unattended. This policy should be automatically enforced whenever possible.
5. IT assets must not be accessed by non-authorized individuals. Authorization can be obtained from Director of Operations.
6. Configuration changes are to be conducted through the change control process, identifying risks and noteworthy implementation changes to security management.
7. All assets must be protected by authentication technologies (e.g., passwords).
8. Passwords must follow the password policy.

9. The Director of Operations must be notified immediately after an asset is discovered to be lost or stolen.
10. Use of personal devices to access IT resources is prohibited.
11. Storage of sensitive information on portable media is prohibited, unless authorized by the Director of Operations.
12. Any sensitive information stored on IT assets, or being transported on a portable device, must be protected in such a way to deny unauthorized access, and must be encrypted in line with industry best practices and any applicable laws or regulations.

Description	Quantity
SuperMicro Servers	6
Allen Bradley 5700 Switches	2
Allen Bradley 8300 Router	1
HP Tower Workstation	1

IT Assets Inventory

3.2.8 Operational Technology (OT) Assets

1. OT assets must not be used for operations they are not assigned or authorized to perform.
2. The Director of Operations and Operators are responsible for the preservation and correct use of the ICS assets they have been assigned.
3. Physical access to OT assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provisioning of a service must be authorized by Director of Operations.
4. All personnel interacting directly with OT assets must have proper training.
5. The Director of Operations is responsible for all OT devices. A Control Engineer is solely responsible for maintenance/configuration of the device they are assigned. No other personnel are authorized to modify OT asset configurations, including any modification to interfacing hardware or software.
6. Usage of security tools on the OT network must be approved by the Director of Operations, and all affected Control Engineers must be notified.
7. Concept of least privilege must be followed when authorizing access to OT assets.
8. OT assets, such as PLCs, safety systems, etc., should have their keys in the "Run" position at all times unless being actively programmed.
9. Accessing IT devices or internet use from the OT network, or OT assets, unless authorized, is prohibited.

10. Accessing IT devices or internet use from the OT network, or OT asset, is prohibited.
11. Use of personal devices to access OT resources is prohibited.

Description	Quantity
Allen Bradley ControlLogix PLC	1

OT Assets Inventory

3.2.9 Lifecycle Accountability of assets

- Any IT or OT asset that needs to be decommissioned must be sanitized of all data, as per the manufacturer guidelines. This task will be usually performed by the IT Support staff.
- In case of an employee termination, an IT asset such as desktop PC or laptop must be reimaged prior to assigning it to a different employee.

3.2.10 System Maintenance

- Any maintenance tasks involving external resources such as Vendors, Contractors or other non-employees must be pre- approved by the Director of Operations. This can be coordinated by filling out the Maintenance Order approval form.
- It is the responsibility of Vendors, Contractors and/or Maintenance personnel with access to Westman's resources that due care is ensured to properly secure their own resources.
- It is responsibility of the IT staff that due care is ensured when using vendor devices on networks.
- All systems and/or technical controls must be verified upon the completion of maintenance for any cybersecurity related impact.
- All systems and/or technical controls must be verified upon the completion of maintenance for any cybersecurity related impact.
- All maintenance work details will be logged in a Maintenance Tracker Excel sheet. The Supervisor will update all details of the work performed in the sheet.

3.2.11 Data

- Access to sensitive data must be authorized by Director of Operations.
- Data should not be shared informally. When access to sensitive information is required, personnel can request it from their supervisors and should take all necessary steps to prevent unauthorized access.
- You must immediately notify the Director of Operations in the event a device containing sensitive data is lost (e.g. mobiles, laptops, USB devices).
- It is recommended personnel use encrypted portable media or secure protocols while transferring data across systems. Director of Operations can provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle sensitive data.

5. If you have been permitted to work remotely you, extra precautions must be taken to ensure sensitive data is appropriately protected.
6. Physical copies of data should be stored in a secure location where unauthorized personnel cannot access it.
7. Personnel should ensure physical copies of sensitive data are not left unattended on a printer.
8. Physical copies of sensitive data should be shredded or disposed in a secure manner.

Description	Digital Files	Physical Copies	Databases
PLC program code	✓		
Chemical formulas	✓	✓	
Quality Assurance Procedures	✓	✓	
Operating manuals and documentation	✓	✓	
Electrical diagrams	✓	✓	
Network diagrams	✓	✓	
Historical production data	✓		✓

Data types considered sensitive, proprietary, or containing trade secrets.

3.2.12 Credentials Management

The purpose of this policy is to establish a standard for the creation of strong passwords, protection of those passwords, frequency of change and employee expectations.

All staff, vendors, contractors or other stakeholders who use Westman's IT and OT systems should be given authenticated access to those systems by assigning individual credentials [username and password]. All access and restrictions to those access will be controlled by these credentials.

The creation and removal of IT system accounts is managed via Microsoft Active Directory. In addition, The IT manager will determine and authorize user access to IT or OT systems.

Westman reserves the right to suspend without notice access to any system or service.

3.2.13 Password Policy for Active Directory Accounts

1. All employee and system passwords must be at least 10 characters long and contain a combination of upper-case and lower-case letters, numbers, and special characters.
2. Passwords must be changed every 90 days and cannot match a password used within the past 12 months.
3. Passwords must not be a dictionary name or proper name.
4. Passwords must not be inserted into email messages or other forms of electronic communication.
5. Employees must choose unique passwords for all company accounts and may not use a password that they are already using for a personal account.
6. Whenever possible, use of multi-factor authentication is recommended.
7. Default passwords, such as those preconfigured in newly-procured assets, must be removed before the asset is installed or connected to any organizational network.
8. Sharing of passwords is forbidden.
9. Passwords must not be revealed or exposed to public sight.
10. Personnel must refrain from writing passwords down.
11. Personnel must not use the “remember password” feature prevalent on many applications.

3.2.14 Privileged Accounts**Privileged Users****• Director of Operations**

- This user has complete control of the manufacturing process within Westman.

• IT Manager

- This user has complete control of the manufacturing process within Westman.

Responsibilities

- Any privileged user within manufacturing environment will have two accounts. A primary account used for normal activities, and a privileged “administrator” account for performing privileged functions.
 - Primary accounts are used for normal daily operations.
 - Primary accounts will have same rights as a standard Westman user account (e.g., email access, Internet access).
 - Privileged accounts will have administrative privileges, and must only be used when performing administrative functions within manufacturing system (e.g., system updates of firmware or software, system reconfigurations, device restarts).
- Privileged users will adhere to securely using Administrative account when performing duties within manufacturing system. If a privilege account becomes compromised this could have a damaging impact on the manufacturing process.

1010 3.2.15 Antivirus

- 1011 1. Antivirus software must be installed on all workstations and servers.
- 1012 2. Virus signatures must be updated daily.
- 1013 3. Antivirus software must provide the capability to push signatures on an ad-hoc basis.

1014 3.2.16 Internet

- 1015 1. Internet access is provided for business purposes.
- 1016 2. Limited personal navigation is permitted from IT networks if no perceptible consumption
- 1017 of organizational system resources is observed, and the productivity of the work is not
- 1018 affected.
- 1019 3. Only authorized Internet access from the OT network is permitted. Authorized access can
- 1020 be obtained from Director of Operations.
- 1021 4. Inbound and outbound traffic must be regulated using firewalls in the perimeter.
- 1022 5. All Internal/External communications must be monitored and logged by in-house
- 1023 network security tools. Logs must be reviewed regularly by the IT staffs and any
- 1024 anomalies detected should be reported to the Director of Operations or IT Manager.
- 1025 6. When accessing the Internet, users must behave in a way compatible with the prestige of
- 1026 the organization.

1027 3.2.17 Continuous Monitoring

- 1028 1. Westman will implement a Security Continuous Monitoring program. This will include
- 1029 performing comprehensive network monitoring using Commercial or Open source tools
- 1030 to detect attacks, attack indicators and unauthorized network connections.
- 1031 2. The Manufacturing system will be monitored for any cybersecurity attack indicators or
- 1032 IOC's.
- 1033 3. All External boundary network communications will be monitored.
- 1034 4. All cybersecurity incidents must be logged in the Incident Response Management tool for
- 1035 documentation purposes.
- 1036 5. All Local, State, and Federal detection activities applying to organization or
- 1037 manufacturing system will be followed in accordance within the law. Detection activities
- 1038 are to include any industry regulations, standards, policies, and other applicable
- 1039 requirements.
- 1040 6. Monitoring activity levels will be increased during periods of increased risk and/or any
- 1041 other factors as necessitated by Westman's Management.

1042

7. All cybersecurity events detected will be communicated to the below list of defined personnel identified by the Director of Operations.

Event Severity	List of Personnel
Low (All Events)	Control Engineers
Medium	IT Staff, Control Engineers
High (Requiring Urgent Attention)	IT Manager, Director of Operations

8. Details of cybersecurity events will be shared with ICS-CERT (<https://ics-cert.us-cert.gov/>) to help secure the organization, including helping secure the industry. Cyber + Infrastructure (CISA) is an agency of Department of Homeland Security which provides reporting capabilities for manufactures related to cybersecurity events

3.2.18 External Service Provider Communications:

1. All communications from External Service Providers to Westman's systems will be monitored to ensure work provided by service provider is done correctly, including following all cybersecurity best practices and complying with Westman's security policies. Monitoring will include designated employee to oversee all activities performed.
2. Any Indicator of Compromise (IOC's) detected while monitoring external service provider communications will be reported and escalated via appropriate communication channels. The Director of Operations will reach out to the External service provider upon verifying the threat to discuss and seek an immediate remediation path accordingly.

3.2.19 User Access Agreement

Each employee provided with access to any Westman's resources, including Email and HR system, is required to review and accept the terms of the User Access Agreement.

As an employee of Westman:

1. You may use Westman's IT, OT systems and networks to which you have been granted access for work related purposes only. Accounts and access are granted based on each individual's roles and responsibilities.
2. You should not expect any privacy on Westman's premises or when using Westman's property or networks either when onsite or accessing remotely
3. You will act responsibly to maintain the security and integrity of the information systems that you use, so as to minimize the chance of any problems or security breaches for Westman.

4. You agree to co-operate with any audit by us or our Contractors of your access to the System.
5. You understand your responsibility for respecting other employee's privacy and protecting the confidentiality of information to which you have access, and will comply with all privacy laws, codes and guidelines including,
6. Internet access must not be used for activities that are not authorized under existing laws, regulations, or organization policies.
7. Any company laptops assigned to you should only be used for the purpose of conducting Westman's business. You are expected to take due care while using laptops.
8. All laptops must be returned at the end of employment.
9. You understand that Transmission or intentional receipt of any inappropriate material or material in violation of law or district policy is prohibited. This includes but is not limited to: copyrighted material; threatening or obscene material: material protected by trade secrets; the design or detailed information pertaining to explosive devices: criminal activities or terrorist acts; gambling; illegal solicitation; racism; inappropriate language.
10. You shall be subject to disciplinary action up to and including termination for violating this agreement or misusing the internet.

3.2.20 Remote Access

This policy applies to the users and devices that need access the organization's internal resources from remote locations.

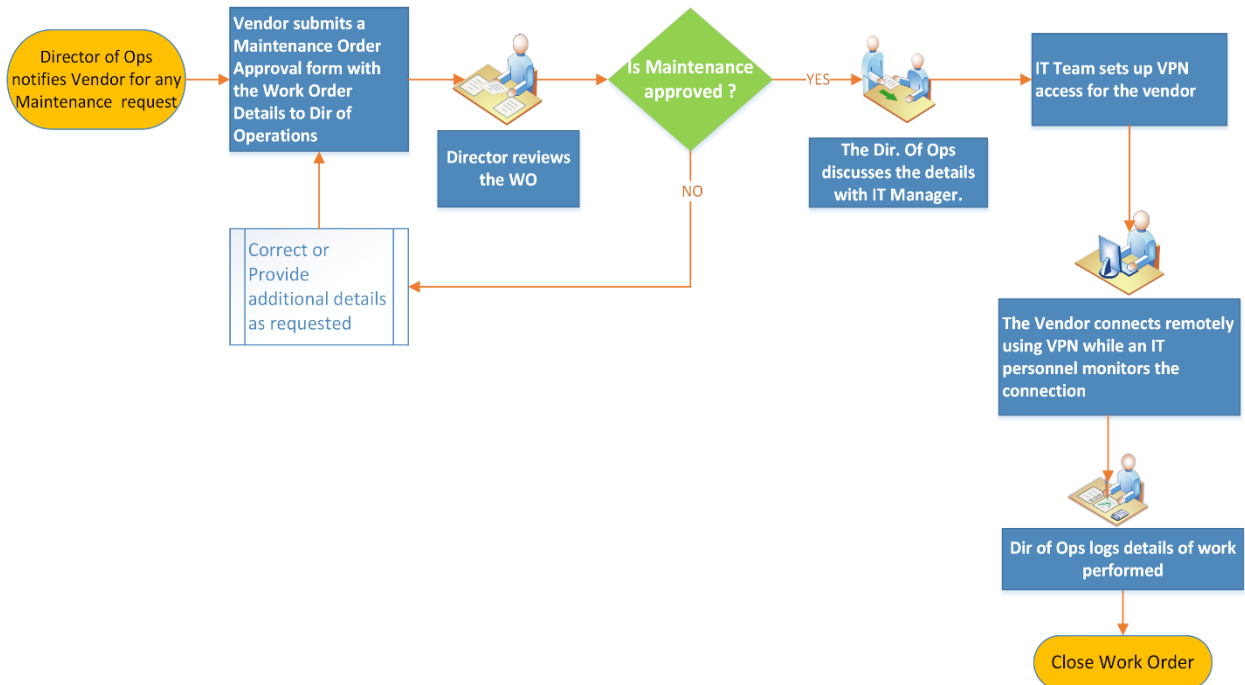
1. Remote access for personnel requires pre-approval by Director of Operations. The IT manager must also be informed. Vendors requesting remote access must be registered with the company and are required to submit all work order details using the Maintenance Order Approval Form.
2. The Director will determine list of authorized users for remote access.
3. Remote access to sensitive or confidential information is not permitted on an unencrypted connection. Exception to this rule may only be authorized in cases where it's strictly required.
4. A VPN account will be setup by the IT Team and credentials shared with the vendor. The Once connected via a VPN, the vendor will be permitted Remote Desktop Access to select systems such as the Engineering Workstation or HMI Server depending on the nature of the task. The access will be disabled upon completion of the work.
5. All activities will be subject to monitoring by IT staff. Monitoring will start and continue until remote session is no longer required, or work has been completed. Appointed individual will indicate when remote session is active and ensure manufacturing system environment has been returned to same state before remote connection was established
6. Installation of any software such as desktop sharing software etc. on authorized devices will be performed by the IT staff.
7. Use of remote access technologies on personal devices is prohibited.

8. All devices connected via remote access technologies must use the most up-to-date anti-virus software and virus signatures.
9. During an onsite visit, all activities will be subject to monitoring. Dedicated IT personnel will be assigned to monitor the vendor over the shoulder while he/she is working off a computer.
10. Split tunneling will be disabled. All internet bound traffic will be directed through Corporate network during a VPN session.

3.2.21 Usage Restrictions

- To avoid confusing official company business with personal communications, employees, contractors, and temporary staff with remote access privileges must never use non-company e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct business.
- No employee is to use Internet access through company networks via remote connection for illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with other existing employee policies.
- Where supported by features of the system, session timeouts are implemented after a period of no longer than 30 minutes of inactivity. Where not supported by features of the system, mitigating controls are implemented.

3.2.22 Remote Maintenance Approval Process



1134 **3.2.23 Maintenance Approval Form**

Maintenance Order Approval Form	
Vendor Name	
Vendor Address	
Vendor Phone number	
Does the Vendor provide support to Westman currently?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Does the Vendor system intended to be used have an Anti-virus installed?	<input type="checkbox"/> YES <input type="checkbox"/> NO
What items will be supported and/or worked upon during this session?	<input type="checkbox"/> PC / Laptops <input type="checkbox"/> Servers <input type="checkbox"/> Control System Devices <input type="checkbox"/> Any other IT/OT Device <input type="checkbox"/> Software Details:
Will any software or program need to be installed on Westman's systems?	<input type="checkbox"/> YES <input type="checkbox"/> NO Details (if YES):
Does this software require licensing to be purchased?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Details of the task to be performed	
Is this a recurring activity	<input type="checkbox"/> YES <input type="checkbox"/> NO
Vendor Signature	
Work Approved (<i>To be filled by Director of Operations</i>)	<input type="checkbox"/> YES <input type="checkbox"/> NO
Director of Operations Signature	

1135

1136 **3.2.24 Communicate Information to Organization**

1137 All critical and operational aspects of the Manufacturing system, key resources should be
 1138 documented in network diagrams, manuals or other artifacts. The documentation will be
 1139 reviewed on a yearly basis by the Supervisor.

1140

1141 This information will be shared with all employees, contractors depending on their role in the
 1142 Company.

1143

1144 **3.2.25 Definitions and Acronyms**

Asset	A device owned by the organization
AV	Anti-virus
AV scanning	The act of scanning a device for viruses
Change control process	A systematic approach to managing all changes made to a product or system. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted and that resources are used efficiently.
Device	Electronic hardware (e.g., machine, computer, laptop, phone, networking equipment)
Employee	An individual directly employed by the organization
External personnel	An individual who is not an employee (e.g., contractor, visitor)
Human machine interface (HMI)	Asset used by personnel to interface and interact with OT (e.g., machines)
ID	Physical identification (e.g., badge)
Industrial control system (ICS)	Typically, the hardware and software used to control processes, or operate machines and manufacturing processes
Information technology (IT)	Hardware devices such as computers, laptops, network switches, firewalls etc.
Least privilege	A user is only authorized to perform the functions necessary to perform their job
Operating system	Software that operates a device (e.g., Windows, Linux); typically, the interface used by the user
Operational technology (OT)	ICS and other devices (typically internetworked) used by the manufacturing process
Personal device	A device owned by an individual; not owned or controlled by the organization

Personnel	All employees and external personnel, excluding visitors
Portable media	USB flash drive, compact disc (CD), external hard drive, laptop
Remote access technologies	Software used to connect a device to the IT or OT network via the Internet, usually performed by personnel located off-site
Sensitive data	Data containing proprietary information or trade secrets pertaining to the operations of the organization; data that could cause damage to the organization if obtained by an attacker
Split tunneling	Split tunneling allows a mobile user access public network (e.g. Internet) and local LAN/WAN Corporate network at the same using same or different network connections
User	Individual using a device
Virus signature	Data used by antivirus software to identify viruses
VPN	Virtual private networking; see 'remote access technologies'.
Vulnerability scanning	Software used to detect common or known vulnerabilities on a device

1145

1146 **3.2.26 References**

- 1147 1. Security Policies by SANS Resources <https://www.sans.org/security-resources/policies>
- 1148 2. Template for Security Policy by Project Management Docs
- 1149 <http://www.projectmanagementdocs.com/template/Security-Policy.doc>
- 1150 3. Data Security Policy by Sophos labs [https://www.sophos.com/en-](https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en)
- 1151 [us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en](https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en)

3.3 Standard Operating Procedures Document Example

Standard Operating Procedures for Westman
--

Document Owner:	Director of Operations, Westman
------------------------	---------------------------------

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

3.3.1 Introduction

This document defines the procedural steps management and employees will follow ensuring consistence daily actives along with response to events occurring within the manufacturing system for Westman. Within this document contains content which should be referred to often ensuring all employees/individuals performing work within manufacturing system are not inadvertently compromising cybersecurity posture by not following Standard Operation Procedures (SOPs).

3.3.2 Purpose

To provide a consistent repeatable process that can be followed to perform tasks within manufacturing system.

1177 3.3.3 Scope

1178 Management, employees, contractors, or individuals requiring access to manufacturing system
1179 for changes should be familiar with the contents included within this document.

1180

1181 IDENTIFY

1182 3.3.4 Asset Inventory

1183 Identifying assets within manufacturing system for Westman is a vital first step in protecting
1184 organization from malicious activities that could result in disruption to production. Westman uses
1185 multiple tools for asset inventory, some manual and some automated. Knowing the environment
1186 and what devices are installed allows the ability to detect non-approved devices on the network
1187 which could be an indication of malicious activity. Keeping devices updated with the latest
1188 patches ensure to mitigate potential weakness within manufacturing system. All patches will be
1189 carefully examined to determine if there could be any performance impact effecting production
1190 within manufacturing system.

1191 Manual

1192 Devices not able to be automatically scanned will be added to the Excel spreadsheet and updated
1193 quarterly. Devices included in manual process would be PLC and machine stations, including
1194 any additional devices that are unable to be scanned automatically with a tool. All inventory will
1195 be conducted during manufacturing system planned down time and inventory will include
1196 hardware and software.

1197 Automated

1198 Devices with the ability to be scanned will be added to Westman's asset inventory tool and
1199 scanned quarterly. Scanning quarterly will ensure manufacturing process is not affected. All
1200 scanning should be performed when manufacturing system has been placed into a non-
1201 production mode (system down time). Westman has chosen an asset inventory tool that has
1202 multiple version from open source to enterprise edition. Westman has selected Enterprise edition
1203 since this version provides the ability to schedule scans, baseline systems for monitoring
1204 changes. For additional information and references see.

1205 Westman inventory management tools will be configured for group access to ensure only
1206 individuals requiring access are allowed. This ensure that people within the organization only
1207 requiring read accesses are not granted a higher level, which could lead to inadvertent changes to
1208 tools configuration. See reference for how groups are created.

1209 Scans of manufacturing system will be conducted quarterly ensuring not to effect manufacturing
1210 process. Scans will audit software including license information, version, and configuration.
1211 Devices within the manufacturing systems will have software inventory audited and reviewed
1212 quarterly. Changes occurring to devices' software before the next update will trigger a required

1213 inventory to remain compliant. See reference for additional details for performing scanning
1214 within manufacturing system.

1215 Westman will apply updates to asset inventory software as they become available. Updates are
1216 required to keep system free from known vulnerabilities while including new features. See
1217 reference for additional information

1218 **3.3.5 Network Baseline**

1219 Network baseline is important as it provides the ability to detect malicious active occurring on
1220 manufacturing system network. Westman will periodically perform baseline scans to identify any
1221 unusual traffic, which could be indication of malicious activity. All traffic observed during
1222 scanning should be reconciled to help create a more secure network. See reference for network
1223 baseline performed.

1224 **3.3.6 External Connections**

1225 Using company provided network diagram tools all network connection for external
1226 communication will be mapped. Mapping will include all relevant information for connection
1227 service provided. Example of information required would be assigned IP address for device
1228 providing service, support phone number, customer number, person of contact, and support level
1229 agreement and hours. External providers will include cloud services. Network diagram will be
1230 updated quarterly.

1231 **3.3.7 Baseline Configurations**

1232 Baseline configurations was captured using two methods since some ICS devices don't allow
1233 automated tool scanning; for these devices' spreadsheet tracking is the preferred method.
1234 Devices lacking SSH, SNMP, WMI ability will require manual entry in spreadsheet.

1235 Steps used to perform automated scanning for Westman.

1236 Baseline configurations Westman implemented within Manufacturing systems helps to ensure
1237 inadvertent changes are detected before systems' integrity has been compromised.

1238 Open-Audit¹ has been chosen for Westman due to scalable configuration depending on
1239 required needs. Instruction are listed for performing scanning. Once scanning has been
1240 performed changes with ICS devices are detectable by running reports identifying new software
1241 changes.

1242 Manufacturing systems was scanned to get initial baseline. Scanning steps used are listed below.
1243 Completed scans result scan be exported to CSV file for storage. See end of instructions for
1244 exported configuration.

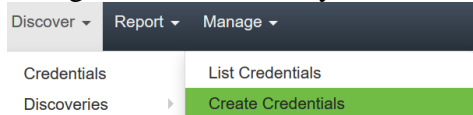
¹ Open-Audit: <https://www.open-audit.org>

1245 **Open-Audit Configuration steps within Process Control System once system has been**
1246 **installed**

1247 **Initial Configuration:**

1248 • Login to Open-Audit via web portal

1249 • Navigate to → Discovery → Credentials → Create Credentials



1250

1251 • Credentials can be assigned to any organization that has already been created. If you want
1252 credentials to only apply to specific organizational group, then select that from the
1253 appropriate drop-down during credential creation and select the desired group these
1254 credentials will apply to.

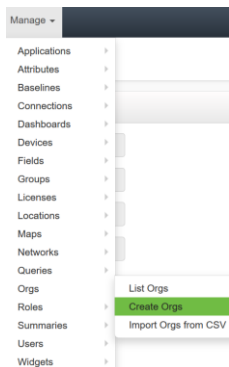
1255 • Our environment consists of mainly Windows machine, so Windows will be used for
1256 connection type.

1257 • Now create a credential and select **Windows** for the type. Once completed click **Submit**.

1258

1259 **Organization Groups Creation:**

1260 • Click on Manage → Orgs → Create Orgs



1261

- 1262 • Now enter **Name:** **Description:** and click submit at the bottom of the page to save.

Name PCS Machines ?

Description Process Control Machines ?

Parent ID Default Organisation ?

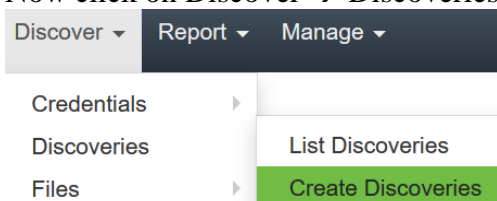
Type Organisation ?

1263

- 1264 • If you have multiple machines / equipment in different locations you can make
1265 Organizational groups based on business units, or related task.

1266 Configure Discovery Scan:

- 1267 • Now click on Discover → Discoveries → Create Discoveries



1268

- 1269 • Enter a meaningful name for discover being created

Name PCS Scans ?

1270

- 1271 • Next, enter the subnet that'll be used for performing this scan. This scan is using
1272 172.16.0.0/22 Subnet 172.16.0.0/22 ? **Search online for additional subnetting**
1273 **information / calculators if you'd like to learn more.**

- 1274 • **Network address:** should already be defaulted to Open-Audit installed location, if this
1275 is not true, click the drop-down arrow and select your installed location.

- 1276 • Now, click on the advanced button to see more options.

- 1277 • Once **Advanced** has been expanded you'll have additional options to select if desired.
1278 These options are **Org, Type, Devices Assigned to Org,** and **Devices Assigned to**
1279 **Location.** These options aren't required but allow you to organize found devices into
1280 groups.

- 1281 • Once all are selected click on **Submit** button to continue.

1282 **Discoveries:**

- 1283 • Once the above steps have been completed clicking on **Submit** button you'll be taken to
1284 a new webpage that will allow you to run discovery process created in the previous step.

- 1285 • To start discovering devices click on **green** arrow button. If you need to verify details for
1286 this scan click on the button that looks like an **eye**: finally, if you need to delete this scan
1287 click on the **trash** can icon to the right. See screen shot for details.



- 1289 • Once discovery has started you'll be taken to a new page allowing you to view status or
1290 cancel.

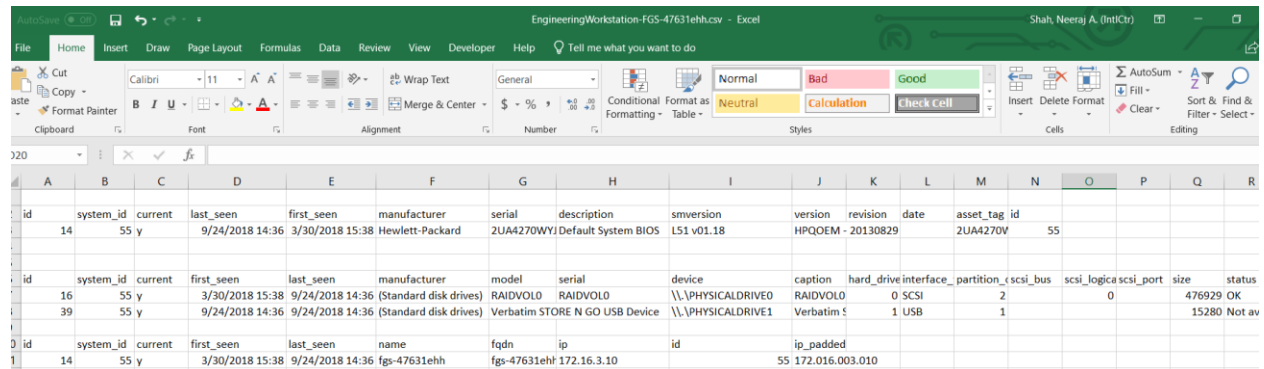
1291 Newly found devices are added to **My Devices** which is found on the home screen.

1292  Process Control System PCS Baseline.zip

1293 Detailed baseline reports generated out of Open-Audit can be obtained from [PCS Baseline Data](#)

1294 Shown below is an export of the baseline data from one of the devices using Open-Audit in the
1295 Process Control System.

1296



id	system_id	current	last_seen	first_seen	manufacturer	serial	description	smversion	version	revision	date	asset_tag	id	size	status
14	55	y	9/24/2018 14:36	3/30/2018 15:38	Hewlett-Packard	2UA4270WVJ	Default System BIOS	LS1 v01.18	HPQOEM	20130829		2UA4270V	55		
16	55	y	3/30/2018 15:38	9/24/2018 14:36	(Standard disk drives)	RAIDVOL0	RAIDVOL0	\\.\PHYSICALDRIVE0	RAIDVOL0	0	SCSI	2		476929	OK
39	55	y	9/24/2018 14:36	9/24/2018 14:36	(Standard disk drives)	Verbatim STORE N GO	USB Device	\\.\PHYSICALDRIVE1	Verbatim	1	USB	1		15280	Not av
1	14	55	y	3/30/2018 15:38	9/24/2018 14:36	fgs-47631ehh	fgs-47631ehh	172.16.3.10	55	172.016.003.010					

d	system_id	current	first_seen	last_seen	mac	net_index	ip	netmask	cidr	version	network	set_by	interface	id	ip_padded
	74	55 n	3/30/2018 9:26	3/30/2018 15:36			172.16.3.10	255.255.255.0	24	4	172.16.3.0/24				55 172.016.003.
	75	55 y	3/30/2018 15:38	#####	40:a8:f0:3d:48:ae		7 172.16.3.10	255.255.255.224	27	4	172.16.3.0/27				55 172.016.003.
	76	55 y	3/30/2018 15:38	9/24/2018 14:36	40:a8:f0:3d:48:ae		7 fe80::5cca:8dfd:2281:992e		64	6					55
d	system_id	current	first_seen	last_seen	name	file_name	file_size	max_file_size	overwrite	id					
	148	55 y	3/30/2018 15:38	9/24/2018 14:36	Application	C:\Windows\	3140	20480	As Needed	55					
	149	55 y	3/30/2018 15:38	9/24/2018 14:36	FTDiag	C:\Windows\	3140	25600	As Needed	55					
	150	55 y	3/30/2018 15:38	9/24/2018 14:36	HardwareEvents	C:\Windows\	68	20480	As Needed	55					
	151	55 y	3/30/2018 15:38	9/24/2018 14:36	Internet Explorer	C:\Windows\	68	1028	As Needed	55					
	152	55 y	3/30/2018 15:38	9/24/2018 14:36	Key Management Serv	C:\Windows\	68	20480	As Needed	55					
	153	55 y	3/30/2018 15:38	9/24/2018 14:36	Media Center	C:\Windows\	68	8192	As Needed	55					
	154	55 y	3/30/2018 15:38	9/24/2018 14:36	Security	C:\Windows\	204804	204800	As Needed	55					
	155	55 y	3/30/2018 15:38	9/24/2018 14:36	Symantec Endpoint Pri	C:\Windows\	6212	8192	As Needed	55					
	156	55 y	3/30/2018 15:38	9/24/2018 14:36	System	C:\Windows\	20484	20480	As Needed	55					
	157	55 y	3/30/2018 15:38	9/24/2018 14:36	Veeam Agent	C:\Windows\	1028	1028	As Needed	55					
	158	55 y	3/30/2018 15:38	9/24/2018 14:36	Windows PowerShell	C:\Windows\	68	15360	As Needed	55					
d	system_id	current	first_seen	last_seen	serial	bank	type	form_factor	detail	size	speed	tag	id		
	10	55 y	3/30/2018 15:38	9/24/2018 14:36		16142323	DIMM4	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55	
	11	55 y	3/30/2018 15:38	9/24/2018 14:36		16142314	DIMM3	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55	
	12	55 y	3/30/2018 15:38	9/24/2018 14:36		16142322	DIMM2	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55	
	13	55 y	3/30/2018 15:38	9/24/2018 14:36		16142352	DIMM1	Synchronous	DIMM	Unknown	4096	1333	Physical Memory	55	
d	system_id	current	first_seen	last_seen	manufacturer	model	serial	description	device	manufact	size	aspect_ratio	edid_versi	cost_code	id
	6	55 y	3/30/2018 15:38	9/24/2018 14:36	Dell	DELL P2414H	27HW349M0EDL	1920 x 1080	A09A	14-Oct	24	16:09			55
	11	55 y	9/24/2018 14:36	9/24/2018 14:36	Sharp	SHARP HDMI		0 1920 x 1080	1.00E+06	13-Jan	80	16:09			55

1297

1298 List of programs installed:

10661	55 y	3/30/2018 15:38	9/24/2018 14:36	Internet Explorer		9.10.9200.17609				#####	1/1/2000 0:00	Microsoft Cor
10662	55 y	3/30/2018 15:38	9/24/2018 14:36	Notepad++ (64-bit x64)		7.5.6				C:\Program Files\Notepad++\un	0000-00-00 00:00	Notepad++ Te
10663	55 y	3/30/2018 15:38	9/24/2018 14:36	Intel(R) Network Connections Drivers			19		C:\Windows\system32	ProunstL.exe	0000-00-00 00:00	Intel
10664	55 y	3/30/2018 15:38	9/24/2018 14:36	OS/soft MS Runtime Redistributables x64		3.1.1				MsiExec.e: 20150306	0000-00-00 00:00	Microsoft / D:\
10665	55 y	3/30/2018 15:38	9/24/2018 14:36	Microsoft Visual C++ 2010 x64 Redistributi		10.0.40219				MsiExec.e: 20150306	0000-00-00 00:00	Microsoft c:\
10666	55 y	3/30/2018 15:38	9/24/2018 14:36	Java 8 Update 60 (64-bit)		8.0.600.27			C:\Program Files\Java\j\	MsiExec.e: 20150928	0000-00-00 00:00	Oracle Cor\
10667	55 y	3/30/2018 15:38	9/24/2018 14:36	Veeam Agent for Microsoft Windows		2.0.0.700			C:\Program Files\Veeam	MsiExec.e: 20170731	0000-00-00 00:00	Veeam Sol\
10668	55 y	3/30/2018 15:38	9/24/2018 14:36	Microsoft SQL Server 2012 Management O		11.1.3000.0				MsiExec.e: 20170731	0000-00-00 00:00	Microsoft C\
10669	55 y	3/30/2018 15:38	9/24/2018 14:36	PI Software Development Kit (PI SDK) x64		1.4.2.445			C:\Program Files\Rockw	MsiExec.e: 20150306	0000-00-00 00:00	Rockwell C\
10670	55 y	3/30/2018 15:38	9/24/2018 14:36	Microsoft Visual C++ 2008 Redistributable		9.0.30729.6161				MsiExec.e: 20150306	0000-00-00 00:00	Microsoft c:\
10671	55 y	3/30/2018 15:38	9/24/2018 14:36	Microsoft .NET Framework 4.6.2		4.6.01590			C:\Windows\Microsoft.f	MsiExec.e: 20180301	0000-00-00 00:00	Microsoft C\
10672	55 y	3/30/2018 15:38	9/24/2018 14:36	PI AF Client (x64) 2012		2.5.1.5159			C:\Program Files (x86)\R	MsiExec.e: 20150306	0000-00-00 00:00	Rockwell / D\
10673	55 y	3/30/2018 15:38	9/24/2018 14:36	Microsoft SQL Server Compact 4.0 x64 ENI		4.0.8482.1			C:\Program Files\Micros	MsiExec.e: 20150306	0000-00-00 00:00	Microsoft D\
10674	55 y	3/30/2018 15:38	9/24/2018 14:36	Microsoft System CLR Types for SQL Server		11.1.3000.0				MsiExec.e: 20170731	0000-00-00 00:00	Microsoft C\
10675	55 y	3/30/2018 15:38	9/24/2018 14:36	SST DeviceNet Products 3.10		3.10.000			C:\Program Files (x86)\S	MsiExec.e: 20171026	0000-00-00 00:00	Molex Inci C\
10676	55 y	3/30/2018 15:38	9/24/2018 14:36	Microsoft SQL Server 2012 Express LocalDI		11.3.6020.0				MsiExec.e: 20170731	0000-00-00 00:00	Microsoft C\
10677	55 y	3/30/2018 15:38	9/24/2018 14:36	Microsoft Message Analyzer		4.0.7948.0				MsiExec.e: 20160519	0000-00-00 00:00	Microsoft E\
10678	55 n	3/30/2018 15:38	9/24/2018 15:41	Symantec Endpoint Protection		14.0.3876.1100			C:\Program Files (x86)\S	MsiExec.e: 20180206	0000-00-00 00:00	Symantec E\
10679	55 y	3/30/2018 15:38	9/24/2018 14:36	FactoryTalk Historian Site Edition 4.00 Live		4.00.00.0104					0000-00-00 00:00	Rockwell Auto
10680	55 y	3/30/2018 15:38	9/24/2018 14:36	FileZilla Client 3.28.0		3.28.0			C:\Program Files\FileZilla	FTP Client	0000-00-00 00:00	Tim Kosse
10681	55 y	3/30/2018 15:38	9/24/2018 14:36	Redundancy Module Config Tool		8.4.1.0			C:\Program Files (x86)\Rockwell Sol	20170926	0000-00-00 00:00	Rockwell / C\
10682	55 y	3/30/2018 15:38	9/24/2018 14:36	AX88772B Windows Drivers		1.0.0.0			C:\Program Files (x86)\ASIX	Electroi 20150914	0000-00-00 00:00	ASIX Electr D\
10683	55 y	3/30/2018 15:38	9/24/2018 14:36	Matrikon OPC Server for Simulation							0000-00-00 00:00:00	
10684	55 y	3/30/2018 15:38	9/24/2018 14:36	MatrikonOPC Sniffer							0000-00-00 00:00:00	
10685	55 n	3/30/2018 15:38	3/30/2018 15:41	Mozilla Firefox 41.0.2 (x86 en-US)		41.0.2			C:\Program Files (x86)\Mozilla	Firefox	0000-00-00 00:00	Mozilla
10686	55 n	3/30/2018 15:38	3/30/2018 15:41	Mozilla Maintenance Service		41.0.2.5765					0000-00-00 00:00	Mozilla
10687	55 y	3/30/2018 15:38	9/24/2018 14:36	OSSEC HIDS 2.9.2		2.9.2					0000-00-00 00:00:00	
10688	55 y	3/30/2018 15:38	9/24/2018 14:36	PI Software Development Kit (PI SDK) x86 2.1.4.2.445					C:\Program Files (x86)\Rockwell Software\FactoryTalk	Hi	0000-00-00 00:00	Rockwell Auto
10689	55 y	3/30/2018 15:38	9/24/2018 14:36	PI Software Development Kit (PI SDK) x64 2.1.4.2.445					C:\Program Files\Rockwell Software\FactoryTalk	Historia	0000-00-00 00:00	Rockwell Auto

1299

1300 List of patches installed:

10880	55 y	3/30/2018 15:38	9/24/2018 14:36	Rockwell Automation Generic Safety Mod; 9.05.3364.0						20150306	0000-00-00 00	
10881	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2764913						1/19/2015	fgs-47631	0000-00-00 00
10882	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2764916						1/19/2015	fgs-47631	0000-00-00 00
10883	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2718695						1/19/2015	fgs-47631	0000-00-00 00
10884	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2670838						1/19/2015	fgs-47631	0000-00-00 00
10885	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2830477						3/6/2018	fgs-47631	0000-00-00 00
10886	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2592687						3/6/2018	fgs-47631	0000-00-00 00
10887	55 y	3/30/2018 15:38	9/24/2018 14:36	KB971033						1/19/2015	fgs-47631	0000-00-00 00
10888	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2479943						1/19/2015	fgs-47631	0000-00-00 00
10889	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2491683						1/19/2015	fgs-47631	0000-00-00 00
10890	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2506014						1/19/2015	fgs-47631	0000-00-00 00
10891	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2506212						1/19/2015	fgs-47631	0000-00-00 00
10892	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2506928						1/19/2015	fgs-47631	0000-00-00 00
10893	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2509553						1/19/2015	fgs-47631	0000-00-00 00
10894	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2511455						1/19/2015	fgs-47631	0000-00-00 00
10895	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2515325						1/20/2015	fgs-47631	0000-00-00 00
10896	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2532531						1/19/2015	fgs-47631	0000-00-00 00
10897	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2533552						1/19/2015	nt authorit	0000-00-00 00
10898	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2533623						1/19/2015	fgs-47631	0000-00-00 00
10899	55 y	3/30/2018 15:38	9/24/2018 14:36	KB2534111						1/19/2015		0000-00-00 00

1301

1302

1303 3.3.8 Update Baseline after Modifications

1304 Manufacturing baseline will be reviewed quarterly and updated with any changes that have
1305 occurred since last review. During period between baseline updates any new equipment added,
1306 or configuration changes implemented will initiate a new baseline scan to be performed.
1307 GRASSMARLIN² and Wireshark³ are the tools used for updating baseline after modification
1308 have occurred. Examples of changes within the manufacturing system would be updating
1309 software, license, system patches, firmware updates, new devices like PLCs' or HMIs' and other
1310 ICS components required for operations.

1311 3.3.9 Network Operations Baseline

1312 Network baseline will be created within manufacturing system to identify all crucial components
1313 required for production to operate. Tools used for this process are as listed, GRASSMARLIN
1314 and Wireshark. Each tool listed provides slightly different capabilities and detail.
1315 GRASSMARLIN generates a diagram for easy visualization, compare to Wireshark which
1316 provides data without diagrams. These tools provide the required network operations baseline
1317 required for manufacturing process.

1318 3.3.10 Priorities for Manufacturing Missions

1319 The priorities for manufacturing missions have been identified in the "Organization Overview"
1320 Section of the Security Program document.

1321 3.3.11 Critical Manufacturing system components and functions

1322 The critical manufacturing system components and functions have been identified in the
1323 Organization Overview Section of the Security Program document.

1324

1325 PROTECT

1326 3.3.12 Security

1327 Security within the organization including the manufacturing system will be followed at all time
1328 to reduce risk of cybersecurity incidents. Sections below contain multiple references to
1329 procedures used at Westman for securing the manufacturing system.

² GRASSMARLIN: <https://github.com/nsacyber/GRASSMARLIN>

³ WireShark: <https://github.com/nsacyber/GRASSMARLIN>

1330 **3.3.13 Training**

1331 Training is a vital role for keeping the company safe for Cybersecurity threats. All employees,
1332 contractors and vendors should have completed required training before being allowed to work
1333 within manufacturing system. Awareness and Training for Third Party Contractors and Vendors
1334 should be reviewed and signed before being allowed to access manufacturing systems.

1335 **3.3.14 Port Security**

1336 Port security allows the ability to configure network ports to be associated with individual
1337 device's Media Access Control (MAC) addresses. Enabling port security ensures only designated
1338 devices are allowed access, any device not already in the approved list will be denied access.
1339 Port Security provides additional protection, when used with defense in depth strategies. See
1340 reference for steps required for setup within Westman.

1341 **3.3.15 Network Segmentation**

1342 Westman network for manufacturing systems has been segmented to improve speed and security
1343 within the environment. Network segmentation provides ability to control traffic from each
1344 network, ensuring only allowed communication can pass between each network. See reference
1345 for steps used for Westman.

1346 **Task: Implement network segmentation.**

- 1347 • The Work Cell consists of the following network hardware.

Type	Description
Allen Bradley Stratix 8300	Boundary protection Firewall, Router
Allen Bradley Stratix 5700	Layer-2 Switch for the Control Network
Allen Bradley Stratix 5700	Layer-2 Switch for the Supervisory Network

- 1348
- 1349 • Network segmentation was implemented using the Allen Bradley Boundary router. The
1350 router has the following sub-networks defined.
1351

Interface	IP address of Interface	Network / Subnet	Description
Fa 1/1	172.16.1.1	172.16.1.0/24	Supervisory Vlan1
Fa 1/2	172.16.2.1	172.16.2.0/24	Control Vlan1
Fa 1/3	172.16.3.1	172.16.3.0/24	Engineering LAN
Fa 1/4	10.100.0.40		Uplink to Cybersecurity LAN

- 1352
- 1353 • One of the Stratix 5700 switches was connected to the Fa 1/1 interface of the 8300 Router
1354 and used for the Supervisory (Vlan1) sub-network. Devices connected to this switch were
1355 assigned an IP address from the 172.16.1.0/24 subnet

1356

- 1357 • The other Stratix 5700 switch was connected to the Fa 1/2 interface of the Router and used
1358 for the Plant (Vlan2) sub- network. Devices connected to this switch were assigned an IP
1359 address from the 172.16.2.0/24 subnet.

1360

Task: Identify and control connections.

	From	To	Direction	Controlled using
Connection	Cybersecurity LAN	Supervisory LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Cybersecurity LAN	Plant LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Supervisory LAN	Plant LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Engineering LAN	Supervisory LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Engineering LAN	Plant LAN	Bi-directional	ACL rules on Boundary Firewall (Allen Bradley)
Connection	Supervisory, Plant and Engineering LAN	Internet	One way	Boundary Firewall (Cisco ASA) in the Cybersecurity LAN

3.3.16 Monitor Boundary Connections

Network traffic will be monitored for external and internal communications using a firewall, or other type of device that allows for the ability to control connection traffic. Required network traffic leaving the manufacturing system will be allowed, all other traffic will be explicitly dropped. Traffic to manufacturing system will be limited to only those machines required for monitor from corporate network to manufacturing system and machines won't be allowed internet access. Device monitoring external/ internal connection/communications will forward all logging to internal Syslog server for archival purposes.

- External Boundary communications are monitored using Cisco ASA Firewall in the Cybersecurity LAN network.

- 1375 • Internal Boundary communications are monitored using Stratix 8300 series Firewall in the
1376 Work Cell.

1377 **Tool: Boundary Protection Device**

1378 The table below lists the boundary protection devices implemented

Type	Description
Allen Bradley Stratix 8300	Firewall/Router for Work Cell
Cisco ASA Firewall	Firewall/Router in the Cybersecurity LAN

1379

1380 **Document: Boundary protection device configuration.**

1381 Refer to section 4.19 Network Boundary Protection

1382 **3.3.17 Actions that can be performed with/without Authentication**

Authentication Required to Physically/Logically Interact with Device?								
	Engineering Workstation	Supervisory PLC	HMI	Controller	Local Historian	OPC Server	VLAN switches	Boundary router
Physical Interaction (All Users*)	Y	N	N	Y	Y	Y	Y	Y
Logical/Network Interaction (All Users*)	Y	Y	Y	Y	Y	Y	Y	Y

1383

HMI User Actions Requiring Authentication			
	View Process Status	Modify Process Setpoints	Silence/Clear Alarms
All Users*	N	Y	Y

1384

Engineering Workstation User Actions Requiring Authentication				
	Login to Workstation	View/Modify PLC Logic	Access Engineering Files	All Other Actions
All Users*	Y	Y	Y	Y

1385

1386

Historian User Actions Requiring Authentication				
	View Historical Data	Modify Historical Data	Modify Configuration	Login to Server Desktop/CLI
All Users*	Y	Y	Y	Y

1387

OPC Server User Actions Requiring Authentication		
	Modify Configuration	Login to Desktop/CLI
All Users*	Y	Y

1388

Controller User Actions Requiring Authentication			
	Modify Configuration	Login to Desktop/CLI	Modify Control Logic
All Users*	Y	Y	Y

1389

1390

VLAN switches User Actions Requiring Authentication		
	Modify Configuration	View switch status
All Users*	Y	Y

1391

PLC Actions Requiring Authentication					
	Power On/Off	Reboot	Process Interaction (Run/Stop/Reset)	Modify Logic	Change Mode (Run/Config)
All Users*	N	N	N	Y	Y

1392 * Authentication for *all users* does not imply authorization has been granted to any specific

1393

1394 **3.3.18 Network Connections**

1395 All network connection with manufacturing system will be documented to include port numbers
1396 and cables will be labeled indicating their designated purpose.

1397 All connection will be reviewed and authorized before being placed into production.

1398 **3.3.19 Remote Maintenance**

1399 Remote maintenance activities will be coordinated and approved before vendor access is
1400 allowed. All remote maintenance activities provided by a vendor will be controlled and
1401 monitored to ensure no harmful or malicious activities occur. Any vendors or contractors
1402 connecting to Westman for remote maintenance will require approval before connecting.
1403 Requests will be documented to ensure proper audit trail for activity conducted within
1404 manufacturing system. See reference for detailed plan.

1405 **3.3.20 System Maintenance**

1406 Reference System Maintenance within Security Policy

1407 **3.3.21 Change Control**

1408 Changes to manufacturing system will be submitted to a change control process ensuring that all
1409 applicable parties are aware and agree on actions being performed. Management will have final
1410 approval since production could be affected by down time.

Changes within the manufacturing systems will be scheduled during non-production hours as not to affect processing within manufacturing system. Changes will be reviewed and authorized before being implemented. Potential system performance issues from the potential change must be determined before the change is made. Once changes have been completed a review will be conducted ensuring same security level continues to be maintained after changes have been implemented.

Responsible parties will evaluate security impact on change controls being performed within the manufacturing system environment. Change control reviewers will have final say for changes being implemented along with changes having an impact on security.

Below is a list of items that need to be change controlled

Device Name	Item Type	Details
Engineering Workstation	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (Factory Talk, RSLinx etc.)
	Hardware	Storage and Memory upgrade
OPC Server	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (PI, FactoryTalk Services Platform, RSLINX, Matrikon OPC)
	Hardware	Storage and Memory upgrade
Historian VM	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), SQL Server patches,
	Hardware	Storage and Memory upgrade
Plant Simulator	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.)
	Hardware	Storage and Memory upgrade
Controller Host	Software	BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (MATLAB, Matrikon OPC)
	Hardware	Storage and Memory upgrade
HMI Host	Software	OS Patches (Windows), BIOS/Firmware patches, IT programs (Antivirus, Backup agent etc.), Plant apps (FactoryTalk View Site, FT Services Platform, FT View Studio)
	Hardware	Storage and Memory upgrade

PLC	Software	Firmware upgrade and any type of configuration change
Allen Bradley Boundary Router	Software	Firmware upgrade, Firewall rules and any type of configuration change
Allen Bradley Layer-2 Switches	Software	Firmware upgrade and any type of configuration change
Cisco ASA Firewall	Software	Firmware upgrade, Firewall rules and any type of configuration change
Switches	Software	Firmware upgrade and any type of configuration change
Active Directory	Software	Group Policy deployment, User account creation/modification
Symantec Antivirus	Software	Antivirus version upgrades, Any Endpoint policy deployment via Symantec Manager
Nessus	Software	Running vulnerability scan(s)

1423

1424 **3.3.22 Media Sanitization for Devices**

Assets / Device type	Method used	Details
Hard Drives on servers, workstations	CLEAR	<p>Tool: DBAN ⁴, Category: Software, Type: Open-Source</p> <p><u>Instructions:</u></p> <p>(1) Download and create a bootable media of DBAN</p> <p>(2) Boot the server using the bootable media</p> <p>(3) Follow the on-screen instructions to run the multiple passes of data wipe.</p> <p>(4) Once complete, verify if wipe was successful by booting the server without the DBAN media</p>

<https://dban.org/>

Allen Bradley 8300 Boundary Router	CLEAR	<p>The below instructions are found in the Allen Bradley manual for Stratix Managed Switches⁵</p> <p><u>Clear:</u></p> <ol style="list-style-type: none"> (1) Login to Web Admin console (2) Navigate to Device Management Restart/Reset in the menu (3) Select Reset Switch to Factory Defaults and click on Submit
Allen Bradley 5700 L2 switch	CLEAR	<p>The below instructions are found in the Allen Bradley manual for Stratix Managed Switches⁶</p> <p><u>Clear:</u></p> <ol style="list-style-type: none"> (1) Login to Web Admin console (2) Navigate to Device Management Restart/Reset in the menu (3) Select Reset Switch to Factory Defaults and click on Submit
HMI	CLEAR	<p>The HMI program is installed on a Windows 7 system. To uninstall this program</p> <ol style="list-style-type: none"> (1) Login to the Windows system via an admin account. Go to Control Panel >> Programs and Features (2) Select and Uninstall all “FactoryTalk®” components. Reboot the machine if required.
Historian	CLEAR	<p>This consists of 2 parts – Historian Suite and SQL Server database. Both are installed on a Windows system. They can be treated as any other program/software on a Windows system.</p> <p>To uninstall Historian program:</p> <ol style="list-style-type: none"> (1) Login to the Windows system via an admin account. Go to Control Panel >> Programs and Features (2) Select and uninstall all “FactoryTalk®” components. Reboot the machine if required. <p>OR</p> <ol style="list-style-type: none"> (1) Click on Start Menu >> Programs >> Rockwell Software >> Factory Talk Site Edition >> Uninstall Factory Talk.

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

		<p>To uninstall the SQL Database</p> <p>(1) From Program and Features select “SQL Server Compact Edition” and uninstall it.</p>
Allen Bradley PLC	CLEAR	<p>The Allen Bradley PLC is a modular chassis consisting of different modules such as DeviceNet Scanner, ControlLogix Module, EthernetIP Module and HIPROM time.</p> <p>To reset the HIPROM Time Module:</p> <p>(1) Follow the instructions as per Allen Bradley HIPROM ⁷ manual and set the Rotary Switch to 888.</p> <p>To reset the DeviceNet Scanner Module</p> <p>(2) Follow the instructions as per Allen Bradley DeviceNet ⁸ manual and set the Rotary Switch to 888.</p> <p>To clear the ControlLogix 5571 Module, Refer to the below instructions. These are defined in Allen Bradley ControlLogix 5000 Manual⁹.</p> <p>Clear the Program from On-board NVS Memory If your application allows it, follow these steps to clear the program from the 1756-L7x controller’s on-board NVS memory.</p> <ol style="list-style-type: none"> 1. Remove the ESM from the controller. 2. Remove power from the controller. <p>You can remove power in either of the following two ways:</p> <ul style="list-style-type: none"> • Turn power off to the chassis while the controller is installed in the chassis. • Remove the controller from a powered chassis. <ol style="list-style-type: none"> 3. Reinstall the ESM into the controller. 4. Restore power to the controller in one of two ways.

1425

1426

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um538_-en-p.pdf

http://literature.rockwellautomation.com/idc/groups/literature/documents/in/1756-in566_-en-p.pdf

http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf

1427 **3.3.23 Backup Procedures**1428 Servers, Workstations:

1429 Refer Section 9.4.5 Veeam Backup and Replication

1430 Network Devices:

1431 1. Launch the TFTP server on Engineering Workstation

1432 2. SSH to the switch / router and run the below commands

```
Router# enable
Router# copy running-config tftp
Address or name of remote host []? <IP-address of Workstation>
Destination filename [router-config]? <Enter a file-name>
```

1433

1434 3. Ensure to manually save the configuration backup at a central secure location

1435 ICS Devices:

1436 Follow the Manufacturer's product manual to perform a backup

1437 Ensure to manually save the configuration backup at a central secure location

1438 **3.3.24 Priority Analysis**

1439 Manufacturing system will be evaluated quarterly to identify devices importance. Devices
1440 importance will be used to provide a criticality report containing the minimum pieces of
1441 equipment required to continue productions.

1442

1443

3.3.25 Vendor Requirements

Service Level Agreements (SLA) will be outlined and discussed, along with the need for required notification when an employee transfers departments', leaves the company, or is terminated that had direct network connectivity into Westman's network

Service Level Agreement:

Service Level Agreement (SLA)
for Vendor
by
Westman

Effective Date: 02-22-2019

Document Owner:	Westman President
------------------------	-------------------

Version

Version	Date	Description	Author
1.0	02-22-2019	Service Level Agreement	Westman President

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this Agreement.)

Approvers	Role	Signed	Approval Date
Westman	Customer		2-22-2019
Vendor	Service Provider		2-22-2019

Agreement Overview

This Agreement represents a Service Level Agreement ("SLA" or "Agreement") between Westman and Vendor (Service Provider) for the provisioning of IT/OT services required to support and sustain the Product or service.

This Agreement remains valid until superseded by a revised agreement mutually endorsed by the stakeholders.

This Agreement outlines the parameters of all IT/OT services covered as they are mutually understood by the primary stakeholders. This Agreement does not supersede current processes and procedures unless explicitly stated herein.

Goals and Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent IT/OT service support and delivery to Westman by the Service Provider(s).

The **goal** of this Agreement is to obtain mutual understanding for IT/OT services provision between the Service Provider and Westman.

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.
- Match perceptions of expected service provision with actual service support and delivery.

Stakeholders

The following Service Provider and Westman will be used as the basis of the Agreement and represent the **primary stakeholders** associated with this SLA:

IT Service Provider: Service Provider

IT/OT Customer: Westman

Periodic Review

This Agreement is valid from the **Effective Date** outlined herein and is valid until further notice. This Agreement should be reviewed at a minimum once per fiscal year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

The **Business Relationship Manager** (“Document Owner”) is responsible for facilitating regular reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

Business Relationship Manager: Westman (President)

Review Period: Yearly (12 months)

Previous Review Date: 02-22-2019

Next Review Date: 02-22-2020

Service Agreement

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement.

Service Scope

The following Services are covered by this Agreement:

- Apply system updates to manufacturing environment per vendor’s recommendation
- Apply system updates to IT equipment when patches are released per vendor.
- Backup configure information for all IT/OT equipment within Westman
- Ensure cybersecurity tools are operating correctly within the environment
- Provide liaison service between OT vendor and Westman
- Product recommendation for new equipment being purchased and installed with Westman’s manufacturing environment
- Manned telephone support
- Monitored email support

- 1531 • Remote assistance using Remote Desktop and a Virtual Private Network where available
- 1532 • Planned or Emergency Onsite assistance (extra costs apply)
- 1533 • Monthly system health check

1534

1535 Customer Requirements

1536

1537 Westman's responsibilities and/or requirements in support of this Agreement include:

- 1538 • Payment for all support costs at the agreed interval.
- 1539 • Reasonable availability of customer representative(s) when resolving a service related
- 1540 incident or request.

1541

1542 Service Provider Requirements

1543

1544 **Service Provider** responsibilities and/or requirements in support of this Agreement include:

1545

- 1546 • Meeting response times associated with service related incidents.
- 1547 • Appropriate notification to Customer for all scheduled maintenance.

1548

1549 Service Assumptions

1550

1551 Assumptions related to in-scope services and/or components include:

1552 Changes to services will be communicated and documented to all stakeholders.

1553 Service Management

1554

1555 Effective support of in-scope services is a result of maintaining consistent service levels. The

1556 following sections provide relevant details on service availability, monitoring of in-scope

1557 services and related components.

1558 Service Availability

1559

1560 Coverage parameters specific to the service(s) covered in this Agreement are as follows:

- 1561 • Telephone support: 8:00 A.M. to 5:00 P.M. Monday – Friday
- 1562 • Calls received out of office hours will be forwarded to a mobile phone and
- 1563 best efforts will be made to answer / action the call, however there will be a
- 1564 backup answer phone service
- 1565 • Email support: Monitored 8:00 A.M. to 5:00 P.M. Monday – Friday
- 1566 • Emails received outside of office hours will be collected, however no action
- 1567 can be guaranteed until the next working day
- 1568 • Onsite assistance guaranteed within 72 hours during the business week

Service Requests

In support of services outlined in this Agreement, the Service Provider will respond to service related incidents and/or requests submitted by Westman within the following time frames:

- 0-8 hours (during business hours) for issues classified as **High** priority.
- Within 48 hours for issues classified as **Medium** priority.
- Within 5 working days for issues classified as **Low** priority.

Remote assistance will be provided in-line with the above timescales dependent on the priority of the support request.

Personal Changes:

When an individual user with remote access leaves service provider, is transferred, or is terminated the service provider will notify Westman. If user had access to Westman's network, that access will be disabled, or deleted as soon as possible. System account passwords the service provider had will need to be changed to ensure user access into the network has been completely removed.

DETECT**3.3.26 Event Logging**

Devices within manufacturing system shall be configured to send log data to central repository (Syslog Server) when supported. Logs sent from devices allow additional forensics analysis, which will be useful after a cybersecurity event. Westman logs all devices events alerts to central log server for review and archive purpose. Recorded events help identify any malicious activity within the manufacturing systems. Logs will be checked periodically looking for abnormal alerts generated from manufacturing system. See reference for additional information.

3.3.27 Event Impacts

Logged events will be examined to determine the impact if any against the manufacturing system. Events impacting manufacturing system will be reviewed to determine correlation with risk assessment outcomes. Once correlation has been completed action will be taken if required to increase cybersecurity posture to lessen future threats.

3.3.28 Monitor

All personnel within the manufacturing system will be required to sign-in upon entering ICS environment with date and time of entry, including when leaving work space. Any person found in violation of mandatory sign-in/sign-out sheet will be escorted out of the manufacturing environment. Individuals will be challenged to ensure they are employees or are being escorted around the environment.

1605 All network switches have been configured for port security, so unauthorized devices won't be
1606 allowed access to the manufacturing network without prior approval.

1607 Weekly wireless scans will be completed using a laptop within manufacturing system. Rouge or
1608 unknown wireless devices will be brought to management's attention for additional review.

1609 Periodic software scans will be performed on devices within manufacturing system to
1610 detect any unauthorized software.

1611 Switch logs within manufacturing system will be checked regularly to ensure no rogue devices
1612 have attempted to connect. Output from switch logs will be compared against hardware
1613 inventory performed in.

1614 **3.3.29 Forensics**

1615 Syslog server will be used for collection of system logs. Logs can analysis to understand the
1616 attack target along with determining the method that was used during the attack against devices
1617 within manufacturing system. In addition, tools such as Security Onion and Wireshark may be
1618 used to analyze events and packet captures respectively.

1619 **3.3.30 Detect non-essential capabilities**

1620 System scanning/auditing tool will be used to identify non-essential software applications
1621 installed on devices within manufacturing system. Software not required for operations will be
1622 removed and baseline configuration updated to reflect new configuration state.

1623 **3.3.31 Ensure resources are Maintained**

1624 Systems performance and resources can have a drastic effect on manufacturing
1625 process. Individual in charge of manufacturing system will be responsible for performing daily
1626 checks on all systems within the manufacturing system environment (OT). Checks will include,
1627 but not limited to physical observation of all operational components ensuring any warning
1628 lights or other area of concern are investigated further. System logs of
1629 all manufacturing devices will be checked at the beginning and end of every shift looking for
1630 any deviation from the normal baseline performance.

1631

1632 **RESPOND**

1633 **3.3.32 Fire Protection Systems**

1634 Fire protection for a manufacturing environment should be designed to safeguard electrical
1635 equipment. Manufacturing systems requiring protection can be PLCs', HMIs', Robots,
1636 Machining equipment, computers and other required devices. Fire Protection should be designed
1637 and implemented to protect human life first and equipment second. Installed fire protection

1638 systems will be certified compliant with existing/new environment by a licensed and accredited
1639 vendor. Check industry standards for any required baselines.

1640 **3.3.33 Emergency and Safety Systems**

1641 Emergency and Safety Systems will compile with Local, State, and Federal laws. This is to
1642 include safety regulations for workers' safety from Occupational Safety and Health
1643 Administration (OSHA). Industry regulation for safety will be followed per guidance from
1644 regulating industry.

1645 Fire Protection Systems will compile with Local, State, and Federal laws. This is to include Fire
1646 Protection Systems specially designed for manufacturing process. Fire Protection System will
1647 place emphasis on human safety first and for most, before concern for manufacturing system.
1648 Fire Protection Systems will be checked minimum once per year unless shorter intervals are
1649 required from superseding regulations.

1650 Only Industry approved Environmental Controls will be used within manufacturing systems, to
1651 included compliance with all Local, State, Federal laws. Environmental Control will be
1652 implemented to place human/community safety first before manufacturing systems.

1653 **3.3.34 Detected Events**

1654 Detected cybersecurity event notification will be investigated to determine root cause and
1655 appropriate remediation steps will be taken to clear events returning the organization /
1656 manufacturing system to known good operating state.

1657 This can be done by reviewing the logs or events in Graylog and/or Security Onion

1658 **3.3.35 Vulnerability Management Process**

1659 Vulnerability management is an essential component of any information security program and
1660 the process of vulnerability assessment is vital to effective vulnerability management.

1661 Vulnerability Scanning and Management Tools

1662 Tenable- Nessus will be used to perform vulnerability scans. The Results report generated by
1663 Nessus at the completion of the scan, is then fed into NamicSoft which is a vulnerability
1664 management, parsing and reporting tool.

1665 NamicSoft can create customized reports and logically group results for a consistent workflow
1666 within the organization. The reports are reviewed by the foreman and then shared with the
1667 machine operators.

1668 Vulnerability Scan Targets

1669 All devices connected to both Plant and Supervisory network segments are scanned. The IT Staff
1670 will configure a scan for all network segments of Westman.

1671 A new scan can be established, or an existing one changed, by submitting a request to the
1672 Director of Operations.

1673 Vulnerability Scan Frequency/Schedule

1674 Scans are performed by the IT Staff on an on-demand, per-request basis as needed. The IT
1675 manager shall make provisions for an assessment once per month.

- 1676 • All IT/OT device scans should be scheduled in the 2 weeks of maintenance window in
1677 December of each year.
- 1678 • All device scans should be performed during hours appropriate to the business needs of the
1679 organization and to minimize disruption to normal operations
- 1680 • Any new device discovered needs to be classified under its appropriate group.

1681 General Rules

- 1682 • The Engineers or IT staff will not make any temporary changes to information systems, for
1683 the sole purpose of "passing" an assessment. Vulnerabilities on information systems shall be
1684 mitigated and eliminated through proper analyses and repair methodologies.
- 1685 • No devices connected to the network shall be specifically configured to block vulnerability
1686 scans from authorized scanning engines.
- 1687 • Use caution when running vulnerability scans against OT Networks such as the Supervisory
1688 LAN and Field LAN Network. Scans should be scheduled off hours and during periods of
1689 maintenance.
- 1690 • It is recommended to run authenticated scans from the vulnerability scanner.

1691 Vulnerability Reporting

1692 Upon completion of a vulnerability scan, the data is fed into NamicSoft out of which report is
1693 generated. A report will always be generated as proof that an assessment occurred.

1694 All IT/OT devices are organized into appropriate groups in NamicSoft as per the system they
1695 reside in. A device may belong to one or more systems. Reporting is done system wise so that
1696 the devices and vulnerabilities can more easily be distributed to the IT Staff, Manager and
1697 Director of Operations. Below is a table of type of reports that will be sent out.

Status Reports	Frequency	Purpose
Host table with affected vulnerabilities	Monthly	Information is presented for each host.
Vulnerability Assessment Report	Monthly	Information is presented for both scanned networks.

Host specific report	Ad-hoc	Information is presented for requested host.
Mitigated vulnerabilities report	Post remediation	Upon re-scanning a host to check if vulnerabilities have been mitigated or not

1698

1699 **Remediation Management and Priorities**

1700 All vulnerabilities discovered must be analyzed by the Director, Control Engineers with
1701 assistance from IT Team and OT Contractor (if needed) to decide on the next course of action.

1702 All vulnerabilities discovered should be remediated.

1703 The below chart should be used for remediation timelines

Severity	Description	Remediation time
Critical	Nessus uses Common Vulnerability Scoring System (CVSS) for rating vulnerabilities. A Critical vulnerability has a CVSS base score of 9.0 or 10.	15 days of discovery
High	High-severity vulnerabilities have a CVSS score between 7.0 and 8.9.	30 days of discovery
Medium	Medium-severity vulnerabilities have a CVSS score of 4.0 to 6.9 and can be mitigated within an extended time frame.	45 days of discovery
Low	Low-severity vulnerabilities are defined with a CVSS score of 1.0 to 3.9. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented	180 days of discovery
Info	Info level do not present security risk and are listed for informational purposes only. It is optional to remediate them.	Not required to remediate

1704

1705 **Exceptions Management**

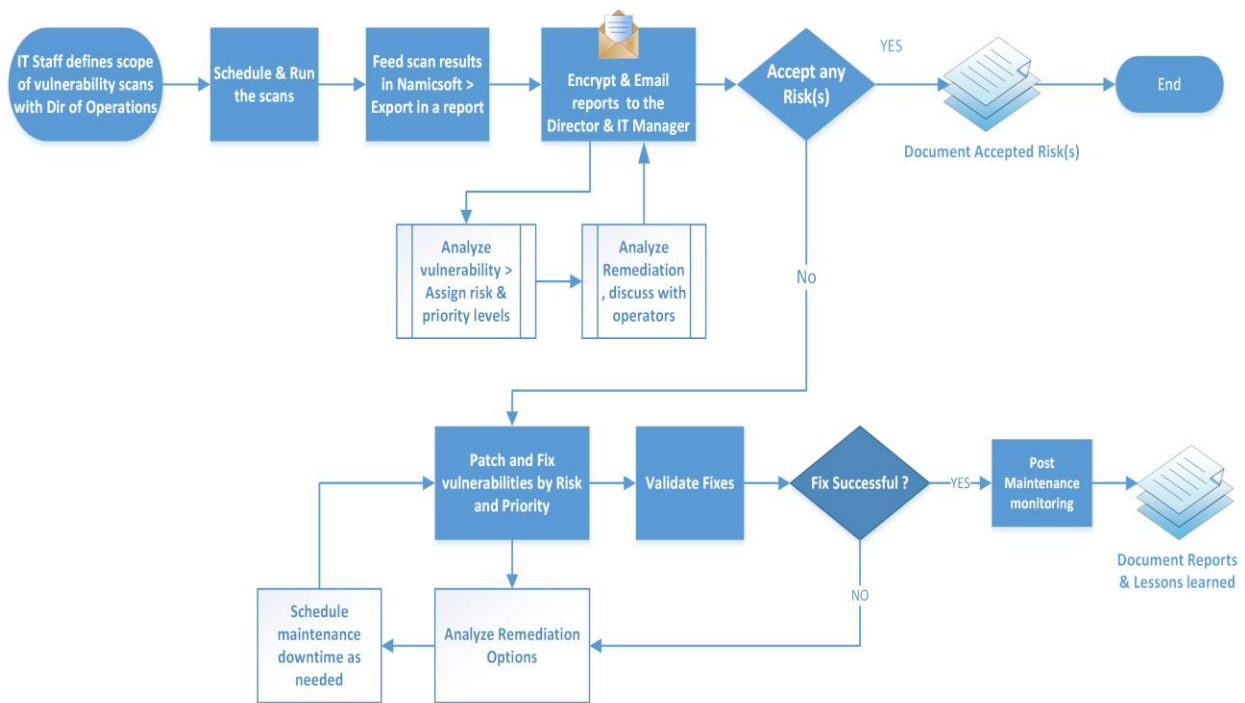
1706 Any exceptions to this policy, such as exemption from the vulnerability assessment process must
1707 be internally discussed and approved by the Foreman.

Vulnerabilities may exist in operating systems, applications, web applications or OT devices. While every effort must be made to correct issues, some vulnerabilities cannot be remediated. Vendors may have appliances that are not patched, services may be exposed for proper application operations, and systems may still be commissioned that are considered end-of-life by the developer and manufacturer. In these cases, additional protections may be required to mitigate the vulnerability. Exceptions may also be made so that the vulnerabilities are not identified as items of risk to the system and organization.

False Positives identification may be documented through emails or the NamicSoft tool with the security staff. Acceptable Risk exceptions must be requested through the IT Team with an explanation containing:

- Mitigating controls – what changes, tools, or procedures have been implemented to minimize the risk.
- Risk acceptance explanation – details as to why this risk is not relevant to the company and systems.
- Risk analysis – if the vulnerability is indeed compromised, what risk and systems will be affected.

Process Overview



Westman Chemicals Vulnerability Management Process

1727 RECOVER**1728 3.3.36 Recovery Plan****1729 Purpose and Objective:**

1730 Westman developed this incident recovery plan (IRP) to be used in the event of a significant
1731 disruption to the features listed in the table below. The goal of this plan is to outline the key
1732 recovery steps to be performed during and after a disruption working to return to normal
1733 operations as quickly as possible.

1734

1735 Scope:

1736 The scope of this IRP document addresses technical recovery only in the event of a significant
1737 disruption. The intent of the IRP is to be used in conjunction with the business continuity plan
1738 (BCP) Westman developed. A IRP is a subset of the overall recovery process contained in
1739 the BCP. Plans for the recovery of people, infrastructure, and internal and external dependencies
1740 not directly relevant to the technical recovery outlined herein are included in the Business
1741 Continuity Plan and/or the Corporate Incident Response and Incident Management
1742 plans Westman has in place.

1743

1744 The specific objectives of this incident recovery plan are to:

- 1745 • Establish a core group of leaders to assess the technical ramifications of a situation;
- 1746 • Set technical priorities for the recovery team during the recovery period;
- 1747 • Minimize the impact of the disruption to the impacted features and business groups;
- 1748 • Stage restoration of operations to back full processing capabilities;
- 1749 • Enable rollback operations once disruption has been resolved and determined appropriate by
1750 recovery team.

1751

1752 Within the recovery procedures there are significant dependencies between and supporting
1753 technical groups within and outside Westman. This plan is designed to identify the steps that are
1754 expected to take to coordinate with other groups / vendors to enable their own recovery. This
1755 plan is not intended to outline all the steps or recovery procedures that other departments need to
1756 take in the event of a disruption, or in the recovery from a disruption.

1757 Incident Recovery Strategies:

1758 The overall IR strategy of Westman is summarized in Section 3.6 Incident Recovery Plan.

3.4 Risk Management Document Example

<p style="text-align: center;">Risk Management Strategy</p> <p style="text-align: center;">for</p> <p style="text-align: center;">Westman</p>
--

Document Owner:	Director of Operations, Westman
------------------------	---------------------------------

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

This Risk Management Plan defines how risks associated with the Westman will be identified, analyzed, and managed. This document can be used by the Director of Operations and Executives to foresee risks, estimate impacts, and define responses to issues.

3.4.1 Scope

Any employee, contractor, or individual with access to the organization's systems or data.

3.4.2 Risk Management Process**Process**

The overall process involves Identifying, Analysis, Categorizing, Reporting and Remediating. Risks will be identified as early as possible in the project to minimize their impact. The steps for accomplishing this are outlined in the following sections.

1784 Risk Identification

1785 Risk identification will involve the Company's Director of Operations, Control Engineers, IT
1786 Manager, evaluation of environmental factors, organizational culture and the project
1787 management plan including the project scope. There are many different types of threats that
1788 can affect IT and OT infrastructure. These can include:

- 1789 • Technical threats — disruption caused by technological advances or failures
- 1790 • Structural threats — anything related to the building that houses your IT infrastructure
- 1791 that could cause it to be harmed
- 1792 • Financial threats — If the business loses funding or experiences another significant
- 1793 financial change
- 1794 • Human threats — human error or loss of important individual
- 1795 • Natural threats — weather and natural disasters such as earthquakes, tornadoes, and
- 1796 floods

1797 A Risk Management Log will be generated and updated as needed, a sample of which is shown
1798 in the latter half of this document

1799
1800 Software tools such as CSET¹⁰ will be used to perform RISK Assessments. The reports
1801 generated will be discussed with the CEO.

1802
1803 Additionally, the Control Engineers and Director of Operations will subscribe to NVD,
1804 USCERT, ICS-CERT and ISACS alert feeds to keep up with the latest vulnerabilities.

1805
1806 This is an iterative process. As the program progresses, more information will be gained about
1807 the program and the risk statement will be adjusted to reflect the current understanding. New
1808 risks will be identified as the project progresses through the life cycle.

1809 Risk Analysis

1810 All risks identified either manually or via CSET will be assessed to identify impact on
1811 operations. Qualification will be used to determine which risks are the top risks and which ones
1812 can be ignored.

1813 Qualitative Risk Analysis

1814 The probability and impact of occurrence for each identified risk will be assessed by the Director
1815 of Operations with input from the control engineers using the following approach:

1816 Probability

- 1817 • High – Greater than <70%> probability of occurrence in a year

¹⁰ CSET: <https://ics-cert.us-cert.gov/Assessments>

- Medium – Between <30%> and <70%> probability of occurrence in a year
- Low – Below <30%> probability of occurrence in a year

Impact

- High – Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
- Low – Risk that has relatively minor impact on cost, schedule or performance

Quantitative Risk Analysis

This involves assigning a numeric value to the risk calculated as the product of probability of occurrence and impact score. Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on project activities will be estimated, a numerical rating applied to each risk based on this analysis, and then documented in the risk management log.

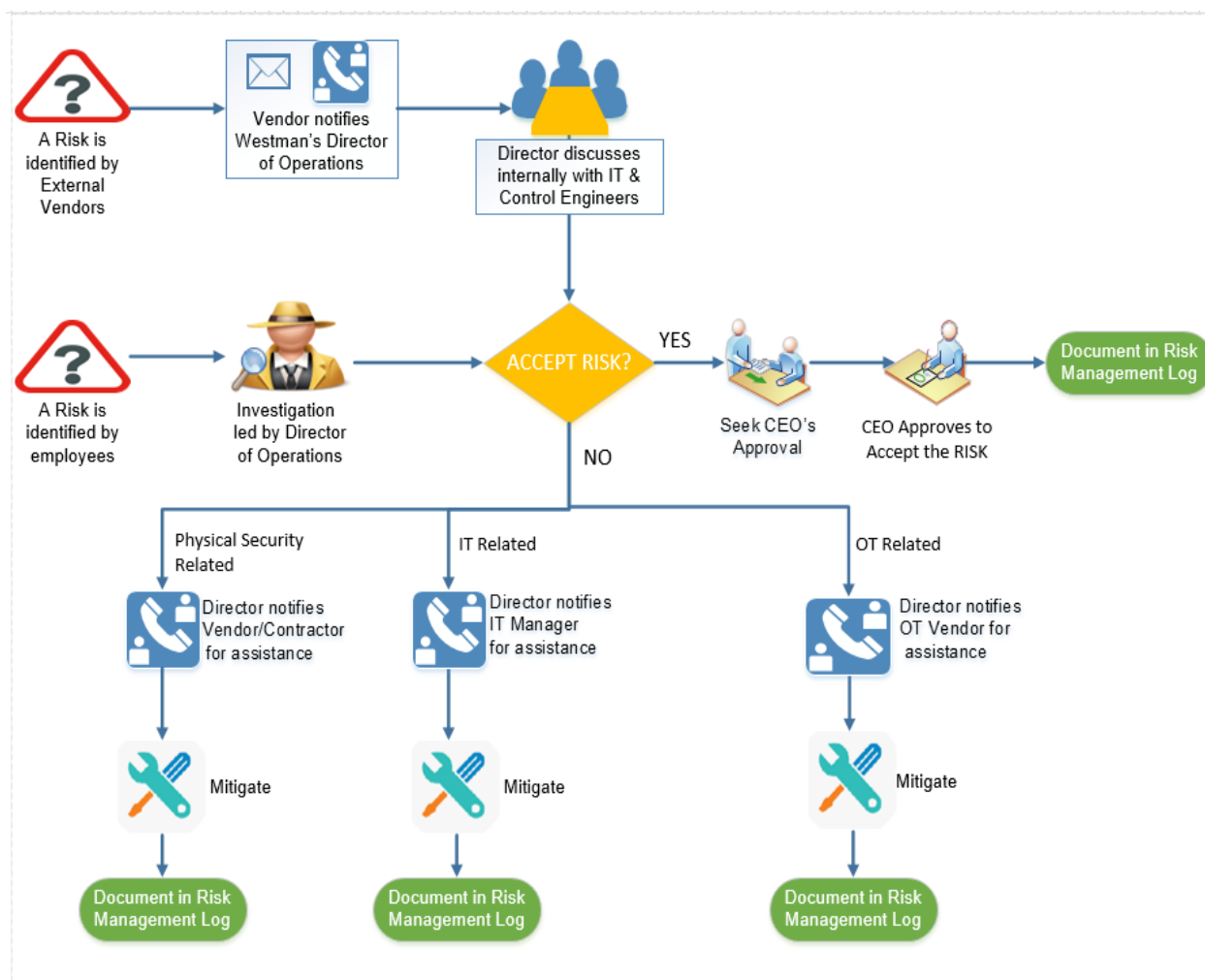
3.4.3 Risk Monitor and Control

The Director of Operations and IT Team will conduct yearly risk assessments which includes CSET assessments, vulnerability scans of the manufacturing system that take into account vulnerabilities and potential impact to the manufacturing operations. An identified risk can be brought to Director's attention either by Westman's employees or by external contractors.

The IT Team will scan the IT and OT assets when called upon; with Nessus to monitor for any software-based risks. The Nessus results will be fed into NamicSoft. Reports will be generated out of this tool and shared with the process owners. Any other type of risks like hardware based, physical, environmental will be identified and documented manually.

All software-based vulnerabilities discovered using Nessus should be mitigated as per the Vulnerability Management Plan.

If a software vulnerability has been remediated; a Nessus scan be re-run to see whether the situation has changed in a way that affects the manufacturing operations. For any corrective action has been taken, the risk management log will be updated.

1853 **3.4.4 Risk Notification Process**

1854

1855 **3.4.5 Risk Response / Remediation Strategy**

1856 For each major risk, one of the following approaches will be selected to address it:

- 1857
- 1858 • **Avoid** – eliminate the threat by eliminating the cause
 - 1859 • **Mitigate** – Identify ways to reduce the probability or the impact of the risk
 - 1860 • **Accept** – Nothing will be done
 - 1861 • **Transfer** – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

1862

1863 For each risk that will be mitigated, the team will identify ways to prevent the risk from re-

1864 occurring or reduce its impact or probability of occurring. This may include

1865

- 1866 • Prototyping.
- 1867 • Adding tasks to the project schedule
- 1868 • Determining and allocating resources.

1869 For each risk that needs to be “Accepted”, a document containing the list of accepted risks will
1870 be maintained by the Director of Operations.

1871
1872 The Director will reach out to an IT/OT Vendor for any risks and request remediation assistance.

1873 **3.4.6 Risk Appetite**

1874 Risk appetite - is the broad-based amount of risk an organization is willing to accept in pursuit of
1875 its mission/vision. [4]

1876 Risk Appetite scale [5]:

- 1877 • High - the manufacturing system accepts disciplined risk taking because the organization
- 1878 has determined the potential benefits outweigh the potential risk.
- 1879 • Moderate - the manufacturing system accepts some risk taking, assuming the
- 1880 organization has reviewed the potential benefits and potential risks.
- 1881 • Low - the manufacturing system accepts minimal risk taking.
- 1882 • None - the manufacturing system accepts no risk taking because the risk is intolerable.

1883 **3.4.7 Risk Tolerance**

1884 Risk tolerance - is the acceptable level of variance in performance relative to the achievement of
1885 objectives. In setting risk tolerance levels, management considers the relative importance of the
1886 related objectives and aligns risk tolerance with risk appetite. [4]

1887 Risk tolerance scale [6]:

- 1888 • Low - the level of risk will not considerably impact the ability of the manufacturing
- 1889 system to meet its mission objectives.
- 1890 • Moderate - the level of risk may impact the ability of the manufacturing system to meet
- 1891 its mission objectives.
- 1892 • High - the level of risk will significantly impact the ability of the manufacturing system
- 1893 to meet its mission objectives.

1894 **3.4.8 Risk Categories**

1895 Risk Categories are used to classify a risk. This table represents a sample of potential categories
1896 that may be applied to each risk.

- 1897
- 1898 • Safety - the risk that human and/or environmental safety are compromised by an incident
- 1899 in the manufacturing system.
- 1900 • Production - the risk that product quality and/or production goals are compromised by an
- 1901 incident in the manufacturing system.
- 1902 • Trade Secrets - the risk that intellectual property and sensitive business data are
- 1903 compromised by an incident in the manufacturing system.

1904

Risk Category	Risk Tolerance	Risk Appetite	Mission Objectives
Safety	Moderate	Moderate	Maintain human safety
			Maintain environmental safety
Production	Moderate	High	Maintain quality of product
			Maintain production goals
Trade Secrets	Moderate	Moderate	Maintain trade secrets

1905

1906 **3.4.9 Risk Reporting**

1907 This table describes the frequency and format of how the Director or IT Manager will document,
 1908 analyze, communicate, and escalate outcomes of the risk management processes.
 1909

Reporting Method	Description	Frequency
Risk Management log	A document to report the results of risk identification, analysis, and response planning	Twice a year
CSET Report	A document describing Risk assessment results	Twice a year
NamicSoft report	A document containing results of Nessus vulnerability scans.	Manual/Post vulnerability assessment

1910

1911 The Director will share the results of risk assessments (either the Risk Management Log or
 1912 CSET Report) with the CEO.

1913

1914 **3.4.10 Sample Risk Management Log**

1915 A Risk Log will be maintained by the Director of Operations and IT manager. These will be
 1916 reviewed in the project team meetings. This log captures the results of a qualitative and
 1917 quantitative risk analysis and the results of planning for response.

Risk	Category (Technical, Management, Contractual, External)	Probability (High / Likely to occur =3, Medium / May or May not occur =2, Low / Unlikely =1)	Impact (High = 3, Medium = 2, Low =1)	Score (Product of Probability x Impact 1-3 Green 4-6 Yellow 7-9 - Red)	Risk Mitigation Strategy (e.g. Avoid, Transfer, Mitigate or Accept the risk)	Actions required	Status (Open, closed, In Progress)	Due Date

1918

1919 **3.4.11 Periodic Review**

1920 This document will be reviewed and updated annually by the Director in consultation with the IT
 1921 Manager.

1922 Annual reviews will be conducted determining component value within the manufacturing
 1923 process being performed. Values will be used to determine required devices for continued
 1924 manufacturing process and the effects if a cyber incident occurs against a device.

1925 **3.4.12 Asset Criticality Matrix**

1926 After a list of Westman assets or systems of value requiring protection have been identified by
 1927 the Hardware Inventory process, they will be assigned a value. Asset Value is the degree of
 1928 impact that would be caused by the unavailability, malfunctioning or destruction of the asset.

1929

1930 Westman will use the following scale to calculate Asset value.

ASSET VALUE	
Critical	10
High	7-9
Medium	3-6
Low	1-2

1931

1932 **Critical** – Loss or damage of this asset would have grave / serious impact to the Operations of
 1933 the Manufacturing system directly impacting production. This can result in total loss of primary
 1934 services, core processes or functions. These assets are single point of failure.

1935 **High** - Loss or damage of this asset would have serious impact to the Operations of the
 1936 Manufacturing system directly impacting production. This can result in major loss of primary
 1937 services, core processes or functions. These assets can also be single point of failure.

1938 **Medium** - Loss or damage of this asset would have moderate impact to the Operations of the
 1939 Manufacturing system or Production. This can result in some loss of primary services, core
 1940 processes or functions.

1941 **Low** - Loss or damage of this asset would have minor to no impact on the Operations of the
 1942 Manufacturing system or Production. This can result in little or no loss of primary services, core
 1943 processes or functions.

1944

1945

1946 A list of assets belonging to Westman with assigned value is presented in the below table.

Asset	Value	Numeric Value
IT / Communication Systems	High	8
OT / Field Devices – PLC, HMI	Critical	10
OT / Machining Stations	High	8
OT / Robots	High	9
Electrical Systems	Critical	10
Utility Systems	Medium	6
Site	Medium	6

1947

1948 3.4.13 Definition and Acronyms

IT	Information Technology which includes devices such as servers, laptops, workstations, switches and routers.
OT	Operational Technology which includes Industrial control system devices that are used by the manufacturing process.
Vulnerability	A weakness or a flaw in the system which an attacker can exploit to gain access.

1949

1950 3.4.14 References

- 1951 1. Risk Management plan – Maryland Department of Information Technology
 1952 doit.maryland.gov/SDLC/Documents/Project%20Risk%20Managment%20Plan.doc
 1953
 1954 2. Sample Risk Management plan – State of North Dakota
 1955 [https://www.nd.gov/itd/sites/itd/files/legacy/services/pm/risk-management-plan-](https://www.nd.gov/itd/sites/itd/files/legacy/services/pm/risk-management-plan-sample.pdf)
 1956 [sample.pdf](https://www.nd.gov/itd/sites/itd/files/legacy/services/pm/risk-management-plan-sample.pdf)
 1957
 1958 3. Office of Management and Budget, “Management’s Responsibility for Enterprise Risk
 1959 Management and Internal Control”, *Office of Management and Budget*, OMB Circular
 1960 No. A-123, 2016. [Online]. Available:

- 1961 [https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf)
1962 [17.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf).
1963
1964 4. United States Agency for International Development, “U.S. Agency for International
1965 Development Risk Appetite Statement”, *United States Agency for International*
1966 *Development*, 2018. [Online]. Available:
1967 [https://www.usaid.gov/sites/default/files/documents/1868/USAID_Risk-Appetite-](https://www.usaid.gov/sites/default/files/documents/1868/USAID_Risk-Appetite-Statement_Jun2018.pdf)
1968 [Statement_Jun2018.pdf](https://www.usaid.gov/sites/default/files/documents/1868/USAID_Risk-Appetite-Statement_Jun2018.pdf).
1969
1970 5. Office of the Comptroller of the Currency, “Enterprise Risk Appetite Statement”, *Office*
1971 *of the Comptroller of the Currency*, 2016. [Online]. Available:
1972 [https://www.occ.treas.gov/publications/publications-by-type/other-publications-](https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/risk-appetite-statement.pdf)
1973 [reports/risk-appetite-statement.pdf](https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/risk-appetite-statement.pdf).

3.5 Incident Response Plan Document Example

Incident Response Plan for Westman

Document Owner:	Director of Operations, Westman
------------------------	---------------------------------

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major revision	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

3.5.1 Statement of Management commitment

Westman's leadership team is committed to information security and appropriate incident response to accidental or deliberate incident within the company. Westman has established the Incident Response Program to establish an actionable information security incident handling capability that includes preparation, detection, analysis, containment, recovery, and reporting for information security incidents. Westman's CEO oversees the Incident Response Program as a whole, supports and funds maintenance of the program and ensures that resources are appropriately maintained for preparedness.

3.5.2 Purpose

An incident can be defined as any event that, if unaddressed, may lead to a business interruption or loss. This document describes the plan for responding to information security incidents at Westman. It defines the roles and responsibilities of participants, characterization of incidents,

2001 relationships to other policies and procedures, and reporting requirements. The purpose of this
 2002 plan is to detect and react to security incidents, determine their scope and risk, respond
 2003 appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the
 2004 likelihood of the incident from reoccurring.

2005 This Plan is to be executed during or after a cybersecurity incident.

2006 3.5.3 Scope

2007 This plan applies to all the employees of Westman.

2008 3.5.4 Roles and Responsibilities

2009 The Westman Incident Response Team is comprised of:

ROLE	RESPONSIBILITIES	CONTACT DETAILS
Director of Operations	<ul style="list-style-type: none"> Supervise other employees and working of the organization. Serves as a primary point of contact for any type of incident Making sure that all employees understand how to identify and report a suspected or actual security incident Leading the investigation for any type of incident, initiating the Security Incident Response Plan, filling out the Incident Report Form and reporting status to the CEO as needed. Documenting details of all incidents. 	Name: Phone: Email:
Control Engineer(s)	<ul style="list-style-type: none"> Reporting a suspected or actual security incident to the Director. Reporting any other operational issues or concerns to the Director Complying with the security policies and procedures of Westman. 	Names: Phone: Email:

IT Manager	<ul style="list-style-type: none"> • Manages access to systems and applications for internal staff. • Complying with the security policies and procedures of Westman. • Assist in investigation, troubleshooting and resolving any IT/OT related incident summoned for. • Advising the Director for any recommendations to procedures, policies and best practices. 	Name: Phone: Email:
General Counsel	<ul style="list-style-type: none"> • Handling of any legal questions/issues relating to security incidents. • Handling of any external communications related to security incidents. 	Name: Phone: Email:
HR Manager	<ul style="list-style-type: none"> • Handling of any personnel and disciplinary issues relating to security incidents. • Inform Law Enforcement if security incident involves data breach of sensitive information. 	Name: Phone: Email:

2010

2011 **3.5.5 Categories of Incident**

2012 Westman defines the following categories/types of incident for internal classification. These
2013 have been mentioned in the Incident Reporting Form as well.

- 2014 • Intrusion
- 2015 • Denial of Service
- 2016 • Loss of Power
- 2017 • Virus / Malware
- 2018 • Social Engineering (Phishing, Phone, Email etc.)
- 2019 • Data Breach
- 2020 • Hardware Stolen
- 2021 • User account compromise
- 2022 • System Misuse
- 2023 • Technical Vulnerability

2024

2025 **3.5.6 Severity Classification**

2026 The Severity of an incident is determined based on the impact to the company and the urgency of
2027 restoration.

SEVERITY	DEFINITION
High	<ul style="list-style-type: none"> • All users of the company are affected • Work stoppage situation • The incident involves sensitive data breach. • The incident threatens Westman's operational goals • There is no viable workaround
Medium	<ul style="list-style-type: none"> • There is a viable workaround • Moderate to Low impact to the Operations. • Service interruption potentially affects specific users and does not involve sensitive or personal data breach.
Low	<ul style="list-style-type: none"> • No impact to operations. • Service interruption potentially affects only one person and does not involve sensitive or personal data breach.

2028

2029 **3.5.7 Restoration Priorities**

RESTORATION PRIORITIES	DEFINITION
High	<ul style="list-style-type: none"> • Service Restoration must be completed immediately, or significant loss of revenue, reputation, or productivity will occur.
Medium	<ul style="list-style-type: none"> • Service Restoration must be completed within two business days or there is a potential for significant loss of revenue, reputation or productivity.
Low	<ul style="list-style-type: none"> • Service Restoration can be delayed up to three or more business days without loss of revenue, reputation or productivity.

2030

2031 3.5.8 Incident Response Policy

- 2032 1. An incident upon detection or being reported needs to be thoroughly investigated as per the
2033 process defined under “Detection and Analysis” step of the IR process in the next section.
2034 The investigation may be performed by the Director or by convening an IR Team.
- 2035 2. The incident needs to be classified as per the categories defined previously.
- 2036 3. Upon Investigation, the impact to the Manufacturing system must be determined. The IR
2037 Team may co-relate detected event information with Risk assessment outcomes to achieve
2038 perspective on the incident impact across the Organization. The incident will accordingly be
2039 assigned a Severity level and reported to the CEO. The Incident Report Template form
2040 should be used for this purpose.
- 2041 4. During the “Detection and Analysis” step, detailed troubleshooting or forensic analysis
2042 should be performed to determine the root cause. This may be done using in place log
2043 management tools or commercial products such as Wireshark.
- 2044 5. Upon investigation, the incident must be mitigated as per the “Containment, Eradication and
2045 Recovery” step of the IR Process.
- 2046 6. The Director of Operations or IT Manager will co-ordinate incident response plan with
2047 Westman stakeholders.
- 2048 7. The Director of Operations or CEO will share information about any cybersecurity incidents
2049 and its mitigation with its designated sharing partners.
- 2050 8. The overall Incident Response process and plan will be revised or improved after every
2051 incident. Procedures must be updated regularly to address evolving threats such as APTs,
2052 Organizational changes, Manufacturing changes and/or after any problems discovered during
2053 implementation, execution or testing
- 2054 9. User awareness Training and Testing procedures will be updates after every incident.
- 2055 10. The Director will communicate any changes or updates made to this policy.

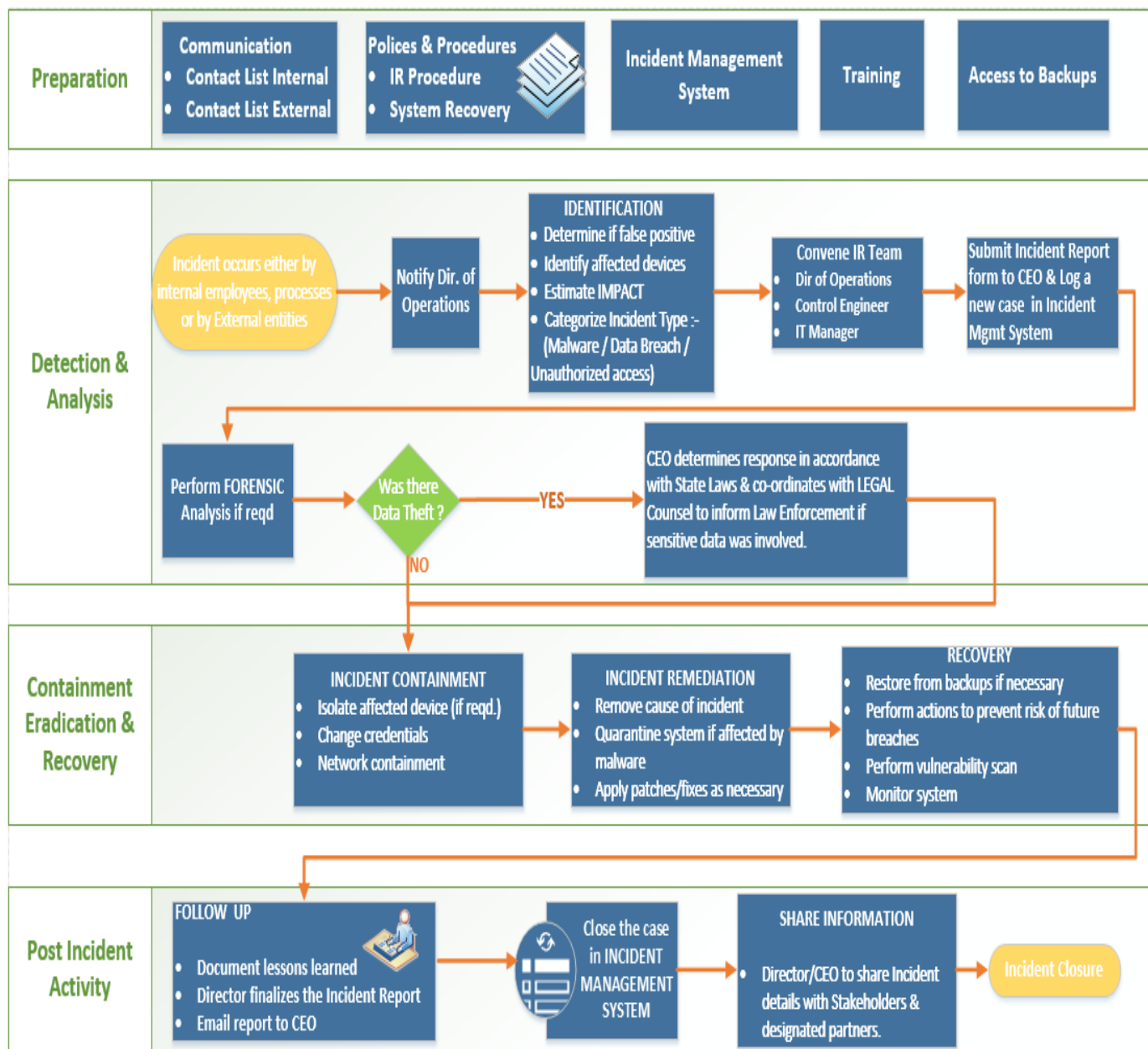
2056 3.5.9 Incident Plan Response Process / Workflow

2057 The [NIST Computer Security Incident Handling \[1\] Guide](#) divides the incident response lifecycle
2058 into the following four steps:

- 2059 1. Preparation
- 2060 2. Detection and Analysis
- 2061 3. Containment, Eradication and Recovery
- 2062 4. Post-incident Activity

2063
2064

2065 Westman' IR process contains the following activities corresponding to each of the above steps:



2066

2067 3.5.10 Guidelines for Information Sharing

2068 Interactions with Law Enforcement

- 2069 • All communications with external law enforcement authorities should be made after
- 2070 consulting with the CEO/General Manager.
- 2071 • The Director of Operations will co-ordinate with the CEO and IT Manager to determine and
- 2072 share the minimum necessary information as required for incident response.

2073 Communications Plan

- 2074 • The CEO will share information about any cybersecurity incidents and its mitigation with its
2075 designated sharing partners. Refer to the Next section for additional details
- 2076 • All public communications about an incident or incident response to external parties outside
2077 of Westman are made in consultation with the CEO.
- 2078 • The minimum information necessary to share for a particular incident is determined by the
2079 CEO in consultation with Director and other staff.

2080 3.5.11 Guidelines for Reporting to Stakeholders**2081 Overview:**

- 2082 • The Director of Operations will compile all the details of incident(s) occurred in consultation
2083 with the IT manager.
- 2084 • The Director will share the details in the IR Report Template form with CEO/General
2085 Manager and General Counsel. This will be used to determine level of severity, allowing the
2086 company to plan according.
- 2087 • The Company's leadership team consisting of CEO/General Manager, Director of
2088 Operations, General Counsel, and IT Manager will make sure all facts have been gathered
2089 relating to the security incident before addressing any concerned with outside parties.
- 2090 • The Company's response needs to be consistent ensuring message being delivered will not
2091 need to be retracted or changed due to lack of clarity.

2092 Who will be responding:

- 2093 • Depending on the severity of the security incident this role can be filled by CEO/General
2094 Manager, Directory of Operations or the General Counsel.
- 2095 • If the severity of a security incident requires additional resources, they should be contacted
2096 and brought in to help gather forensic information along with responding to inquiries.
 - 2097 ○ Examples:
 - 2098 ■ Public Relation
 - 2099 ■ Forensic Investigator
 - 2100 ■ IT consultant (Work in conjunction with IT Manager)
 - 2101 ■ Security Consultant (Work in conjunction with IT Manager and Director of
2102 Operations)
 - 2103 ■ Law Enforcement (Depends on severity)

2104 Notification:

- 2105 • General Counsel will oversee notification planning since the potential for legal actions
2106 against Westman arising from security incident in question.
- 2107 • If required, an outside Public Relations firm may be required depending on the severity level
2108 of the incident to help with crafting a response.

- 2109 • General Counsel approval is required for work with any outside agency.
- 2110 • CEO and General Counsel will both approve all communication being sent out regarding a
- 2111 security incident.

2112 **Communications:**

- 2113 • CEO/General Manager will contact primary partners/vendors via phone call to inform them
- 2114 of the security incident. This should be done once all information has been gathered and a
- 2115 corporate response has been prepared.
- 2116 • No voicemails will be left concerning the security incident in question. If recipient is
- 2117 unavailable schedule a follow up call.
- 2118 • Director of Operations, Director of Marketing, Controller/Finance, General Counsel and IT
- 2119 Manager are the **only** Westman employees authorized to call partners/vendors not already
- 2120 contacted by CEO/General Manager.
- 2121 • Responses to partners/vendors should be scripted to ensure the delivered message is
- 2122 consistent, while ensuring only information regarding security incident are discussed.
- 2123 • Email communication will be completed as a follow-up to a phone.
- 2124 • Any email communications being sent will have additional proof reading completed by either
- 2125 Director of Operations, Controller/Finance, General Counsel, IT Manager.
- 2126 • Depending on the impact of security incident a Public Relation firm may be required to help
- 2127 with a response when providing communications via electronic or verbal.
- 2128 • Media communication can **ONLY** be approved by CEO/General Manager and General
- 2129 Counsel.

2130

2131 **Restoring Trust:**

- 2132 • Westman's CEO or Director of Operations with the advice consultants and Forensic experts
- 2133 will notify partners/vendors and customers with the steps being taken to restore and strength
- 2134 system security.
- 2135 • Westman IT Manager, Director of Operations will discuss with employees what caused
- 2136 security incident and what is being done to avoid a similar issue in the future.
- 2137 • Once the security incident has been resolved and all fact are known Westman leadership
- 2138 team will provide a full report which will be made publicly available containing facts
- 2139 relating to the security incident, along with the steps being taking to safe guard IT
- 2140 infrastructure ensuring this and future events don't happen again.

2141 **3.5.12 Incident Report Form Template**

Incident Reporting Template Form			
Contact information			
Date Reported :			Time Reported:
Name:	Title:	Dept:	
Office Phone:			
Details			
Date of Incident :	Time of Incident:		
Type of Incident - Check all that apply			
<input type="checkbox"/> Intrusion	<input type="checkbox"/> Social Engineering (Phishing, Phone,Email etc)	<input type="checkbox"/> Technical Vulnerability	
<input type="checkbox"/> Denial of Service	<input type="checkbox"/> Data breach	<input type="checkbox"/> System misuse	
<input type="checkbox"/> Loss of power	<input type="checkbox"/> Hardware stolen	<input type="checkbox"/> Others, pls specify	
<input type="checkbox"/> Virus / Malware	<input type="checkbox"/> User account compromise		
Incident Description			
Provide a brief description:			
Impact / Potential impact - Check all of the following that apply to this incident.			
<input type="checkbox"/> Loss / Compromise of Data	<input type="checkbox"/> Financial Loss		
<input type="checkbox"/> Damage to systems	<input type="checkbox"/> Other Organizations affected		
<input type="checkbox"/> Damage to public	<input type="checkbox"/> Damage to Integrity or Delivery of Goods, Services		
<input type="checkbox"/> System downtime	<input type="checkbox"/> Unknown at this time		
Provide a brief description:			
Affected System(s) information			
Host	IP	Application (if any)	O.S
Sensitivity of Data compromised (incase of Data loss)			
<input type="checkbox"/> Public (Information is already approved for release & unauthorized disclosure will not cause problems for the Company).			
Internal Use (Information is intended for internal use within the Company or with other affiliated orgnizations, business partners.			
<input type="checkbox"/> Unauthorized disclosure may be against laws, regulations and may harm the Company or its business partners or its customers. For example: Email contacts, emails etc).			
Confidential (Related to Privacy Violation. Information is private & sensitive in nature. It must be restricted to those with legitimate			
<input type="checkbox"/> business need for access. Unauthorized disclosure is against laws, regulations and will harm the Company or its business partners or its Customers. For example: Trade secrets, Software code, Citizen's data etc).			
Details of the Data loss			
Provide a description of what was compromised:			
Follow up action taken so far			
<input type="checkbox"/> Law enforcement notified	<input type="checkbox"/> System disconnected from Network.		
<input type="checkbox"/> Restored backups	<input type="checkbox"/> Log files examined		
<input type="checkbox"/> AV Virus definition updated	<input type="checkbox"/> Any other action taken, pls specify		
<input type="checkbox"/> System reimaged or quarantined	<input type="checkbox"/> No action taken		
Supervisor's Name:			
Supervisor's Signature:		Date:	

2142

2143 **3.5.13 Definitions and Acronyms**

CEO	Head of the organization. Serves as an escalation point.
HR Manager	An employee who deals with recruitment efforts and overall administration.
Incident	An event that is not part of normal operations that disrupts operational processes.
Director of Operations	An employee who supervises other employees and working of the organization.
Vulnerability	A weakness or flaw in the system which an attacker can exploit to gain access to.
Vulnerability Scan	The act of scanning a device or network for vulnerabilities
Control Engineer	An employee who operates the manufacturing equipment and reports to Director of Operations
Legal Counsel	Handles all legal matters. Reports to the CEO.
Stakeholders	Business Owners, System Owners, Integrators, Vendors, Human Resources Offices, Physical and Personnel Security Offices, Legal Departments, Operations Personnel.

2144

2145

2146 **3.5.14 References**

2147 1. NIST Publication for handling Computer Security Incident

2148 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

2149

3.6 Incident Recovery Plan Document Example

<p style="text-align: center;">Incident Recovery Plan</p> <p style="text-align: center;">for</p> <p style="text-align: center;">Westman</p>
--

Document Owner:	Director of Operations, Westman
------------------------	---------------------------------

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Director of Operations
2.0	04-21-2018	Major changes to the initial draft	Director of Operations

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	CEO/General Manager		4-22-2018

3.6.1 Scope

The scope and purpose of this document is to inventory all of infrastructure and capture information relevant to the Westman's ability to recover its IT/OT environment from a cybersecurity incident. It, in turn also aims to provide an effective and efficient recovery effort.

3.6.2 Objectives

This plan has been developed to accomplish the following objectives:

1. Limit the magnitude of any loss by minimizing the duration of a critical application service interruption.
2. Assess damage, repair the damage, and activate the repaired computer center.
3. Manage the recovery operation in an organized and effective manner.

4. Prepare technology personnel to respond effectively in an incident recovery situation.

This IR Plan is to be executed during or after a cybersecurity incident.

The person discovering the incident must notify the Director of Operations or IT Manager, who collectively assume responsibility for deciding which - if any - aspects of the IR plan should be implemented, and for establishing communication with employees, management, partners and customers.

3.6.3 RPO and RTO Targets

Westman defines the following SLA's or Restoration times for operations recovery

Type of Incident	RTO [2]	RPO [2]	Restoration Priority
Environmental Disasters such as Fire, Flood.	72 hours	24 hours	High
Recovery from Virus/Malware attack	24 hours	24 hours	High
Recovery from user account compromise	24 hours	24 hours	Medium
Recovery from Data Breach	48 hours	24 hours	High
Hardware failure, System Parts Replacement	48 hours	24 hours	High

Westman's Incident Response (IR) Team will consists of the following individuals.

ROLE	RESPONSIBILITIES
Director of Operations	<ul style="list-style-type: none"> Lead and oversee the entire IR process Contact any Contractors/Vendors for assistance as needed. Making sure that all employees understand their roles and responsibilities. Update this document as per the Maintenance policy Notify the CEO for any escalation issues.
CEO / President	<ul style="list-style-type: none"> Assist the IR Lead (Director) in their role as required. Make any Business decisions that are out of scope for the Director. Serve as point of escalation for any issues.

Control Engineers, IT Staff	<ul style="list-style-type: none"> • Install, implement or assist in implementing any tools, hardware software and systems as required • Escalate any issues related to recovery to the Director. • Complying with this plan.
OT Contractors, Vendors	<ul style="list-style-type: none"> • Assist in Recovery, Troubleshooting and resolving any OT related incident summoned for • Advising the Director for any recommendations to procedures, policies and best practices. • Complying with this plan

2192

2193 **3.6.4 Contact Information**

Name	Title	Contact Type	Contact Information
Employee A	ABC	Work	555-555-5555 ext 2
		Mobile	
		Alternate	
		Email	
Employee B	ABC	Work	555-555-5555 ext 3
		Mobile	
		Alternate	
		Email	
Employee C	ABC	Work	555-555-5555 ext 4
		Mobile	
		Alternate	
		Email	

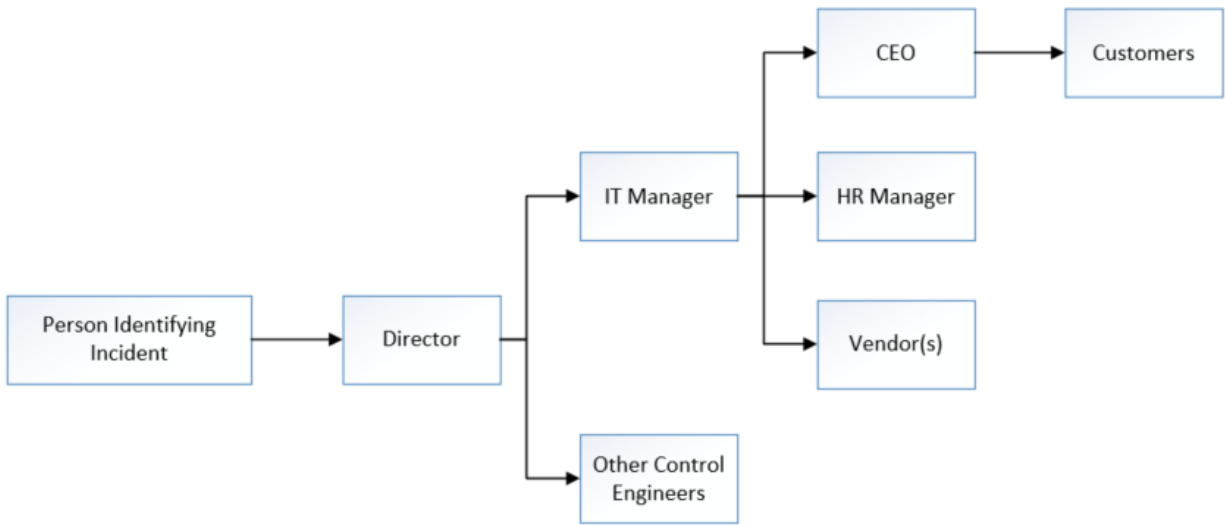
2194

2195

2196 **External Contacts**

Name	Title	Contact Type	Contact Information
Account #		Mobile	
		Alternate	
		Email	
IT Contractor		Work	
Account #		Mobile	
		Alternate	
		Email	
OT Contractor		Work	
Account #		Mobile	
		Alternate	
		Email	
Network Provider		Work	
Account #		Mobile	
		Alternate	
		Email	
Telecom Carrier		Work	
Account #		Mobile	
		Alternate	
		Email	
Insurance Provider		Work	
Account #		Mobile	
		Alternate	
		Email	
Hardware Provider		Work	
Account #		Mobile	
		Email	

2197

2198 **3.6.5 Notification Calling Tree**

2199

2200

2201 **3.6.6 Communications**2202 **Notification**

- 2203 • The Director of Operations in consultation with the IT manager and Control Engineers will
- 2204 periodically update the CEO, Executives on the progress of Recovery Activities.
- 2205 • General Counsel will oversee notification planning since the potential for legal actions
- 2206 against Westman arising from security incident in question.
- 2207 • If required, an outside Public Relations firm may be required depending on the severity level
- 2208 of the incident to help with crafting a response.
- 2209 • General Counsel approval is required for work with any outside agency.

2210 **Communications**

- 2211 • CEO/General Manager will contact primary partners/customers via phone call to inform
- 2212 them about Recovery activities. This should be done once all information has been gathered
- 2213 and a corporate response has been prepared.
- 2214 • Director of Operations, Director of Marketing, Controller/Finance, General Counsel and IT
- 2215 Manager are the **ONLY** Westman employees authorized to call partners/vendors not already
- 2216 contacted by CEO/General Manager.
- 2217 • Responses to partners/vendors should be scripted to ensure the delivered message is
- 2218 consistent, while ensuring only information regarding security incident are discussed.
- 2219 • Email communication will be completed as a follow-up to a phone.
- 2220 • Any email communications being sent will have additional proof reading completed by either
- 2221 Director of Operations, Controller/Finance, General Counsel, IT Manager.

- 2222 • Depending on the impact of security incident a Public Relation firm may be required to help
2223 with a response when providing communications via electronic or verbal.
- 2224 • Media communication can **ONLY** be approved by CEO/General Manager and General
2225 Counsel.

2226 **Restoring Trust**

- 2227 • Westman's CEO or Director of Operations with the advice consultants and Forensic experts
2228 will notify partners/vendors and customers with the steps being taken to restore and strength
2229 system security.
- 2230 • Westman's IT Manager, Director of Operations will discuss with employees what caused
2231 security incident and what is being done to avoid a similar issue in the future.
- 2232 • Once the security incident has been resolved and all fact are known Westman leadership
2233 team will provide a full report which will be made publicly available containing facts
2234 relating to the security incident, along with the steps being taking to safe guard IT
2235 infrastructure ensuring this and future events don't happen again.

2236 **3.6.7 Plan Testing and Maintenance**

2237 **Maintenance**

- 2238 • The IRP will be revised and updated after every recovery executed following a
2239 cybersecurity incident, Organizational changes, Manufacturing changes and/or after any
2240 problems discovered during implementation, execution or testing.
- 2241 • The Director of Operations will be responsible for updating the document in consultation
2242 with Machine Operators and other personnel as required.
- 2243 • During Maintenance periods, any changes to the IR Team must be accounted for.
- 2244 • The plan will be updated after any Organizational or Manufacturing System changes.

2245 **Testing**

- 2246 • Walkthroughs- IR Team members will verbally go through the specific steps as
2247 documented in the plan to confirm effectiveness, identify gaps or other weaknesses. The
2248 team should be familiar with procedures, equipment and operations.
- 2249 • Simulations- An incident is simulated so that normal operations will not be interrupted.
2250 Hardware, software, personnel, communications, procedures, supplies and forms,
2251 documentation and utilities should be thoroughly tested in a simulation test.
- 2252 • Full-Interruption Testing- IR Team members will perform a full-interruption test to
2253 activate a total IRP scenario. Caution must be exercised as this type of test disrupts
2254 normal operations.

2255

2256 **3.6.8 Hardware Information**

SYSTEM TYPE	HARDWARE INFORMATION	
IT Servers	Hostname: FGS-47631EHH System Model: HP Z230 IP Address: 172.16.3.10 Network: Engineering LAN Location: Cabinet 101 Type: Physical Other: Eng. Workstation, Windows 7	Hostname: FGS-61338PSH System Model: Supermicro Z97X IP Address: 172.16.2.3 Network: Supervisory LAN Location: Cabinet 101 Type: Physical Other: Plant Simulator, Windows 7
	Hostname: FGS-613380SH System Model: Supermicro Z97X IP Address: 172.16.2.5 Network: Supervisory LAN Location: Cabinet 101 Type: Physical Other: OPC Server, Windows 7	Hostname: FGS-61338CH System Model: Supermicro Z97X IP Address: 172.16.1.5 Network: Control LAN Location: Cabinet 101 Type: Physical Other: Controller, Windows 7
	Hostname: FGS-61338HH System Model: Supermicro Z97X IP Address: 172.16.1.4 Network: Control LAN Location: Cabinet 101 Type: Physical Other: HMI Server, Windows 7	Hostname: WIN-FPVTDCDEUCR System Model: Supermicro Z97X IP Address: 172.16.2.14 Network: Supervisory LAN Location: Cabinet 101 Type: Virtual Other: Controller, Windows 2008
Network Devices	Model: Allen Bradley 8300 Management IP: 10.100.2.8 Location: Cabinet 101 Function: Boundary Router	Model: Allen Bradly 5700 Management IP: N/A Location: Cabinet 101 Function: Supervisory LAN Switch
	Model: Allen Bradly 5700 Management IP: N/A Location: Cabinet 101 Function: Control LAN SW	
OT Devices	Model: Allen Bradley Logix 5571 IP Address: 172.16.2.102 Location: Cabinet 101 Function: PLC	

2257 **3.6.9 Backup Strategy**

SYSTEM TYPE	BACKUP STRATEGY
IT Servers	Frequency Weekdays (M-F): Directory level backup using Veeam Quarterly: Full system image backup using Veeam
Application Code	Source code is checked into a secure central network share. Server hosting the network share is backed up using Veeam.
Network Devices Boundary Router	Frequency: Quarterly - Manual using Manufacturer Instructions <u>Note:</u> All Allen Bradley devices support Cisco IOS Command line. 1.SSH into the network switch/router from a Windows workstation which has a TFTP server installed. 2. Log in > Enter “ enable ” mode > Issue a “ copy running-config tftp ” command > Supply the IP address of TFTP Server > Give the backup file a meaningful name > Hit Enter. 3.The backup file will then be transferred over to the Windows workstation. Once done, copy the file over to a central secure location.
OT Devices	Frequency: Quarterly - Manual using Manufacturer Instructions. 1.Control Engineer to either download the current image off the PLC using RSLINX Configuration Utility installed on the Workstation or pull out the MicroSD Card from the PLC and access the image using a card reader. For instructions on using RSLINX, refer to the product manual [3]

	2.Copy over the image to the central secure location before making any change or upgrading the program.
--	---

2258

2259 **3.6.10 Recovery Procedures**

- 2260 • The Incident Recovery plan will be executed following a cybersecurity incident.
- 2261 • Any exceptions or issues during the Recovery process must be communicated to the Director
- 2262 and/or IT Manager.
- 2263 • Depending on the incident, and on the number and nature of the IT services affected, one or
- 2264 more of the following IR procedures may be activated by the IR team:

Type of Incident	Plan of Action
Environment Disaster – Fire, Flooding	<ol style="list-style-type: none"> 1. Identify root cause, co-ordinate initial response 2. Remove damaged systems from the work cell. 3. Evaluate damage 4. Review Insurance policies and reach out to Insurance companies. 5. Procure new hardware systems as required. Reach out to a Data recovery company for data recovery from damaged hard drives.
Virus / Malware – IT / OT Systems	<ol style="list-style-type: none"> 1. Disconnect the affected systems from the network. 2. Reach out to the IT/OT Contractor for assistance. 3. Perform a full manual Anti-virus scan on the system 4. If the Anti-virus software cannot detect or quarantine the infection, you may need to reinstall or restore the entire Operating System. Use Veeam to restore a full image backup, if the system in question is an IT system.

	<p>5. Upon reinstalling the operating system, install all the appropriate patches to fix known vulnerabilities.</p> <p>6. Depending on the nature of the virus attack, change your original passwords as these could have been compromised during the infection.</p>
Data Theft	<p>1. Fulfill all legal obligations. The CEO/General Manager to inform law enforcement and other customer protection agencies notifying them of breach.</p> <p>2. Immediately change system credentials, account passwords to public websites (if personal data is involved)</p> <p>3. Monitor in-house security controls or tools for any signs of new activity.</p> <p>4. Identify and erase any new files or programs that may have been installed as part of this attack. Use system baselines for reference.</p> <p>5. Engage a Contractor or other professional to conduct security audit.</p>
Data Loss - IT Systems	<p>1. Browse through the list of directory level backups captured by Veeam for that host to select the backup to restore data from.</p> <p>2. Initiate a restore of the file or directory from the affected system using Veeam. If the system in question is a virtual machine, restore the most recent full VM image as it is using Veeam.</p> <p>3. Verify the file, folders and their permissions upon completion of the restore.</p>

Hardware failure – IT Systems	<ol style="list-style-type: none">1. Follow up with the vendor for getting the faulty hardware replaced.2. Install and setup the new hardware as per the original baseline configuration.3. Refer to File system table below to configure any File system dependencies such as NFS mount points.4. Initiate a Restore operation from the most recent backup using Veeam. The restore procedure varies depending on if the system is physical or virtual. For more details, refer to the Veeam Backup guide.5. Upon completion of restore, verify connectivity and operations.
Hardware failure –Network Devices	<ol style="list-style-type: none">1. Order a replacement from a vendor.2. Setup and configure the new device as per its original counterpart. For more details, refer to the asset inventory database and/or any supporting documentation to reference the original baseline config such as Firewall rules, ACLS, Vlan, etc.3. Restore system configuration using Manufacturer instructions from the secure central repository.4. Verify connectivity between devices. Run operations to confirm.

Hardware failure / Configuration Restore- OT Systems	<ol style="list-style-type: none"> 1. Order a replacement from a vendor. 2. Setup the new device by assigning it the original static IP address and restore the configuration on it as per manufacturers manual. Following are high level instructions for config restore of the Allen Bradley PLC <ul style="list-style-type: none"> ➤ Pull out the microSD card from the PLC and load a previously saved image on it using a card reader. A working image can be pulled from the central secure location used to save backups. Alternatively, a new base image can also be obtained from the manufacturer. ➤ Insert the microSD card back into the PLC and power on the device. ➤ Test Connectivity and operations.
---	---

Filesystems as of Sep 2018

Host	Local Drives	Size	Network Drives
FGS-47631EHH	C:\	465GB (500GB HDD)	
FGS-61338PSH	C:\	233GB (250GB HDD)	
FGS-613380SH	C:\	465GB (500GB HDD)	H:\ HMI_Share (\\172.16.1.4)
FGS-61338CH	C:\	233GB (250GB HDD)	
FGS-61338HH	C:\	233GB (250GB HDD)	O:\ OPC_Share (\\172.16.2.5)
FGS-61338LHH	C:\	465GB (500GB HDD)	
WIN-FPVTDCDEUCR	C:\	50GB	W:\ Eng_Workstation (\\172.16.3.10)

3.6.11 Restoration Priorities

Should an incident occur and Westman need to exercise this plan, this section will be referred to reference restoration priorities in bringing systems online.

2273 **IT Systems**

Priority	IT System	Description
High	LAN-AD	Active Directory / DNS Server
High	Veeam	Veeam Backups Server
High	FGS-613380SH	OPC Server
High	FGS-61338CH	Controller Server
High	FGS-61338HH	HMI Server
High	FGS-61338LHH	Local Historian Host server
High	WIN-FPVTDCDEUCR	Local Historian Database Virtual Machine
Medium	FGS-61338PSH	Plant Simulator
Medium	FGS-47631EHH	Engineering Workstation
Medium	PI-DMZ	DMZ Historian Database Server
Medium	SymantecMgr	Symantec Antivirus
Low	Security Onion	Snort IDS
Low	Graylog	Syslog server
Low	GTB Inspector	DLP
Low	Hive	Incident Response Server

2274

2275

2276 **Networking Equipment**

Priority	Device Info	Description
High	Boundary Router	Allen Bradley Router 8300
High	Supervisory LAN Switch	Allen Bradley Stratix 5700
High	Control LAN Switch	Allen Bradley Stratix 5700

2277

2278 **OT Systems**

Priority	OT System	Description
High	PLC	Allen Bradley Control Logix 5571
High	HMI Server	Factory Talk View Studio

2279

2280 **3.6.12 Definitions and Acronyms**

SLA	Service Level Agreement
Recovery Time Objective (RTO)	RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the Maximum Tolerable Downtime. [2]
Recovery Point Objective (RPO)	The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. [2]

2281

2282 **3.6.13 References**

- 2283 1. SANS Guide for DR: [https://www.sans.org/reading-room/whitepapers/recovery/disaster-](https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564)
2284 [recovery-plan-strategies-processes-564](https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564)
2285 2. NIST SP 800-34 Contingency planning guide for Federal Systems
2286 <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf>

- 2287 3. Allen Bradley ControlLogix 5571 Manual
2288 [https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-](https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf)
2289 [um001_-en-p.pdf](https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf)

4. Technical Solution Implementations

4.1 Introduction

This section includes proof-of-concept technical solution implementations developed for the fictional company Westman. An overview of these technical solutions is discussed in Section 6 of Volume 1 and potential technical solutions are discussed in Section 7 of Volume 1. Each organization's information security experts should identify the technical solutions that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

There are five main areas of performance indicators being collected in the Process Control System:

1. Manufacturing process performance: measures the performance of the manufacturing process, i.e. the chemical continuous process.
2. Network performance: measures the performance of the underlying TCP/IP network.
3. Computing resources performance: measures the performance of the computers, hardware, and software processes.
4. Industrial protocol performance: measures the performance of the industrial communication protocol, i.e. the DeviceNet in the PCS.
5. OPC Data Exchange performance: measures the performance of the data exchange mechanism of the system.

Measurements in different areas provide insight of the entire system performance from different perspectives. The manufacturing process performance provides indicators on how well the high-level manufacturing process and overall system perform. However, this may not be able to provide enough detail on the performance of the sub-systems, therefore measurements are also performed at sub-system levels. For example, a typical chemical continuous manufacturing is a relatively slow process in comparison with computer networking. Therefore, a moderate TCP/IP network delay may not reflect in the measurement of the high-level manufacturing process performance. However, such TCP/IP delay may have significant impact on the sub-systems. The effects will not be reflected in the high-level measurement until significant delays are accumulated in sub-systems. Measurements in multiple levels provide details and in-depth understanding to key performance areas of the entire system. It helps to understand how the aggregate effects will impact the performance. Aggregate effects will be important to the high-level manufacturing performance.

Each of the technical solution implementation is organized as an experiment. For the measurement purpose, each experiment has a fixed runtime of 4 hours (14,400 seconds). Performance metrics and network packet capture are collected during the entire experiment run.

After the experiment is completed, all the collected metrics and network packet capture will go through the post processing stage to filter, sort and rearrange data in proper order. The last step is to compute the key performance indicators from the sorted dataset using a set of Python scripts developed by NIST.

2328 More technical detail of the Process Control System and the measurement process is described in
2329 [NISTIR 8188: Key Performance Indicators for Process Control System Cybersecurity](#)
2330 [Performance Analysis.](#)

2331 **4.1.1 Implementation Note – Due Diligence Implementing Technical Solutions**

2332 It is important to note that the procedures used during this implementation (i.e., install a tool,
2333 then measure the impact) should not be used in a production system. Care must be taken before
2334 using any technical solutions, especially those that actively scan the manufacturing system
2335 network and its devices; manufacturers should first conduct an assessment of how these tools
2336 work and what impact they might have on the connected control equipment [3]. Technology
2337 evaluations may include testing in similar, non-production control system environments to
2338 ensure that the tools do not adversely impact the production systems. Impact could be due to the
2339 nature of the information or the volume of network traffic. While this impact may be acceptable
2340 in IT systems, it may not be acceptable in a manufacturing system. In general, any operation that
2341 actively scans the manufacturing network should be scheduled to occur only during planned
2342 downtimes. [3]

2343

2344 4.2 Open-Audit

2345 4.2.1 Technical Solution Overview

2346 Open-Audit is an asset inventory tool providing scanning of hardware and software within the
2347 manufacturing environment. Open-Audit scans are highly customizable to each environment,
2348 depending on the level required. The cost depends on the level of functionality desired for your
2349 environment. Editions offered by Open-Audit vary from entry level community edition which is
2350 free, all the way up to enterprise edition. Enterprise was chosen since it contains the ability to
2351 setup schedule scanning, dashboards, and baselining of equipment.

2352
2353 Open-Audit is a downloadable OVA which is easy to install. OVA install allows installation in
2354 a Hyper-Visor environment allowing for installation within an existing virtual environment
2355 without requiring purchasing additional hardware. Configure for initial discovery scans are
2356 straight forward and easy to configure and perform.
2357

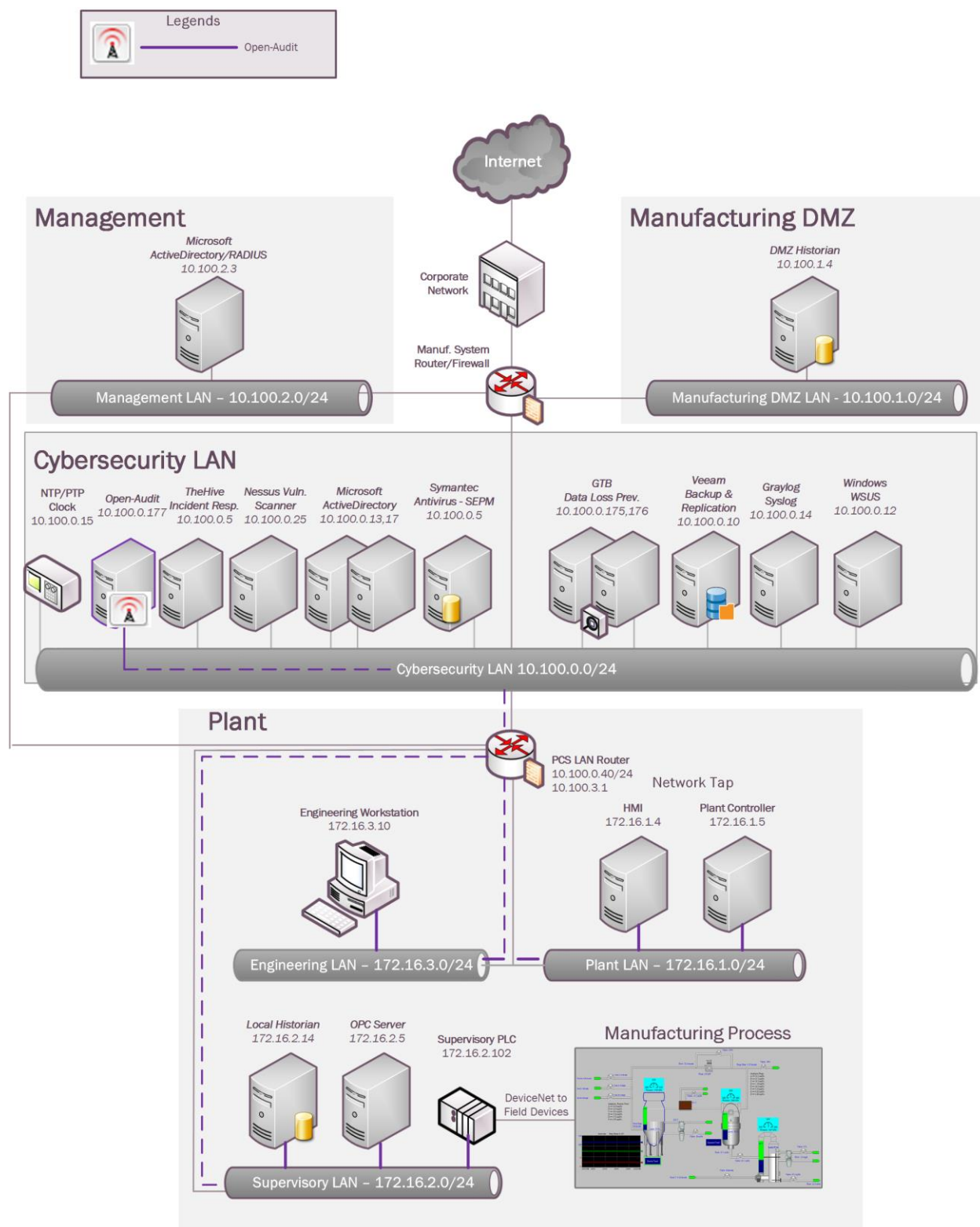
2358 4.2.2 Technical Capabilities Provided by Solution

2359 Open-Audit provides components of the following Technical Capabilities:

- 2360 • Hardware Inventory
- 2361 • Software Inventory
- 2362 • System Development Lifecycle Management
- 2363 • Configuration Management
- 2364 • Baseline Establishment (Enterprise Edition)
- 2365 • Change Control

2366 4.2.3 Subcategories Addressed by Implementing Solution

2368 ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, PR.DS-3, PR.IP-1, PR.IP-2, PR.IP-3, PR.IP-4,
2369 PR.IP-6, PR.MA-1, DE.AE-1, DE.CM-7

2370 **4.2.4 Architecture Map of Where Solution was Implemented**

2371

4.2.5 Installation Instructions and Configurations

Prerequisites:

- Identify if physical hardware or virtual machine will be used
- Requirements from Opmantek who developed “**Open-Audit**” indicate the specification required are low. Please see this link for exact details provided by the vendor [link](#).

Instructions:

Download:

1. Download and save **Opmantek Virtual Appliance** from Opmantek website.¹¹



Opmantek Virtual Appliance

8.6.3g

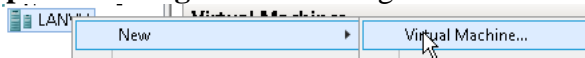
Experience the power of the complete Opmantek suite in one easy-to-install Virtual Appliance. This package includes NMIS8, Open-Audit, and all downloadable commercial modules. This package is created by Opmantek and is the easiest way to try out all our apps without the bother of setting up a dedicated server.

[Virtual Appliance](#)
[Release Notes](#) [Installation Guide](#)

- Once download has completed “.ova” file will need to be extracted to view the contents and move to the next step (any tool supporting extracting .ova and .gz can be used).
- Open the folder where the files were extracted too. There should be a total of four files.
- Next, extract the two files with extension (.vmdk.gz) since this file is still compressed. Once completed two files with the same extension (.vmdk) should now exist.
- Now two files just extracted need to be convert to “**VHDX**” format, so we can run these disk in a Hyper-V environment. See this link for instruction and additional information useful for converting virtual drive format.
- Once both drives have been converted to “**VHDX**” format proceed to next section.

Virtual Machine Setup:

1. On the virtual server host open “**Hyper-V Manager**” and then right click on server name selecting **New Virtual Machine**
2. Now type in the name you going to give this server.



¹¹ Opmantek Intelligent Network Management Software <https://opmantek.com/>

- 2396 3. Place a check in the box **“Store the virtual machine in a different location”** click **Next**.

Name: NewServerBuild

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☒ Store the virtual machine in a different location:

Location: D:\Hyper-V\ Browse...

- 2397 4. The step above will place the configuration and hard drive files for the newly create
- 2398 Virtual Machine in D:\Hyper-V\NewServerBuild (See Screenshot)
- 2399 5. Leave **Generation 1** selected and click Next. This machine doesn't require additional
- 2400 features provided from **Generation 2**.
- 2401 6. Now assign how much memory your new machine will be given for use. For our
- 2402 environment we are using **“2048”** Click next to continue.
- 2403 7. Select the network this virtual machine will be using and click **Next**.
- 2404 8. Now select **“Attach a virtual disk later”** and click **Next**.
- 2405

☒ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

- 2406 9. Now a screen appears displaying a configuration summary, click **Finish** to complete.
- 2407

Description:

Name: NewServerBuild

Generation: Generation 1

Memory: 2048 MB

Network: Not Connected

Hard Disk: None

To create the virtual machine and close the wizard, click Finish.

- 2408 10. Next, open Windows Explorer and navigate to the location of your newly created virtual
- 2409 machine and create a new folder labeled **“Virtual Hard Disk”**
- 2410

Virtual Hard Disks	3/1/2018 2:02 PM	File folder
Virtual Machines	3/1/2018 1:59 PM	File folder

- 2411 11. Now moves the hard drive files converted earlier to this new folder location just created.
- 2412

Name	Date modified	Type	Size
OpmantekVM-disk1.vhdx	3/1/2018 2:12 PM	Hard Disk Image F...	7,180,288 KB
OpmantekVM-disk2.vhdx	2/28/2018 11:19 AM	Hard Disk Image F...	1,708,032 KB

- 2413 12. Open Hyper-V Manager and right click on Virtual Machine just created and
- 2414 select **“Setting...”**
- 2415

Connect...

Settings...

Start

Checkpoint

Move...

Export...

Rename...

Delete...

Enable Replication...

Help

2416

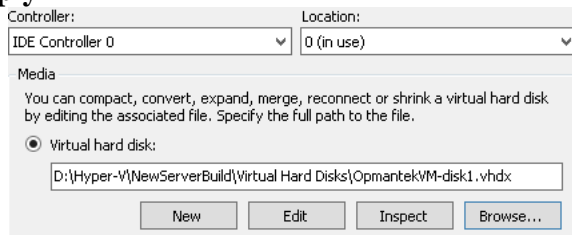
13. Memory should be configured for **“2048”**

14. Virtual Processor **“2”**

15. Click on **“IDE Controller 0”** then click on **“Add”** button to attach a virtual hard.

16. Click browse button and select the first virtual drive that was moved earlier, click

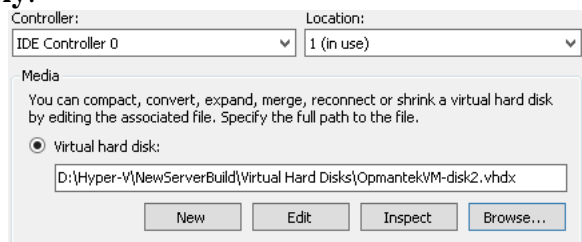
Apply.



17. Now click on **“IDE Controller 0”** again and click **“Add”** button to attach a virtual hard.

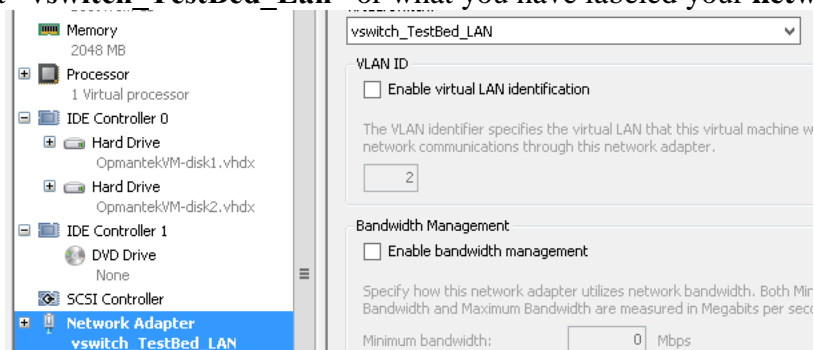
18. Click browse button and select the second virtual drive that was moved earlier, click

Apply.



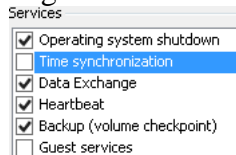
19. Now, select Network adapter and click the drop down and

select **“vswitch_TestBed_Lan”** or what you have labeled your **network**.



20. Click on Name and make sure to add some descriptive information that will allow other to easily see this information without having to login into machine.

21. Select Integration Service and remove check from **“Time Synchronization”** Time will sync using internal NTP server via DNS pointer. Click **“Apply”** and then **“OK”**.



Configure Virtual Machine Networking:

1. Open Hyper-V Manager and then right click on newly created machine and select start.
2. Double click on machine being configured to open a Console window.

- 2438 3. Now type in “root” and then hit enter. Now type in Password which is
 2439 →“NM1\$88” without the quotes. Additional information for default login credentials can be
 2440 found [here](#).
 2441 4. Now type this command without the quotes to copy a static configuration for
 2442 networking. `cp ifcfg-eth0.static /etc./sysconfig/network-scripts/ifcfg-eth0` if prompted to
 2443 overwrite file type “Yes”
 2444 5. Now type this command without the quotes “`sudo nano /etc./sysconfig/network-`
 2445 `scripts/ifcfg-eth0`”
 2446 6. Now use the arrow keys to change the highlighted fields to your desired network
 2447 configuration.

```

DEVICE="eth0"
NM_CONTROLLED="yes"
ONBOOT=yes
TYPE=Ethernet
BOOTPROTO=static
IPADDR=192.168.1.7
NETMASK=255.255.255.0
BROADCAST=192.168.1.255
GATEWAY=192.168.1.1
IPV4_FAILURE_FATAL=yes
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=yes
NAME=eth0

```

- 2448 7. Once all fields have been updated use **Ctrl + O “^O”** to write the file and then **Ctrl +**
 2449 **X “^X”** to
 2450 exit.
 2451



- 2452 8. Now type “**service network restart**” These restarts networking services with the
 2453 newly configured settings.
 2454
 2455
 2456

2457 Complete Additional Setup via Web Browser:

- 2458 1. Now with any web browser navigate to “IP Configured Earlier” example would
 2459 be “10.100.0.177”
 2460 2. If prompted to proceed to untrusted site, select “Yes”. This error is produce since SSL
 2461 has not been configured and Open-Audit redirects HTTP sessions over to HTTPS.
 2462 3. Once this page opens you’ll see lots of different options this tool provides. We’re using
 2463 “**Open-Audit Enterprise**” This version allows for up to 20 nodes to be audited /
 2464 monitored for free.

[Opmantek Documentation and Community](#)

[NMIS8 Dashboard](#)

[opCharts - interactive Charts and Dashboards](#)

[opEvents - Event Management](#)

[opFlow - NetFlow Analysis](#)

[opConfig - Configuration and Compliance Management](#)

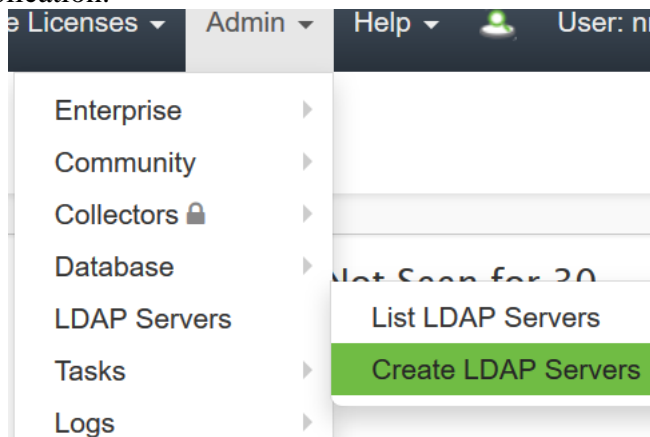
[opReports 3.0 - Network Reporting](#)

[Open-Audit Enterprise](#)

[Open-Audit V2 Dashboard](#)

[Open-Audit Documentation and Community](#)

4. You'll now be prompted for login with username and password. This default information is provided above **"username / password"**.
5. Once logged in we need to make some required changes to allow this produce to function in our environment.
6. Click on **"Admin → LDAP Server → Create LDAP Servers"** This will allow integration with Active Directory using LDAP authentication for logging into this application.



2474 7. Required setting for LDAP server connection. Screen shot provide for
2475 reference.

Name	TestConnection	?
Description	Documentation	?
Organisation	Default Organisation	?
Domain	LAN.LAB	?
Host	10.100.0.17	?
Port	389	?
Use Secure (LDAPS)	No	?
Version	3	?
Use LDAP for Roles	Yes	?
Type	Active Directory	?
Base DN	CN=Users,DC=lan,DC=lab	?

- 2476 a. Name – **TestConnection**
 2477 b. Description -- **Documentation**
 2478 c. Domain – **LAN.LAB**
 2479 d. Host – **10.100.0.17**
 2480 e. Use LDAP Roles -- **Yes** (Additional configuration is required in AD Groups. See
 2481 section below in this document for additional steps.
 2482 f. Base DN – “**cn=user,dc=lan,DC=lab**”

2483 8. Click “**Submit**” once all information has been entered.

2484 **Active Directory Groups for LDAP Integration:**

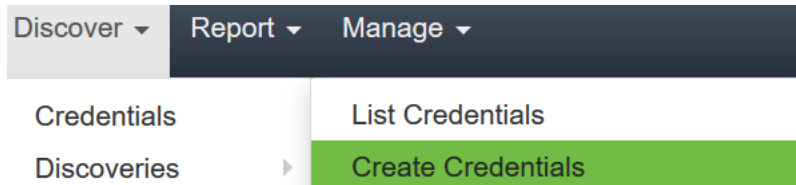
2485 1. Groups listed below are required for integration to work with Open-Audit and
 2486 Active Directory.

- 2487 a. **Admin** “open-audit_roles_admin”
 2488 b. **org_admin** “open-audit_roles_org_admin”
 2489 c. **reporter** “open-audit_roles_reporter”
 2490

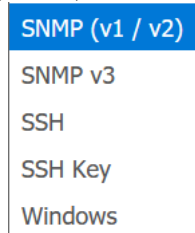
- d. user “open-audit_roles_user”
- e. **Default Organization “open-audit_orgs_default_organisation”**
2. Create each group listed within quotes in your Active Directory. Each group should be created with Group Scope (**Global**) Group Type (**Security**)
3. Once each group has been created and the appropriate users add you can now login with your Active Directory credentials.

Discover Credentials and Discover Scans

1. From the home screen click on **Discover >> Discoveries >> Create Credentials**.



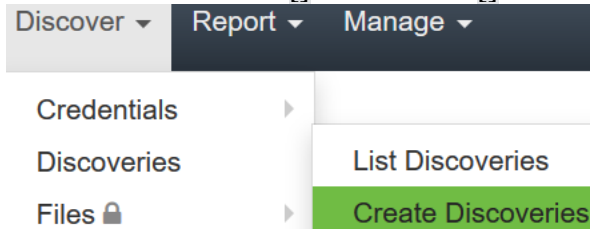
2. Now enter in the requested information.
 - a. Name – Name of the Credentials being used. Example (**SSH**)
 - b. Organization – Default Organization is selected. Pickup another if your configuring more the one organization.
 - c. Description – Description of item being added.
 - d. Type – Select which type of credentials will be used. (**SNMP (v1 / v2)**, **SNMP v3**, **SSH**, **SSH Key**, or **Windows**)



- e. Credentials – enter the appropriate credentials for the select type from above.
- f. Click submit to save this entry.

Discovered Scan:

1. Click Discover button [] Discoveries [] Create Discoveries.



2. Name – The name for this scan which should be unique.
3. Subnet – The network discovery will be performed on.
4. Click submit to save and return to main discovery screen.
5. Main discovery screen allows you to start a scan at any time. Scans can also be configured to run on a schedule interval.

Useful information and links:

1. Default password were not changed, so remember to change all default password before this is put into production. **(THIS IS VERY IMPORTANT)**
2. Software Vendor webpage. → <https://opmantek.com>
3. Community forums. → <https://community.opmantek.com>
4. Software is Open Source. Your able to use Professional Edition for up to 20 machines after that there is a cost which is relatively inexpensive.
5. Comparison Chart

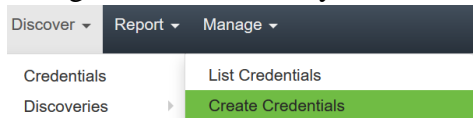
Both the community and enterprise products share a common code base, however, Open-Audit Enterprise includes additional modules that improve discovery, simplify administration and increase reporting ability. Use the comparison chart below to decide which version best suits your organization's requirements.

	Community	Professional	Enterprise
Network Discovery	Yes	Yes	Yes
Device and Software Auditing (including Device Port and Storage Appliances)	Yes	Yes	Yes
Configuration Changes Detection and Reporting	Yes	Yes	Yes
Hardware Warranty Status	Yes	Yes	Yes
Inventory Management	Yes	Yes	Yes
Custom Fields	Yes	Yes	Yes
Interactive Dashboard		Yes	Yes
Geographical Maps		Yes	Yes
Devices Export		Yes	Yes
Scheduling – discovery and reporting		Yes	Yes
Enhanced Reports including Time based, Historical and Multi Reporting		Yes	Yes
High Scale			Yes
High Availability			Yes
File Auditing			Yes
Baselines			Yes
Configurable Role Based Access Control including Active Directory and LDAP			Yes
Integration with agents and CMDB			Yes
Commercial Support		Yes	Yes

6. Ability to perform baseline scan on devices is provided by Enterprise edition. This could be very useful for determining changes over a period of time.

2535 **Install Steps for Process Control**2536 **Open-Audit Configuration steps within Process Control System once system has been installed**
25372538 **Initial Configuration:**

- 2539 • Login via web portal
- 2540 • Navigate to → Discovery → Credentials → Create Credentials



- 2541 • Credentials can be assigned to any organization that has already been created. If you want
- 2542 credentials to only apply to specific organizational group, then select that from the
- 2543 appropriate drop down during credential creation and select the desired group these
- 2544 credentials will apply to.
- 2545 • Our environment consists of mainly Windows machine, so Windows will be used for
- 2546 connection type.
- 2547 • Now create a credential and select **Windows** for the type. Once completed click **Submit**.
- 2548

 A screenshot of the 'Create Credentials' form in the Open-Audit web interface. The form contains the following fields:

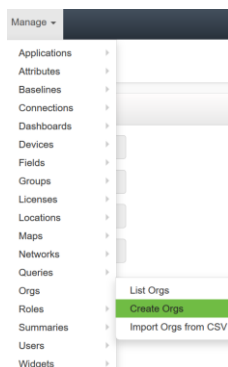
- ID**: A text input field with a question mark icon.
- Name**: A text input field containing 'PCS SCans' with a question mark icon.
- Organisation**: A dropdown menu showing 'Default Organisation' with a question mark icon.
- Description**: A text input field containing 'Perform Windows Scans' with a question mark icon.
- Type**: A dropdown menu showing 'Windows' with a question mark icon.
- Username**: A text input field containing 'Open-Audit@lan.lab'.
- Password**: A password input field with masked characters (dots).
- Edited By**: A text input field containing 'nmis' with a question mark icon.
- Edited Date**: A text input field containing '2018-09-26 14:33:24' with a question mark icon.

 At the bottom of the form is a blue 'Submit' button.

2549

2550 **Organization Groups Creation:**

- 2551 • Click on Manage → Orgs → Create Orgs



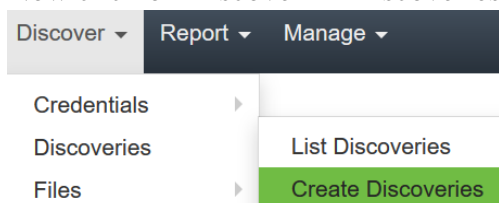
- Now enter **Name:** **Description:** and click submit at the bottom of the page to save.

Name ?
Description ?
Parent ID ?
Type ?

- If you have multiple machines / equipment in different locations you can make Organizational groups based on business units, or related task.

Configure Discovery Scan:

- Now click on Discover → Discoveries → Create Discoveries



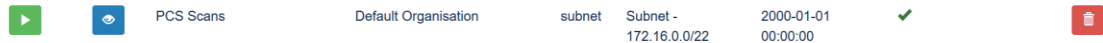
- Enter a meaningful name for discover being created

Name ?

- Next, enter the subnet that'll be used for performing this scan. This scan is using 172.16.0.0/22 Subnet ? **Search online for additional subnetting information / calculators if you'd like to learn more.**
- Network address:** should already be defaulted to Open-Audit installed location, if this is not true, click the drop-down arrow and select your installed location.
- Now, click on the advanced button to see more options. [Advanced](#)
- Once **Advanced** has been expanded you'll have additional options to select if desired. These options are **Org**, **Type**, **Devices Assigned to Org**, and **Devices Assigned to Location**. These options aren't required, but allow you to place found devices into different Organizations groups.
- Once all selection have been made click on **Submit** button to continue.

2575 **Discoveries:**

- 2576 • Once the steps above have been completed clicking on **Submit** button you'll be taken to
- 2577 a new webpage that'll allow you to run discovery process created in the previous step.
- 2578 • To start discovering devices click on **green** arrow button. If you need to verify details for
- 2579 this scan click on the button that looks like an **eye**: finally, if you need to delete this scan
- 2580 click on the **trash** can icon to the right. See screen shot for details.



- 2581
- 2582 • Once discovery has started you'll be taken to a new page allowing you to view status, or
- 2583 cancel if needed.
- 2584 • Newly found devices are added to **My Devices** which is found on the home screen.

2585

2586 **Lesson Learned:**

2587 Ensure default password are changed

2588 Use Secure LDAP (LDAPS) If unable to use LDAPS make sure account being used for syncing

2589 groups has least privilege rights. (Not an Administrator and not a Domain Administrator)

2590 When configuring SNMP make sure to use SNMP V3 if possible

2591 **4.2.6 Highlighted Performance Impacts**

2592 The following performance measurement experiment was performed for the Open-Audit tool

2593 while the manufacturing system was operational:

2594 Experiment PL003.1- Open-Audit asset inventory tool network scan and authenticated scan

2595 A small performance impact to the network behavior was observed in the PCS system during the

2596 Open-Audit scan. The network traffic was slightly increased in part of the PCS system during

2597 the scan. For example, the path delay from PLC to OPC was slightly higher especially in the

2598 latter part of the experience when Open-Audit was performing the authenticated scan. However,

2599 the round trip time from the Controller to the OPC was mostly the same throughout the scan. It

2600 appears that some part of the system has a more noticeable impact than the other parts.

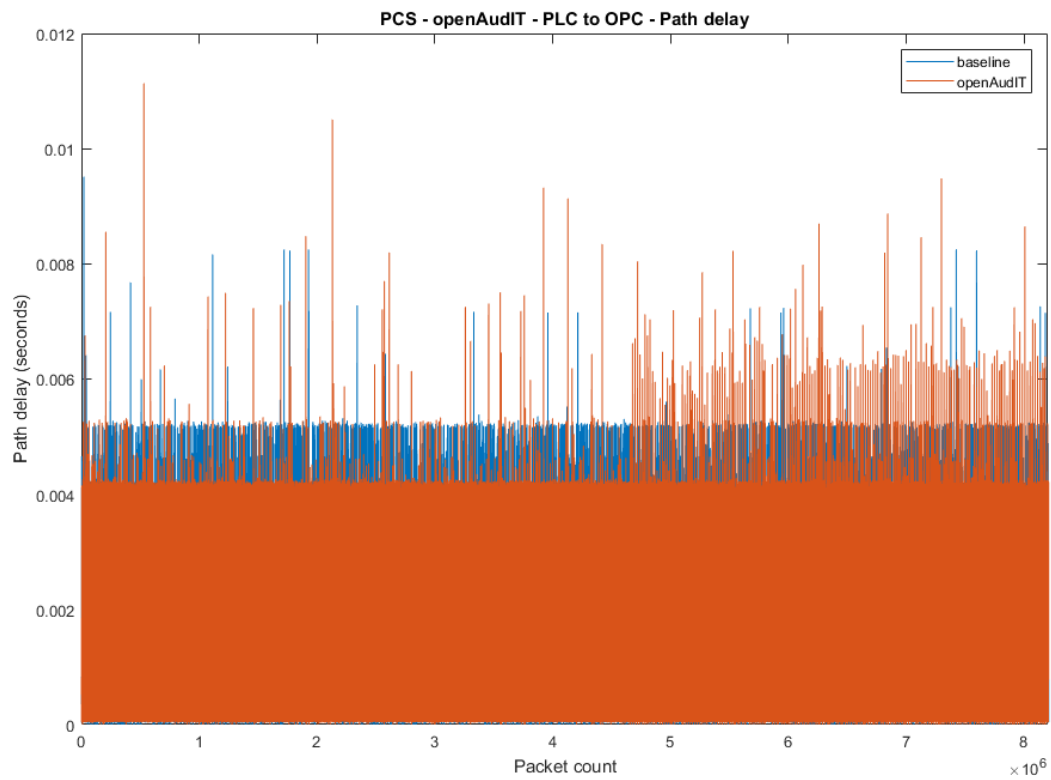


Figure 4-1 Plot showing the path delay from the PLC to OPC server

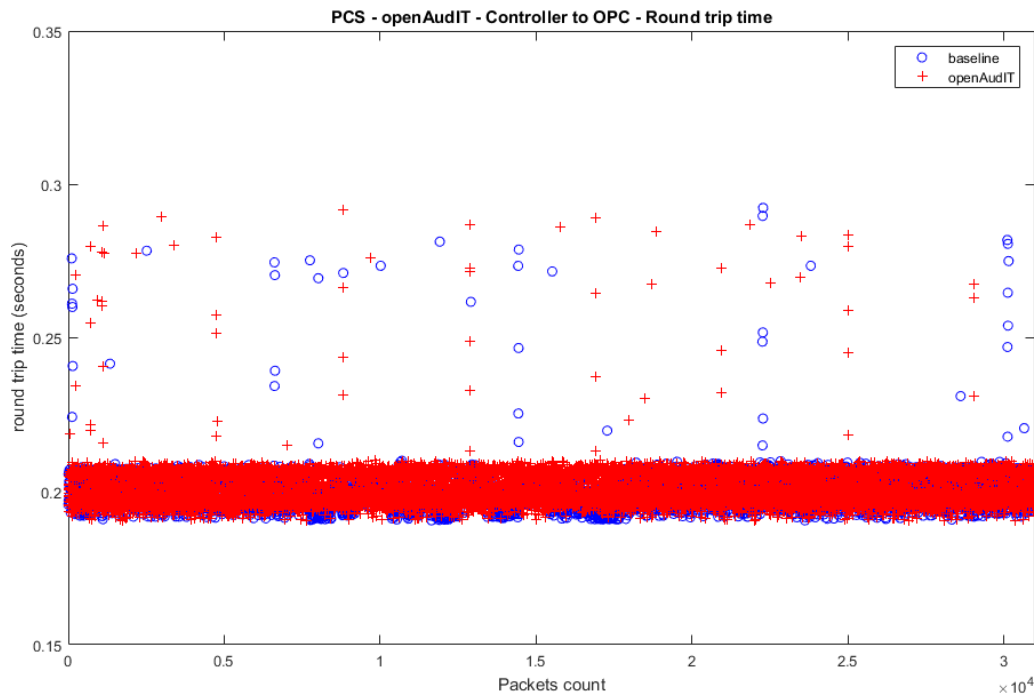


Figure 4-2 Plot of the packet round trip time from Controller to OPC

A small impact to the manufacturing process was observed. The product flow of the manufacturing process was slightly higher than the optimal level. The reactor pressure was slightly higher than the optimal level specially at the latter part of the experiment when Open-Audit was performing the authenticated scan. However, the impact was small within the tolerance of the system.

It is hypothesized that the impacts were caused by increased network delays between the hosts of the system. There is a time delay before the network impact will start impacting the manufacturing process due to the iterative nature of the process simulation and sensor and actuator values exchange.

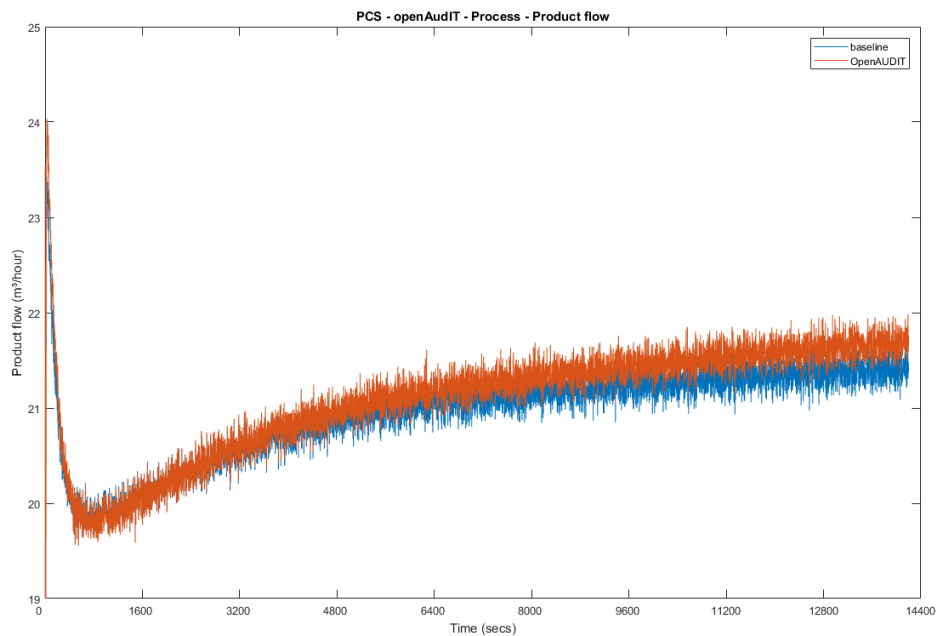


Figure 4-3 Plot of the production flow of the manufacturing process

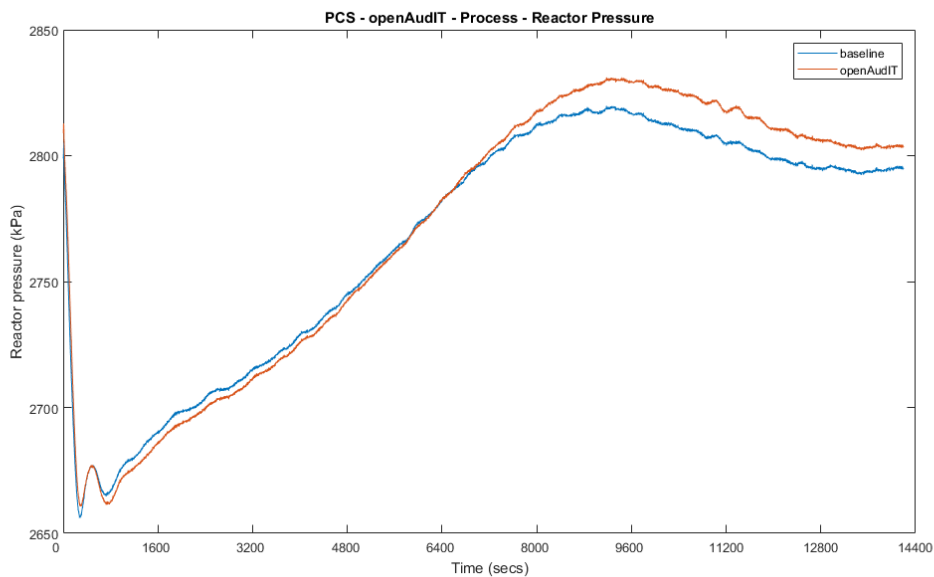


Figure 4-4 Plot of the reactor pressure of the manufacturing process

4.2.7 Link to Entire Performance Measurement Data Set

[Open-Audit KPI data](#)

[Open-Audit measurement data](#)

2625 **4.3 CSET**

2626 **4.3.1 Technical Solution Overview**

2627 Cyber Security Evaluation Tool (CSET) is a tool provide by Department of Homeland Security
2628 for performing Cybersecurity evaluation against an organization. This evaluation is completely
2629 manual process of answering multiple questions to determine organizational security posture in
2630 regard to implemented current cybersecurity practices against current security status. This
2631 evaluation will help identify area within the organization that required more attention and
2632 resources.

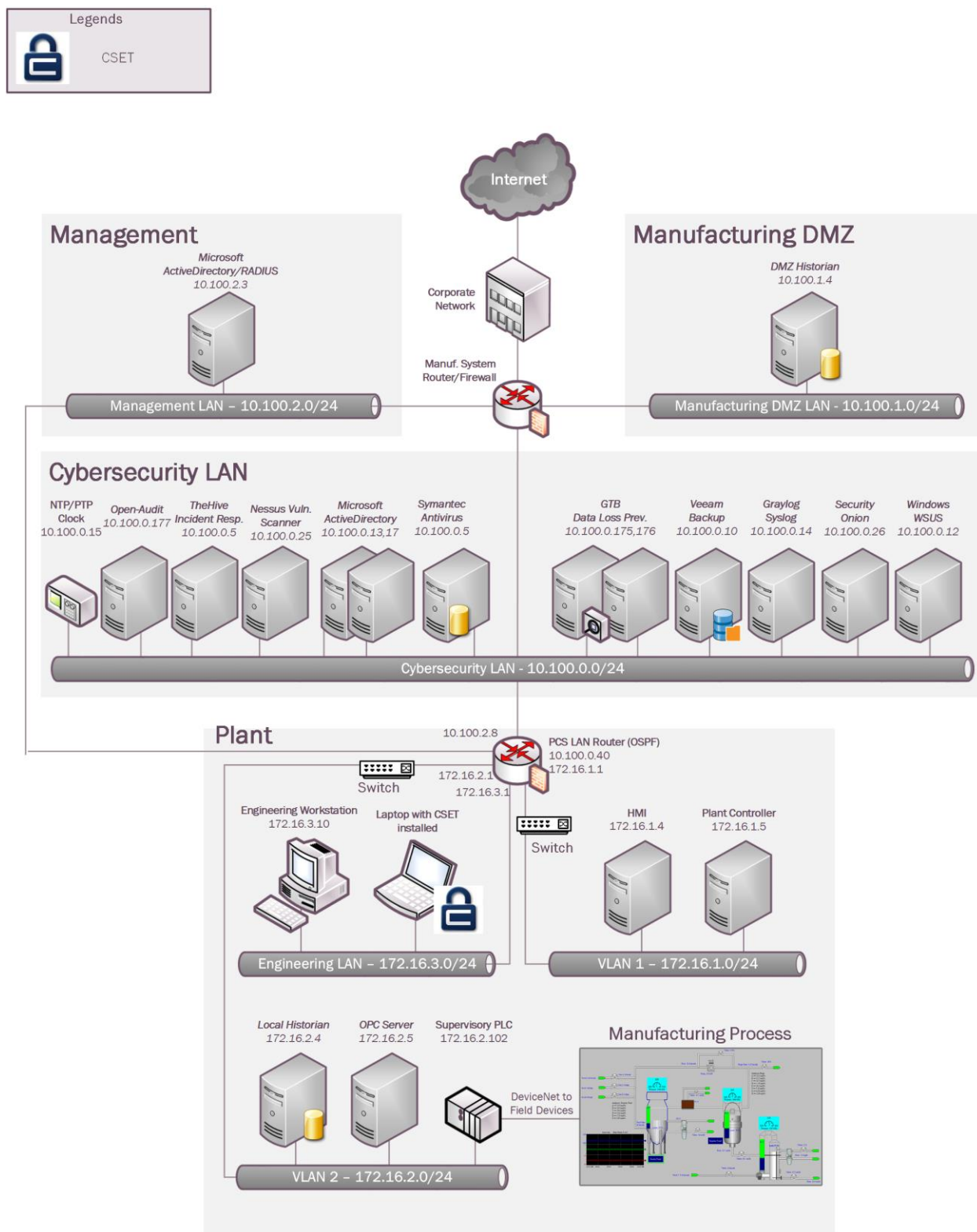
2633 **4.3.2 Technical Capabilities Provided by Solution**

2634 CSET provides components of the following Technical Capabilities described in Section 6 of
2635 Volume 1:

- 2636 • Network Architecture Documentation
- 2637 • Risk Assessment

2638 **4.3.3 Subcategories Addressed by Implementing Solution**

2639 ID.RA-1

2640 **4.3.4 Architecture Map of Where Solution was Implemented**

2641

4.3.5 Installation Instructions and Configurations

CSET Installation and Configuration

Download and Installation Instructions: Provided by DHS

Download CSET using the link at the bottom of this page or by clicking [here](#). After clicking the link, you will be asked to identify yourself and will then be given the opportunity to download the file *CSET_x.x.iso* (where *x.x* represents the download version).

The CSET download is in a file format known as “ISO.” This file is an “image” of the equivalent installation files included on the CSET CD. Because of this format, it is necessary to process the download using one of the following methods:

1. **Decompressing the File** - Open the file using any one of the newer compression utility software programs.
2. **Mounting the File** - this method loads the ISO file using utility software to make the file appear like a virtual drive with the original CD loaded.
3. **Burning the file to CD** - this method uses CD-burn software and the ISO file to burn the files onto your own CD to create a physical disk identical to the CSET original.

These methods require separate software utilities. There are a variety of both free and purchased utility programs available through the Internet that will work with the ISO file format. As DHS does not recommend any specific application or vendor, it will be necessary for you to find a product that provides the necessary functionality. Step by step instructions for each method are provided below:

Decompressing the File

1. CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to your hard drive of choice (i.e., your computer hard drive or USB drive) maintaining the file name and extension (.iso).
3. OPEN the ISO file with a compression utility program and SAVE the files to your hard drive of choice maintaining the original names and file extensions.
4. COMPLETE the *Installing the CSET Program* instructions below.

Mounting the File

1. CLICK the “Download CSET” link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to your hard drive of choice (i.e., your computer hard drive or USB drive) maintaining the file name and extension (.iso).
3. RUN your ISO-specific utility program that is capable of mounting the file. COMPLETE the instructions within the utility software to create a virtual drive using the ISO file. If

2678 you do not have an ISO utility application, you will need to find and install one before
2679 continuing with these instructions.

2680 4. COMPLETE the *Installing the CSET Program* instructions below.

2681 **Burning the file to CD**

2682 1. CLICK the "Download CSET" link at the bottom of this page and complete the requested
2683 information to download the ISO file.

2684 2. SAVE the file to the hard drive on your computer maintaining the filename and extension
2685 (.iso).

2686 3. INSERT a blank, writable CD into the computer's CD drive.

2687 4. RUN your CD-burn utility program. COMPLETE the instructions on your utility
2688 program to burn the ISO image to your DVD. (If you do not have an application that can
2689 do this, then you will need to find and install one before continuing with these
2690 instructions.)

2691 5. COMPLETE the *Installing CSET Program* instructions below.

2692 **Installing the CSET Program**

2693 1. FIND the CSET_Setup.exe file in the folder, virtual drive, or CD containing the CSET
2694 files.

2695 2. DOUBLE-CLICK the CSET_Setup.exe file to execute. This will initiate the installer
2696 program.

2697 3. COMPLETE the instructions in the installation wizard to install the CSET program.

2698 4. READ the material within the ReadMe document for a summary explanation of how to
2699 use the tool. Help is also available through the User Guide, screen guidance text,
2700 and video tutorials.

2701 **Video Tutorials**

2702 A number of video tutorials are available to help you better understand how to use this tool. They
2703 are designed to play within YouTube, therefore, you must have an active internet connection to
2704 view them. You can access these videos by navigating to the CSET YouTube channel
2705 (<https://www.youtube.com/c/CSETCyberSecurityEvaluationTool>).

2706 To view close captioning in YouTube, click on the "cc" icon on the video window.

2707 **System Requirements**

2708 In order to execute CSET, the following minimum system hardware and software is required:

- 2709 • Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- 2710 • CD-ROM drive if creating a physical CD
- 2711 • 5 GB free disk space
- 2712 • 3 GB of RAM

- 2713 • Microsoft Windows 7* or higher
- 2714 • A Microsoft Office compatible (.docx) document reader is required to view reports in
- 2715 .docx format
- 2716 • A Portable Document Format (PDF) reader such as Adobe Reader is required to view
- 2717 supporting documentation. The latest free version of Adobe Reader may be
- 2718 downloaded from <http://get.adobe.com/reader/>
- 2719 • Microsoft .NET Framework 4.6 Runtime (included in CSET installation)
- 2720 • SQL Server 2012 Express LocalDB (included in CSET installation)

2721 **NOTE:** For all platforms, we recommend that you upgrade to the latest Windows Service Pack
 2722 and install critical updates available from the Windows Update website to ensure the best
 2723 compatibility and security.

2724 CSET Hash Values

2725 SHA-256:
 2726 B7061B169E3461A298E58B99FADC9978D9F6CE22A0747669A538BDAF39C214ED

2727 MD5: 53f2f71eb6e3bb54471e75318eaa64ee

2728 SHA-1: f2b020e3a73db9b72ff85bd9b5e158449f6c003a

2729 To download CSET, select the following link:



2730 [Download CSET](#)

2731 If you are unable to download or install CSET from the link, you may request a copy be shipped.
 2732 To request a copy, please send an email to: cset@hq.dhs.gov. Please insert "CSET" in the subject
 2733 line and include the following in your email request:

- 2734 • Your name
- 2735 • Organization name
- 2736 • Complete street address (no P.O. boxes)
- 2737 • Telephone number
- 2738 • The error or installation issue you encountered when attempting the download

2739

2740 Running CSET for First time:

- 2741 1. Once install of CSET has been completed find the application just installed and double
- 2742 click to run. 
- 2743 2. Once program has launched you will see the home screen.
- 2744 3. Click on File and select "New Assetment"  New Assessment Ctrl+N

2745 4. Now, click on Start Here button in the lower right corner of program. **Start Here >>**

2746 5. Next, enter all required information.

Assessment Name	Assessment Date	
Process Control	4/22/2019	
Facility Name		
Westman Chemical Company		
City or Site Name		
Gaithersburg		
State, Province, or Region		
Maryland		
Assessor Name	Assessor Email	Assessor Telephone
John Doe		

2747 6. Click continue to proceed.

2749 7. Now click on drop down menu and select the appropriate choices. Change any highlight options required.

2750

Sector

Chemical Sector (Not Oil and Gas)

Industry

Other

What is the gross value of the assets you are trying to protect?

< \$1,000,000

What is the relative expected effort for this assessment?

Small (1-2 hours)

☒ Privacy is a significant concern for the assets I am trying to protect.

☒ My organization is concerned with the cybersecurity integrity of our procurement supply chain.

☒ My organization uses industrial control systems (ICS).

2751 8. Click continue to proceed.

2753 9. If you want to create a network diagram click the button, otherwise click “Continue”.

2754 10. Change Mode Selection to “Advanced” and “Cybersecurity Framework-based Approach”

- ☐ Basic - Generate a basic assessment using the provided demographic information
- ☒ Advanced - Let me choose which cybersecurity standard(s) the assessment will be based on:

Before selecting which cybersecurity standards your assessment is based on, please choose one of the following options.

☐ Questions-based Approach
The questions-based approach uses simple questions and allows for partial credit.

☐ Requirements-based Approach
The requirements-based approach uses the exact wording of the standard and is best for those industries that are regulated by a specific standard.

☒ Cybersecurity Framework-based Approach
The cybersecurity framework-based approach uses allows you to define a custom profile based on the Cybersecurity Framework.

2755 11. Click continue.

2756 12. Click continue to use default profile or create a new profile.

2757 13. Click continue again.

2758 14. Now answer the questions as they appear.

2759 15. Complete all questions and generate a final report.

2761 Lessons Learned:

- 2762 • The tool is only as good as information entered. Make sure each answer is thought out
- 2763 before answering.

- 2764 • Mark any answer for review as needed so there will be follow up.
2765 • When completed your organization will receive a 0 to 100 score depending on readiness.
2766

2767 **4.3.6 Highlighted Performance Impacts**

2768 No performance measurement experiments were performed for CSET due to its typical
2769 installation location (i.e., external to the manufacturing system).

2770 **4.3.7 Link to Entire Performance Measurement Data Set**

2771 N/A

2772

2773 4.4 GRASSMARLIN

2774 4.4.1 Technical Solution Overview

2775 GRASSMARLIN is an open source, passive network mapper dedicated to industrial networks
2776 and developed by the National Security Agency (NSA). GRASSMARLIN gives a snapshot of
2777 the industrial system including:

- 2778 • Devices on the network
- 2779 • Communications between these devices
- 2780 • Metadata extracted from these communications

2781 Points to consider:¹²

- 2782 • Passive IP network mapping tool
- 2783 • Hardware agnostic portable Java based tool
- 2784 • Can only see and map hosts where you are capturing data from.

2785 4.4.2 Technical Capabilities Provided by Solution

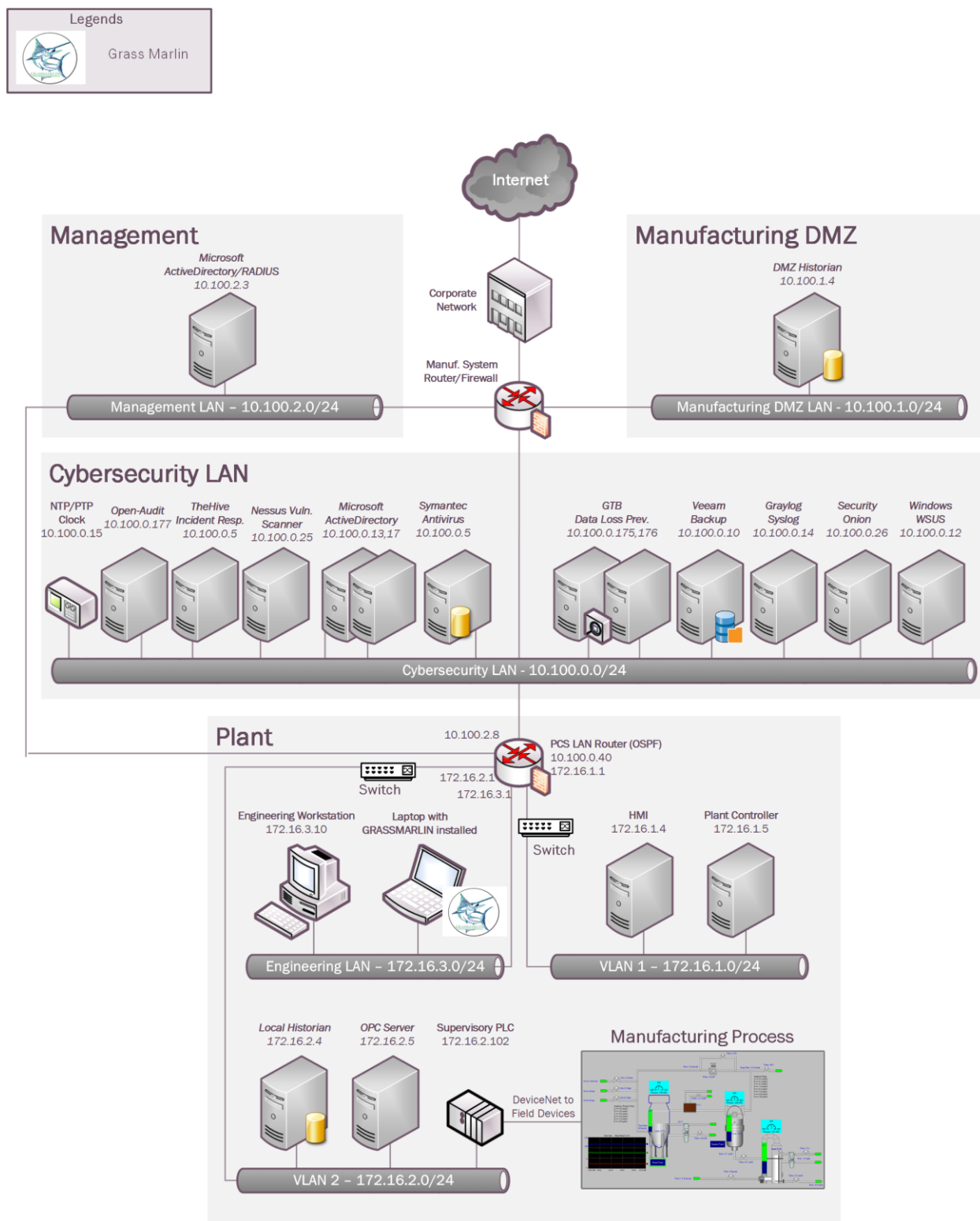
2786 GRASSMARLIN provides components of the following Technical Capabilities described in
2787 Section 6 of Volume 1:

- 2788 • Network Architecture Documentation
- 2789 • Baseline Establishment
- 2790 • Map Data Flows

2791 4.4.3 Subcategories Addressed by Implementing Solution

2792 ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.MA-1, DE.AE-1, DE.CM-7

¹² GRASSMARLIN Briefing Powerpoint 2017: https://github.com/nsacyber/GRASSMARLIN/blob/master/GRASSMARLIN_Briefing_20170210.pptx

2793 **4.4.4 Architecture Map of Where Solution was Implemented**

2794

4.4.5 Installation Instructions and Configurations

Details of the solution implemented:

Name	Version
GRASSMARLIN	3.2.1

Setup

- GRASSMARLIN is supported on the following platforms¹³

Microsoft Windows (64bit, 7 8 and 10)

Fedora Linux

Ubuntu (14.04 ,15.10)

Kali Linux 2.0

CentOS (6,7)

Debian (8)

Download GRASSMARLIN from <https://github.com/nsacyber/GRASSMARLIN/releases> as per the OS version of your system. Upon download, run the installer. The installer will install additional programs such as Java and Wireshark during the setup.

- GRASSMARLIN can operate in a real time passive mode by sniffing the live traffic or by importing a recorded pcap file. Data in GRASSMARLIN is stored in a Session. The Session contains imported files and visual state information.
- A temporary Windows 10 laptop would be setup in the Process Control System as and when required with GRASSMARLIN installed.

Using the Software:

- A captured pcap file from the system was imported in GRASSMARLIN to generate a network baseline. The pcap was captured by the running the tcpdump command on a Linux system which had a network connection from a Network aggregator device. This Aggregator was configured with mirror port connections in coming from the different network segments such as Supervisory LAN and Control LAN.

```
tcpdump -i <mirror-port interface> -w mypcap.pcap
```

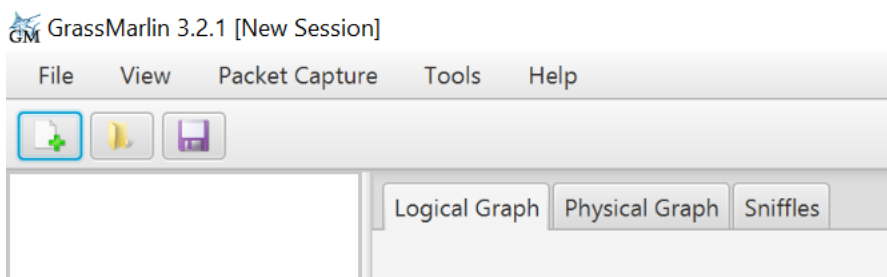
For example: tcpdump -i eth1 -w /home/icssec/pcs.pcap

Where eth1 is our mirror port connection

- To run GRASSMARLIN on a Windows or a Linux system with a Desktop, simply double click on the “GRASSMARLIN” shortcut or icon from the Programs Menu. To run it on a

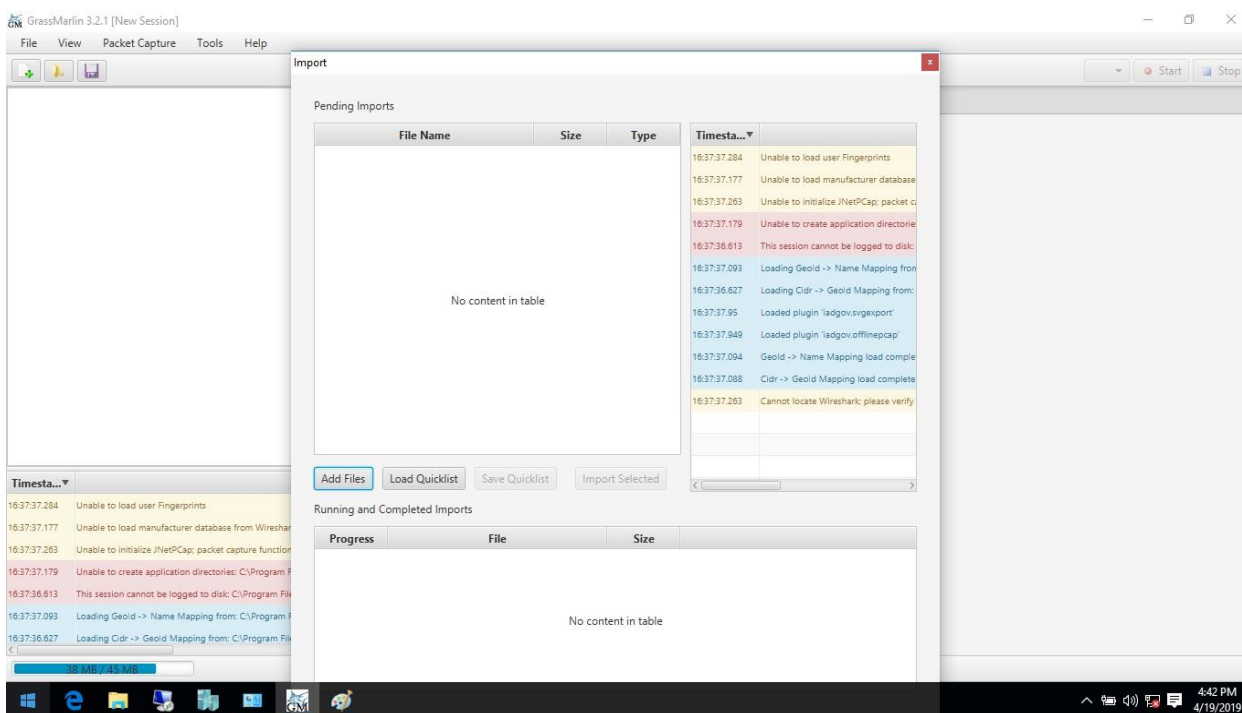
¹³ GRASSMARLIN User Guide: <https://github.com/nsacyber/GRASSMARLIN>

- 2828 Linux system without a Desktop, type the command “**GRASSMARLIN**” or “**sudo**
- 2829 **GRASSMARLIN**” and the interface should load up.
- 2830
- 2831 • To Import a pcap in GRASSMARLIN, click on the **Import** icon in the toolbar (or select
- 2832 **Import files** from the File Menu)



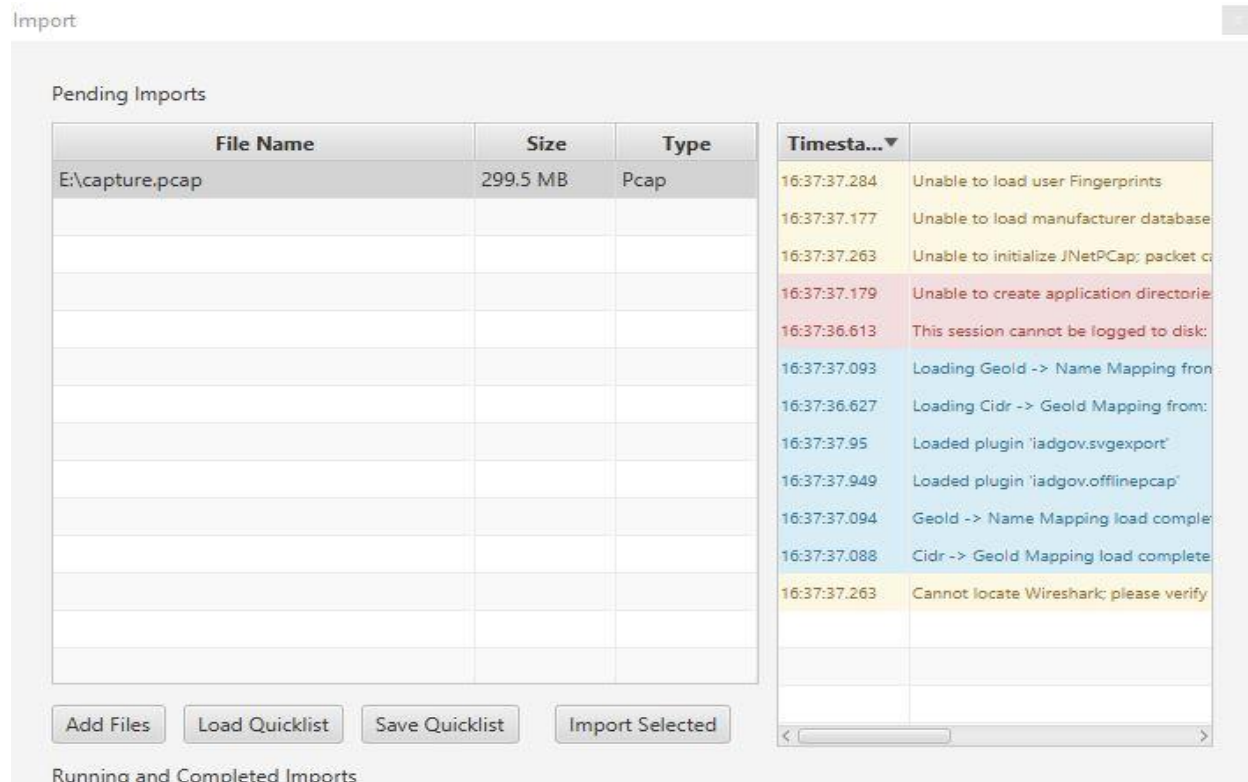
2833

- 2834 • Click on **Add Files**. Browse to the PCAP



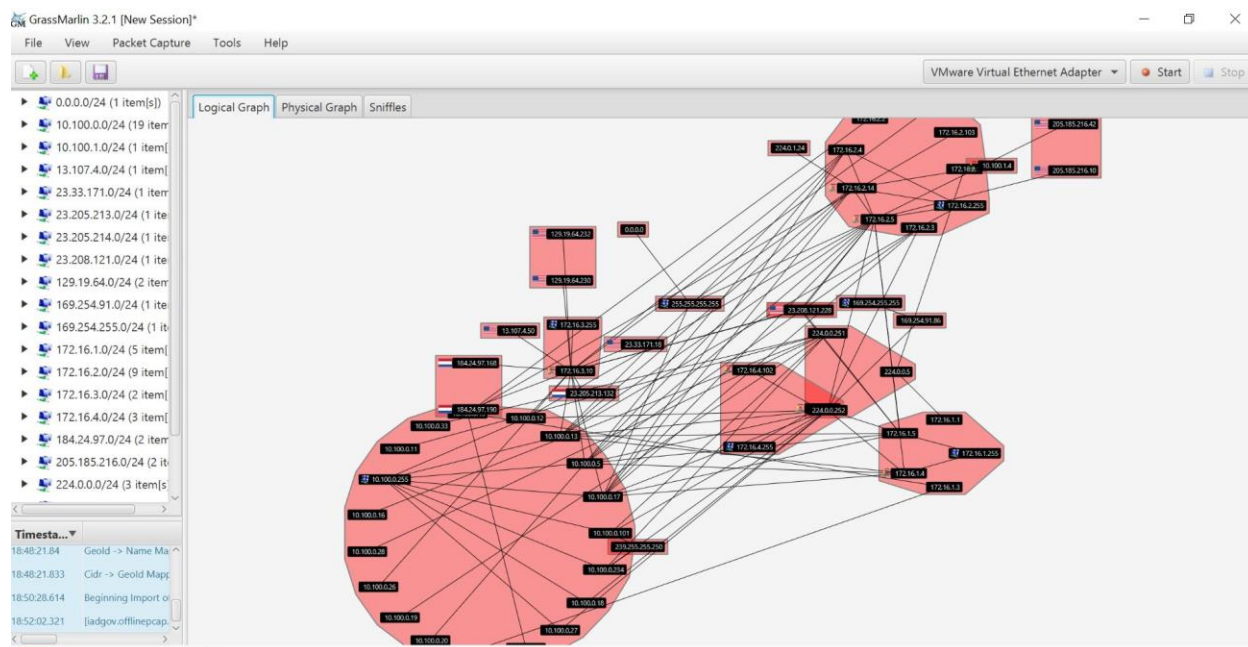
2835

- 2836 • The Pcap will now show up under Pending Imports. Select the file and click on “**Import**
- 2837 **Selected**”. Hit the **Close** button upon completion to back to the Main interface. The Import
- 2838 process can take several minutes to **hours** depending on the size of the pcap file.



2839

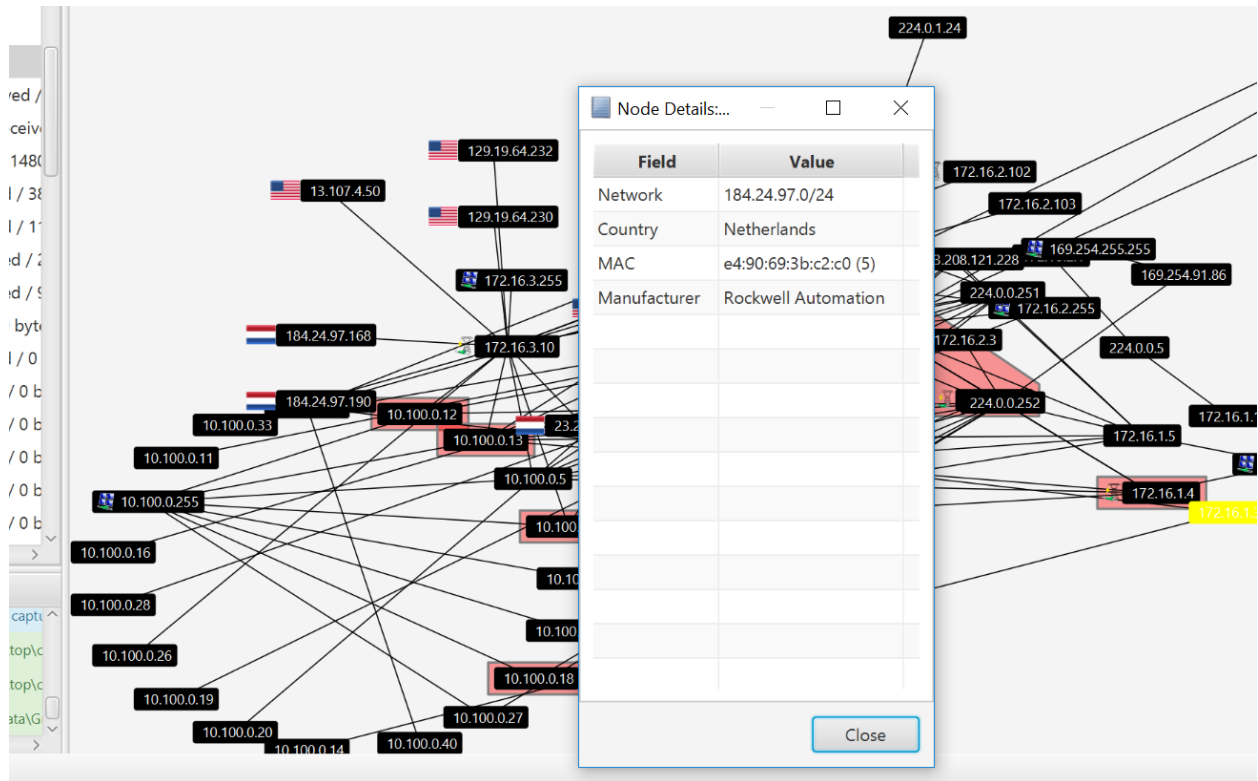
- 2840 • Upon the completion of Import, the main screen will display a Logical Graph of the network topology as shown below.
- 2841



2842

- Take a moment to review the logical graph. The public IP addresses will also be highlighted with their respective Country's flag. This can be useful in finding out information about any external IP's that your network is communicating with.

Right-click on any external IP address in question >> View Details. For instance, the below image shows a host with ip172.16.3.10 communicating with an IP address from Netherlands.



- To Generate a list of all nodes in the Logical Graph, click on **View (Top Menu) >> Logical Nodes Report**. By default, only a single column (IP) is present, although additional columns can be added with any Property present in the set of Nodes.

To add a column, select the Property Name from the drop-down and click the Add button.

Logical Node Reports

☒ All
☐ Source
☐ Destination
☐ Source and Destination

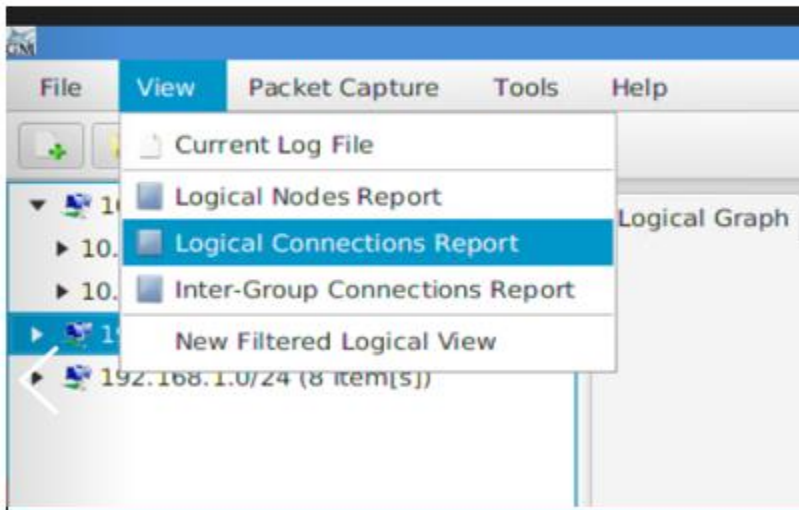
Add Export CSV...

IP	ICSProtocol	EtherNetIP.ICSProtocol	Service
172.16.3.10	Allen Bradley Rockwell PLC Allen Bradley Rockwell PLC ETHERNETIP	ETHERNETIP (5)	Authentication File Replication Service LDAP Authentication File Replication Service
172.16.2.102	ETHERNETIP	ETHERNETIP (5)	
172.16.2.4			LDAP Authentication
172.16.4.5	Allen Bradley Rockwell PLC Allen Bradley Rockwell PLC ETHERNETIP	ETHERNETIP (5)	File Replication Service
172.16.4.102	ETHERNETIP	ETHERNETIP (5)	
172.16.1.4			LDAP Authentication File Replication Service
172.16.2.14			LDAP Authentication

Browser Protocol.Domain/Workgroup
 Browser Protocol.MicrosoftProtocol
 Domain Controller.Role
 Domain Controller.Service
 Operating System.OS
 Role
 Windows Version
 OS
 Domain/Workgroup
 MicrosoftProtocol

2857

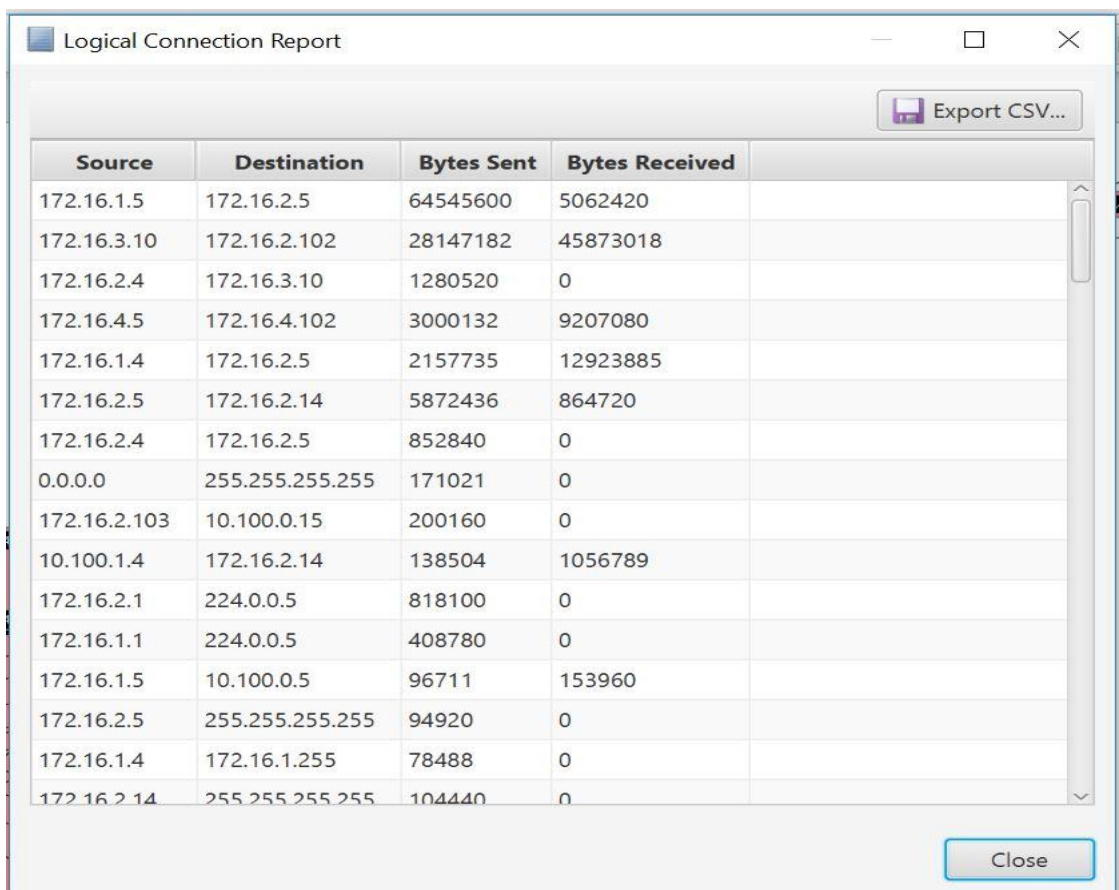
- 2858 • To Generate a Report of all connections in the pcap file, click on **View (Top Menu)**>>
- 2859 **Logical Connections Report**
- 2860



2861

2862

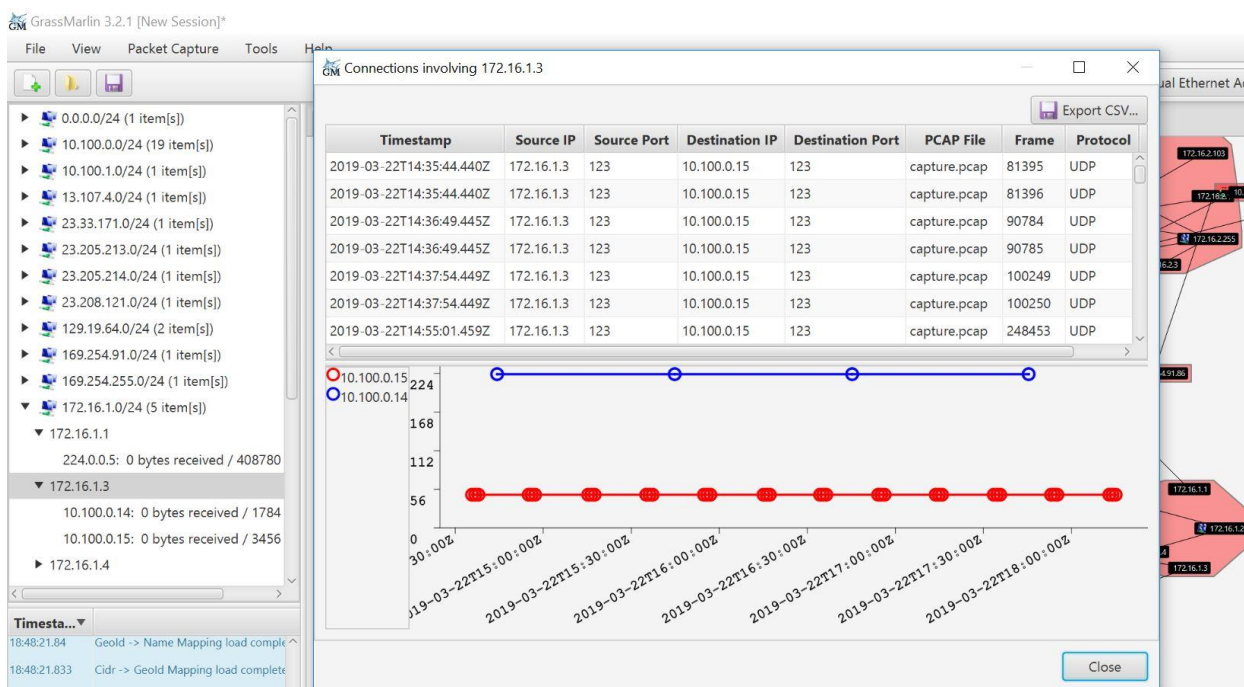
- 2863 • This will generate an output similar to below shown image. Click on **Export CSV** for further
- 2864 analysis of all the communications happening on your network.
- 2865



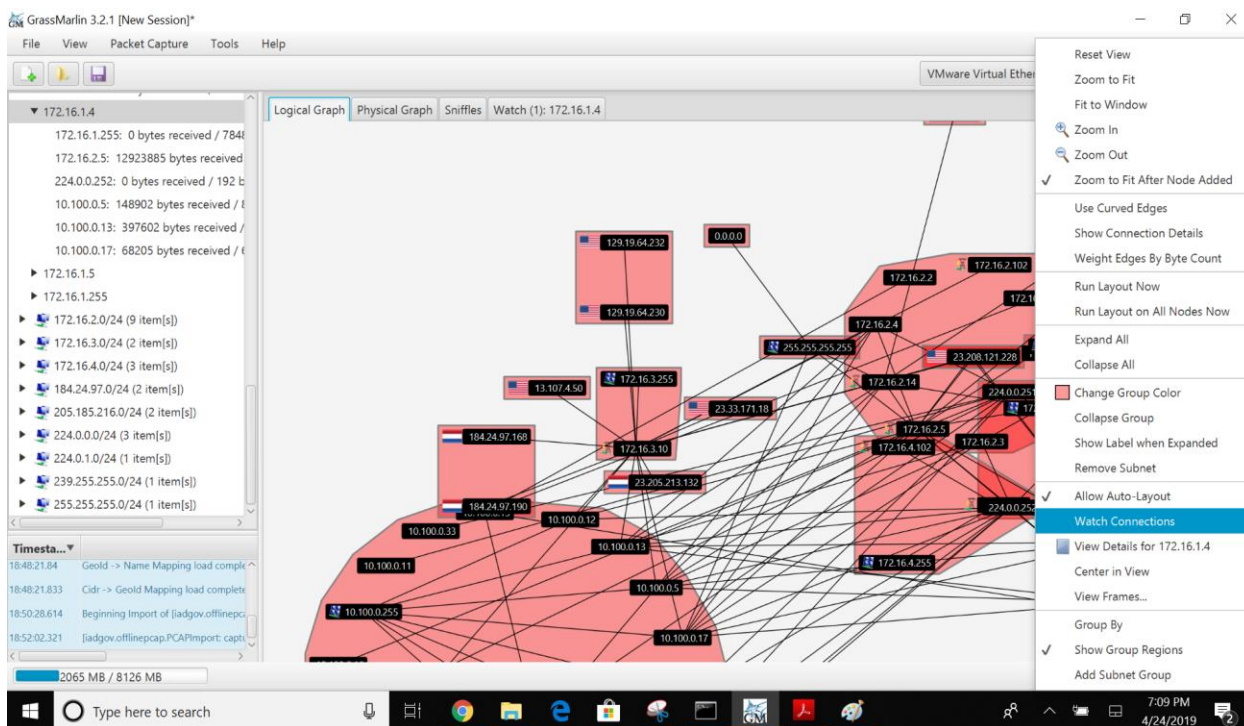
Source	Destination	Bytes Sent	Bytes Received
172.16.1.5	172.16.2.5	64545600	5062420
172.16.3.10	172.16.2.102	28147182	45873018
172.16.2.4	172.16.3.10	1280520	0
172.16.4.5	172.16.4.102	3000132	9207080
172.16.1.4	172.16.2.5	2157735	12923885
172.16.2.5	172.16.2.14	5872436	864720
172.16.2.4	172.16.2.5	852840	0
0.0.0.0	255.255.255.255	171021	0
172.16.2.103	10.100.0.15	200160	0
10.100.1.4	172.16.2.14	138504	1056789
172.16.2.1	224.0.0.5	818100	0
172.16.1.1	224.0.0.5	408780	0
172.16.1.5	10.100.0.5	96711	153960
172.16.2.5	255.255.255.255	94920	0
172.16.1.4	172.16.1.255	78488	0
172.16.2.14	255.255.255.255	104440	0

- To view all the logical communications for a specific host for capturing a baseline, under the left-side explorer right-click on a **Node >> View Frames**. This opens a new screen as shown below displaying all the different IP addresses that particular host is communicating with including Port and Protocol information. You may click further on “**Export CSV**” button to export this data to a csv file.

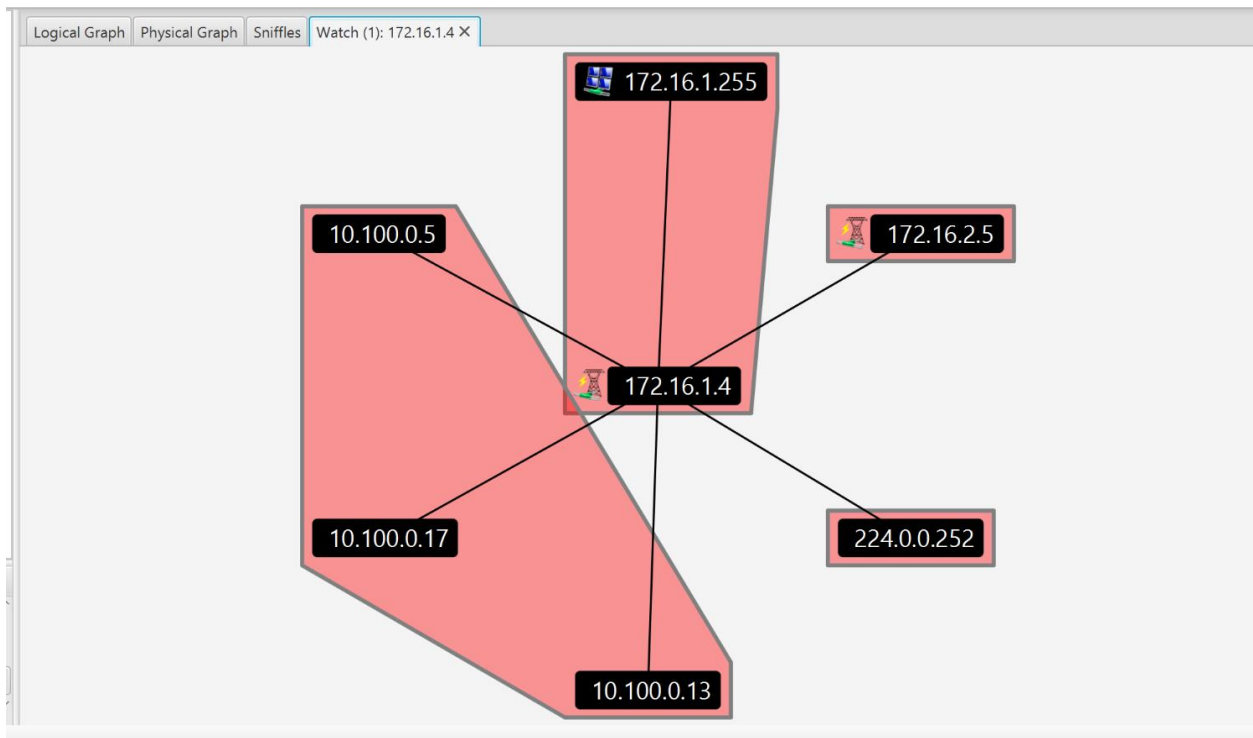
Note: This process needs to be repeated for every node.



- Another interesting feature is Watch-Graphs. A Watch Graph is a subset of Logical graph, created for a particular node and shows all the different nodes connected to it. This can be generated using **Watch-connections** menu. Right-click a node >> select **Watch Connections**. This will generate a graph in a new window “**Watch <IP address>**”



2885



2886

2887

2888 4.4.6 Highlighted Performance Impacts

2889 No performance measurement experiments were performed for the use of GRASSMARLIN due
2890 to its installation location and how it was used (i.e., the software performed offline analysis of
2891 PCAP files captured by other software).

2892 4.4.7 Link to Entire Performance Measurement Data Set

2893 N/A

2894

2895 **4.5 Wireshark**

2896 **4.5.1 Technical Solution Overview**

2897 Wireshark is a free and open-source packet analyzer. It is user friendly, simple to implement, just
2898 need to ensure network connection plugged in is configured to display traffic correctly i.e. Port
2899 mirroring.

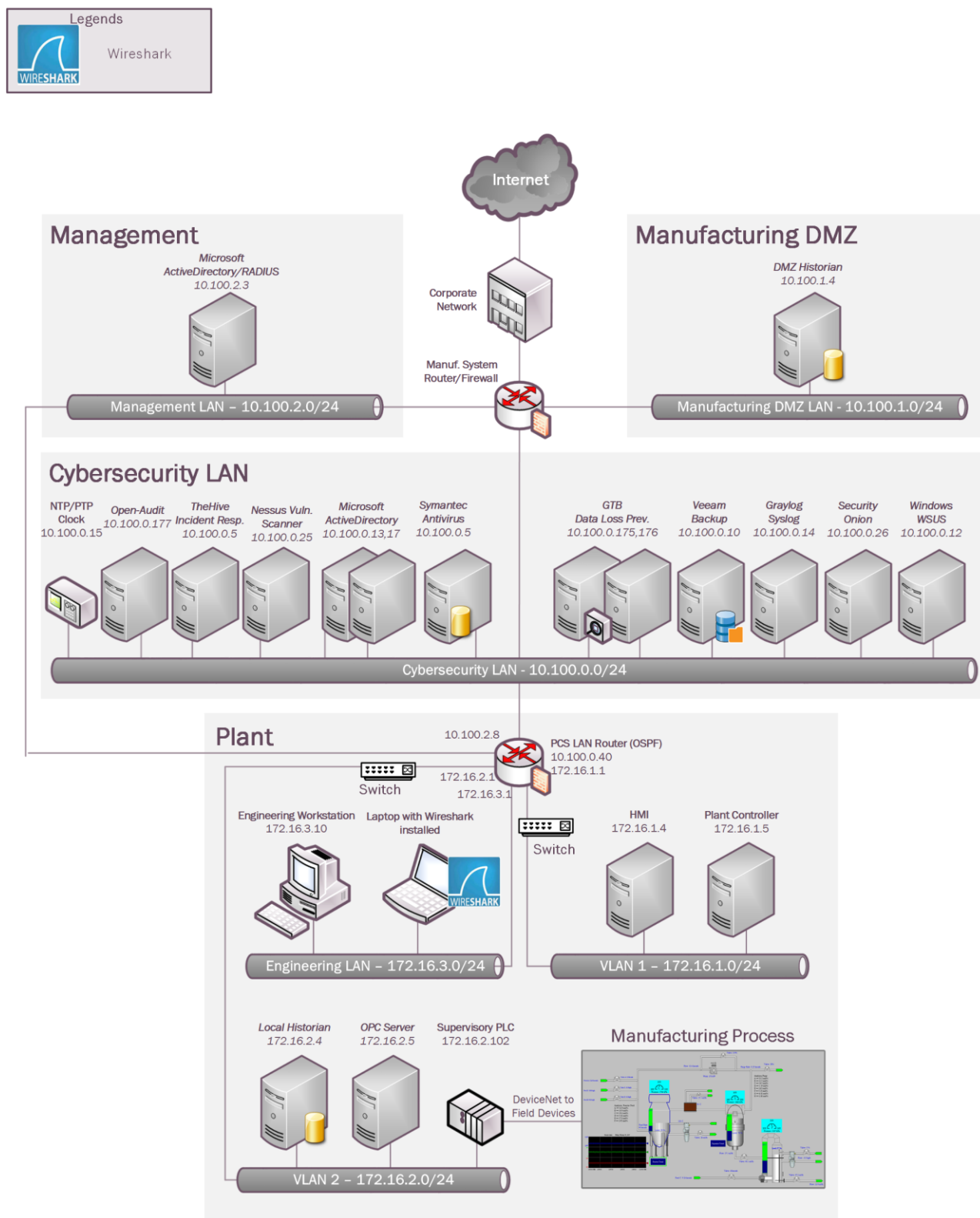
2900 **4.5.2 Technical Capabilities Provided by Solution**

2902 Wireshark provides components of the following Technical Capabilities described in Section 6
2903 of Volume 1:

- 2904 • Network Architecture Documentation
- 2905 • Baseline Establishment
- 2906 • Map Data Flows
- 2907 • Forensics

2908 **4.5.3 Subcategories Addressed by Implementing Solution**

2909 ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.MA-1, DE.AE-1, DE.AE-2,
2910 DE.CM-7, RS.AN-3
2911

2912 **4.5.4 Architecture Map of Where Solution was Implemented**

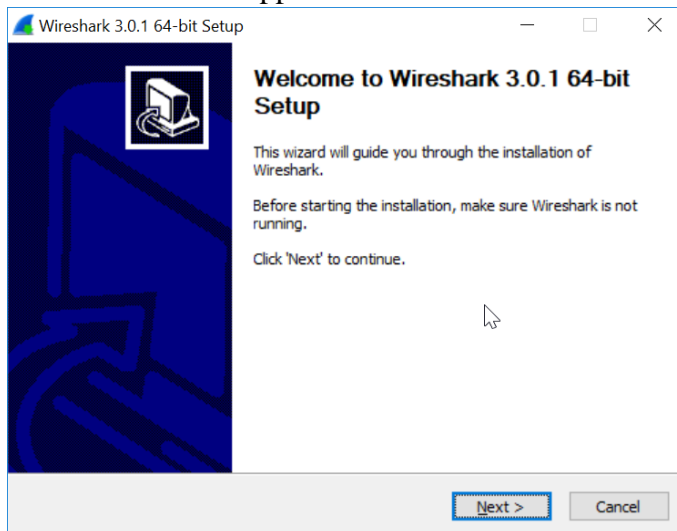
2913

4.5.5 Installation Instructions and Configurations

Steps for installing Wireshark

Download and Installation instructions:

1. Only download Wireshark from <https://www.wireshark.org> (Select 32bit or 64 bit)
2. Once download has completed locate the executable just downloaded and double click to start install process. C:\Users\johndoe\Downloads\Wireshark-win64-3.0.1.exe
3. If prompted for password enter administrator account on local machine.
4. When first Screen appears click “NEXT”

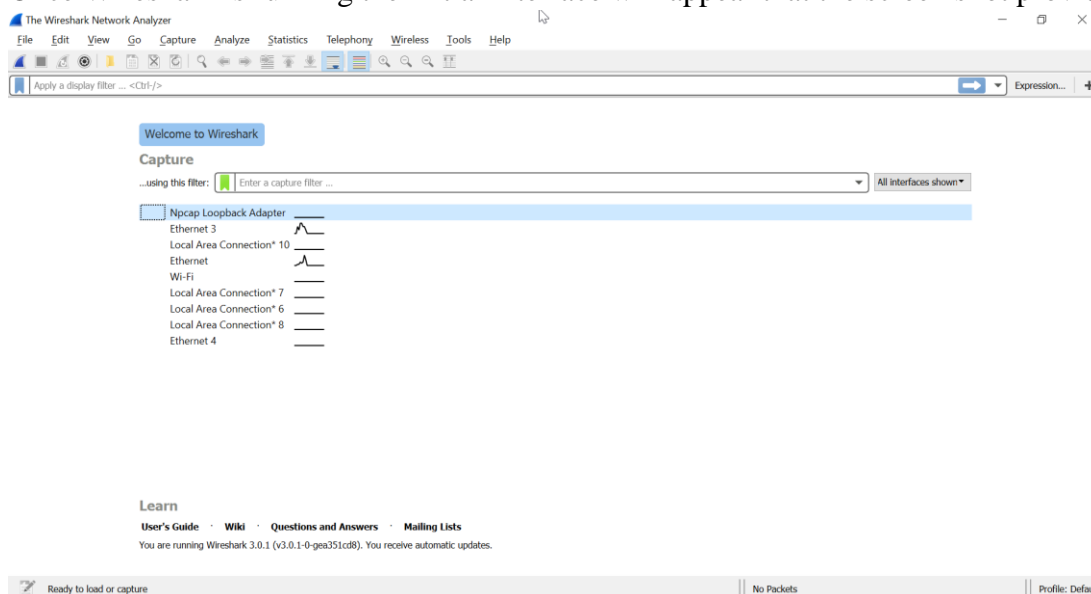


5. Click “Agree” to continue.
6. Leave default selected and click “Next” five times to continue install. (Make changes if all features aren’t required. This will be uncommon)
7. When prompted for Npcap install click “I Agree” to continue.
8. Leave default and click “Install”.
9. Now click “Next and Finish” to start process.
10. Click next and then select “Reboot Now” or “I want to manually reboot later”
11. Click “Finish” to complete.

Running Wireshark and configure

1. Click start button and find program labeled “Wireshark”.
2. Once Wireshark is found right click on icon and select **More→Run as Administrator (Windows 10)** Older operating system can just hold down “Shift + Right Click” menu will appear for run as, select administrator to continue.
3. Wireshark requires administrative privileges to be fully functional, otherwise there will be undesired results.

- 2939 4. Once Wireshark is running the initial interface will appear that the screen shot provided.



- 2940 5. Select the interface to be monitored.

2942 Wireshark provide lots of information and can be hard to decipher <https://www.wireshark.org>
2943 provides documentation along with searches for additional command syntax.

2944 Capturing Network Baseline using Wireshark

- 2945 1. Launch Wireshark. Click **Open** to load a previously captured pcap file or run a “**Start**
2946 **Capture**” as explained in the previous section to record traffic.
2947 2. Upon loading the pcap or capturing live traffic; click on **Statistics >> Conversations**
2948 3. This will generate a window similar to the one below which will list all the different
2949 types of communications happening between all endpoints in your traffic. Click **COPY**
2950 >> **as Csv** to save this data as a Csv file for further analysis.

Wireshark · Conversations · capture.pcap

Ethernet · 95		IPv4 · 75		IPv6 · 22		TCP · 853		UDP · 670			
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.100.0.16	224.0.0.251	2	174	2	174	0	0	0109.13388	3600.1009	0	0
10.100.0.17	172.16.1.4	342	33 k	171	17 k	171	16 k	3235.241245	5111.8544	27	25
10.100.0.17	172.16.3.10	349	81 k	163	34 k	186	47 k	3341.621642	4829.8745	57	77
10.100.0.17	172.16.2.4	1,097	305 k	484	123 k	613	181 k	3360.223085	4796.3020	206	303
10.100.0.17	10.100.0.255	74	9571	74	9571	0	0	3391.429714	4801.4406	15	0
10.100.0.17	224.0.0.252	4	264	4	264	0	0	3475.946375	3600.5112	0	0
10.100.0.17	172.16.2.14	1,106	332 k	511	123 k	595	209 k	3529.909695	4587.6312	214	366
10.100.0.17	172.16.2.5	2,534	298 k	1,260	170 k	1,274	128 k	3656.383446	4381.4873	311	234
10.100.0.17	172.16.2.3	688	203 k	295	78 k	393	125 k	3773.279386	4514.4789	139	221
10.100.0.17	172.16.1.5	228	45 k	102	18 k	126	27 k	0868.02465	1285.4367	114	170
10.100.0.18	10.100.0.255	13	2456	13	2456	0	0	3272.279835	4581.1734	4	0
10.100.0.18	224.0.0.252	4	264	4	264	0	0	3272.280802	3600.5087	0	0
10.100.0.19	224.0.0.251	1	87	1	87	0	0	1365.30458	0.0000	—	—
10.100.0.27	10.100.0.255	114	10 k	114	10 k	0	0	3271.772421	5102.5099	16	0
10.100.0.27	224.0.0.252	2	132	2	132	0	0	1061.46345	0.4104	2572	0
10.100.0.28	224.0.0.251	1	87	1	87	0	0	1828.86474	0.0000	—	—
10.100.0.33	224.0.0.251	1	81	1	81	0	0	1229.03123	0.0000	—	—
10.100.0.101	224.0.0.252	47	3248	47	3248	0	0	2215.07204	1624.9433	15	0
10.100.0.101	239.255.255.250	77	16 k	77	16 k	0	0	2215.69742	2163.4997	61	0
10.100.0.101	224.0.0.251	6	492	6	492	0	0	2219.20341	3.0087	1308	0
10.100.0.101	10.100.0.255	116	13 k	116	13 k	0	0	2223.70201	1964.5661	55	0
10.100.0.234	239.255.255.250	311	62 k	311	62 k	0	0	3213.476484	5163.1292	96	0
10.100.0.234	224.0.0.252	6	394	6	394	0	0	0471.43449	3172.9687	0	0
10.100.0.234	10.100.0.255	6	552	6	552	0	0	0591.45248	3054.4517	1	0
10.100.1.4	172.16.2.14	9,390	638 k	6,252	406 k	3,138	232 k	3213.771225	5185.1215	626	357
23.205.214.21	172.16.3.10	39	2522	0	0	39	2522	2536.51692	1523.2062	0	13

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time
 Conversation Types ▾

Copy ▾ Follow Stream... Graph... Close Help

172.16.2.102 172.16.3.10 555 [TCP Retransmission] 448
 172.16.2.5 172.16.1.4 60 65227 → 50005 [ACK] Seq=
 172.16.2.5 172.16.1.4 60 [TCP Dup ACK 1176#1] 652

2951

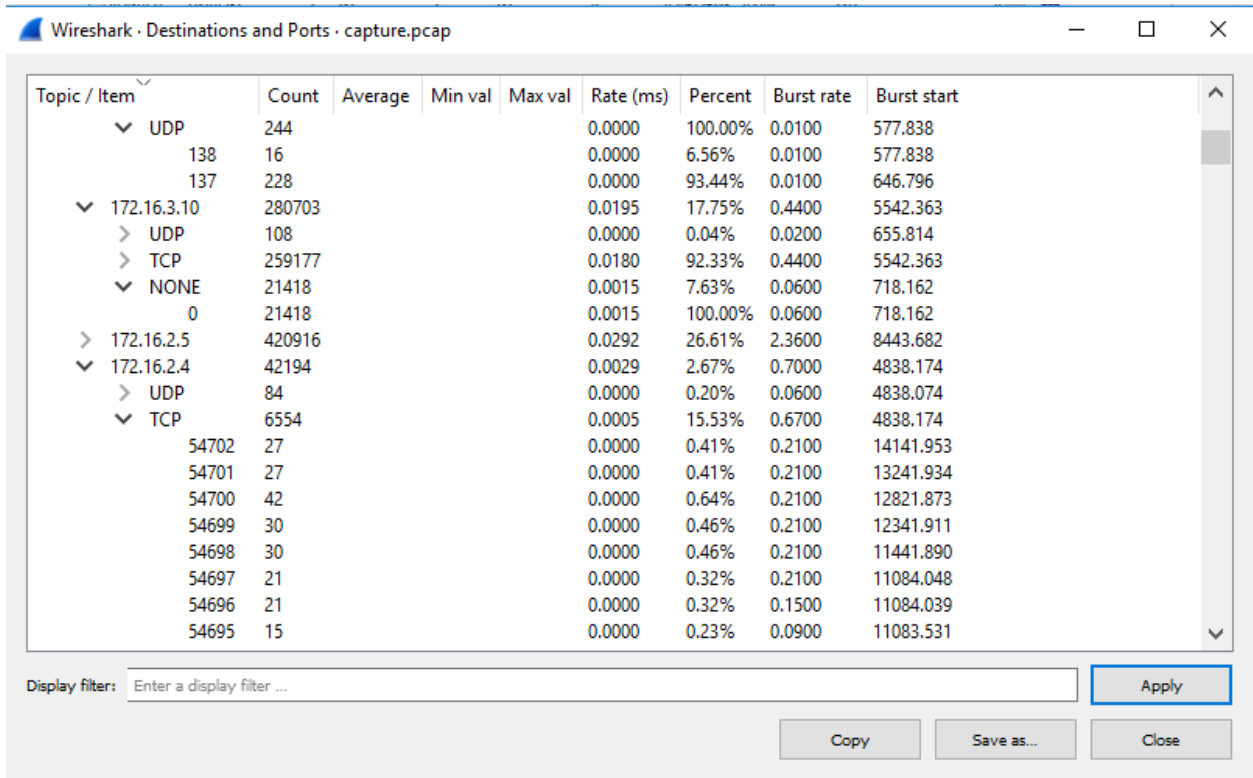
2952

2953

2954

2955

- To get a list of ports used, Click on **Statistics >> IPv4 Statistics >> Destination and Ports**. This will generate a list of ports used by all the IP addresses in the traffic. Click **Copy**, to copy the results to a word document or click **Save as** to save as a plain text file. Hit **Close** when done.



Wireshark · Destinations and Ports · capture.pcap

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ UDP	244				0.0000	100.00%	0.0100	577.838
138	16				0.0000	6.56%	0.0100	577.838
137	228				0.0000	93.44%	0.0100	646.796
▼ 172.16.3.10	280703				0.0195	17.75%	0.4400	5542.363
> UDP	108				0.0000	0.04%	0.0200	655.814
> TCP	259177				0.0180	92.33%	0.4400	5542.363
▼ NONE	21418				0.0015	7.63%	0.0600	718.162
0	21418				0.0015	100.00%	0.0600	718.162
> 172.16.2.5	420916				0.0292	26.61%	2.3600	8443.682
▼ 172.16.2.4	42194				0.0029	2.67%	0.7000	4838.174
> UDP	84				0.0000	0.20%	0.0600	4838.074
▼ TCP	6554				0.0005	15.53%	0.6700	4838.174
54702	27				0.0000	0.41%	0.2100	14141.953
54701	27				0.0000	0.41%	0.2100	13241.934
54700	42				0.0000	0.64%	0.2100	12821.873
54699	30				0.0000	0.46%	0.2100	12341.911
54698	30				0.0000	0.46%	0.2100	11441.890
54697	21				0.0000	0.32%	0.2100	11084.048
54696	21				0.0000	0.32%	0.1500	11084.039
54695	15				0.0000	0.23%	0.0900	11083.531

Display filter: Apply

Copy Save as... Close

2956

2957 **4.5.6 Highlighted Performance Impacts**

2958 The following performance measurement experiment was performed for the Wireshark tool
 2959 while the manufacturing system was operational:

2960 Experiment PL015.2-wireshark

2961 Significant performance impact on computing resources was observed when using Wireshark for
 2962 network traffic capture. Both the processor and memory utilization of the host were significantly
 2963 higher than normal. There was no performance impact to the manufacturing process observed.

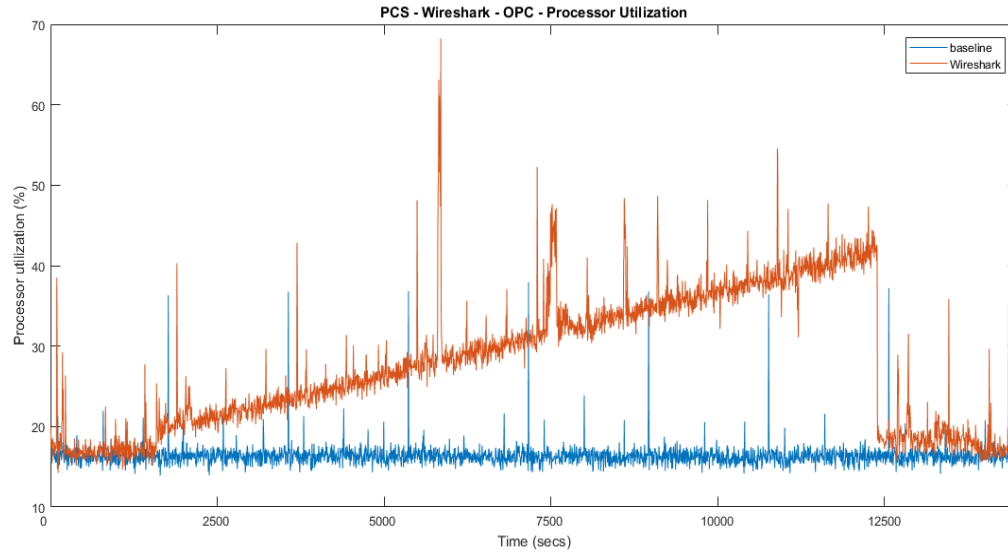


Figure 4-5 Processor utilization of the OPC computer during Wireshark network capture

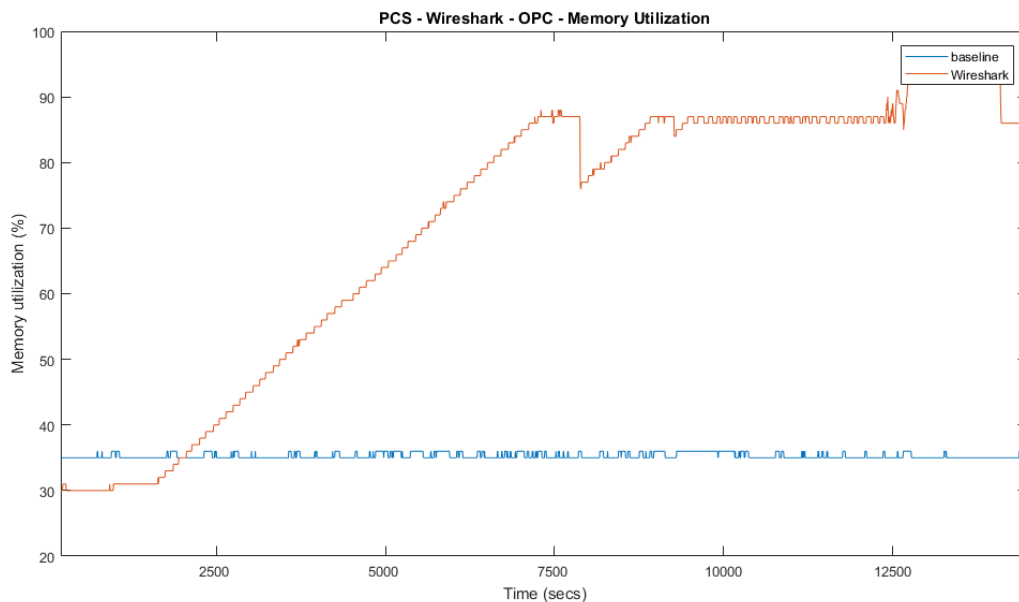


Figure 4-6 Memory utilization of the OPC computer during Wireshark network capture

Wireshark started at around 1900 seconds experiment time and continued to capture network traffic for about 3 hours. During this period of time, the processor utilization of the OPC computer kept going up. Wireshark has a sizeable impact to the processor utilization. The Wireshark data file was about 2.3GB in this case.

The memory utilization has a similar impact to the processor utilization, except the memory utilization stayed high after Wireshark has stopped capturing the network traffic. It is hypothesized that Wireshark stored the captured data in memory until the data was saved into the

2975 hard drive. Therefore, the memory utilization stayed high even after the Wireshark has stopped
2976 the network capture. Even though the processor and memory utilization were significantly
2977 higher, they were still below the full capability of the computer and therefore did not have major
2978 impact to the manufacturing process. However, for the manufacturing system that has a high
2979 utilization in normal run time, the use of Wireshark may cause a performance impact.

2980 The PCS system uses an external computer to use Wireshark to perform network traffic capture
2981 for this reason. Care should be taken if using Wireshark on a production system.

2982 **4.5.7 Link to Entire Performance Measurement Data Set**

2983 [Wireshark KPI data](#)

2984 [Wireshark measurement data](#)

2985

2986

2987 **4.6 Veeam Backup and Replication**

2988 **4.6.1 Technical Solution Overview**

2989 Veeam Backup and Replication is a proprietary backup and incident recovery software
2990 developed by Veeam for virtual environments. It is built on VMware vSphere and Microsoft
2991 Hyper-V hypervisors. The software provides backup, restore and replication functionality for
2992 virtual machines. Veeam® Backup and Replication suite delivers availability for all workloads -
2993 virtual, physical, cloud (including VMware vSphere and Microsoft Hyper-V) -from a single
2994 management console. It provides fast, flexible and reliable recovery of your applications and
2995 data, and brings backup and replication together into a single software solution [1].

2996 The Veeam Backup Free Edition lets you back up your VMs on the fly and provides you with
2997 flexible storage options, including file-based (NFS) primary storage, for easy archiving and
2998 quick recovery. Veeam also has products such as “Veeam agent for Windows” and “Veeam
2999 agent for Linux” for backing up physical Windows and Linux servers respectively.

3000 Points to consider:

- 3001 • Free backup edition available for virtual and physical servers.
- 3002 • Support for file level backups as well as system image type of backups.
- 3003 • Backups can be run without having to shut down the system. This can be very critical in
3004 ICS/SCADA environments.
- 3005 • Tech support available for Free edition users.
- 3006 • Easy to setup and use. Lot of documentation available online to get started.

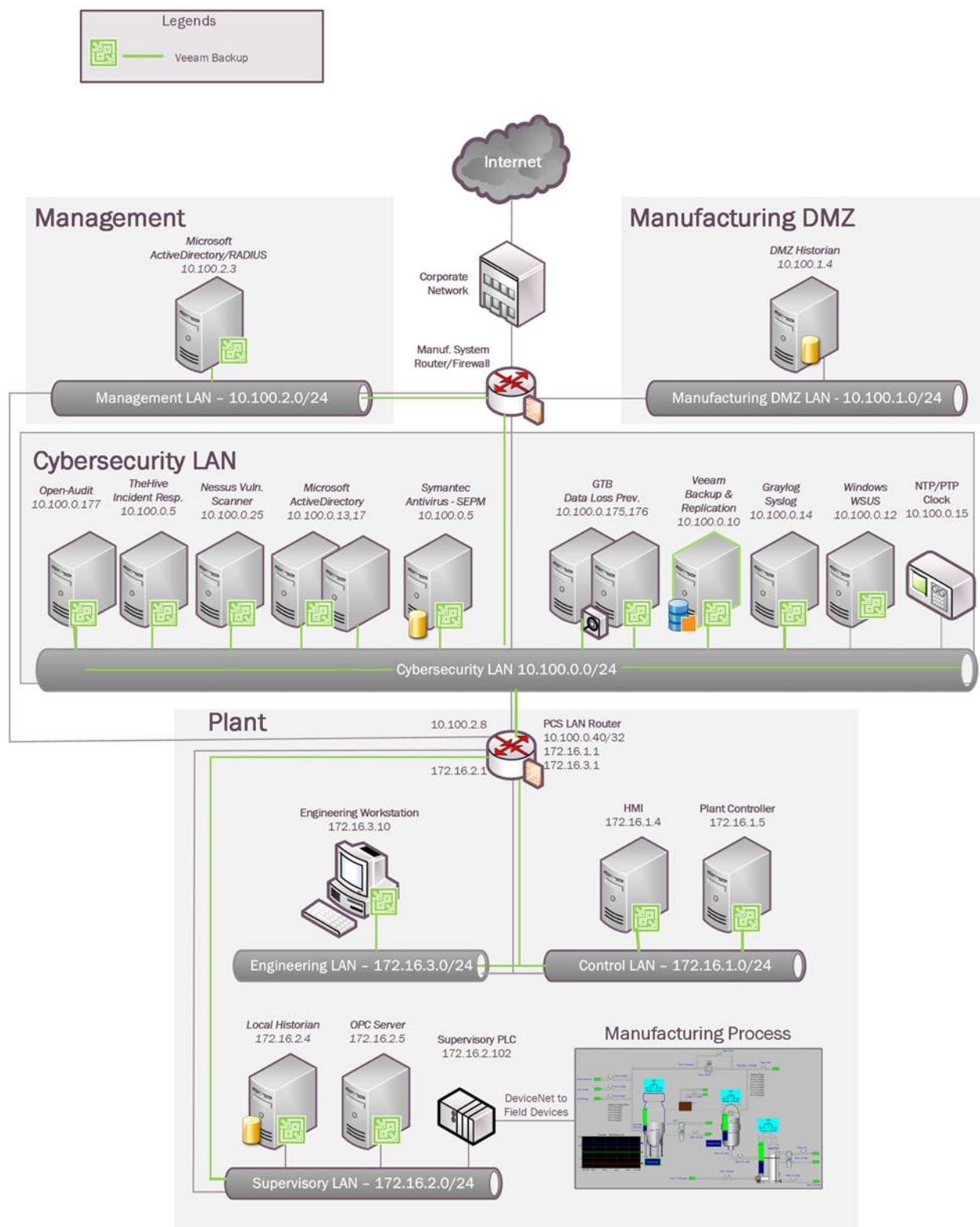
3007 **4.6.2 Technical Capabilities Provided by Solution**

3008 Veeam Backup and Replication provides components of the following Technical Capabilities
3009 described in Section 6 of Volume 1:

- 3010 • Data Backup
- 3011 • Data Replication

3012 **4.6.3 Subcategories Addressed by Implementing Solution**

3013 PR.IP-4

3014 **4.6.4 Architecture Map of Where Solution was Implemented**

3015

4.6.5 Installation Instructions and Configurations

Setup

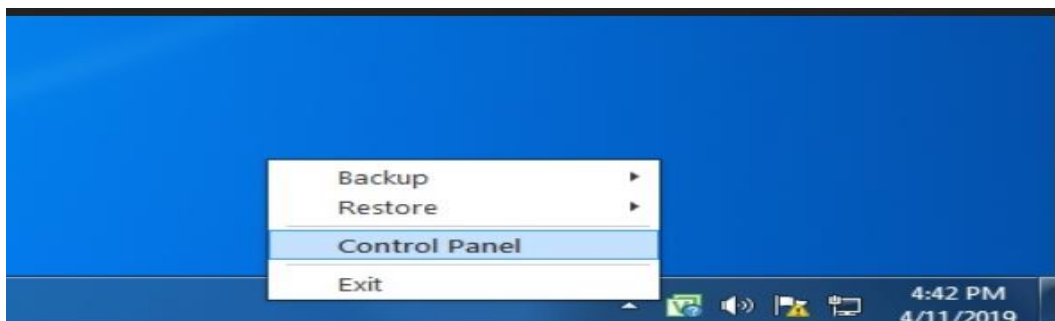
- The following products from Veeam were implemented

Name	Purpose	Version
Veeam Backup and Replication	Veeam Backup Server and Repository	9.5
Veeam Agent for Windows (Free version)	For backup/recovery of Physical Windows Systems in Process Control Network	3.0.0.748

- A Windows 2012 Virtual Machine was setup in the Cybersecurity LAN for installing Veeam Backup and Replication Server. Around 4TB of storage was allocated to this VM for backup storage.
- The Free Edition of Veeam Backup and Replication lets you manage virtual machine backups from the Central Veeam Backup and Replication Console. However, any physical servers configured for backup using the Veeam agent cannot be managed from the Central console in the Free edition. These need to be managed locally on the endpoint or client system itself.
- A parent folder called “**backups**” was created on the 4TB storage drive for saving the backups. Within this folder, different sub folders were created as per the Server names of Process Control System. Each system’s backup was configured to save its data into its corresponding server name folder. The backups folder was then configured as a network share.
- A service account named “**veeamuser**” was created in Active Directory (Cybersecurity LAN) for backup and recovery purposes. This user was granted Read/Write permissions on the above share.

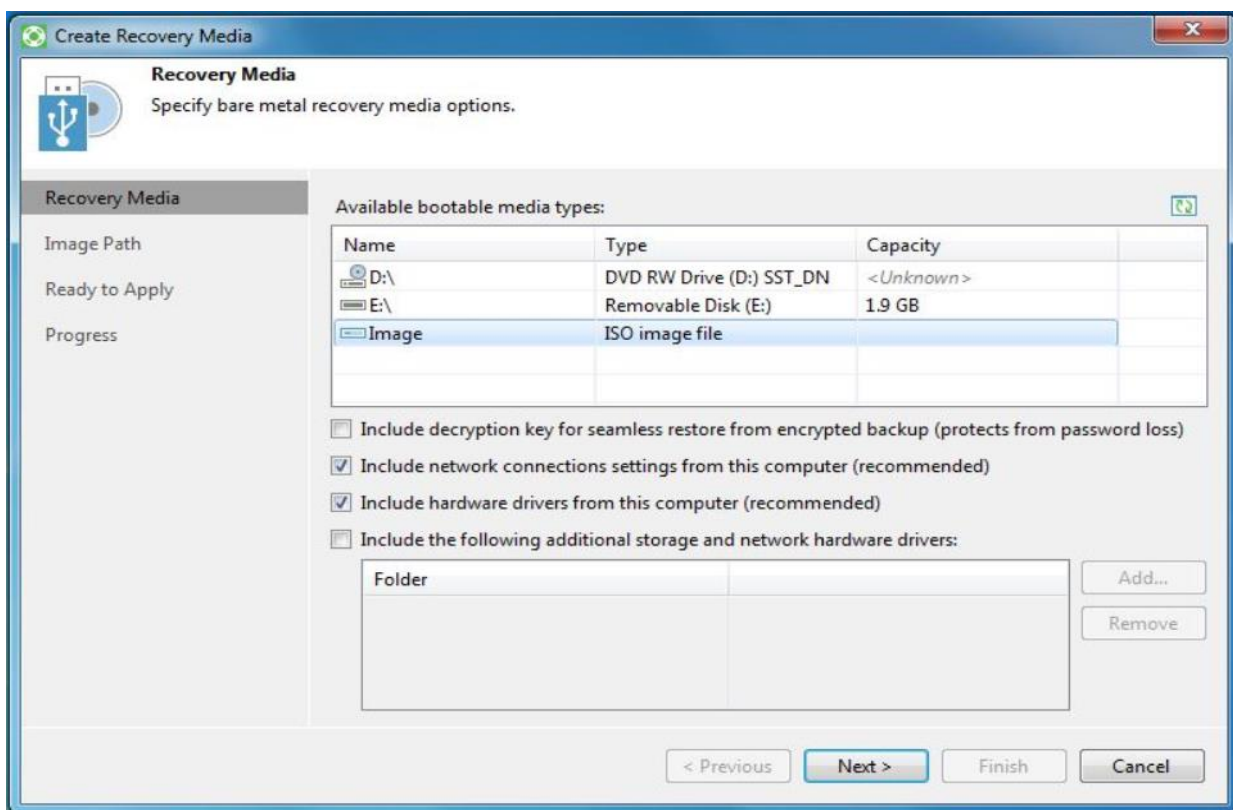
Backups

- All Windows systems of Process Control Network were configured for Backup using Veeam Agent for Microsoft Windows [2].
- The Veeam agent was installed on all Windows clients (systems). Connectivity between each client and the Veeam Server was verified by accessing the “**backups**” share folder (created in the above section) from each client.
- In the Free version, a backup or restore operation needs to be initiated from the client system. Once the agent is installed on the client system, double click the “**Veeam backup icon**” in the System tray to launch the wizard.

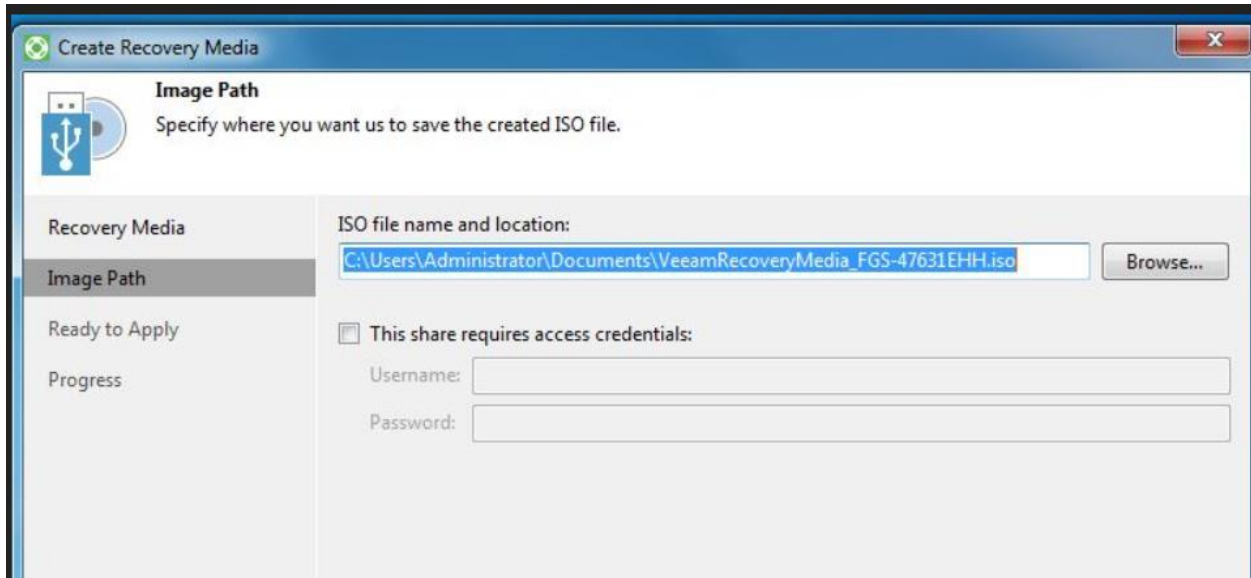


- If this is your first time, the setup wizard will prompt to create a “Recovery Media” which is required for Bare metal backup and restore operations. It is recommended to create this Media if your backup mode is a Full Computer image.

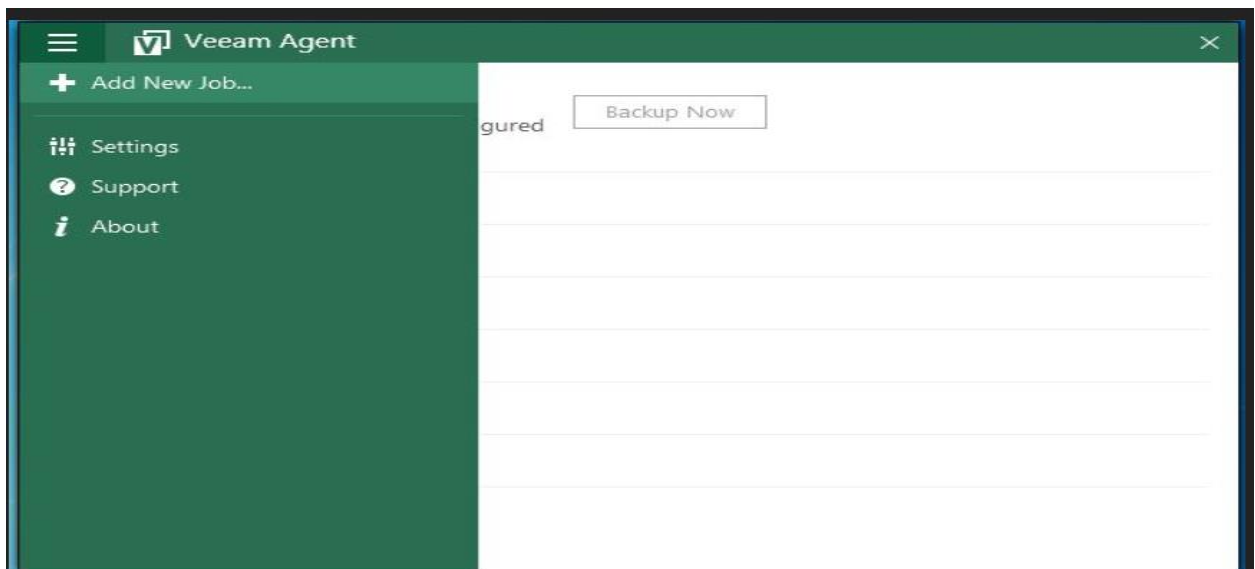
This media creation wizard can also be launched manually by running **Veeam.Endpoint.RecoveryMedia.exe** program under **C:\Program Files\Veeam\Endpoint Backup** directory. Once launched, select one of the 3 options under **Available Bootable Media Types** as per your requirement



- If ISO option is selected, enter the name and location to save the ISO.



- 3061
- 3062
- 3063
- 3064
- 3065
- 3066
- 3067
- 3068
- 3069
- 3070
- 3071
- The system will need to be booted off the ISO when performing a Restore / Recovery option of the Entire Computer or Volume based backups.
 - There are 3 types of backup jobs supported –
 - (1) Entire Computer which is the system image
 - (2) Volume level
 - (3) File level backup.
 However, only one type of backup job can be scheduled in the Free version.
 - To configure a backup job, Right-click on the Veeam Tray, select “**Control Panel >> Backup**” >> Click on **Add New Job**



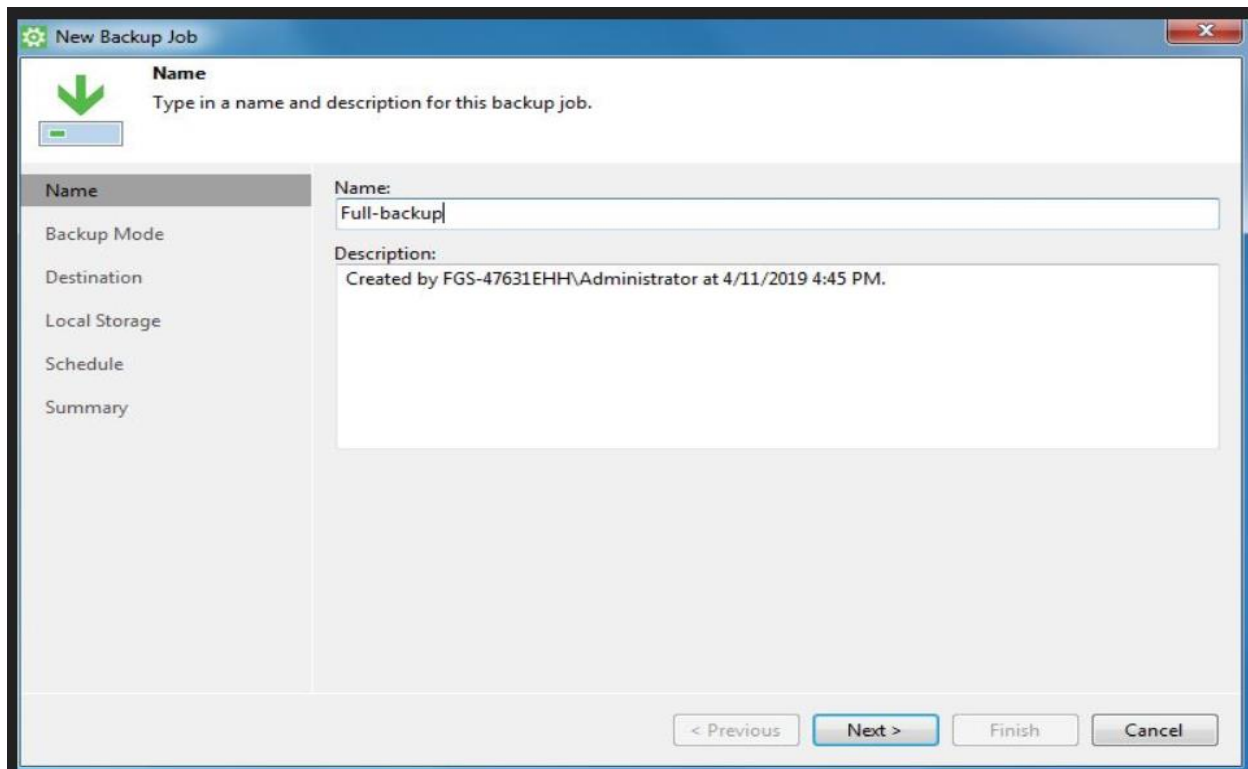
3072

3073

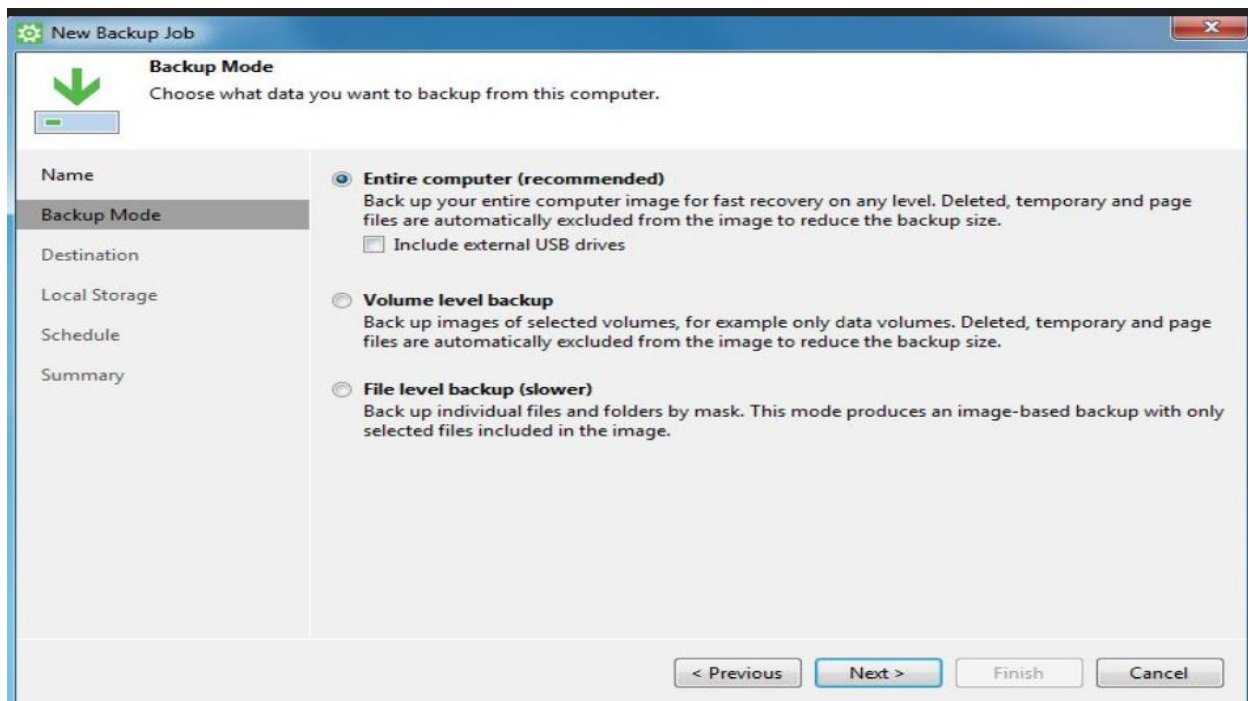
3074

3075

- 3076 • Enter a Name for the Backup Job
3077

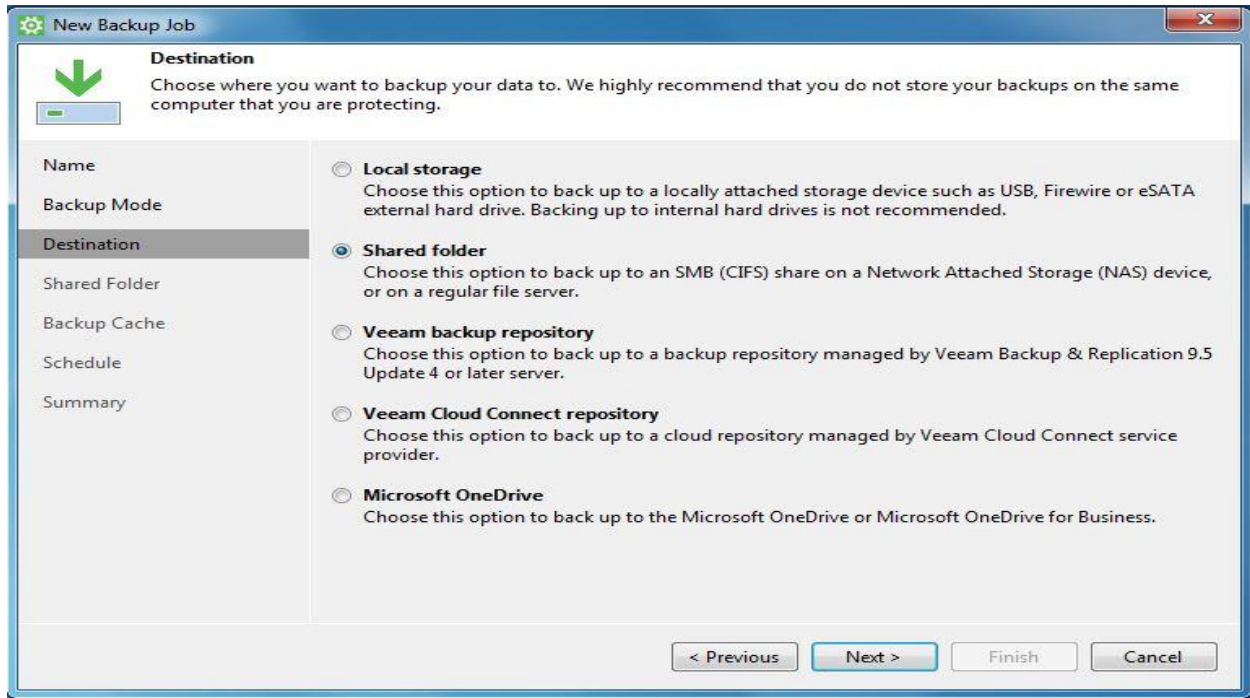


- 3078
3079
3080 • Select a Backup Mode. For instance: Entire Computer
3081

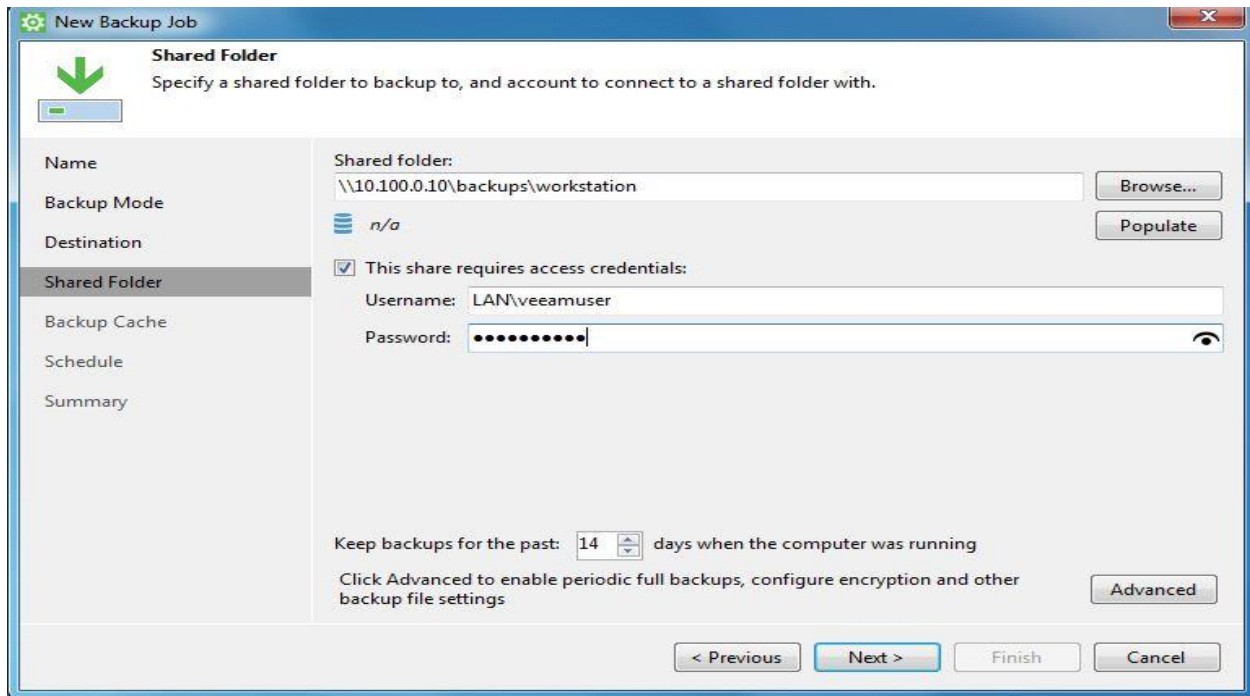


3082

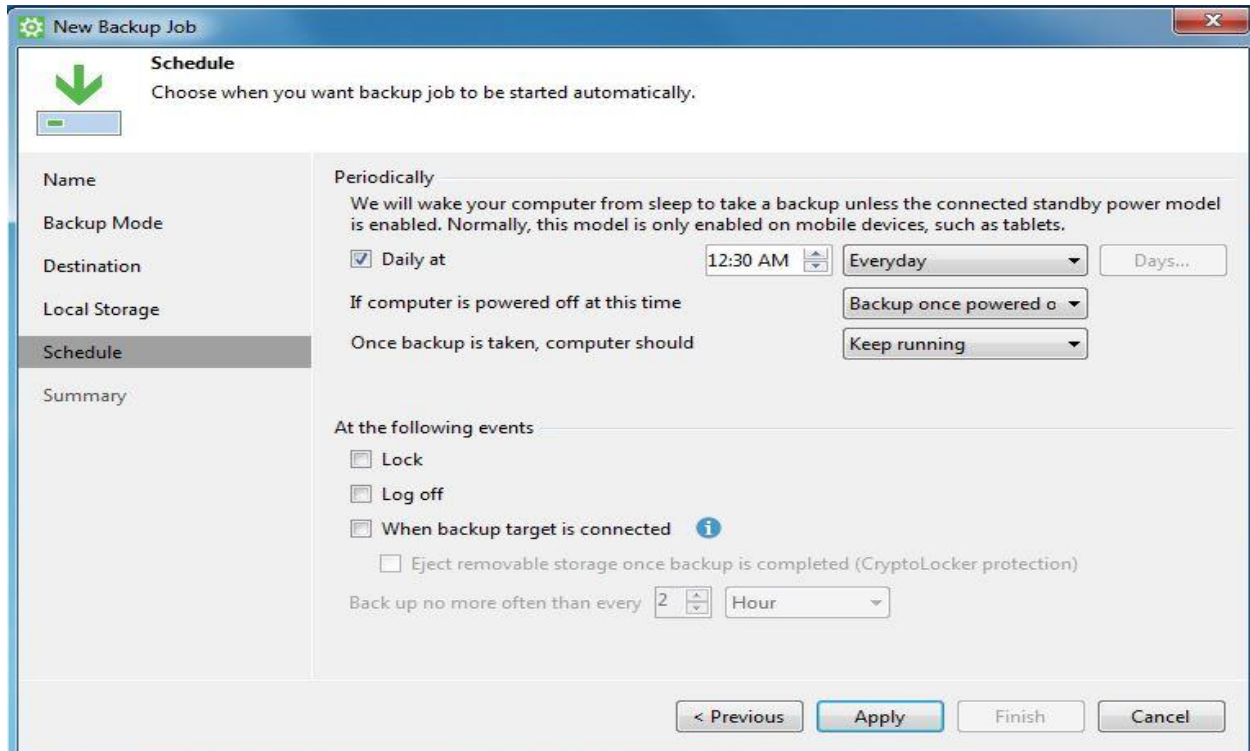
- Select a Backup Destination. Choose “**Shared folder**” if saving the backups to a network share as in our case.



- Enter the path of the Network share and the Active Directory user credentials created earlier. Select the Number of Restore Points as per your retention policy.

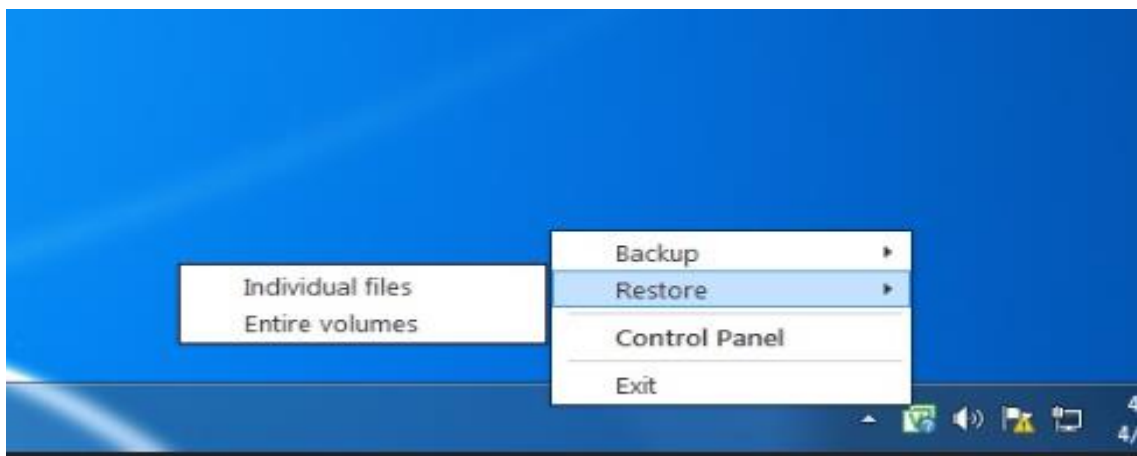


- Configure a Schedule. Hit **Apply** when done.

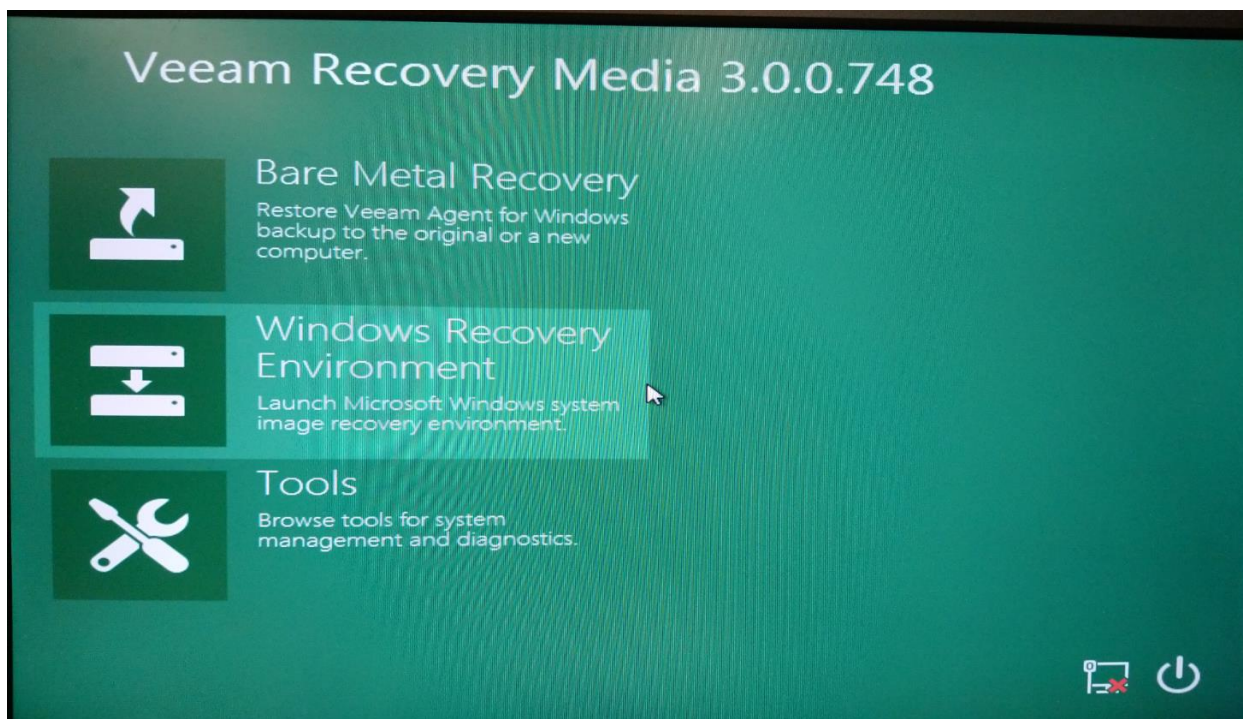


Recovery:

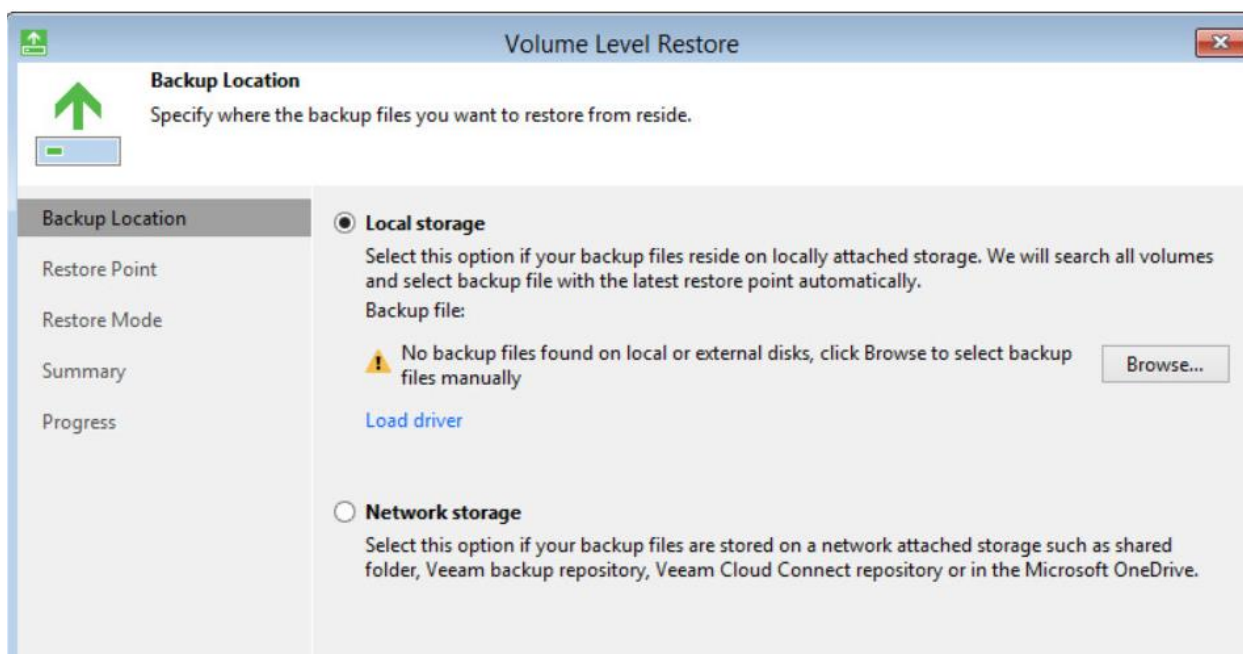
- Recovery of Individual files or Volumes can be done using the Veeam agent in the System Tray itself. Double click on the Agent icon >> **Restore** >> Select <Type> >> Follow the steps.
- Note:** This is dependent on having a successful File-level or Volume-level Backups captured previously.



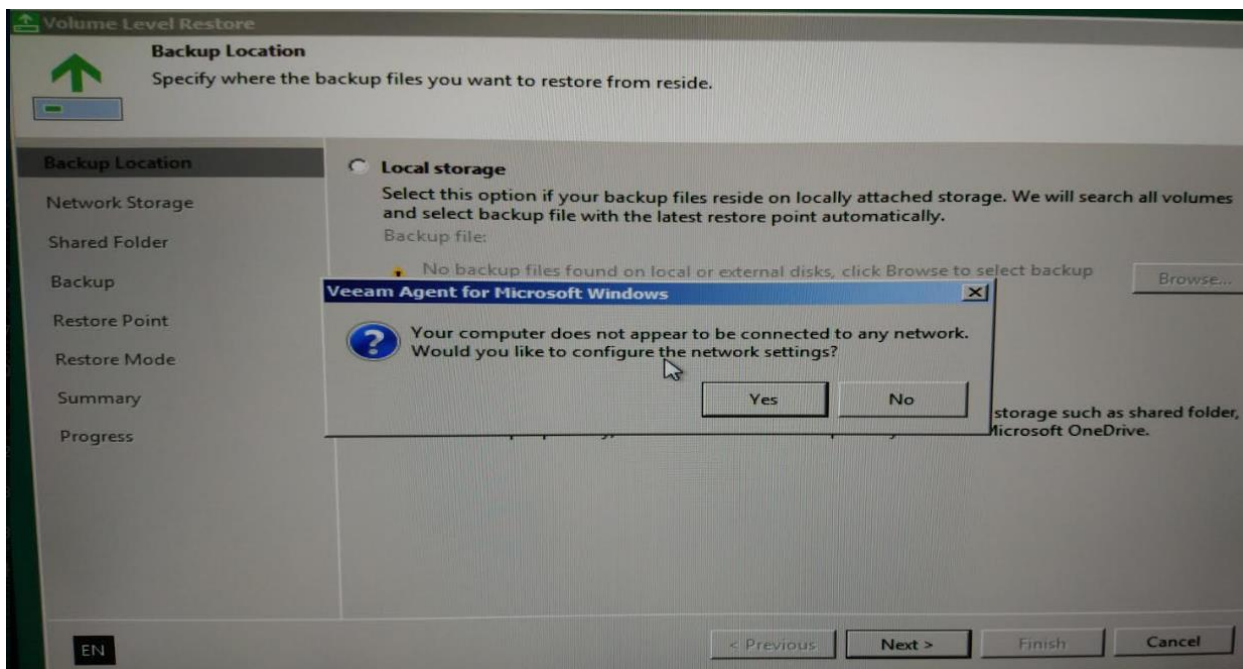
- To perform a Bare Metal restore of the Entire Computer, Boot the system using the Recovery media created earlier. Click on “Bare Metal Recovery”



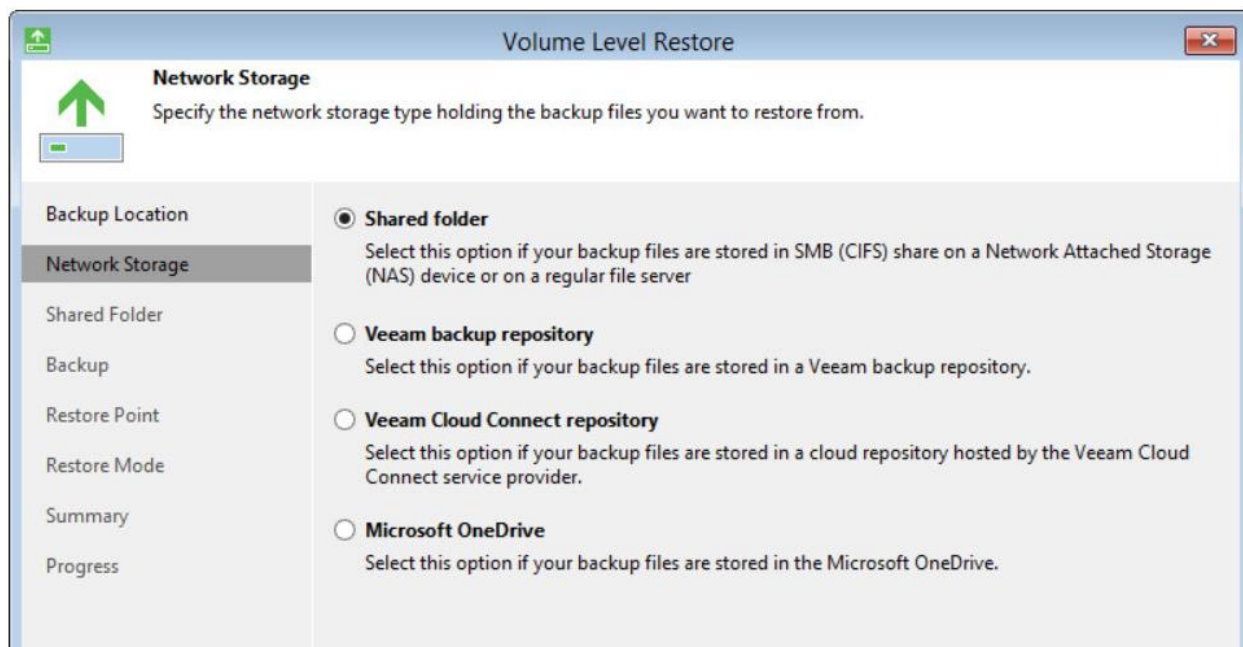
- Select “**Local Storage**” if restoring backups from an External USB Drive or “**Network Storage**” if restoring from a network share as in our case.



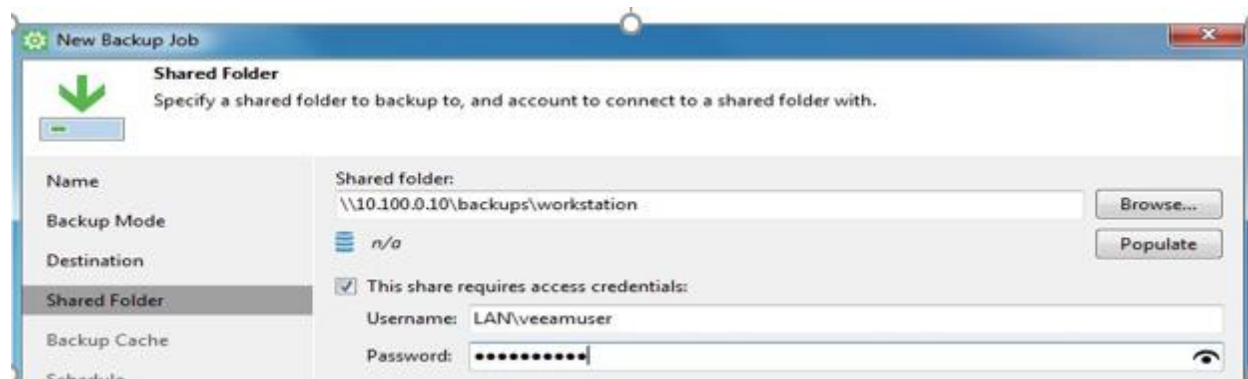
- An option will be presented to configure Network Settings. Choose either DHCP or Static IP and hit Continue.



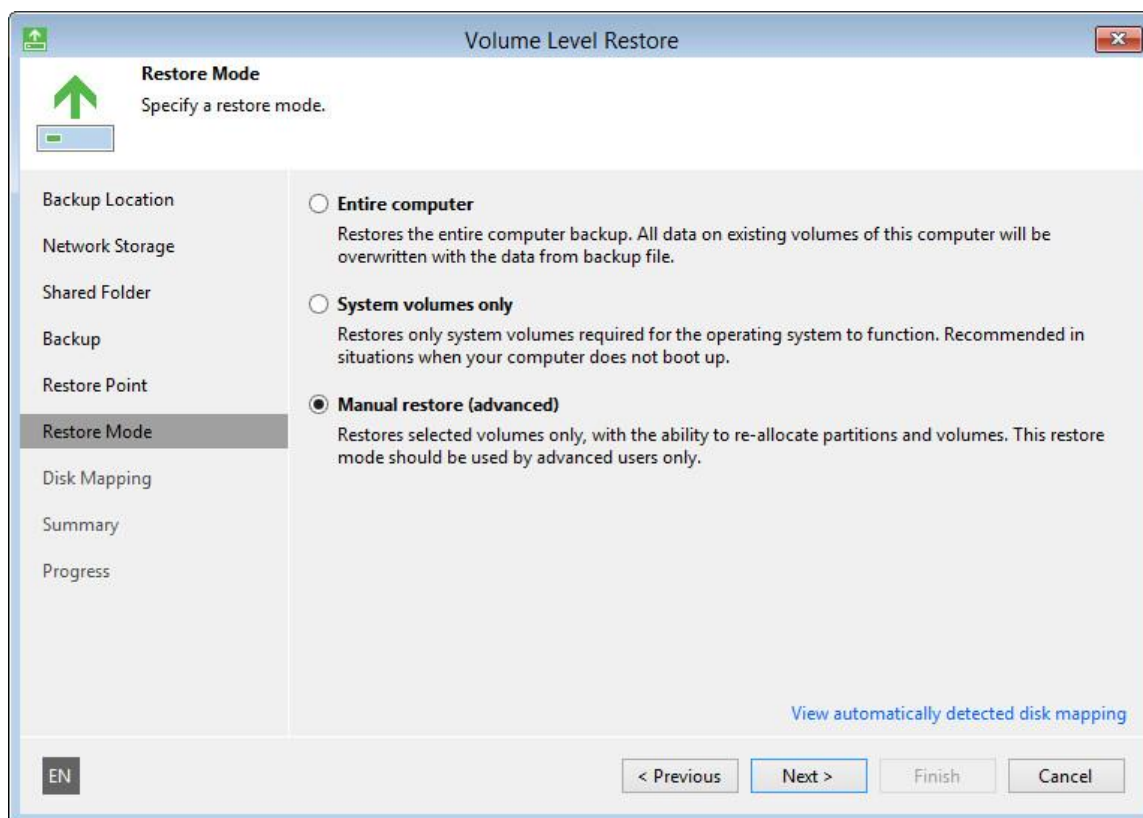
- Under “Network Storage”, select **Share folder**. Hit **Next**



- Enter the path of Share folder to restore from. For instance:



- Next, assuming the wizard is able to connect to the Network share, it will populate a list of Backups. Select a Backup and hit Next.
- Under **Restore Points** select a restore point from which you want to recover data. Veeam Agent for Microsoft Windows displays only restore points of volume-level backups.
- Select a Restore Point and hit Next.
- Under **Restore Mode**, choose a Restore Mode. If the disk type and layout on the system has not changed select "Entire Computer". There is a Manual restore available for advanced users.



- 3134 • Under **Disk Mapping**, Map restored drives as per your system layout. For detailed
3135 instructions on how to map, refer to
3136 [https://helpcenter.veeam.com/docs/agentforwindows/userguide/baremetal_disk_mapping.htm](https://helpcenter.veeam.com/docs/agentforwindows/userguide/baremetal_disk_mapping.html?ver=30)
3137 [l?ver=30](https://helpcenter.veeam.com/docs/agentforwindows/userguide/baremetal_disk_mapping.html?ver=30)
3138 • Under **Summary** Page, review the summary. Hit **Restore** to start the restore process.

3139 **References:**

- 3140 [1] Veeam Backup and Replication [https://www.veeam.com/vm-backup-recovery-replication-](https://www.veeam.com/vm-backup-recovery-replication-software.html)
3141 [software.html](https://www.veeam.com/vm-backup-recovery-replication-software.html)
3142 [2] Veeam agent for MS Windows Free edition [https://www.veeam.com/windows-endpoint-](https://www.veeam.com/windows-endpoint-server-backup-free.html)
3143 [server-backup-free.html](https://www.veeam.com/windows-endpoint-server-backup-free.html)

3144 **4.6.6 Highlighted Performance Impacts**

3145 The following performance measurement experiment was performed for the Veeam Backup tool
3146 while the manufacturing system was operational:

- 3147 Experiment PL009.2- Veeam full backup
3148 Experiment PL010.1- Veeam incremental backup

3149 A small performance impact to the manufacturing process was observed in, however, a more
3150 noticeable impact was observed in the network traffic. For example, the round trip time from the
3151 Controller to the OPC was increased significantly during the backup. The path delay from the
3152 OPC to HMI was also increased significantly during the backup. The amount of backup traffic
3153 could take up a large portion of the available bandwidth.

3154 Also, there is storage consideration, example of backup size in the PCS system: HMI: 96GB,
3155 OPC: 29GB, Controller: 31GB, Historian: 194GB

3156 Network usage should be taken into consideration on when to perform a full backup, a low
3157 network utilization time is likely to reduce the impact to the system One important feature of the
3158 Veeam backup is its ability to throttle to adapt to the network utilization in order to avoid taking
3159 up all the available bandwidth for the backup traffic.

3160 Incremental backup should be considered for periodic backup instead of full image backup.

3161 During the full backup, the network traffic increased dramatically, in one case, the backup of the
3162 HMI and Controller hosts represented 99.6% of the total traffic verse 0.4% of the normal traffic.

3163

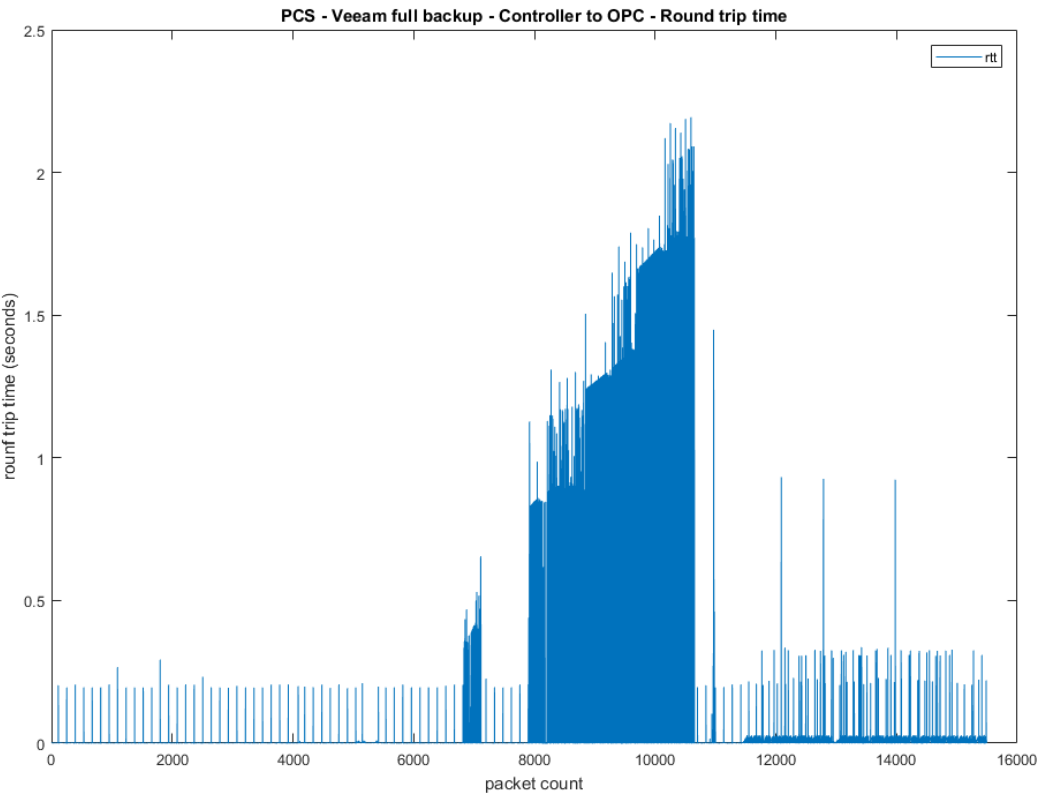


Figure 4-7 Plot of packet round trip time from Controller to OPC during Veeam full backup

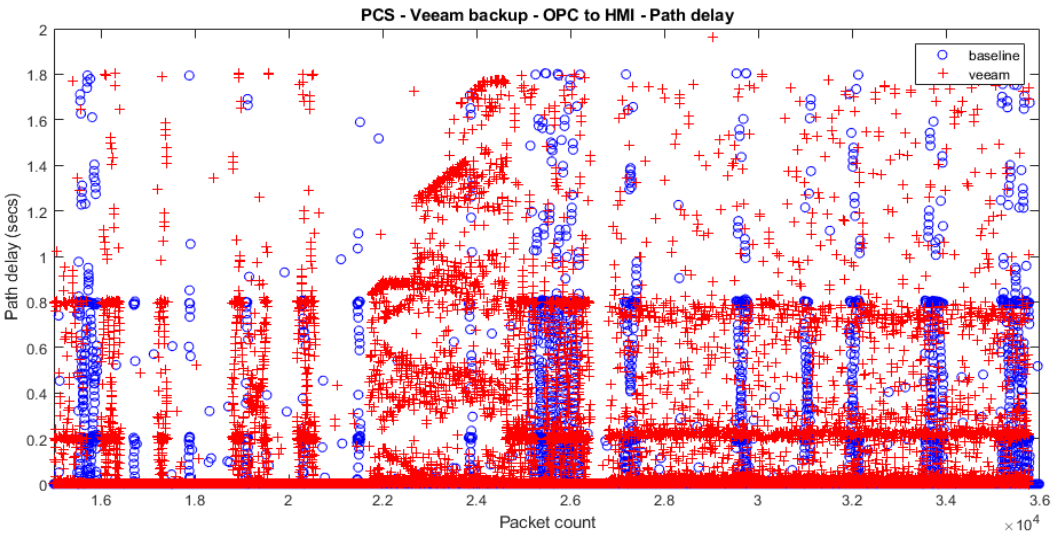


Figure 4-8 Plot of the path delay from OPC to HMI during Veeam full backup

Incremental backup should be considered, the amount of network resources consumed was much lower compare with full backup. The round trip time from Controller to OPC during an incremental backup was increased only for a short amount of time.

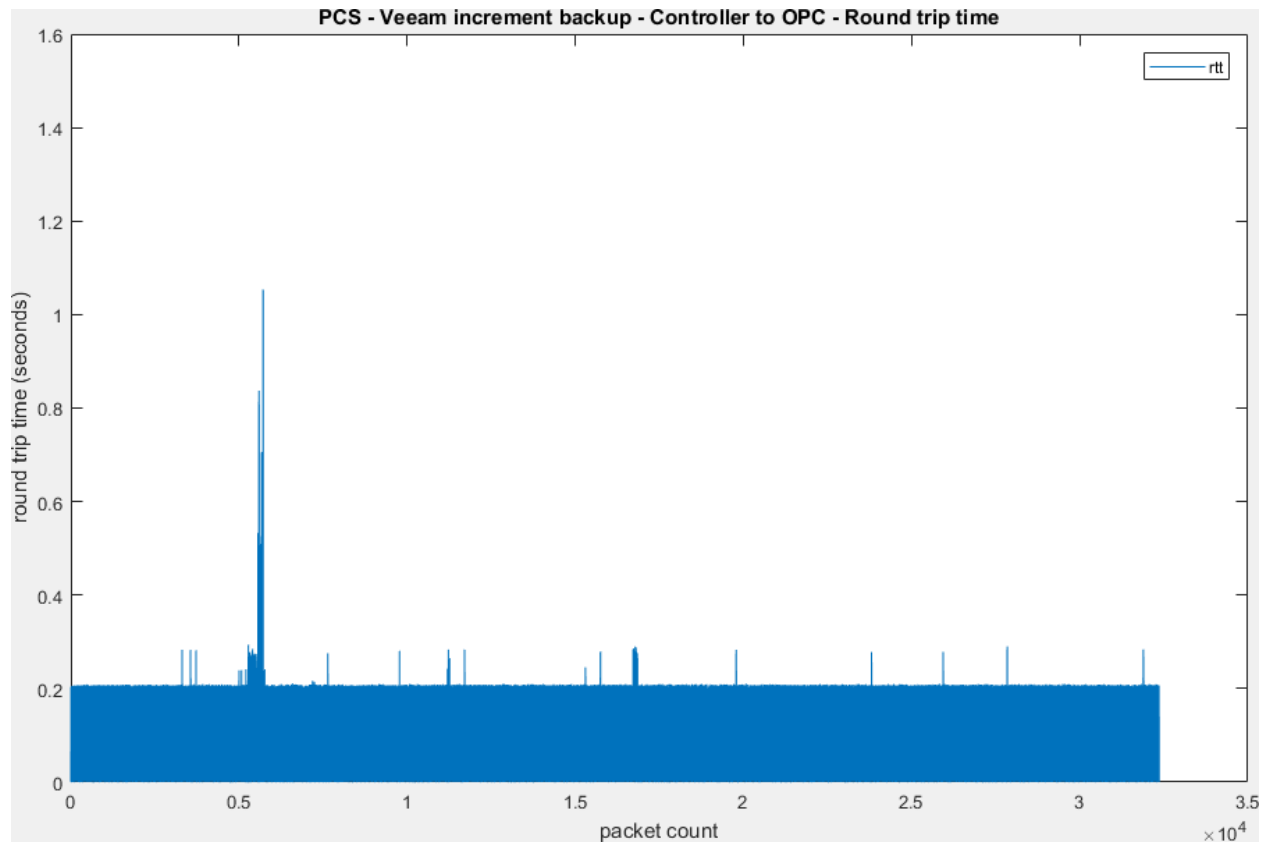


Figure 4-9 Plot of the packet round trip time from Controller to OPC during Veeam incremental backup

There was a small performance impact to the manufacturing process observed during the full backup. The product flow was slightly lower and the reactor pressure overshoot their normal levels in the experiment.

It is hypothesized that the impacts were caused by increased network latency and traffic which caused a delay of the sensor and actuator information exchange between the Controller and the simulated plant. Therefore, a degrade performance of the control loop causing a slight impact to the performance of the system. The ability of the Veeam backup to throttle the rate of backup according to the network condition helped reduce the impact to the network traffic and latency during the full backup.

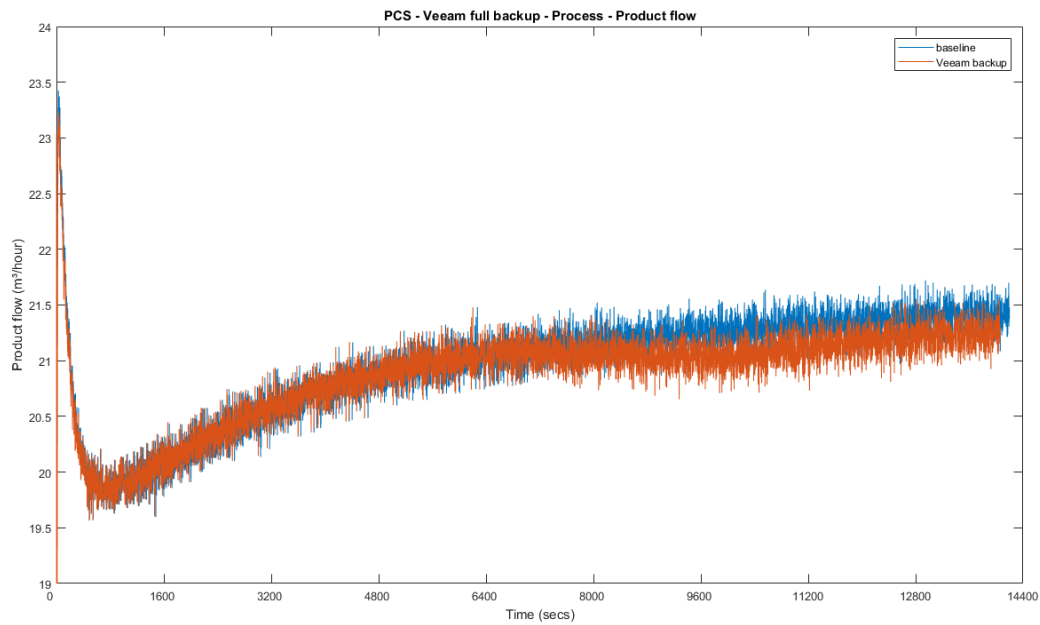


Figure 4-10 Plot of the production flow of the manufacturing process during Veeam full backup

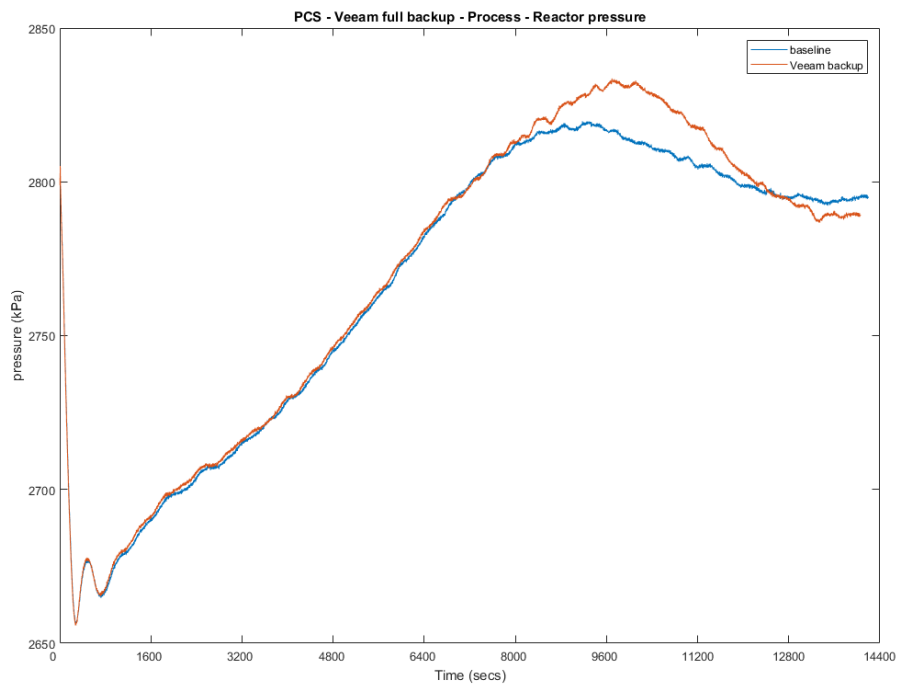


Figure 4-11 Plot of the reactor pressure of the manufacturing process during Veeam full backup

3190 **4.6.7 Link to Entire Performance Measurement Data Set**

3191 [Veeam full backup KPI data](#)

3192 [Veeam full backup measurement data](#)

3193 [Veeam incremental backup KPI data](#)

3194 [Veeam incremental backup measurement data](#)

3195

3196

3197 **4.7 Security Onion**

3198 **4.7.1 Technical Solution Overview**

3199 Security Onion is a free and open source Linux distribution for intrusion detection, enterprise
3200 security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort,
3201 Suricata, Bro, OSSEC, Sguil, Squert, NetworkMiner, and many other security tools.¹⁴ Security
3202 Onion combines three core functions:

- 3203 • full packet capture;
- 3204 • network-based and host-based intrusion detection systems (NIDS and HIDS,
3205 respectively);
- 3206 • and powerful analysis tools

3207 Points to consider:

- 3208 • Open source software, available as an ISO distribution to deploy in any type of
3209 environment (physical or virtual).
- 3210 • Collection of different open-source tools such as SNORT, BRO, OSSEC SGQUIL,
3211 KIBANA, ELSA etc. integrated into one product which otherwise would require lot of
3212 manual work to integrate.
- 3213 • Support for standalone instance and distributed deployment for large organizations.
- 3214 • Provides a front-end to Snort and BRO IDS which natively are command line-based
3215 tools.
- 3216 • Fully customizable rule-set. Has inbuilt detection rules to detect a variety of cyber-attacks
3217 and anomalies for both IT and OT environments.
- 3218 • Learning curve associated. Familiarity with SNORT and BRO IDS rule-set.
- 3219 • Hardware Resource intensive.
- 3220 • No reporting capabilities out of the box.

3221 **4.7.2 Technical Capabilities Provided by Solution**

3222 Security Onion provides components of the following Technical Capabilities described in
3223 Section 6 of Volume 1:

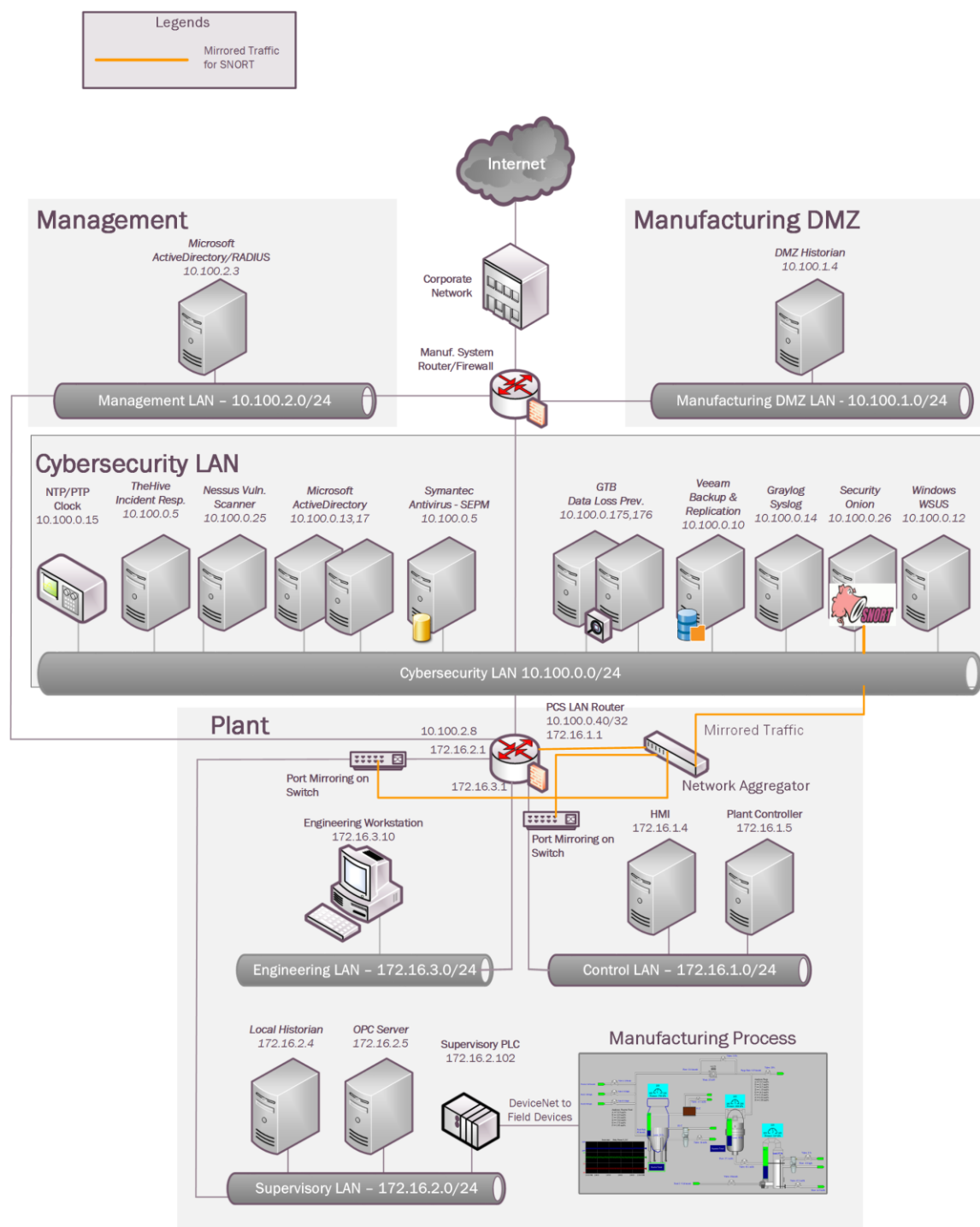
- 3224 • Network Boundary Protection
- 3225 • Network Monitoring
- 3226 • Event Logging
- 3227 • Forensics

¹⁴ Security Onion: <https://securityonion.net/>

3228 **Subcategories Addressed by Implementing Solution**

3229 PR.DS-5, PR.PT-4, DE.AE-2, DE.CM-1, DE.CM-6, DE.CM-7

3230

3231 **4.7.3 Architecture Map of Where Solution was Implemented**

3232

4.7.4 Installation Instructions and Configurations**Setup**

- An ISO image of the Security Onion was downloaded from their website (<https://securityonion.net/>) and deployed on a Microsoft Hyper-V virtual host in the Cybersecurity LAN network. Ensure to assign appropriate hardware resources as recommended in the product documentation.¹⁵

Details of the solutions implemented:

Name	Version	Hardware details
Security Onion	16.04.5.2	Virtual Machine with 4 virtual cores, 20GB Memory, 400GB Disk

- Ours is a standalone single server deployment. For larger environments, Security Onion supports a distributed deployment mode consisting of multiple remote sensors. Detailed setup documentation is available on their wiki.¹⁶

- Security Onion requires 2 physical network connections as follows –

- (i) **(eth0)** for management IP address
- (ii) **(eth1)** for the monitoring interface. This interface needs to be configured in promiscuous mode to leverage the SNORT and BRO IDS components for monitoring network traffic.

For (i) a virtual switch connection was provisioned from the Cybersecurity LAN and assigned to the Security Onion VM. This is for setting up an IP address to login to Security Onion interface or the server itself.

For (ii) Port Mirroring was configured on the two network switches and the Boundary Firewall. These mirrored port(s) were further connected to a Network Aggregator device.

The Network Aggregator device is used for aggregating traffic from these network devices of the Process Control System. An outbound connection from its Aggregated interface was made to the **monitoring interface (eth1)** of the Security Onion VM. Figure 1 below shows the setup of security onion in our environment.

¹⁵ Security Onion Documentation: <https://securityonion.readthedocs.io/en/latest/>

¹⁶ Security Onion WIKI: <https://github.com/Security-Onion-Solutions/security-onion/wiki>

- Once the two network connections are connected, power on the virtual machine and complete the default Linux OS setup as per the instructions on the screen. Upon a system reboot, login to the console locally and click on the **Setup** icon on the “**Desktop**” to configure the network interfaces. This step includes assigning a static IP address for management and setting up the monitoring port of the instance. Ensure to select the correct interfaces for each role. A Reboot is required upon completion.
- Reboot the system and click on the Setup icon again to complete the next phase of the setup. It will display the below message. Click **YES, Continue!** and then select **Evaluation Mode** in the next screen for standalone deployments.



- Follow the on-screen options and complete the wizard. A system reboot would again be required.
- Security Onion by default allows SSH only from localhost. To connect to it remotely, run the command “**sudo so-allow**” to configure the appropriate firewall rules for remote connectivity. Select “**a – analyst**” option and whitelist the IP address or ip-range of client-pc where you intend to access security onion interface from. Instructions to setup the firewall can be found here: <https://github.com/Security-Onion-Solutions/security-onion/wiki/Firewall>
- Upon completion of both setup phases, security onion should now be accessible using any of the 3 methods below:
- SQUERT Web Interface: This is the web interface to the backend Sguil database. The URL is <https://IP address-of-security-onion/>
- Kibana: Kibana is an open source data visualization plugin for Elasticsearch. It can be accessed via <https://ip-address-of-security-onion/app/kibana>
- Sguil client: A windows-based client is available for querying the Sguil database at <https://bammv.github.io/sguil/index.html> for installing on a remote workstation.
- The credentials to login to the above URLs should be the one that were created earlier during the setup process.

- 3295 • Ensure to set the OS time-zone to UTC as Security Onion uses UTC by default. Changing
3296 time-zone can cause other issues.
- 3297 • The command **sudo nsm_sensor_ps-status** can be used to check the status of each
3298 Security Onion component/service.

3299

3300 **Configuring Updates:**

- 3301 • Register on SNORT.org for an account to be eligible for downloading the “Registered” Rule
3302 set. Upon registration, note down the OINK code tied to your account. Copy-paste the OINK
3303 code in the “rule_url” parameter in **/etc./nsm/pulledpork/pulledpork.conf** file of the server
3304 and save the changes.

3305 **rule_url=https://www.snort.org/reg-rules/|snortrules-snapshot.tar.gz|<oink-code>**

3306

3307 Security Onion by default requires internet access to download Snort signatures. If your
3308 Security Onion server has internet access, uncomment and set

3309 **“LOCAL_NIDS_RULE_TUNING=no”** in **/etc./nsm/securityonion.conf** file. Run the **“sudo**
3310 **rule-update”** command to update the rule set. This will download new rules from Snort.org
3311 and save them in **/etc./nsm/rules/downloaded.rules** file.

3312

- 3313 • For Air-Gapped environments (w/o Internet), set **LOCAL_NIDS_RULE_TUNING=yes**
3314 in the securityonion.conf file and the snort updates would have to be manually downloaded
3315 on a different system and transferred via USB device or network to **/tmp** folder on the
3316 Security Onion server. Once done run the **sudo rule-update** command.

3317 **SNORT IDS Setup:**

- 3318 • Define the network variables such as \$HOME_NET, \$EXTERNAL_NET etc. as per your
3319 environment in the snort configuration file (snort.conf) located at **/etc./nsm/<hostname-**
3320 **MonitorInterface>/.** Once done, the snort service should be restarted by running the
3321 command:

3322 **sudo nsm_sensor_ps-restart --only-snort**

3323

3324 Below is a snippet of the **snort.conf** in our instance

3325


```
#####
# Step #1: Set the network variables.  For more information, see README.variables
#####

# Setup the network addresses you are protecting
ipvar HOME_NET [192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]

ipvar NETWORK_DEVICES [172.16.1.3,172.16.3.1,172.16.2.2,192.168.0.239,192.168.0.2,192.168.1.2]
ipvar ICS_DEVICES [172.16.2.102,172.16.4.102,192.168.0.30,192.168.0.60]
ipvar PCS_ICS_DEVICES [172.16.2.100/30]
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS [10.100.0.17]

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
```

- The Snort module uses the downloaded.rules under **/etc./nsm/rules/ directory** for its IDS rule set in addition to any local rules defined under **/etc./nsm/rules/local.rules** file. All custom rules should be defined under this **local.rules** file. Upon adding a custom rule, the snort rule set must be updated using this command: **sudo rule-update**

This command will also result in local rules getting merged into downloaded.rules file. Additionally, you can manually verify the same by running **tail -n 100 downloaded.rules**. If the defined local rules do not appear in the downloaded.rules file; the **/etc./nsm/<interface>/snortu-1.log** file must be reviewed for any syntax errors.

Below are some of the rules we setup to detect common IT and ICS-specific anomalies.

Detect NMAP scan, ICMP attack, TCP-SYN Flood attack

```

alert udp any any -> $PCS_ICS_DEVICES any (msg: "Nmap UDP Scan"; sid:10000002; rev:1;)
alert icmp any any -> $HOME_NET any (msg: "NMAP ping sweep Scan"; dsize:0; sid:10000004;
rev:1;)
alert icmp any any -> $HOME_NET any (msg: "Ping Large ICMP Packet"; dsize:>800; classtype:bad-
unknown; sid:10000030; rev:1;)
alert tcp any any -> $HOME_NET [80,22,443] (msg: "TCP SYN flood attack detected"; flow: stateless;
flags:S,12; detection_filter:track by_dst, count 100, seconds 10; classtype: attempted-recon;
sid:10000005; rev:1;)

```

Detect FTP Attempt to Public IP-address & other FTP events

```

alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000003;
rev:1;)
alert tcp $HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: "|53 54 4f 52|";
sid:10000020; rev:1;)
alert tcp any 21 -> $HOME_NET any (msg: "FTP file successfully uploaded"; content: "|54 72 61 6e 73
66 65 72 20 63 6f 6d 70 6c 65 74 65|"; sid:10000027; rev:1;)
alert tcp any 21 -> $HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf";
sid:10000031; rev:1;)

```

Detect Credit card number in cleartext

```

alert tcp any any <> any any (pcr: "/5\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; msg: "MasterCard
number detected in clear text"; content:"number"; nocase; sid:10000013; rev:1;)
alert tcp any any <> any any (pcr: "/3\d{3}(\s|-)?\d{6}(\s|-)?\d{5}/"; msg: "American Express number
detected in clear text"; content:"number"; nocase; sid:10000014; rev:1;)
alert tcp any any <> any any (pcr: "/4\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; msg: "Visa number
detected in clear text"; content:"number"; nocase; sid:10000015; rev:1;)

```

Telnet activity monitoring

```

alert tcp $TELNET_SERVERS 23 -> $HOME_NET any (msg: "Telnet Password in Clear text"; content:
>Password"; sid:10000010; rev:1;)
alert tcp $HOME_NET any -> $TELNET_SERVERS 23 (msg: "TELNET login attempt";
classtype:default-login-attempt; sid:10000007; rev:1;)
alert tcp $HOME_NET any -> $TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default
Password"; content: "|73 77 69 74 63 68|"; sid:10000008; rev:1;)
alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Login
failed"; fast_pattern:only; nocase; classtype:bad-unknown; sid:10000038; rev:1;)

```

3340

3341

3342

3343 Snort Rules for ICS/ SCADA¹⁷

3344

#ICS-SCADA specific rules [4]

```

alert tcp $HOME_NET any -> $ICS_DEVICES 44818 (msg: "PROTOCOL-SCADA Rockwell firmware
change attempt"; flow:to_server,established; content:"|6F 00|"; content:"|00 00 00 00|"; within:4; distance:6;
content:"|00 00 00 00|"; within:4; distance:8; pcre:"/(\x20\xa1\x21\x00\xa1\x00)(\x24[\x01-
\xff][\x25\x00[\x01-\xff]\x00)/smi"; reference:cve,2012-6437;
reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=27868; classtype:policy-violation;
sid:1000019; rev:1;)
alert tcp $HOME_NET any -> $ICS_DEVICES $HTTP_PORTS (msg: "ICS-SCADA PLC Web access
attempted "; sid:1000033; rev:1;)
alert tcp any any -> $HOME_NET 22350 (msg: "PROTOCOL-SCADA TwinCAT PLC DOS attempt";
flow:to_server,established; dsize:>2000; content:"|A2 1D CB AA AA 75 48 B4 91 DB F4 06 B0 B0 2D|";
fast_pattern:only; metadata:policy max-detect-ips drop, policy security-ips drop;
reference:url,www.beckhoff.com/english.asp?twincat/overvw.htm; classtype:attempted-dos; sid:41743;
rev:2;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus user-defined function code
- 65 to 72"; flow:to_server,established; byte_test:1,>,64,7; byte_test:1,<,73,7;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:15074; rev:5;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus user-defined function code
- 100 to 110"; flow:to_server,established; byte_test:1,>,99,7; byte_test:1,<,111,7;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:15075; rev:5;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus read multiple coils - too
many inputs"; flow:to_server, established; modbus_func:read_coils; byte_test:2,>,2000,10;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:15077; rev:6;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write multiple registers
from external source"; flow:to_server,established; modbus_func:write_multiple_registers;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:17782; rev:4;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write single coil from
external source"; flow:to_server,established; modbus_func:write_single_coil;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:17784; rev:4;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write multiple coils from
external source"; flow:to_server,established; modbus_func:write_multiple_coils;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-
command-decode; sid:17785; rev:4;)

```

3345

¹⁷ Snort Rules for ICS/ SCADA: <https://github.com/ITI/ICS-Security-Tools/blob/master/configurations/rules/talos-snort.rules>

Accessing switch via Web URL & use of default password

```

alert tcp any -> $NETWORK_DEVICES 80 (msg: "WEBAPP Netgear Default Password";
flow:established,to_server; content:"POST"; nocase; http_method;
uricontent: "/base/cheetah_login.html"; content:"password"; nocase; sid:1000009; rev:1;)
alert tcp $HOME_NET any -> $NETWORK_DEVICES $HTTP_PORTS (msg: "WEBAPP Rockwell
Automation default password login attempt"; flow:to_server,established; content:"Authorization[3A]";
nocase; http_header; content:"YWRtaW5pc3RyYXRvcjptbDE0MDA="; fast_pattern:only; http_header;
metadata:service http; classtype:default-login-attempt; sid:10000011; rev:1;)

```

SSH Activity monitoring

```

alert tcp any any -> $EXTERNAL_NET 22 (msg: "SSH Attempt to Public Host"; sid:10000018; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg: "Potential SSH Brute Force Attack"; flow:to_server,
established; flags:S+; detection_filter:track by_src, count 30, seconds 10; classtype:attempted-dos;
priority:1; sid:10000006; rev:1;)

```

DNS traffic to social media websites

```

alert udp $HOME_NET any -> $DNS_SERVERS 53 (msg: "DNS Request to Twitter.com Detected";
content: "|6e 69 73 74|"; sid:10000016; rev:1;)
alert udp $HOME_NET any -> $DNS_SERVERS 53 (msg: "DNS Request to Facebook.com Detected";
content: "|66 61 63 65 62 6f 6f 6b|"; sid:10000017; rev:1;)

```

File upload activity to a public web server

```

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "WEB-PHP file upload
attempt"; flow:to_server, established; uricontent: "/upload.php"; nocase; content:"filename=";
reference:bugtraq,3361; reference:cve,2001-1032; classtype:attempted-admin; sid:10000029; rev:1;)
alert tcp $Robotics_devices any -> $EXTERNAL_NET $HTTP_PORTS (msg: "Web Access to Public
IP attempted"; sid:10000039; rev:1;)

```

3346

3347 **Tuning Security Onion:**

- 3348 • The default database retention period for Sguil database is 30 days. This can be changed by
3349 editing the **DAYSTOKEEP** parameter in the **/etc./nsm/securityonion.conf** file.
- 3350 • A number of rules defined in the **downloaded.rules** file are commented out by default. This
3351 is intentional to reduce the volume of alerts and leaving the onus on the end user to
3352 customize it depending on the environment. To use any of the commented-out rules from
3353 downloaded.rules file, note down the Generator ID (GID) and Signature ID (SID) value
3354 defined in the rule that's commented out and list them in
3355 **/etc./nsm/pulledpork/enablesid.conf** file. Avoid directly uncommenting them. This will
3356 enable that rule and will be persistent next time when the **downloaded.rules** gets updated.
- 3357 • Likewise, to silence any false alerts note down the Generator ID (GID) and Signature ID
3358 (SID) value of the rule that is generating the alert and define them in the
3359 **/etc./nsm/pulledpork/disablesid.conf** file. Detailed instructions are available on the Snort
3360 documentation [5] under "Managing alerts".
- 3361 • Shown below is a snippet from our **disablesid.conf** file showing the SIDs we have disabled.
3362
3363
3364

```
# example disablesid.conf V3.1
```

```
# Example of modifying state for individual rules
```

```
# 1:1034,1:9837,1:1270,1:3390,1:710,1:1249,3:13010
```

```
3:19187
```

```
119:19 # http_inspect: LONG HEADER
```

```
123:8 # frag3: Fragmentation overlap
```

```
128:4 # ssh: Protocol mismatch
```

```
129:4 # stream5: TCP Timestamp is outside of PAWS window
```

```
129:5 # stream5: Bad segment, overlap adjusted size less than/equal 0
```

```
129:7 # stream5: Limit on number of overlapping TCP packets reached
```

```
129:12 # stream5: TCP Small Segment Threshold Exceeded
```

- PCAPS can fill up the storage space on server. Follow the instructions on the wiki to manage the pcap files.

BRO IDS Setup:

- Security Onion also uses BRO IDS alongside SNORT for network monitoring. The BRO logs are stored in **/nsm/bro/logs** directory. Similar to local.rules in SNORT, any custom scripts for BRO must be placed in **/opt/bro/share/bro/policy/** directory. Please refer to the security onion wiki [3] for additional reference on BRO.
- To leverage BRO capabilities for Windows SMB File share monitoring, add the below line at the end of **/opt/bro/share/bro/site/local.bro** file

```
@load policy/protocols/smb
```

Once done restart BRO using the command: `sudo nsm_sensor_ps-restart --only-bro`

OSSEC Setup:

- OSSEC server (now replaced with **Wazuh**) comes along with Security Onion. Ossec is a Host Intrusion Detection System (HIDS). The OSSEC server module is installed and running by default in the Security Onion server. OSSEC alerts can be viewed either from Kibana or Squert web interface.
- To configure additional client systems for monitoring using OSSEC, download the agent installer from OSSEC [website](http://www.ossec.net/) (<http://www.ossec.net/>) specific to your Operating System, copy over the agent to the client system and run the setup process using the instructions mentioned on the Ossec website. During the install, mention the IP address of Security Onion server as the IP address of Ossec server. Ensure to open firewall ports on Security Onion server to receive data from Ossec clients.

- It is beyond the scope of this document to explain detailed working of the OSSEC product. The Ossec official website and other documentation links under References can be a useful source.
- Similar to Snort and Bro, any custom OSSEC rules for monitoring should be added in **local_rules.xml** file under **/var/ossec/rules** directory. If a decoder is required to parse custom logs, it should be defined under in **local_decoder.xml** file under **/var/ossec/etc.** directory.
- On Windows systems, OSSEC agents can be configured to monitor Event Viewer logs, Rootkit Detection, File Integrity Monitoring (FIM), Registry changes and any other custom application logs. Instructions are available on OSSEC [website](#).
- Similarly, on Linux systems, OSSEC can perform File Integrity Monitoring, Process Monitoring, Rootkit changes and any other host intrusion attempts such as failed SSH logins.
- Ossec agent was installed on the **Engineering workstation** in Process Control System to detect following anomalies:
 - USB Drive detection [5].
 - Allen Bradley Factory Talk Administration Console login failures.
 - Monitoring Unauthorized Assets.

USB Drive Detection:

- The following lines were added to the local **ossec.conf** file on the Agent side (Engineering Workstation) where an USB drive would be monitored for

```
<agent_config os="Windows">
  <localfile>
    <log_format>full_command</log_format>
    <command>reg QUERY
      HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR</command>
    <alias>usb-check</alias>
  </localfile>
</agent_config>
```

- Next, the following lines were added to the **/var/ossec/rules /local_rules.xml** file on the Security Onion server to generate an alert


```
<rule id="140125" level="7">
  <if_sid>530</if_sid>
  <match>ossec: output: 'usb-check':</match>
  <check_diff />
  <description>New USB device connected</description>
</rule>
```

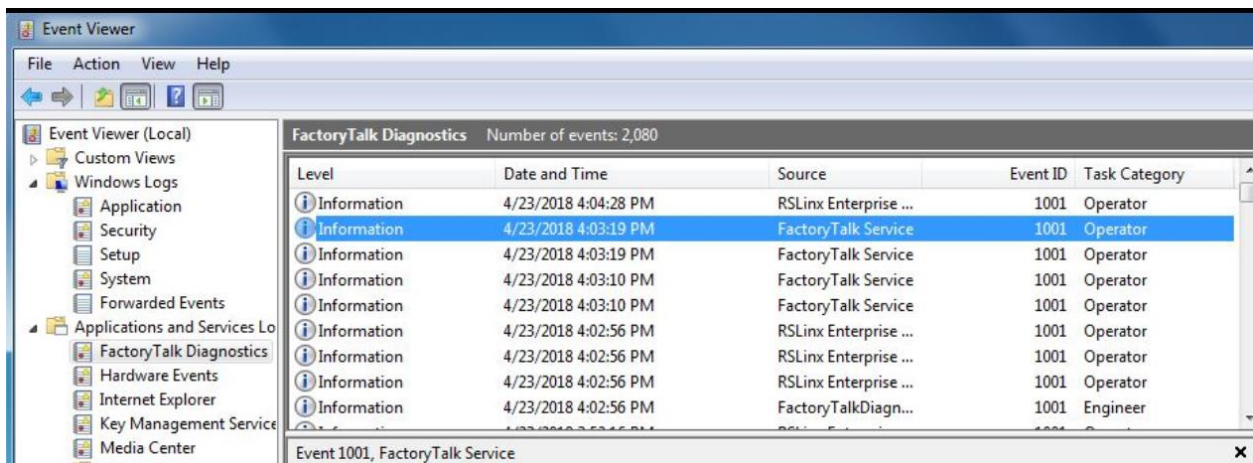
3430
3431

Detecting Allen Bradley-Factory Talk Login failures:

3432
3433

- The Factory Talk Administration Console (installed on the Engineering Workstation) logs all authentication attempts and other diagnostic events under Windows Event Viewer as shown below.

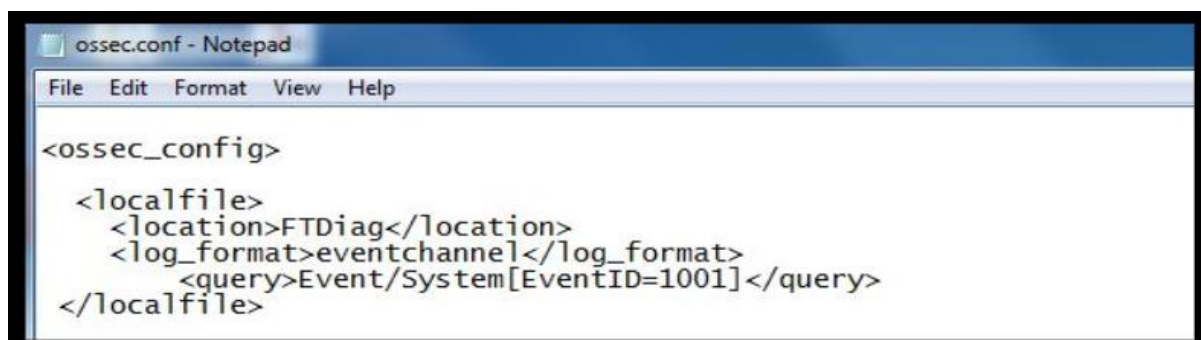
3434
3435
3436
3437



3438
3439

- To alert on login failures from Factory Talk Admin console, the below config was placed in the local **ossec.conf** file of the windows workstation. This line tells Ossec to look for event ID 1001 under “**Factory Talk Diagnostics**” category also referenced as “**FTDiag**” in Event Viewer and forward those events to Ossec server.

3440
3441
3442
3443



```

<ossec_config>
  <localfile>
    <location>FTDiag</location>
    <log_format>eventchannel</log_format>
    <query>Event/System[EventID=1001]</query>
  </localfile>

```

3444

- 3445 • Next on the Ossec server, the following lines were added in **local_rules.xml** file to generate
3446 an alert.

3447

```

<group name="syslog">
  <rule id="110001" level="0">
    <if_sid>18104</if_sid>
    <match>FactoryTalkDiagnostics</match>
    <description>FactoryTalk Audit Event</description>
  </rule>
  <rule id="110002" level="7">
    <if_sid>110001</if_sid>
    <match>failure</match>
    <description>FactoryTalk Administration Console login failure</description>
  </rule>

```

3448

3449 Monitoring for Unauthorized assets:

3450

- 3451 • Rogue/Unauthorized Asset discovery can be implemented using **Arpwatch** and Ossec. To
3452 configure this, install the “arpwatch” package on the Security Onion server. Arpwatch
3453 package is available in all Linux distributions. Upon installation start the arpwatch service
3454 and configure it to listen to the network interfaces using the `arpwatch -i <interface>`
3455 command.

3456

3457 For instance: `arpwatch -i eth1` where eth1 is monitoring port.

- 3458 • The Security Onion server already has an inbuilt decoder and a rules file for **arpwatch**
3459 located at `/var/ossec/etc/arpwatch_decoder.xml` and
3460 `/var/ossec/rules/arpwatch_rules.xml`. A new rule was added to our **local_rules.xml** file as
3461 shown below which references this inbuilt decoder and alerts when a new/bogon device is
3462 plugged into our network.


```

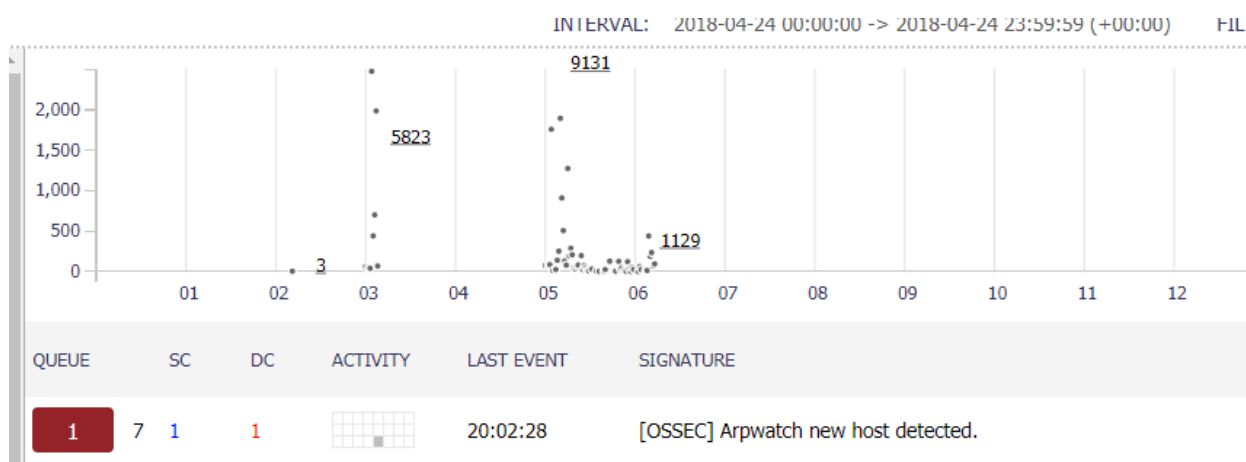
<rule id="110003" level="7">
  <if_sid>7200</if_sid>
  <match>new|logon</match>
  <description>Arpwatch new host detected. </description>
  <group>new_host,</group>
</rule>

```

3463

- 3464 • Once done, restart the OSSEC server upon adding any local rules.
- 3465 • The below image shows a sample alert in Squert Web Interface, when a new system was
- 3466 physically connected to the network:

3467



3468

3469

3470

3471 **Note:** This package relies on ARP cache of the local system to detect new devices. It is

3472 possible for an intruder to spoof this system's mac-address or poison arp-cache and remain

3473 un-noticed.

3474 Lessons Learned:

- 3475 • The full packet capture feature in Security Onion can fill up the hard disk space quickly
- 3476 depending on the amount of network traffic in your environment. Ensure to plan and allocate
- 3477 substantial amount of storage for the server along with configuring the necessary data
- 3478 retention options in securityonion.conf file. Trimming your pcaps can allow you to store pcap
- 3479 for longer periods of time. For an example, please
- 3480 see [https://www.netresec.com/?page=Blog&month=2017-12&post=Don%27t-Delete-PCAP-](https://www.netresec.com/?page=Blog&month=2017-12&post=Don%27t-Delete-PCAP-Files---Trim-Them)
- 3481 [Files---Trim-Them](https://www.netresec.com/?page=Blog&month=2017-12&post=Don%27t-Delete-PCAP-Files---Trim-Them)

3482

3483

3484 4.7.5 Highlighted Performance Impacts

3485 No performance measurement experiments were performed for the use of Security Onion due to
3486 its installation location and how it was used (i.e., the software performed passive analysis of
3487 network traffic external to the manufacturing system).

3488 4.7.6 Link to Entire Performance Measurement Data Set

3489 N/A

3490

3491 **4.8 Cisco AnyConnect VPN**

3492 **4.8.1 Technical Solution Overview**

3493 The AnyConnect Secure Mobility Client is a modular endpoint software product by Cisco. It not
3494 only provides VPN access through Secure Sockets Layer (SSL) and IPsec IKEv2 but also offers
3495 enhanced security through various built-in modules. These modules provide services such as
3496 compliance through the VPN with ASA or through wired, wireless, and VPN with Cisco Identity
3497 Services Engine (ISE), web security alongside Cisco Cloud Web Security, network visibility into
3498 endpoint flows within Stealth watch, or off-network roaming protection with Cisco Umbrella.
3499 AnyConnect clients are available across a broad set of platforms, including Windows, macOS,
3500 Linux, iOS, Android, Windows Phone/Mobile, BlackBerry, and ChromeOS.¹⁸

3501 Points to consider

- 3502 • Provides additional security in the form of Web Security and DNS-Based security.
- 3503 • OS Platform independent: The VPN clients are supported on Windows, Mac and Linux.
- 3504 • Administrators can control which networks or resources for endpoints to connect. It provides
3505 an IEEE 802.1X supplicant that can be provisioned as part of authentication, authorization,
3506 and accounting (AAA) capabilities along with some unique encryption technologies such as
3507 MACsec IEEE 802.1AE.
- 3508 • Cisco Proprietary Product. This replaces the earlier free product called AnyConnect VPN
3509 client. You must either have a Cisco Adaptive Security appliance(ASA) Firewall or Cisco
3510 Firepower Services Appliance and an active AnyConnect Secure Mobility Client license.

3511 **4.8.2 Technical Capabilities Provided by Solution**

3512 Cisco AnyConnect VPN provides components of the following Technical Capabilities described
3513 in Section 6 of Volume 1:

- 3514 • Secure Remote Access
- 3515 • Data Replication

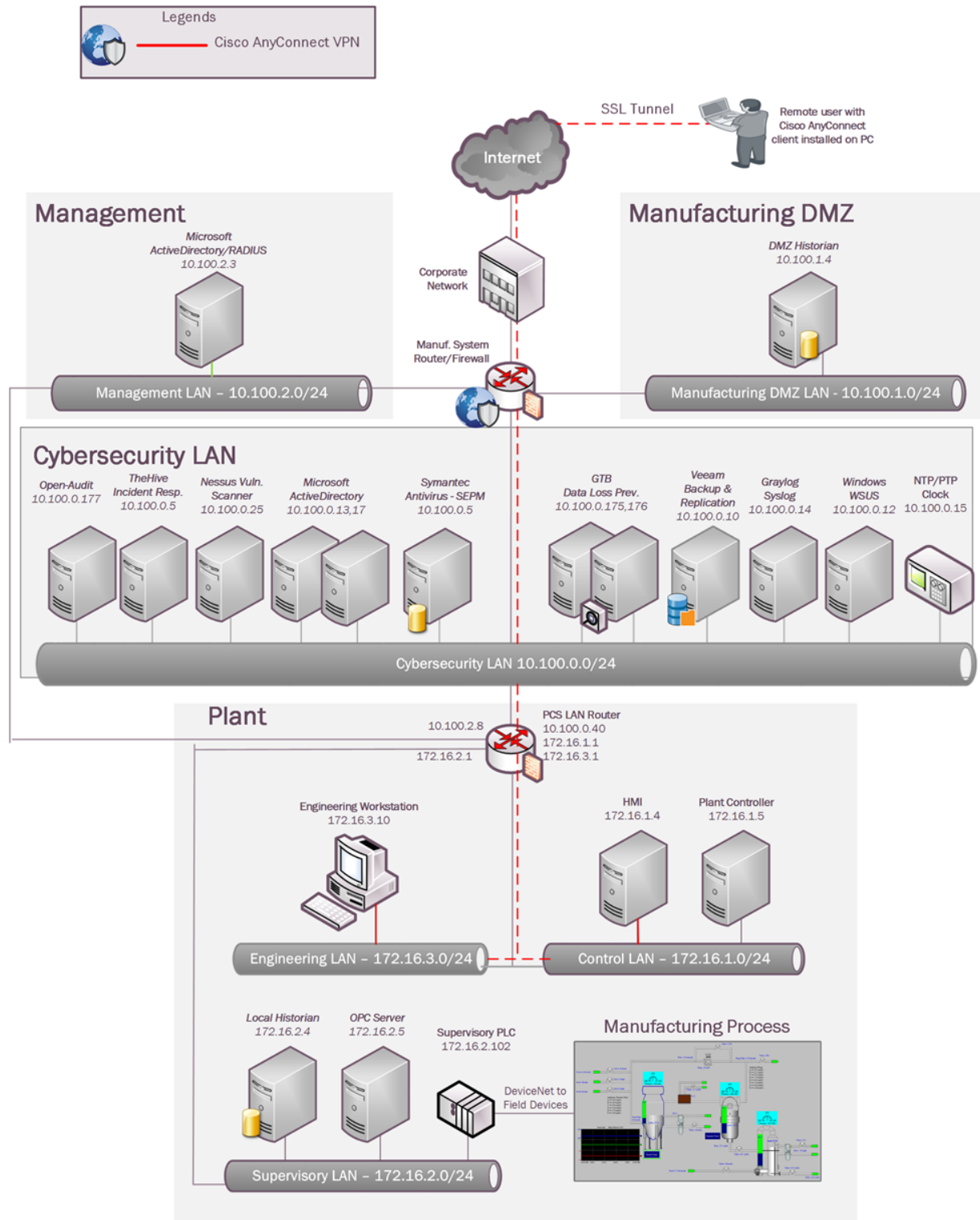
3516 **4.8.3 Subcategories Addressed by Implementing Solution**

3517 PR.MA-2

3518

¹⁸ Cisco AnyConnect VPN https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/at_a_glance_c45-578609.pdf

4.8.4 Architecture Map of Where Solution was Implemented



4.8.5 Installation Instructions and Configurations

Secure Remote Access was implemented for PCS system using the Cisco AnyConnect VPN. The AnyConnect VPN was configured on the top-level firewall - Cisco ASA in the Cybersecurity LAN network.

Overview

The following devices are involved in this setup

Device	Function	OS / Version
Cisco ASA 5512 with Firepower services	Firewall	FTD 6.2.3
AnyConnect VPN	VPN Client software	4.7.01076
A Server in the Management LAN	Active Directory, Radius	Windows 2012 R2

Setup of Radius server

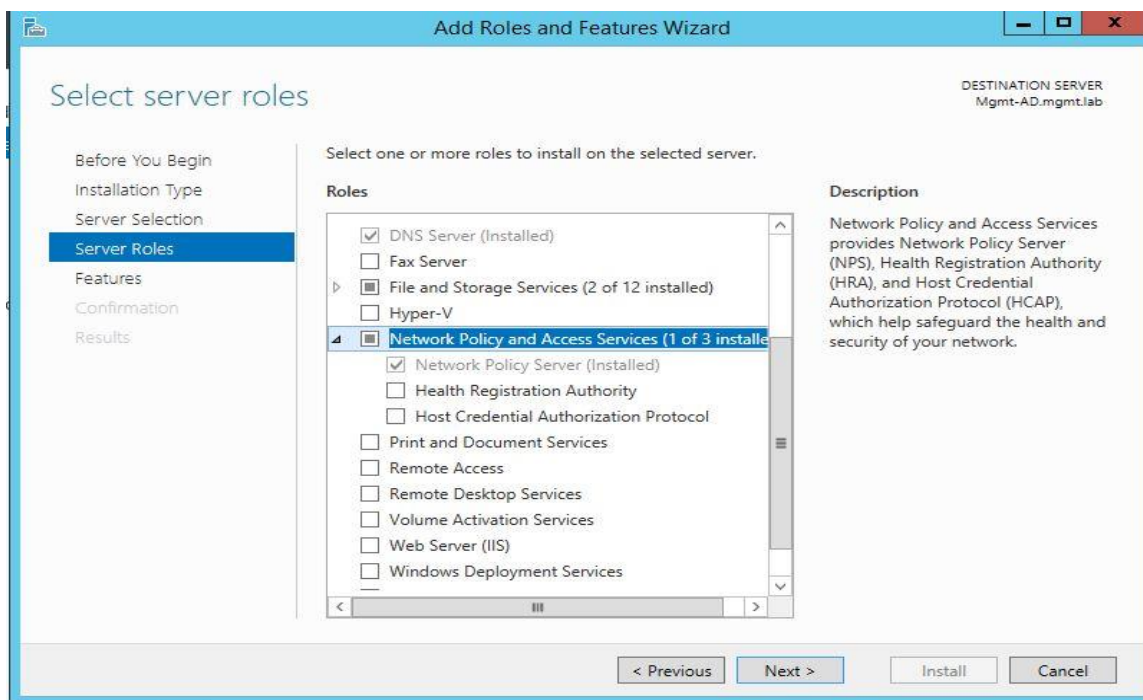
A Windows server was setup in the Management LAN for hosting Active Directory and Radius Authentication services for VPN clients.

Configuration Steps:

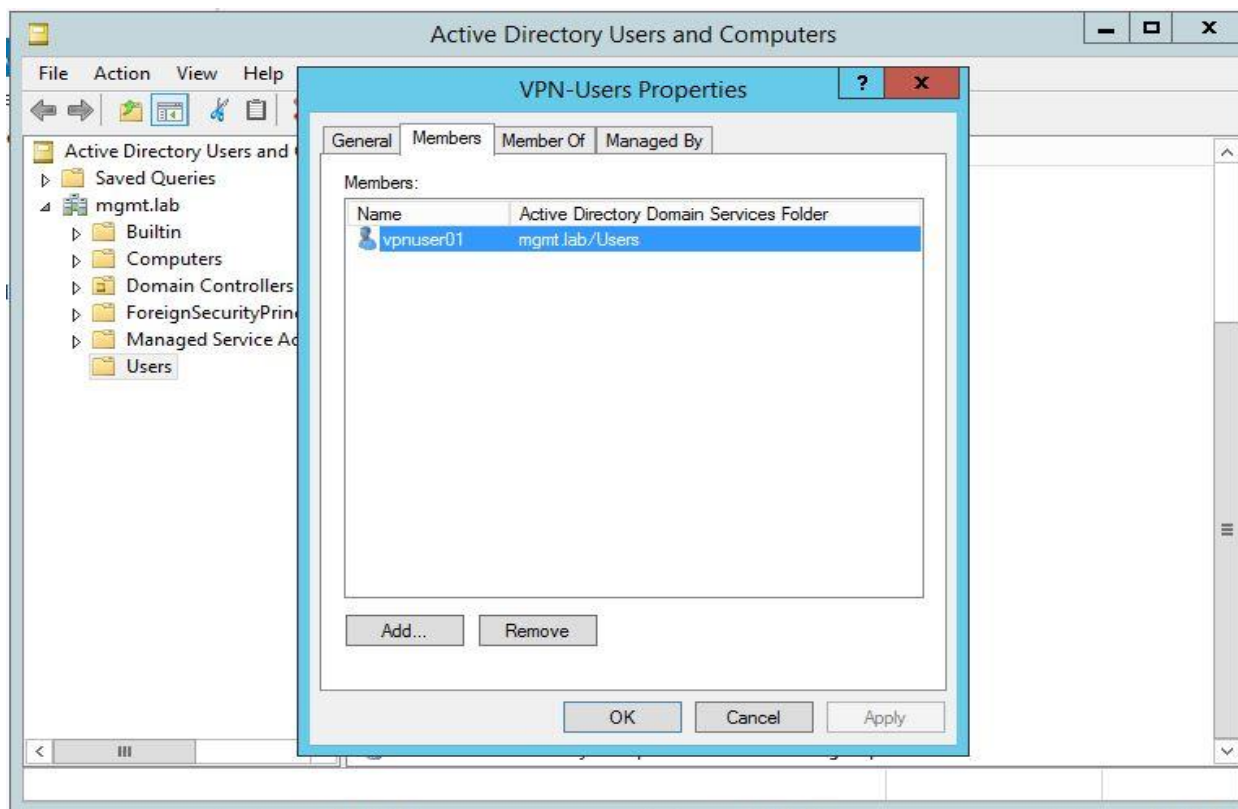
Install the following roles on the server. Different servers can be used to separate out the Roles and for redundancy.

- Active Directory Services
- DNS Server
- Network Policy Server

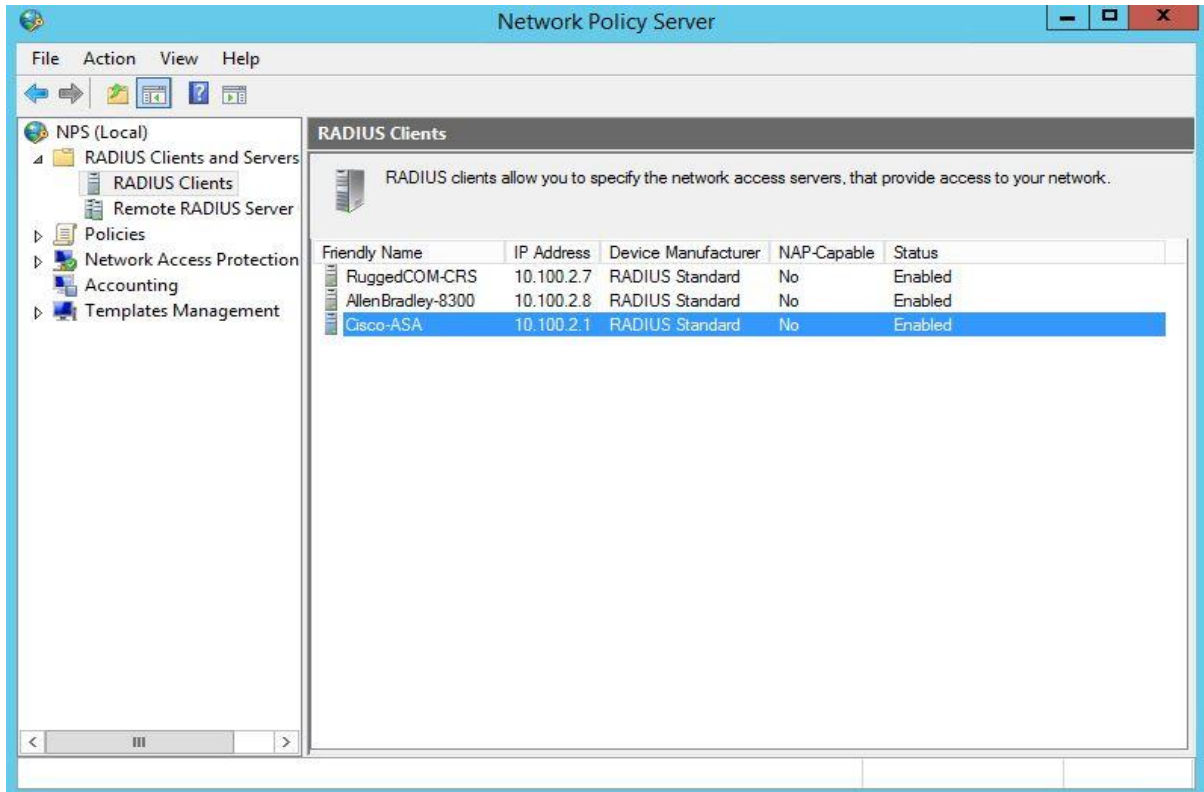
- All the above 3 roles can be installed using Windows Server Manager >> Add Roles and Features wizard. Below image shows the role to be installed for Network Policy server



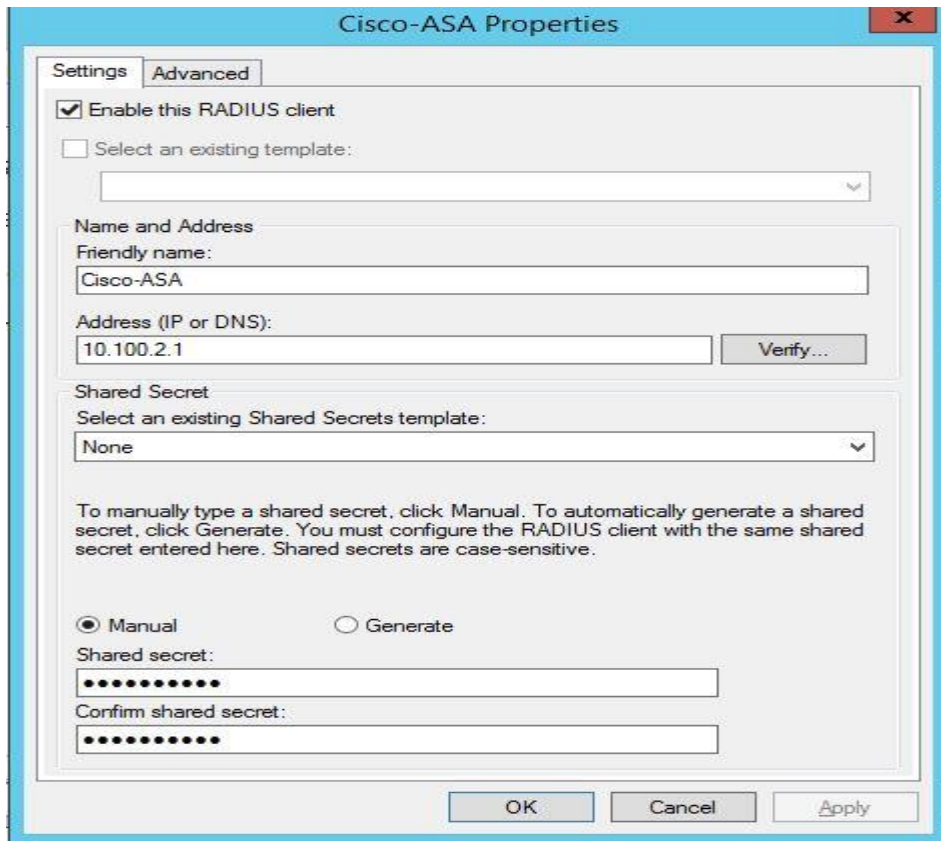
- Create a security group in Active Directory for VPN users and add those users to this group requiring VPN Access. A group called **VPN-users** was created in our AD server and a user **vpnuser01** was added to this group.



- Open up the “**Network Policy Server**” console, click on **Radius Clients** and create a client for your firewall device. Below image shows a Radius client created for our Cisco-ASA firewall.



- While creating the Client, enter the IP address of the Interface on the ASA. This is typically the Default Gateway of the subnet where the AD/Radius server is in. Enter a strong password for Shared secret. This secret will later be used during the setup of a AAA group on the Firewall.
Hit **OK** when done.



The image shows a screenshot of the 'Cisco-ASA Properties' dialog box, specifically the 'Advanced' tab. The dialog has a title bar with 'Cisco-ASA Properties' and a close button. Inside, there are two tabs: 'Settings' and 'Advanced'. The 'Advanced' tab is selected. The main content area is divided into several sections. At the top, there is a checkbox labeled 'Enable this RADIUS client' which is checked. Below it is a checkbox labeled 'Select an existing template:' which is unchecked, followed by a dropdown menu. The next section is titled 'Name and Address'. It contains a text field for 'Friendly name:' with the value 'Cisco-ASA'. Below that is a text field for 'Address (IP or DNS):' with the value '10.100.2.1' and a 'Verify...' button. The next section is titled 'Shared Secret'. It contains a dropdown menu for 'Select an existing Shared Secrets template:' with the value 'None'. Below this is a paragraph of text: 'To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.' Below the text are two radio buttons: 'Manual' (selected) and 'Generate'. Below the radio buttons are two text fields: 'Shared secret:' and 'Confirm shared secret:', both containing masked characters (dots). At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

Cisco-ASA Properties

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:

Cisco-ASA

Address (IP or DNS):

10.100.2.1 Verify...

Shared Secret

Select an existing Shared Secrets template:

None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

Shared secret:

Confirm shared secret:

OK Cancel Apply

- Under **Policies** >> Click on **Network Policies**. Create a Network Policy here corresponding to the Radius client setup earlier. Below image shows network policy created for the Cisco-ASA client. Ensure the policy is enabled.

Cisco-ASA Access Properties

Overview | Conditions | Constraints | Settings

Policy name:

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☒ Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

☒ Grant access. Grant access if the connection request matches this policy.

☐ Deny access. Deny access if the connection request matches this policy.

☐ Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

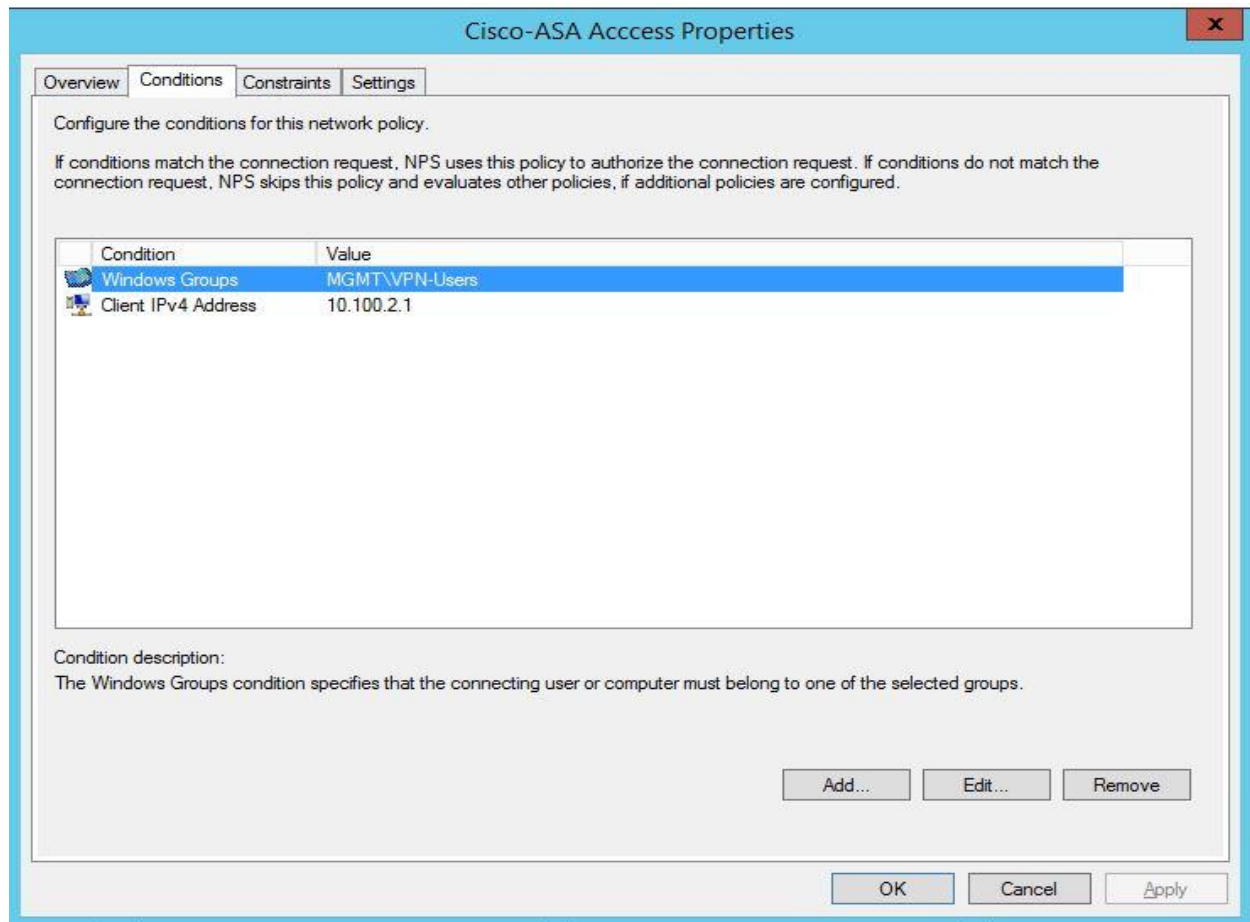
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:

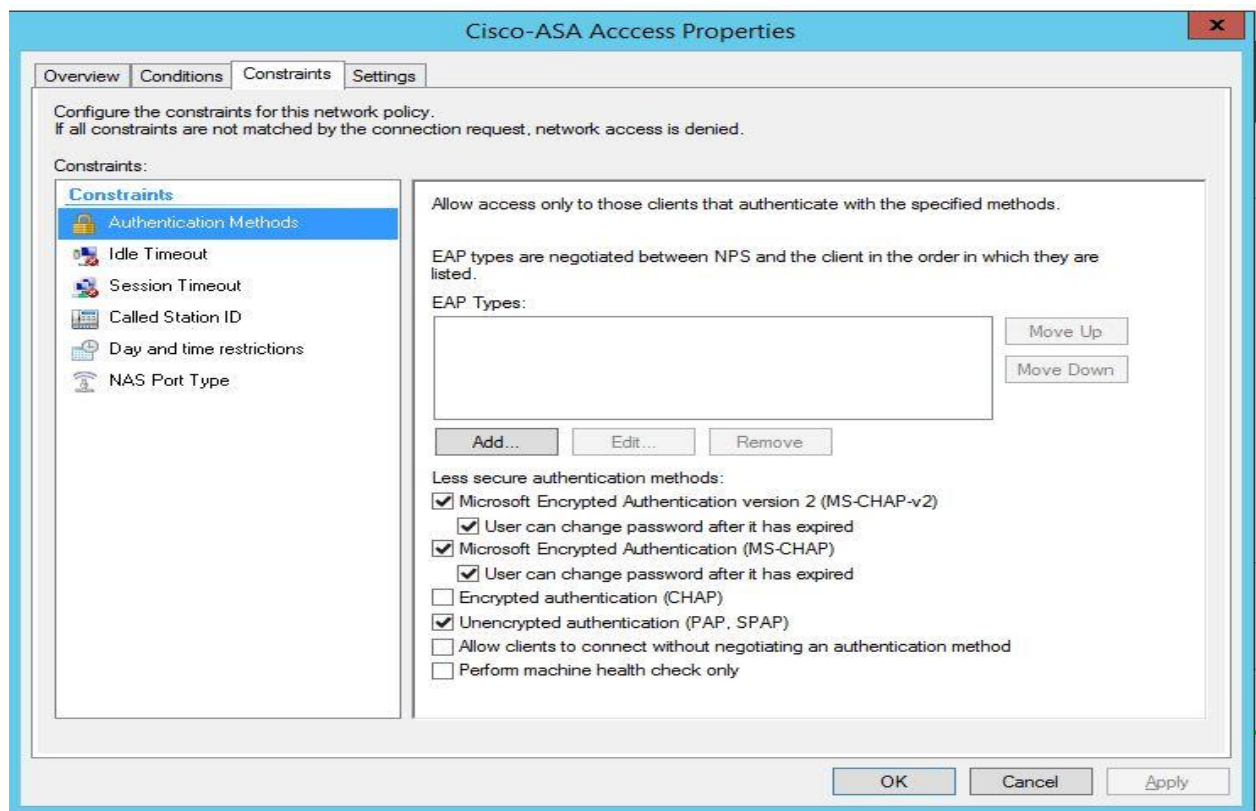
☐ Vendor specific:

OK Cancel Apply

- 3595 • Under **Conditions** tab, click **ADD** to add the following two conditions. More conditions can
3596 be added as per your requirement.
- 3597 ○ **VPN-Users** security group created earlier.
 - 3598 ○ **Client IPv4 Address:** IP address of the Radius client created earlier.

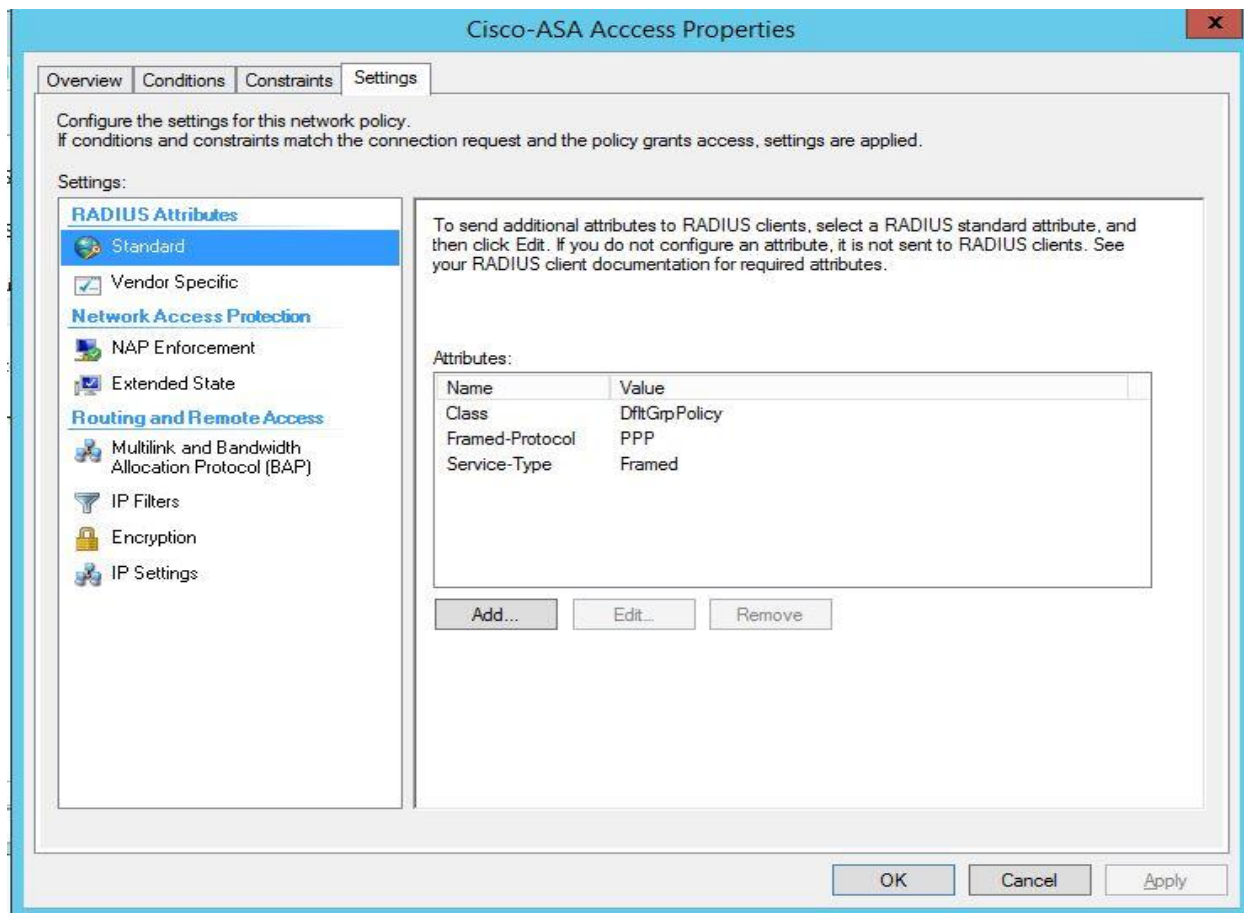


- Under **Authentication Methods**, select the methods shown below. This is as per Cisco documentation.¹⁹



¹⁹ Cisco ASA VPN User Authentication: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/117641-config-asa-00.html>

- Under **Settings >> Radius Attributes >> Standard** set the following attributes
 - Framed Protocol= **PPP**
 - Service-Type=**Framed**
 - Class = <**Name of group policy**>. This policy is configured in the Firewall for VPN



VPN Setup on Cisco-ASA firewall

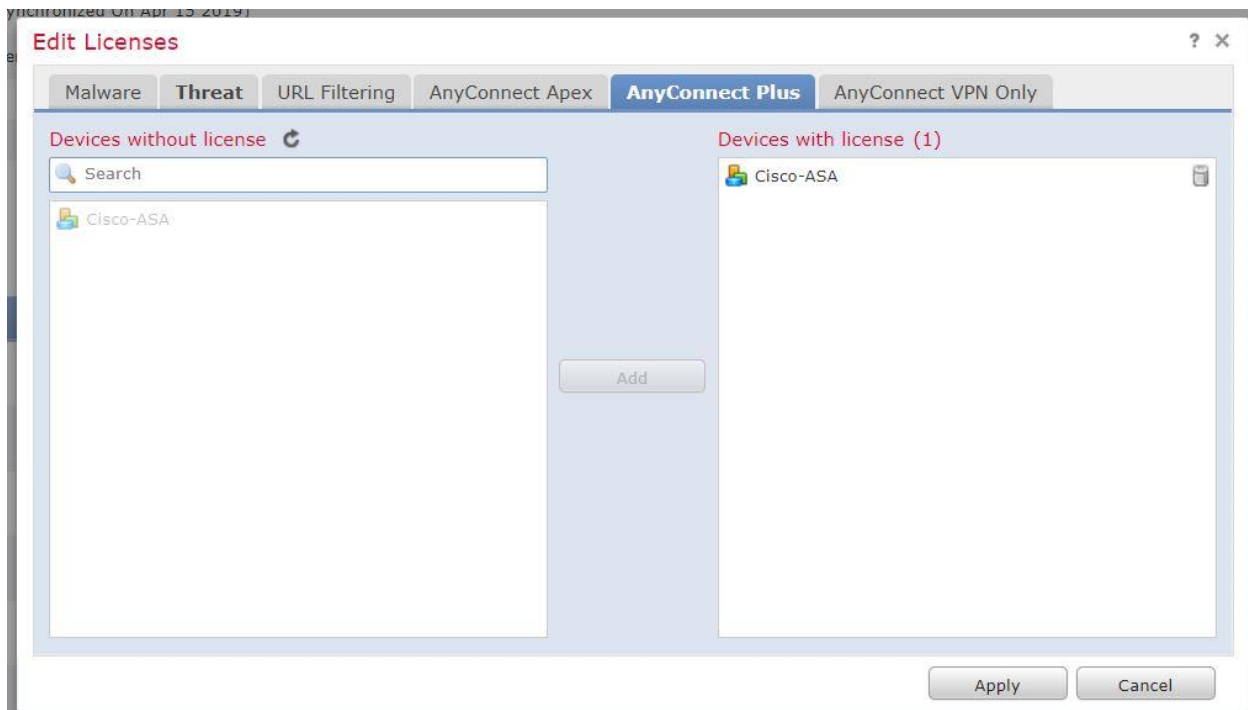
Below are the high-level steps for configuring Remote Access VPN in the FMC (Firepower Management Console)

- Go to **Licenses >> Smart Licenses >>** Verify if either **AnyConnect Plus** or **AnyConnect VPN** license has been enabled (if not already).

To enable license (assuming an AnyConnect license has been procured and tied to your Cisco smart account), Click **Edit Licenses >>** Select the corresponding firewall device from the left side window “**Devices without license**” and move it to the right side under “**Devices with license**”. Hit **Apply**.

3627

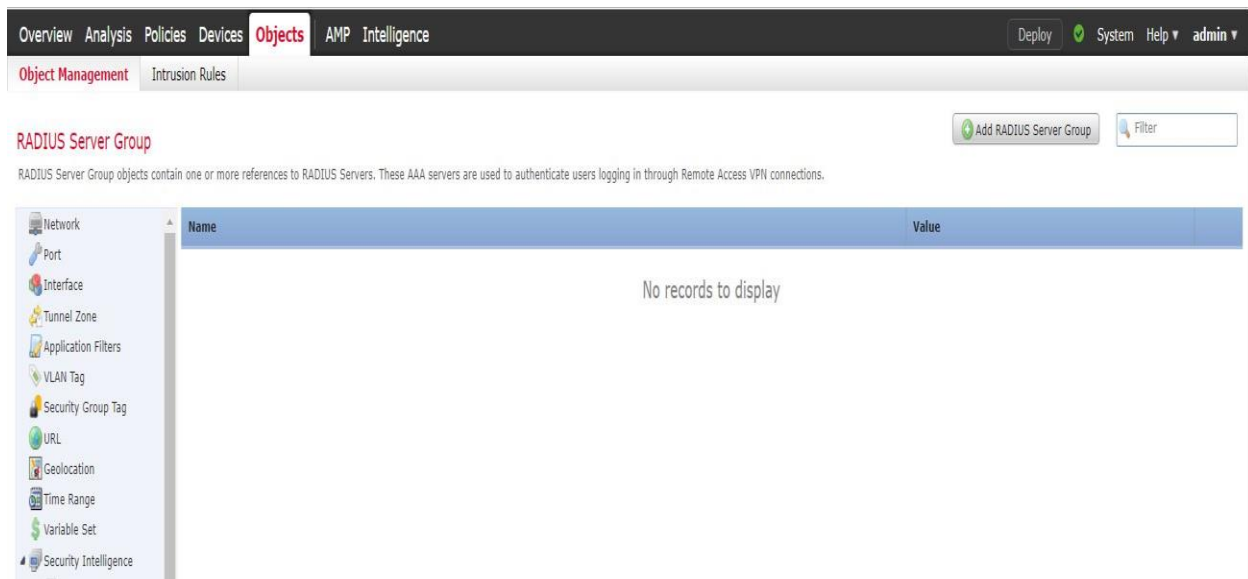
3628



3629

- Go to **Objects menu >> Object Management >> Radius Server Group >> Add Radius Server Group** (if not already configured)

3631



3632

3633

- 3634 • Under **Add Radius Server Group** >> Enter a Name and Description >> Under **Radius**
3635 **Servers** in the bottom menu >> Click on + to add one.
3636 • Under **New Radius Server** wizard >> Enter the IP address of the Radius Server. Shared
3637 Secret. Hit Save.

The screenshot shows a web-based configuration interface. The background window is titled "Add RADIUS Server Group" and contains fields for "Name:*" (Mgmt-Radius) and "Description:" (Radius server on Mgmt AD). Overlaid on this is a "New RADIUS Server" dialog box. The dialog box contains the following fields and options:

- IP Address/Hostname:* 10.100.2.3 (with a note: "Configure DNS at Threat Defense Platform Settings to resolve hostname")
- Authentication Port:* 1812 (range: 1-65535)
- Key:* (masked with dots)
- Confirm Key:* (masked with dots)
- Accounting Port: 1813 (range: 1-65535)
- Timeout: 10 (range: 1-300) Seconds
- Connect using: ☒ Routing ☐ Specific Interface (with an info icon)
- Default: Diagnostic Interface (dropdown menu with a green plus icon)
- Redirect ACL: (empty dropdown menu with a green plus icon)

At the bottom of the dialog box are "Save" and "Cancel" buttons.

3638

3639

- Next, go to **Devices** menu >> **VPN** >> **Remote Access** >> **Wizard** >> **Add a new Configuration.**

Step 1: Policy Assignment

- Define a **Name, Description.**
- Select a protocol (SSL, IPSec-IKEv2). It is possible to select both.
- Move the appropriate firewall device under “**Available Devices**” (left-side) to “**Selected Devices**” right-side window

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:* AnyconnectRemoteAccessVPN

Description:

VPN Protocols: ☒ SSL ☐ IPsec-IKEv2

Targeted Devices: **Available Devices** **Selected Devices**

Search

Cisco-ASA

Add

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure [Realm](#) or [RADIUS Server Group](#) to authenticate VPN clients.

AnyConnect Client Package

Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

3651 Step 2: Connection Profile

- 3652
- Choose Authentication Method – For instance AAA.

The screenshot shows the 'Remote Access VPN Policy Wizard' in a web interface. The navigation bar at the top includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Below the navigation bar, the wizard title 'Remote Access VPN Policy Wizard' is displayed. The progress bar shows five steps: 1 Policy Assignment, 2 Connection Profile (current), 3 AnyConnect, 4 Access & Certificate, and 5 Summary.

Connection Profile Name: AnyconnectRemoteAccessVPN
This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):
Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: AAA Only

Authentication Server: Mgmt-Radius (Realm or RADIUS)

Authorization Server: Use same authentication server (RADIUS)

Accounting Server: (RADIUS)

Client Address Assignment:
Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

☐ Use AAA Server (RADIUS only)

☐ Use DHCP Servers

☒ Use IP Address Pools

IPv4 Address Pools: VPN-Pool

IPv6 Address Pools:

Group Policy:
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy: DfltGrpPolicy (Edit Group Policy)

Buttons: Back, Next, Cancel

- Under **Authentication Server**, select the Radius Server configured earlier under.
- Select “**Use IP Address Pool**”, click to Create a New IPv4 Address Pool. Below image our **VPN-Pool**

Add IPv4 Pool

Name:* VPN-Pool

IPv4 Address Range:* 192.168.100.10-192.168.100.20
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask: 255.255.255.0

Description:

Allow Overrides: ☒

! Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Override (0)

Save Cancel

Under **Group Policy** >> **Edit the Default Group Policy** or Create a new one as per your requirement. This is the policy name to be referenced on the Radius server setup on Windows.

The following changes were put in our Default Group Policy

- Under **General** >> VPN Protocols >> **SSL**
- Under **General**>> **Banner** >> Enter a custom welcome message
- Under **General** >> Split Tunneling >> Allow all traffic over tunnel (Split tunnel was disabled)

The screenshot shows the 'Edit Group Policy' window with the following details:

- Title Bar:** Edit Group Policy
- Name:** DfitGrpPolicy
- Description:** (Empty field)
- Tabs:** General (selected), AnyConnect, Advanced
- Left Navigation Panel:**
 - VPN Protocols
 - IP Address Pools
 - Banner
 - DNS/WINS
 - Split Tunneling (highlighted)
- Main Content Area (General tab):**
 - IPv4 Split Tunneling: Allow all traffic over tunnel
 - IPv6 Split Tunneling: Allow all traffic over tunnel
 - Split Tunnel Network List Type: ☒ Standard Access List ☐ Extended Access List
 - Standard Access List: (Empty list box with a green plus icon)
 - DNS Request Split Tunneling
 - DNS Requests: Send DNS requests as per split tunnel policy
 - Domain List: (Empty text area)

- 3676 ○ Under AnyConnect, Create a new Client Profile (if not already)

The screenshot shows the 'Edit Group Policy' window with the 'AnyConnect' tab selected. The 'Name' field is 'DfltGrpPolicy' and the 'Description' field is empty. The left sidebar shows 'Profiles', 'SSL Settings', and 'Connection Settings'. The main area contains text about AnyConnect profiles and a 'Client Profile' dropdown menu. A link to the 'Cisco Software Download Center' is provided for downloading a standalone profile editor.

3677

- 3678 Under **Advanced** >> **Session Settings** >> Idle Session Timeout was set to 30 minutes

The screenshot shows the 'Edit Group Policy' window with the 'Advanced' tab selected. The 'Name' field is 'DfltGrpPolicy' and the 'Description' field is empty. The left sidebar shows 'Traffic Filter' and 'Session Settings'. The main area displays settings for 'Access Hours' (Unrestricted), 'Simultaneous Login Per User' (3), 'Connection Time' (Max Connection Time: 1 Minutes, Alert Interval: 1 Minutes), and 'Idle Time' (Idle Timeout: 30 Minutes, Alert Interval: 1 Minutes).

3679

3680

3681 Step 3: AnyConnect:

- 3682 • Select the AnyConnect Image for OS Supported (Windows, Linux, MacOS)

Device Management NAT **VPN • Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile **3 AnyConnect** 4 Access & Certificate 5 Summary

AAA

AnyConnect Client Image
The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#). [Show Re-order buttons](#)

Select at least one AnyConnect Client image

AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/> Anyconnect-Win-Image	anyconnect-win-4.7.01076-webdeploy-k9.pkg	Windows
<input type="checkbox"/> Anyconnect-Linux-image	anyconnect-linux64-4.6.04056-webdeploy-k9...	Linux

3683

- 3684 • The Image files can be added manually by clicking on + icon.

AAA

AnyConnect Client Image
The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection

Download AnyConnect Client

Select at least one AnyC

Add AnyConnect File

Name:* Anyconnect-Linux-image

File Name:* anyconnect-linux64-4.6.04056-webdeploy-k9 Browse..

File Type:* AnyConnect Client Image

Description:

Save Cancel

3685

3686

3687 Step 4: Access and Certificate:

- 3688 ○
- Interface group/Security Zone:**
- Select your
- outside**
- interface

Overview Analysis Policies **Devices** Objects AMP Intelligence

Dashboards Reporting Summary

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

AAA

Network Interface for Incoming VPN Access
Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* fake_public_nccoe

☒ Enable DTLS on member interfaces

Device Certificates
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:*

3689

3690

3691

- 3692 ○ **Device Certificates:** Select a Name and Certificate can be imported manually or Click +
3693 to create a Self-signed Certificate. A self-signed certificate was used in our environment.

AAA

Network Interface for Incoming VPN Access
Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* fake_public_nccoe

☒ Enable DTLS on member interfaces

Device Certificates
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* Self-Signed

☒ Enroll the selected certificate object on the target devices

3694

3695

Add Cert Enrollment ? X

Name:* Self-Signed

Description:

CA Information Certificate Parameters Key Revocation

Enrollment Type: Self Signed Certificate ▼

⚠ Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.

Allow Overrides: ☐

Save Cancel

3696

3697

3698 Step 5: Summary:

- 3699 • Review the
- Summary**
- . If all OK, click
- Finish**
- to apply the changes.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN • Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 **Summary**

Connection Alias: AnyconnectRemoteAccessVPN

AAA:

Authentication Method: AAA Only

Authentication Server: Mgmt-Radius

Authorization Server: Mgmt-Radius

Accounting Server: -

Address Assignment:

Address from AAA: -

DHCP Servers: -

Address Pools (IPv4): VPN-Pool

Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images: Anyconnect-Win-Image, Anyconnect-Linux-Image

Interface Objects: fake_public_nccoe

Device Certificates: Self-Signed

Device Identity Certificate Enrollment

Certificate enrollment object 'Self-Signed' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

NAT Exemption

If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.

DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.

Port Configuration

SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#), or other services before deploying the configuration.

Network Interface Configuration

Make sure to add interface from targeted devices to SecurityZone object 'fake_public_nccoe'

Back Finish Cancel

3700

3701 Further Configuration Requirements:

3702 Once the Wizard is completed, the following configuration requirements need to be done for RA

3703 VPN to work on all device targets:

3704 **Access Control Policy:** An ACL rule must be defined to allow VPN traffic on to whichever

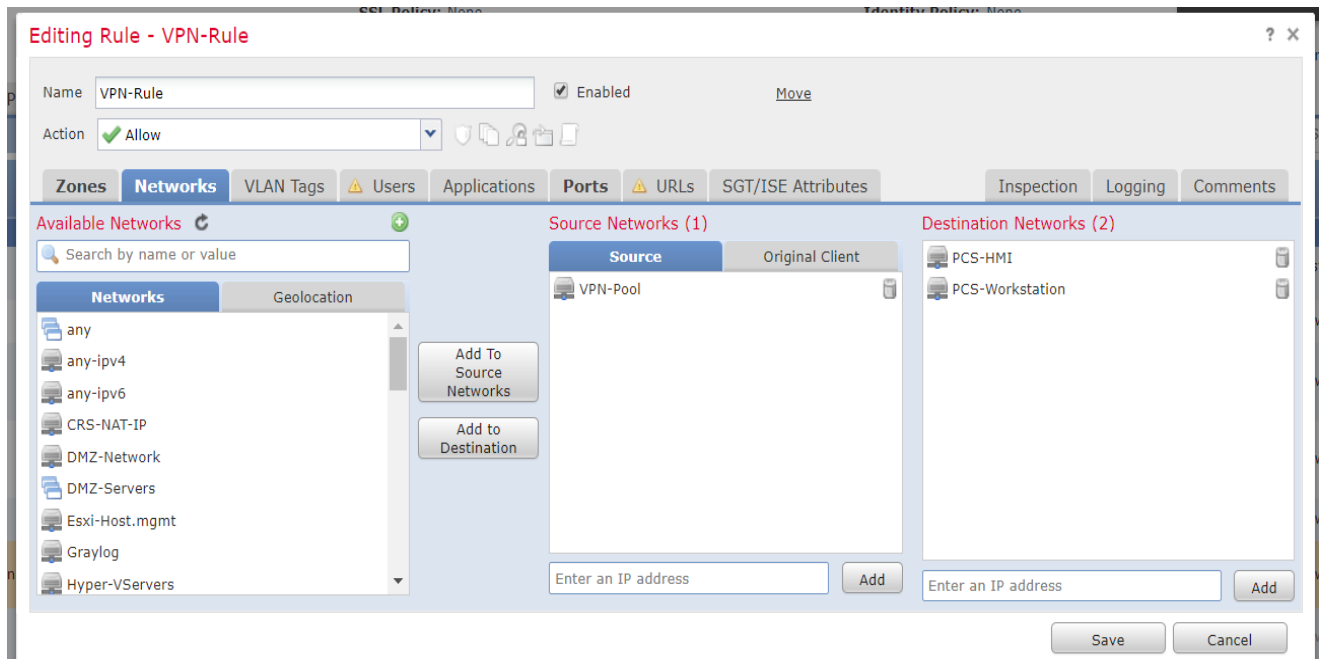
3705 network segments you wish to permit.

3706

3707 The image below shows an ACL configured to allow VPN traffic from outside to only a couple
3708 of internal servers in the Process Control system over Remote Desktop Port 3389.

	Source	Destination	Selection
Zones	Outside	Inside	
Networks	VPN_Pool (Network)	HMI Server (Host) Workstation (Host)	
Ports	Any	3389 TCP	
Action			Allow
Inspection			Enabled. Balanced connectivity over Security.

3709



3710

3711

Editing Rule - VPN-Rule ? X

Name: ☒ Enabled [Move](#)

Action:

Zones **Networks** **VLAN Tags** **Users** **Applications** **Ports** **URLs** **SGT/ISE Attributes** **Inspection** **Logging** **Comments**

Available Ports

- AOL
- Bittorrent
- DNS_over_TCP
- DNS_over_UDP
- FTP
- HTTP
- HTTPS
- IMAP
- LDAP
- NetBIOS-TCP

Selected Source Ports (0)

Selected Destination Ports (1)

- RDP-Windows

Protocol: Port: Protocol: Port:

3712

3713

3714 **Device Certificate:** Associate the certificate created earlier with the Firewall device.

Overview **Analysis** **Policies** **Devices** **Objects** **AMP** **Intelligence** [Deploy](#) **System** [Help](#) **admin**

Device Management **NAT** **VPN** **QoS** **Platform Settings** **FlexConfig** **Certificates**

Name	Domain	Enrollment Type	Status
Cisco-ASA			
Self-Signed			

Add New Certificate ? X

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: Self-Signed

Enrollment Type: Self-Signed

SCEP URL: NA

3715

3716

3717

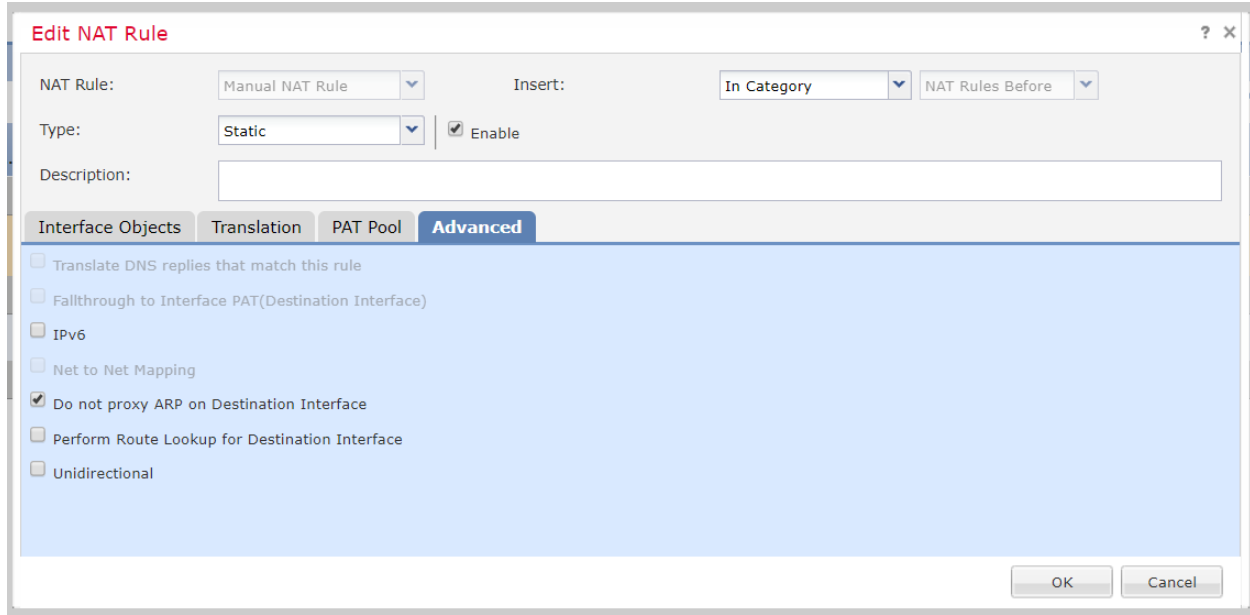
3718 **Create a NAT Exemption rule:** If NAT is enabled on the firewall, you must define a NAT rule
3719 to exempt VPN traffic.

3720 Go to **Devices Menu >> NAT >> Select <NAT Policy> >> Add Rule.**

3721 Below images show a NAT Rule created to exempt VPN Traffic

The screenshot shows the 'Edit NAT Rule' dialog box with the 'Interface Objects' tab selected. The 'NAT Rule' is set to 'Manual NAT Rule', 'Type' is 'Static', and 'Enable' is checked. The 'Description' field is empty. The 'Interface Objects' section shows 'Available Interface Objects' on the left, including 'dmz', 'fake_public_nccoe', 'inside', 'management', and 'outside'. The 'Source Interface Objects (1)' list contains 'inside', and the 'Destination Interface Objects (1)' list contains 'fake_public_nccoe'. 'Add to Source' and 'Add to Destination' buttons are visible between the lists. 'OK' and 'Cancel' buttons are at the bottom right.

The screenshot shows the 'Edit NAT Rule' dialog box with the 'Translation' tab selected. The 'Original Packet' section has 'Original Source:*' set to 'PCS-Network', 'Original Destination' set to 'Address', and 'VPN-Pool' selected below it. The 'Translated Packet' section has 'Translated Source' set to 'Address', 'Translated Destination' set to 'PCS-Network', and 'VPN-Pool' selected below it. All fields have a green plus icon to the right. 'OK' and 'Cancel' buttons are at the bottom right.



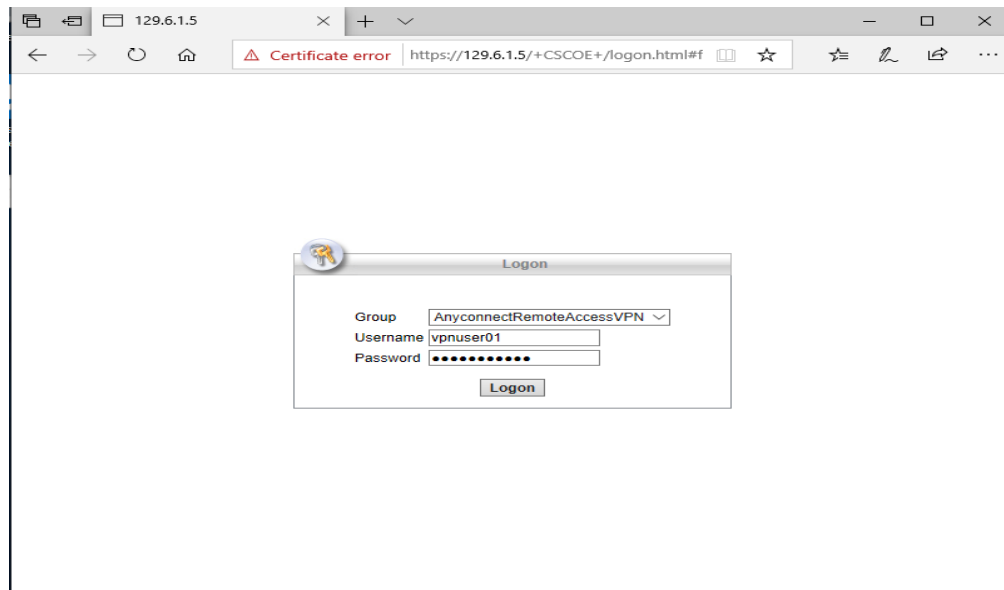
3726

3727

3728 Client Connection:

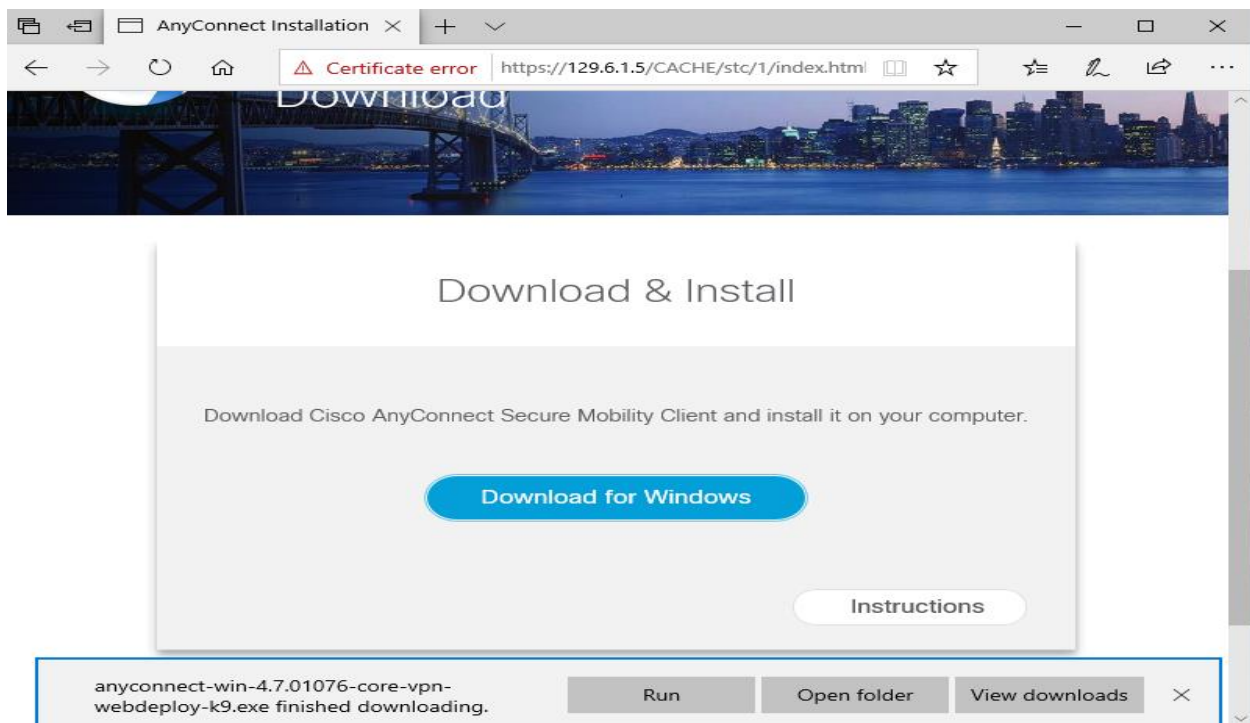
3729 Clients can use a web browser to connect to the Outside interface of the device. Once they login,
 3730 the AnyConnect image is automatically downloaded or updated. After that, clients can connect
 3731 using the AnyConnect software installed on their device, which already has the AnyConnect
 3732 XML profile with all the parameters for the RA VPN connection.

- 3733 • Accessing the outside interface should give a similar page as shown below. Enter the Active
 3734 Directory user credentials created earlier to Logon.



3735

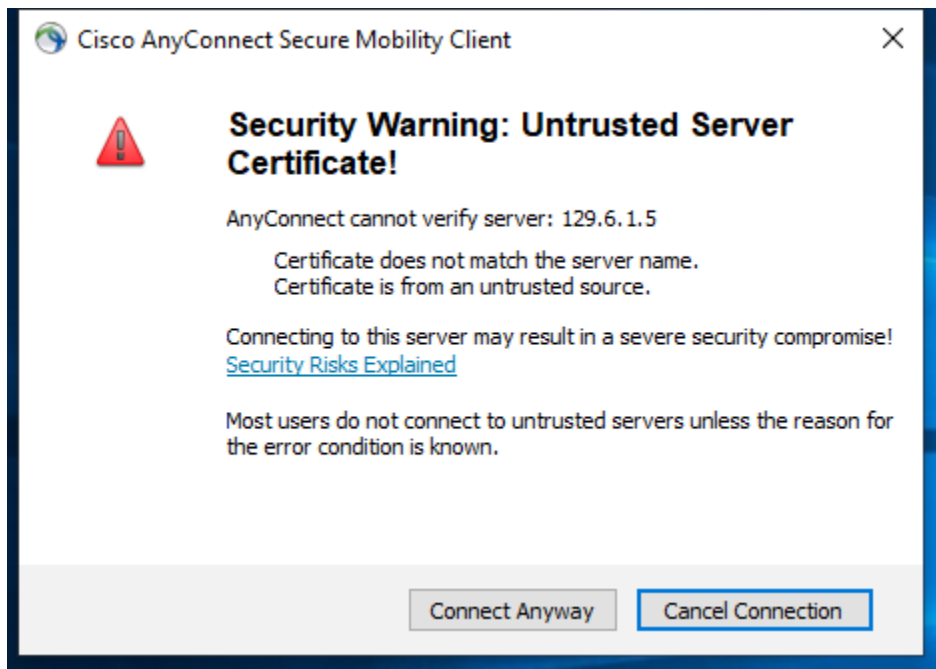
- 3736
- Download the Client software and Install it.



3737

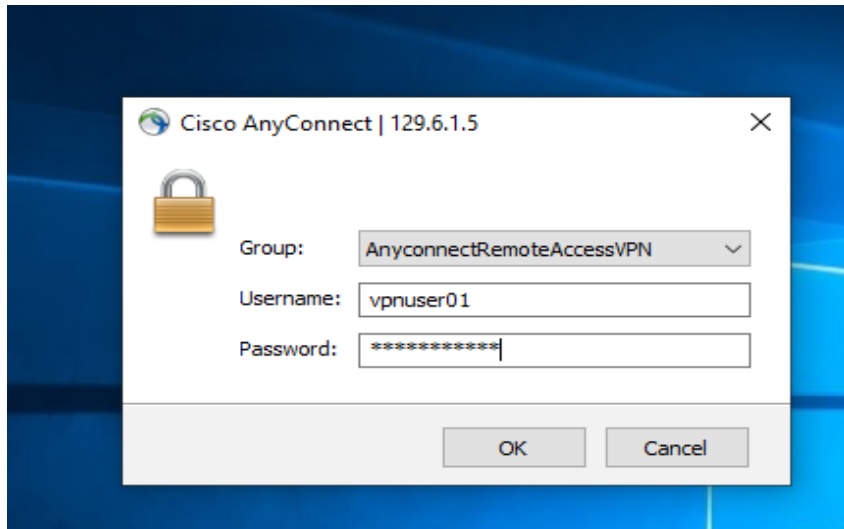
3738

- 3739
- If using a self-signed certificate as in our case, you will be presented with this warning. Hit
- 3740 **Connect Anyway**

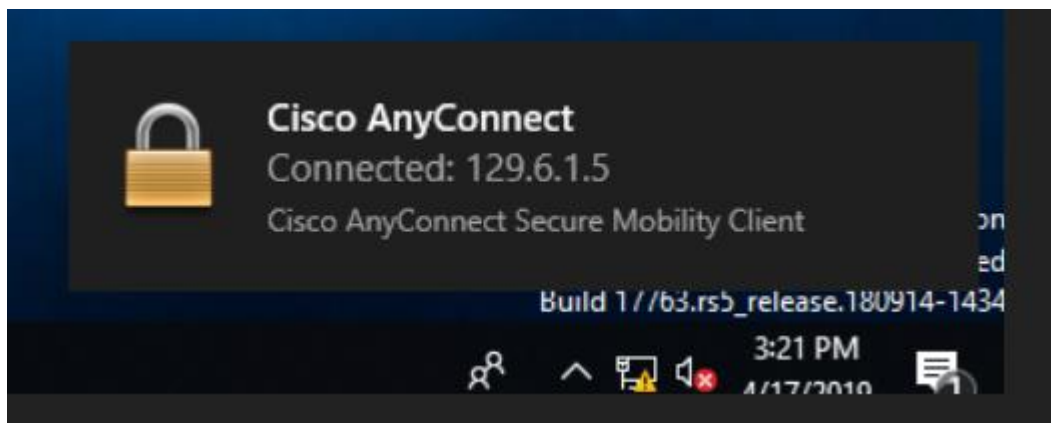


3741

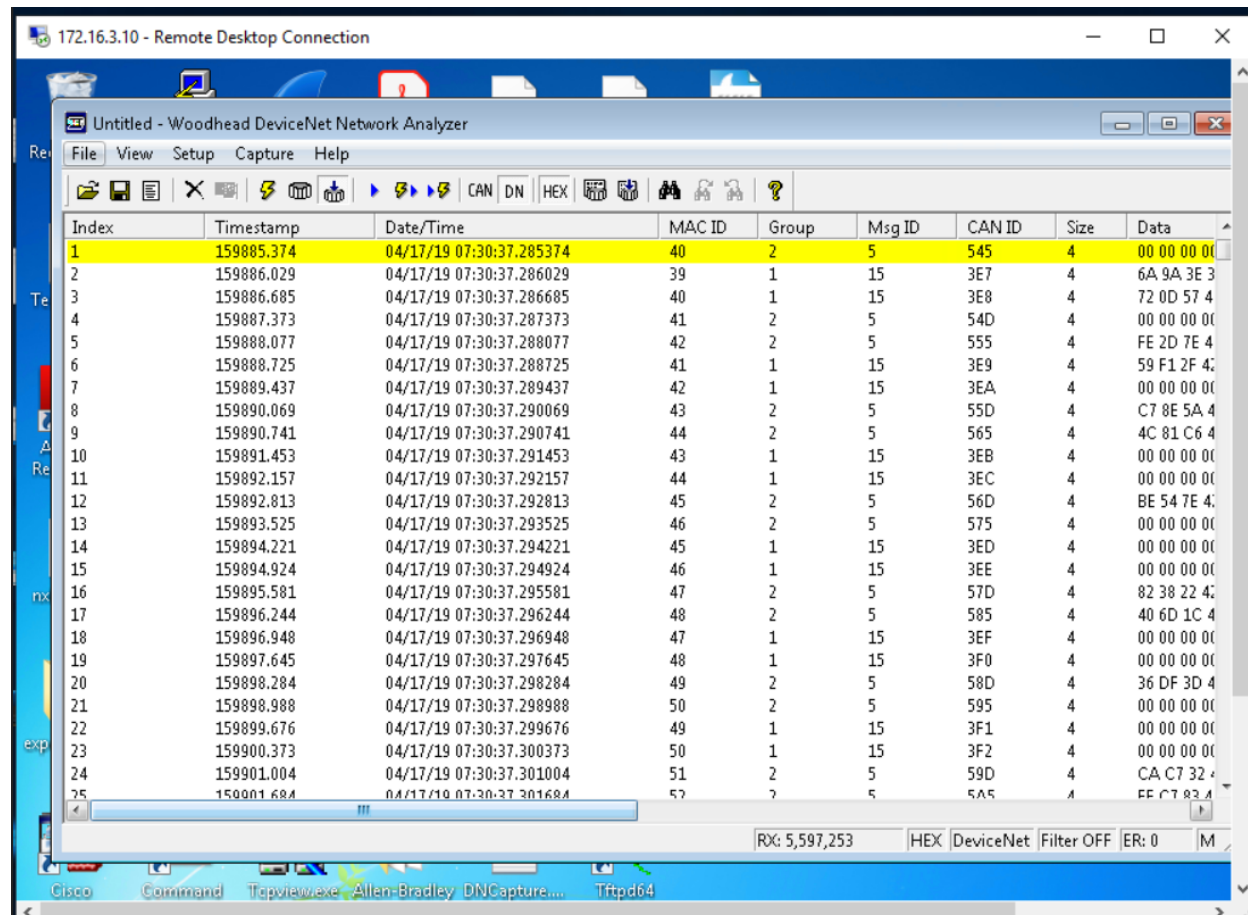
- Enter the AD user credentials



- When connected, a pop-up message appears showing the Client as Connected.



- Upon establishing the connection, the two servers in Process Control System whitelisted earlier in the ACL Rule were accessed using RDP to perform Remote Maintenance.



172.16.3.10 - Remote Desktop Connection

Untitled - Woodhead DeviceNet Network Analyzer

Index	Timestamp	Date/Time	MAC ID	Group	Msg ID	CAN ID	Size	Data
1	159885.374	04/17/19 07:30:37.285374	40	2	5	545	4	00 00 00 00
2	159886.029	04/17/19 07:30:37.286029	39	1	15	3E7	4	6A 9A 3E 3
3	159886.685	04/17/19 07:30:37.286685	40	1	15	3E8	4	72 0D 57 4
4	159887.373	04/17/19 07:30:37.287373	41	2	5	54D	4	00 00 00 00
5	159888.077	04/17/19 07:30:37.288077	42	2	5	555	4	FE 2D 7E 4
6	159888.725	04/17/19 07:30:37.288725	41	1	15	3E9	4	59 F1 2F 4
7	159889.437	04/17/19 07:30:37.289437	42	1	15	3EA	4	00 00 00 00
8	159890.069	04/17/19 07:30:37.290069	43	2	5	55D	4	C7 8E 5A 4
9	159890.741	04/17/19 07:30:37.290741	44	2	5	565	4	4C 81 C6 4
10	159891.453	04/17/19 07:30:37.291453	43	1	15	3EB	4	00 00 00 00
11	159892.157	04/17/19 07:30:37.292157	44	1	15	3EC	4	00 00 00 00
12	159892.813	04/17/19 07:30:37.292813	45	2	5	56D	4	BE 54 7E 4
13	159893.525	04/17/19 07:30:37.293525	46	2	5	575	4	00 00 00 00
14	159894.221	04/17/19 07:30:37.294221	45	1	15	3ED	4	00 00 00 00
15	159894.924	04/17/19 07:30:37.294924	46	1	15	3EE	4	00 00 00 00
16	159895.581	04/17/19 07:30:37.295581	47	2	5	57D	4	82 38 22 4
17	159896.244	04/17/19 07:30:37.296244	48	2	5	585	4	40 6D 1C 4
18	159896.948	04/17/19 07:30:37.296948	47	1	15	3EF	4	00 00 00 00
19	159897.645	04/17/19 07:30:37.297645	48	1	15	3F0	4	00 00 00 00
20	159898.284	04/17/19 07:30:37.298284	49	2	5	58D	4	36 DF 3D 4
21	159898.988	04/17/19 07:30:37.298988	50	2	5	595	4	00 00 00 00
22	159899.676	04/17/19 07:30:37.299676	49	1	15	3F1	4	00 00 00 00
23	159900.373	04/17/19 07:30:37.300373	50	1	15	3F2	4	00 00 00 00
24	159901.004	04/17/19 07:30:37.301004	51	2	5	59D	4	CA C7 32 4
25	159901.684	04/17/19 07:30:37.301684	52	2	5	5A5	4	FF C7 83 4

RX: 5,597,253 HEX DeviceNet Filter OFF ER: 0 M

Taskbar: Cisco, Command, Topview.exe, Allen-Bradley DNCapture..., Tftpd64

Session Termination

To terminate a VPN Session, log on to the Cisco FMC Web interface, go to **Analysis >> Users >> Active Sessions**. Select the **session** and click **Logout**

The screenshot shows the Cisco FMC Web interface. The top navigation bar includes 'Overview', 'Analysis' (selected), 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Below this, a sub-navigation bar shows 'Context Explorer', 'Connections', 'Intrusions', 'Files', 'Hosts', 'Users > Active Sessions' (selected), 'Correlation', 'Advanced', and 'Search'. The main content area is titled 'Active Sessions' and includes a link to 'Table View of Active Sessions'. A search bar is present. Below the search bar is a table with columns: 'Login Time', 'Last Seen', 'User', 'Authentication Type', 'Current IP', and 'Realm'. A single row is visible with the following data: '2019-04-19 15:25:16', '2019-04-19 15:25:16', 'Discovered Identities\vpnuser01 (LDAP)', 'VPN Authentication', '192.168.100.10', and 'Discovered Identity'. A 'Logout' dialog box is overlaid on the table, containing a question mark icon and the text: 'If you have selected VPN sessions, the users will be logged out of VPN. Other sessions will be removed from the active sessions list.' The dialog has 'Continue' and 'Cancel' buttons.

References:

[1] Cisco AnyConnect VPN

https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/at_a_glance_c45-578609.pdf

[2] Cisco ASA VPN User Authentication:

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/117641-config-asa-00.html>

4.8.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Cisco AnyConnect VPN tool while the manufacturing system was operational:

Experiment PL012.1- VPN connection from testbed LAN

In this experiment, a remote user was accessing the HMI from a remote computer through the VPN connection. A remote computer was first connected to the testbed LAN through the VPN, then used the Remote Desktop to connect to the HMI computer to access the HMI screen.

Although there was slightly increased network traffic between the testbed LAN and the PCS system due the Remote desktop session, there was no significant performance impact observed in the PCS system. The packet round trip time between the HMI and OPC remained mostly constant with and without the VPN connection.

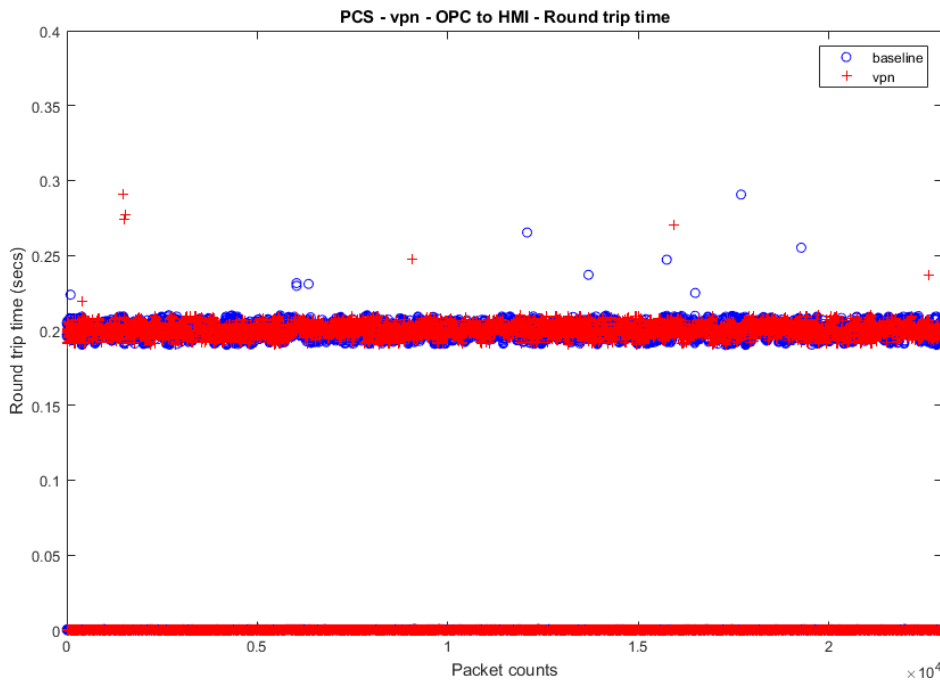


Figure 4-12 Plot of packet round trip time from OPC to HMI computer during the use of VPN connection from a remote computer

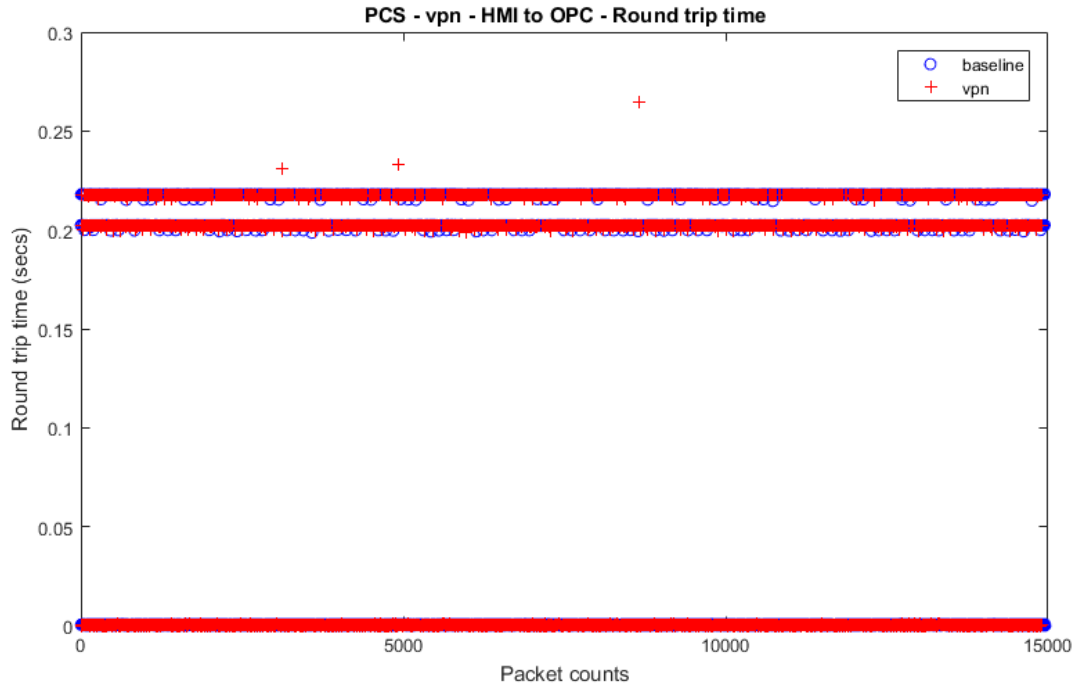
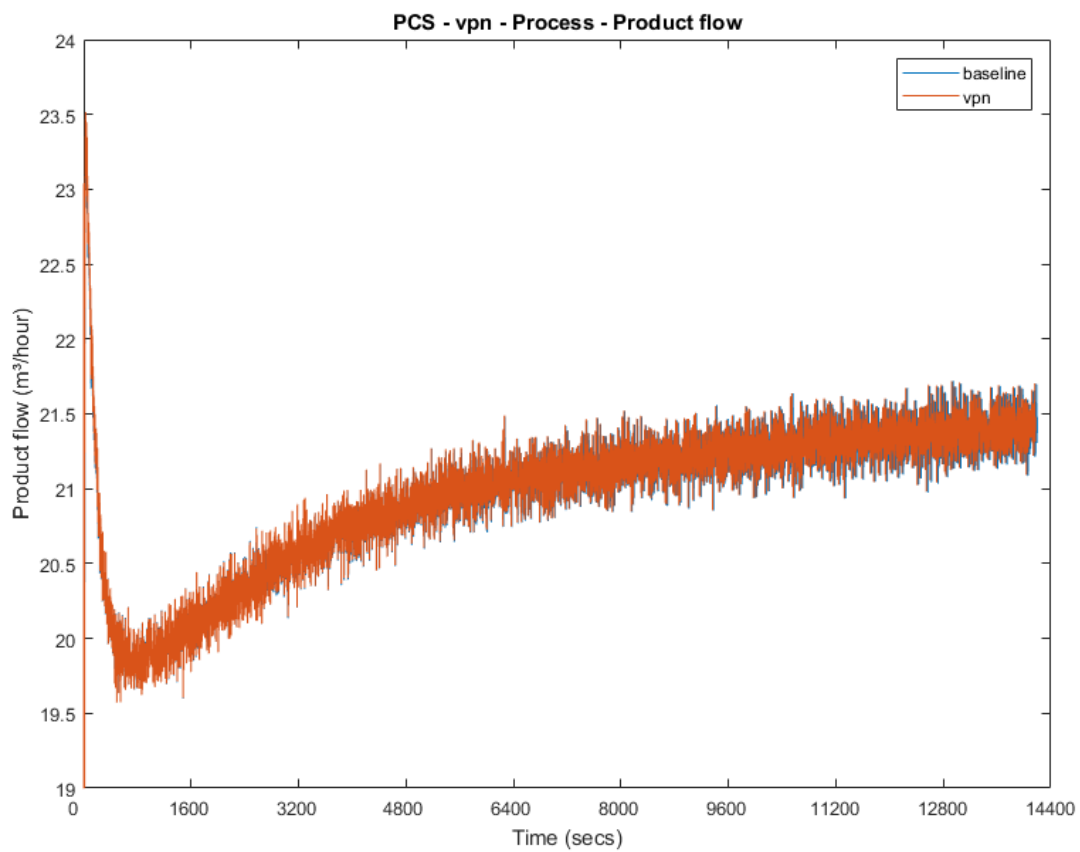


Figure 4-13 Plot of packet round trip time from HMI to OPC computer during the use of VPN connection from a remote computer

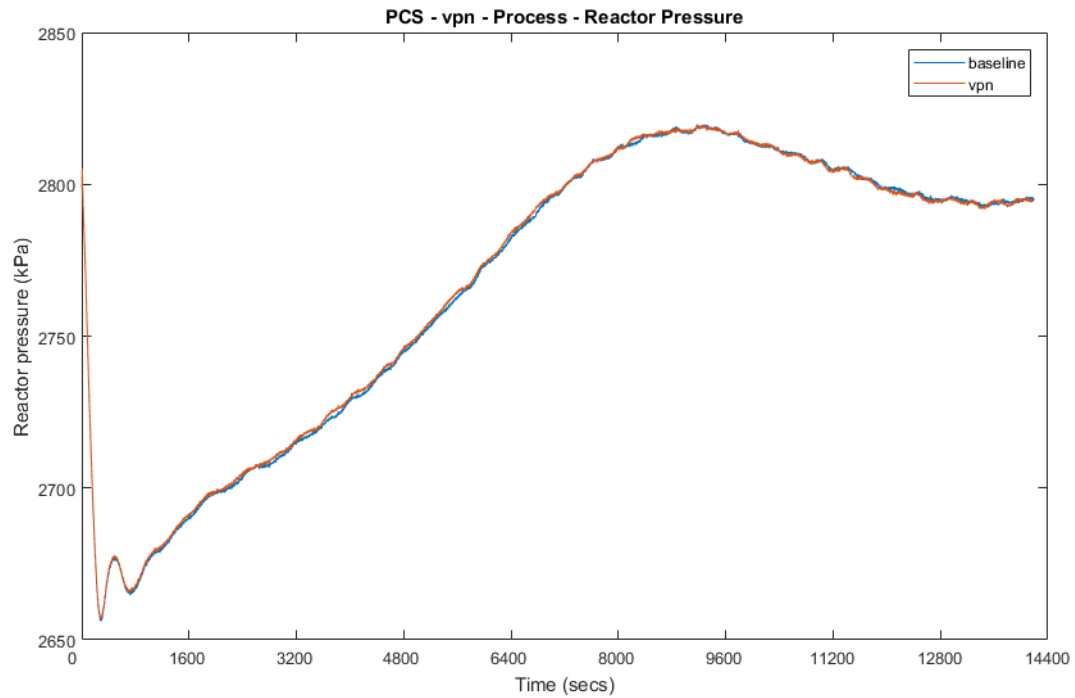
The manufacturing process also remained stable without any significant performance impact observed. The reactor pressure and product flow rate remained constant with and without the VPN connection.



3796

3797
3798

Figure 4-14 Manufacturing process product flow rate during the use of VPN connection from a remote computer



3799

3800

3801

Figure 4-15 Manufacturing process reactor pressure during the use of VPN connection from a remote computer

3802

4.8.7 Link to Entire Performance Measurement Data Set

3803

[Cisco VPN KPI data](#)

3804

[Cisco VPN measurement data](#)

4.9 Microsoft Active Directory

4.9.1 Technical Solution Overview

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information. A server running Active Directory Domain Services (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. Active Directory uses Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos and DNS.²⁰

Points to consider

- Cost of infrastructure can get high.
- Requires expertise to setup and maintain. Setup involves detailed planning.
- It is prone to being hacked.

4.9.2 Technical Capabilities Provided by Solution

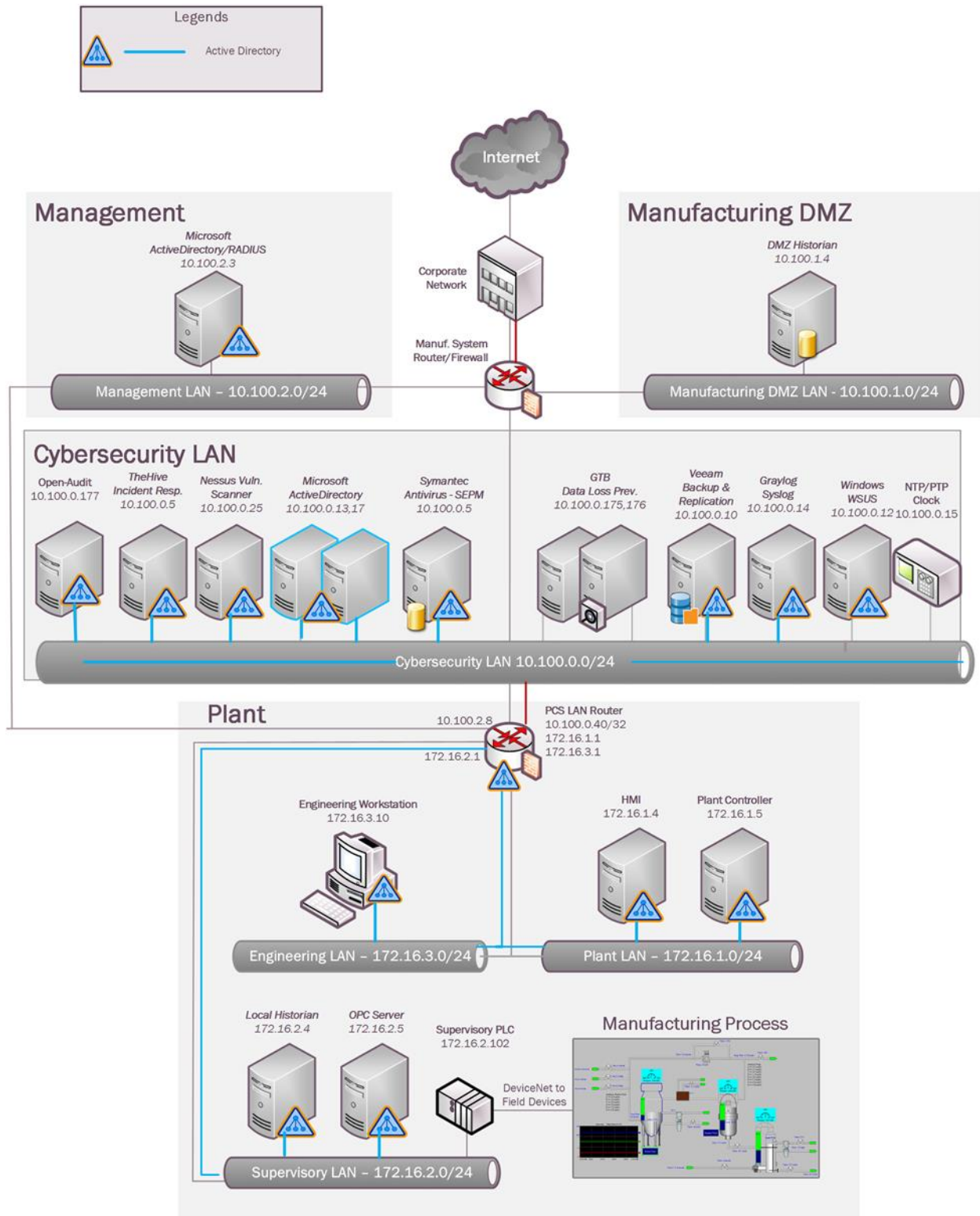
Microsoft Active Directory provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Credential Management
- Authentication and Authorization

4.9.3 Subcategories Addressed by Implementing Solution

PR.AC-1, PR.MA-1, PR.MA-2, PR-PT-3, PR.PT-4, DE.CM-3

²⁰ <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

3832 **4.9.4 Architecture Map of Where Solution was Implemented**

3833

3834 **4.9.5 Installation Instructions and Configurations**3835 **Setup:**

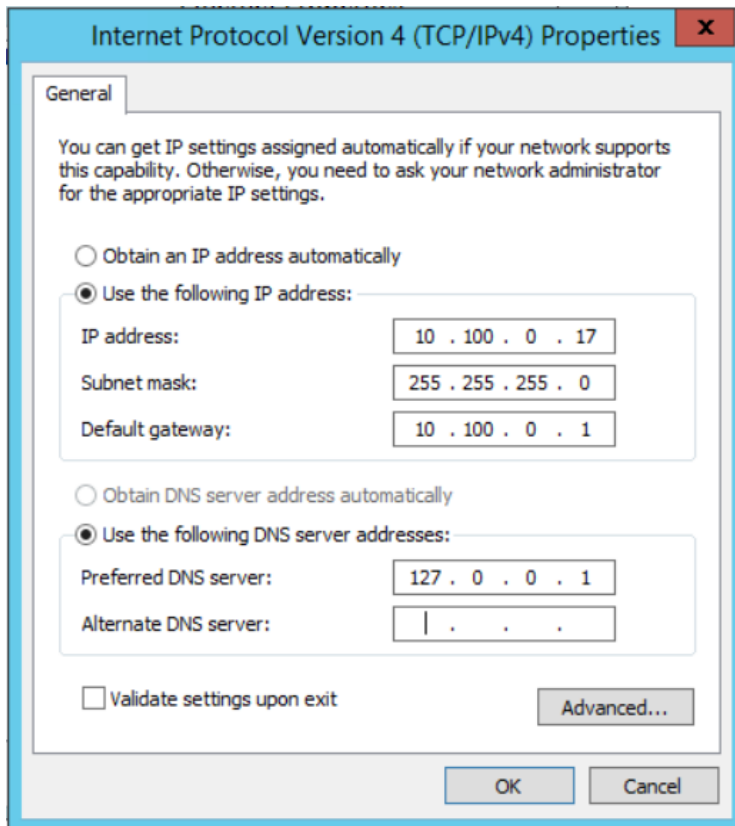
3836 Our setup consists of two separate Active Directory domain environments; one for the
 3837 Cybersecurity -LAN network and other for the Management network. For security reasons, The
 3838 AD domain in the Cybersecurity LAN network is separate from the domain that's in the
 3839 Management network. A pair of Domain Controllers (DC) running on Windows 2012 R2 were
 3840 setup in the Cybersecurity LAN network for authenticating Windows/Linux devices and another
 3841 separate DC on Windows 2012 R2 was setup in the Management network for authenticating
 3842 VPN users and network devices such as boundary routers. This DC in the Management network
 3843 is used in conjunction with a Windows NPS (Radius) server for authenticating the network
 3844 devices.

Hostname	IP address	Roles	Domain Name
LAN-AD	10.100.0.17	Active Directory, DNS, Network Policy Server (Radius)	LAN.lab
LAN-AD02	10.100.0.13	Active Directory, DNS, Network Policy Server (Radius)	LAN.lab
Mgmt-AD	10.100.2.3	Active Directory, DNS, Network Policy Server (Radius)	Mgmt.lab

3845

3846 **Installation:**

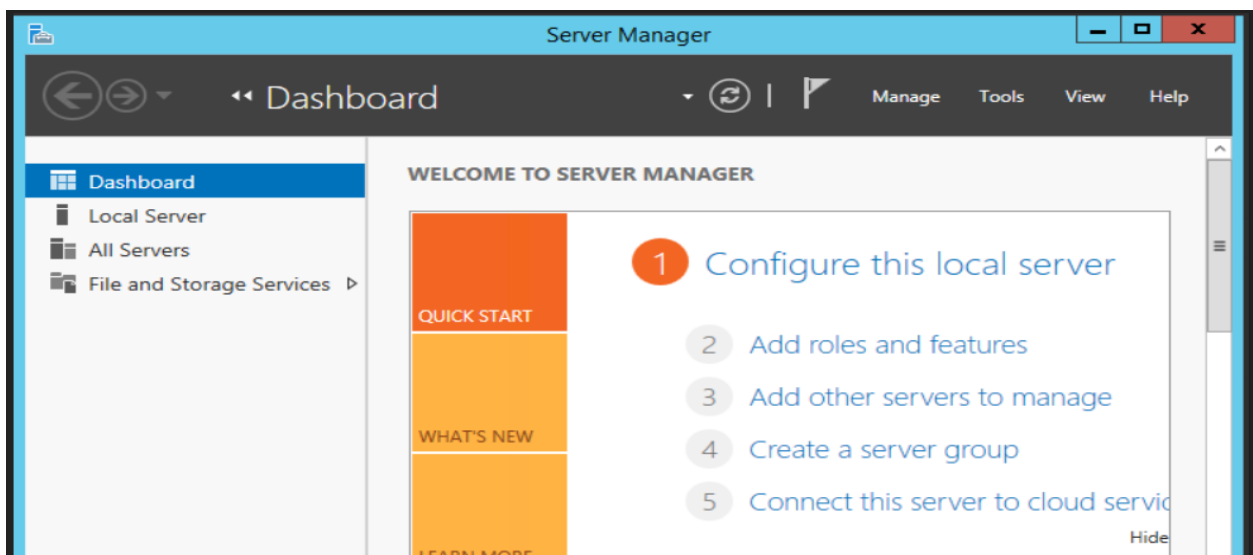
- 3847 • Below are high level instructions for installing Active Directory services (ADDS) on a
 3848 Windows 2012 R2 server.
- 3849 • It is recommended to have 2 servers running AD for redundancy. Ensure the servers are up to
 3850 date with patches and have meaningful hostnames as per their role. Begin by configuring a
 3851 static IP address on the network interface of your server. Since the server will also act as
 3852 DNS server, for DNS server field you can use local host address 127.0.0.1



3853

- Launch “Server Manager” and click on “Add Roles and Features”

3855

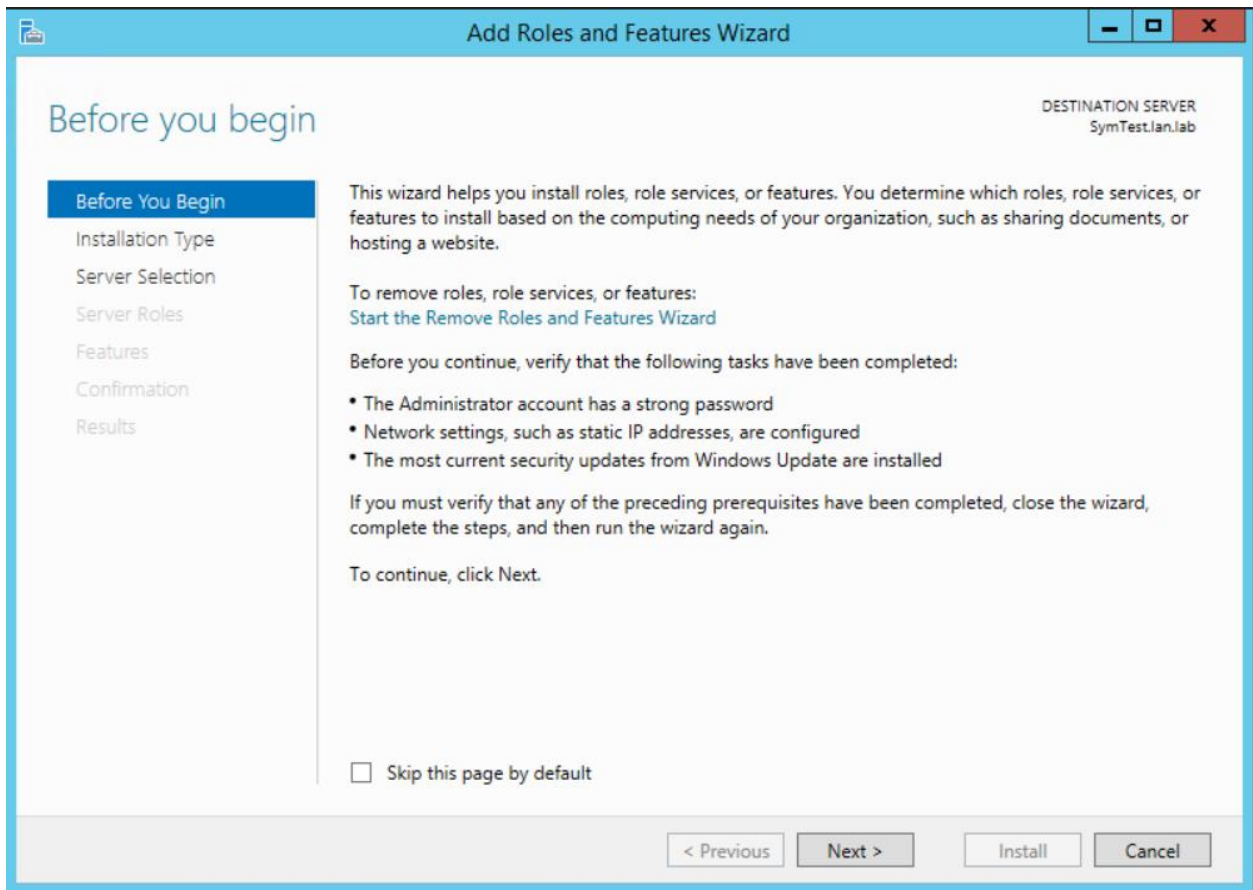


3856

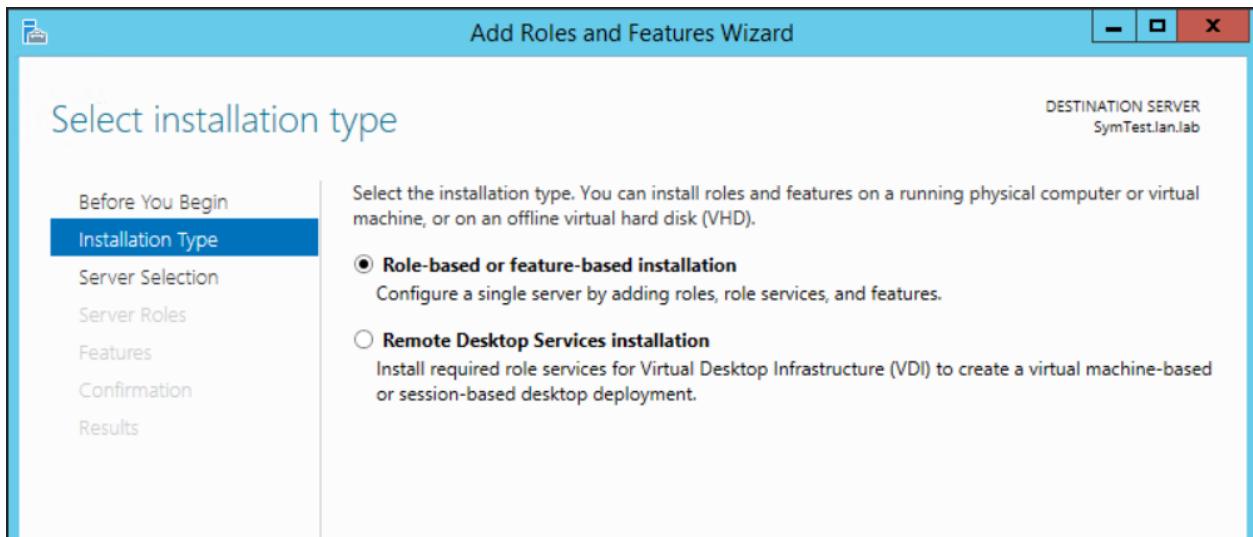
3857

3858

- 3859 • Click “**Next**” at the first page
3860

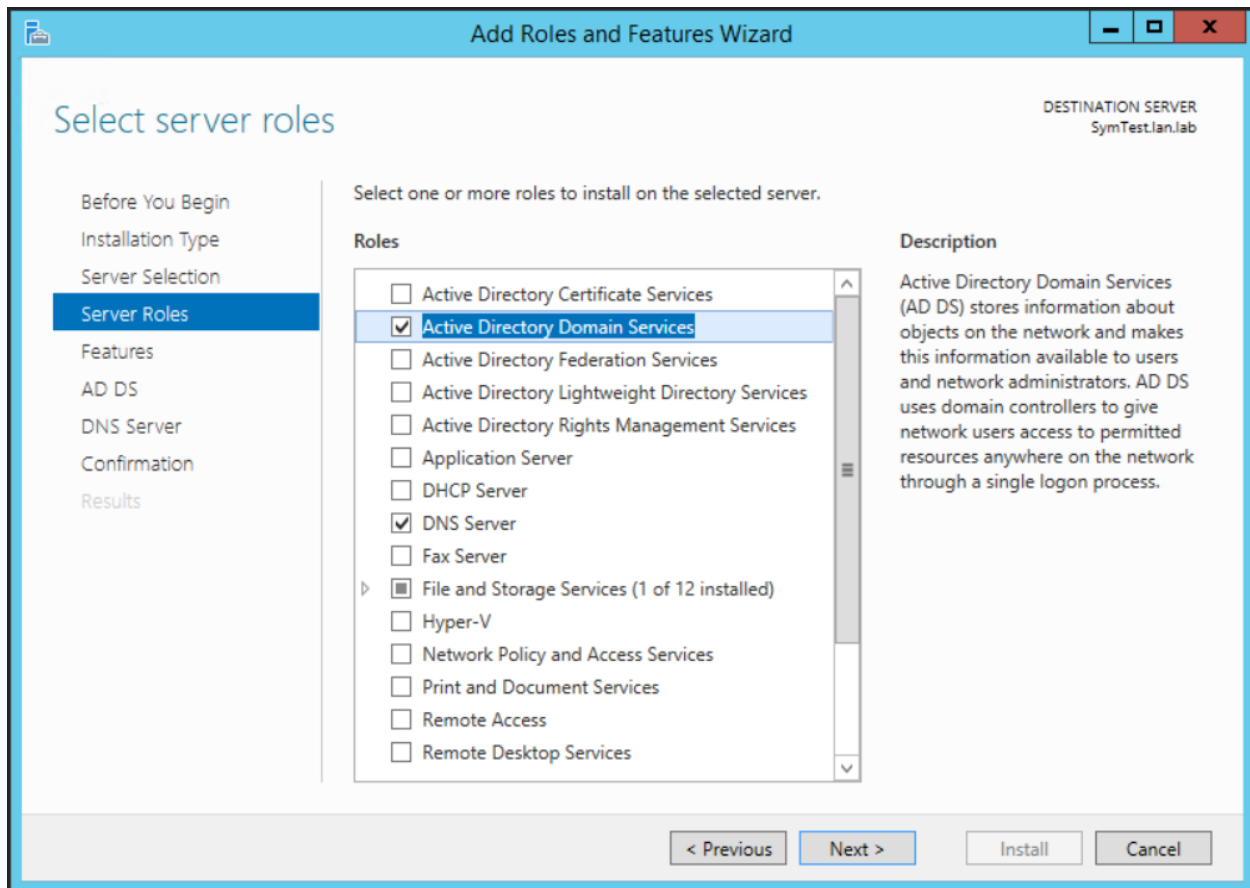


- 3861
3862
3863 • Select “**Role Based or Feature Based Installation**” under Installation Type
3864



3865
3866

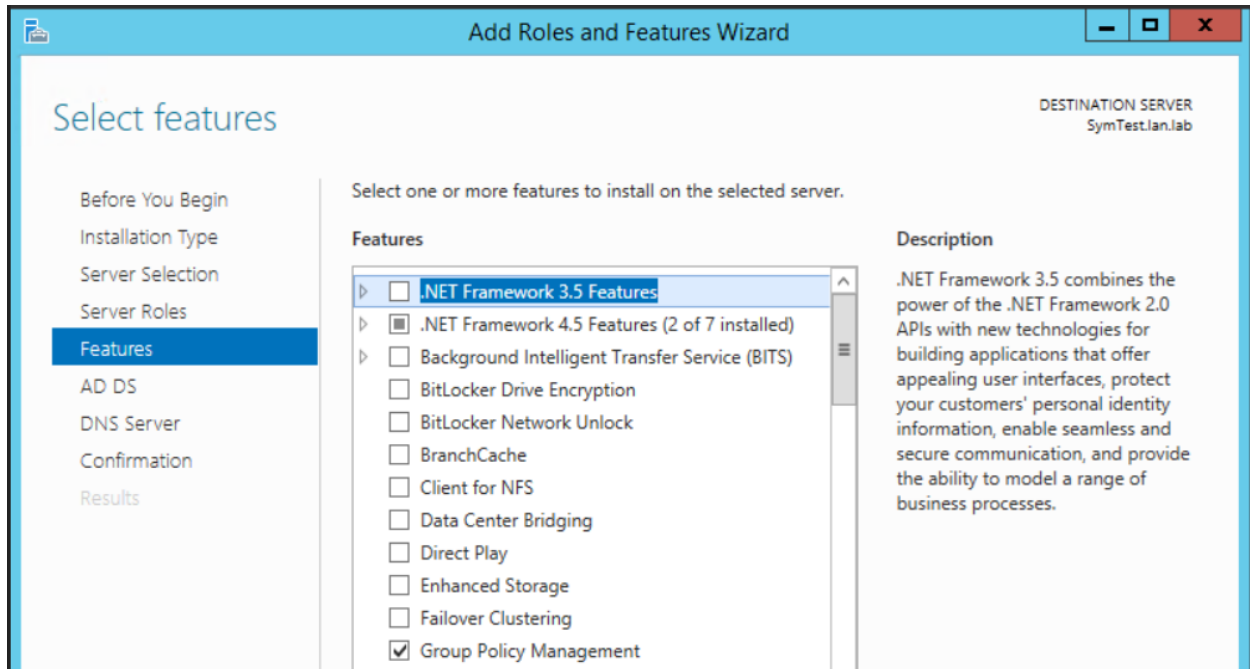
- 3867 • Select “**Active Directory Domain Services**” and “**DNS Server**” to install. Click Next



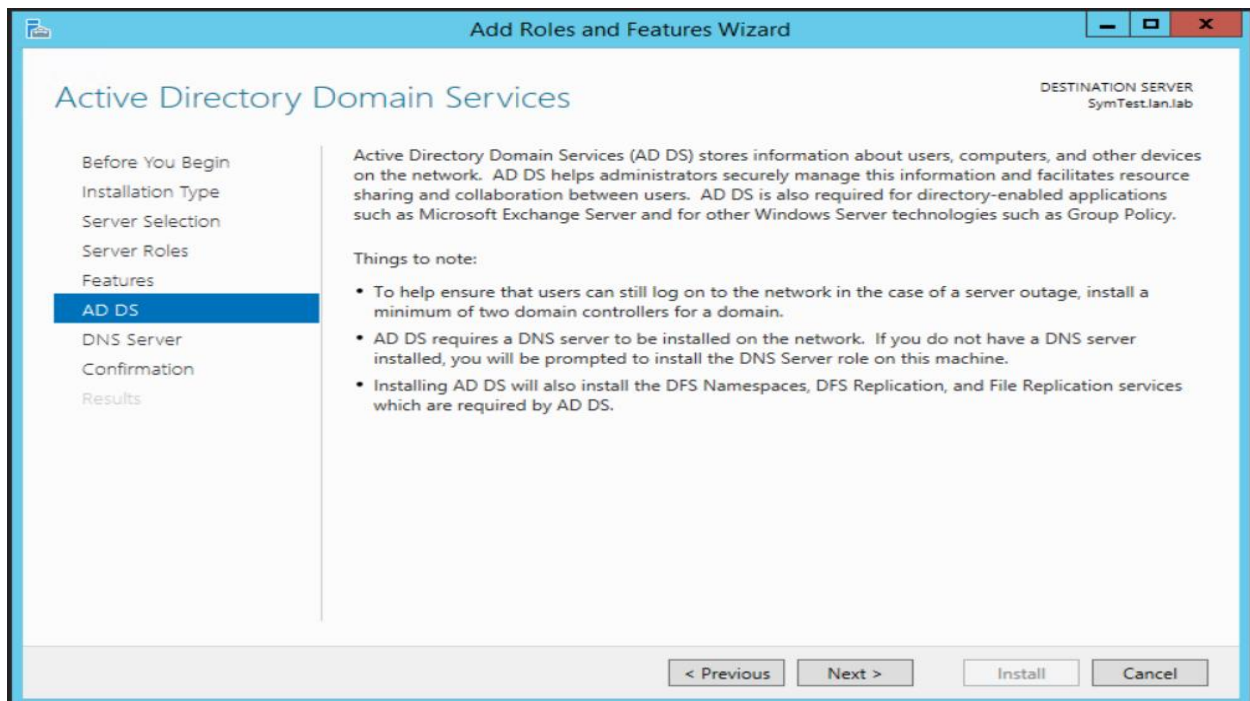
3868

3869

- 3870
- Under “**Features**”, leave the default options selected and click **Next**.



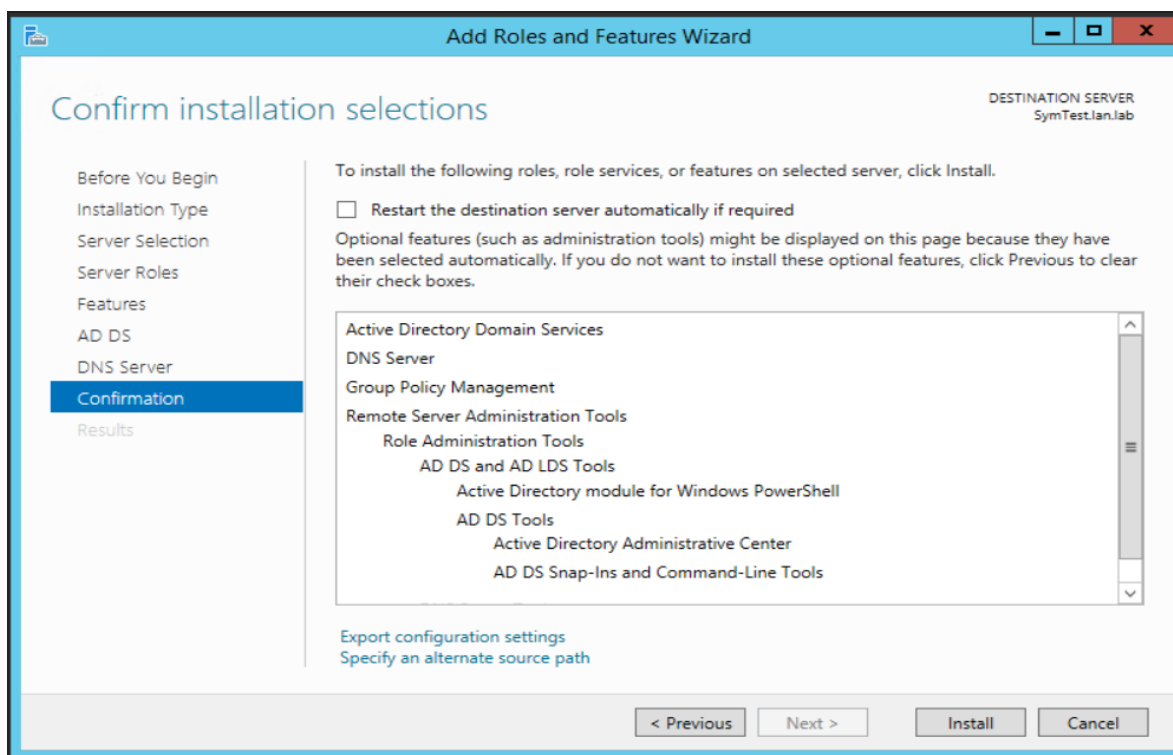
- 3871
- 3872
- On the “**AD DS**” page, click **Next**. Likewise, on the “**DNS Server**” page click **Next** as well.



3873

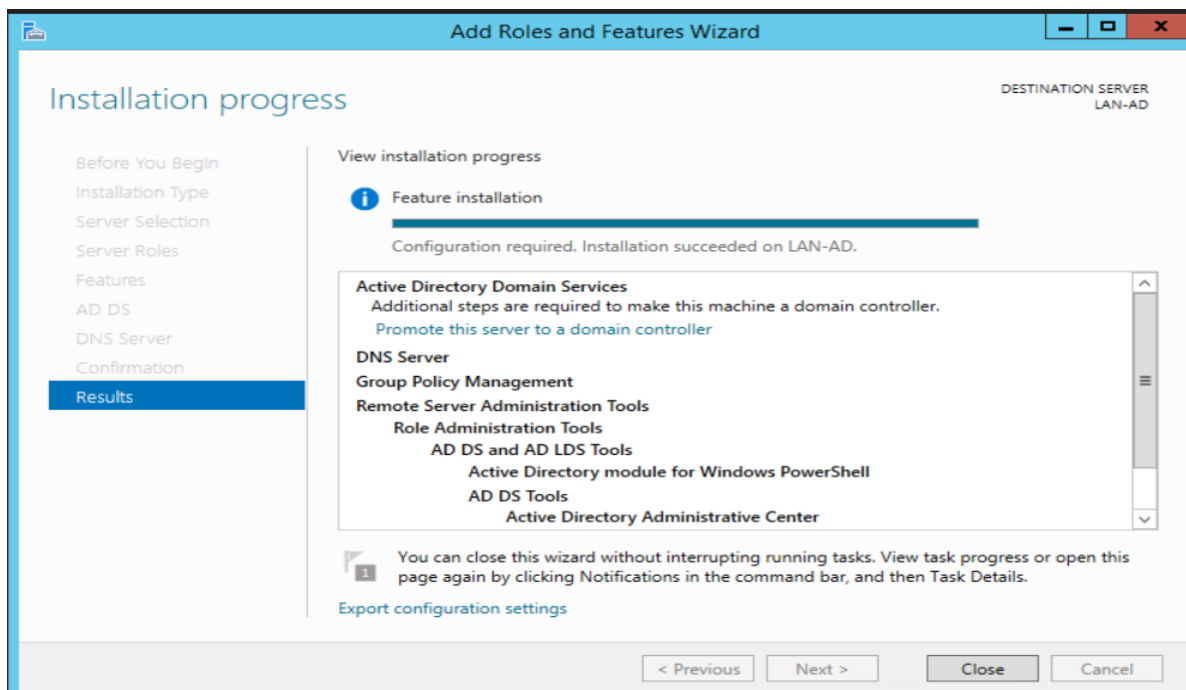
3874

- 3875
- Verify your settings on the “**Confirmation**” page. Click **Install** to proceed.



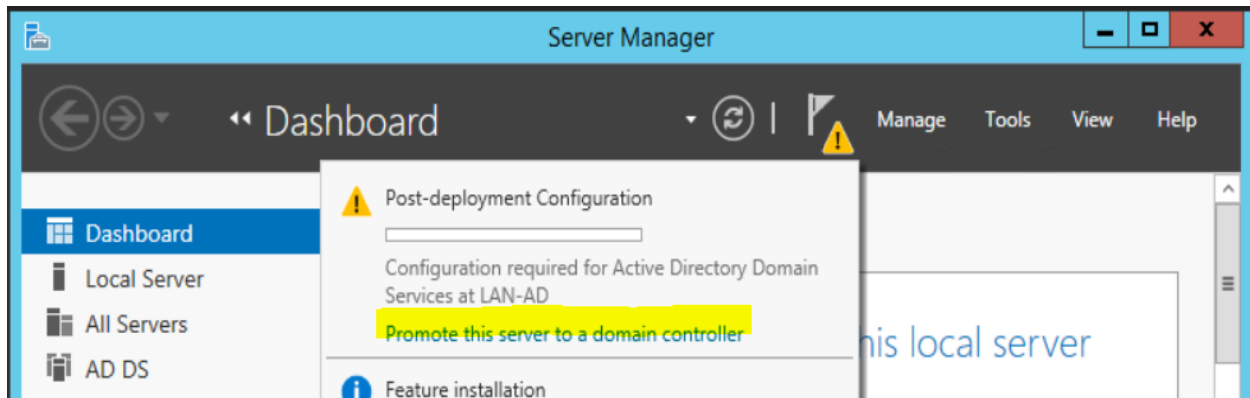
3876

- 3877
- 3878
- The installation process will run and will show an “Installation succeeded” message upon completion. Hit **Close** button.

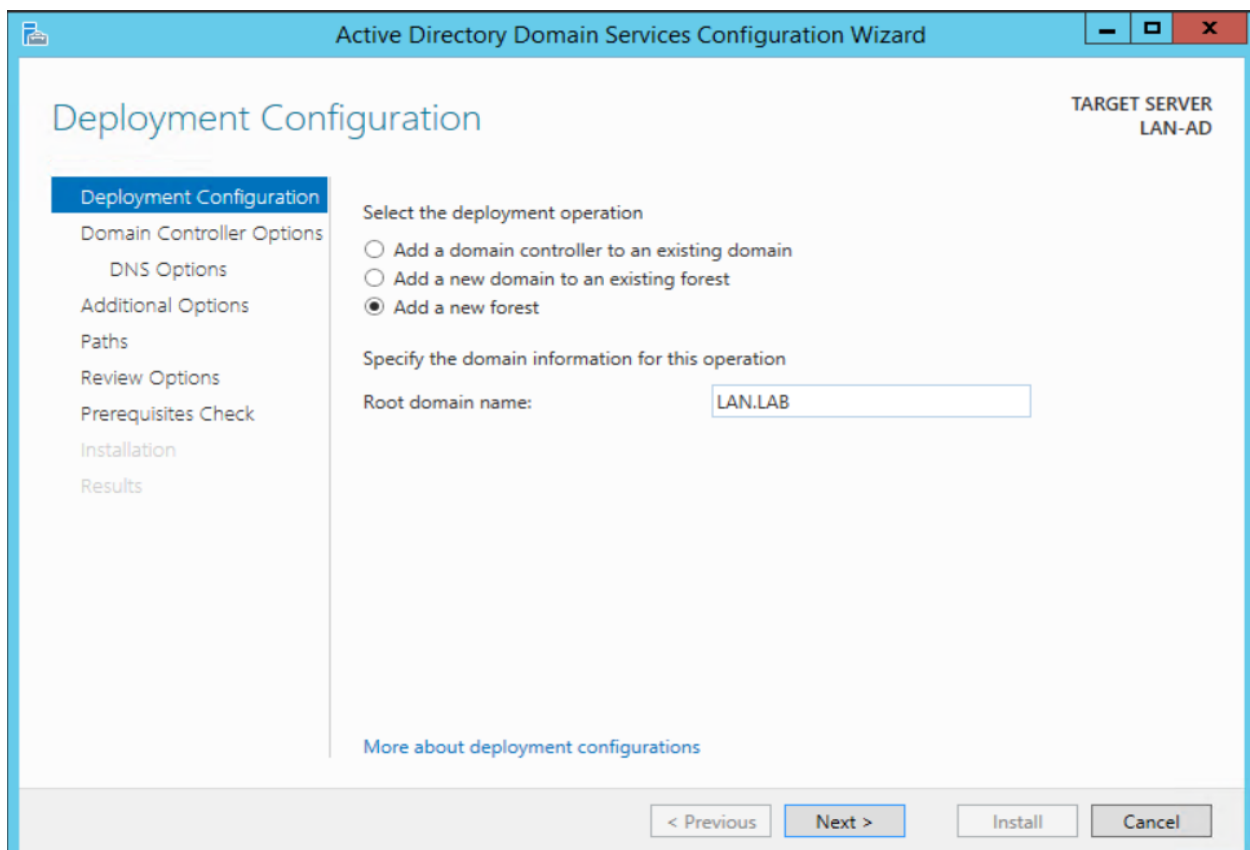


3879

- 3880 ➤ Launch “**Server Manager**” again and click on “**Promote this server to a domain**
3881 **controller**”



- 3882
- 3883 • On the “Deployment Configuration” step, select “**Add a new forest**” as this would be a new
3884 domain controller in a new forest. Mention a Root Domain name as applicable to your
3885 environment.



- 3888
- Set a Directory Services Restore Mode password in the next step. Click **Next**

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes a file icon, the text 'Active Directory Domain Services Configuration Wizard', and standard window controls. The main window has a blue header with the title 'Domain Controller Options' and a 'TARGET SERVER LAN-AD' label. On the left is a navigation pane with links: 'Deployment Configuration', 'Domain Controller Options' (highlighted), 'DNS Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select functional level of the new forest and root domain'. It contains two dropdown menus: 'Forest functional level:' and 'Domain functional level:', both set to 'Windows Server 2012 R2'. Below these is a section 'Specify domain controller capabilities' with three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). At the bottom, there is a section 'Type the Directory Services Restore Mode (DSRM) password' with two password fields labeled 'Password:' and 'Confirm password:', each containing a series of dots.

3889

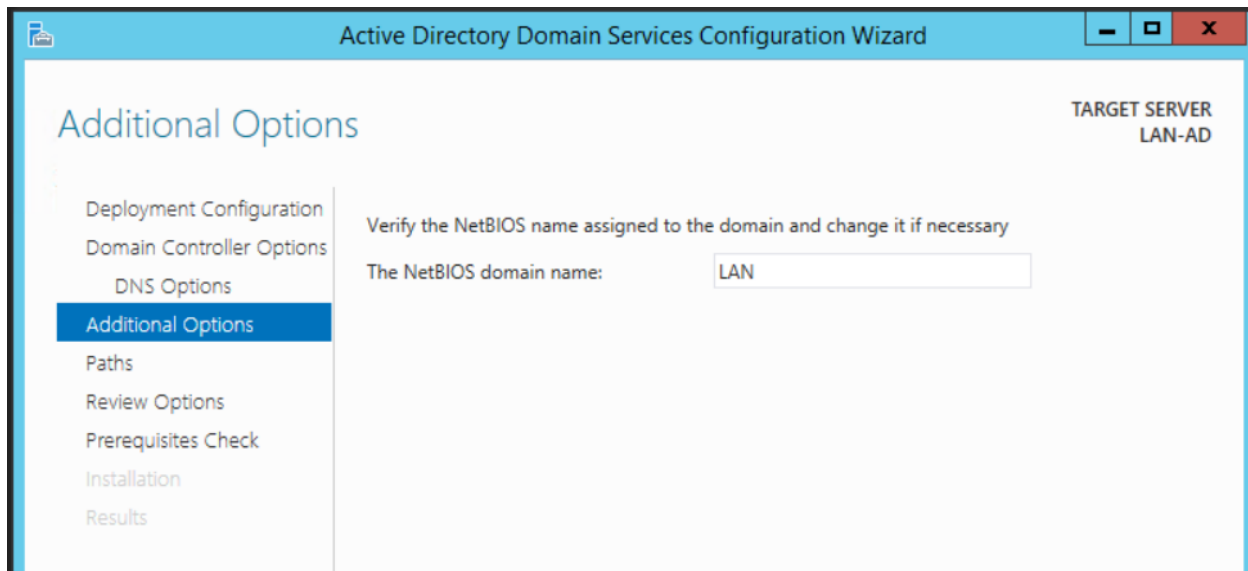
- 3890
- Under “**DNS Options**” leave the default options selected. Click **Next**

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, now on the 'DNS Options' page. The title bar and window controls are the same. The main window has a blue header with the title 'DNS Options' and a 'TARGET SERVER LAN-AD' label. The left navigation pane has 'DNS Options' highlighted. The main content area is titled 'Specify DNS delegation options' and contains a single checkbox labeled 'Create DNS delegation', which is unchecked. At the top of the main content area, there is a yellow warning banner with a triangle icon, the text 'A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...', a 'Show more' link, and a close button (X).

3891

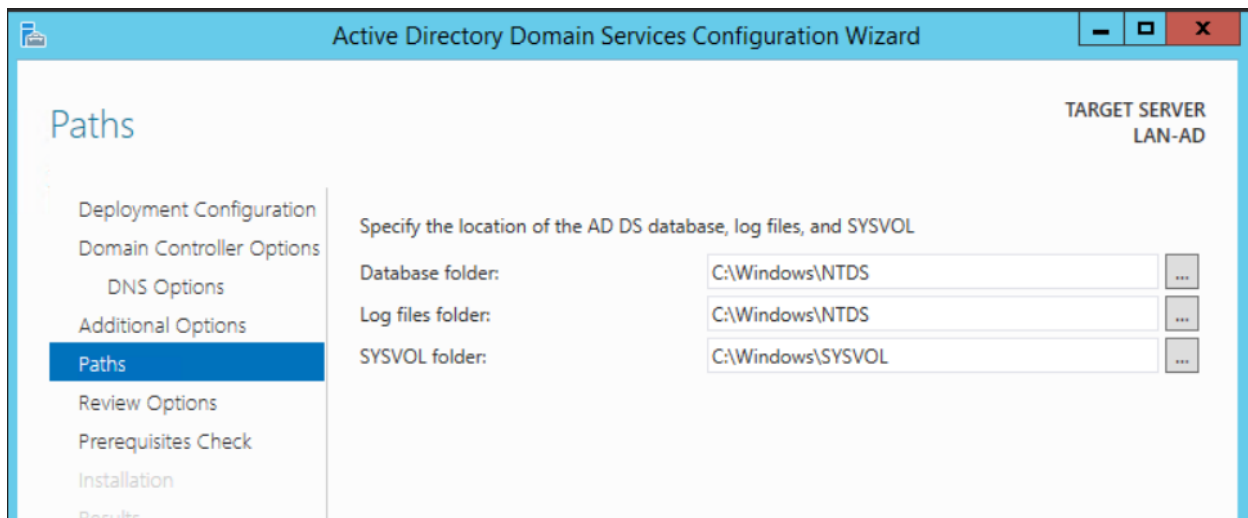
3892

- 3893
- Under “**Additional Options**”, confirm the NETBIOS domain name. Click **Next**.



3894

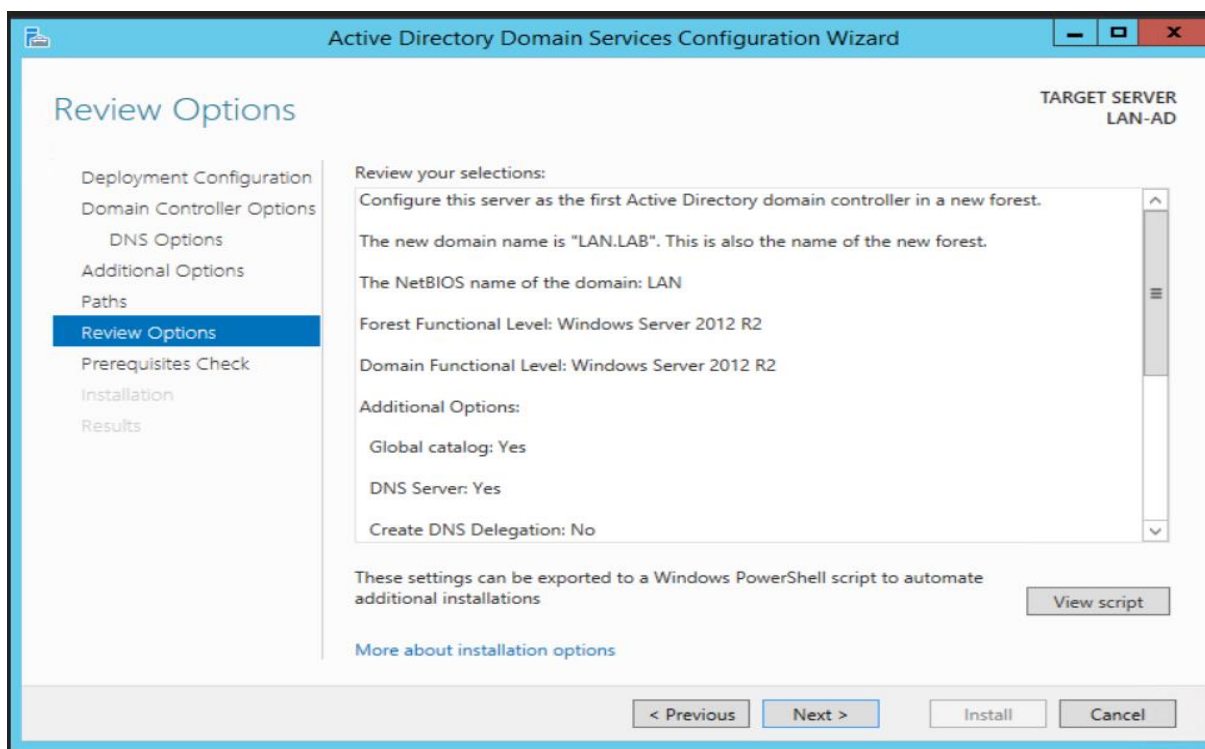
- 3895
- Under “**Paths**”, leave the default folder paths as it is. Click **Next**



3896

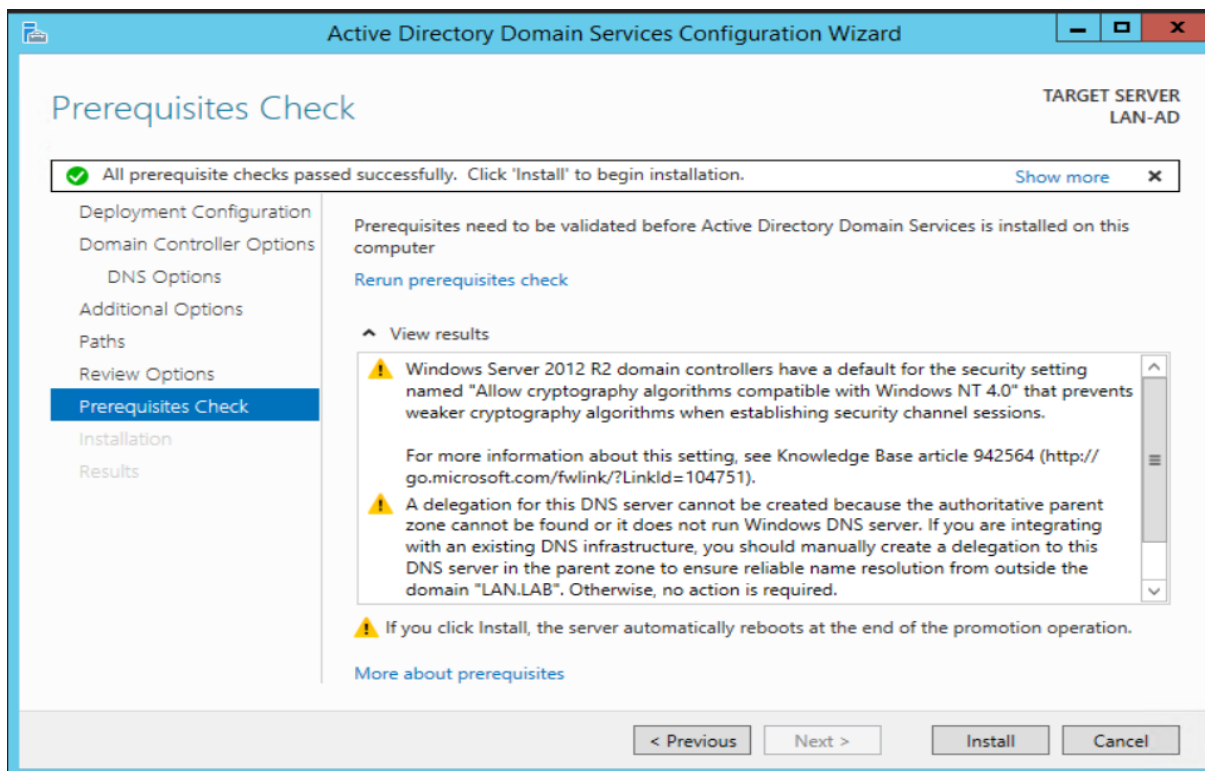
3897

- 3898
- On the “**Review Options**” page, confirm all the settings and click **Next**.



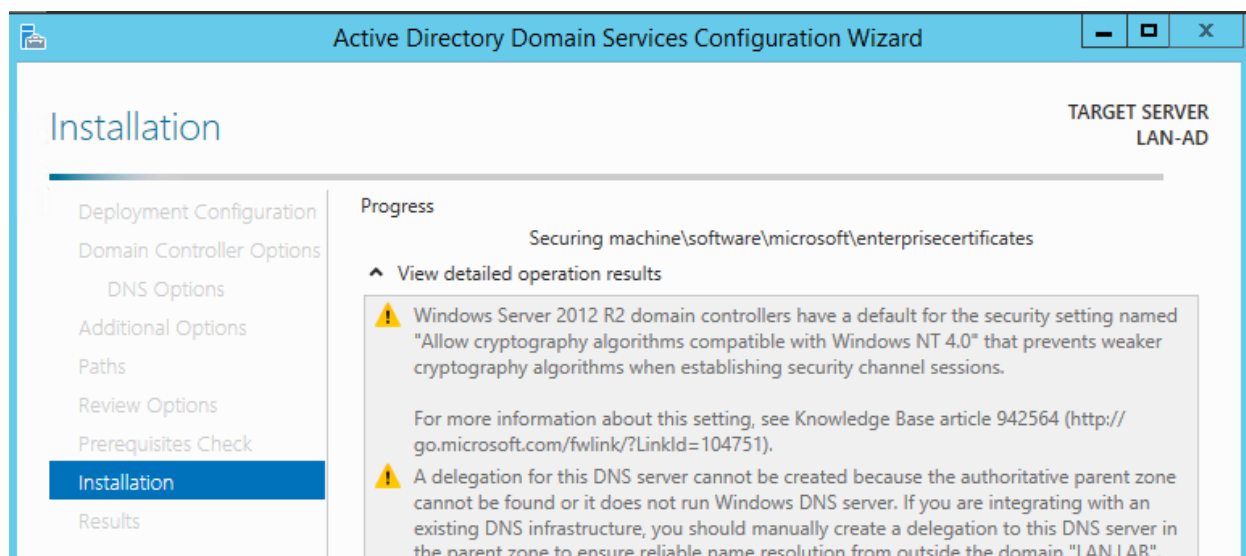
3899

- 3900
- On the “**Prerequisites Check**”, click Install to launch the installation process.

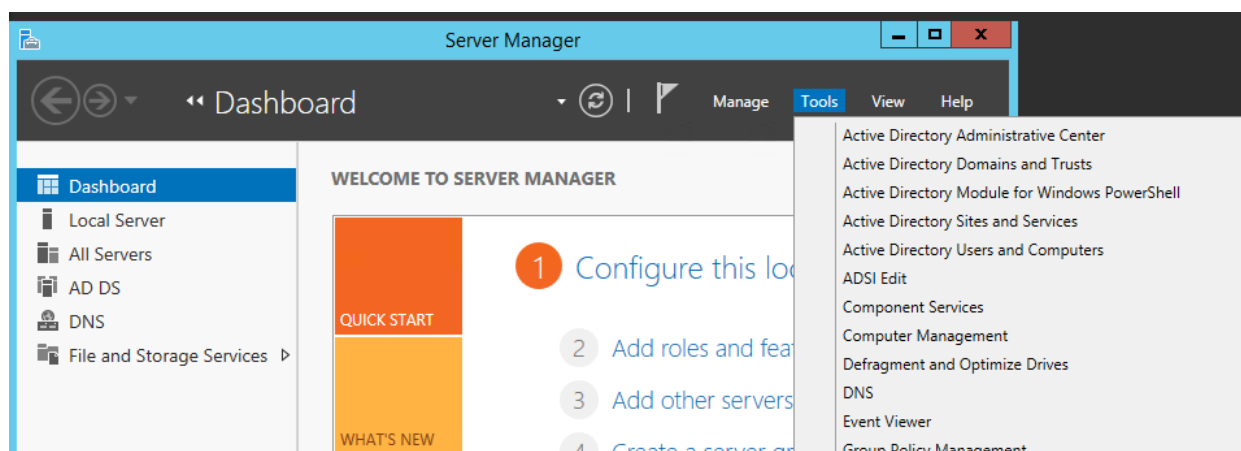


3901

- 3902 • The installation process will now run displaying the Progress bar. Upon completion, the
3903 server should auto reboot.



- 3904
- 3905 • Upon reboot, login with domain administrator credentials. Open "Server Manager" and click
3906 on "Active Directory Users and Computers" under Tools to manage your AD.



- 3907
- 3908 **Configurations:**

- 3909 ▪ All windows systems were domain joined to the AD domain in the Cybersecurity LAN
3910 network. The initial domain join process is a onetime task and involves a system restart. In
3911 addition to authentication piece, the Domain Controllers also have DNS role installed. They
3912 also act as internal DNS servers. Any system that is joined to AD, will automatically create a
3913 DNS record for itself. For any system that isn't joined to AD such as a switch or a router the
3914 DNS record for these would have to be manually created.
- 3915
- 3916 ▪ The procedure to integrate or join Windows machines to AD can be found [here](#).
3917

- Once the machines were domain joined, different user accounts with varying levels of privileges were provisioned depending on the role i.e. machine operators, process owners and service accounts. On Windows systems, the accounts used by the process owners were granted administrator privileges on each Windows system by adding them to the local Administrators group while the operator user accounts were only granted “Remote Desktop” rights. The individual user accounts are subjected to a password policy whereas the service accounts are set to not expire.
- On the OPC server, we are running a Matrikon OPC server. The Microsoft Distributed Component Object Model (DCOM) service plays a vital role in integration the OPC server with AD. Having the correct DCOM settings in place when using AD is critical for plant operations. We have followed the steps documented in this Matrikon OPC guide²¹ to apply the necessary DCOM settings. Please refer to the section below “**OPC Server DCOM Configuration**” for our settings.
- For using AD authentication against network devices, we leveraged Microsoft Network Policy Services (NPS) to use as a Radius server along with AD DS. Within the Radius server, a connection request policy and a network policy was created for each network device. Please refer to the section below “**Radius Server Setup**”
- A physical network connection was made to the Management port of the Boundary Firewall This port was then assigned a static IP address from the Management subnet on each device so that it could communicate with the above Radius and AD server. Typically, each network device has an option to configure Radius authentication. In addition, we enabled the auditing feature on the DC to track for successful/failed logins. Once the setup is done, you should be able to use AD user accounts to login to your network devices.

OPC Server DCOM Configuration

Pre-requisites:

- All windows systems participating need to be domain joined to the AD server.
- Ensure all systems are getting their time synced from the AD server and verify the time on each server is consistent with the time on the AD (Domain Controller). Time sync is critical.
- Verify TCP port 135 is open between all OPC clients and the OPC server.

Shown below are the changes implemented

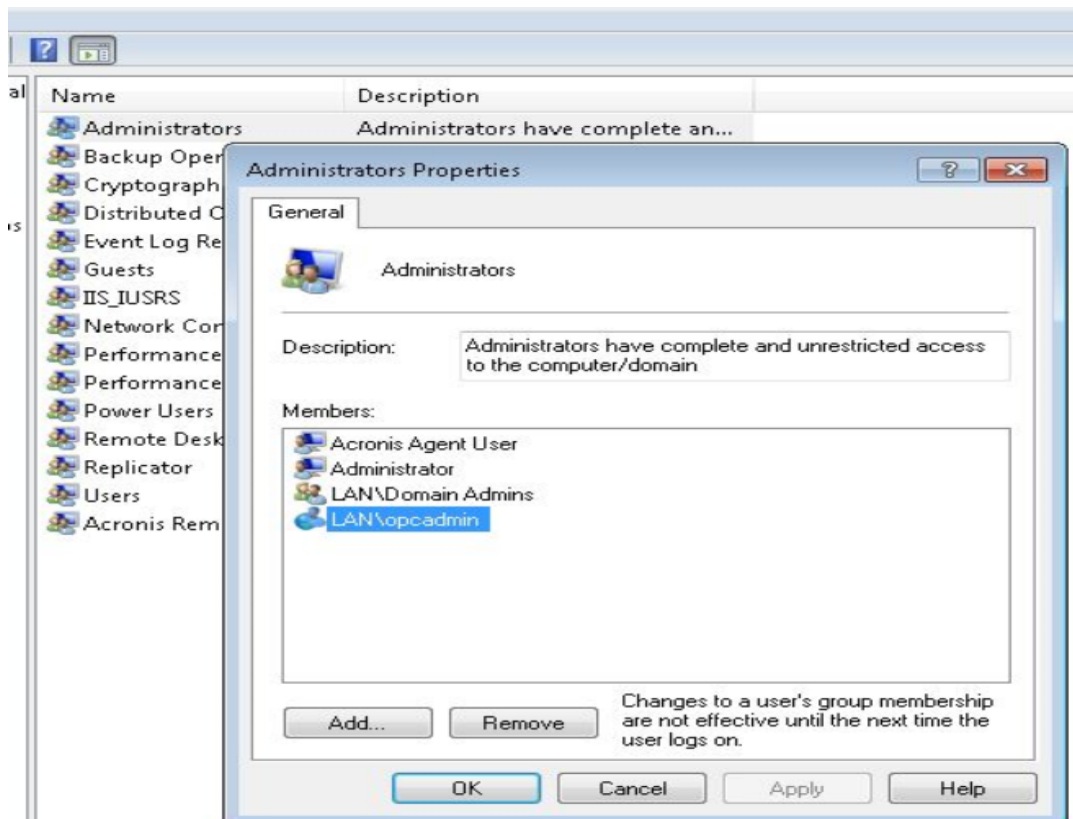
²¹ Matrikon OPC DCOM Setup: <https://www.matrikonopc.com/downloads/1128/whitepapers/index.aspx>

- Created 2 domain users “**opcadmin**” and “**opcuser**” in our AD. The “**opcadmin**” will be the admin user. The other “**opcuser**” will be treated as a non-admin user and is optional to configure. Add the **opcadmin** user to the Local Administrators group on the OPC Server and client.

Systems taking part in the OPC setup:

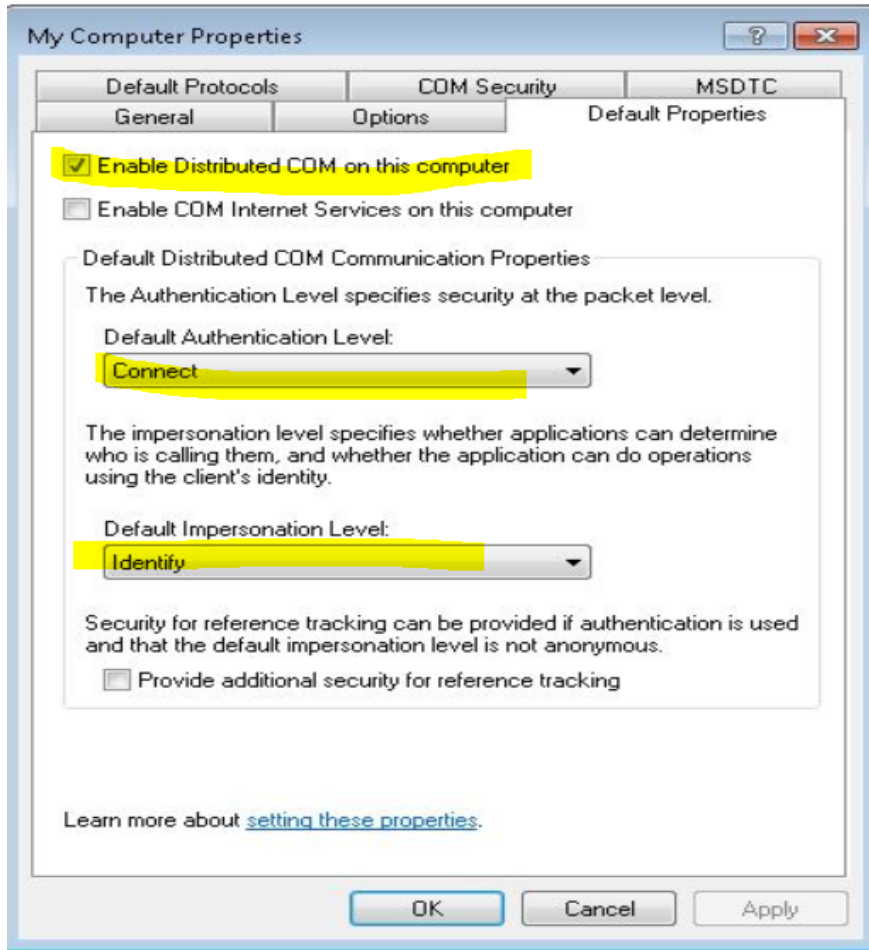
Hostname	IP address	Roles	Administrators
OPC Server	172.16.2.5	OPC_Server	opcadmin
Controller	172.16.1.5	OPC Server + Client	opcadmin, opcuser

For example: Below is a snap from one of the OPC clients.

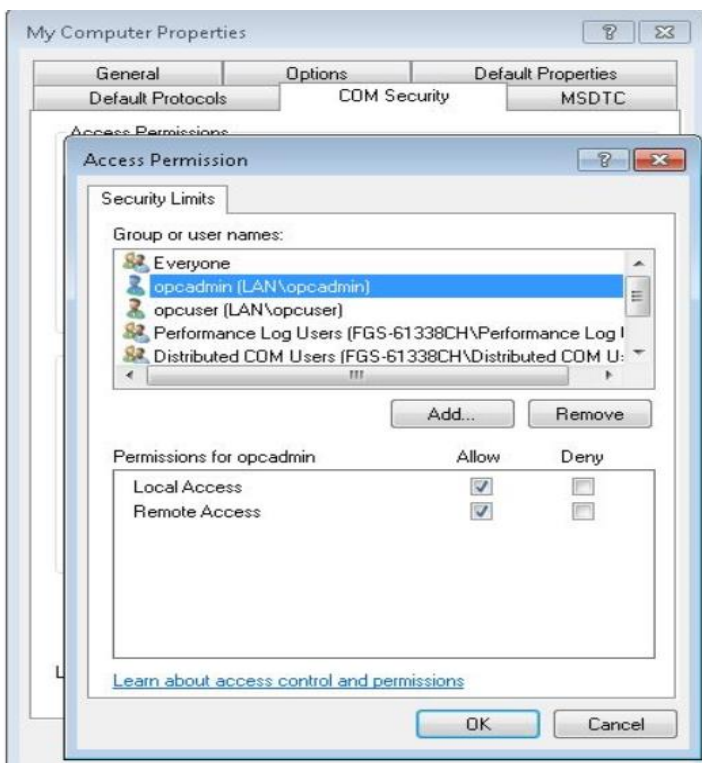


- On the OPC Client, make the following changes to DCOM properties. Launch the “Control Panel >> **Administrative Tools** >> **Component Services** snap-in to open the DCOM console. Alternatively, you can also run “**dcomcnfg**” (without quotes) command from command prompt to launch the DCOM snap-in.

- Expand **Console Root > Component Services > Computers**, Right-click **My Computer** and then click **Properties**. Ensure the settings are as follows



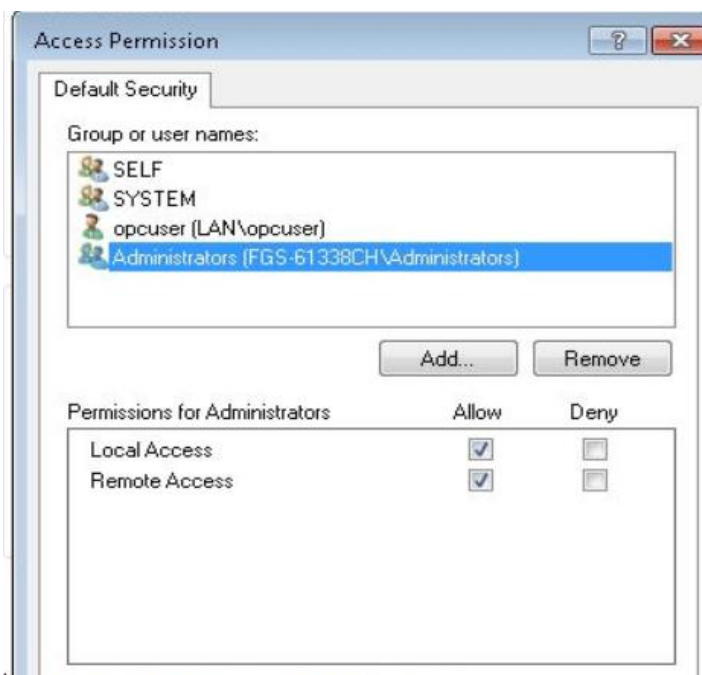
- Click on “**COM Security**” tab. Under “**Access Permissions**” >> “**Edit Limits**” button >> Add the opcadmin user to the list and check on the Allow boxes for both “**Local Access**” and “**Remote Access**” categories. You can add the “**opcuser**” as well if needed and grant it Allow permission for only “**Local Access**”.



3976

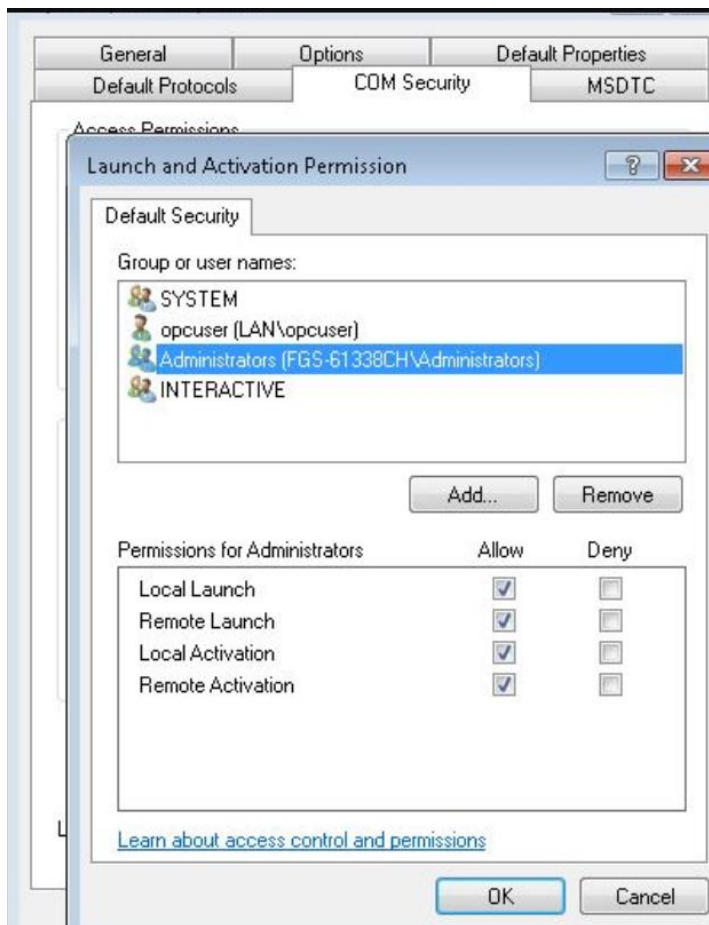
- 3977 • Under “**Access Permissions**” >> “**Edit Default**” button >> Ensure that “<server-
3978 name>\Administrators” group has all the boxes checked. The **opcadmin** user was made part
3979 of this Administrators group earlier.

3980 If you are adding the **opcuser**, grant it Allow permissions for “Local Access” only.



3981

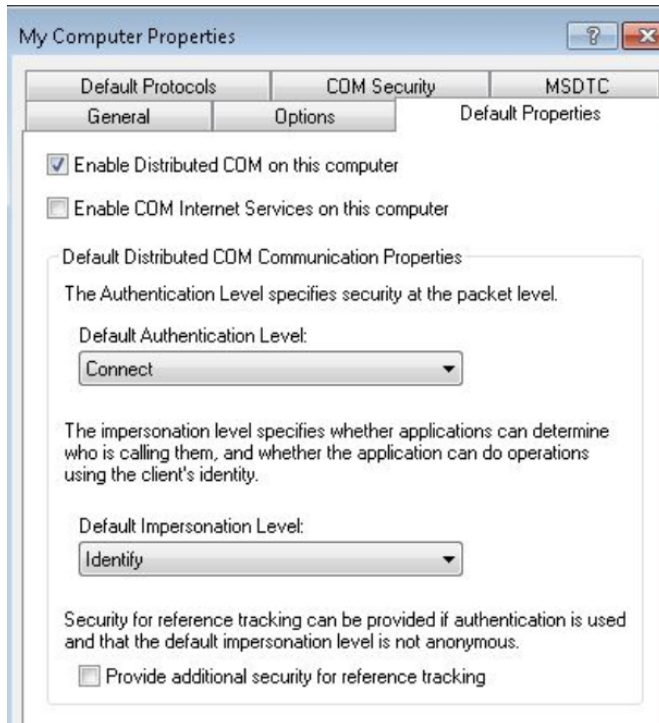
- 3982 • Under the “**Launch and Activation Permissions**” >> “**Edit Default**” button >> ensure the
 3983 “**Administrators**” group has **ALLOW** Permissions for all 4 categories. The other “opcuser”
 3984 should have ALLOW only for “**Local Launch**”



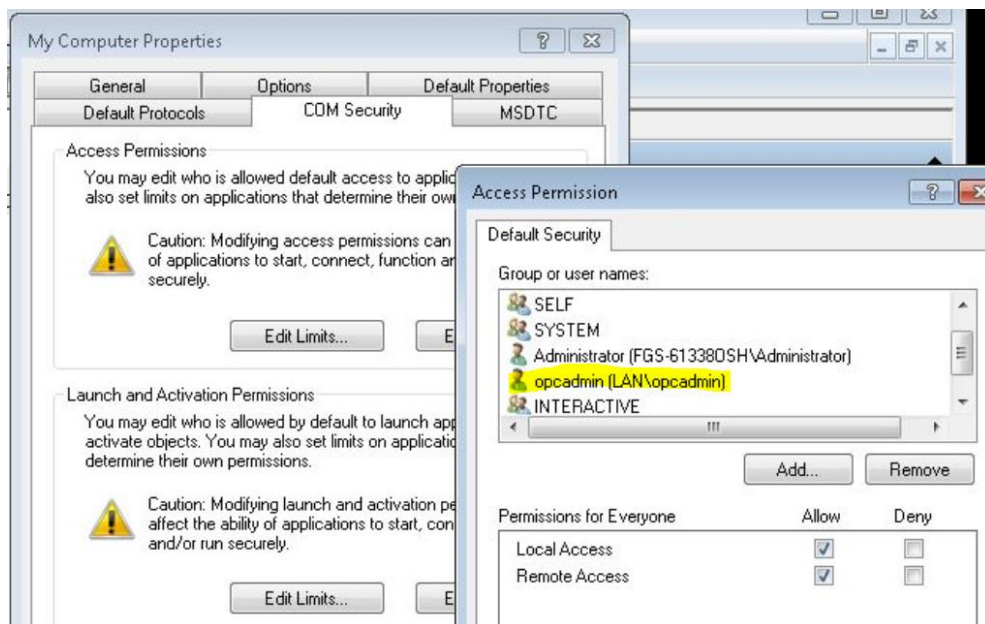
- 3985
- 3986 • This completes the OPC client-side configuration. Reboot the system after these changes are
 3987 made. Repeat the process on each client.
- 3988 • On each OPC Server machine, make the following changes to DCOM properties. Launch the
 3989 “**Control Panel >> Administrative Tools >> Component Services**” snap-in to open the
 3990 DCOM console.

3991

- 3992 • Expand Console Root > Component Services > Computers, right-click **My Computer** and
 3993 then click Properties. Ensure the settings are as follows
 3994

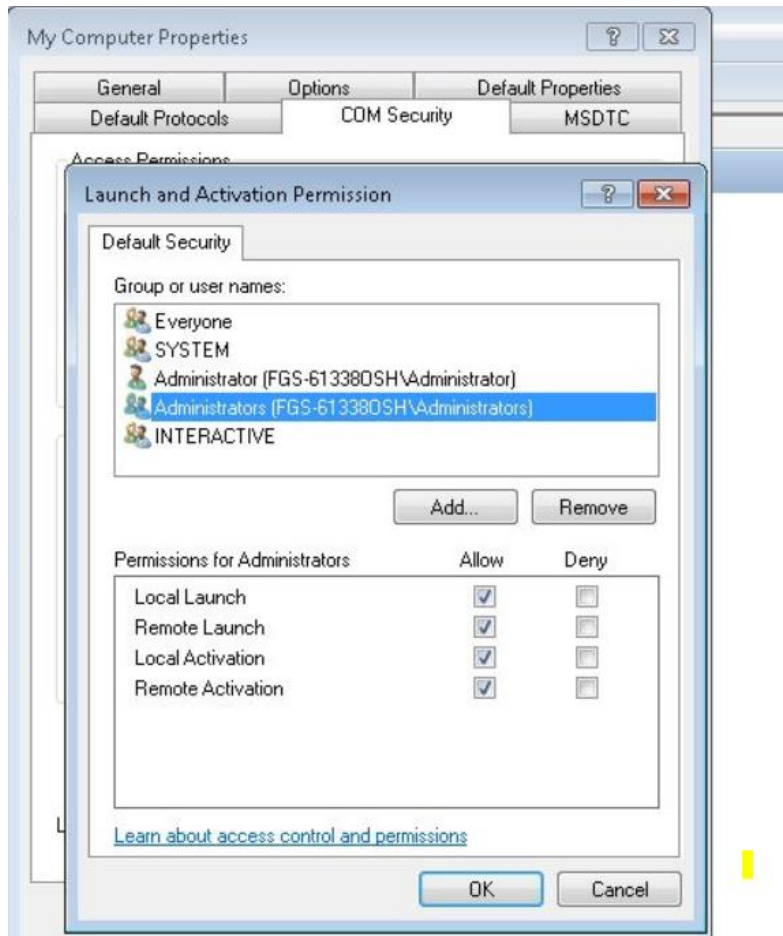


- 3995
 3996
 3997 • Click on the “**COM Security**” tab >> **Access Permissions** >> “**Edit Default**” >> Add the
 3998 **opcadmin** user and grant it **ALLOW** permissions for Local Access and Remote Access
 3999 boxes.
 4000



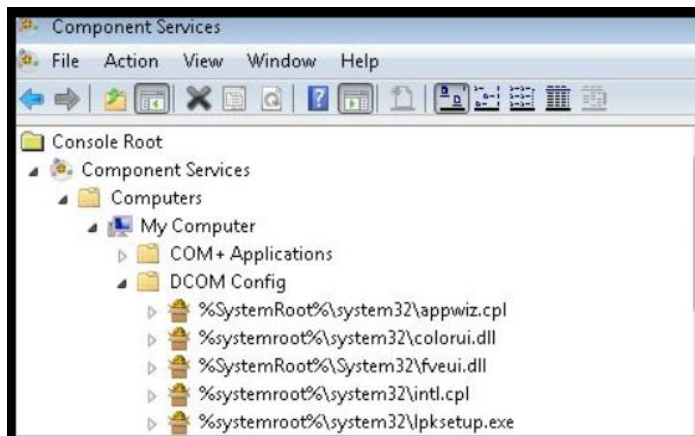
4001
 4002

- Similarly, under “**Launch and Activation Permissions**” >> “**Edit Default**” >> Add the “Administrators” group and check on **ALLOW** Boxes for all 4 categories. If adding the other opcuser, it will only have Local Launch permissions.



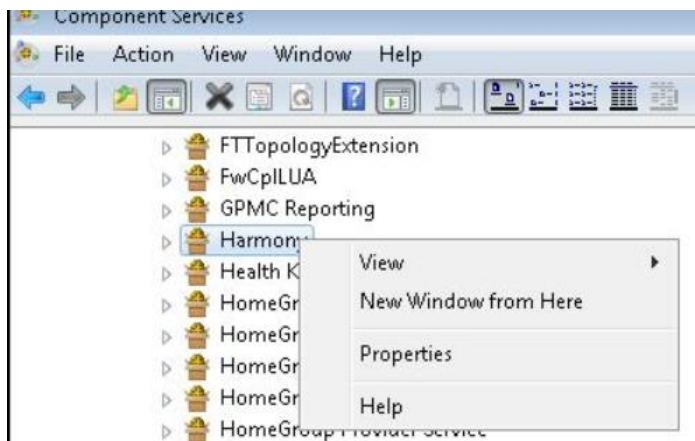
- Note down the names of the opc-server software installed in your environment and make the below shown DCOM changes on each of their application folders. In our case, the list of the s/w is as follows
 - Harmony (Installed on OPC Server)
 - RSLINX (Installed on OPC Server)
 - MATLAB (Installed on the Controller)
- We will start with the main OPC-Server and then move on to the Controller host. Launch the DCOM console and browse to **Console Root > Component Services > Computers > My Computer > DCOM Config**. In the list of applications in the right pane, right-click your OPC server (application folder) and choose **PROPERTIES**.

4022



4023

4024



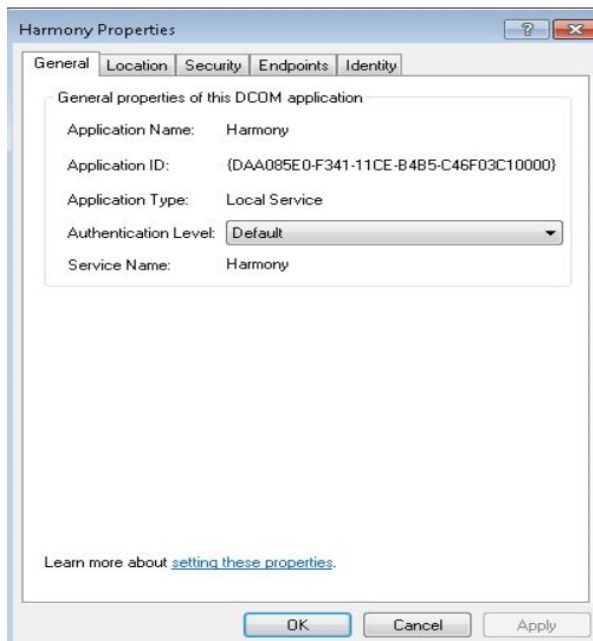
4025

4026

4027

4028

For example, find the “**Harmony**” folder, right click to view its Properties. On the **General** tab, set **Authentication Level** to **Default**.

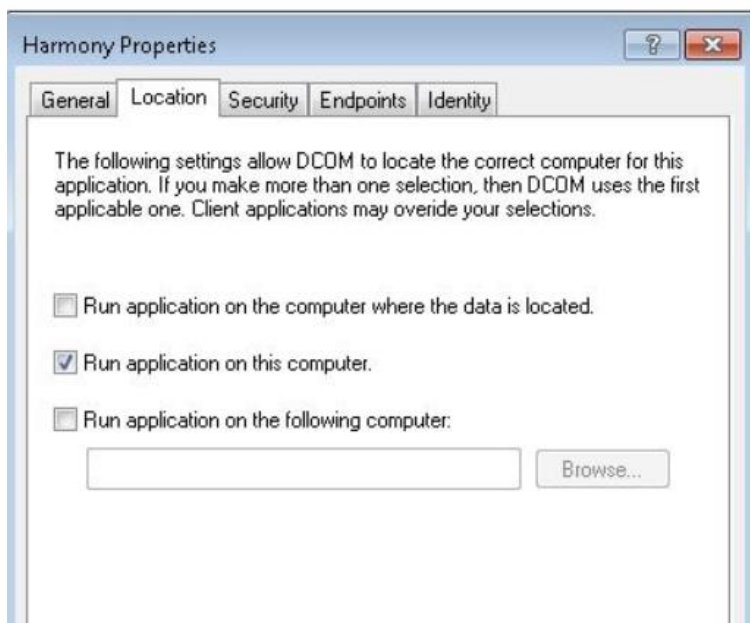


4029

4030

4031

- On the Location tab, Select - **Run application on this computer.**



4032

4033

4034

4035

4036

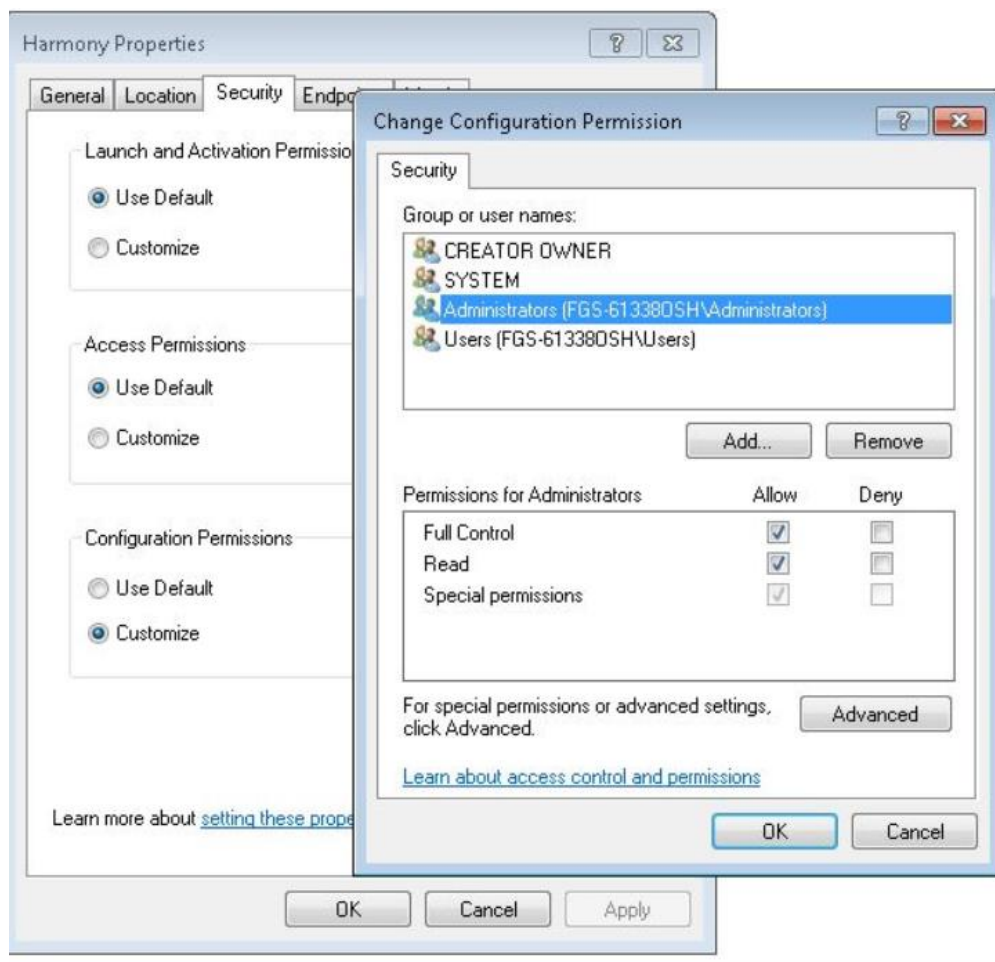
4037

4038

4039

- On the Security tab, typically set permissions as follows:
OPC users: (opcuser)
 - Launch and Activation Permissions: Use System Defaults

- 4040 • Access Permissions: Use System
- 4041 • Configuration Permissions: Allow Read
- 4042
- 4043 OPC administrators: (opcadmin)
- 4044 • Launch and Activation Permissions: Use System Defaults
- 4045 • Access Permissions: Use System Defaults
- 4046 • Configuration Permissions: Customize Full Control as shown below. (Note opcadmin is a
- 4047 member of Administrators group)
- 4048

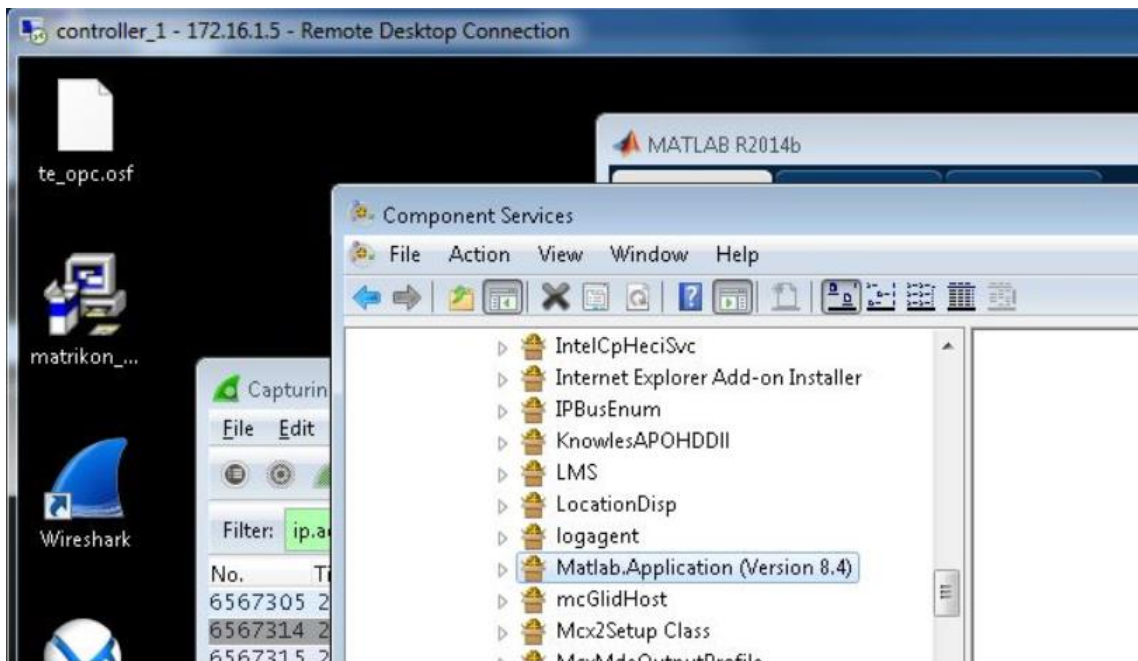


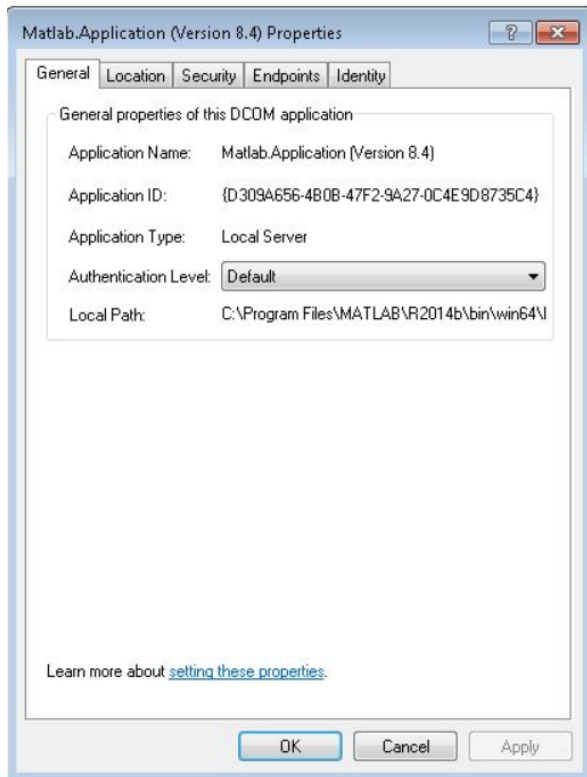
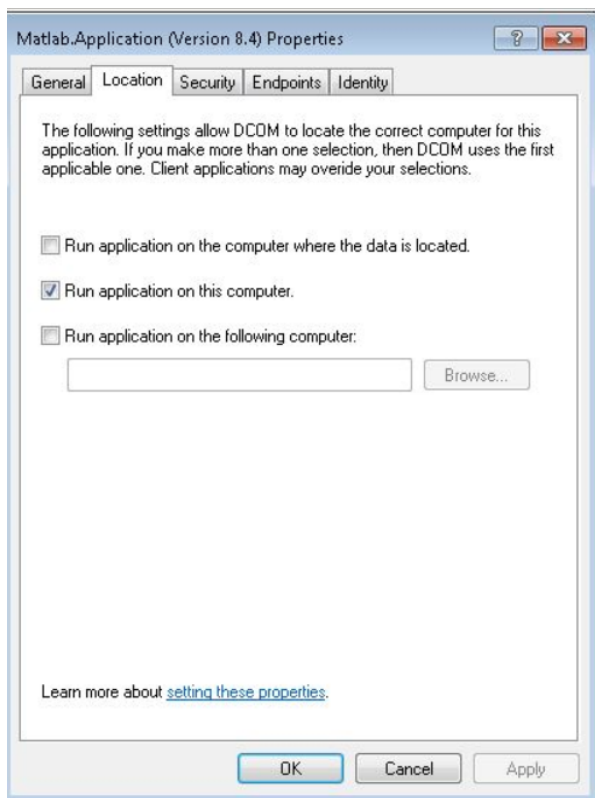
- 4049
- 4050
- 4051 • On the Identity tab, choose the “This user” option and enter the user name and password for
- 4052 the AD user you created. We will select opcadmin as the user in our case. Click OK to save
- 4053 your settings. Reboot system.

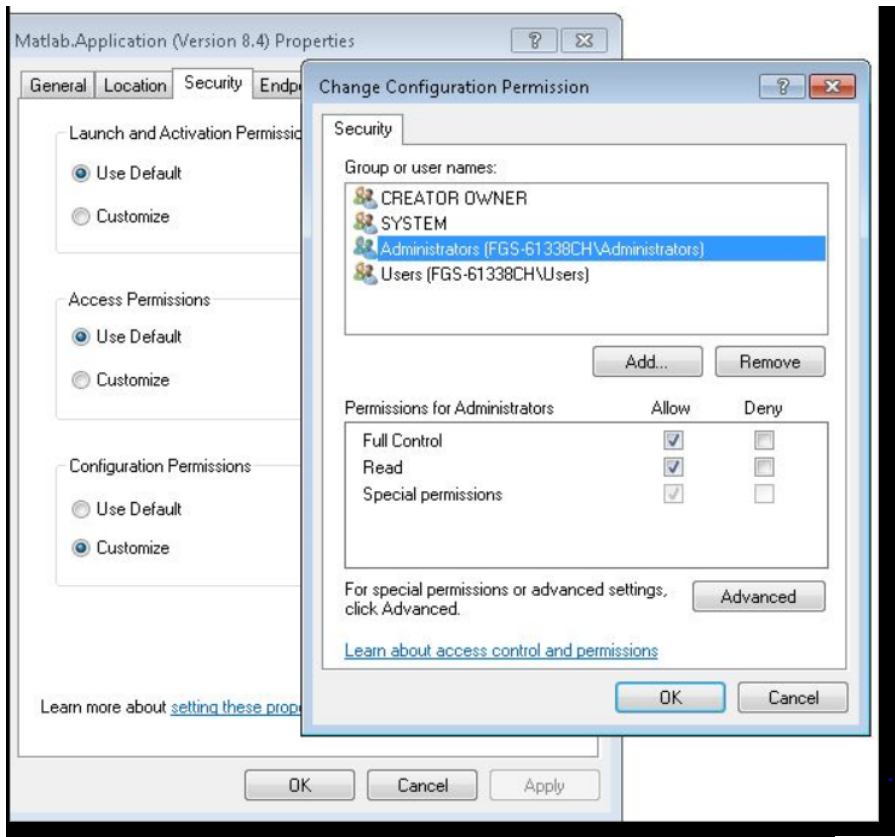


- Repeat the above steps 3.e.1 to 3.e.5 on the “RSLINX” folder (on the OPC Server) and on the MATLAB Application folder (on the Controller Server). Reboot system when done. Some screenshots for the MATLAB folder are shown below.

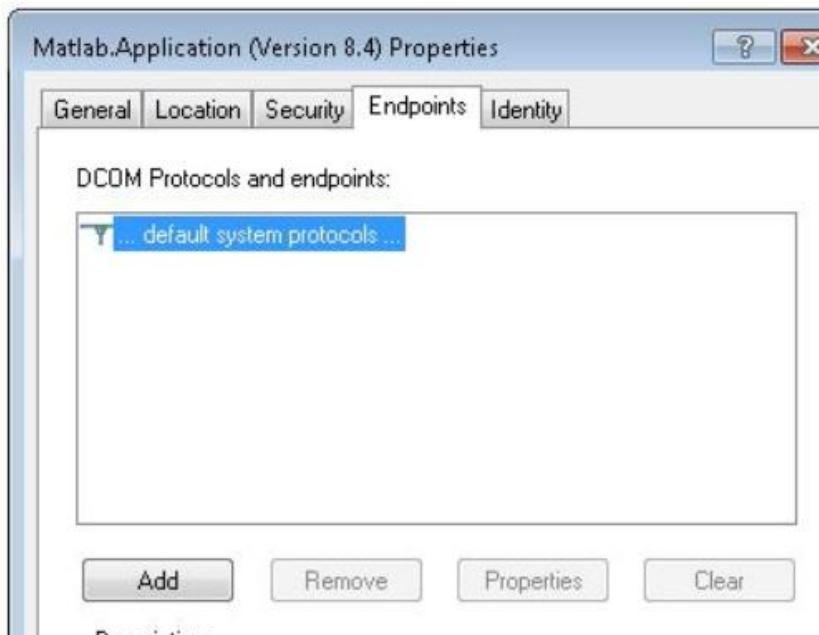
Note: These settings may not be necessary for the RSLINX folder and depends on the environment.

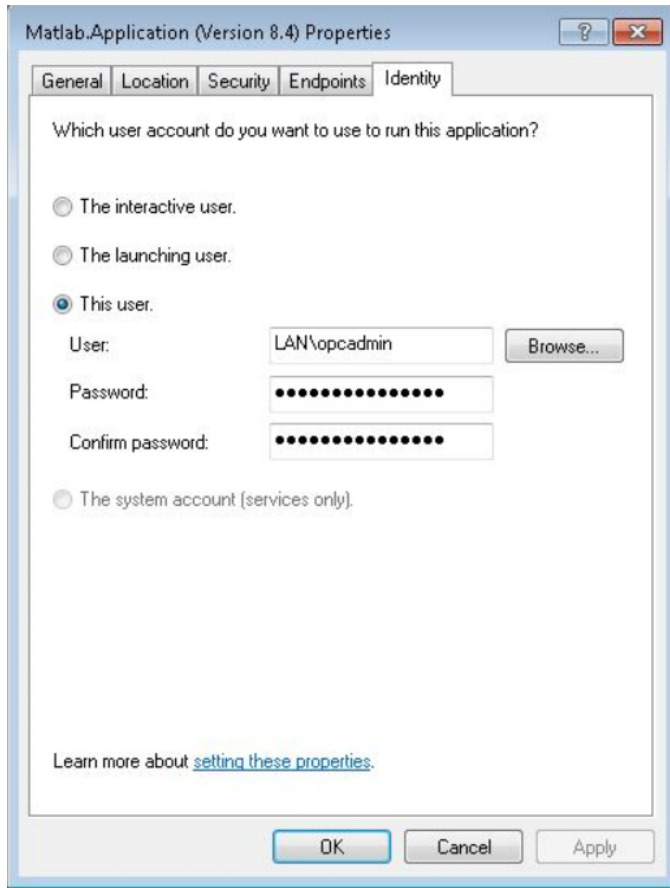


4065
40664067
4068



4069

4070
4071
4072
4073
4074
4075



4076
4077

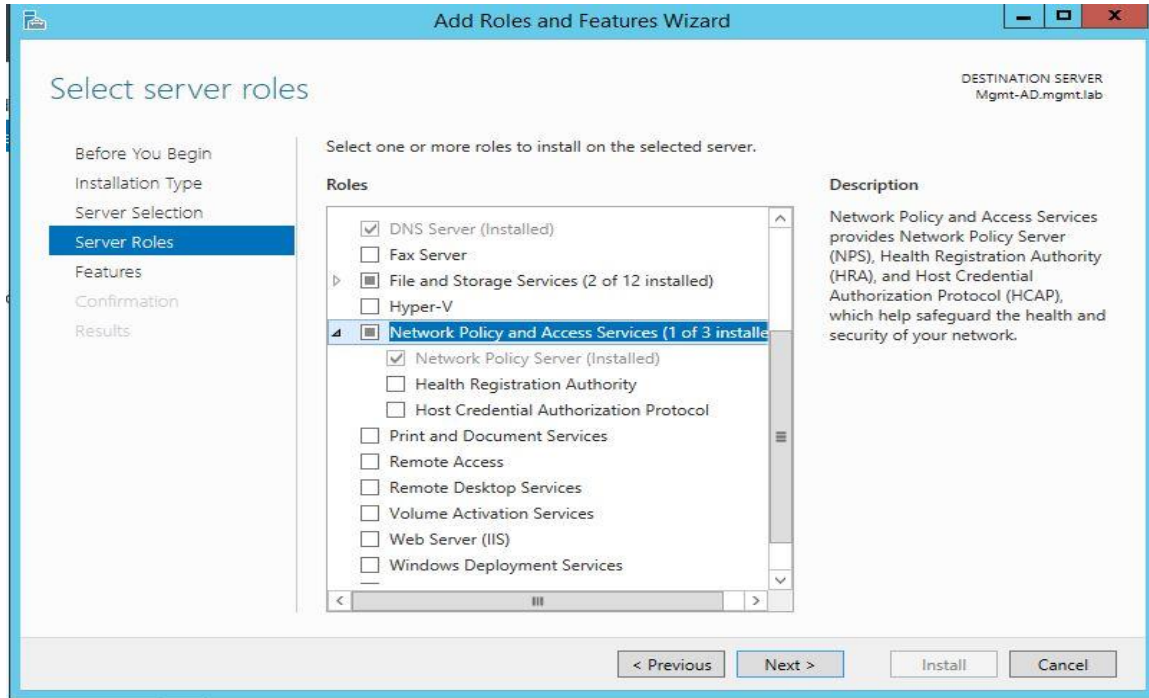
4078 Radius Server Setup

- 4079 • A Windows 2012 R2 server running Active Directory and Windows Network Policy Server
4080 (NPS) was setup in the Management LAN to authenticate the boundary firewall and VPN
4081 users. Technically both the roles can be on the same server but its recommended to keep
4082 them separate for redundancy.
- 4083 • High level setups
 - 4084 ○ Setup the AD Server
 - 4085 ○ Create an AD Domain
 - 4086 ○ Setup the Radius Server
 - 4087 ○ Join Radius server to the AD Domain
 - 4088 ○ Register Radius Server with AD
 - 4089 ○ Register Radius Server with AD

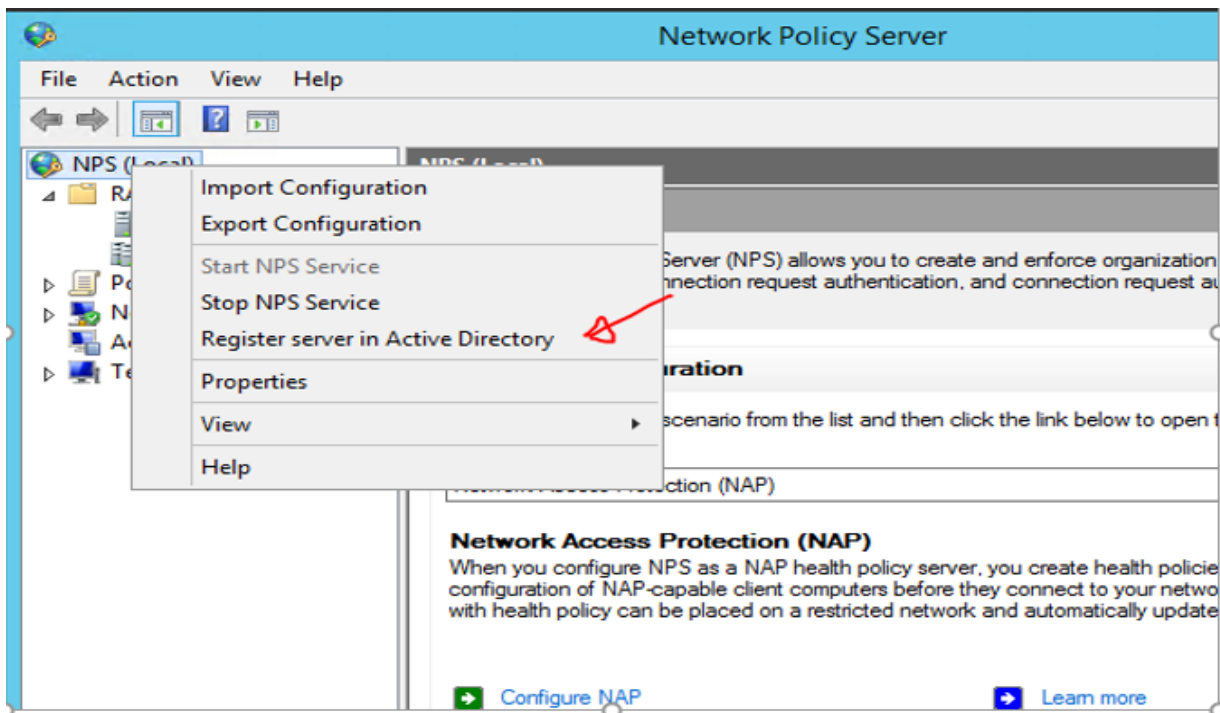
4090 Details of the AD Server and Domain in Management Network

Hostname	IP address	Roles	Domain Name
Mgmt-AD	10.100.2.3	Active Directory, DNS, Network Policy Server (Radius)	Mgmt.lab

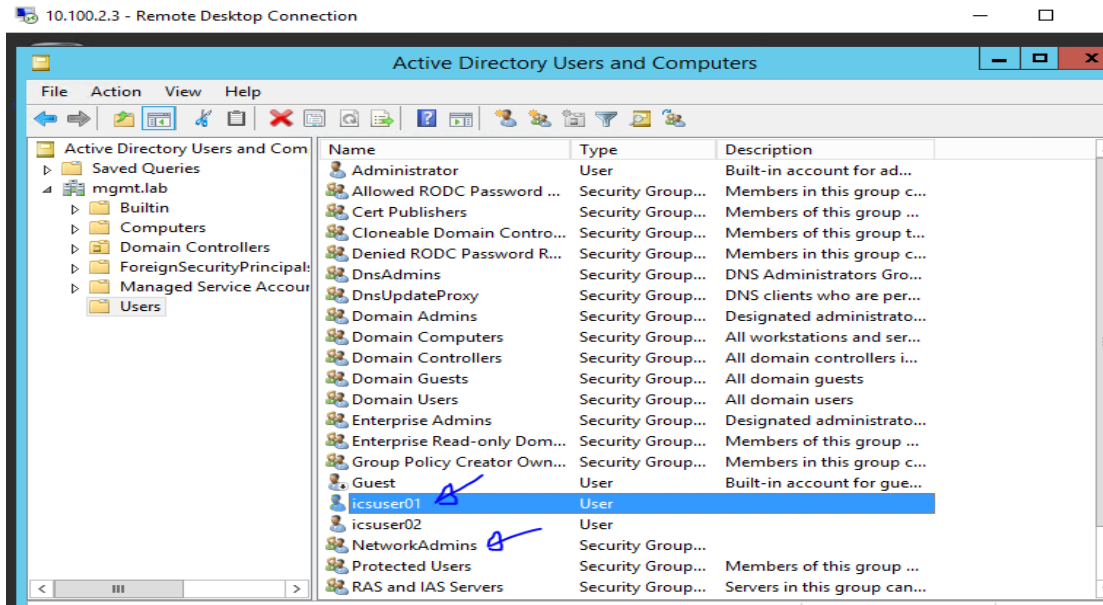
- 4091 • To setup Radius services on Windows 2012 R2, install the **Network Policy Server** role. This
4092 can be done from **Server Manager >> Add Roles and Features Wizard** as shown below



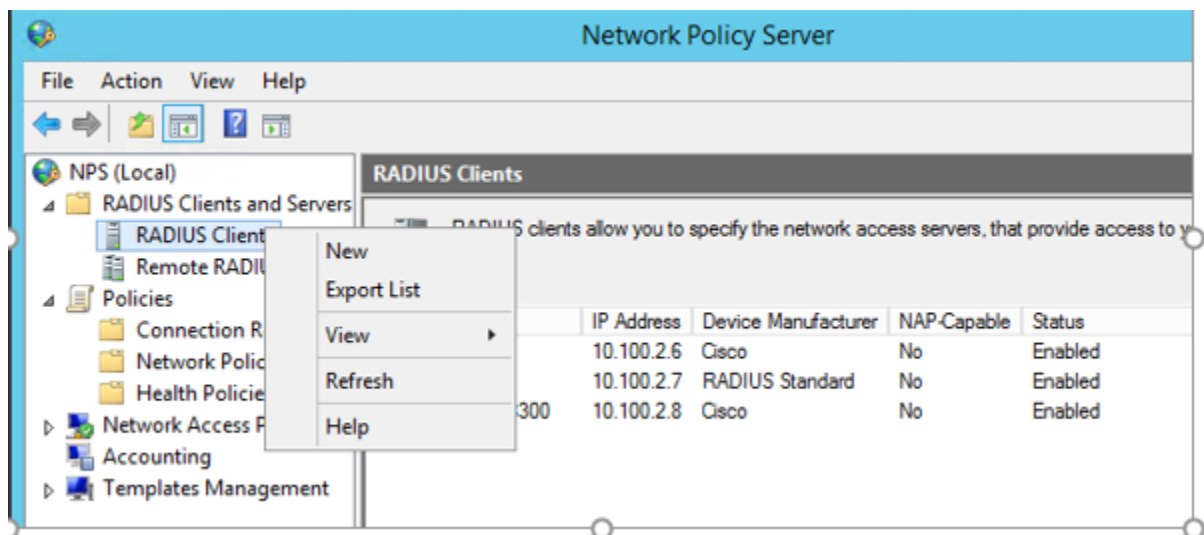
- 4093
- 4094 • Open the Network Policy Server Console, Click on **Register Server in Active Directory**
4095



- 4098 • Create user accounts in AD. A User account called “**icsuser01**” and a Security Group “**Network**
4099 **Admins**” were created in our **Mgmt.lab** domain. The **icsuser01** user was added to the Network
4100 Admins group.
4101



- 4102 • Create Radius Clients and Policies in NPS:
4103
4104
4105
4106
4107
4108 ○ Launch the **Network Policy Server** snap-in to create a Radius client for the Network
4109 Device you did like to integrate. A Radius client was created for the Boundary Firewall
4110 (Allen Bradley) of the Process Control System.
4111



- Enter a matching name of the Network Device, IP address of the management interface and create a “passphrase “. Hit OK when done. This will create the Radius client. Make sure you can ping the Management IP of the network device from the Radius server

The screenshot shows the 'AllenBradley8300 Properties' dialog box with the 'Advanced' tab selected. The 'Settings' tab is also visible. The 'Enable this RADIUS client' checkbox is checked. Below it is a 'Select an existing template:' dropdown menu. The 'Name and Address' section contains a 'Friendly name:' field with the value 'AllenBradley8300' and an 'Address (IP or DNS):' field with the value '10.100.2.8'. A 'Verify...' button is next to the address field. The 'Shared Secret' section has a 'Select an existing Shared Secrets template:' dropdown menu with the value 'None'. Below this is a text box explaining that to manually type a shared secret, the 'Manual' radio button should be selected, and to automatically generate a shared secret, the 'Generate' radio button should be selected. The 'Manual' radio button is selected. Below the radio buttons are two text boxes for the shared secret, both containing a series of dots.

AllenBradley8300 Properties

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:

AllenBradley8300

Address (IP or DNS):

10.100.2.8 Verify...

Shared Secret

Select an existing Shared Secrets template:

None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

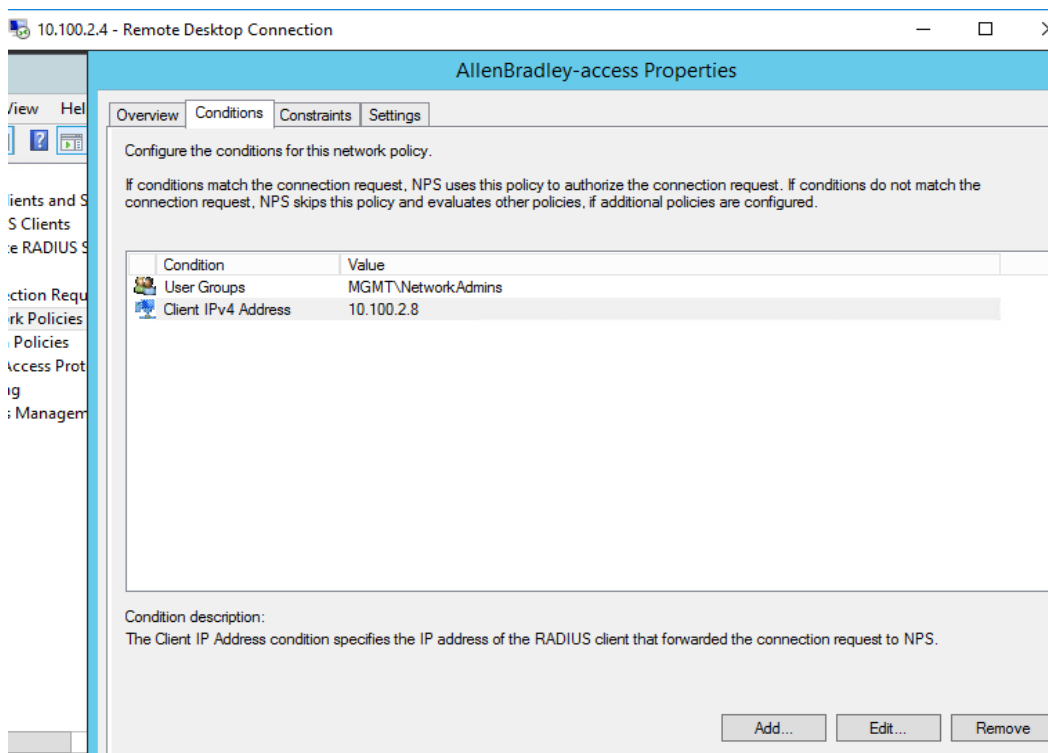
Shared secret:

Confirm shared secret:

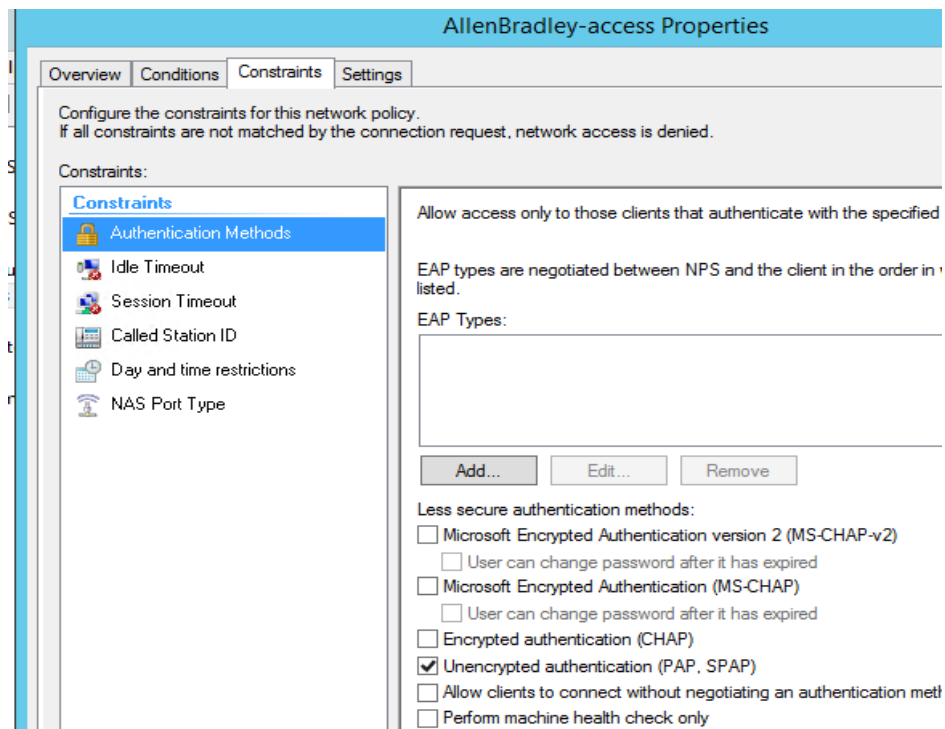
- 4123 ○ Next, under Policies >> Network Policies >> Create a new policy for the radius client.
4124 The below image shows the network policy created for the Allen Bradley firewall

The screenshot shows the 'AllenBradley-access Properties' dialog box. The 'Overview' tab is active. The 'Policy name' field contains 'AllenBradley-access'. The 'Policy State' section shows 'Policy enabled' checked. The 'Access Permission' section shows 'Grant access' selected. The 'Network connection method' section shows 'Type of network access server' selected with a dropdown menu showing 'Unspecified'.

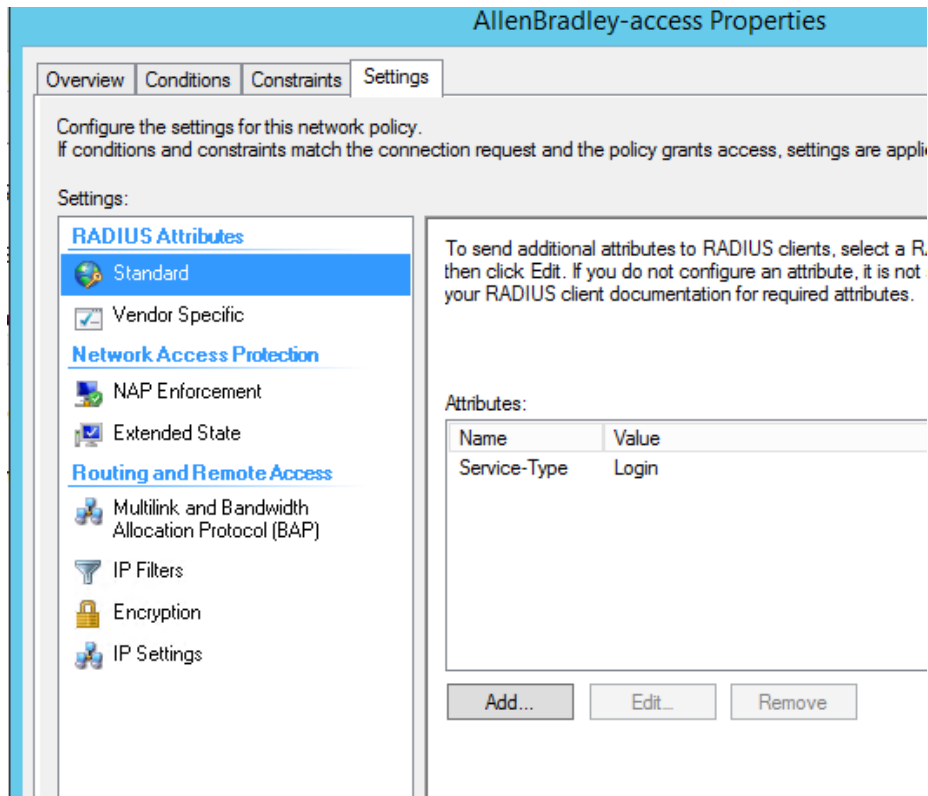
- 4125
- 4126 ○ Under “Conditions”, click on the ADD button, look for “user/groups option”, select the
4127 “Network-Admins” security group we setup earlier in our AD. This will allow users
4128 from this group to login as admins for managing the switch. Also add another condition
4129 to check for the IP address of our Allen-Bradley. Look for “Client IPv4 address”
4130 option, enter the IP address of our Allen-Bradley and add it. Below is how the
4131 Conditions page should like once both conditions are added. Hit Next to proceed to the
4132 next screen.
4133



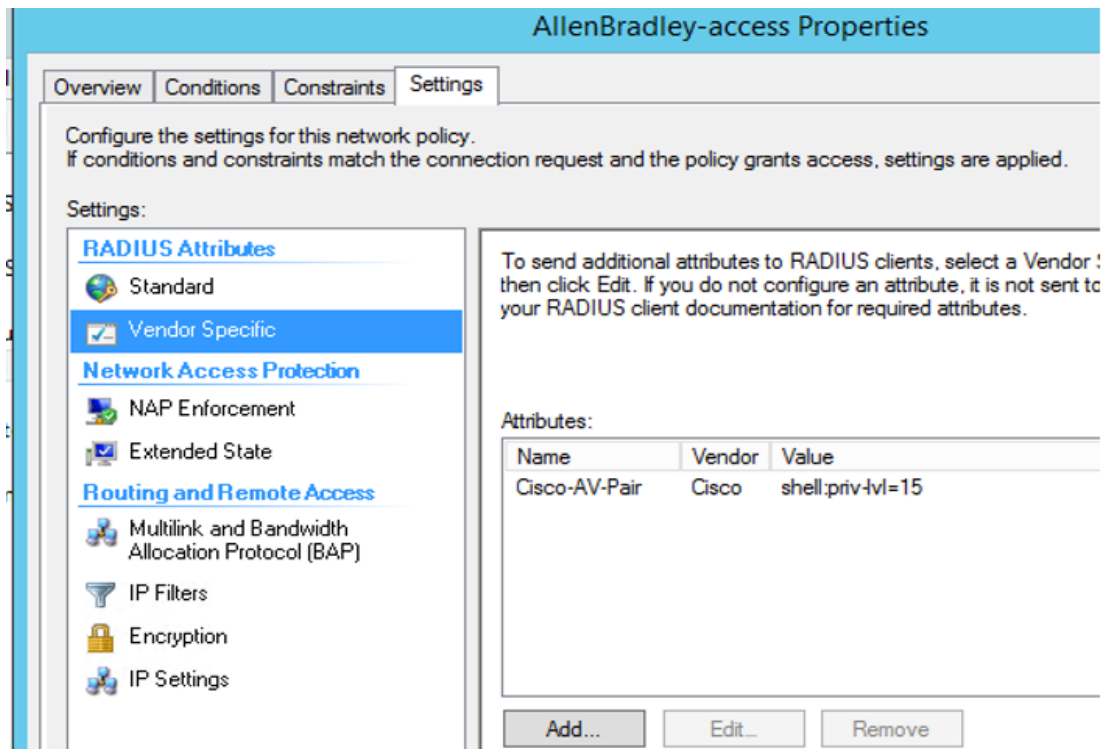
- Under Authentication methods choose the “**PAP, SPAP**” method as Cisco IOS supports these ones. Click **Next** to proceed to the Settings page.



- Under **Settings >> Radius Attributes >> Standard** >> Remove the 2 default attributes. Click **ADD** to add a new attribute with **Name = “Service-Type”** and **Value = “Login”** as shown below.



- Under Vendor Specific Attributes, add a new attribute by selecting “Cisco-AV-pair” from the list, Vendor= “**Cisco**” and value = “**shell:priv-lvl=15**”. This will allow the user to login with privilege level =15 meaning admin privileges. Click on **OK/Apply** button to save the changes



- Configuring Boundary Firewall for Radius Authentication:
 - The following commands were run on the Allen Bradley Boundary firewall to enable it to authenticate against the above Radius server.

```
# enable
# configure terminal
# aaa new-model
# aaa authentication login default group radius local
# aaa authorization exec default group radius local
# radius server host <IP address of our radius server>
# radius server-key <passphrase>
# quit
# wr mem
```

4167 **4.9.6 Highlighted Performance Impacts**

4168 The following performance measurement experiment was performed for the Active Directory
4169 service while the manufacturing system was operational:

4170 PL002.1 Active Directory service active with non-OPC accounts being configured as non-
4171 Administrator privilege.

4172 There was no performance impact to the manufacturing process observed during the experiment.
4173 However, performance impact was observed at the implementation of the Active Directory (AD)
4174 service. At the initial implementation, the team focused on the Active Directory installation and
4175 user configuration, but not knowing the need for DCOM configuration initially, causing
4176 unplanned production interruption. DCOM and user account configuration for every OPC client
4177 have to be modified to use AD instead of local authentication. Without modification, the OPC
4178 client failed to communicate with the OPC DA server and caused all OPC data exchange to cease
4179 operation. This failure caused the manufacturing process entered the emergency shutdown state.

4180 Another impact observed at implementation was the **time synchronization** source with the AD.
4181 Authentication failed due to time discrepancy between hosts and AD. It is because the hosts were
4182 synchronized to a different time source than the AD and the time difference was greater than 5
4183 minutes. When the host joins the AD domain, each host should use the same time source as AD.
4184 For example, all hosts in PCS use AD as the time source, and AD uses an external NTP server as
4185 its time source.

4186 Care should be taken to ensure proper operation of the Active Directory service. Failure in
4187 authentication causes error in operation of the OPC server, which handles all the data exchange
4188 of the controller and the plant operation. The manufacturing process entered emergency
4189 shutdown state because the controller lost the ability to communicate to the sensors and
4190 actuators. Redundancy and backup is highly recommended. Ability to switch between primary
4191 and secondary AD should be seamless to avoid impact to the system.

4192 There was no significant impact to the network performance observed. For example, the round
4193 trip time from OPC to HMI is mostly the same with the Active Directory.

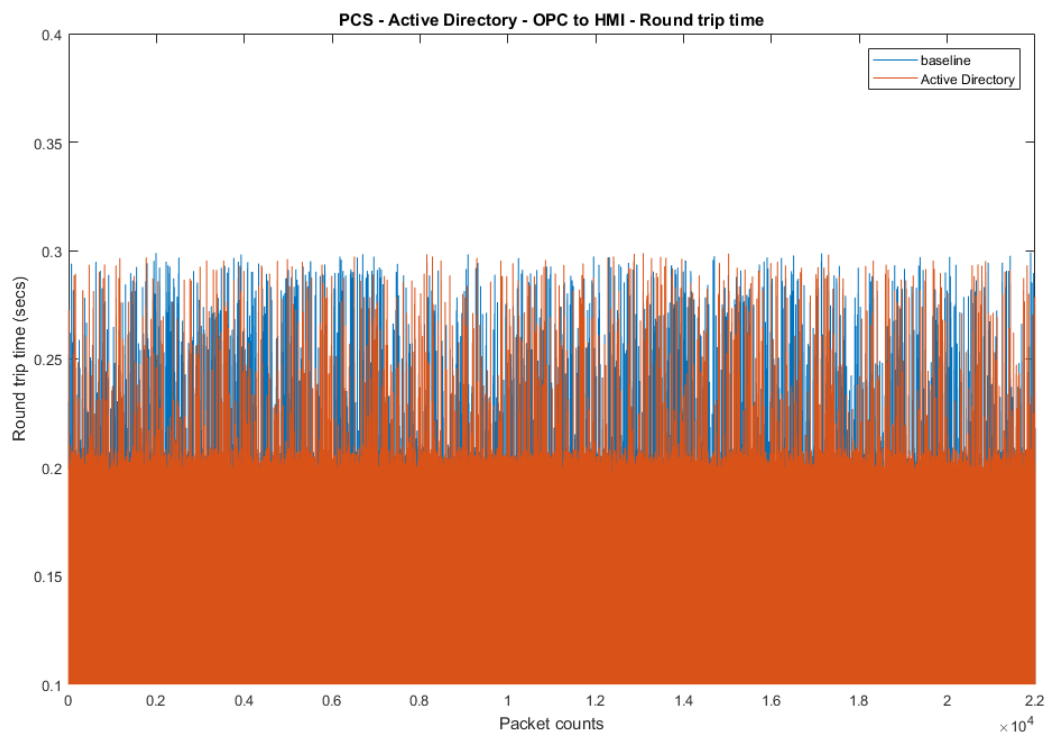
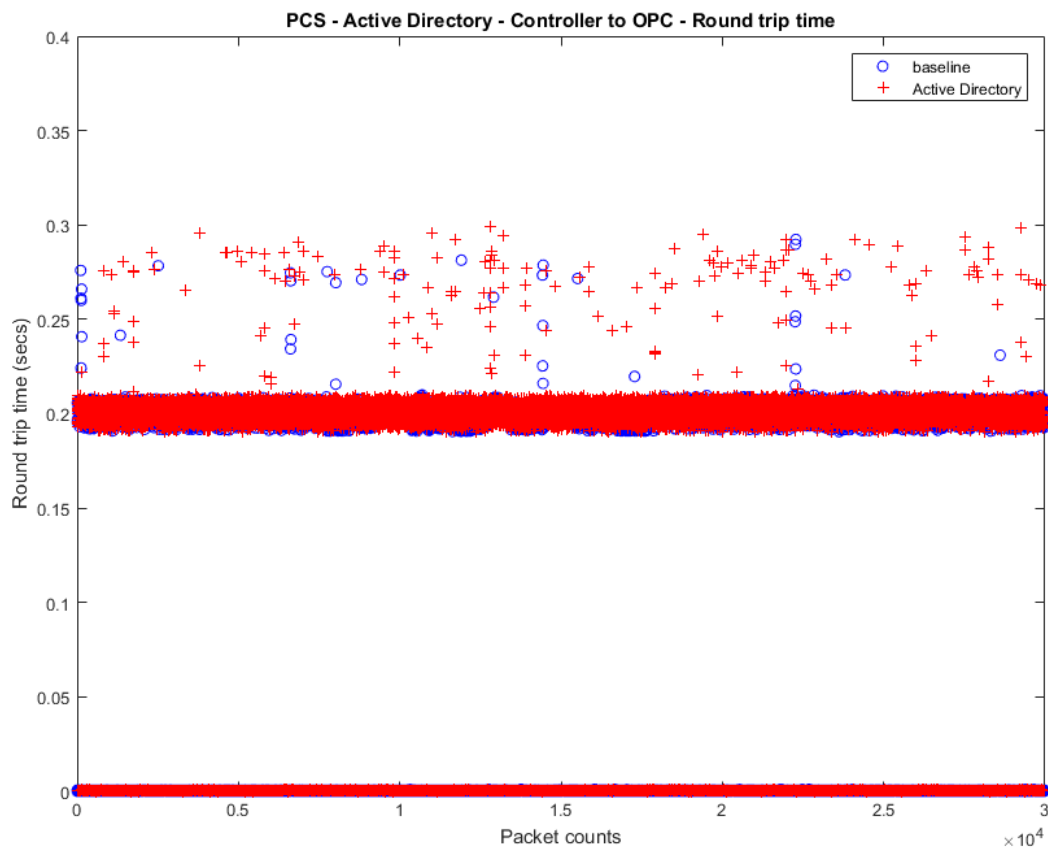


Figure 4-16 Packet round trip time from OPC to HMI with Active Directory.

The controller is another major component required modification to use Active Directory. The Controller authenticates against the AD server. The controller also has the updated DCOM so that it can continue to communicate with the OPC server. The packet round trip time from the Controller to OPC was slightly elevated, with a small number of packets had a slightly increased round trip time. There was no significant increase in inter packet delay from the Controller to OPC observed.



4203

4204

Figure 4-13 Packet round trip time from Controller to OPC with the Active Directory enabled (red)

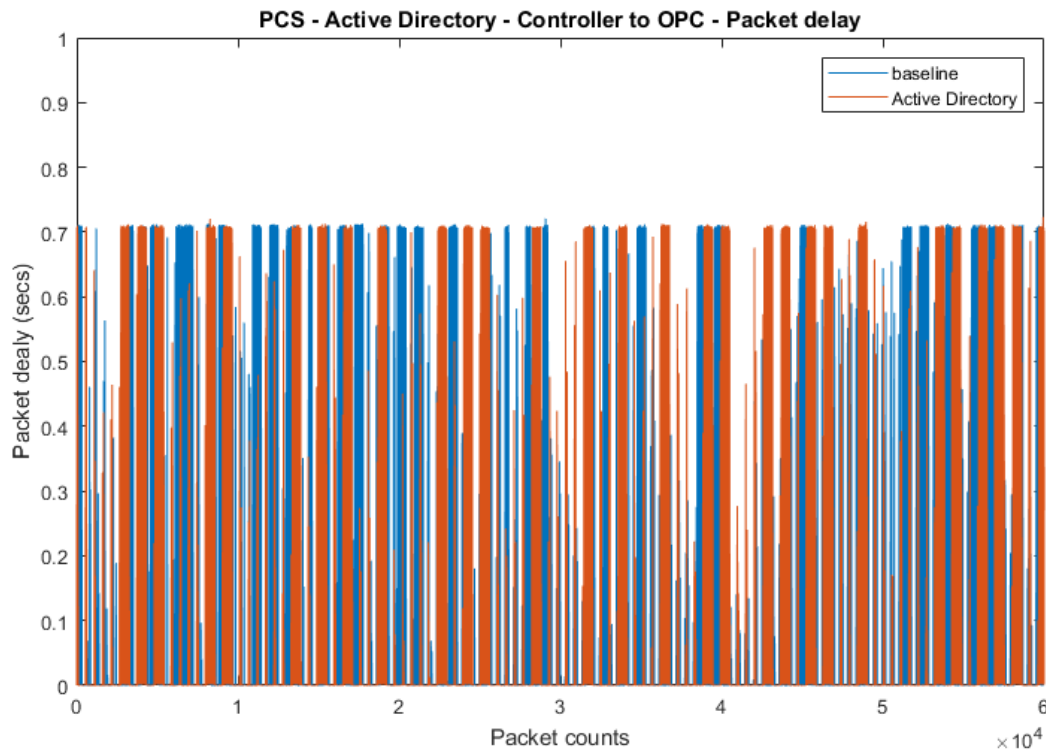


Figure 4-14 Inter packet delay of Controller to OPC with the Active Directory enabled (red)

There was no significant performance impact to the manufacturing process observed with the use of Active Directory. For example, the product flow rate remained consistent with and without the use of Active Directory.

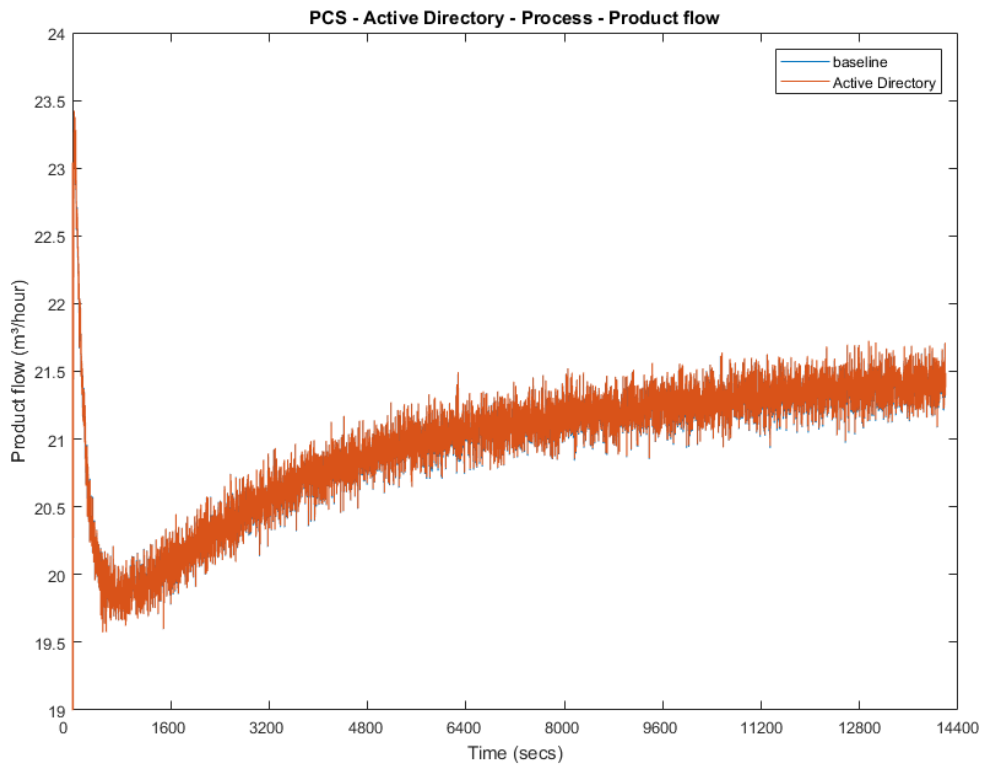


Figure 4-19 Manufacturing process product flow rate during the use of Active Directory (red)

A misconfiguration on the Active Directory cased the manufacturing process to enter the emergency shutdown state in about 600 seconds of the experiment time due to the reactor pressure too high

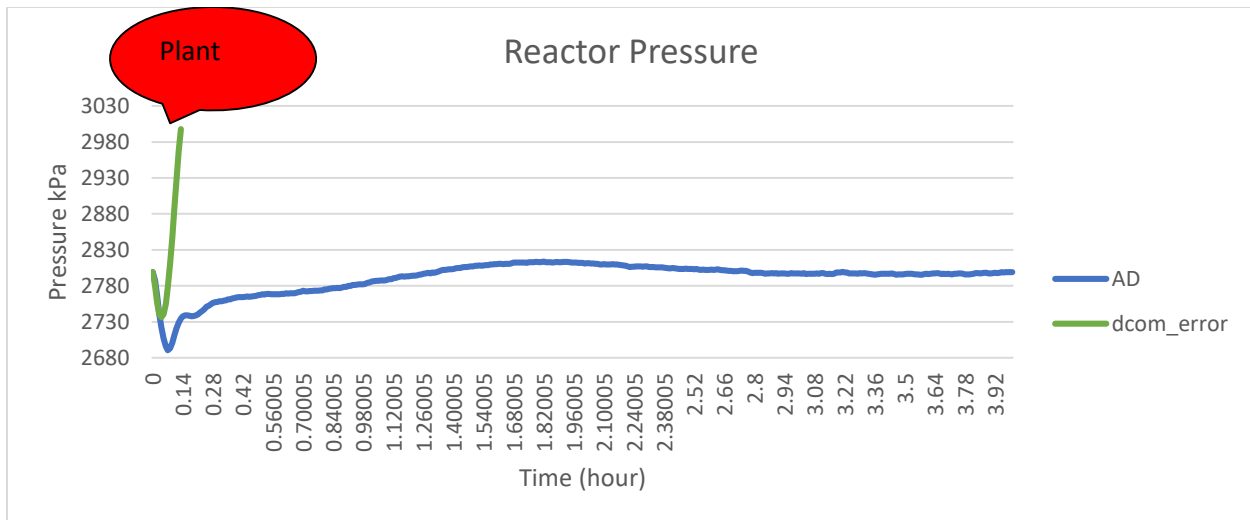


Figure 4-20 Plot of the manufacturing process reactor pressure. The process entered emergency shutdown mode when DCOM communication failed.

4219

4220 **4.9.7 Link to Entire Performance Measurement Data Set**

4221 [Active Directory KPI data](#)

4222 [Active Directory measurement data](#)

4223

4224 4.10 Symantec Endpoint Protection

4225 4.10.1 Technical Solution Overview

4226 Symantec Endpoint Protection:

4227 Symantec Endpoint Protection (SEP) is a complete endpoint protection solution from Symantec.
4228 It delivers superior, multilayer protection to stop threats regardless of how they attack your
4229 endpoints. SEP integrates with existing security infrastructure to provide orchestrated responses
4230 to address threats quickly. Its lightweight SEP agent offers high performance without
4231 compromising end-user productivity. SEP also defends against ransomware and other emerging
4232 threats with multilayered protection that fuses signatureless technologies like advanced machine
4233 learning, behavior analysis and exploit prevention with proven protection capabilities like
4234 intrusion prevention, reputation analysis and more.²²

4235

4236 Points to Consider:

- 4237 • Next Generation Antivirus / Endpoint protection solution to prevent against virus attacks
4238 and emerging cyber threats such as zero-day attacks, ransomware etc.
- 4239 • OS Platform independent: The endpoint agents are supported on Windows and Linux.
- 4240 • Comes with a lightweight agent and virus definition sets that require minimal network
4241 bandwidth.
- 4242 • Diverse Feature set: Core capabilities include Antivirus, Host Firewall, Intrusion
4243 Prevention, Host Integrity, System lockdown, Application White listing and USB Device
4244 Control.
- 4245 • Centralized Management: All endpoints, rule sets, policies can be centrally managed from
4246 the Symantec Endpoint Manager console.
- 4247 • The Symantec Manager component is supported only on Windows OS.
- 4248 • The Linux agent requires the OS kernel on Linux systems to be at a certain level for
4249 installation. In addition, the Linux agent is a 32-bit installer. If installing on a 64-bit Linux
4250 system, it requires certain 32-bit packages/libraries to be installed as a pre-requisite. This
4251 may conflict with some of the existing packages on the system.
- 4252 • The endpoint agent on each system by default needs to communicate outbound with a range
4253 of public IP addresses for its Reputation analysis and Global Threat intelligence feature. It is
4254 recommended to allow this traffic from your firewall to leverage the advanced features of
4255 the product.
- 4256 • **Important:** System reboot is required to complete the installation process on
4257 clients/endpoints. Plan ahead of time.

²² Symantec Endpoint Protection: <https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-14-en.pdf>

4258

4259

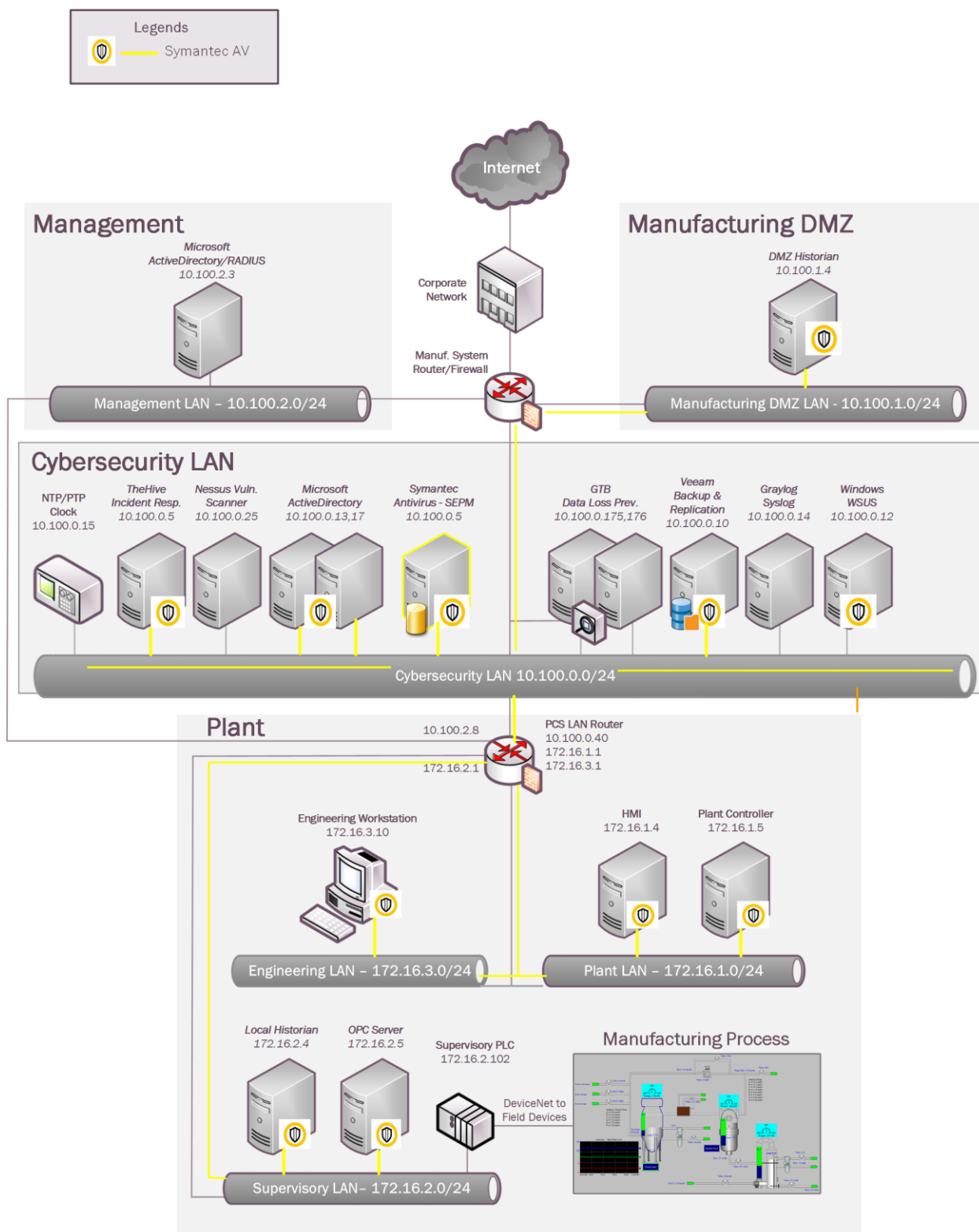
4260 **4.10.2 Technical Capabilities Provided by Solution**

4261 Symantec Endpoint Protection provides components of the following Technical Capabilities
4262 described in Section 6 of Volume 1:

- 4263 • Anti-virus/malware

4264 **4.10.3 Subcategories Addressed by Implementing Solution**

4265 PR.AC-1, DE.CM-3, DE.CM-4

4266 **4.10.4 Architecture Map of Where Solution was Implemented**

4267

4.10.5 Installation Instructions and Configurations**Setup Overview:**

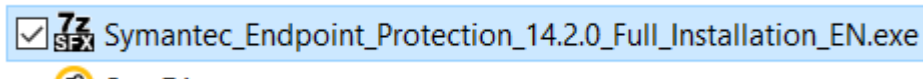
Setup consists of a single Symantec Endpoint Protection Manager (SEPM) instance in the Cybersecurity LAN network. This central instance communicates with all the endpoint agents deployed on to the Process Control systems. Likewise, all endpoints report their status to the Manager server. The communication ports required to be opened are different for Windows clients as compared to Mac/Linux clients. Detailed list of firewall ports can be obtained from Symantec website. The SEP Manager server downloads its daily signature updates from the Symantec cloud servers, so this necessary traffic was allowed to pass thru the Manufacturing System Firewall.

Details of the software used

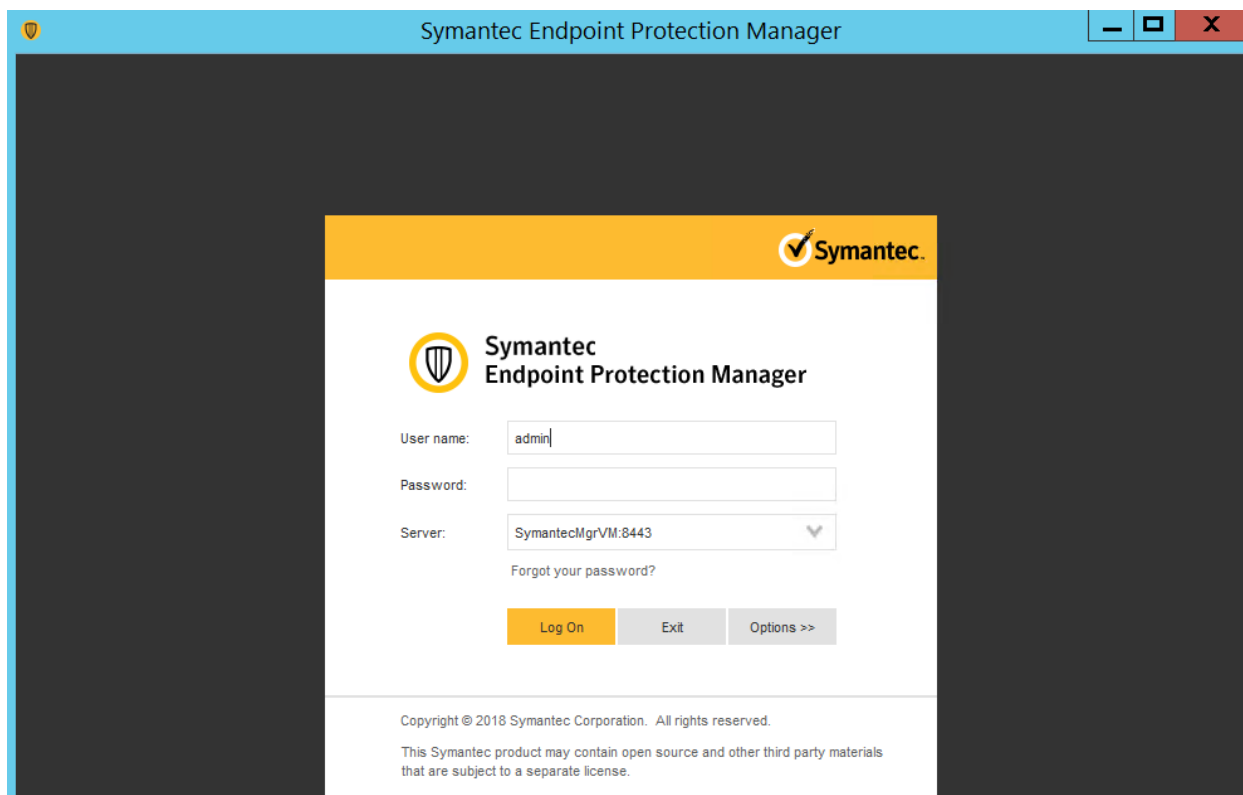
Product Name	Version
Symantec Endpoint Protection Manager (SEPM)	14.2 Build 758
Symantec Endpoint agent for Windows (Client)	14.2.758.0000

Installation of SEP Manager:

- SEPM is supported only on Windows server platforms. A Windows Server 2012 R2 virtual machine was setup in the Cybersecurity LAN to install the SEPM component.
- Upon purchase, there will be a license file emailed to you along with the link to download the install binaries. Download the zip bundle from the Symantec website. Extract the zip file which will be like the one below depending on whatever is the latest version available.



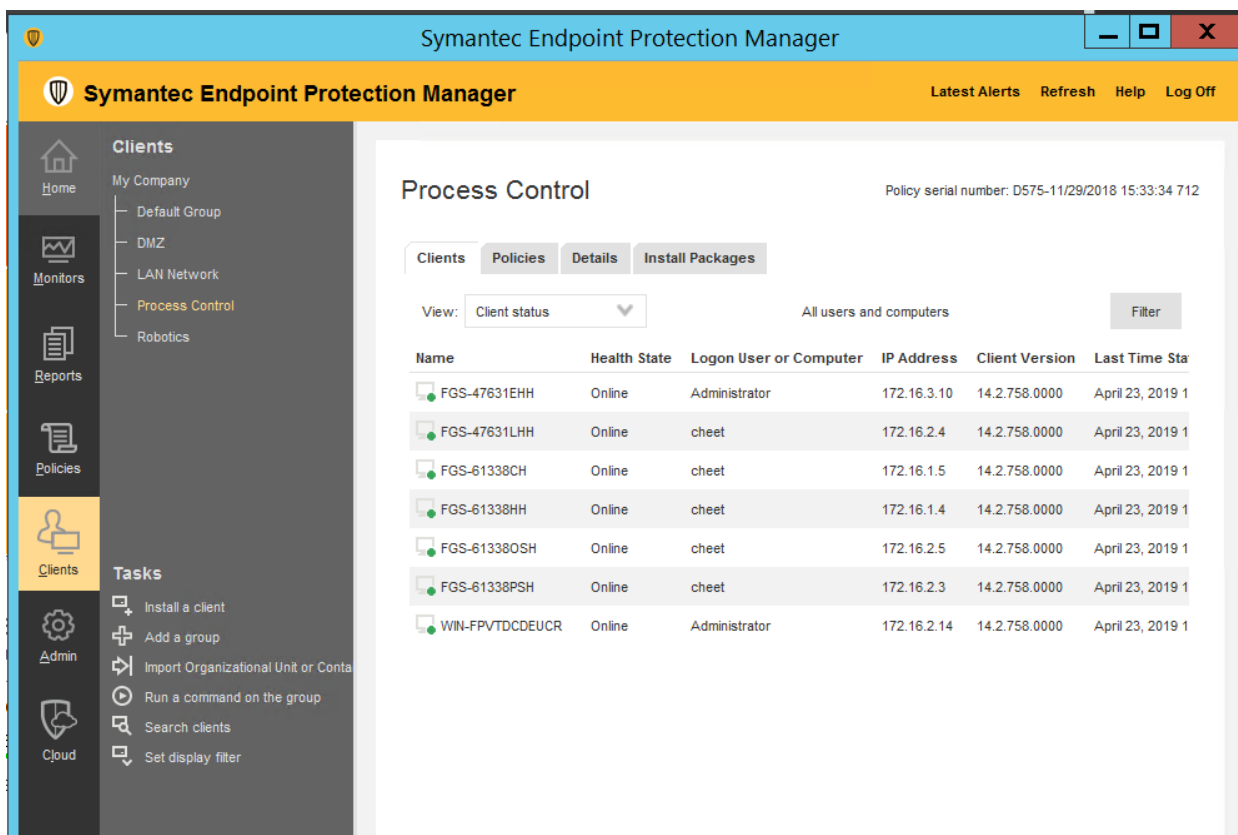
- Open the extracted folder and run the **Setup.exe** file. Mid-way during the setup, the install wizard will prompt to select a password for the admin user. Enter a strong password and hit **Next**.
- On the **Backed Database** selection page, there are two options - "**Embedded**" and "**MS SQL Server**". Choose the **Embedded database** if you do not have a MS SQL Server. Follow the on-screen instructions and complete the installation wizard. Reboot the server once done.
- Launch the SEP Manager console and login with the admin user created earlier.



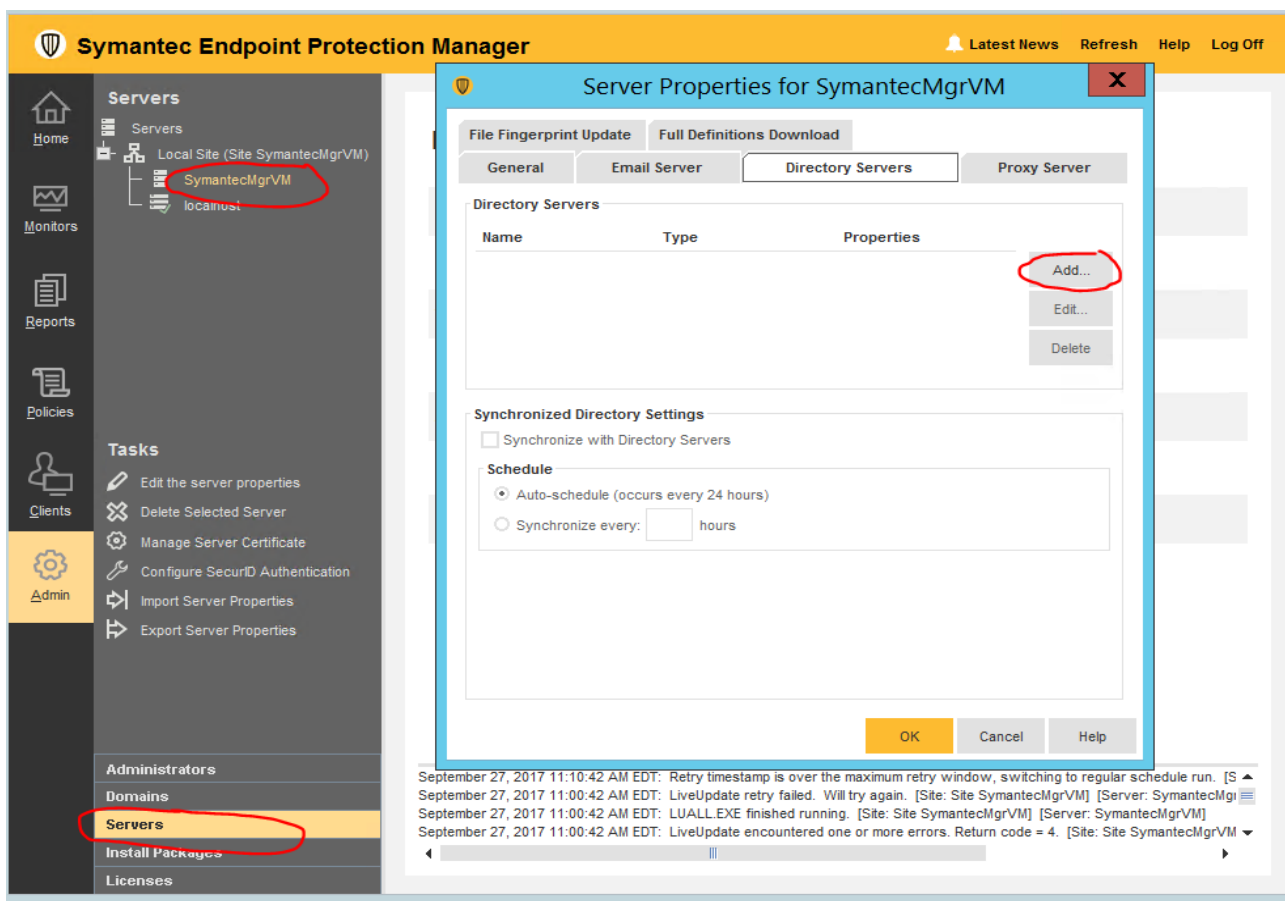
- Upon completing the installation of Symantec Endpoint Manager, the next steps are to activate the license, configuring client groups to group devices and installing the antivirus agent on each endpoint/client system.
- Link to Official Symantec Endpoint Protection v14 installation guides - https://support.symantec.com/en_US/article.DOC9449.html
- Ensure to open the necessary ports on the firewall for communication between the SEPM server and endpoints. A complete list of ports is available at https://support.symantec.com/en_US/article.HOWTO81103.html

Custom Configuration of SEPM server

- The following client groups were created to group devices from each of the systems. Upon installing the AV agent on the endpoints, the devices were moved to their respective groups.



- For integrating SEP Manager with AD/LDAP server, click on **ADMIN >> Servers >> Local Site >> <Server Name> >> Edit Server Properties >> Directory servers**. Click further on “**ADD**” button as shown below to configure domain details. Once done, logout and try logging in back with your AD credentials.



- Similarly, Email server can be configured by clicking on the “Email Server” tab.

Getting started with Endpoint installs

High level steps:

- Create a deployment package specific for a client group
- Deploy the package from the SEPM server to the endpoint using Network Deployment options or manually copy over the package to the endpoint for installation.
- Restart the endpoint. Verify the device shows up in the SEPM console.

Creating a deployment package:

- Login to the Symantec Manager console, click on **CLIENTS** >> <Group Name> where the device needs to be in >> Click on **Install client under TASKS**. For instance, to create a deployment package for the group “**Process Control**”, click on that group name followed by **Install Client** option.
- Select “**New Package Deployment**” if this is your first agent installation of that group. If you have already deployed the agent on other systems of this group, you can re-use the same package and skip this wizard completely.

Client Deployment Wizard

Select Deployment Type Symantec.

Welcome to the Client Deployment Wizard

Use this wizard to install the protection client on computers in your network or update existing client communication settings.

? Click to view the Install Client tour

Note: For instructions to install the client on a computer that runs Symantec Mail Security or Symantec Scan Engine, see the Symantec Technical Support knowledge base article:

? Click here

☒ New Package Deployment

Select packages from the server and specify client group and features.

☐ Existing Package Deployment

Choose from previously exported packages that are located on your hard drive.

Browse...

Communication Update Package Deployment

Create a package that changes the communication settings on an existing Symantec Endpoint Protection client installation. Use this option to restore communication between the client and Symantec Endpoint Protection Manager, to connect the client to a new Symantec Endpoint Protection Manager, or to convert an unmanaged client to a managed client.

☒ Create a package for Symantec Endpoint Protection clients that run on Windows. 🖥️

☐ Create a package for Symantec Endpoint Protection clients that run on Mac. 🍏

< Back Next > Cancel

- Click “Next” >> Choose the appropriate OS Platform as per the endpoint OS, from the dropdown list of **Install Packages**. You will notice the Group Name is already pre-populated. This ensure the client will be placed directly in that group upon install. Under **Content Options**; Select “**Include virus definitions in the client installation package**” [optional]. Click **Next**.

Client Deployment Wizard

Select Group and Install Feature Sets Symantec

Install Packages:

- Windows - Symantec Endpoint Protection version 14.2.758.0000 - English
- Windows - Symantec Endpoint Protection version 14.2.758.0000 - English**
- Mac - Symantec Endpoint Protection version 14.2.758.0000 - English
- Linux - Symantec Endpoint Protection version 14.2.758.0000 - English
- Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English
- Mac - Symantec Endpoint Protection version 14.0.3929.1200 - English
- Linux - Symantec Endpoint Protection version 14.0.3929.1200 - English
- Windows - Symantec Endpoint Protection version 14.0.3892.1101 - English
- Windows - Symantec Endpoint Protection version 14.0.3876.1100 - English

Group: My Company\Process Control **Browse...**

Install Feature Sets: Full Protection for Clients

Recommended for laptops and desktops - Includes all protection technologies.
Some security features are not supported on some platforms. Please refer to product documentation for details.

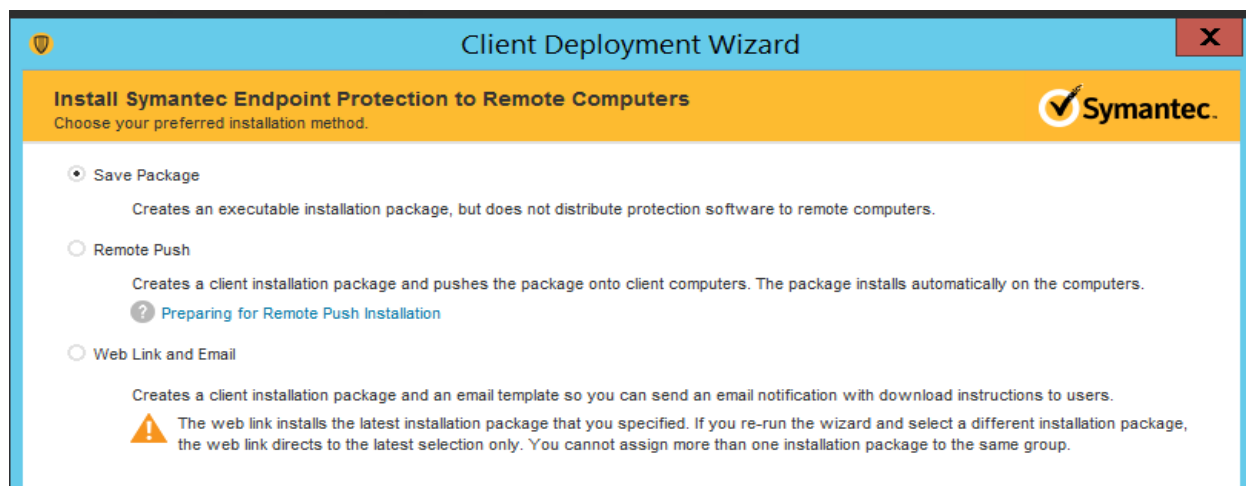
Install Settings: Default Standard client installation settings for Windows **Options...**

Content Options: ☐ Include virus definitions in the client installation package.

Uncheck this option to create a smaller client installation package that does not include virus definitions but does include all other content. After the client is installed, run LiveUpdate immediately on the clients to download the virus definitions.

< Back **Next >** Cancel

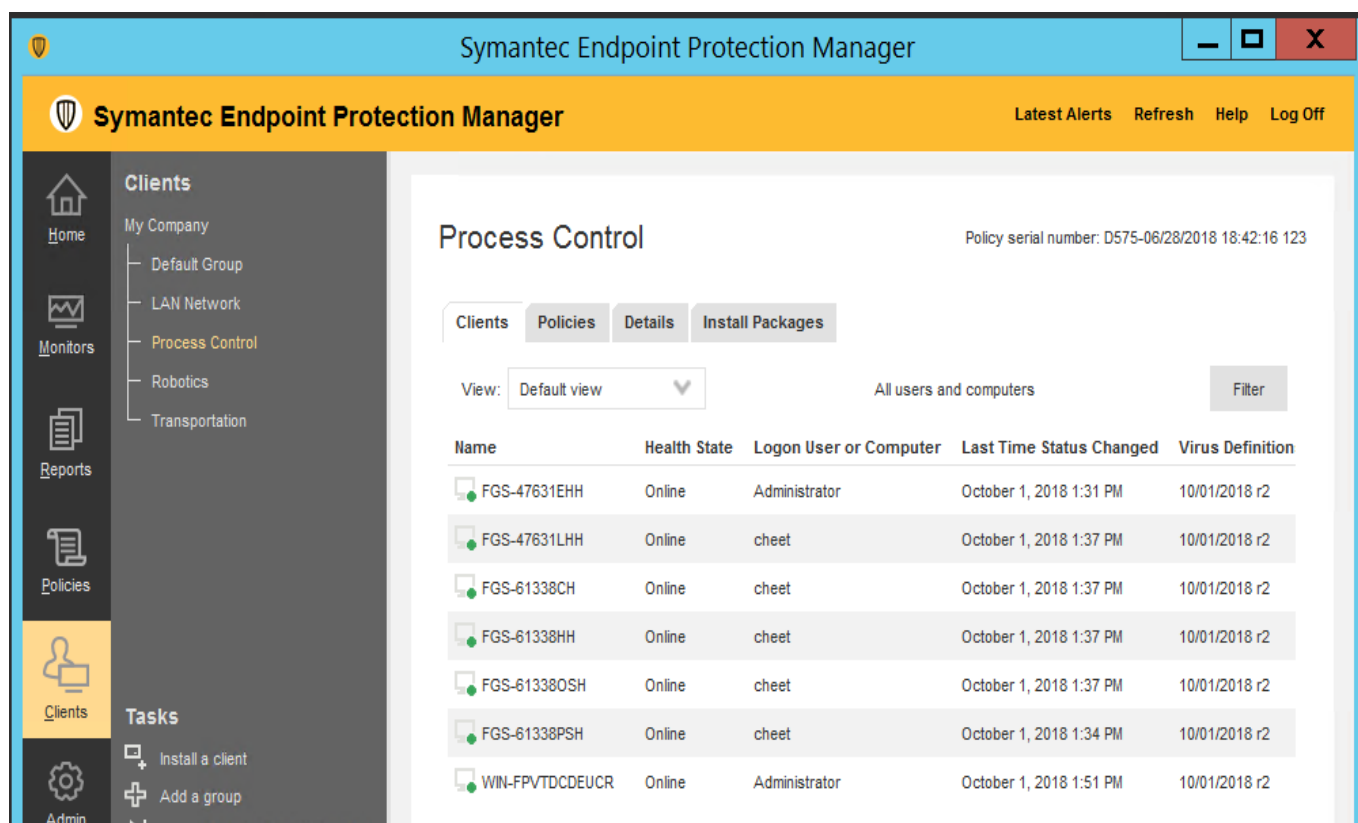
- On the next page, choosing the **“Save Package”** will create a local installer which needs to be copied over the target machine manually and the **“Remote Push”** will make the SEPM server perform a network deployment to the target machine(s). Choose your preferred option and hit **Next**.



4350

4351 **Installing the AV on Process Control System**

- 4352 • An installation package was first created as described in the previous section by selecting
- 4353 “**Process Control**” group and install package as “**Windows**”. The executable installer was
- 4354 then manually copied over to each Windows system in the network and run.
- 4355 • Upon installation, the system requires a **restart**. All systems were rebooted post installation.
- 4356 • The SEPM console on the central server was checked to confirm all the clients from the
- 4357 group were reporting **green ONLINE** and their **Virus Definitions** were current.
- 4358

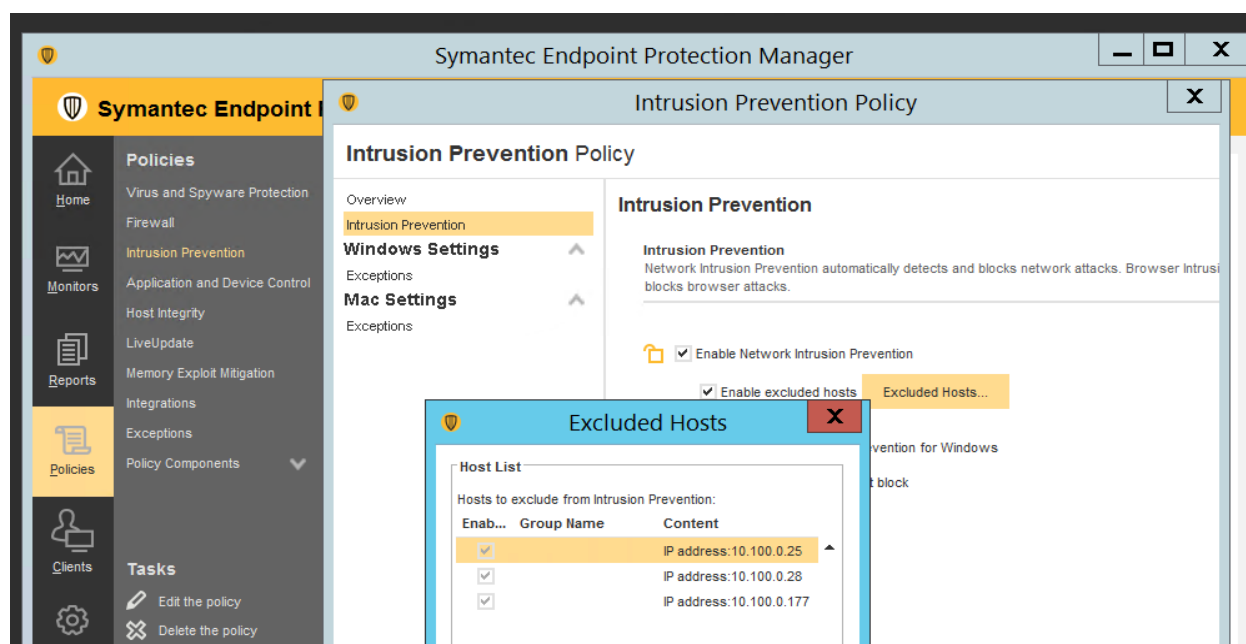


4359

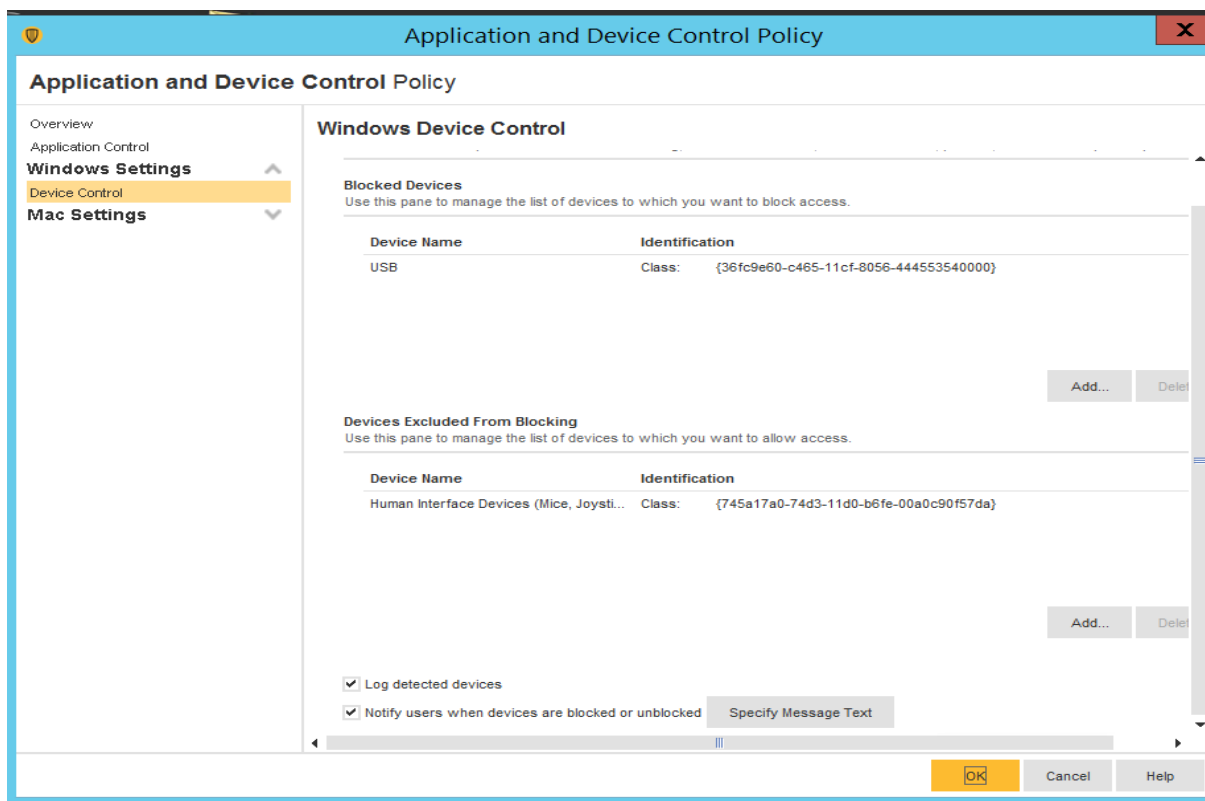
- The official install guide for Windows systems can be found at https://support.symantec.com/en_US/article.DOC9445.html

Additional Configuration

- Symantec AV on each system by default blocks any port scan related traffic. If you have a vulnerability scanner or security tools in your environment, ensure those IP addresses are whitelisted in the SEPM console. The recommended way to do this is by creating a policy under **Policies >> Intrusion Prevention >> Excluded Hosts** and linking it to the appropriate client group. The figure below shows the settings page of excluded hosts.



- To setup device control such as restricting USB devices, create a policy under “**Application and Device Control**”. Detailed instructions can be found [here](#). Below shown image shows the USB policy implemented in our use case.



Lessons learned

- Using Symantec's Firewall: SEP also provides a firewall for clients. Firewall rules control how the client protects the client computer from malicious traffic. When you install the console for the first time, it adds a default Firewall policy to each group automatically. Similarly, a client typically gets default firewall settings if a firewall policy is not configured from the console. Ensure to disable Windows OS or Host OS firewall if using Symantec's firewall.

4.10.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Symantec anti-virus tool while the manufacturing system was operational:

Experiment PL008.2- Symantec AV scan

During the Symantec anti-virus scan, sizeable performance impact was observed on the host processor Utilization. However, no significant performance impact was observed on the manufacturing process. A full Symantec scan can take up a considerable amount of processor power.

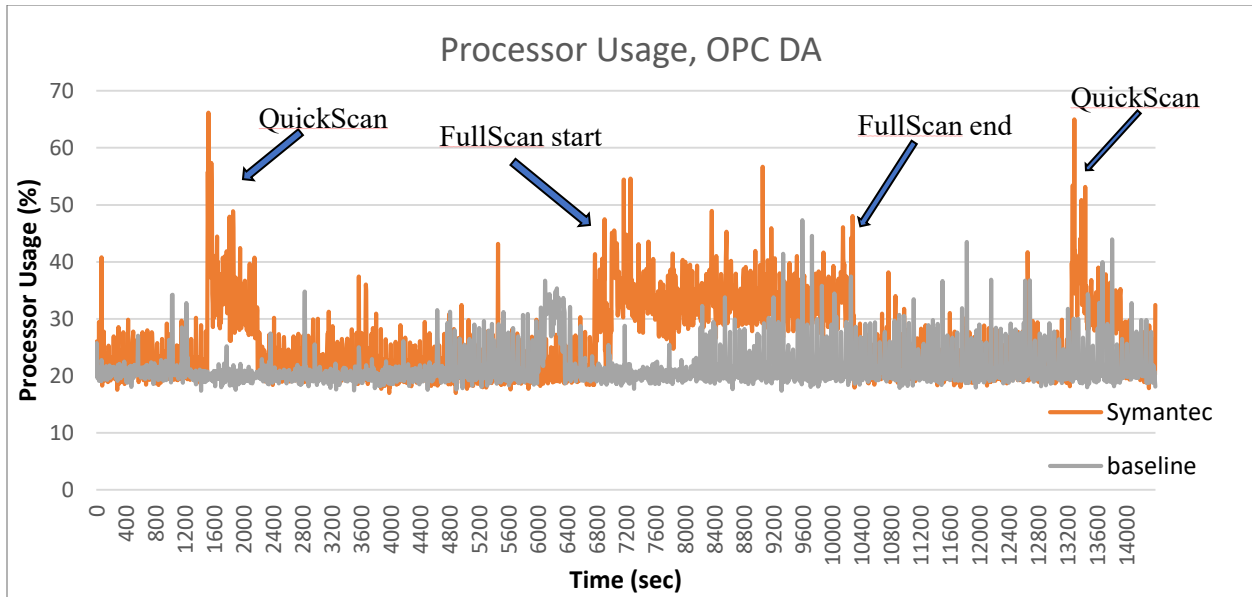


Figure 4-21 Plot of processor utilization of the OPC computer during the Symantec anti-virus scan (Red), and the baseline processor utilization (gray)

No significant performance impact to the network was observed. For example, the packet round trip time between the OPC and PLC remained mostly the same.

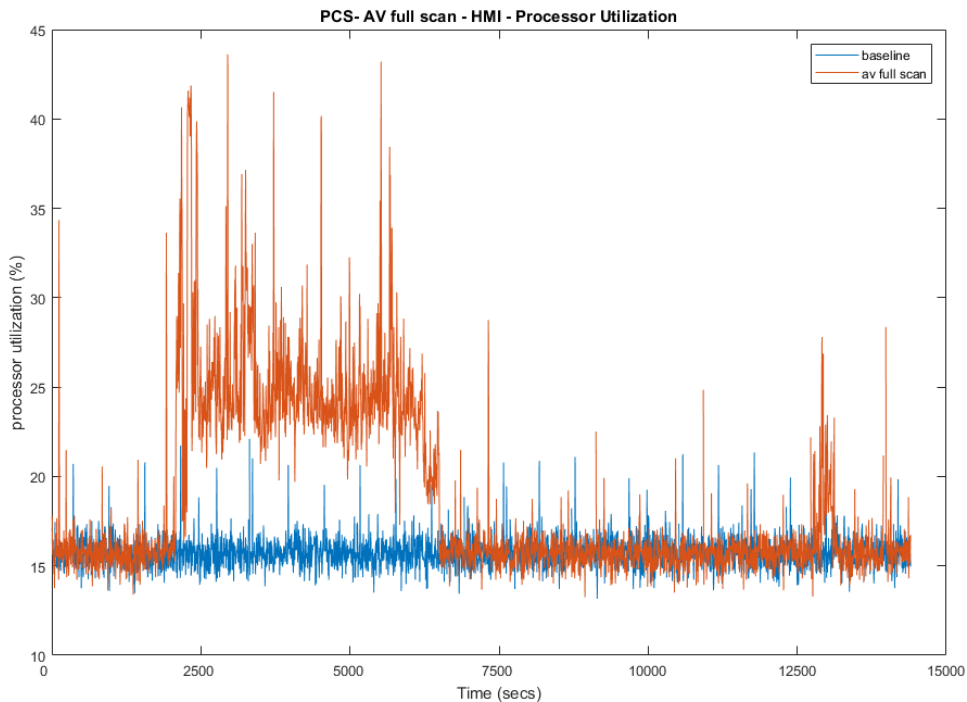
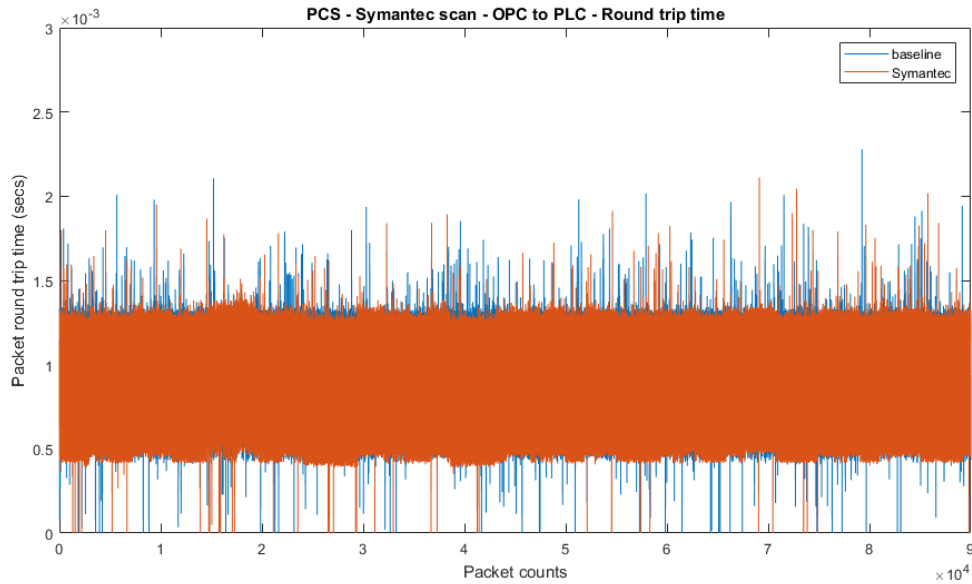


Figure 4-22 Plot of processor utilization of HMI computer during a Symantec scan (red) and without a Symantec scan (blue)

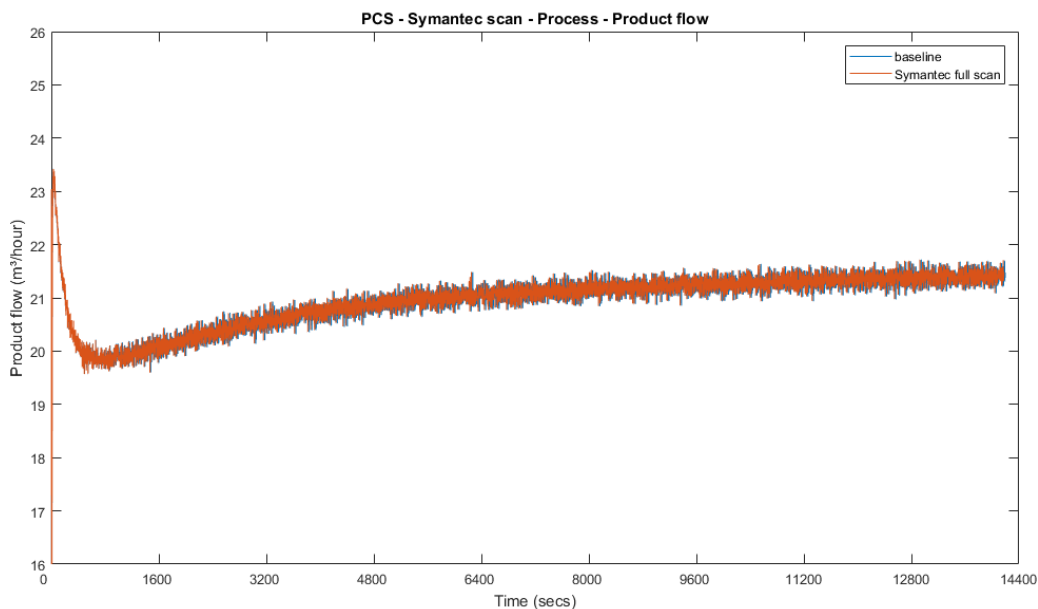
4402 No significant performance impact to the network was observed. For example, the packet round
 4403 trip time between the OPC and PLC remained mostly the same.



4404

4405 **Figure 4-23 Packet round trip time between OPC and PLC during Symantec scan (red)**

4406 There was no significant impact to the manufacturing process observed. The product flow and
 4407 the reactor pressure remain very close to the baseline measurement during the Symantec scan.



4408

4409 **Figure 4-24 Manufacturing process product flow rate**

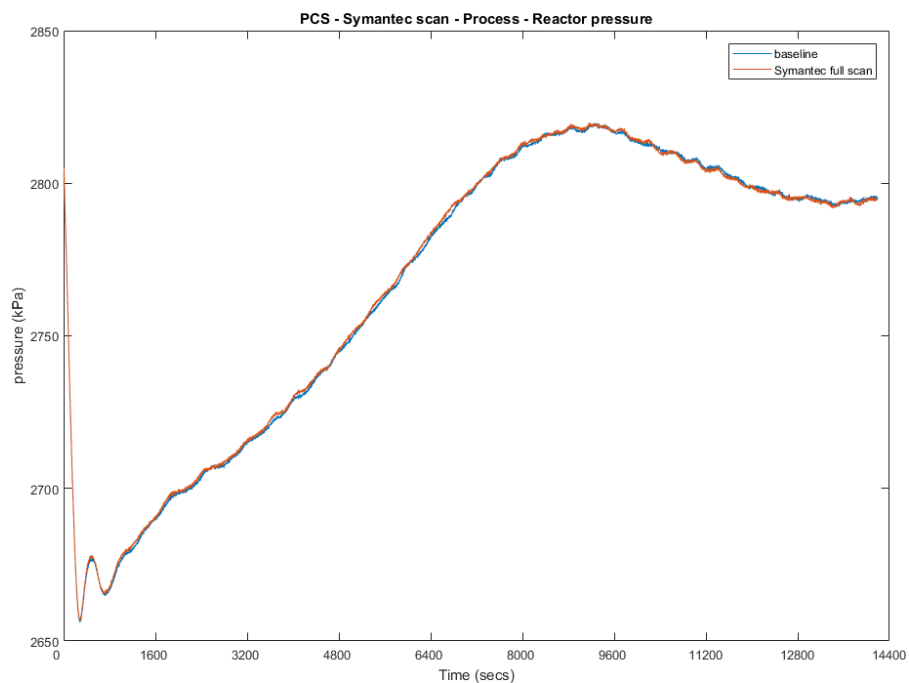


Figure 4-25 Manufacturing process Reactor pressure

It is hypothesized that the impact to the processor utilization was caused by the Symantec AV during the scan. In the case of the PCS system, the normal processor utilization is relatively low and therefore the increased usage did not cause any performance impact to the manufacturing process. If the normal utilization of the host is close to 100%, there is potential performance impact due to the increase utilization during scan time.

4.10.7 Link to Entire Performance Measurement Data Set

[Symantec AV KPI data](#)

[Symantec AV measurement data](#)

4.11 Tenable Nessus

4.11.1 Technical Solution Overview

Nessus Professional is a vulnerability assessment software from Tenable. It features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery and more. Nessus supports technologies such as scanning operating systems, network devices, next generation firewalls, hypervisors, databases, web servers and critical infrastructure for vulnerabilities, threats and compliance violations.²³ It supports both authenticated and unauthenticated scans.

Points to consider:

- Easy to setup, User friendly dashboard, fast scanning and can be configured to work in a distributed environment.
- Support for Industrial Protocols such as MODBUS, DNP3 etc. It has the necessary plugins to detect vulnerabilities on ICS/SCADA systems making it ideal to use in OT environments.
- Comes with a variety of Out-of-box policy and configuration templates.
- No limit on number of IPs or number of assessments you can run.
- Support for scanning devices behind a firewall.
- No integration available with LDAP or AD in the Professional edition.
- Multiple user accounts not supported for logging in to the Web UI.

4.11.2 Technical Capabilities Provided by Solution

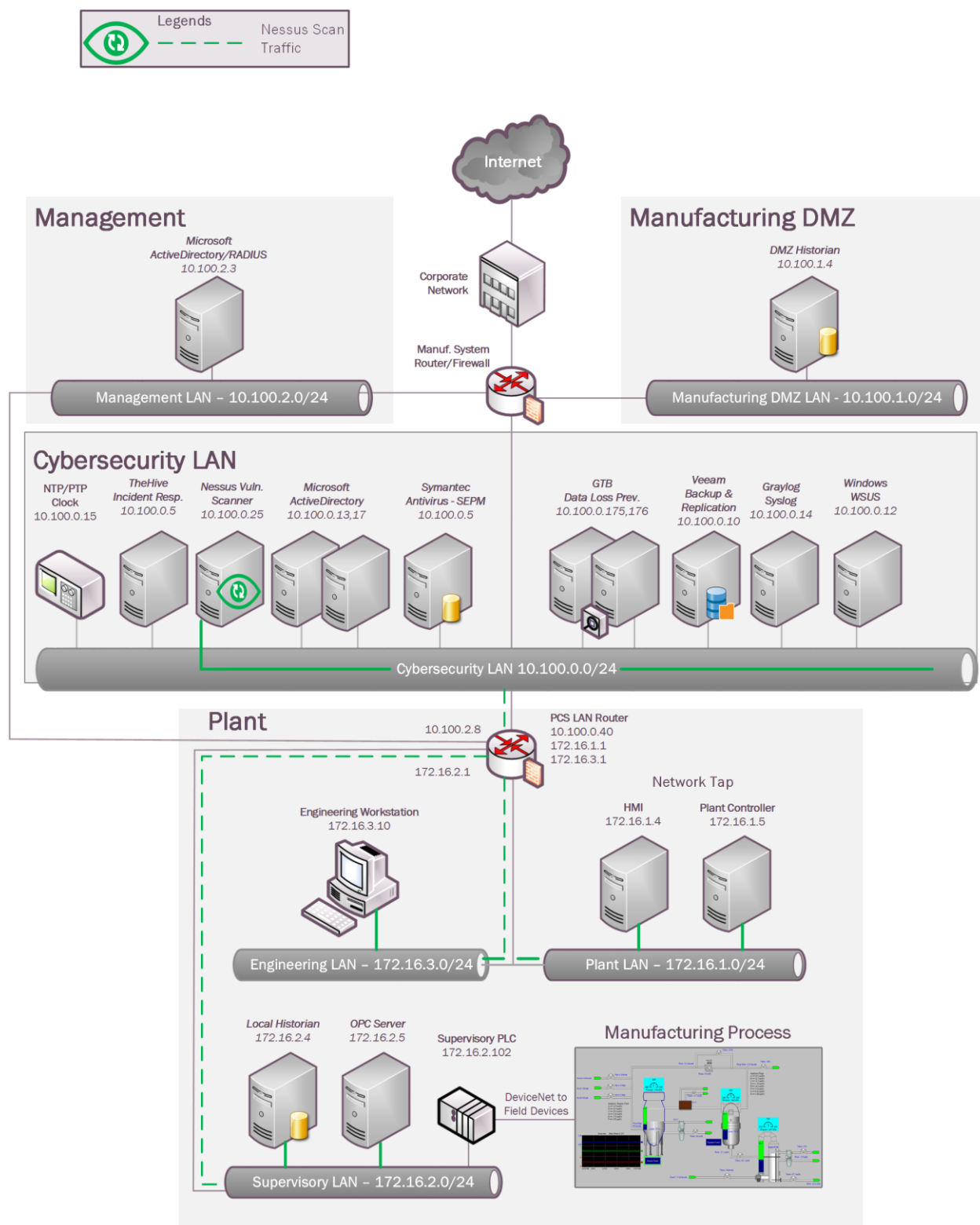
Tenable Nessus provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Vulnerability Scanning
- Vulnerability Management

4.11.3 Subcategories Addressed by Implementing Solution

ID.AM-3, ID.AM-4, ID.RA-1, DE.CM-4, DE.CM-8

²³ Nessus Professional: http://info.tenable.com/rs/934-XQB-568/images/NessusPro_DS_EN_v8.pdf

4446 **4.11.4 Architecture Map of Where Solution was Implemented**

4447

4.11.5 Installation Instructions and Configurations

Details of the solutions implemented:

Name	Version
Nessus Professional	7.2.0

Setup Overview:

- A Nessus Professional 7.x version package file was downloaded from Tenable website and was installed on a Windows 2012 R2 Virtual machine in the Cybersecurity-LAN network. Nessus is supported on Windows, Linux and Mac OS platforms. Detailed installation instructions can be found in official product guide.²⁴
- Ours was a single instance deployment. For distributed environments, Nessus supports distributed architecture of having multiple Nessus servers called as remote scanners linked to a central Nessus manager instance.
- During the setup, the wizard will prompt for registration. The Registration process and updates can be configured either in online or offline mode. An online mode is suitable for environments where Nessus server is connected to the internet while an offline mode is for air-gapped environments. Detailed instructions for registering Nessus offline can be found in the product guide. Upon completion, Nessus can be accessed via <https://<IP address of Nessus server>:8834>
- The Nessus server needs to have network connectivity from whichever networks or subnets that are intended to be scanned. In addition, if performing authenticated scans then appropriate firewall rules should be in place to allow SSH, WMI or SNMP traffic depending on the type of hosts. If performing unauthenticated scan, the firewall should be allowed for any-any communication between the Nessus server and target network.

Configuration:

- The Process Control Network has direct network connectivity with the Cybersecurity-LAN network, therefore no additional configuration was required other than allowing ports for WMI communication for scanning the Windows systems located in the Process Control network.

²⁴Nessus Official Documentation: <https://docs.tenable.com/nessus/Content/GettingStarted.htm>

- The following is a list of settings that must be true for credentialed (authenticated) scans to run successfully on Windows systems. All of these were enabled on the client (target) machines of Process Control System.
 1. The Windows Management Instrumentation (WMI) service must be enabled on the target. (<https://technet.microsoft.com/en-us/library/cc180684.aspx>)
 2. The **Remote Registry** service must be enabled on the target.
 3. File and Printer Sharing must be enabled in the target's network configuration.
 4. An SMB account must be used that has local administrator rights on the target. (You can use a domain account, but that account must be a local administrator on the devices being scanned.)
 5. Ports 139 (TCP) and 445 (TCP) must be open between the Nessus scanner and the target.
 6. Ensure that no Windows security policies are in place that block access to these services. See below for more information.
 7. The default administrative shares (i.e. IPC\$, ADMIN\$, C\$) must be enabled (AutoShareServer = 1). These are enabled by default and can cause other issues if disabled (<http://support.microsoft.com/kb/842715/en-us>).
 - Run all commands from an elevated Command prompt or PowerShell (Right click **CMD** > **Run as administrator**) on a host in the same network as the target
 1. This command will see if we can access the IPC\$ share without a username (This is how Nessus tests to see if SMB is running):
`*Change x.x.x.x with the target's IP address.* net use \\x.x.x.x\ipc$ /user:""`
 2. If this returns "Failed to connect to the IPC\$ share anonymously." then SMB is not running correctly.
 - For SMB log-on test, run the following commands, with "username" being the username of the account and "password" as the password for the account being used for the scan:
`net use \\x.x.x.x\ipc$ /user:username password`
`net use \\x.x.x.x\admin$ /user:username password`
- These commands should return "The command completed successfully." If it does not, then the credentials did not work or do not have sufficient privileges.

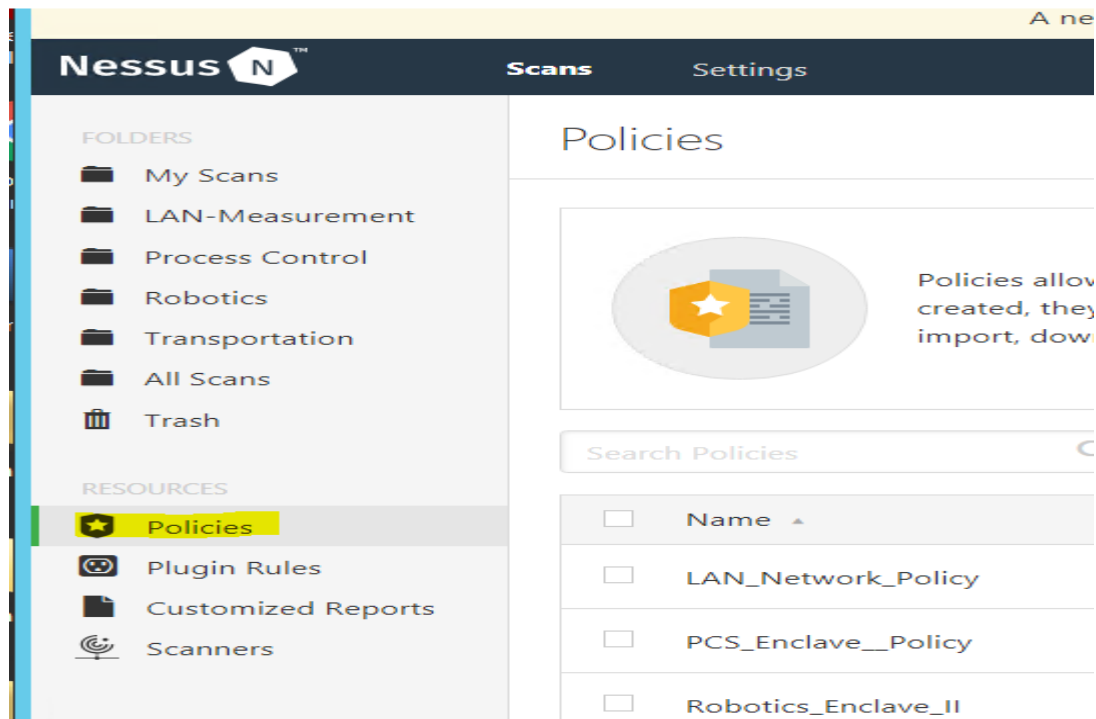
- Run the following command to check if the remote registry is running:

```
reg query \\x.x.x.x\hkln
```

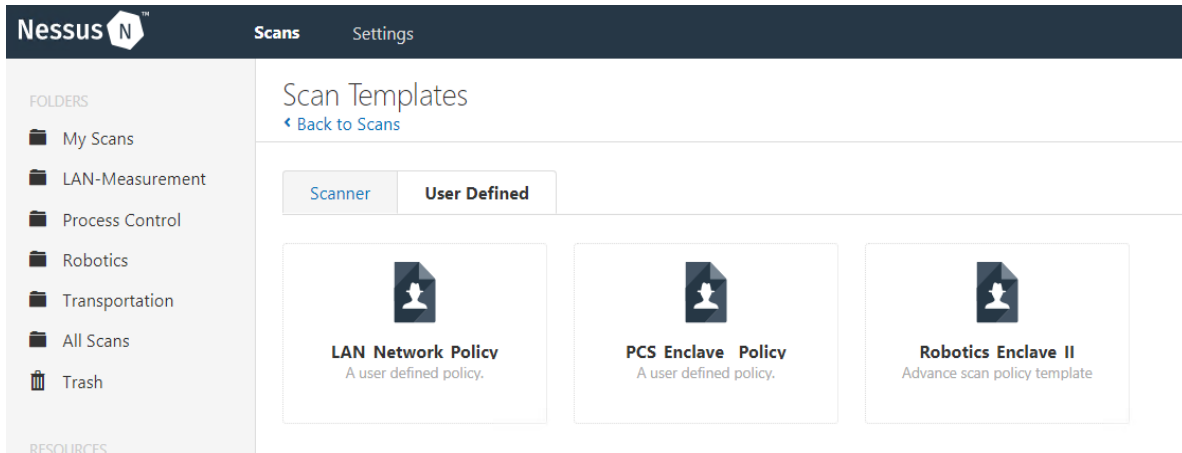
If this returns registry keys, the service is running and accessible. If this returns "ERROR: The network path was not found." then the service is not running and must be enabled.

To have a successful credential scan, these commands should not return errors.

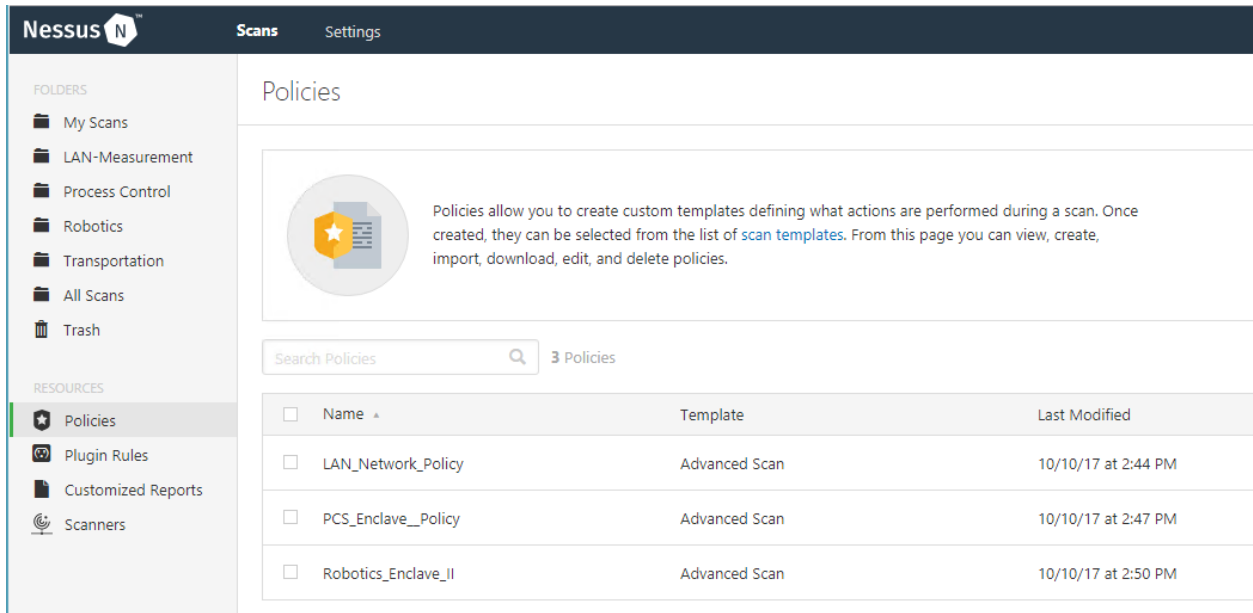
- It is recommended to use the “**Policy**” feature of Nessus for performing **credentials checks**, A Policy lets you create a scan template where in device credentials and other custom settings can be saved for scanning assets. Once created, a policy can then later be assigned to a scan.
- To create a policy, Click on “**Policies**” from the left-side explorer bar and further click on “**New Policy**” button.



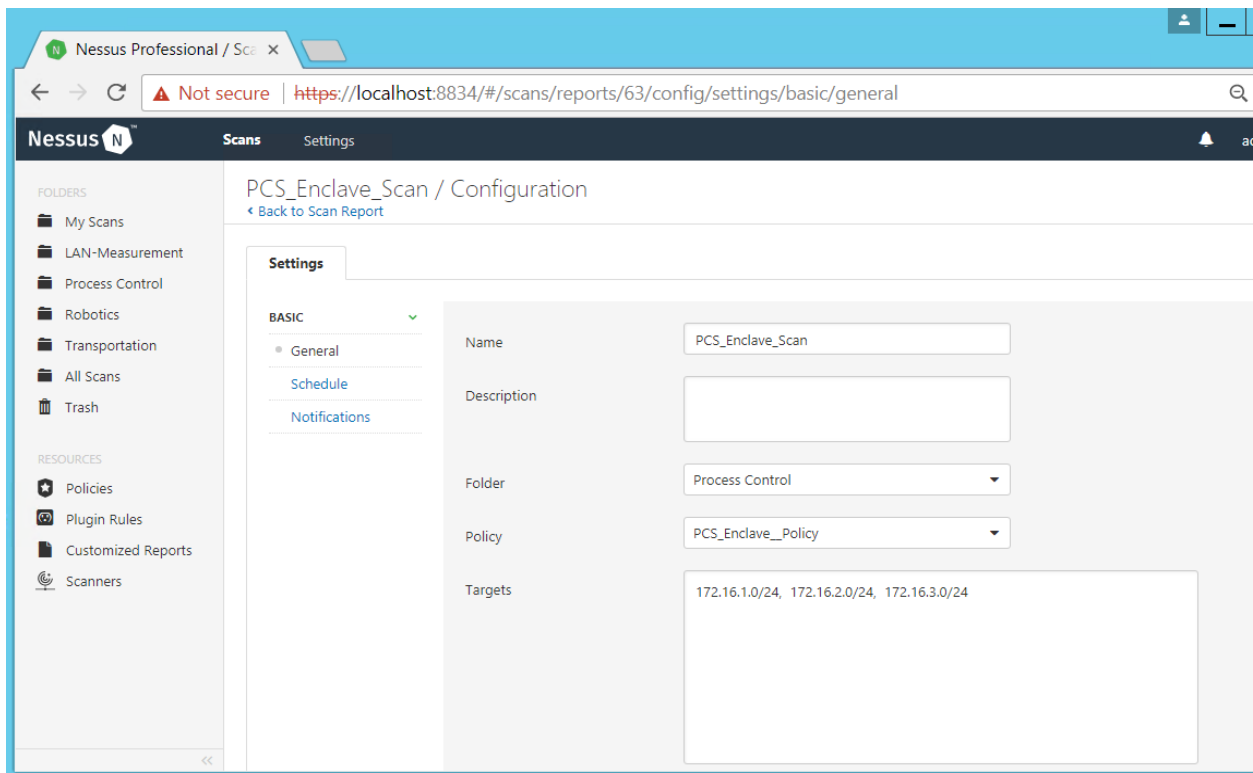
- Choose from any on the default templates available. The “**Advanced Scan**” template was selected for our use. Click on “**Credentials**” tab under a template to configure host based credentials (SSH, Windows, SNMP, etc.). Hit **Save** when done.
- Next, Create a Scan. On the home-page, click “**Scans**” from left-side explorer bar >> **New Scan** >> **User Defined** >> **Select <Policy>** >> Enter a **Name, Description** and **Network Range or Host IP addresses**. Hit **Save**.



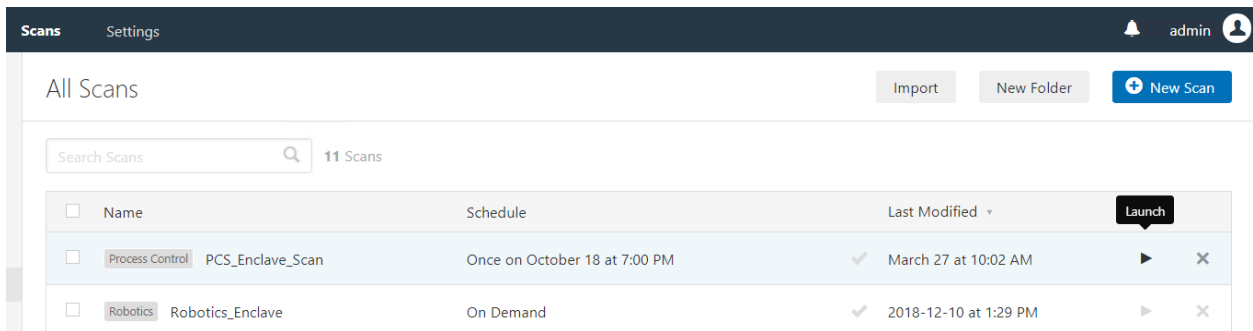
- Click “**All Scans**” >> Click on the <**Scan**> created above >> Under **Policy**, Select the appropriate Policy from the drop down list to associate the scan with a policy. Click **Save**.
- The figure below shows the different policies created in our Nessus Manager specific to each system. The policy for this Process Control system is named “**PCS_Enclave_Policy**”



- 4559 • The figure below shows the corresponding scan job settings which has the
 4560 “PCS_Enclave_Policy” assigned to it
 4561



- 4562 • To kick-off a manual on-demand scan, click on the launch button next to the scan.
 4563
 4564
 4565



4.11.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Nessus vulnerability assessment tool while the manufacturing system was operational:

Experiment PL006.1- Nessus vulnerability network scan

There was no significant performance impact to the manufacturing process was observed during the Nessus vulnerability scan. No significant network traffic increased during the Nessus scan was observed. For example, the packet round trip time from the Controller to OPC stayed mostly constant throughout the Nessus scan.

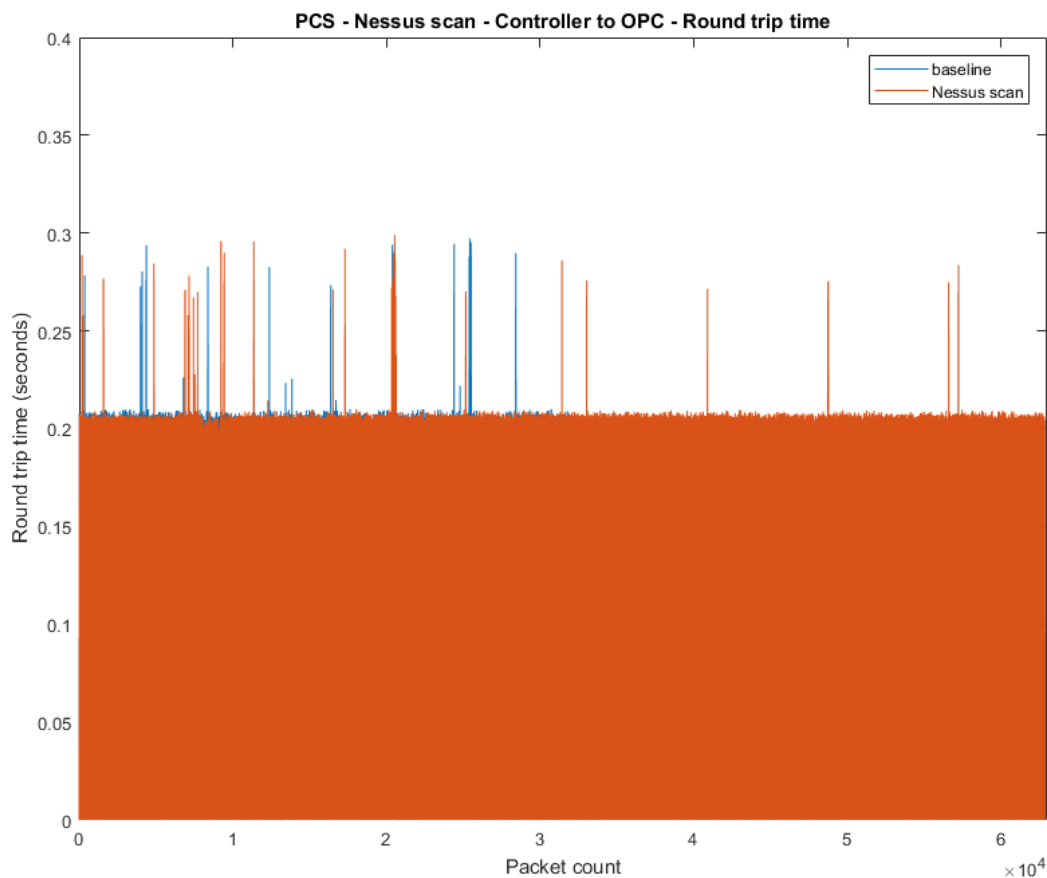


Figure 4-26 Packet round trip time from Controller to OPC during Nessus scan

Some part of the system recorded a slightly increased network traffic, for example, the network utilization and average bit rate from OPC to HMI during the Nessus scan was about 14.11% and

4584 1.41Mbit/sec respectively, while the baseline is 13.81% and 1.38Mbit/sec respectively The
4585 network utilization from PLC to OPC during the Nessus scan was about 2.2% higher than
4586 baseline.

4587 The performance of the manufacturing process mostly remained the same. For example, the
4588 product flow and the reactor pressure remained align with the baseline measurement.

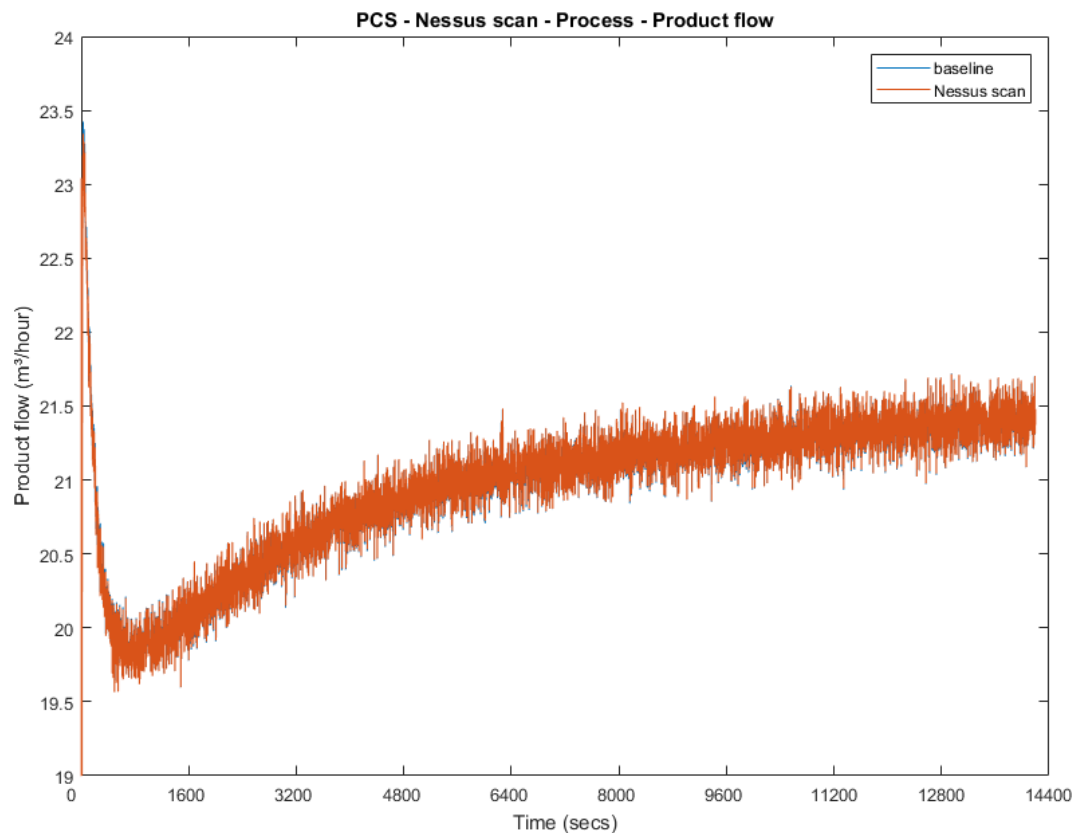


Figure 4-27 Manufacturing process product flow rate at Nessus scan

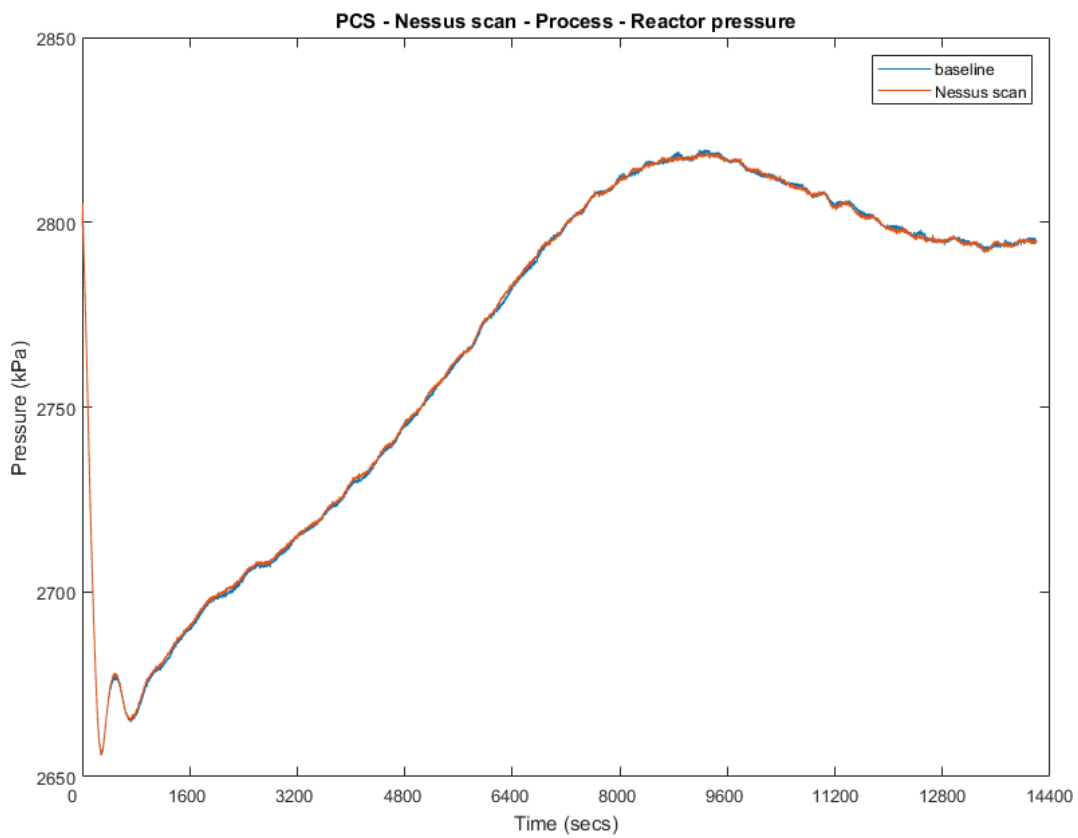


Figure 4-28 Manufacturing process reactor pressure at Nessus scan

4.11.7 Link to Entire Performance Measurement Data Set

[Nessus KPI data](#)

[Nessus measurement data](#)

4602 **4.12 NamicSoft**

4603 **4.12.1 Technical Solution Overview**

4604 NamicSoft Scan Report Assistant, a parser and reporting tool for Nessus, Burp, Nexpose
4605 OpenVAS and NCATS.²⁵

4606 **4.12.2 Technical Capabilities Provided by Solution**

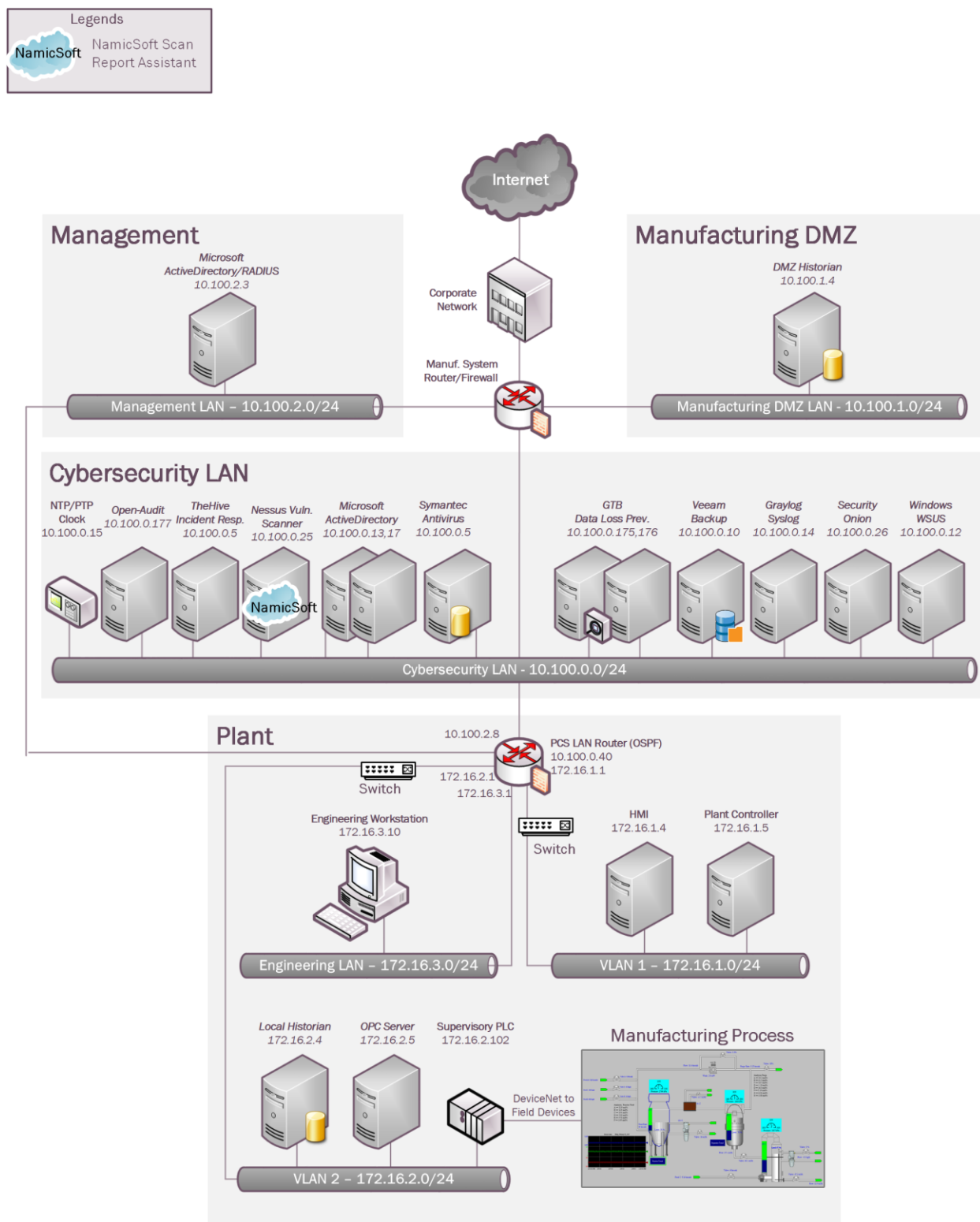
4607 NamicSoft provides components of the following Technical Capabilities described in Section 6
4608 of Volume 1:

- 4609 • Vulnerability Management

4610 **4.12.3 Subcategories Addressed by Implementing Solution**

4611 ID.RA-1, DE.CM-4, RS.MI-3

²⁵ Namicsoft <https://www.namicsoft.com/>

4612 **4.12.4 Architecture Map of Where Solution was Implemented**

4613

4614 **4.12.5 Installation Instructions and Configurations**

4615 Details of the solutions implemented:

Name	Version
NamicSoft Scan Report Assistant	3.5.0

4616

4617 Setup:

- 4618 • Download NamicSoft from <https://www.namisoft.com> and run the installer on a Windows
- 4619 PC. NamicSoft is currently supported on 64-bit Windows with .Net Framework 4.5 installed
- 4620 • The installation is tied to a user account. Any changes made by a user would not be visible to
- 4621 a different user logging in to the same system.
- 4622 • If using for the first time, the installation will prompt for a license file. If a license is not
- 4623 entered, it runs in free mode. The free mode is limited to five hosts.
- 4624 • NamicSoft was installed on the Nessus Server itself in the Cybersecurity LAN network of
- 4625 our Process Control System.

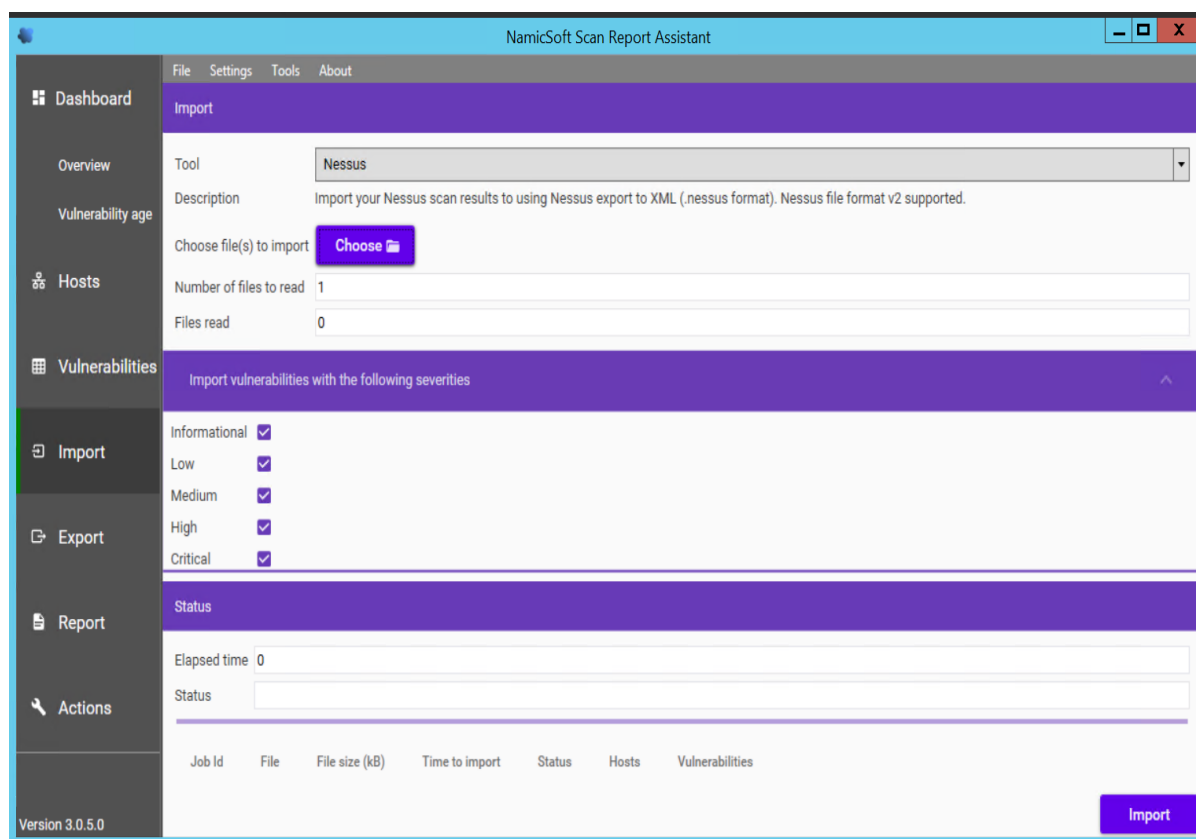
4626 Configuration for reporting Nessus scans:

- 4627 • Export a Scan Report of **nessus** format from the Nessus web interface.
- 4628 • Launch NamicSoft Report Assistant. Click **Import** on left-side explorer, select **Nessus**

4629

- 4630
- Click on **Choose** button to import files

4631



4632

- 4633
- Browse to the nessus scan report. Under **Import Vulnerabilities with following vulnerabilities**, Check / Un-check whichever severity of vulnerabilities you wish to be included in the report. Click **Import**
- 4634
- 4635

4636

4637 The below image shows “Informational” type being excluded. When the **Import** finishes, the
4638 Status bar should display **All files read**

4639

The screenshot displays the 'NamicSoft Scan Report Assistant' application window. The left sidebar contains a navigation menu with options: Dashboard, Overview, Vulnerability age, Hosts, Vulnerabilities, Import (selected), Export, Report, and Actions. The main content area is titled 'Import' and shows the following details:

- Tool:** Nessus
- Description:** Import your Nessus scan results to using Nessus export to XML (.nessus format). Nessus file format v2 supported.
- Choose file(s) to import:** A 'Choose' button with a file icon.
- Number of files to read:** 1
- Files read:** 1

Below this, a section titled 'Import vulnerabilities with the following severities' shows a list of severity levels with checkboxes:

- Informational: ☐ (unchecked)
- Low: ☒ (checked)
- Medium: ☒ (checked)
- High: ☒ (checked)
- Critical: ☒ (checked)

The 'Status' section at the bottom shows:

- Elapsed time:** 7
- Status:** All files read

At the bottom right, there is a large purple 'Import' button. The bottom left corner of the window displays 'Version 3.0.5.0'.

4640

4641

- 4642 • Upon completion of Import, go to **Hosts** page to view all the hosts level summary. Similarly,
- 4643 clicking on **Vulnerabilities** page shows all the vulnerabilities
- 4644

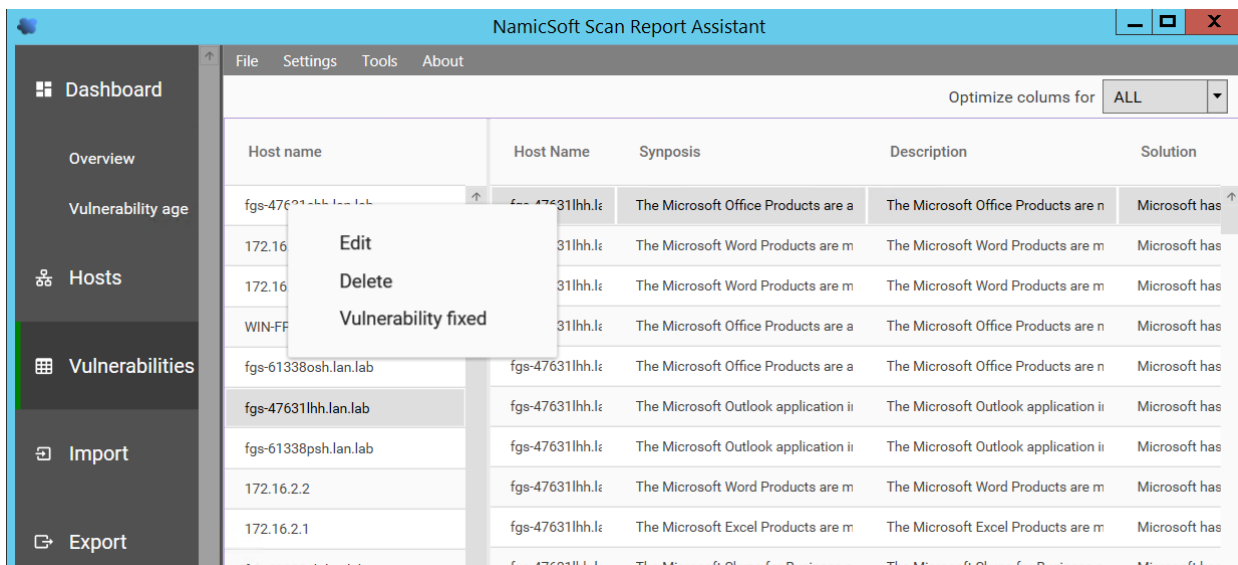
Name	IP	Operating System	MAC	NetBIOS
172.16.2.103	172.16.2.103			
172.16.2.102	172.16.2.102	Digital UNIX 4.0		
WIN-FPVTDCDEUCR	172.16.2.14	Microsoft Windows Server 2008 R2 Standard Service Pack 1	08:00:27:AE:99:58	WIN-FPVTDCDEUCR
fgs-61338osh.lan.lab	172.16.2.5	Windows 6.1	0C:C4:7A:32:B3:00 0C:C4:7A:32:B3:01	
fgs-47631lhh.lan.lab	172.16.2.4	Microsoft Windows 7 Professional Service Pack 1		FGS-47631LHH
fgs-61338psh.lan.lab	172.16.2.3	Microsoft Windows 7 Professional Service Pack 1		FGS-61338PSH
172.16.2.2	172.16.2.2	CISCO IOS Cisco IOS XE		
172.16.2.1	172.16.2.1	CISCO IOS 15.2(4a)EA5	E4:90:69:3B:C2:81 E4:90:69:3B:C2:82 E4:90:69:3B:C2:85 E4:90:69:3B:C2:C0 E4:90:69:3B:C2:C1 E4:90:69:3B:C2:C2 E4:90:69:3B:C2:C3 E4:90:69:3B:C2:C6 E4:90:69:3B:C2:C7	
fgs-61338ch.lan.lab	172.16.1.5	Microsoft Windows 7 Professional Service Pack 1	0C:C4:7A:31:3E:D7	FGS-61338CH

Version 3.0.5.0 Total: 13 Selected: 0

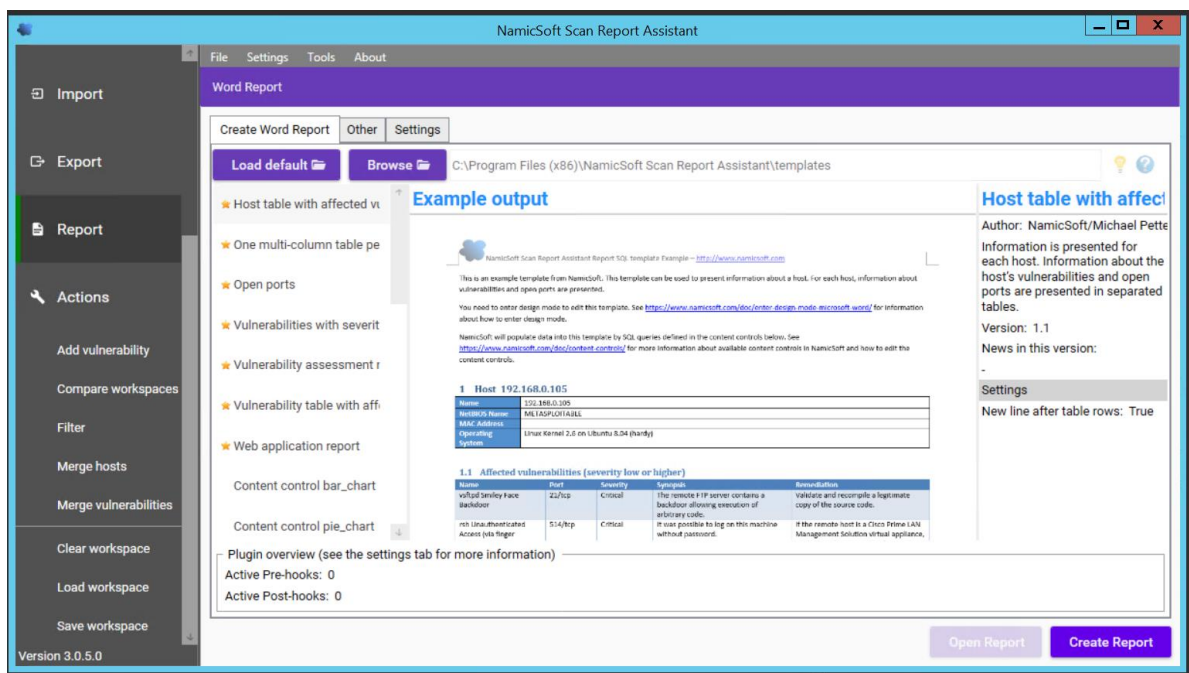
Host name	Host Name	Synopsis	Description	Solution
fgs-47631lhh.lan.lab	fgs-47631lhh.lan	The Microsoft Office Products are a	The Microsoft Office Products are n	Microsoft has
172.16.2.103	fgs-47631lhh.lan	The Microsoft Word Products are m	The Microsoft Word Products are m	Microsoft has
172.16.2.102	fgs-47631lhh.lan	The Microsoft Word Products are m	The Microsoft Word Products are m	Microsoft has
WIN-FPVTDCDEUCR	fgs-47631lhh.lan	The Microsoft Office Products are a	The Microsoft Office Products are n	Microsoft has
fgs-61338osh.lan.lab	fgs-47631lhh.lan	The Microsoft Office Products are a	The Microsoft Office Products are n	Microsoft has
fgs-47631lhh.lan.lab	fgs-47631lhh.lan	The Microsoft Outlook application ii	The Microsoft Outlook application ii	Microsoft has
fgs-61338psh.lan.lab	fgs-47631lhh.lan	The Microsoft Outlook application ii	The Microsoft Outlook application ii	Microsoft has
172.16.2.2	fgs-47631lhh.lan	The Microsoft Word Products are m	The Microsoft Word Products are m	Microsoft has
172.16.2.1	fgs-47631lhh.lan	The Microsoft Excel Products are m	The Microsoft Excel Products are m	Microsoft has
fgs-61338ch.lan.lab	fgs-47631lhh.lan	The Microsoft Skype for Business o	The Microsoft Skype for Business o	Microsoft has
fgs-61338hh.lan.lab	fgs-47631lhh.lan	The Microsoft Outlook application ii	The Microsoft Outlook application ii	Microsoft has
172.16.1.3	fgs-47631lhh.lan	The Microsoft Outlook application ii	The Microsoft Outlook application ii	Microsoft has

Version 3.0.5.0 Total: 557 Displayed: 176 Selected: 0

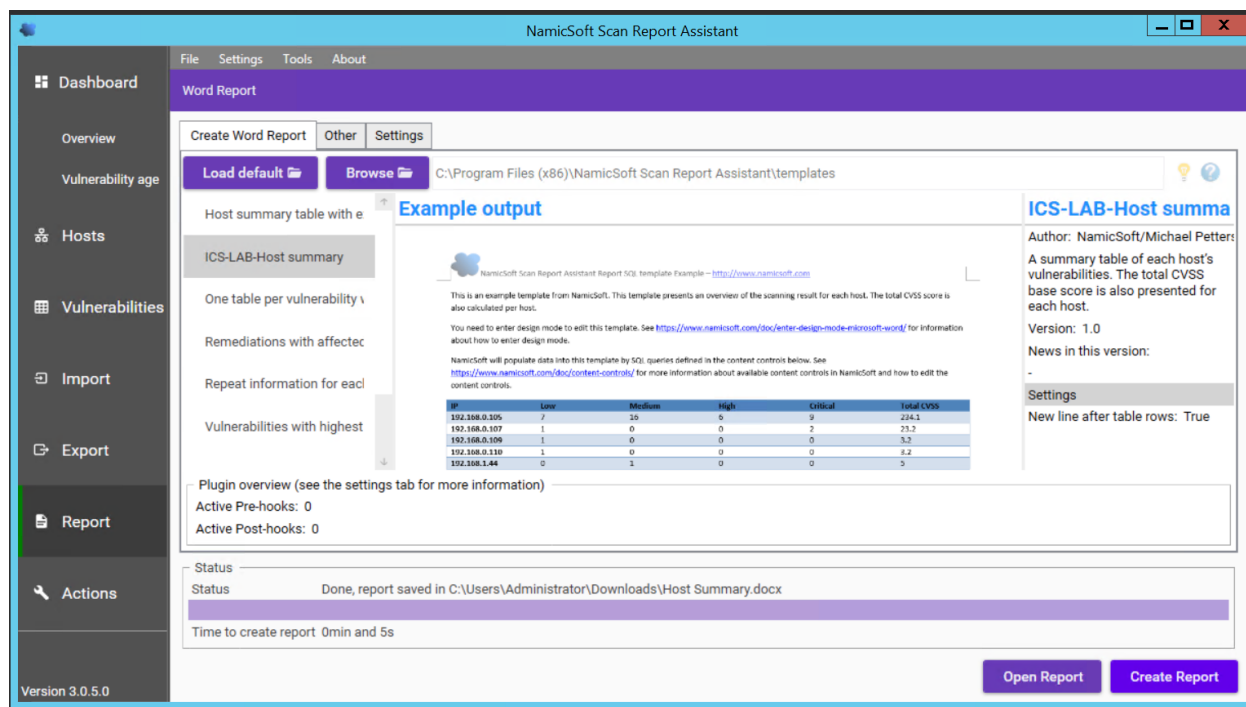
4648 To mark a Vulnerability as Fixed, select the Vulnerability >> Right Click >> Vulnerability
4649 Fixed.



- 4650
- 4651
- 4652 • Under **Actions**, click on **Save Workspace**. Ensure to **Save your workspace** after every
- 4653 change made. When running NamicSoft the next time, you can load this saved workspace
- 4654 file.
- 4655
- 4656 • To generate a Report, click on **Report**. You can select one of the default reporting templates
- 4657 from the list or create a custom one. To use a default template, select one from the list >>
- 4658 **Create Report**.



- 4660
- To view the Report, click **Open Report**.



4661

- 4662
- To create a custom template, copy one of the template files located under **C:\Program Files(x86)\NamicSoft Scan Report Assistant\templates** and save it to a different folder. Open the copied file in MS Word to begin editing. The image below shows a customized template file created for CRS system. This report generates a summary of hosts and their respective vulnerabilities based on the Severity level.
- 4663
- 4664
- 4665
- 4666
- 4667



Vulnerability Assessment Report

Process Control System Vulnerability Scan Summary

IP	Hostname	Low	Medium	High	Critical	Total CVSS
DummyValue	DummyValue	DummyValue	DummyValue	DummyValue	DummyValue	DummyValue

SELECT DISTINCT x.ip, x.hostname, (SELECT COUNT(*) FROM queryTable y WHERE severitynumber=3 AND y.ip=x.ip), (SELECT COUNT(*) FROM queryTable y WHERE severitynumber=2 AND y.ip=x.ip), (SELECT COUNT(*) FROM queryTable y WHERE severitynumber=1 AND y.ip=x.ip), (SELECT COUNT(*) FROM queryTable y WHERE severitynumber=0 AND y.ip=x.ip), (SELECT ROUND(SUM(cvssBaseScore),1) FROM queryTable y WHERE y.ip=x.ip) FROM queryTable x ORDER BY ipSortValue

A summary table of each host's vulnerabilities. The total CVSS base score is also presented for each host.

1.0

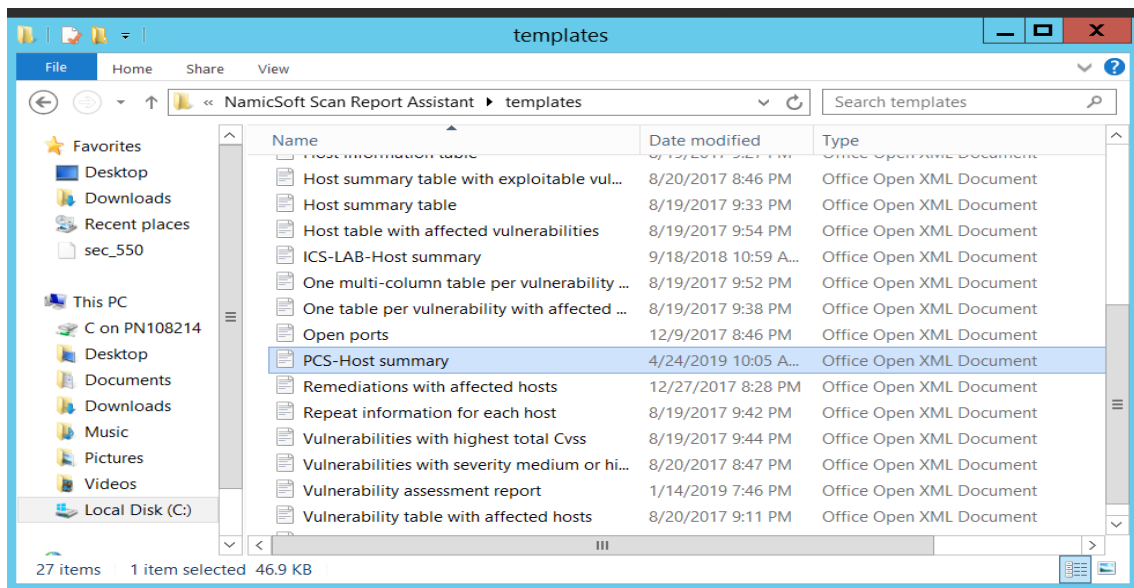
-

NamicSoft/Michael Pettersson Solutions AB

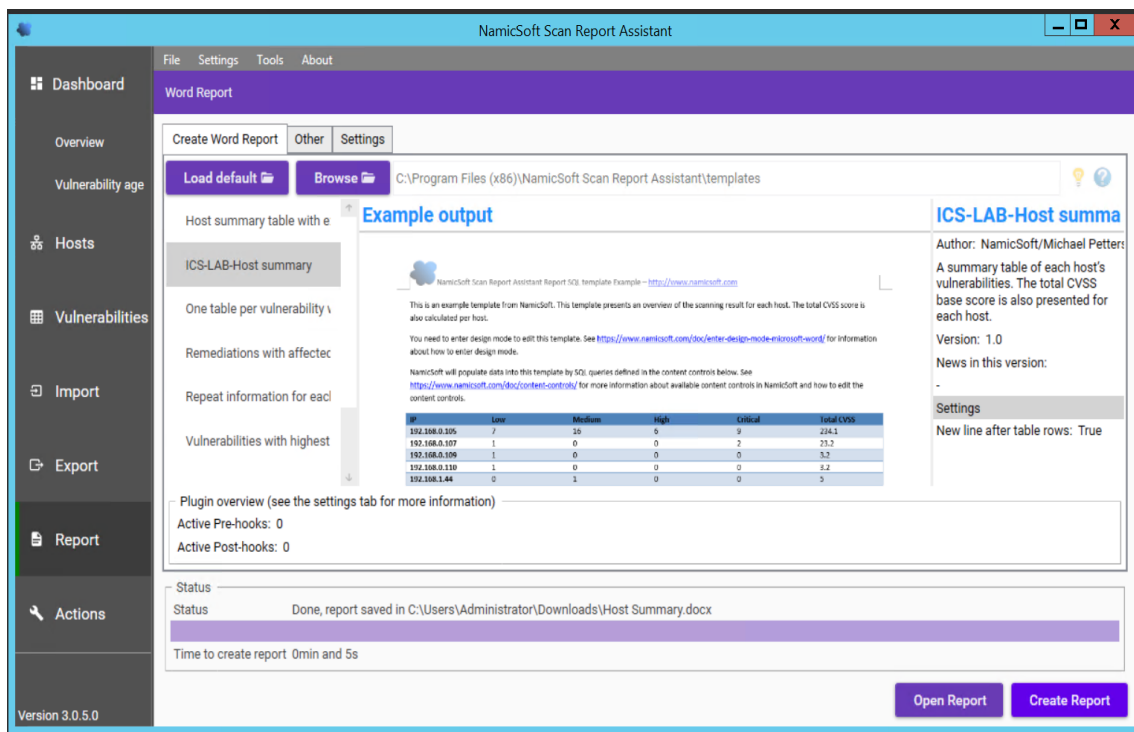
Host summary table Image.PNG

4668

- Detailed instructions for creating custom reports are available on the NamicSoft website under <https://www.namicsoft.com/doc/content-controls/>
- Save your changes and give the file a suitable name. Copy this file back to the “Templates” directory. For instance, the below image shows our customized file – **PCS- Host Summary** copied back to the templates folder.



- Launch NamicSoft again. The custom report should now appear under the list. Select it and click on **Create Report**.



- 4678
- The output should appear as per your changes.



Vulnerability Assessment Report

Process Control System Vulnerability Scan Summary

IP	Hostname	Low	Medium	High	Critical	Total CVSS
172.16.1.1	172.16.1.1	4	6	2	0	58.6
172.16.1.3	172.16.1.3	1	6	0	0	36.2
172.16.1.4	fgs-61338hh.lan.lab	3	26	39	6	542.3
172.16.1.5	fgs-61338ch.lan.lab	3	24	42	5	547.6
172.16.2.1	172.16.2.1	4	6	2	0	58.6
172.16.2.2	172.16.2.2	0	6	0	0	33.6
172.16.2.3	fgs-61338psh.lan.lab	2	23	41	5	538.3
172.16.2.4	fgs-47631lhh.lan.lab	3	40	122	11	1420.3
172.16.2.14	WIN-FPVTDCDEUCR	3	18	92	11	1047.5
172.16.3.10	fgs-47631ehh.lan.lab	0	0	0	1	10

4679

- 4680
- To report on Vulnerabilities remediated based off the previous vulnerability scans, use the
- 4681 **“Compare Workspaces”** feature under Action Menu

- 4682
- Load Nessus result from your previous scan. Save as a workspace.
- 4683
- Clear the workspace in the GUI (or restart NamicSoft)
- 4684
- Load Nessus results from the latest scan
- 4685
- Open Actions --> Compare workspaces. Choose **Compare** with current workspace
- 4686
- and point Workspace 2 to your workspace saved earlier.
- 4687
- Choose Excel output file (target)
- 4688
- Click "Compare Workspaces"

4689 4.12.6 Highlighted Performance Impacts

4690 No performance measurement experiments were performed for the use of NamicSoft due to its

4691 installation location and how it was used (i.e., the software performed offline analysis of

4692 vulnerability data captured by other software at a location external to the manufacturing system).

4693 4.12.7 Link to Entire Performance Measurement Data Set

4694 N/A

4695

4696 **4.13 The Hive Project**

4697 **4.13.1 Technical Solution Overview**

4698 A scalable, open source and free Security Incident Response Platform, tightly integrated with
4699 MISP (Malware Information Sharing Platform), designed to make life easier for SOC's, CSIRT's,
4700 CERT's and any information security practitioner dealing with security incidents that need to be
4701 investigated and acted upon swiftly.²⁶

4702

4703 **4.13.2 Technical Capabilities Provided by Solution**

4704 The Hive Project provides components of the following Technical Capabilities described in
4705 Section 6 of Volume 1:

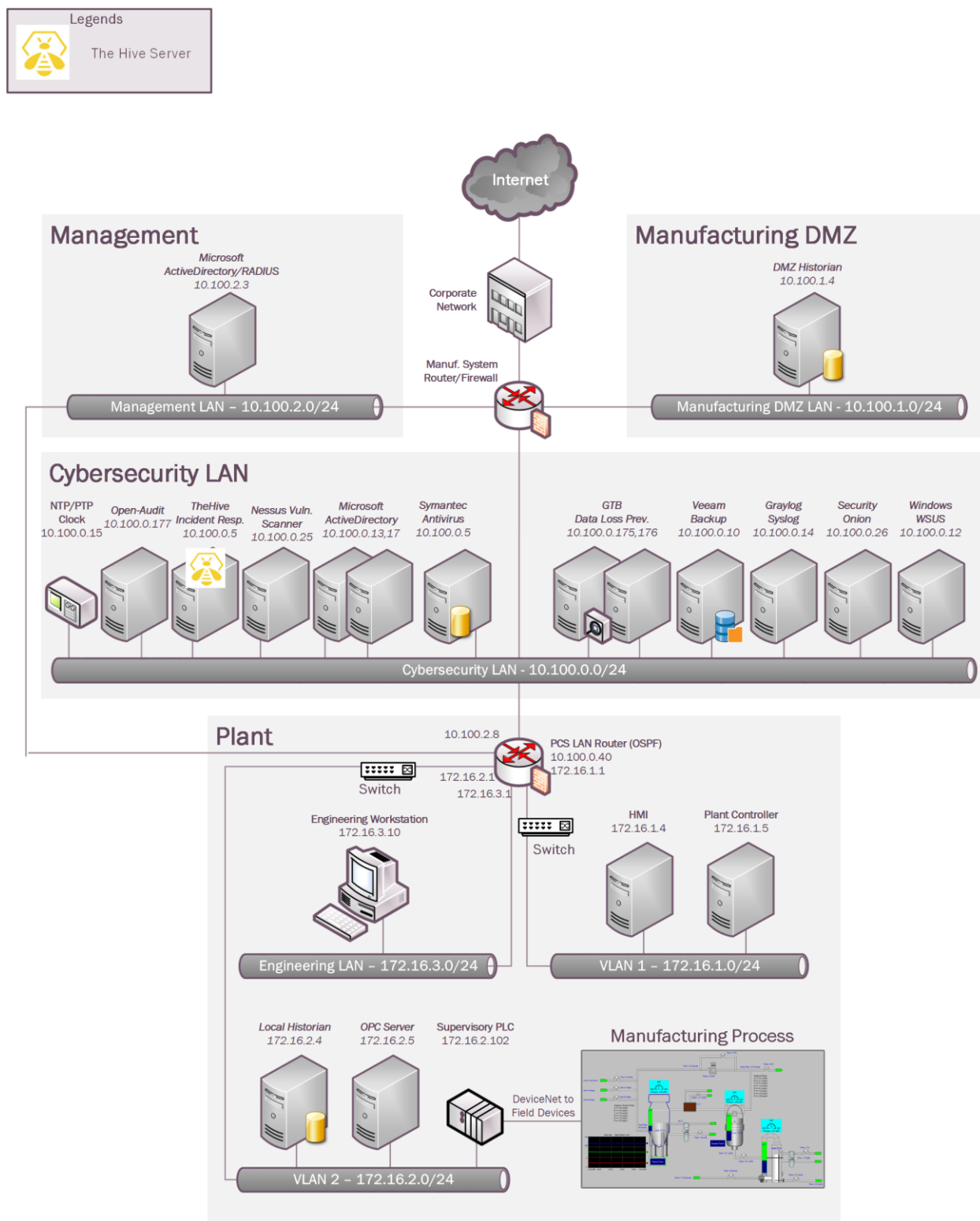
- 4706 • Incident Management

4707 **4.13.3 Subcategories Addressed by Implementing Solution**

4708 RS.MI-2 and RS.MI-3

4709

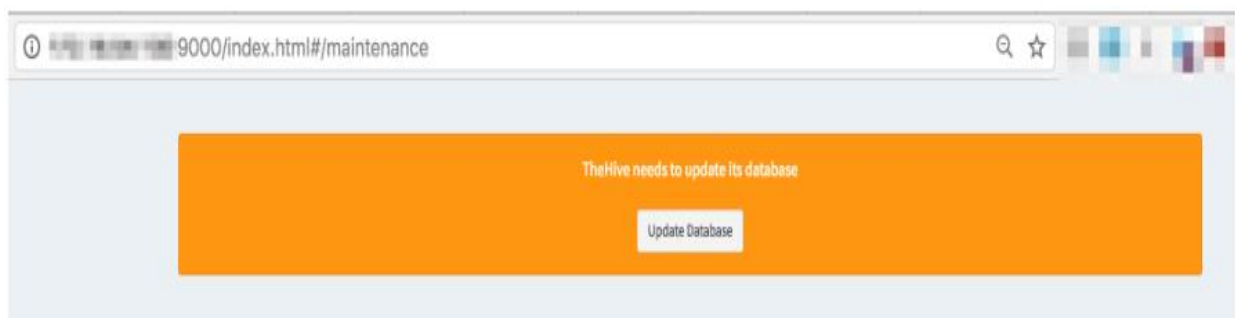
²⁶ The Hive Project: <https://thehive-project.org/>

4710 **4.13.4 Architecture Map of Where Solution was Implemented**

4711

4712 **4.13.5 Installation Instructions and Configurations**4713 **Setup:**

- 4714 • The Hive Project's website provides detailed setup [guide](#) for Linux platform. Additionally,
4715 there is a preconfigured training VM available for non-production environments. This can be
4716 downloaded from <https://github.com/TheHive-Project/TheHive>
- 4717 • The preconfigured VM was deployed in our environment. Deploy the ova file on a
4718 Hypervisor and assign the VM a static IP address. Once done, the URL of application is
- 4719 • `http://IP_OF_VM:9000`
- 4720 • The first time you access **TheHive**, you'll need to create the associated database by clicking
4721 on the **Update Database** button as shown below:
4722



- 4723 • Follow the wizard to setup a user account. Login to TheHive url with these credentials.
4724
4725
4726

4727

- 4728 • The default page will show you a List of Cases assigned to your account
4729

List of cases (1 of 1)

Quick Filters Sort by Stats Filters 15 per page

1 filter(s) applied: status: Open Clear filters

Title	Severity	Tasks	Observables	Assignee	Date
#1 - Outage None	M	2 Tasks	0	I	09/20/18 13:07

- 4730 • User accounts can be created by going to **Admin >> Users >> User Management** page.
4731 Click on “+Add User” to create a new user.
4732
4733
4734

User management

Add user 10 per page

Login	Full Name	Roles	Password	API key	Actions
icssec	icssec	read, write, admin	New password	Create API Key	Lock Edit
seconion	seconion	alert	New password	Renew Revoke Reveal	Lock Edit

4735
4736

4737

- To create a new Incident / case, click on the “New Case” menu option and fill in all the details. Hit “Create Case” button when done.

Create a new case

Case details

Title *

Date * **now**

Severity * ☐ L ☒ M ☐ H

TLP * ☐ WHITE ☐ GREEN ☒ AMBER ☐ RED

Tags

Description *

Case tasks

Add task

No tasks have been specified

Cancel * Required field **+ Create case**

- Once you’ve created a case, you can create, assign, and track tasks within a case. A task can be useful to track status updates or notes within a case. Click on “**+Add Task**” to add a task description under a case. Each task can be individually assigned to an analyst for the work to be performed. By default, a task doesn’t have an owner until someone clicks into it, or “takes” it from the Waiting tasks queue in the top menu bar.
- Custom Case templates can be created via the Case Template Management Screen. Click on **+New Template** button to create a new template of your own.
- Custom “Observables” such as domain names, IP addresses, files, filenames etc. can be added to a case by clicking on “**Observables**” tab >> **+Add Observables**. In addition, observables can also be marked as Indicators of Compromise (IOC).

The screenshot shows the TheHive web interface for Case #1 - Outage. The top navigation bar includes 'New Case', 'My tasks' (1), 'Waiting tasks' (0), 'Alerts' (0), and 'Dashboards'. The case details show it was created by 'icssec' on 'Thu, Sep 20th, 2018 13:07 -04:00'. The 'Observables' tab is selected, showing an 'Observable List (0 of 0)' with a 'No records.' message. A '+ Add observable(s)' button is visible.

4756
4757

The screenshot shows the 'Create new observable(s)' modal form in TheHive. The form has the following fields and options:

- Type ***: A dropdown menu with 'domain' selected.
- Value ***: A text input field.
- TLP ***: A text input field.
- Tags ****: A text input field.
- Description ****: A text input field.

A legend at the bottom right indicates: *

4758
4759

- Analysts can use “Cortex” engine to perform detailed analysis on observables or IOCs such as domain names, IP addresses, hashes. This can be achieved by enabling or creating Analyzers in Cortex. The default URL for Cortex Web UI is http://<CORTEX_IP>:9001

The high-level steps in configuring Cortex are:

- Setup Cortex
- Create an Administrator account
- Create an Organization
- Create an Organization Administrator account
- Enable or Configure Analyzers
- Integrate with the Hive instance

Detailed instructions on setting up Cortex are available at <https://github.com/TheHive-Project/CortexDocs>

Integration with Security Onion

- Integration with other products can be done via API keys to connect with the Hive. A dedicated user account was created for this purpose with permissions to “Allow alerts creation”. Ensure **Roles: None** is set for security purposes of this user account.

The screenshot shows a web form titled "Add user". It contains the following fields and controls:

- Login ***: Text input field containing "seconion".
- Full name ***: Text input field containing "seconion".
- Roles ***: Dropdown menu with "none" selected.
- Additional Permissions**: A checkbox labeled "Allow alerts creation" which is checked.
- Buttons**: "Cancel" button on the bottom left and "Save user" button on the bottom right.

- 4783 • An API key was created for this user, by clicking on “**Create API Key**” for this dedicated
4784 user account
4785

User management

Add user				
Login	Full Name	Roles	Password	API key
icssec	icssec	read, write, admin	New password	Create API Key
seconion	seconion	read, write, alert	New password	Create API Key

- 4786
4787
4788 • Our Security Onion instance was integrated with the Hive Instance to create a case for IDS
4789 alerts generated by Security Onion. This was accomplished by creating a new rules file
4790 **hive.yaml** under the **/etc/elastalert/rules** directory of the Security Onion server. Detailed
4791 instructions are available at <https://securityonion.readthedocs.io/en/latest/hive.html#thehive> .
4792

Extract from our hive.yaml

```
# hive.yaml
# Elastalert rule to forward IDS alerts from Security Onion to a specified TheHive instance.
#
es_host: elasticsearch
es_port: 9200
name: TheHive - New IDS Alert!
type: frequency
index: "*:logstash-ids*"
num_events: 1
timeframe:
  minutes: 10
buffer_time:
  minutes: 10
allow_buffer_time_overlap: true

filter:
- term:
  event_type: "snort"

alert: hivealerter

hive_connection:
hive_host: https://10.100.0.51
hive_port: 9000
hive_apikey: APIKEY
```

4795

4796 4.13.6 Highlighted Performance Impacts

4797 No performance measurement experiments were performed for the use of the Hive Project due to
4798 its typical installation and usage location (i.e., external to the manufacturing system).

4799 4.13.7 Link to Entire Performance Measurement Data Set

4800 N/A

4801

4802

4803 4.14 Microsoft EFS**4804 4.14.1 Technical Solution Overview**

4805 EFS is file level encryption tool provided by Windows. The Encrypted File System, or EFS,
4806 provides an additional level of security for files and directories. It provides cryptographic
4807 protection of individual files on NTFS file system volumes using a public-key system.²⁷

4808 4.14.2 Technical Capabilities Provided by Solution

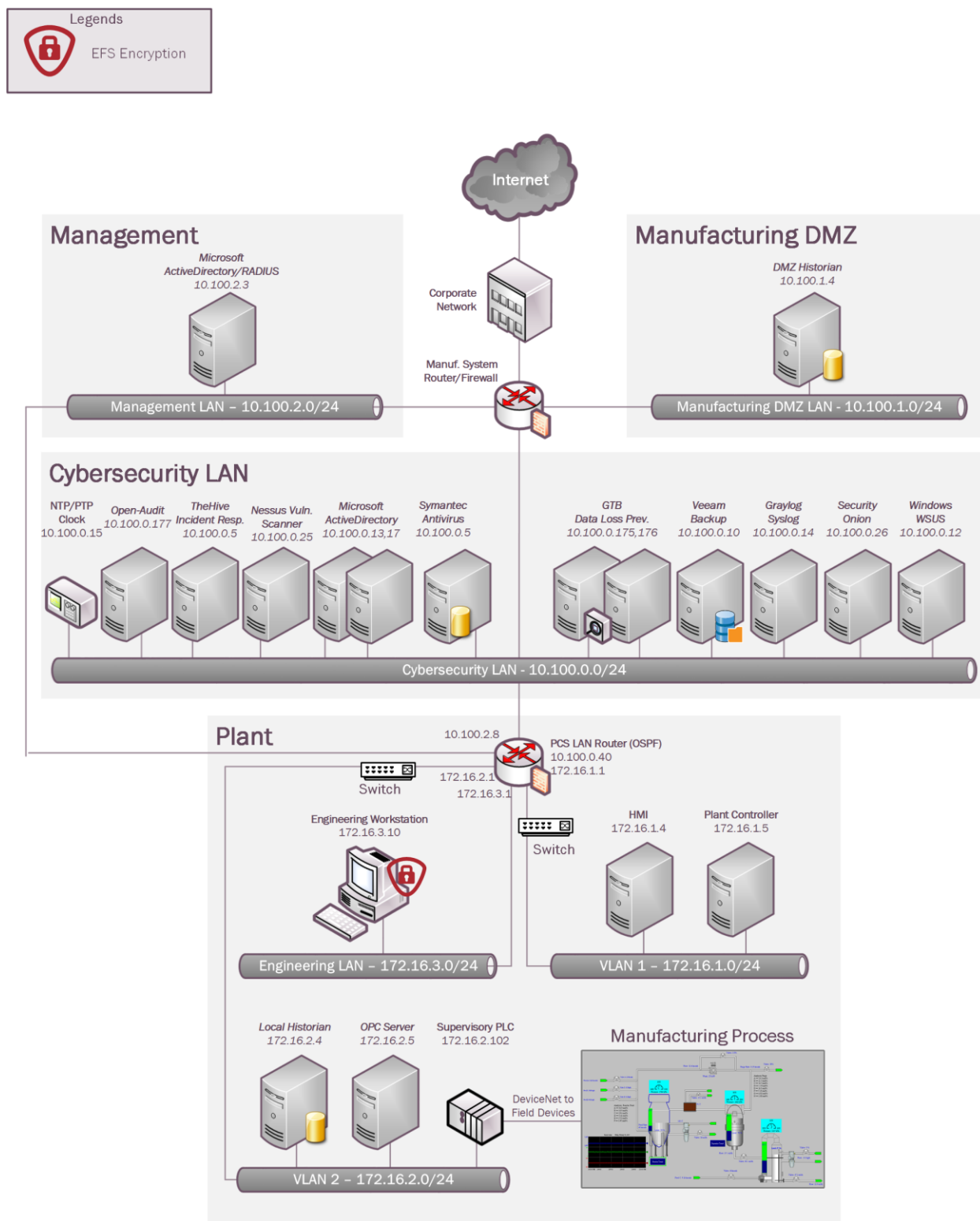
4809 Microsoft EFS provides components of the following Technical Capabilities described in Section
4810 6 of Volume 1:

- 4811 • Encryption

4812 4.14.3 Subcategories Addressed by Implementing Solution

4813 PR.DS-5

²⁷ <https://docs.microsoft.com/en-us/windows/desktop/fileio/file-encryption>

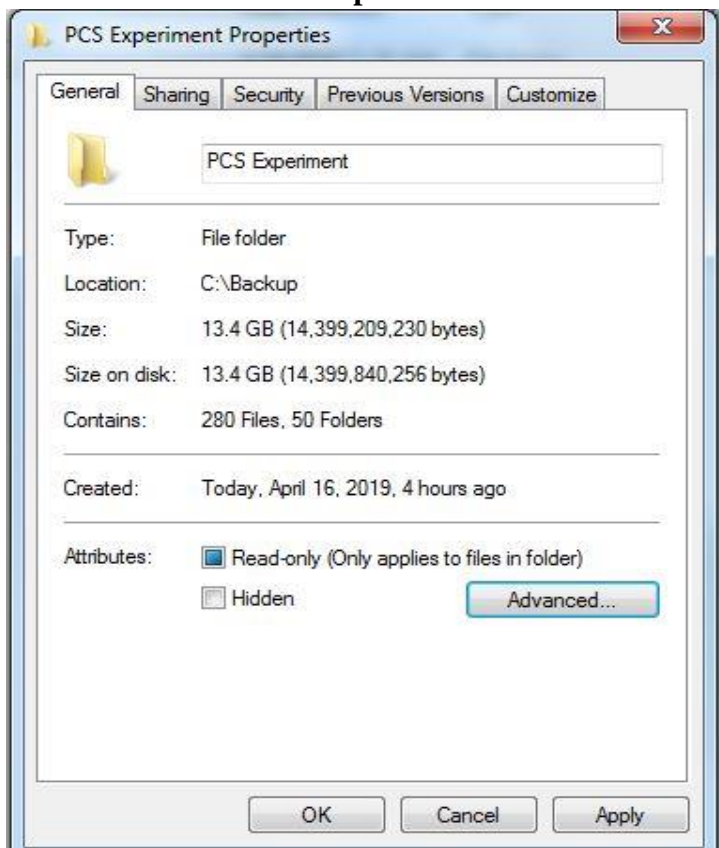
4814 **4.14.4 Architecture Map of Where Solution was Implemented**

4815

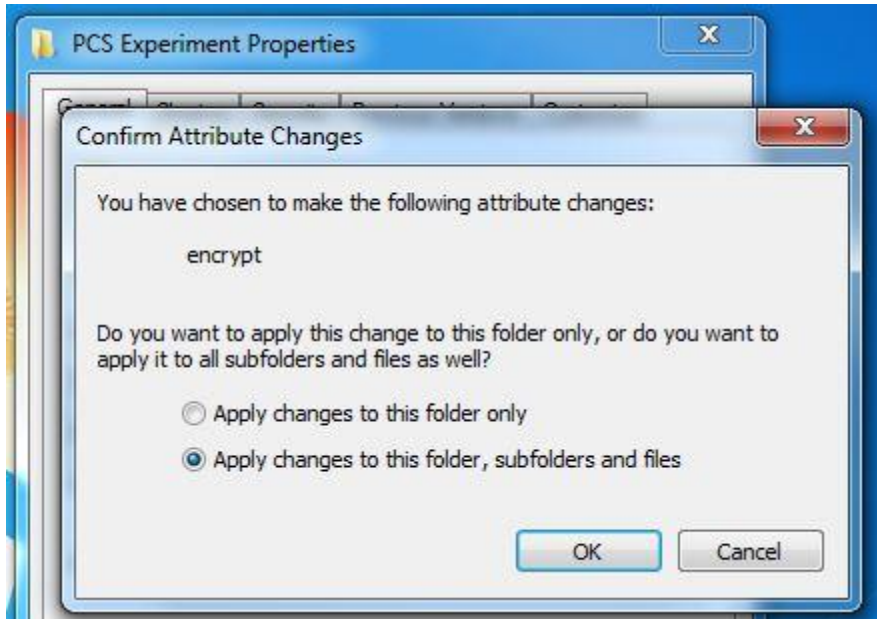
4.14.5 Installation Instructions and Configurations**Setup:****Note:** These steps were performed on the below system

Hostname	IP_Address	OS
Engineering Workstation	172.16.3.10	Windows 7 Professional 64bit

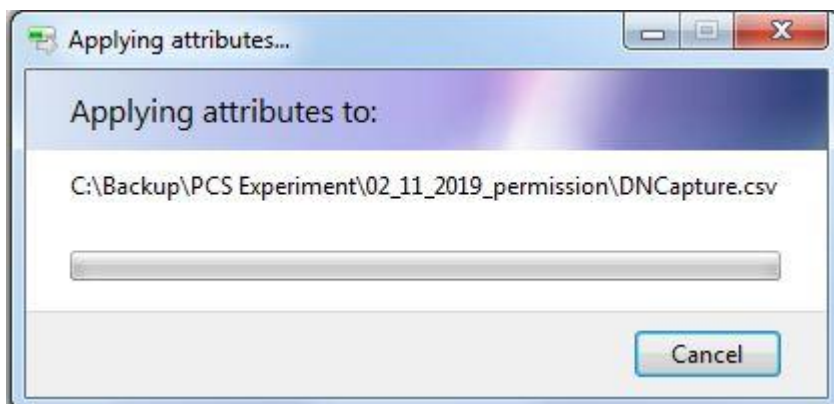
- Windows EFS was used to encrypt confidential folders on the Windows workstation of Process Control System.
- To begin encrypting, select a parent folder which you wish to encrypt. Right Click on the Folder Name >> Click **Properties** >> **General Tab** >> Click **Advanced**



- Under Confirm Attribute Changes, choose how extensive you want the encryption to be, click **OK**. We recommend selecting the option of “**Apply changes to folder, subfolders and files**”



- Click **Apply**. This will begin the encryption process.



- 4839 • Upon encryption, the subfolders or file names would change to Green color as shown below
 4840 Any new folder added to this parent folder will be automatically encrypted.

Name	Date modified	Type	Size
02_11_2019_permission	4/16/2019 3:23 PM	File folder	
02_14_2019_openAudit	4/16/2019 3:24 PM	File folder	
02_24_19_firewall	4/16/2019 3:25 PM	File folder	

- 4841
- 4842 **Backing up the Encryption Key**
- 4843 • When a file or folder is encrypted for the first time, a pop-up message saying “Backup your
 4844 encryption key” should appear in the task-bar. Double click to launch the backup process.
 4845 • Alternatively, this process can also be launched manually by going to **Control Panel** >> All
 4846 Control Panel **Items** >> **User Accounts** >> **Manage your encryption certificates**
 4847 **Note:** This process is different for a Windows 10 system.



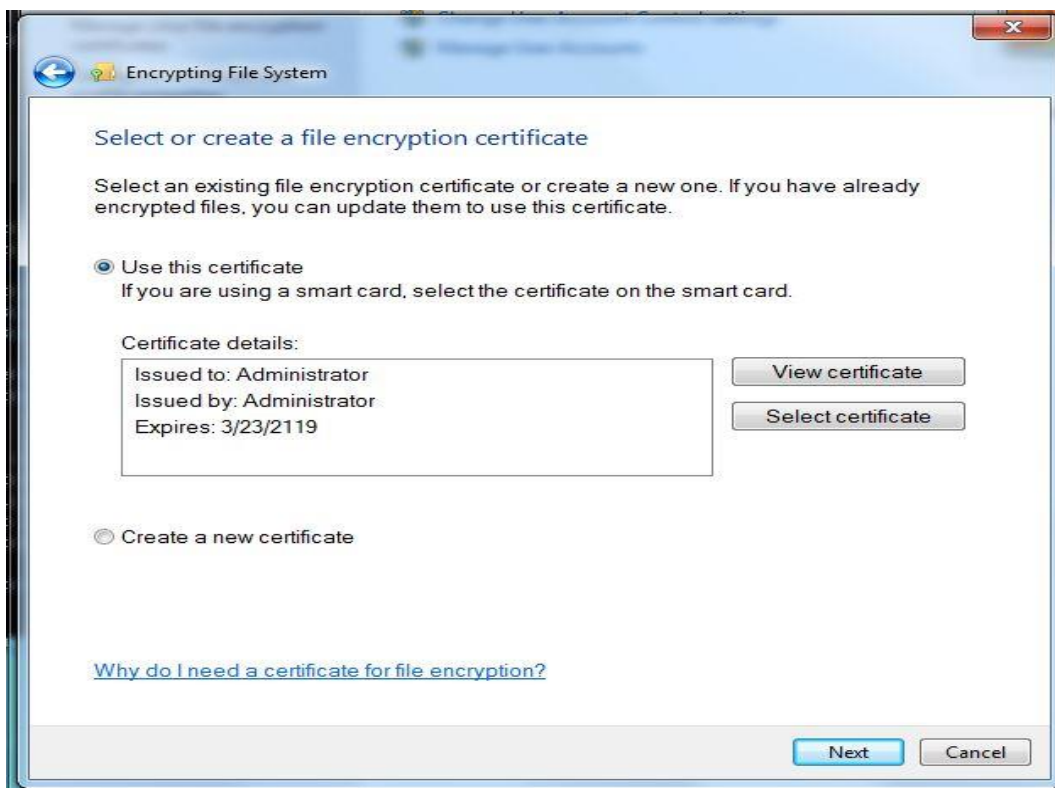
- 4850 • Click **Next**



4851

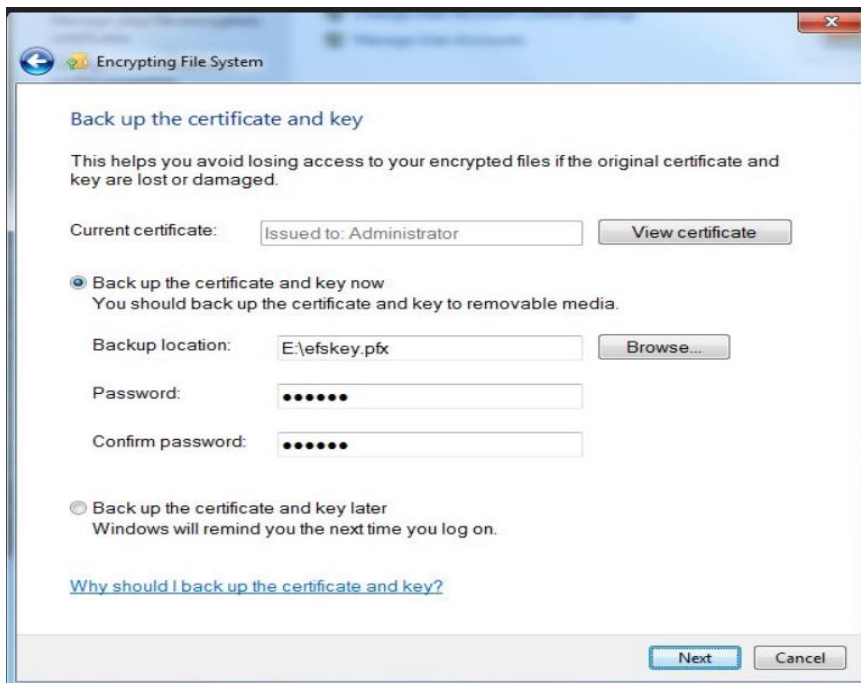
- 4852 • Select existing Certificate or Create a new one. It is safe to go with the default option

4853

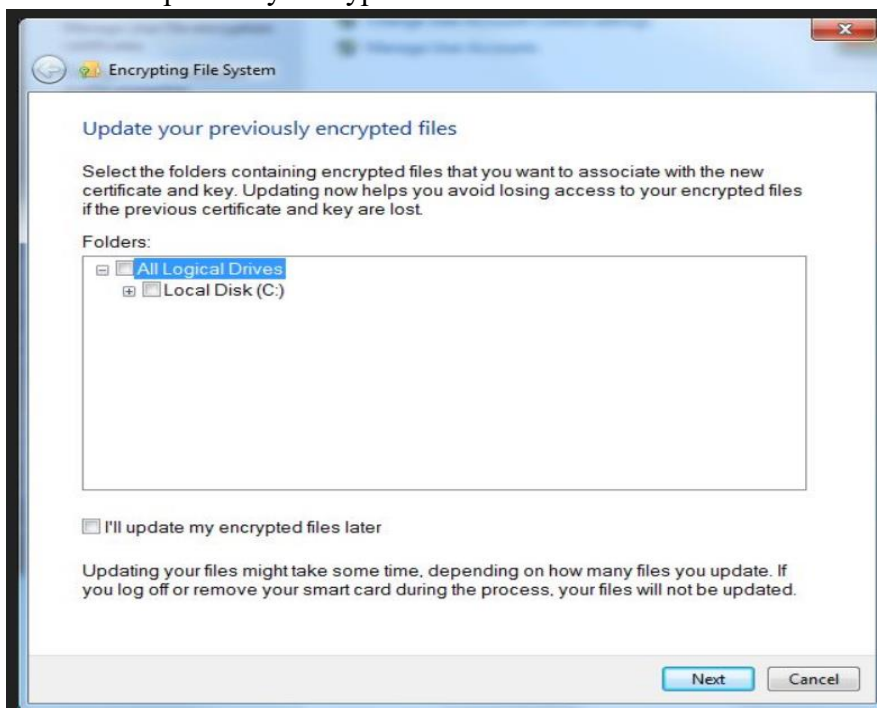


4854

- 4855 • Select “**Backup the Certificate and Key Now**”. Click **Browse** to choose a destination for
4856 saving the pfx bundle file. For instance: a USB drive. Enter a password for added protection.
4857

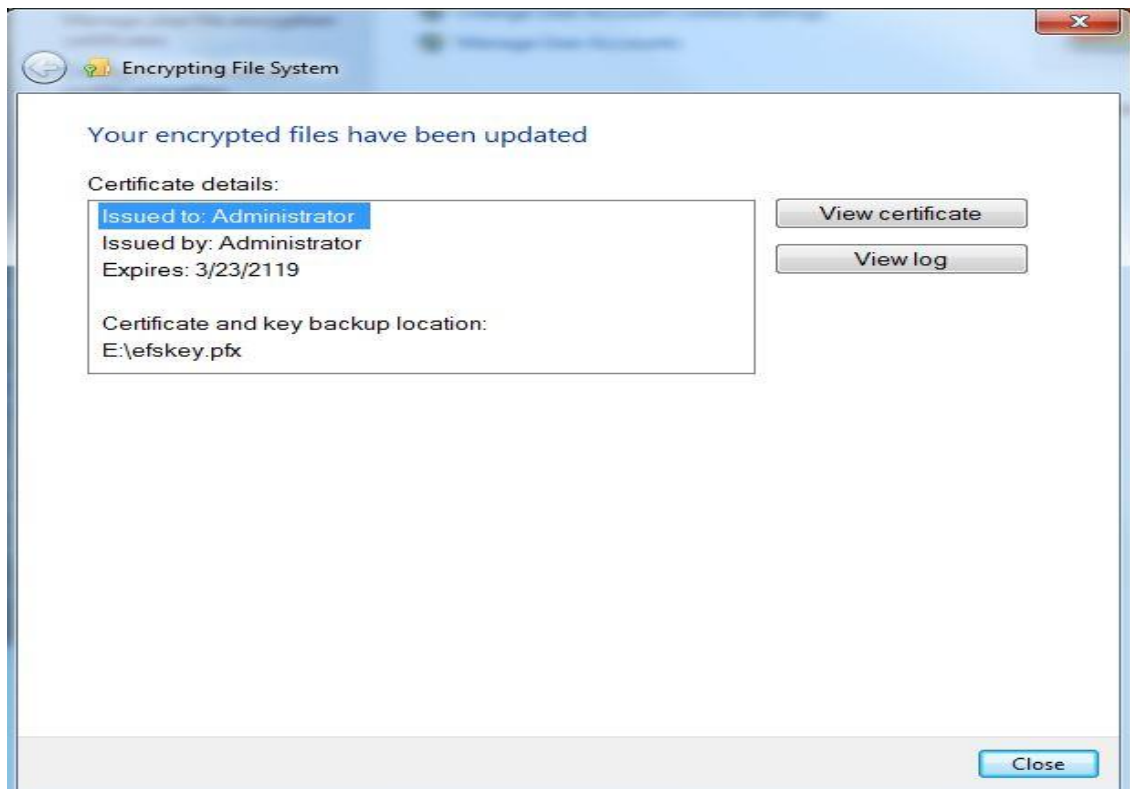


- 4858
4859
4860
4861 • Select the appropriate folder to associate with the new certificate and key OR Alternatively
4862 select “I’ll update my encrypted files later”. Click **Next**



4863

- A confirmation message as below will be shown next. This completes the backup of the Recovery key



Using Encrypted files on a Different Computer

If you want to use your encrypted files on another computer, you need to export the EFS certificate and key from your computer or the USB backup and then import it at the other computer.

4.14.6 Highlighted Performance Impacts

The following performance measurement experiment was performed for the Microsoft EFS tool while the manufacturing system was operational:

Experiment PL013.1- Enable file level encryption on HMI host

The FactoryTalk HMI application has a designated file folder to contain the log files for the HMI data. EFS tool was used to encrypt the data log file in this experiment.

There were noticeable performance impacts to the computing resources observed when the EFS was activated for the data log files, especially at the initial operation of the HMI. The processor utilization was noticeable higher from 450 seconds to 750 seconds experiment time and occasionally higher throughout the first 3000 seconds. The disk write operation was significantly higher in the first 800 seconds of the experiment time. The HMI application attempted to access the data log files at the initialization stage and therefore most of the impacts were observed at the beginning of the operation.

On the network side, no significant performance impact was observed. The packet round trip time between the HMI and OPC in both directions reminded mostly constant before and after the EFS was enabled.

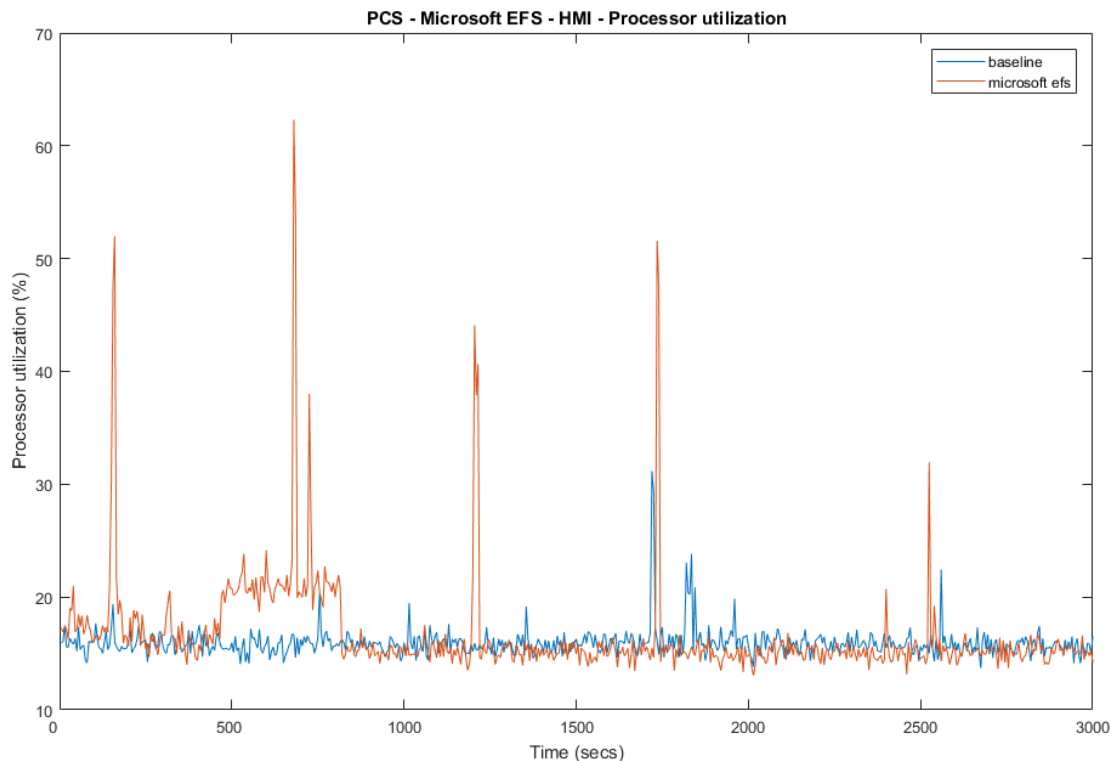


Figure 4-29 HMI computer processor utilization with EFS enable (red) and without EFS enable (blue)

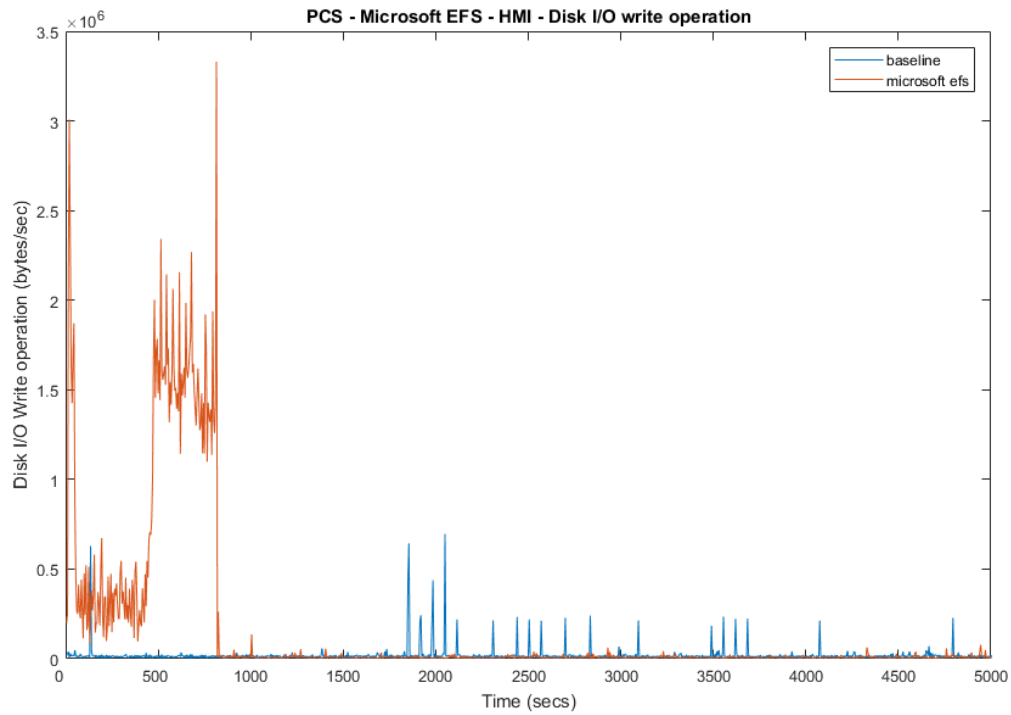


Figure 4-30 HMI computer disk write operation with EFS enable (red) and without EFS enable (blue)

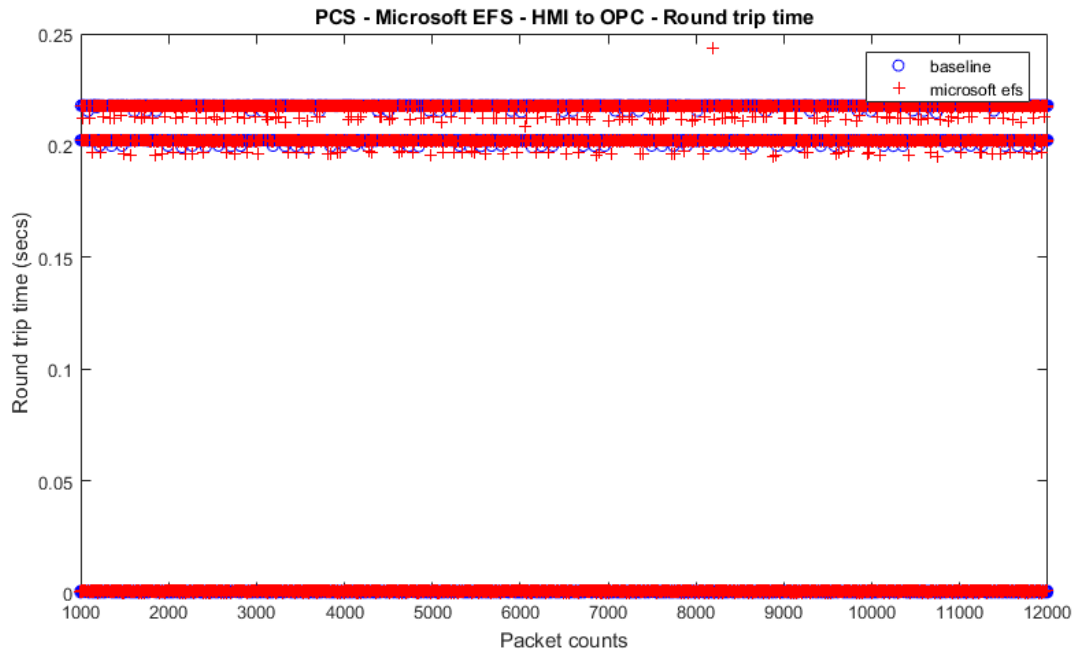


Figure 4-31 Packet round trip time from HMI to OPC with EFS enable (red) and without EFS enable (blue)

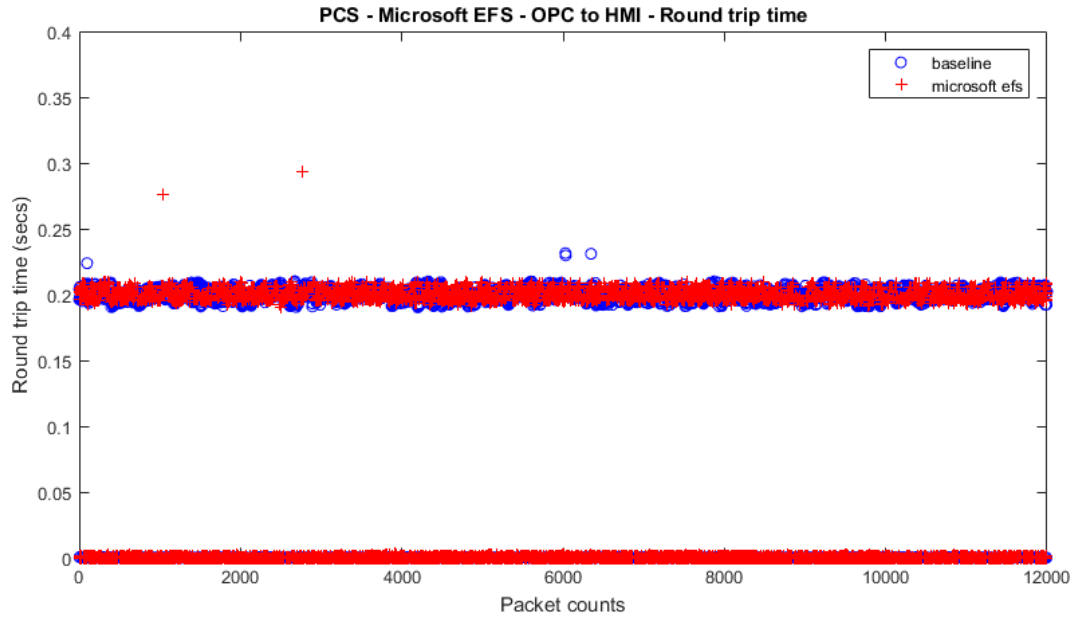


Figure 4-32 Packet round trip time from OPC to HMI with EFS enable (red) and without EFS enable (blue)

The HMI application was not able to access the data log files and new data from operation was not logged. The HMI flagged an error/warning message to the operator.

Care should be taken for encrypting application specific files or folders. There is performance impact to the manufacturing process in the form of losing the ability to log data files in the HMI.

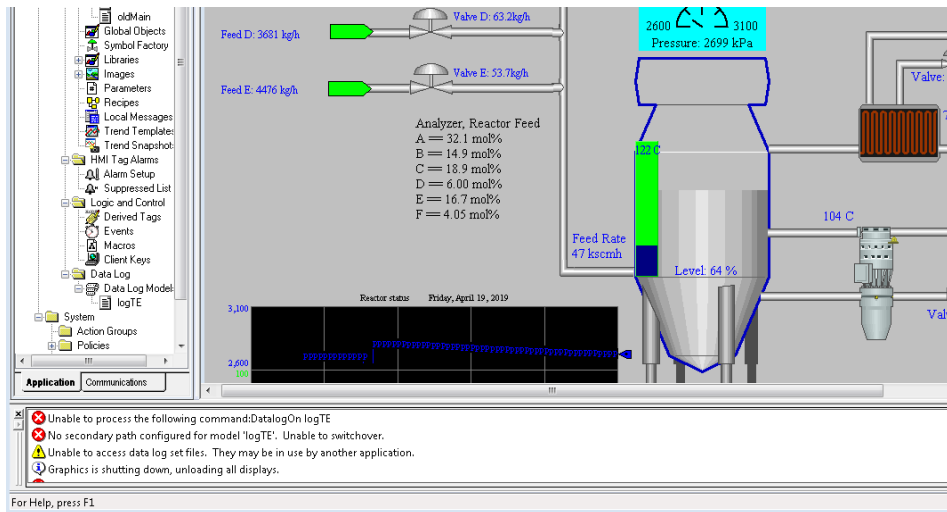


Figure 4-33 HMI screen with warning message "Unable to access data log set files"

4906 **4.14.7 Link to Entire Performance Measurement Data Set**

4907 [File Encryption KPI data](#)

4908 [File Encryption measurement data](#)

4909

4910 **4.15 GTB Inspector**

4911 **4.15.1 Technical Solution Overview**

4912 GTB Inspector by GTB Technologies is a DLP solution that has been evaluated in our lab
4913 environment for low baseline manufacturing profile. GTB Inspector's built in ability to detect,
4914 log, and block network traffic trying to leave premise. Inspector detects and blocks FTP, Email,
4915 HTTP, HTTPS (SSL/TLS), Finger Printed files, USB protection, and other configured
4916 exfiltration methods. GTB Inspector is the main component that analyzes all network traffic and
4917 depending on the configuration Bridge (In-Line), Monitoring (OOL), TAP, Transparent Proxy
4918 (TPROXY), and Load Balancing if required. GTB Central Console which is the device Inspector
4919 reports back to, so there is always a log of violation that occurred. Central Console allows for
4920 groups and escalation paths depending on the alerting required.

4921 GTB is configured within the corporate network. This option was chosen to ensure we could get
4922 the best protection for the entire environment.

4923 All DLP products have a high cost to implement, but GTB Technologies provides a product that
4924 can grow as your company does.

4925 Once installed and configured system requires little maintenance.

4926 Install time within the lab was approximately 16 hours for configuration, but for simple data
4927 capture setup took about an hour.

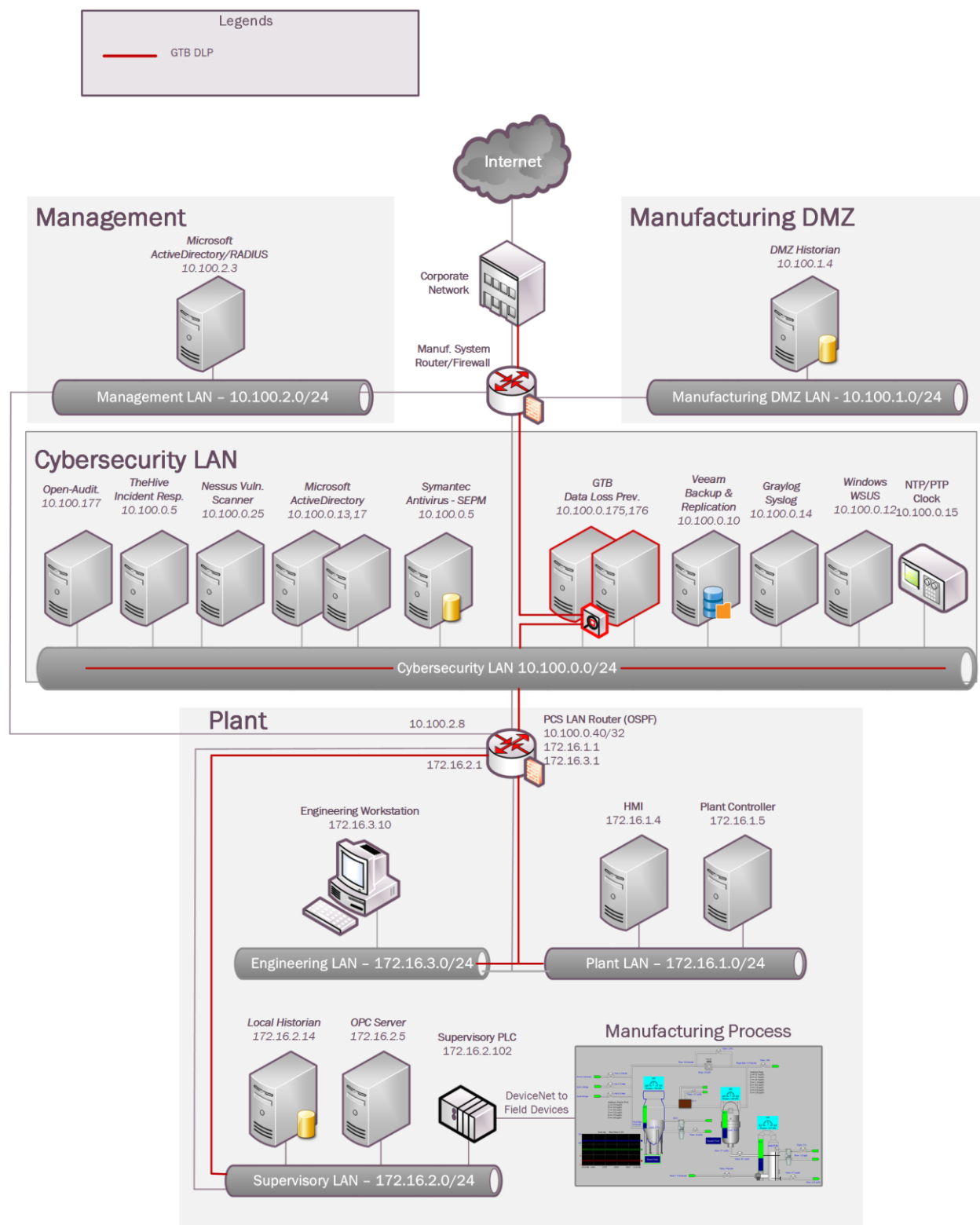
4928 **4.15.2 Technical Capabilities Provided by Solution**

4929 GTB Inspector provides components of the following Technical Capabilities described in
4930 Section 6 of Volume 1:

- 4931 • Data Loss Prevention

4932 **4.15.3 Subcategories Addressed by Implementing Solution**

4933 PR.DS-5

4934 **4.15.4 Architecture Map of Where Solution was Implemented**

4935

4.15.5 Installation Instructions and Configurations

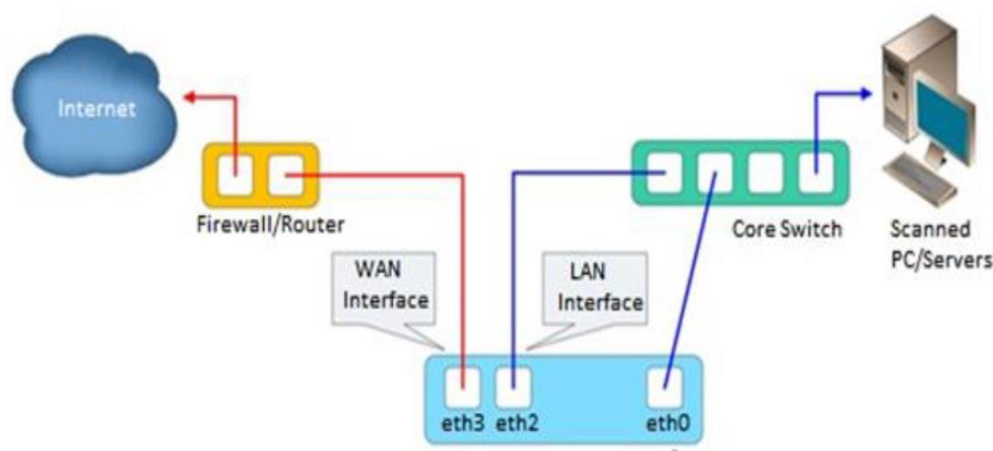
Steps for installing GTB Central Console and Inspector

- Both products are virtual machines and downloadable from <https://gttb.com/downloads/> select desired product for download.
- Once downloaded extract each zip file to its own folder.
- Inside newly created folders there'll be a “**installation guide**” along with the extracted files for each product.
- See attached PDF for current “**system requirements**” for each component being installed.



GTB DLP Installation
Requirements for a G

- Currently “**GTB Inspector**” network configuration is enabled in “**Bridge [Inline]**” mode. This diagram is within “**installation guide**” GTB Inspector DLP, installation methods. Displayed is Bridge [Inline] mode which monitors.



Hyper-V Install Configuration

- Create two virtual machines (See below for current specification of our environment)
- GTB Inspector (VM #1)
 - VHDX -- D:\Hyper-V\GTB Inspector\Virtual Hard Disks\GTB Inspector.vhdx
 - Memory – 16GB (16384MB)
 - Processor – 4 CPU
 - Network Adapter
 - “vswitch_TestBed_LAN” Management Port
 - Management port IP is (10.100.0.175)
 - “Eth2 for GTB Inspector” Connects to Monitor Port 1 on Tap Device
 - “Eth3 for GTB Inspector” Connects to Monitor Port 2 on Tap Device
- GTB Central Console (VM #2)

- 4963 ○ VHDX -- `D:\Hyper-V\GTB Central Console\Virtual Hard Disks\GTB Central Console.vhdx`
- 4964 ○ Memory – 16GB (16384MB)
- 4965 ○ Processor – 4 CPU
- 4966 ○ Network Adapter
- 4967 ■ **“vswitch_TestBed_LAN” Management Port / Connection**
- 4968 ● Management Port / Connection IP is (10.100.0.176)

4969 Install Instructions for Each Virtual Machine and any additional configuration

4970 ● Inspector

- 4971 ○ See install guide for most updated instructions, or attachment below. **Changes**
- 4972 **made within our environment are included below.**
- 4973 ○ Each network connection was installed and rebooted to ensure they were assigned
- 4974 correct name / location, and if not, this command can be used to rename the
- 4975 network to reflect and needed changes. `/usr/local/gtb/libexec/manage_nics -i ethX -o ethX`
- 4976 **(This syntax is included within installation guide)**
- 4977 ○ **IP Address (10.100.0.175)**
- 4978 ○ **Hostname = gtbinspector / gtpinspector.lan.lab**
- 4979 ○ Created DNS A record for “gtbinspector” along with reverse lookup
- 4980 ○ **Configured LDAP integration with Active Directory (10.100.0.17)**
- 4981 ○ **UPN is required for username**
- 4982 ○ **Configured email**
 - 4983 ■ SMTP Server Hostname (**postmark.nist.gov**)
 - 4984 ■ Send email from (GTBInspector@nist.gov)
 - 4985 ■ SMTP Server Port (**25**)
- 4986 ○ Check and ensure LAN and WAN interfaces are configured for eth2 (WAN) eth3
- 4987 **(LAN)**
- 4988 ■ Configuration tab, Network, #-3 and #-4



GTB Inspector
Installation Guide.pdf

4989 4990 ● Central Control

- 4991 ○ See install guide for most updated instructions or attachment below. **Changes**
- 4992 **made within our environment are included below.**
- 4993 ○ **IP Address (10.100.0.176)**
- 4994 ○ **Hostname = gtbcc / gtbcc.lan.lab**
- 4995 ○ Created DNS A record for “gtbcc” along with reverse lookup
- 4996 ○ **Configured LDAP integration with Active Directory (10.100.0.17)**
- 4997 ○ **UPN is required for username**
- 4998 ○ **Configured email**
 - 4999 ■ SMTP Server Hostname (**postmark.nist.gov**)
 - 5000 ■ Send email from (GTBInspector@nist.gov)

5001 ▪ SMTP Server Port (25)



GTB Central Console
Installation Guide.pdf

5002

5003 • **Install information for VMware**

5004 ○ **Install**

5005 ▪ Installed a separate physical machine with vSphere (10.100.0.180) for testing
5006 since problems were observed with Hyper-V ability to block rule violations
5007 with HTTP/HTTPS traffic.

5008 ▪ Configured two network cards in vSphere for pass thru access. This was
5009 completed to give the virtual machine access to physical network cards to
5010 eliminating possible configuration issues being observed in Hyper-V. (Will try
5011 to confirm if possible still exist with Hyper-V since new release from GTB
5012 has been released)

5013 ▪ GTB's Inspector (10.100.0.181) is currently at release 15.4 and contains an
5014 option under **“Configuration → Network”** labeled (Failover Mode). In our
5015 environment this option is set to **“NO”** since we don't have a bypass card
5016 installed. This setting allows all web traffic to be filter via scanning engine.

14 Failover mode No Select "Yes" to enable failover mode of the Bypass Network Card in Bridge and TPROXY. Select "No" to enable fail closed mode.

5017 ▪ Email filtering is designed to use **“MTA”** from Inspector and then forward
5018 along to intended recipient after been scanning for any rule violations.

5019 ▪ Added GTTB Certificate to **“Default Domain Policy”** so any machine within
5020 the domain will update with the required Trusted Certificate Authority so as
5021 not to get a warning message. **(Confirmed working)**

5022

5023 ▪ **Lesson learned:**

5024 ▪ Microsoft Hyper-V solution detects and logs traffic, however even
5025 when configured for blocking, only detection occurs. Support has
5026 indicated that this is since we're not using a bypass network card
5027 stated earlier with a physical box.

5028

5029 ▪ **Performance Impact:**

5030 ▪ This tool has not been configured and ran against ICS enclaves
5031 currently, so there has been no performance impact that were aware of.

5032

5033

5034

5035 Specific configuration steps for GTB's Inspector and Central Console

5036 *This section contains information for configuration within our environment. If scanning email*
 5037 *for content violation, you'll need to configure email clients to point SMTP to 10.100.0.175*
 5038 *(Inspector - MTA) for email scanning. For additional configuration information please see*
 5039 *vendors Administrator Guides which are included in download package from vendor.*

5040 Inspector

5041 Generating and applying License:

- 5042 • **Generating**

- 5043 ○ Click on middle top web page once logged into Inspector

License expires in 349 days

- 5044 •
- 5045 • You will now be directed to a page that allows you to download, email, or
- 5046 upload a license file.
- 5047 • License files should be emailed to support@gttb.com . Support will reply
- 5048 with an updated file to be uploaded.

- 5049 • **When to generate a new license file**

- 5050 ○ Anytime a network change effects the **MAC (Media Access Control)** address for
- 5051 Inspector you'll need to generate a new license key an email support@gttb.com.
- 5052 Before emailing change the extension from **“.dat”** to **“.txt”**. Example: **Inspector**
- 5053 – **“7-31-2018-sysinfo_inspector.dat to 7-31-2018-sysinfo_inspector.txt”**. This
- 5054 change may be required if your email provider blocks **“.dat”** file extension.

- 5055 • **Configuration Setting**

- 5056 ○ Login into GTB Inspector web page and click **“Configuration”** tab.

Events	Rule Viewer	Quarantine	Configuration	Logs	Statistics	Administration
--------	-------------	------------	---------------	------	------------	----------------

- 5057 ○ All setting are accessible via **“Groups”** located on left side of webpage.
- 5058 ○ Central Console = **“gtbcc.lan.lab”**
- 5059

5060

○ **Network = Screenshot below**

Network		
1	Inspector location	GTBInspector.lan.lab
2	Deployment mode	TProxy
3	LAN interface	eth2
4	WAN interface	eth3
5	OOL LAN	10.100.0.0/24, 172.16.3.0/24
6	OOL WAN	
7	TProxy LAN	10.100.0.0/20, 192.168.0.0/20, 172.16.0.0/20
8	TProxy source exceptions	10.100.0.14, 10.100.0.11
9	TProxy destined exceptions	
10	TProxy IP address	10.100.0.175
11	TProxy netmask	255.255.255.0
12	TProxy gateway	10.100.0.1
13	TProxy routing	10.100.0.0/24 via 10.100.0.1 dev eth0 192.168.0.0/20 via 10.100.0.1 dev eth0 172.16.0.0/20 via 10.100.0.1 dev eth0
14	Fallover mode	No
15	OOL/TAP blocking	Yes
16	Blocking interface	eth2
17	DNS servers	10.100.0.17, 10.100.0.13
18	Network Overload Protection	No
19	Network MTU	9000
20	CRC checking	No

5061

5062

5063

○ **Emails Alerts = Screenshot below**

Email Alerts		
1	Security Respondents	wesley.downard@nist.gov, neeraj.shah@nist.gov
2	Special Case Security Respondents	
3	MD5 Recipients	
4	System Administrator Email	wesley.downard@nist.gov, neeraj.shah@nist.gov
5	Notify about system errors by email	Yes
6	Send Emails From	GTBInspector-ICSLab-220-A230@nist.gov
7	SMTP Server Hostname	postmark.nist.gov
8	SMTP Server Port	25
9	Use SSL/TLS	No
10	Email Username	
11	Email Password	
12	Time between Alerts	60
13	Enable HTTP Block Response	Yes
14	HTTP Response Message	http://testpage.gtbtechnologies.com:

5064

5065

5066

5067

○ **LDAP Intergration = Screenshot below**

LDAP Integration		
1	LDAP Server Hostname	10.100.0.17
2	LDAP Server Port	389
3	LDAP Username (bind DN)	gttbldap@lan.lab
4	LDAP Password	*****
5	LDAP SSL	No
6	LDAP Cache Refresh Period	1800
7	Hostnames Cache Refresh Period	3600
8	NRH UDP Port	2222
9	Cache Persistence Timeout	450

5068

309

5069

○ **Mail Transfer Agent = Screenshot below**

Mail Transfer Agent		
1	List Of Allowed Hosts	*
2	Route Emails	Yes
3	Email Username	
4	Email Password	
5	Domain Routing Rules	* 129.6.16.94
6	Excluded domains	
7	Bcc domain inspection	
8	MTA Listening Ports	
9	Email Size Limit	20
10	Alert on Queue Above	4
11	Backup Emails	None
12	Reject Email on fail	No

5070

5071

5072

○ **SIEM = Screenshot below**

SIEM		
1	SIEM Receiver Hostname	10.100.0.27
2	Log Content	Yes
3	Arcsight CEF	Yes

5073

5074

○ **SSL Proxy = Screenshot below****SSL Proxy**

General		
Enable SSL Proxy	Yes <input checked="" type="radio"/> No <input type="radio"/>	Select "Yes" to enable SSL Proxy.
Proxy Port	<input type="text" value="3128"/>	SSL Proxy listening port.
Transparent Proxy HTTP Ports	<input type="text" value="80"/>	List of HTTP ports separated by commas for transparent proxy. Works only in the TPROXY mode. Example 80, 81, 82.
Transparent Proxy HTTPS Ports	<input type="text" value="443"/>	List of ports separated by commas for which HTTPS decryption is performed transparently. Works only in TPROXY mode. Example: 443, 444, 445.
Transparent Proxy Source IP	Yes <input checked="" type="radio"/> No <input type="radio"/>	Select "Yes" to enable source IP address in TPROXY mode (allows user client IP to the firewall).
Enable RESPMOD	Yes <input type="radio"/> No <input checked="" type="radio"/>	Enables server response inspection.
RESPMOD for internal servers	<input type="text"/>	Inspects responses of external requests to internal servers such as OWA, WEB-Servers, etc. Make sure traffic is forwarded on the same port to the Inspector. Example: 192.168.0.10:444, owa.gttb.com:445.
RESPMOD for internal users	<input type="text"/>	List of IP addresses or subnets for which responses inspection is enabled. Example: 192.168.0.0/24, ws12.local
Bypass inspection on failure	Yes <input checked="" type="radio"/> No <input type="radio"/>	Select "Yes" to bypass on failure and forwards traffic without inspection.
Proxy Server Identity	<input type="text" value="gttbinspector"/>	The Inspector name, which is shown in user browsers in case of SSL Proxy errors.
System Administrator	<input type="text"/>	Email address of System Administrator shown in SSL Proxy errors.
Append domain name	<input type="text"/>	Appends local domain name to hostnames without any dots in them. Must begin with a period. Example: .foo.net
Access Control		
Restricted Sources	<input type="text"/>	List of source IP address or subnets which are restricted to use the SSL Proxy. Example: 192.168.1.10, 192.168.2.0/24.
Restricted Destinations	<input type="text"/>	List of destined domains which are basically blocked by SSL Proxy. Example: foo.net, www.bar.net.
Allowed ports	<input type="text"/>	List of ports which are allowed SSL Proxy to connect to. Example: 21,80,443
SSL Decryption		
Current Certificate	Issued to: www.gttb.com CA Issued by: www.gttb.com CA Valid from 06.15.2012 to 05.28.2024	Detailed information about the certificate used for the HTTPS decryption.
Download Certificate	Public certificate Key and certificate	Save and view the certificate used for HTTPS decryption.
Upload Certificate	<input type="button" value="Browse..."/> No file selected.	Customer defined SSL Certificate in PEM format to be used for HTTPS decryption. The file should include both RSA private key and public certificate in plain text.
Block Invalid Sites	Yes <input type="radio"/> No <input checked="" type="radio"/>	Select "Yes" to block destined domains with invalid certificates.
Exception Source List	<input type="text"/>	List of source IP addresses, subnets, or domains for which HTTPS decryption is disabled. Example: 192.168.1.10, 192.168.2.0/24.
Exception Source List file (Upload empty file to clear list)	<input type="button" value="Browse..."/> No file selected.	List of source IP addresses, subnets, or domains for which HTTPS decryption is disabled. Upload empty file to clear it. Each source should be on a separate line no other separators are needed. Example: 192.168.1.10 192.168.2.0/24 foo.net www.bar.net
Exception Source List Download	Source exceptions file was not uploaded.	List of sources IP and domain addresses file download.
Exception Destinations List	<input type="text"/>	List of destined IP addresses, subnets, or domains for which HTTPS decryption is disabled. Example: www.bar.net, .foo.net, 192.168.1.10, 192.168.0.1/24.
Exception Destinations List File (Upload empty file to clear list)	<input type="button" value="Browse..."/> No file selected.	List of destined IP addresses, subnets, or domains for which HTTPS decryption is disabled. Upload empty file to clear it. Each source should be on a separate line no other separators are needed. Example: 192.168.1.10 192.168.2.0/24 .foo.net www.bar.net
Exception Destinations List Download	Destination exceptions file was not uploaded.	List of destination IP and domains address file download.
Enable SSLv2	Yes <input type="radio"/> No <input checked="" type="radio"/>	Select "Yes" to enable SSLv2.
Enable SSLv3	Yes <input type="radio"/> No <input checked="" type="radio"/>	Select "Yes" to enable SSLv3.
Enable TLSv1.0	Yes <input checked="" type="radio"/> No <input type="radio"/>	Select "Yes" to enable TLSv1.0.
Enable TLSv1.1	Yes <input checked="" type="radio"/> No <input type="radio"/>	Select "Yes" to enable TLSv1.1.
Enable TLSv1.2	Yes <input checked="" type="radio"/> No <input type="radio"/>	Select "Yes" to enable TLSv1.2.
<input type="button" value="Apply Settings"/> <input type="button" value="Discard Settings"/>		

5075

5076

5077 • **Administration setting**

5078

5079 ○ Licensing = Used for download and uploading license information.

5080 ○ Health Check = Ability to perform “Self-Test” to check Inspector install health.

5081 ○ Account Manager = Used to add new personal who will be administrating

5082 Inspector or responding to alerts for further investigation.

5083 ○ **System Time = Screenshot below**

System Time

Edit Date/Time: 08/02/2018 11:30:10 Apply

Edit NTP Server: 10.100.0.15 Apply

Select Timezone: (GMT-05:00) Eastern Time (US & Canada) Apply

5084

5085 **Central Console**

5086 Generating and applying License:

5087 • **Generating**

- 5088 ○ Click on middle top web page once logged into Central Console

Please acquire Endpoint licenses (support@gttb.com)

- 5089 •
- 5090 • You will now be directed to a page that will allow you to download, email,
- 5091 or upload a license file.
- 5092 • License files should be emailed to support@gttb.com . Support will reply
- 5093 with an updated file to be uploaded.

5094 • **When to generate a new license file**

- 5095 ○ Anytime a network change effects the **MAC (Media Access Control)** address for
- 5096 Central Console you’ll need to generate a new license key and email it to
- 5097 support@gttb.com. Before emailing change the extension from “.dat” to “.txt”.
- 5098 Example: **Central Console - 7-31-2018-sysinfo_cc.dat to 7-31-2018-**
- 5099 **sysinfo_cc.txt**. This change may be required if your email provider blocks “.dat”
- 5100 file extension.

5101 • **System settings**

- 5102 ○ Click on “DLP Setup” tab

- 5103 ○
- Network (Located under Categories)**

- 5104 • Enter required information. See below for screenshot

Parameter	Value
This Console's IP or Domain name:	10.100.0.176
DNS Server IP :	10.100.0.17,10.100.0.13

- 5105 • Click save to continue.
- 5106

5107

5108 ○ **LDAP**

- 5109 • Enter information for screenshot below. This user has been created and
- 5110 only has Domain User right. Check for password in database.

ID	LDAP Server	Port	Is Forest ?	Domain/Username	Password	Use SSL	Refresh, Hrs
1	10.100.0.17	389	<input type="checkbox"/>	gttblab@lan.lab	*****	<input type="checkbox"/>	24

- 5111 • User name = gttblab@lan.lab
- 5112 • Password = check database
- 5113 • LDAP Server = 10.100.0.17

5115 ○ **Email and alerts**

- 5116 • Enter information from screenshot below

Parameter	Value
Email Server:	10.100.0.175
Email Port:	25
Email User Name:	
Email Password:	
Email Originator:	GTBCC-ICSLab-220-A230@nist.gov
Encryption:	None
Alert manager:	<input type="checkbox"/> Network (SMTP only)

- 5117 • Email Server = 10.100.0.175
- 5118 • Email Originator = GTBCC-ICSLab-220-A230@nist.gov
- 5119 • Click save

5121 ○ **Data and Time**

- 5122 • NTP Server = 10.100.0.15 (Click set time to sync)
- 5123 • Time Zone = Eastern Time (US and Canada) (Click Apply to save)
- 5124 • Click Save

5125 Other settings under **DLP Setup → System** aren't currently configured. These setting will be

5126 updated an included when these features are enabled.

5127 Lesson learned: If integrating with Active Directory using LDAP it's recommended to use

5128 Secure LDAP to ensure user name and password are not sent in plaintext.

5129 **How ACL rules are created for use with GTB DLP Inspector.**

5130 **GTB DLP Inspector views data as it passes thru the device and responds based on**

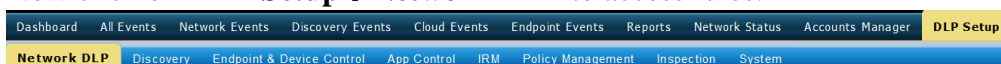
5131 **configured rules.**

5132 **GTB Central Console is the portal were all policy rules and other settings are configured.**

5133 **ACL Rules:**


- 5134 • Login into to Central Console via web browser (E.g. 10.100.0.176).

- 5135 • Now click on **DLP-Setup→Network DLP** to access rules.



- 5136 • Now, look to the left of window under categories and select your Inspector installation.
- 5137



- 5138 • Once selected you will see on the right current **ACL** Rules being applied.
- 5139 • Click Add button. 
- 5140
- 5141 • A new window will appear titled “Add New ACL Rule”

- 5142 • Now type in a name for the new rule being created.
- 5143 • Change Protocol to desire setting. This can be left to “**ANY**” which will look at all protocols passes thru the Inspector (*This may cause a performance impact on you Inspector installation depending on the number of clients within your organization*).
- 5144
- 5145 • **Source:** Choices are → **Any, IP Address, Hostname, Hostname (Custom), and**
- 5146 **Group (User/Computer).**
- 5147 • **Destination:** Choices are → **Any, IP Address, Hostname, Hostname (Custom), and**
- 5148 **Group (User/Computer).**
- 5149 • **File type:** Choices are → **None, All Files, Encrypted, and Extension.**
- 5150
- 5151 • **File Size:** Choices are → **Any, and Not more than.**
- 5152

- 5153
- **Comments:** Give a description of the rule being applied then click **Add** button.

Edit ACL Rule

Rule

Name*: CRS

Protocol*: Any

Source: Any

Destination: Any

File type: None

File size: Any

Comment: This rule applies to Collaborative Robotics System

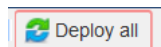
Enforcement:

+ Add - Delete

Policy/Sets	Action	Alerts	File capture	
<input type="checkbox"/> All	Block	Security	<input type="checkbox"/>	↑ ↓

Save Cancel

- 5154
- 5155
- 5156
- 5157
- 5158
- 5159
- 5160
- 5161
- 5162
- 5163
- 5164
- Once Add has been clicked you'll have an option to select a **"Policy/Sets"** to enforce. Default policies that are enforce are (Credit Card Number **CCN** and Social Security Numbers **SSN**).
 - Next, select the action to be taken. There are four choices, **Log**, **Block**, **S-Block**, and **Pass**.
 - Now select if you would like additional personal to be notification upon rule violations.
 - Finally, place a check in **File Capture** if you want to retain a copy of the offending data.
 - Click **Save** to complete.
 - Last step is to click on **Deploy all** button. This sends newly created policy to Inspector. This button will have a red blinking box around it indicating required action.



5166

5167 **Useful Information:**

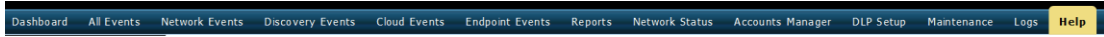
- 5168
- 5169
- 5170
- 5171
- Once a new rule has been created double click on that rule to adjust the ordering from top to bottom by click the **UP** or **Down** arrows towards the right. ↑ ↓
 - Remember rules work from **Top → Down**, so think about ordering process. If unsure move the rule all the way to the top and then click **Deploy all** again.


5172

5173

5174 **How to Fingerprint Files using GTB Security Manager for DLP Protection**5175 **Download:**

- 5176 • First download “**GTB Security Manager**” by clicking on **Help** tab within Central
5177 Console server web portal then select “**GTB Security Manager**” link to start download.

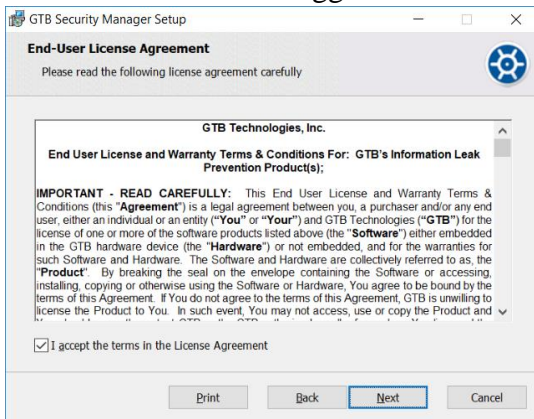


5178  [GTB Security Manager \(19 MB\) - Fingerprinting Management System](#)

- 5179 • Select location to save file being downloaded.
5180 • Double click to start install for “**GTBSecurityManager_15.3.0.msi**” from location
5181 where file was saved to (version number might be different than one listed above).
5182 • Once first screen appears click on “**Next**” to continue.
5183

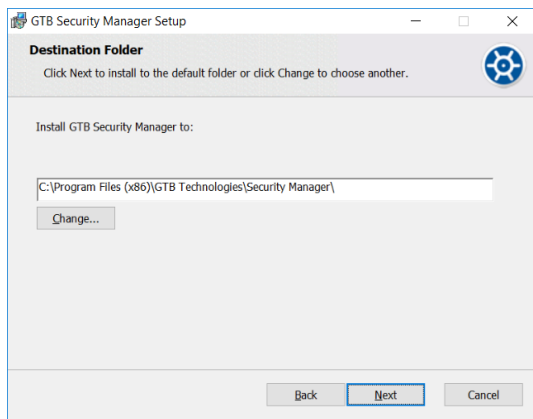


- 5184 • Select Yes to License Agreement and click “**Next**” to continue.
5185

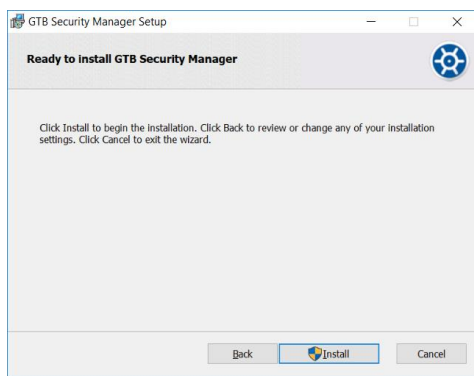


5186

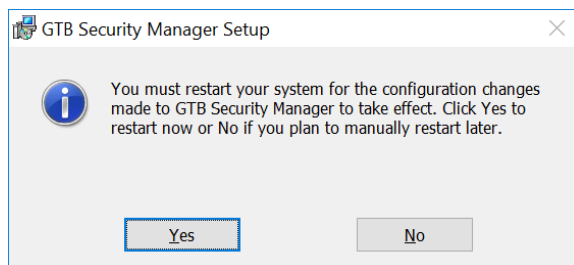
- 5187
- Leave Destination Folder as default and Click **“Next”**



- 5188
- 5189
- Click **“Install”** to continue.

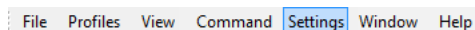


- 5190
- 5191
- 5192
- 5193
- 5194
- 5195
- 5196
- 5197
- 5198
- When prompted by **User Access Control (UAC)** enter administrator password to continue install.
 - If prompted to close Open Applications, select either option. Reboot is required if second option is selected.
 - Click **“OK”** to continue.
 - Once install has completed click **“Finish”** to complete install.
 - If prompted to reboot, select **“Yes”**. **MAKE SURE TO SAVE ALL OPEN FILES BEFORE SELECTING “YES”**

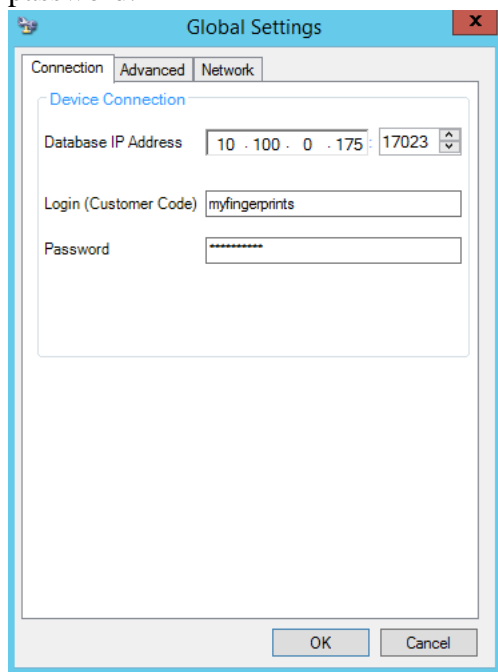


- 5199
- 5200
- 5201
- 5202
- Once machine has completed rebooting open **“GTB Security Manager”** by right click and selecting **“Run as administrator”**
 - When prompted enter administrator password for application to start.

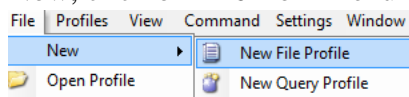
- Once “**GTB Security Manager**” has opened, click on setting button on menu bar.



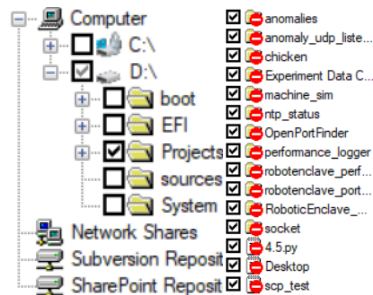
- Now enter the IP Address of where “**Central Console**” is installed. Login and password are already populated with default credentials from vendor. Both can be changed. See foot notes for additional steps required to change Fingerprint Inspections login and password.



- Once IP Address has been entered click “**OK**” to save changes.
- Now, click on **File** from menu bar and select **New → New File Profile**




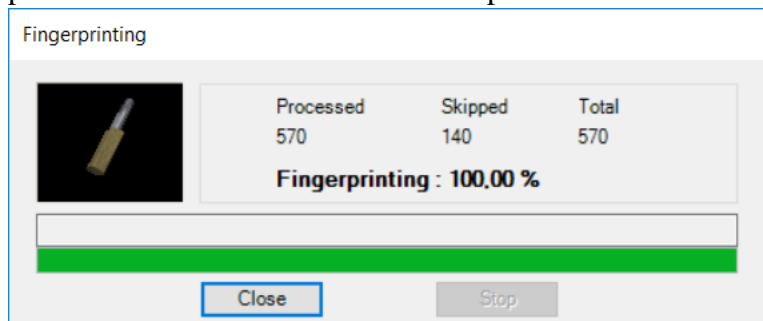
- A new window will appear allowing the ability to select files to be added. Files can be copied to **Local Machine**, or accessed from a **Network Share**, **Subversion Repositories**, or **SharePoint Repositories**.
- Select the folder, or files that need fingerprinting. Once a folder is selected all files within selected folder will receive a check mark indicating which files will be fingerprinted.

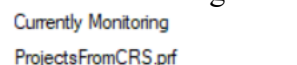


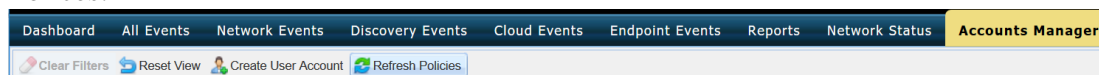
- Now click on floppy disk icon to save.
- Select location to save newly created profile.



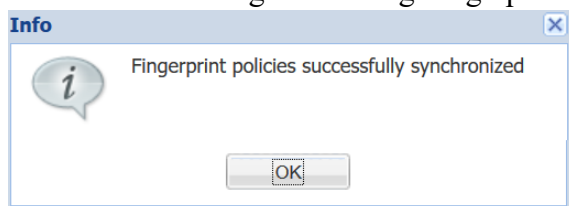
- 5221 • Now the profile has been saved click the **padlock** icon to start fingerprinting process 
- 5222 (Depending on the number of files being fingerprinted this can take a few minutes).
- 5223 • To view the process see the Output screen that will display what files have been
- 5224 processed and there status. Once completed click **Close**



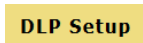
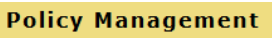
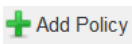

- 5225 • Now look to the right side window for a tab labeled “**Profiles**” if this is missing click on
- 5226 “**View**” from menu bar and select “**Profiles Window**”. Click on Profile tab and a slide
- 5227 out appears show all the Profiles that can be monitored.
- 5228 • Now select the Profile that was created earlier and right click, then select **Start**
- 5229 **Monitoring**.
- 5230 • Once monitoring is enabled it’ll appears under “**Currently Monitoring**” under help.
- 5231 
- 5232 • Files that were included in fingerprinting profile will now have **ACL rules applied from**
- 5233 **Network DLP section from Central Console**.
- 5234 • Login to **Central Console** and navigate to **Account Manager** Tab and click Refresh
- 5235 **Polices**.
- 5236



- 5237 You’ll see a message indicating Fingerprint polices successfully synchronized.
- 5238



- 5239
- 5240 **How to add policy to GTB Central Console for detecting fingerprinted files**

- 5241 • Login to Central Console
- 5242 • Click on DLP Setup tab. 
- 5243 • Now select Policy Management tab. 
- 5244 • Now double click on Default to launch a new window.
- 5245 • Click Add Policy. 
- 5246 • Click drop down and select File. 

- 5247
- Now click save button for setting to be applied.

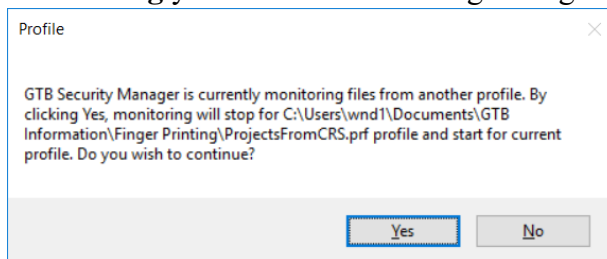
5248 All fingerprinted files from above steps will automatically be added to default Network DLP
5249 policy applied ACL. New Default values are “SSN, CCN, and File”

5250

5251 Additional Information for Fingerprinting:

- 5252
- Recommended to configured **GTB Security Manager** to connect to IP address of DLP
5253 Inspector.

- 5254
- Fingerprint only allows for one active Profile at a time. If another profile is set to **Start**
5255 **Monitoring** you’ll receive a warning asking if you’d like to disable the active profile.

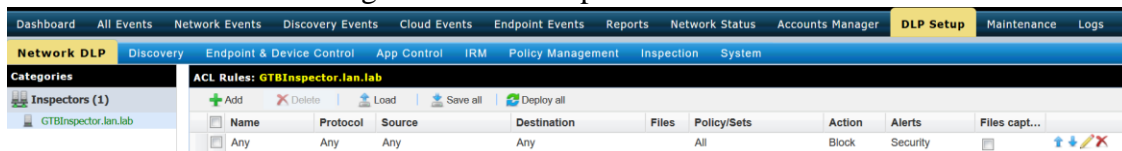


5256

- 5257
- Recommendation would be to install **GTB Security Manager** on a machine that can be
5258 the central repository for all fingerprinted files. Creating a large folder where the files can
5259 be placed into for fingerprinting. Files don’t have to remain in saved location once the
5260 profile has been fingerprinted and uploaded to **Central Console**. Access to fingerprinted
5261 files is only required when changes are made to profile containing said files.

- 5262
- Although only one profile is able to be monitored at a time you are able to define multiple
5263 Policies within that profile. This is useful since when a fingerprint violation is triggered it
5264 will be tagged with the Defined Policy name, which allows for easier usability.

- 5265
- Fingerprinted files follow **ACL Rules**: created within **Central Console** under **DLP**
5266 **Setup → Network DLP**. Rules are processed in order from top to bottom. This means
5267 the first rule with a matching violation takes precedence over rules below.



5268

5269

5270

5271

5272 4.15.6 Highlighted Performance Impacts

5273 No performance measurement experiments were performed for the installation of GTB into the
5274 PCS due to its location within the network topology. No manufacturing process components
5275 across the boundary on a regular basis while the system is operational.

5276 4.15.7 Link to Entire Performance Measurement Data Set

5277 N/A

5278

5279 4.16 Graylog

5280 4.16.1 Technical Solution Overview

5281 Graylog is an open source log management tool. It can collect, parse and enrich logs, wire
5282 data, and event data from any data source. Graylog also provides centralized configuration
5283 management for 3rd party collectors such as beats, fluentd and nxlog. The processing
5284 pipelines allow for greater flexibility in routing, blacklisting, modifying and enriching
5285 messages in real-time as they enter Graylog. It has a powerful search syntax to help query
5286 exactly what we are looking for. With Graylog one can even create dashboards to visualize
5287 metrics and observe trends in one central location.²⁸

5288 Points to consider

- 5289 • Open source product with good community support
- 5290 • Easy to setup and customize. Support log collection from any OS platform.
- 5291 • It is packaged for major Linux distributions, has a VM ready for use and Docker images are
5292 also available.
- 5293 • The dashboard part, even if though well integrated and useful, lacks many features and
5294 visualizations contained in other elastic search tools such as Kibana (like aggregations).

5295 4.16.2 Technical Capabilities Provided by Solution

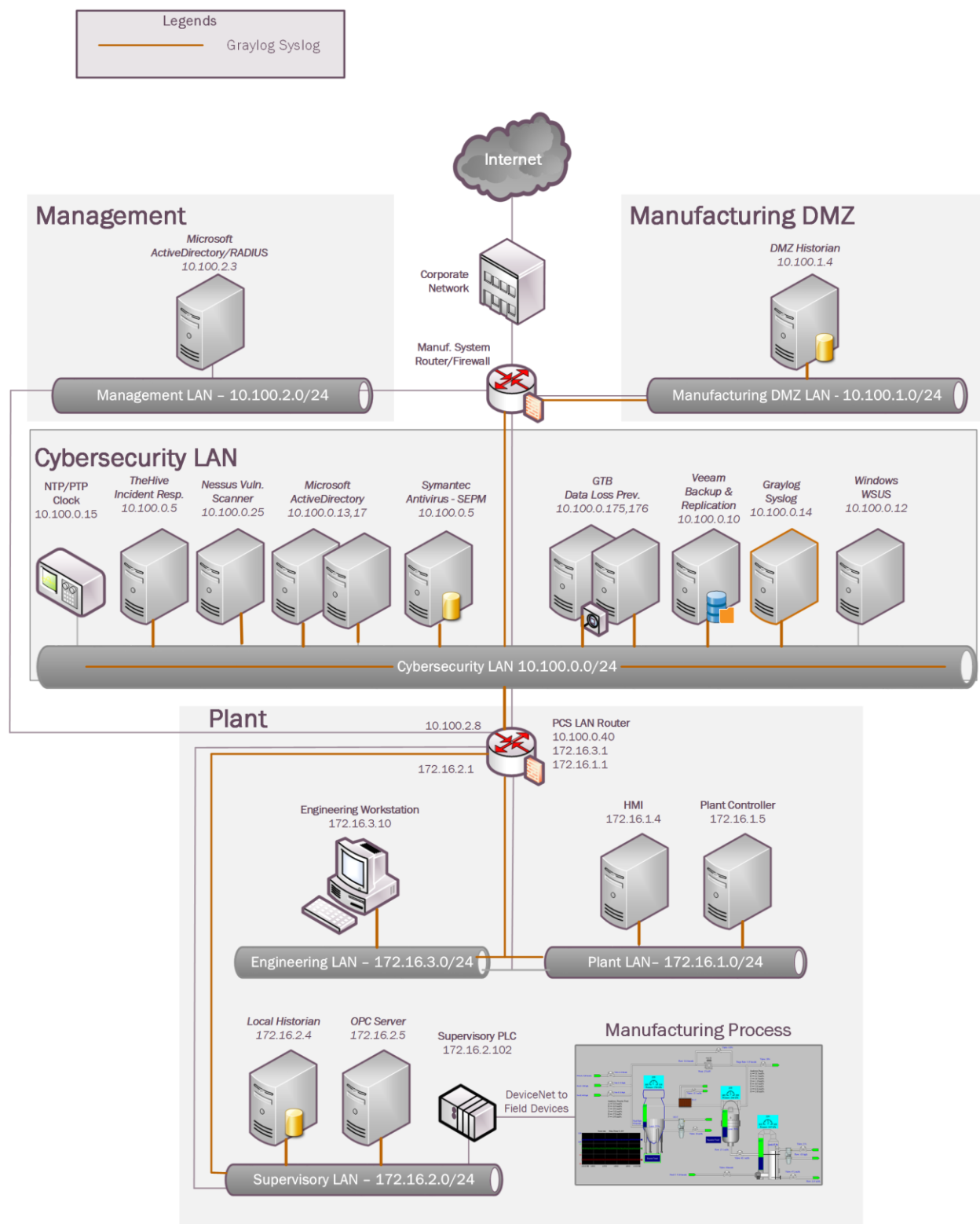
5296 Graylog provides components of the following Technical Capabilities described in Section 6 of
5297 Volume 1:

- 5298 • Network Monitoring
- 5299 • Event Logging
- 5300 • Forensics

5301 4.16.3 Subcategories Addressed by Implementing Solution

5302 PR.DS-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-6, DE.DP-3, RS.AN-3

²⁸ Graylog Documentation <http://docs.graylog.org/en/3.0/>

5303 **4.16.4 Architecture Map of Where Solution was Implemented**

5304

5305

5306 **4.16.5 Installation Instructions and Configurations**

5307 Details of the solutions implemented:

Name	Version	Daily volume of logs	Server
Graylog Enterprise	2.4.6	< 5GB per day	Ubuntu 14

5308

5309 **Setup:**

- 5310 • Download the installation package from the Graylog website (<https://www.graylog.org/>).
5311 Graylog can be installed on any flavor of Linux. In addition, Graylog also provides a
5312 preconfigured virtual machine for **non-production** environments. This virtual machine
5313 template (OVA) file was used in our environment.
- 5314 • The OVA file was deployed on a Microsoft Hyper-V host server in our Cybersecurity LAN
5315 network.
- 5316 • The Graylog server at a minimum requires UDP port 514 which is the default syslog port to
5317 be opened. Accordingly, UDP 514 was permitted in the firewall rules. Additional ports such
5318 as UDP 5415 and 12202 are also used if configuring other features of Graylog as described in
5319 the [documentation](#).
- 5320 • Upon deploying the OVA file, the virtual machine will default to a DHCP IP address. Login
5321 to the system to assign it a static IP address as per below shown instructions.
5322

Assign a static IP

Per default the appliance make use of DHCP to setup the network. If you want to access Graylog under a static IP please follow these instructions:

```
$ sudo ifdown eth0
```

Edit the file `/etc/network/interfaces` like this (just the important lines):

```
auto eth0
iface eth0 inet static
address <static IP address>
netmask <netmask>
gateway <default gateway>
pre-up sleep 2
```

Activate the new IP and reconfigure Graylog to make use of it:

```
$ sudo ifup eth0
$ sudo graylog-ctl reconfigure
```

Wait some time until all services are restarted and running again. Afterwards you should be able to access Graylog with the new IP.

- Login to the Web Interface using the default credentials and change the admin password.
- Active Directory (AD)-integration is supported in Graylog. To configure, on the Top Menu Bar, Click on **System >> Authentication**. On the Authentication Management page, click on **LDAP / Active Directory** and fill out the AD server details. Detailed instructions can be found in product documentation.²⁹
 - Note: Any AD domain user that's added is assigned "**Reader**" access by default. This can be changed by configuring **Group Mapping** options in the same page. Change the Default User Role depending on your requirement. Adding permissions can be assigning by clicking on **LDAP Group Mapping** button on the same page

²⁹ Configuring External Authentication in Graylog
http://docs.graylog.org/en/2.3/pages/users_and_roles/external_auth.html?highlight=ldap

4. Group Mapping (optional)

Group Search Base DN	<div style="border: 1px solid #ccc; padding: 5px; min-height: 20px;">Group Search Base</div> <p>The base tree to limit the LDAP group search query to, e.g. <code>cn=users,dc=example,dc=com</code>.</p>
Group Search Pattern	<div style="border: 1px solid #ccc; padding: 5px; min-height: 20px;">Group Search Pattern</div> <p>The search pattern used to find groups in LDAP for mapping to Graylog roles, e.g. <code>(objectClass=groupOfNames)</code> or <code>(&(objectClass=groupOfNames)(cn=graylog*))</code>.</p>
Group Name Attribute	<div style="border: 1px solid #ccc; padding: 5px; min-height: 20px;">Group Id Attribute</div> <p>Which LDAP attribute to use for the full name of the group, usually <code>cn</code>.</p>
Default User Role	<div style="border: 1px solid #ccc; padding: 5px; min-height: 20px;">Reader - basic ▾</div> <p>The default Graylog role determines whether a user created via LDAP can access the entire system, or has limited access. You can assign additional permissions by mapping LDAP groups to Graylog roles, or you can assign additional Graylog roles to LDAP users below.</p>

5338

5339 Configuration:

5340 Syslog from Windows servers:

- 5341 • NXLOG (<https://nxlog.co/>) was used to forward logs from the Windows hosts in the Process
- 5342 Control System. The free community edition of NXLOG was installed on each windows
- 5343 host. In addition, it was also installed on Active Directory servers in Cyber-security LAN
- 5344 network.
- 5345
- 5346 • Once NXLOG is installed, edit the nxlog.conf file located at **C:\Program Files**
- 5347 **(x86)\nxlog\conf** directory as per whichever category of events you want to forward to your
- 5348 Graylog server. Detailed instructions on NXLOG configuration can be found on its website.³⁰
- 5349 Below is a sample nxlog.conf from one of the Windows hosts in the Process Control system
- 5350

³⁰ <https://nxlog.co/documentation/nxlog-user-guide/>

```

## Please set the ROOT to the folder your nxlog was installed into,
## otherwise it will not start.

#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog

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

<Extension _syslog>
  Module xm_syslog
</Extension>

<Input in>
  Module im_msvistalog
  ReadFromLast True
  Query <QueryList>\
    <Query Id="0">\
      <Select Path="System">*[System[(EventID=1074)]]</Select>\
      <Select Path="Application">*[System[(EventID=1034)]]</Select>\
      <Select Path="Security">*[System[(EventID=4625)]]</Select>\
      <Select Path="Security">*[System[(EventID=4689)] and
EventData[Data[@Name='ProcessName'] and (Data='C:\Program Files (x86)\Common
Files\Rockwell\RsvcHost.exe')]]</Select>\
      <Select Path='Microsoft-Windows-TerminalServices-
LocalSessionManager/Operational'>*</Select>\
      <Select Path="Veeam Agent">*[System[(EventID=190)]]</Select>\
      <Select Path="FTDiag">*[System[(EventID=1001)]]</Select>\
    </Query>\
  </QueryList>
</Input>

<Output out>
  Module om_udp
  Host 10.100.0.14
  Port 514
  Exec to_syslog_bsd();
</Output>
<Route 1>
  Path in => out

```

5351
5352

5353 As per the screenshot above, we have configured it to forward the below types of events

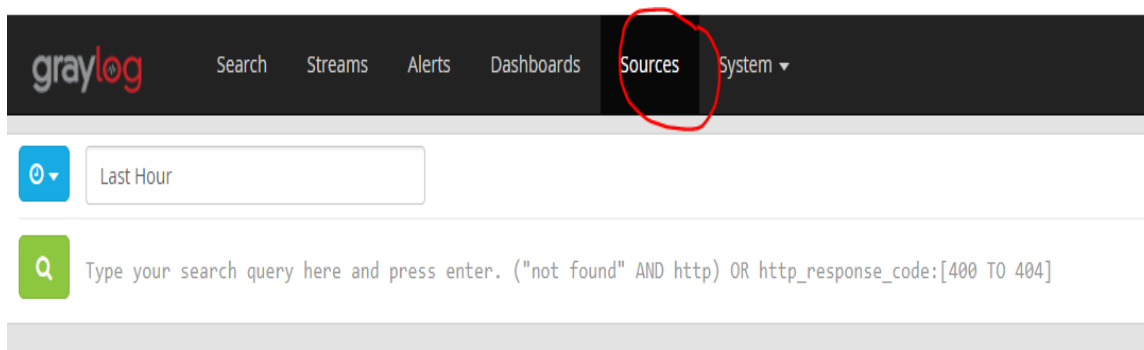
5354 ➤ Event ID 1074 from “System” category to notify us when system gets rebooted

- 5355 ➤ Event ID 1034 from “Application” category
 5356 ➤ Event ID 4625 from “Security” category
 5357 ➤ Event ID 4689 from “Security” category and ProcessName= to notify us when the
 5358 process for Rockwell Automation software stops.
 5359 ➤ All events [*] from “*Microsoft-Windows-TerminalServices-LocalSessionManager*”
 5360 category to notify us when a user logs in or logs out of the system.
 5361 ➤ Event ID 190 from Veeam category to notify us for backup completion messages
 5362 ➤ Event ID 1001 from FTDiag category which is a custom event ID generated by Factory
 5363 Talk Administration Software where there is an authentication failure.

5364 You can add other categories like “**Application**” or “**System**” should you need to collect
 5365 those events as well. Ensure to balance out the type of events you are sending from your
 5366 host. Too much noise will eventually make it difficult to search for meaningful logs in
 5367 Graylog.

5368 Save the nxlog.conf once edited and restart the **NXLOG** windows service. The device will
 5369 now begin sending syslog (events) to the Graylog server. If the service fails to start, please
 5370 check the syntax of your nxlog.conf file for any blank spaces or missing parenthesis.
 5371 Nxlog.conf file is very **sensitive** to proper indentation.

- 5372 • Login to Graylog Web UI and you should start seeing the events from these windows hosts.
 5373 Click on “**Sources**” in the Top menu bar to verify if the windows host shows up under the list
 5374 of “Selected sources”. Any device which you configure to send syslog data should begin
 5375 showing up here under “**Selected Sources**” assuming your configuration is correct. If you
 5376 don’t see your device in here, verify the nxlog config and network connectivity between the
 5377 end device and Graylog server.



Sources

This is a list of all sources that sent in messages to Graylog. Note that the list is cached for a few seconds so you might have to wait a bit until a new source



Use your mouse to interact with the table and graphs on this page, and get a better overview of the sources sending data into Graylog.

5378

Selected sources

Search Show: 100 ▼

Name	Percentage	Message count	
Top sources			
lan-ad.lan.lab	53.40%	636	Q
ciscoasa	31.40%	374	Q
ruggedcom	8.82%	105	Q
fgs-47631ehh.lan.lab	5.12%	61	Q
vcontroller1	0.25%	3	Q
mintaka	0.25%	3	Q
polaris	0.25%	3	Q

5379

5380

- 5381 • Search for events from a host by entering a search query and selecting the appropriate time
5382 interval in the home page.

5383 For example: To search for events by hostname, enter “*source: <windows hostname>*”
5384 (without quotes) in the Search *box* as shown below

graylog Search Streams Alerts Dashboards Sources System ▼

Search in the last 5 minutes ▼

Q source:fgs-47631ehh.lan.lab

Search result
Found **93 messages** in 23 ms, searched in **1 index**.
Results retrieved at 2017-08-17 10:32:53.

Add count to dashboard ▼ Save search criteria

More actions ▼

Fields Decorators

Histogram
Year, Quarter, Month, Week, Day, Hour, Minute

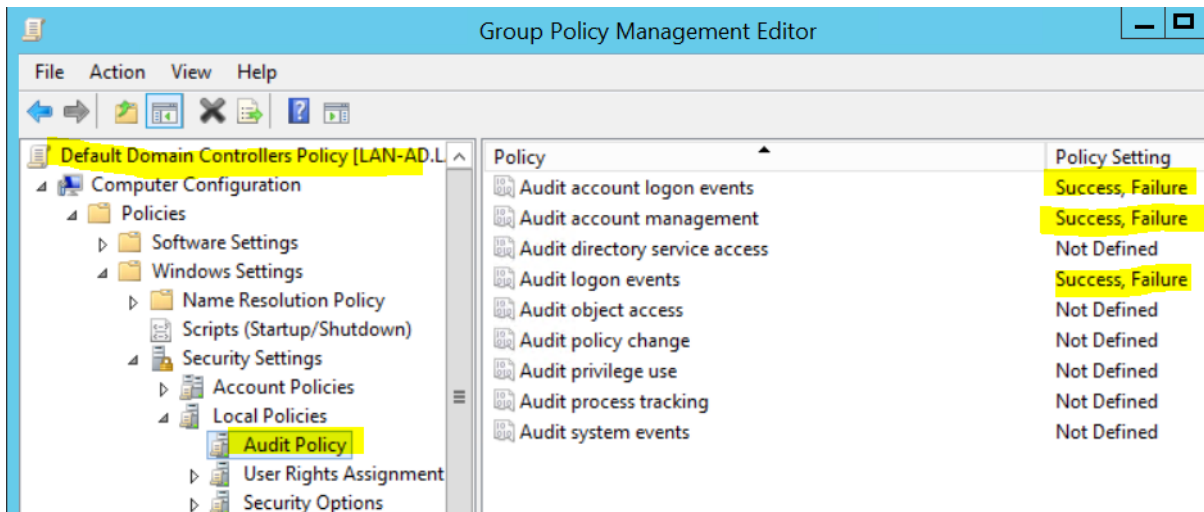
5385

5386

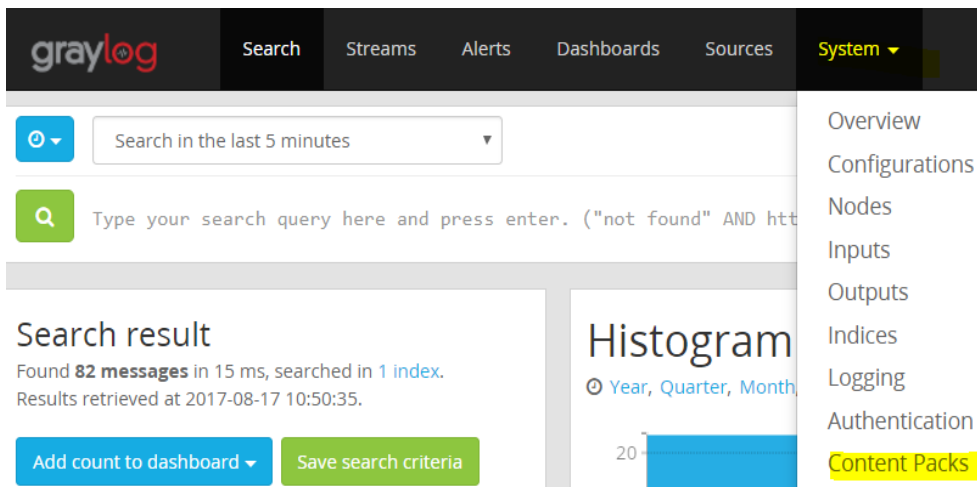
5387

5388 Syslog from Active Directory Domain Controllers

- 5389 • The **nxlog.conf** configuration remains same on the Domain Controllers as that for a member
 5390 server except the PORT number to send the data on. In addition, there is a **Content** pack
 5391 available at Graylog Marketplace, which if installed can parse Active Directory events and
 5392 generate useful graphs. This content pack requires a different **UDP Port (5414)**.
 5393 Accordingly, this port was used in the nxlog.conf of the Domain Controllers instead of the
 5394 default 514. The AD content pack can be downloaded from:
 5395 <https://marketplace.graylog.org/addons/750b88ea-67f7-47b1-9a6c-cbbc828d9e25>
 5396
 5397 • Ensure to first enable **Auditing** on Domain Controllers (as mentioned in the Requirements
 5398 section of the Content pack) prior to importing this content pack. This can be done using the
 5399 “**Default Domain Controllers Policy**” in the Group Policy Management Console on the
 5400 Domain Controller.
 5401

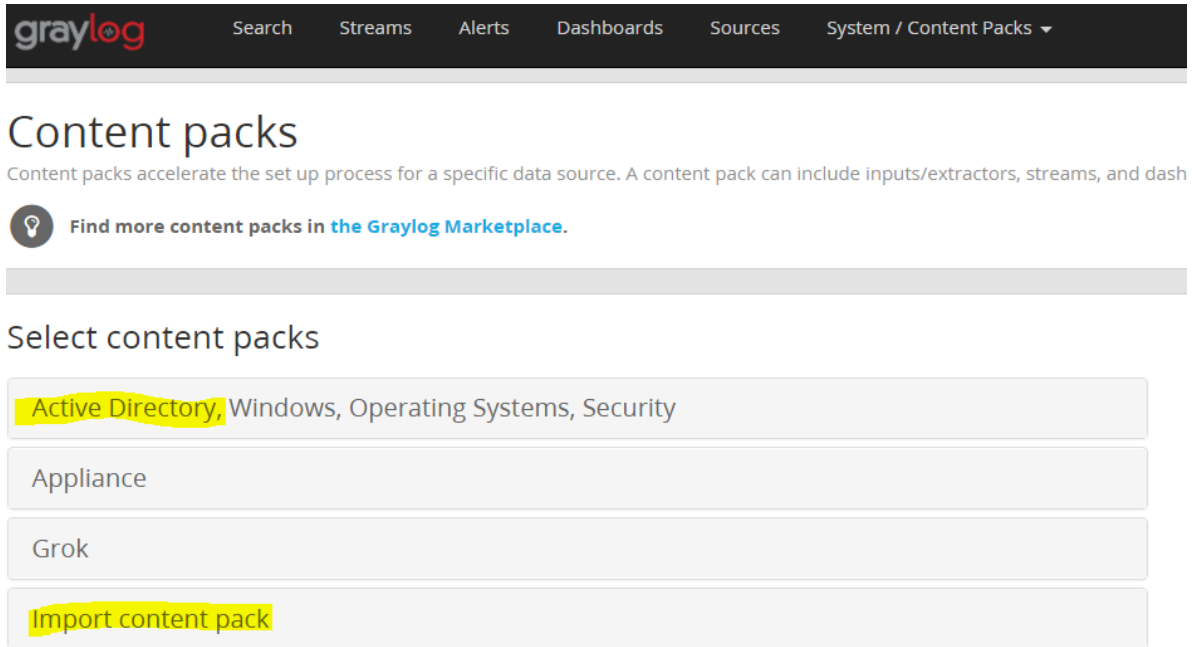


- 5402
 5403
 5404 • Next, login to the Graylog Web UI. Click on “System” >> “Content Packs”

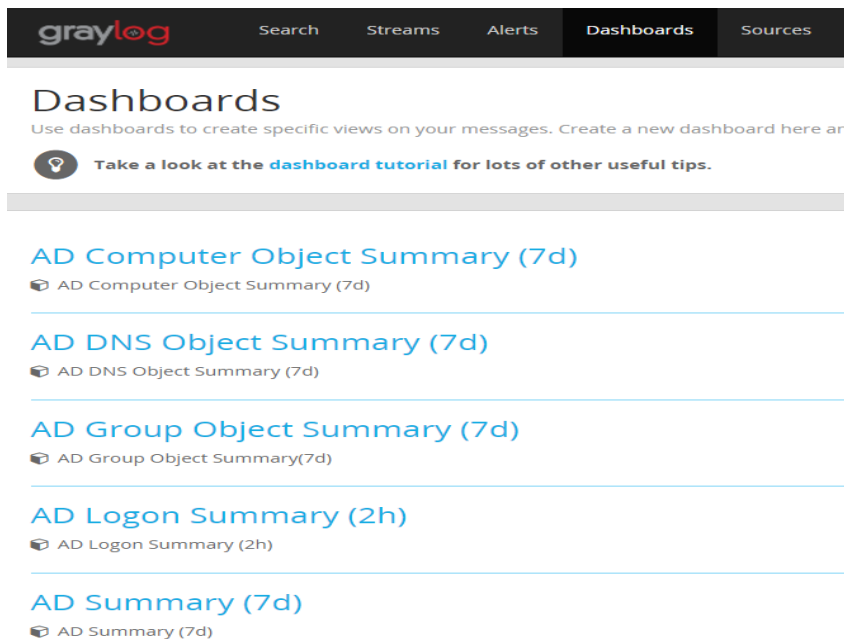


5405

- 5406 • Download the Active Directory Content pack. Next, click on “**import content packs**” to
 5407 import it. Once import is completed you should see “**Active Directory**” under “Select
 5408 Content packs”. This is the pack we just imported.
 5409



- 5410 • Click on “**Dashboards**” to view the new graphs of the AD user and group activities. The
 5411 graphs will begin populating data assuming the AD server is successfully sending over the
 5412 events to Graylog server.
 5413



5414

- 5415 • On the main dashboard look for events from the AD server. Use the search query as
5416 explained in previous steps to look for events using the server hostname.

5417

5418

- 5419 • **Note:** Likewise, there are lot of useful Content packs and plugins available at [Graylog](#)
5420 [Marketplace](#) for vendor specific technologies / devices such as Cisco, Microsoft DNS, Bro
5421 IDS, Cacti, Symantec etc. Download and install each as per the infrastructure in your
5422 environment.

5423 Syslog from Boundary Firewall/Network Devices:

- 5424 • All network devices such as switches and boundary routers from Process Control system
5425 were configured to send their syslog data to the Graylog server. There is a device specific
5426 setting in each network device to log to a Syslog server. This can be done either via Web UI
5427 or CLI of the device.

5428

5429 The below commands were used on the Boundary Router of the system which is an Allen
5430 Bradley Stratix firewall.

5431

5432

5433

5434

- Enable
- configure terminal
- logging enable
- logging 10.100.0.14
- (Optional) To limit the messages sent based on priority level, enter:
- logging trap informational
- end
- wr mem

- It was observed that these messages however ended up in Graylog under the device's **IP address** as the **Source** instead of its hostname. This is an expected behavior as different vendor devices log in different formats.

To overcome this, Graylog offers native features such as Pipelines, Rules, Grok Patterns and Lookup Tables to get around this. Their documentation offers details on creating these <http://docs.graylog.org/en/2.4/pages/pipelines.html>
Additional guidance on creating pipelines can be found at <https://jalogisch.de/2018/working-with-cisco-asa-nexus-on-graylog/>

Configuring Pipelines /Rules for Network devices:

- The following screenshots show some pipelines and rules that were created.

Pipelines can be created by clicking on **System/Pipelines >> Pipelines** option in the TOP Menu bar

Pipelines overview

Pipelines let you transform and process messages coming from streams. Pipelines consist of stages where rules are evaluated and applied. Messages can go through one or more stages.

[Read more about Graylog pipelines in the documentation.](#)


Manage pipelines Manage rules Simulator

Filter pipelines Filter Reset [Add new pipeline](#)

Pipeline	Connected to Streams	Processing Timeline	Actions
Correct ASA Name Correct ASA Name Throughput: 0 msg/s	All messages	Stage 0	Delete Edit
Correct PCS 8300 Router Name Throughput: 0 msg/s	All messages	Stage 0	Delete Edit
Correct PCS Vlan01 Switch Name	All messages		Delete Edit

Pipeline Rules

Rules are a way of applying changes to messages in Graylog. A rule consists of a condition and a list of actions. Graylog evaluates the condition against a message and executes the actions if the condition is satisfied.

 Read more about Graylog pipeline rules in the [documentation](#).

Filter Rules

Filter

Reset

Create Rule

Title	Description	Created	Last modified	Throughput	Errors	Actions
Correct CiscoASA hostname	Correct CiscoASA hostname	4 months ago	4 months ago	0 msg/s	0 errors/s (0 total)	<div>DeleteEdit</div>
Correct PCS 8300Router Name	Correct PCS 8300Router Name	4 months ago	4 months ago	1 msg/s	0 errors/s (0 total)	<div>DeleteEdit</div>
Correct PCS Vlan01 Switch	Correct PCS Vlan01 Switch Name	4 months ago	4 months ago	0 msg/s	0 errors/s (0 total)	<div>DeleteEdit</div>
Correct PCS Vlan02 SwitchName	Correct PCS Vlan02 Switch Name	4 months ago	4 months ago	0 msg/s	0 errors/s (0 total)	<div>DeleteEdit</div>
Correct Siemens Switch hostname	Correct i800 SwitchName	4 months ago	4 months ago	0 msg/s	0 errors/s (0 total)	<div>DeleteEdit</div>

- The following screenshots show details of one such pipeline “**Correct PCS 8300 Router Name**” and its corresponding rule “**Correct PCS 8300 Router Name**” that was created to make the Allen Bradley Boundary Router display its hostname correctly.

Pipeline *Correct PCS 8300 Router Name*

Pipelines let you transform and process messages coming from streams. Pipelines consist of stages where rules are evaluated and applied. Messages can go through one or more stages.

[Manage pipelines](#)[Manage rules](#)[Simulator](#)

After each stage is completed, you can decide if messages matching all or one of the rules continue to the next stage.

Details

[Edit pipeline details](#)

Title: Correct PCS 8300 Router Name
Description:
Created: 4 months ago
Last modified: 4 months ago
Current throughput: 1 msg/s

Pipeline connections

This pipeline is processing messages from the stream "All messages".

[Edit connections](#)

Pipeline Stages

Stages are groups of conditions and actions which need to run in order, and provide the necessary control flow to decide whether or not to run the rest of a pipeline.

[Add new stage](#)

Stage 0 Contains 1 rule

There are no further stages in this pipeline. Once rules in this stage are applied, the pipeline will have finished processing.
Throughput: 1 msg/s

[Delete](#)[Edit](#)

Title	Description	Throughput	Errors
Correct PCS 8300Router Name	Correct PCS 8300Router Name	0 msg/s	0 errors/s (0 total)

Rule: Click on “**Manage Rule**” to create a rule to associate with the pipeline.

Rule source

```
1 rule "Correct PCS 8300Router Name"
2   when
3     has_field("source") AND contains(to_string($message.source), "10.100.0.40")
4   then
5     set_field("source", "PCS-AB8300");
6   end
```

- 5466 • End Result in the “Search” pane now shows the hostname “PCS-AB8300” as configured in
5467 the Rule.
5468

The screenshot displays the Graylog Search interface. The top navigation bar includes the Graylog logo, a 'Search' button, and links for Streams, Alerts, Dashboards, Sources, and System. On the right, it shows 'In 0 / Out 0 msg/s', 'Help', and 'Admin'.

The left sidebar shows the 'Search result' section with the following text: 'Found 141 messages in 12 ms, searched in 1 index. Results retrieved at 2019-03-28 12:20:39.' Below this are buttons for 'Add count to dashboard', 'Save search criteria', and 'More actions'.

The main search results pane displays a list of messages. The first message is highlighted with a yellow background and shows the hostname 'PCS-AB8300'. The message content is: '%SEC-6-IPACCESSLOGP: list plant-vlan-acl permitted tcp 172.16.1.4(51211) -> 172.16.2.5(1332), 1 packet'. The second message shows the hostname 'PCS-AB8300' and the content: '%SEC-6-IPACCESSLOGP: access-list logging rate-limited or missed 61 packets'. The third message shows the hostname 'PCS-AB8300' and the content: '%SEC-6-IPACCESSLOGP: list plant-vlan-acl permitted tcp 172.16.1.4(3389) -> 172.16.3.10(56806), 481 packets'. The fourth message shows the hostname 'PCS-AB8300' and the content: '%SEC-6-IPACCESSLOGP: list Manf-vlan-ACL permitted tcp 172.16.2.5(50006) -> 172.16.1.5(56551), 1292 packets'. The fifth message shows the hostname 'PCS-AB8300' and the content: '%SEC-6-IPACCESSLOGP: list Manf-vlan-ACL permitted tcp 172.16.2.5(3389) -> 172.16.3.10(51187), 546 packets'.

5469
5470

5471 Configuring Email Notifications for Alert conditions:

- 5472 • You can create email alerts for any custom events, alert condition as per your requirement.
5473 Below process show how our Graylog was configured to send out email notifications, for any
5474 Veeam backup events that it received from the Windows clients. Follow this process to
5475 define your custom alert conditions
- 5476 • There are multiple configuration settings required for email notification to work – Creating a
5477 **stream**, adding an **alert condition** and creating a **notification**.
- 5478 • To create a stream, click on **Streams** on the Top-Menu >> **Create a Stream** >> Enter Title,
5479 Description, and Index Set which should default to “**Default index set**”
- 5480 • Click **Save** to save the changes
5481

Editing Stream



Title

Backup Notifications



Description

Backup Messages

Index Set

Default index set



Messages that match this stream will be written to the configured index set.

☐ Remove matches from 'All messages' stream

Remove messages that match this stream from the 'All messages' stream which is assigned to every message by default.

Cancel

Save

- 5482
- 5483 • Next, click on “**Alerts**” options on the top menu >> Click on **Manage conditions** >> Click
- 5484 on **Add new condition** to define a condition.
- 5485 • Click drop menu under “**Alert on Stream**” and select the stream created earlier. Click on
- 5486 “**Condition Type**” menu drop down and select “**Message Count Alert Condition**”
- 5487

Condition

Define the condition to evaluate when triggering a new alert.

Alert on stream

Backup Notifications



Select the stream that the condition will use to trigger alerts.

Condition type

Message Count Alert Condition



Select the condition type that will be used.

- 5488
- 5489 • Click “**Add Alert Condition**”. Once window appears fill out the required information.
- 5490

5491
5492
5493

- Click **Save** to complete (See below for example of current Message Count Alert Condition).

Update *Veeam Backup Alerts*

Message Count Alert Condition description

This condition is triggered when the number of messages is higher/lower than a defined threshold in a given time range.

Title

Veeam Backup Alerts

The alert condition title

Time Range

2

Evaluate the condition for all messages received in the given number of minutes

Threshold Type

more than

Select condition to trigger alert: when there are more or less messages than the threshold

Threshold

0

Value which triggers an alert if crossed

Grace Period

1

Number of minutes to wait after an alert is resolved, to trigger another alert

Message Backlog

1

The number of messages to be included in alert notifications

☒ Repeat notifications (optional)

Check this box to send notifications every time the alert condition is evaluated and satisfied regardless of its state.

Cancel
Save

5494
5495
5496
5497
5498
5499
5500
5501
5502
5503
5504

- Now create a **notification**.
 - Click on “**Manage notifications**” blue button in upper right-hand corner.
 - Click green button for “**Add new notification**”
 - Under “**Notify on Stream**” select notification created earlier from drop down menu.
 - Under “**Notification type**” select “**Email Alert Callback**” from drop down menu.
 - Click “**Add alert notification**” button
 - Title: “**Veeam Backup Alerts**”

○ Email Subject: “Successfull Veeam Backup source: \${foreach backlog message}\${message.source}\${end}” without the quotes, see below for screen shot of current callback wording.

○ Sender: < sender address >

○ E-mail Body: “This can be adjusted as required”

Alert Description: \${check_result.resultDescription}

Date: \${check_result.triggeredAt}

Stream ID: \${stream.id}

Stream title: \${stream.title}

Stream description: \${stream.description}

Alert Condition Title: \${alertCondition.title}

\${if backlog}Last messages accounting for this alert:
\${foreach backlog message}\${message}

\${end}\${else}<No backlog>

\${end}

○ User Receivers: “Select a Graylog user if desired”

○ Email Receivers: “Enter email address for individuals receiving these alerts”

○ Click **Save**

- Test new Streams / Alerts / Notifications to ensure they are configured correctly.

4.16.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the use of the Graylog due to its typical installation and usage location (i.e., external to the manufacturing system).

4.16.7 Link to Entire Performance Measurement Data Set

N/A

5537 4.17 DBAN**5538 4.17.1 Technical Solution Overview**

5539 DBAN is a free open source data wiping utility allowing the ability to sanitize hard drives to
5540 ensure data is not left behind when drives are beginning decommissioned and prepared for
5541 removal from on-premise. DBAN and other hard drive sanitization tools only work with spinning
5542 hard drives, SSD hard drives and other flash media refer to vendors for specific directions for
5543 sanitizing media before removing from company control.

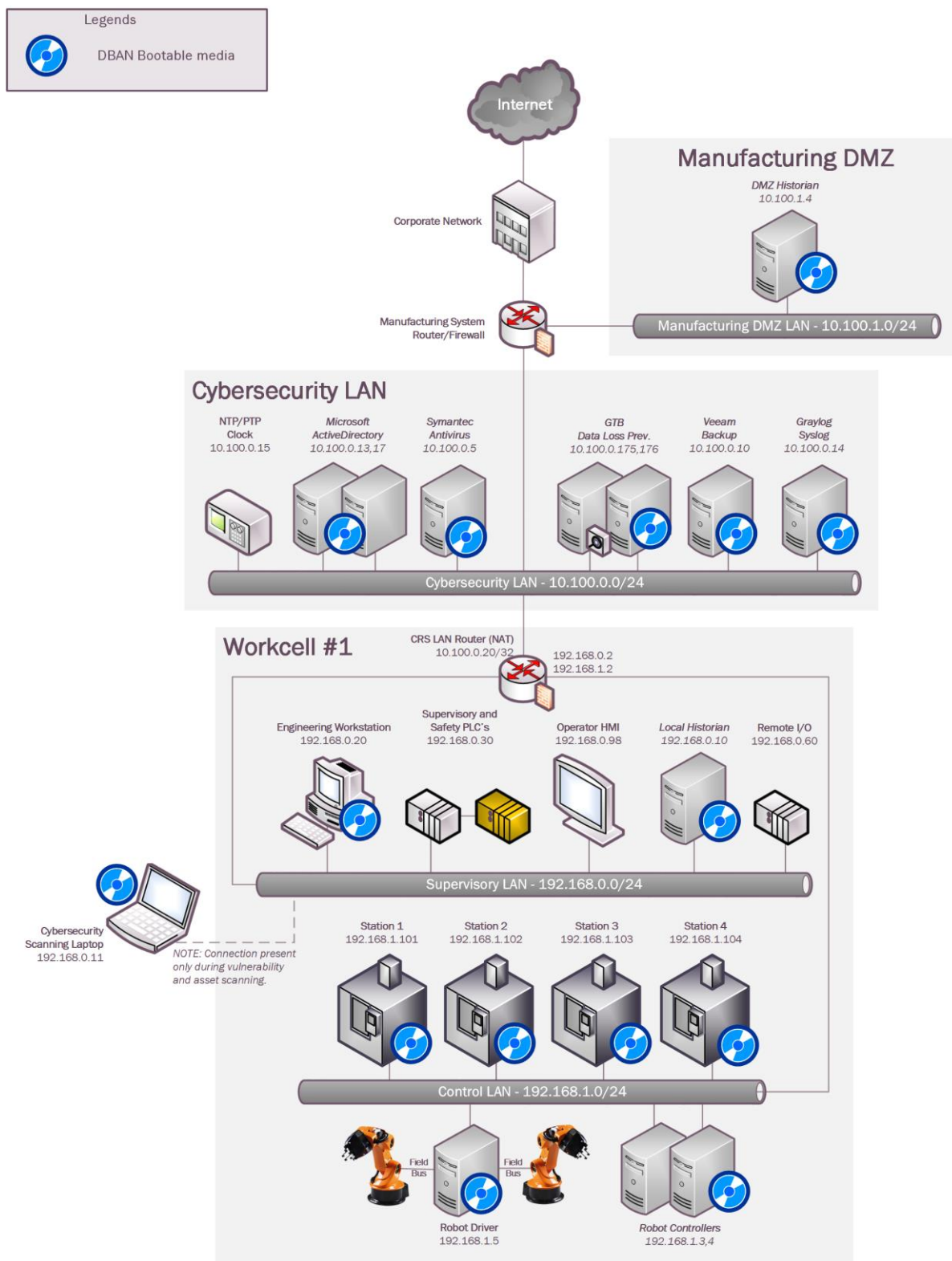
5544 4.17.2 Technical Capabilities Provided by Solution

5545 DBAN provides components of the following Technical Capabilities described in Section 6 of
5546 Volume 1:

- 5547 • Media Sanitization

5548 4.17.3 Subcategories Addressed by Implementing Solution

5549 PR.DS-3, PR.IP-6

5550 **4.17.4 Architecture Map of Where Solution was Implemented**

5551

4.17.5 Installation Instructions and Configurations

Instructions for installing DBAN and use

Download:

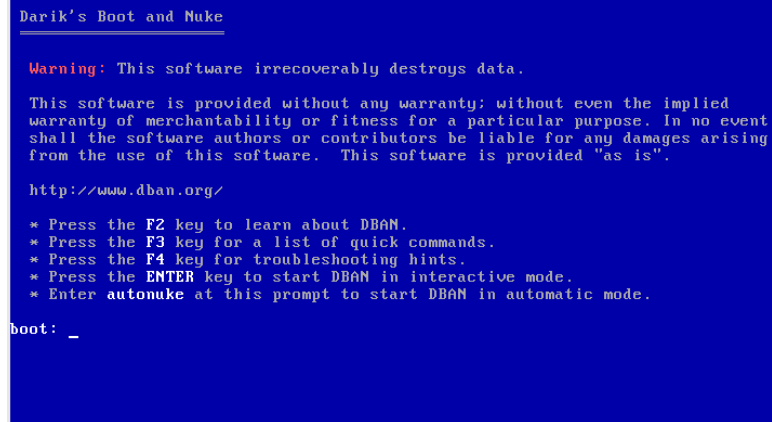
DBAN can be downloaded from <https://dban.org>

Click download link which redirects the page and a pop will appear to start download process for ISO image file “**dban-2.3.0_i586.iso**”.

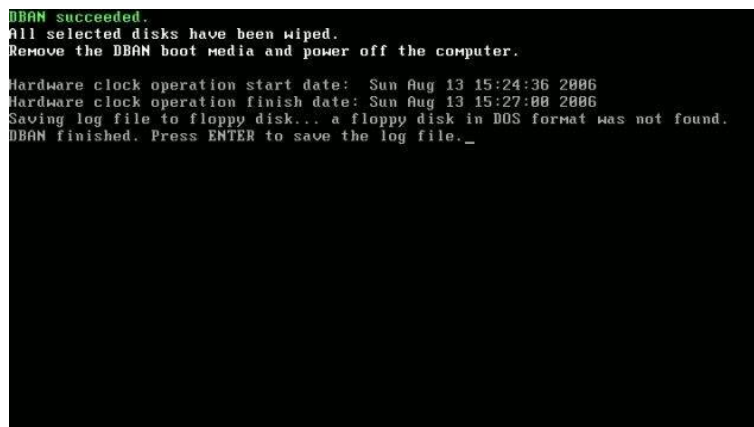
Download ISO file and burn to CD/DVD, or USB drive using widely available ISO bootable utilities.

Instructions:

1. Once ISO has been burned to bootable media go to device requiring sanitization.
2. Power on machine and boot from USB or CD/DVD depending on the install option from earlier steps above. (**Change Boot order in BIOS if no option for Boot Menu is available during machine power-up**)
3. Once machine has booted from media select desire option for media sanitization.



4. Select option to continue. Default sanitization mode is “**short DoD 5520.22-M**”, but this can be changed depending on the level your security program indicates.
5. Follow menu options to start wiping process.
6. Once the wipe has completed, you will see a screen like the image below.



5573 7. Once sanitization has completed, remove hard drive from device and label wiped
5574 ready for disposal.

5575 **Lesson Learned and things to know:**

5576 Not all hard drives are able to be wiped clean using this sanitization method. Media that is either
5577 SSD or flash memory is written differently than spinning drives, so follow SSD/Flash media
5578 vendors' recommendations for proper media sanitization for all non-spinning hard drives.

5579 **4.17.6 Highlighted Performance Impacts**

5580 No performance measurement experiments were performed for the use of DBAN due to its
5581 typical installation and usage location (i.e., external to the manufacturing system).

5582 **4.17.7 Link to Entire Performance Measurement Data Set**

5583 N/A

5584

5585 **4.18 Network Segmentation and Segregation**

5586 **4.18.1 Technical Solution Overview**

5587 Network segmentation and segregation solutions enable a manufacturer to separate the
5588 manufacturing system network from other networks (e.g., corporate networks, guest networks),
5589 segment the internal manufacturing system network into smaller networks, and control the
5590 communication between specific hosts and services.

5591 Each Router's native capabilities were leveraged to implemented network segmentation.

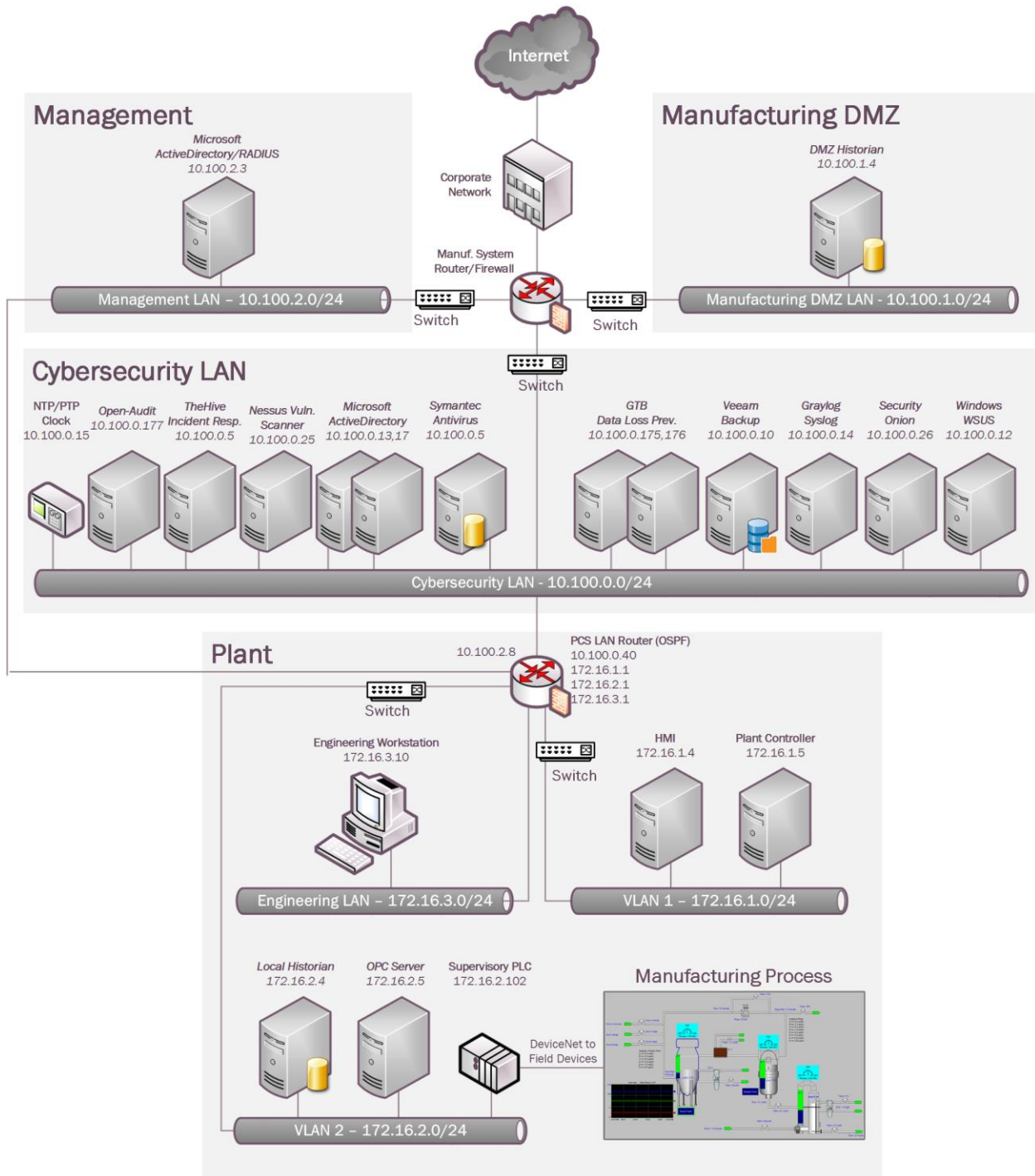
5592 **4.18.2 Technical Capabilities Provided by Solution**

5593 Network Segmentation and Segregation provides components of the following Technical
5594 Capabilities described in Section 6 of Volume 1:

- 5595
 - Network Segmentation and Segregation

5596 **4.18.3 Subcategories Addressed by Implementing Solution**

5597 PR.AC-5

5598 **4.18.4 Architecture Map of Where Solution was Implemented**

5599

5600

5601

4.18.5 Installation Instructions and Configurations

The following devices were involved in implementing Network Segmentation

Device	Details	Location
Cisco-ASA 5512	NGFW, running Firepower Services FTD 6.2.3	Manufacturing System
Allen Bradley Stratix 8300	Firewall, Router	Work cell

- Segmentation in the Cybersecurity LAN:**

Following is a list of interfaces created on the Boundary Router/Firewall – Cisco ASA of the Cybersecurity LAN network

Interface	IP address of Interface	Subnet	Description
GE 0/0	129.6.66.x	129.x.x.x/x	Uplink to Corporate
GE 0/1	10.100.0.1	10.100.1.0/24	Cybersecurity LAN
GE 0/2	129.6.1.x	129.x.x.x/x	VPN users
GE 0/3	10.100.2.1	10.100.2.0/24	Management LAN
GE 0/4	10.100.1.1	10.100.0.0/24	Manufacturing DMZ LAN

- Segmentation in the Plant:**

- The Work Cell consists of the following network devices.

Type	Description
Allen Bradley Stratix 8300	Boundary protection Firewall, Router
Allen Bradley Stratix 5700	Layer-2 Switch for the Control Network
Allen Bradley Stratix 5700	Layer-2 Switch for the Supervisory Network

- Following is a list of interfaces created on the Boundary Router – Allen Bradley 8300

Interface	IP address of Interface	Subnet	Description
Fa 1/1	172.16.1.1	172.16.1.0/24	Supervisory Vlan1
Fa 1/2	172.16.2.1	172.16.2.0/24	Control Vlan1
Fa 1/3	172.16.3.1	172.16.3.0/24	Engineering LAN
Fa 1/4	10.100.0.40		Uplink to Cybersecurity LAN
Gi 1/1	10.100.2.8		Management interface

AB

Allen-Bradley

Stratix 8300

Device Manager - Switch

Dashboard

Network | Port Settings

Physical Port Table

Edit

	Port Name	Description	Port Status	Speed	Duplex
<input type="radio"/>	Fa1/1	Supervisory VLAN1 Switch	<div></div>	Auto-100Mb/s	Auto-Full
<input type="radio"/>	Fa1/2	Control VLAN2 Switch	<div></div>	Auto-100Mb/s	Auto-Full
<input type="radio"/>	Fa1/3	Engg LAN Workstation	<div></div>	Auto-100Mb/s	Auto-Full
<input type="radio"/>	Fa1/4	Uplink to Cybersecurity LAN	<div></div>	Auto-100Mb/s	Auto-Full
<input type="radio"/>	Gi1/1	Mgmt	<div></div>	Auto-1000Mb/s	Auto-Full
<input type="radio"/>	Gi1/2		<div></div>	Auto	Auto

- One of the Stratix 5700 switches was connected to the Fa1/1 interface of the 8300 Router and used for the Supervisory (Vlan1) sub-network. Devices connected to this switch were assigned an IP address from the 172.16.1.0/24 subnet
- The other Stratix 5700 switch was connected to the Fa 1/2 interface of the Router and used for the Plant (Vlan2) sub- network. Devices connected to this switch were assigned an IP address from the 172.16.2.0/24 subnet.

4.18.6 Highlighted Performance Impacts

No performance measurement experiments were performed for network segmentation and segregation due to it being implemented on the PCS before the Manufacturing Profile implementation was initiated.

4.18.7 Link to Entire Performance Measurement Data Set

N/A

5634 **4.19 Network Boundary Protection**

5635 **4.19.1 Technical Solution Overview**

5636 Boundary Protection devices are implemented to monitor and control connections and
5637 communications at the external boundary and key internal boundaries within the organization.
5638 Boundary protection mechanisms include for example, Routers, Firewalls, Gateways, Data
5639 diodes separating system components into logically separate networks and sub networks.

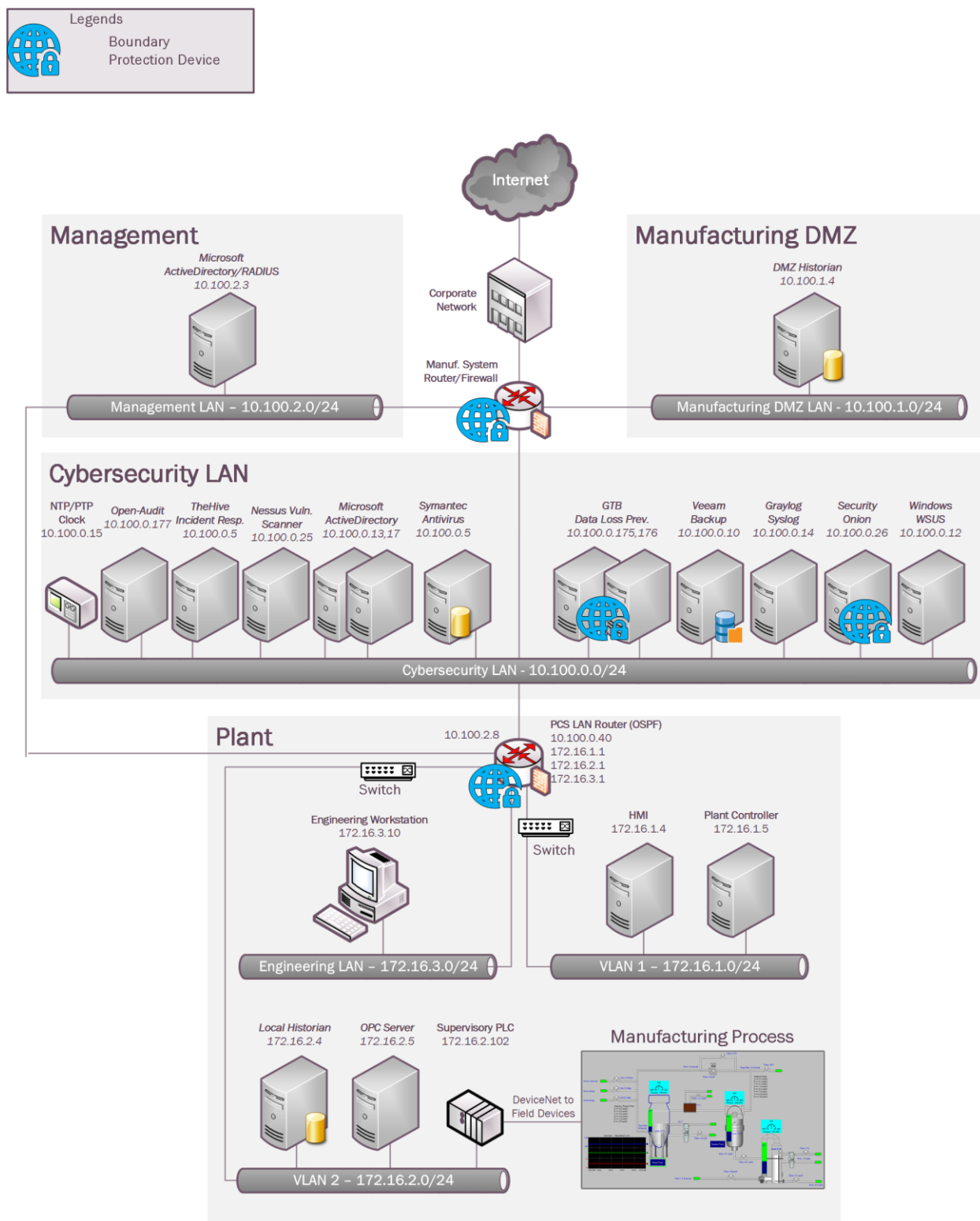
5640 **4.19.2 Technical Capabilities Provided by Solution**

5641 Network Boundary Protection provides components of the following Technical Capabilities
5642 described in Section 6 of Volume 1:

- 5643
 - Network Boundary Protection

5644 **4.19.3 Subcategories Addressed by Implementing Solution**

5645 PR.AC-5, PR.PT-4, DE.CM-1

5646 **4.19.4 Architecture Map of Where Solution was Implemented**

5647

5648 **4.19.5 Installation Instructions and Configurations**5649 **Setup:**

5650 The following devices were implemented for Boundary protection in the PCS System

Device	Details	Location
Cisco-ASA 5512	NGFW, running Firepower Services FTD 6.2.3	Manufacturing System
Allen Bradley Stratix 8300	Firewall, Router	Work cell
GTB Inspector	Data Loss Prevention (DLP) virtual appliance	Cybersecurity LAN
Security Onion	Running Snort, BRO IDS	Cybersecurity LAN

5651

5652 • **Configuration on Cisco-ASA:**

5653 The following features, settings were enabled on the ASA firewall

- 5654 • Network Segmentation
- 5655 • ACL Rules
- 5656 • NAT policy for Internet access
- 5657 • Snort Inspection
- 5658 • DMZ network

5659 **Network Segmentation**

5660 Separate network interfaces were configured for the different network segments as listed below

- 5661 • Inside Interface (Network: 10.100.0.0/24)
- 5662 • DMZ Interface (Network: 10.100.1.0/24)
- 5663 • Outside Interface (Network: 129.6.91.x/24, Uplink to NIST Corporate for Internet)
- 5664 • Public interface (Network: 129.6.1.x/24 For VPN Users)

5665 **Access Control List (ACL) rules**5666 The following rules were put in place on the ASA with a default Action to **Block all traffic**.

5667

5668

Source	Source Port	Destination	Dest Ports	Protocol	Action
10.100.0.0/24, 172.16.0.0/22	Any	DMZ network	SSH,RDP,ICMP	TCP	Trust
PCS-Historian (172.16.2.14)	TCP_High_Ports	DMZ-Historian	5450	TCP	Trust
DMZ Historian	TCP_High_Ports	PCS-Historian	5450	TCP	Trust
CRS-NAT (10.100.0.20)	TCP_High_Ports	DMZ-Historian	5450, 5460, 5671, 5672	TCP	Trust
DMZ Historian	TCP_High_Ports	CRS-NAT (10.100.0.20)	5457, 5450	TCP	Trust
DMZ Historian	Any	Active Directory (10.100.0.17)	53	UDP	Allow
Veeam Server	Any	Hyper-V Host servers, Esxi Host Server	NETBIOS, ICMP, HTTPS, 445, TCP_High_ports, 2500-5000, 6160- 6163	TCP	Trust
Hyper-V Host Servers, Esxi Host Server	Any	Veeam Server	ICMP, 2500-5000	TCP	Trust
inside_interface	Any	outside_interface	Any	Any	Allow
DMZ Historian	Any	Symantec Server	SMB (445), HTTPS	TCP	Trust
Symantec Server	Any	DMZ Historian	HTTP, HTTPS, 8014	TCP	Trust
DMZ Historian	Any	Graylog Server	514	UDP	Trust
VPN_Pool (192.168.100.10 - .20)	Any	PCS-HMI-Server, PCS-Workstation	3389	TCP	Allow

5669

5670

5671

The screenshot displays the Cisco ASA configuration interface for the 'Mandatory - AC-Policy (1-13)'. The rules are as follows:

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	ISE/S...	Action
1	Allow-SSH-RDP-DMZ	Any	Any	Testbed-LAN-Network PCS-Network	DMZ-Network	Any	Any	Any	Any	ICMP (1) SSH RDP-Windows	Any	Any	Trust
2	PI-To-PI	Any	Any	PCS-Historian	PI-Server-DMZ	Any	Any	Any	TCP_high_ports	PI-to-PI	Any	Any	Trust
3	PI-to-PI-PCS	Any	Any	PI-Server-DMZ	PCS-Historian	Any	Any	Any	TCP_high_ports	PI-to-PI	Any	Any	Trust
4	CRS-PI-PI	Any	Any	CRS-NAT-IP	PI-Server-DMZ	Any	Any	Any	TCP_high_ports	TCP (8):5671 TCP (8):5672 PI-Connector PI-DCM	Any	Any	Trust
5	CRS-PI-To-PI-2	Any	Any	PI-Server-DMZ	CRS-NAT-IP	Any	Any	Any	TCP_high_ports	TCP (8):5457 PI-to-PI	Any	Any	Trust
6	Allow-DNS-DMZ	Any	Any	DMZ-Network	LAN-AD01-DNS-Serv	Any	Any	Any	Any	DNS_over_UDP	Any	Any	Allow
7	Veeam-Mgmt-Hosts	Any	Any	Veeam	Hyper-V-Servers Exsi-Host.mgmt	Any	Any	Any	Any	ICMP (1) TCP_high_ports Veeam-channel-ports Veeam-SQL-TCP (4 more...)	Any	Any	Trust
8	HyperV-Hosts-Veeam	Any	Any	Exsi-Host.mgmt Hyper-V-Servers	Veeam	Any	Any	Any	Any	ICMP (1) Veeam-channel-ports	Any	Any	Trust
9	Internet-Access	inside	outside	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow
10	Symantec-DMZ-1	Any	Any	SymantecMgr	PI-Server-DMZ	Any	Any	Any	Any	TCP (8):445 SMB-Windows HTTPS	Any	Any	Allow
11	Symantec-DMZ-2	Any	Any	PI-Server-DMZ	SymantecMgr	Any	Any	Any	Any	HTTPS HTTP Symantec	Any	Any	Allow
12	DMZ-Syslog	Any	Any	PI-Server-DMZ	Graylog	Any	Any	Any	Any	SYSLOG	Any	Any	Allow

Displaying 1 - 13 of 13 rules

5672

5673 NAT Policy

- 5674
- A Dynamic NAT policy was configured to allow internet access.

Type of NAT rule	Auto NAT [1]
Source Interface	inside
Destination Interface	outside
Original sources	10.100.0.0/8
Translated Source	Destination Interface IP
Options	Translate DNS Replies that match this Rule: False

5675

5676

5677 **Snort Inspection**

- 5678 • Snort Inspection was enabled on the following ACL rules

Name of the ACL	Intrusion Policy
Allow-DNS-DMZ	Balanced connectivity and security
Internet-Access rule	Balanced connectivity and security
VPN-Rule	Balanced connectivity and security

5679

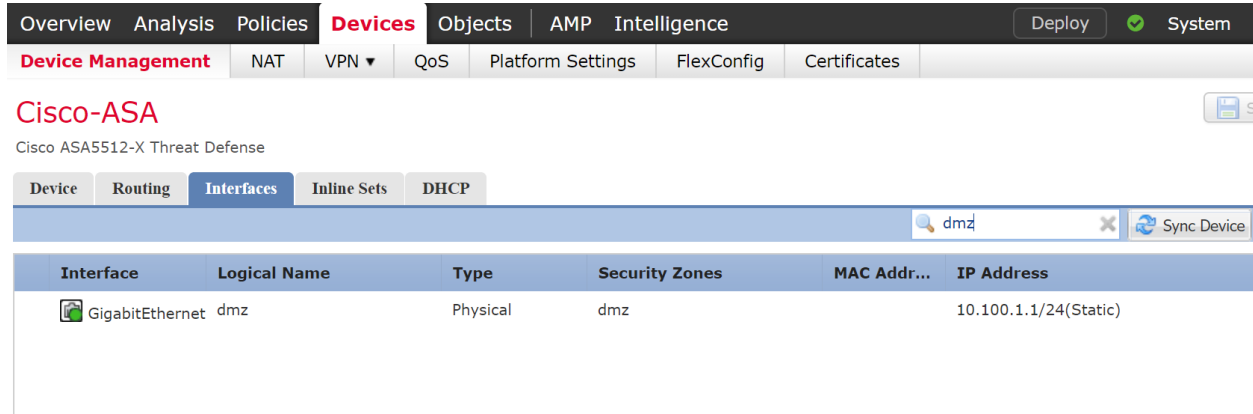
5680

5681

5682

5683 **DMZ Network**

5684 A Separate interface was setup for the Manufacturing DMZ LAN Network for hosting the **DMZ**
5685 **Historian** server.



5686

5687 • **Configuration of Allen Bradley Firewall:**

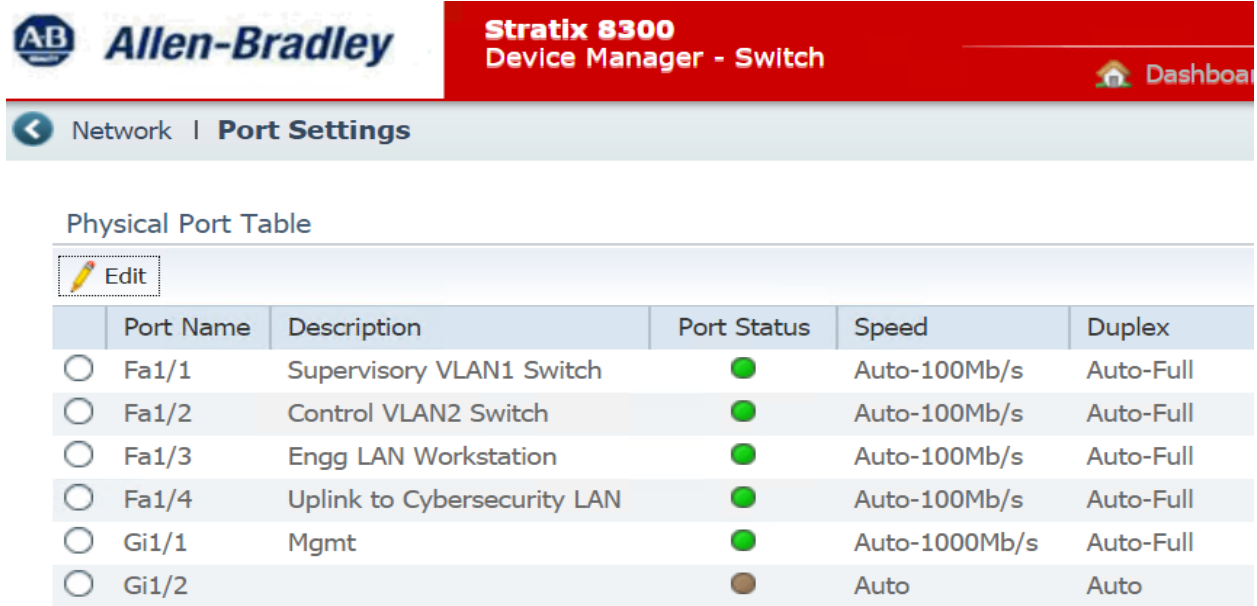
5688 The following features, settings were enabled on this firewall

- 5689 • Network Segmentation
5690 • ACL Rules

5691 **Network Segmentation**

5692 Separate network interfaces were configured for the different network segments as listed below

- 5693 • Supervisory VLAN1 (Network: 172.16.1.0/24)
5694 • Control VLAN2 Interface (Network: 172.16.2.0.0/24)
5695 • Engineering LAN (Network: 172.16.3.0/24)
5696 • Uplink (IP:10.100.0.40, Uplink to Cybersecurity LAN)
5697 • Management interface (IP:10.100.2.8)



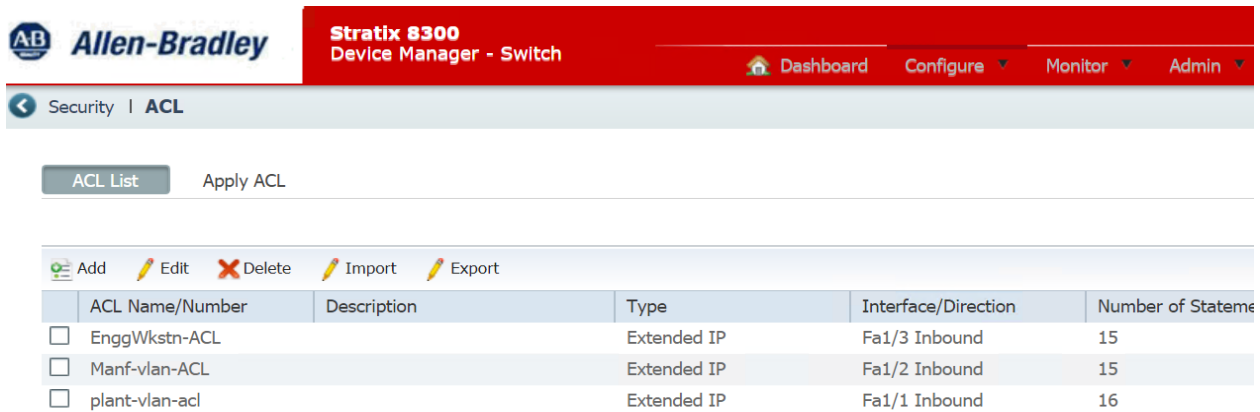
The screenshot shows the 'Stratix 8300 Device Manager - Switch' interface. The top navigation bar includes the Allen-Bradley logo and a 'Dashboard' link. Below the navigation bar, the 'Network | Port Settings' section is active. The 'Physical Port Table' is displayed, featuring an 'Edit' button and a table with the following data:

	Port Name	Description	Port Status	Speed	Duplex
<input type="radio"/>	Fa1/1	Supervisory VLAN1 Switch	●	Auto-100Mb/s	Auto-Full
<input type="radio"/>	Fa1/2	Control VLAN2 Switch	●	Auto-100Mb/s	Auto-Full
<input type="radio"/>	Fa1/3	Engg LAN Workstation	●	Auto-100Mb/s	Auto-Full
<input type="radio"/>	Fa1/4	Uplink to Cybersecurity LAN	●	Auto-100Mb/s	Auto-Full
<input type="radio"/>	Gi1/1	Mgmt	●	Auto-1000Mb/s	Auto-Full
<input type="radio"/>	Gi1/2		●	Auto	Auto

5698

5699 **Access Control List (ACL) rules**

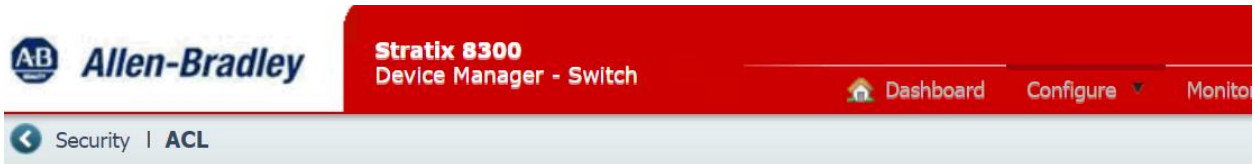
5700 Three ACLs of Extended type were created as shown below. Each one was associated to a
 5701 specific network interface as an Inbound ACL



The screenshot shows the 'Stratix 8300 Device Manager - Switch' interface. The top navigation bar includes the Allen-Bradley logo and links for 'Dashboard', 'Configure', 'Monitor', and 'Admin'. Below the navigation bar, the 'Security | ACL' section is active. The 'ACL List' is displayed, featuring an 'Apply ACL' button and a table with the following data:

	ACL Name/Number	Description	Type	Interface/Direction	Number of Stateme
<input type="checkbox"/>	EnggWkstn-ACL		Extended IP	Fa1/3 Inbound	15
<input type="checkbox"/>	Manf-vlan-ACL		Extended IP	Fa1/2 Inbound	15
<input type="checkbox"/>	plant-vlan-acl		Extended IP	Fa1/1 Inbound	16

5702



The image shows the top navigation bar of the Allen-Bradley Stratix 8300 Device Manager. It includes the Allen-Bradley logo, the title 'Stratix 8300 Device Manager - Switch', and navigation links for 'Dashboard', 'Configure', and 'Monitor'. Below this is a breadcrumb trail: 'Security | ACL'.

ACL List

Port Name	Inbound ACL	Outbound ACL	
Fa1/1	plant-vlan-acl	None	
Fa1/2	Manf-vlan-ACL	None	
Fa1/3	EnggWkstn-ACL	None	
Fa1/4	None	None	

ip access-list extended EnggWkstn-ACL

```

permit ip host 172.16.3.10 10.100.0.0 0.0.0.255
permit tcp host 172.16.3.10 172.16.1.0 0.0.0.15 eq 3389
permit tcp host 172.16.3.10 172.16.2.0 0.0.0.15 eq 3389
permit icmp host 172.16.3.10 any
permit tcp host 172.16.3.10 host 172.16.2.102 eq 44818
permit ip host 172.16.3.10 host 172.16.3.1
permit ip host 172.16.3.10 host 172.16.2.2
permit ip host 172.16.3.10 host 172.16.1.3
permit tcp host 172.16.3.10 host 10.100.1.4 eq 3389
permit tcp host 172.16.3.10 host 129.6.1.2 eq ftp
permit tcp host 172.16.3.10 host 129.6.1.2 eq 22
permit tcp host 172.16.3.10 host 129.6.1.2 eq www
permit tcp host 172.16.3.10 host 172.16.2.102
permit tcp 192.168.100.0 0.0.0.255 host 172.16.3.10 eq 3389
permit tcp host 172.16.3.10 host 192.168.100.10 gt 49000

```

ip access-list extended Manf-vlan-ACL

```

permit ip 172.16.2.0 0.0.0.15 172.16.1.0 0.0.0.15 log
permit icmp 172.16.2.0 0.0.0.255 any log
permit tcp 172.16.2.0 0.0.0.255 host 172.16.3.10 gt 49000 log
permit ip 172.16.2.0 0.0.0.255 host 10.100.0.5 log
permit ip 172.16.2.0 0.0.0.255 host 10.100.0.10 log
permit ip 172.16.2.0 0.0.0.255 host 10.100.0.13 log
permit ip 172.16.2.0 0.0.0.255 host 10.100.0.17 log
permit ip 172.16.2.0 0.0.0.255 host 10.100.0.25 log
permit ip 172.16.2.0 0.0.0.255 host 10.100.0.177 log
permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.234 log
permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq www log
permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq 443 log
permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq 8530 log
permit udp 172.16.2.0 0.0.0.255 host 10.100.0.14 eq syslog log
permit tcp host 172.16.2.14 host 10.100.1.4 gt 49000 log

```

5706

ip access-list extended plant-vlan-acl

```

permit ip 172.16.1.0 0.0.0.15 172.16.2.0 0.0.0.15 log
permit icmp 172.16.1.0 0.0.0.255 any log
permit tcp 172.16.1.0 0.0.0.255 host 172.16.3.10 gt 49000 log
permit ip 172.16.1.0 0.0.0.255 host 10.100.0.5 log
permit ip 172.16.1.0 0.0.0.255 host 10.100.0.10 log
permit ip 172.16.1.0 0.0.0.255 host 10.100.0.13 log
permit ip 172.16.1.0 0.0.0.255 host 10.100.0.17 log
permit ip 172.16.1.0 0.0.0.255 host 10.100.0.25 log
permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.234 log
permit udp 172.16.1.0 0.0.0.255 host 10.100.0.14 eq syslog log
permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq www log
permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq 443 log
permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq 8530 log
permit ip 172.16.1.0 0.0.0.255 host 10.100.0.177 log
permit tcp 192.168.100.0 0.0.0.255 host 172.16.1.4 eq 3389 log
permit tcp host 172.16.1.4 192.168.100.0 0.0.0.255 gt 49000 log

```

5707

5708 • **Configuration of GTB Inspector:**

5709 Refer to Section 4.15 for details.

5710 • **Configuration of Security Onion:**

5711 Refer to Section 4.7 for details

5712 4.19.6 Highlighted Performance Impacts

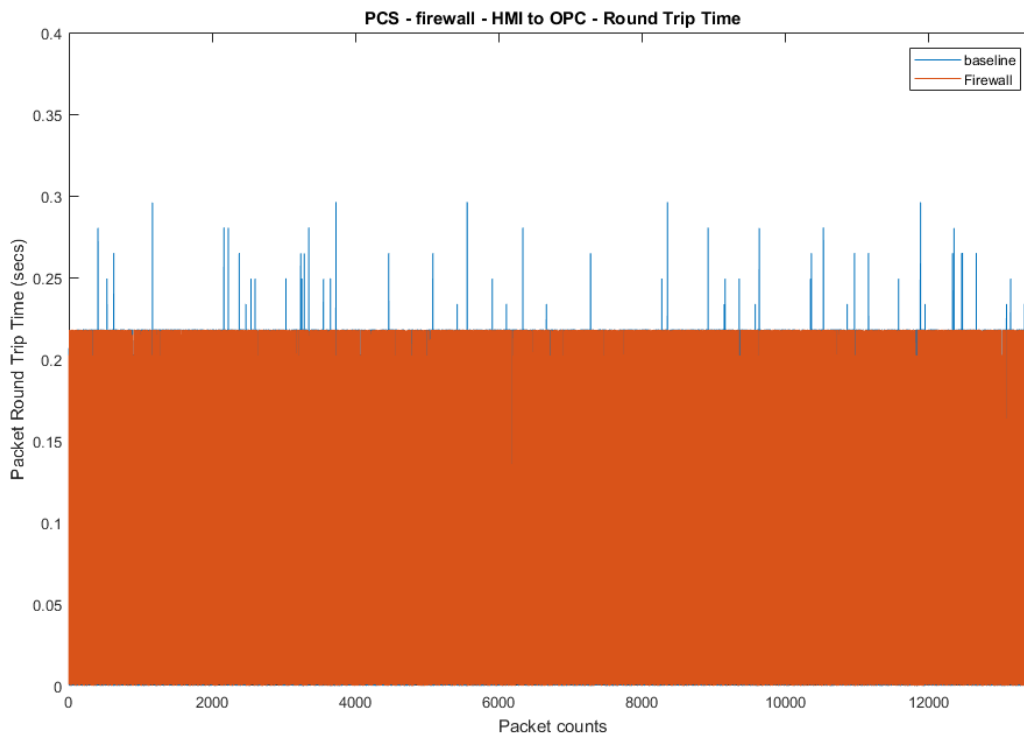
5713 The following performance measurement experiment was performed for the network boundary
5714 protection while the manufacturing system was operational:

5715 Experiment PL004.1- Firewall rules are activated at the PCS boundary router

5716 There was no significant performance impact observed when firewall rules were activated. For
5717 example, the packet round trip time between the HMI and OPC remained mostly constant before
5718 and after the firewall rules were activated.

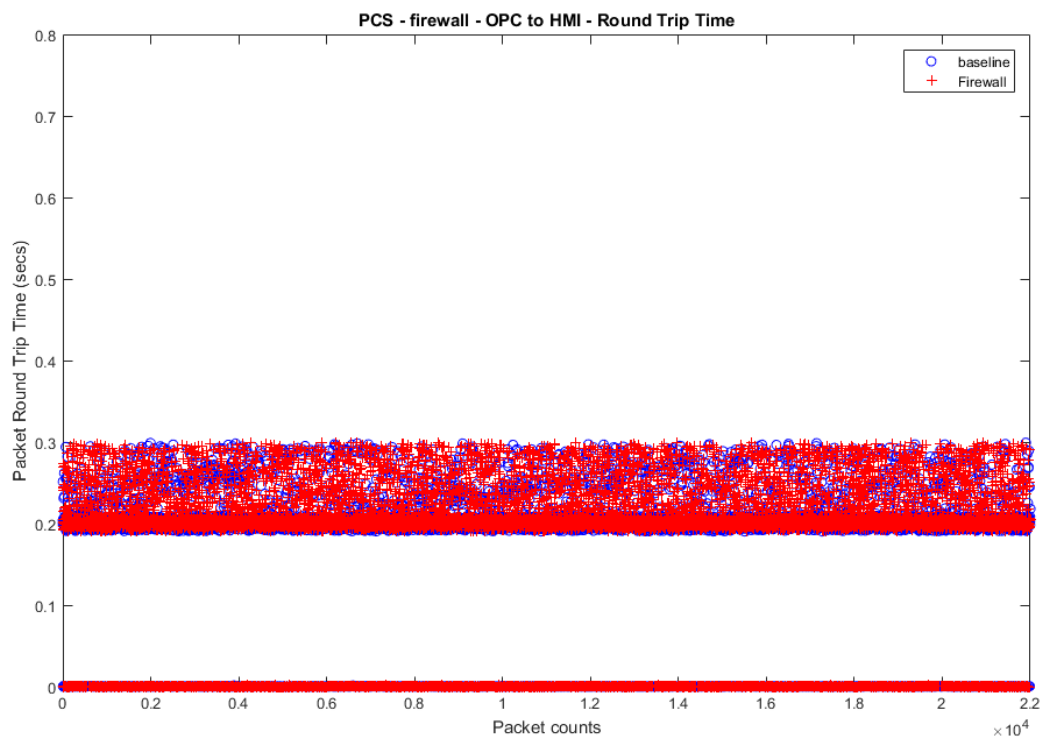
5719 Care needs to be used for implementation of the rules and a thorough understanding of the
5720 system is important. A misconfigured firewall rule can block a legitimate connection and cause
5721 system failure.

5722 In the PCS system implementation, a thorough analysis on network connections was performed
5723 to identify all the legitimate connections in order to implement the firewall rules. Some network
5724 connections are legitimate but not obvious or only stayed connected for a short amount of time.
5725 Validation test was performed to ensure all the legitimate network connections for normal
5726 operation are allowed. The implementation and validation test was completed during a planned
5727 system down time.



5728

5729 **Figure 4-35 Packet round trip time from HMI to OPC before and after firewall rules were activated**

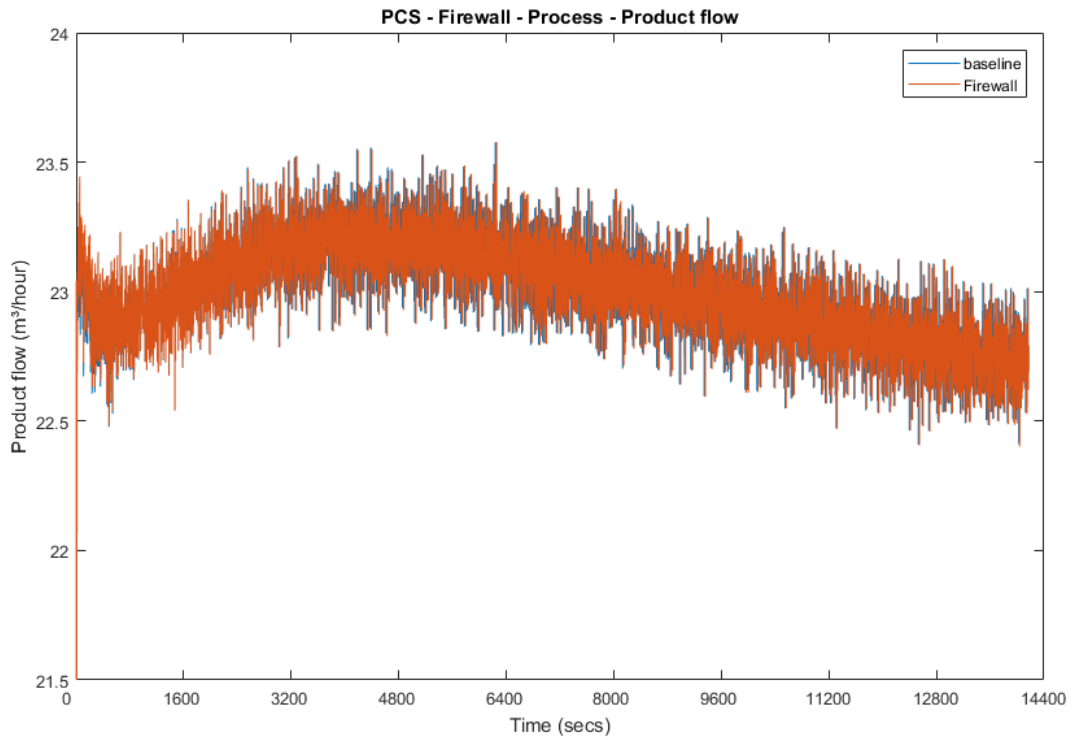


5730

5731

Figure 4-36 Packet round trip time from OPC to HMI before and after firewall rules were activated

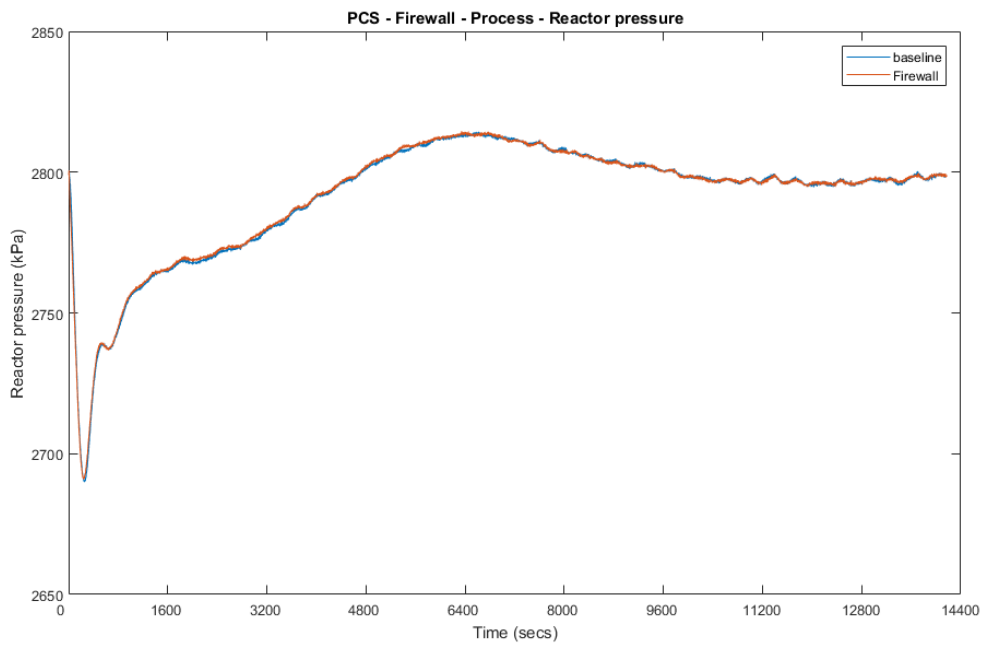
5732



5733

5734

Figure 4-37 Manufacturing process product flow rate before and after firewall rules were activated



5735

5736

Figure 4-38 Manufacturing process reactor pressure before and after firewall rules were activated

5737

5738 **4.19.7 Link to Entire Performance Measurement Data Set**

5739 [Firewall KPI data](#)

5740 [Firewall measurement data](#)

5741

5742

5743 **4.20 Managed Network Interfaces**

5744 **4.20.1 Technical Solution Overview**

5745 Managing network interfaces controls what network devices are plugged into switches within
5746 manufacturing system, along with physical labeling connections to help with system
5747 identification and classification. Required actions will be performed directly on the exterior of
5748 the switch. Switch port in use will be labeled logically within switch console itself, along with
5749 the corresponding network cable for easy identification. All cable should be labeled/identified at
5750 the switch and at the opposite end of the network cable. Switch Port Security should be
5751 configured to restrict access to only allowed preconfigured Media Access Control (MAC)
5752 addresses devices.

5753 Minimal cost for labeling. Effort of implement is high, but not difficult. The effort will be spent
5754 taking the required time to accurately identify cabling connections.

5755 Most switches have built in Port security. Since this technical control is built into switches there
5756 is no additional cost for implementation. Configuration for Port security is well documented and
5757 easily configured

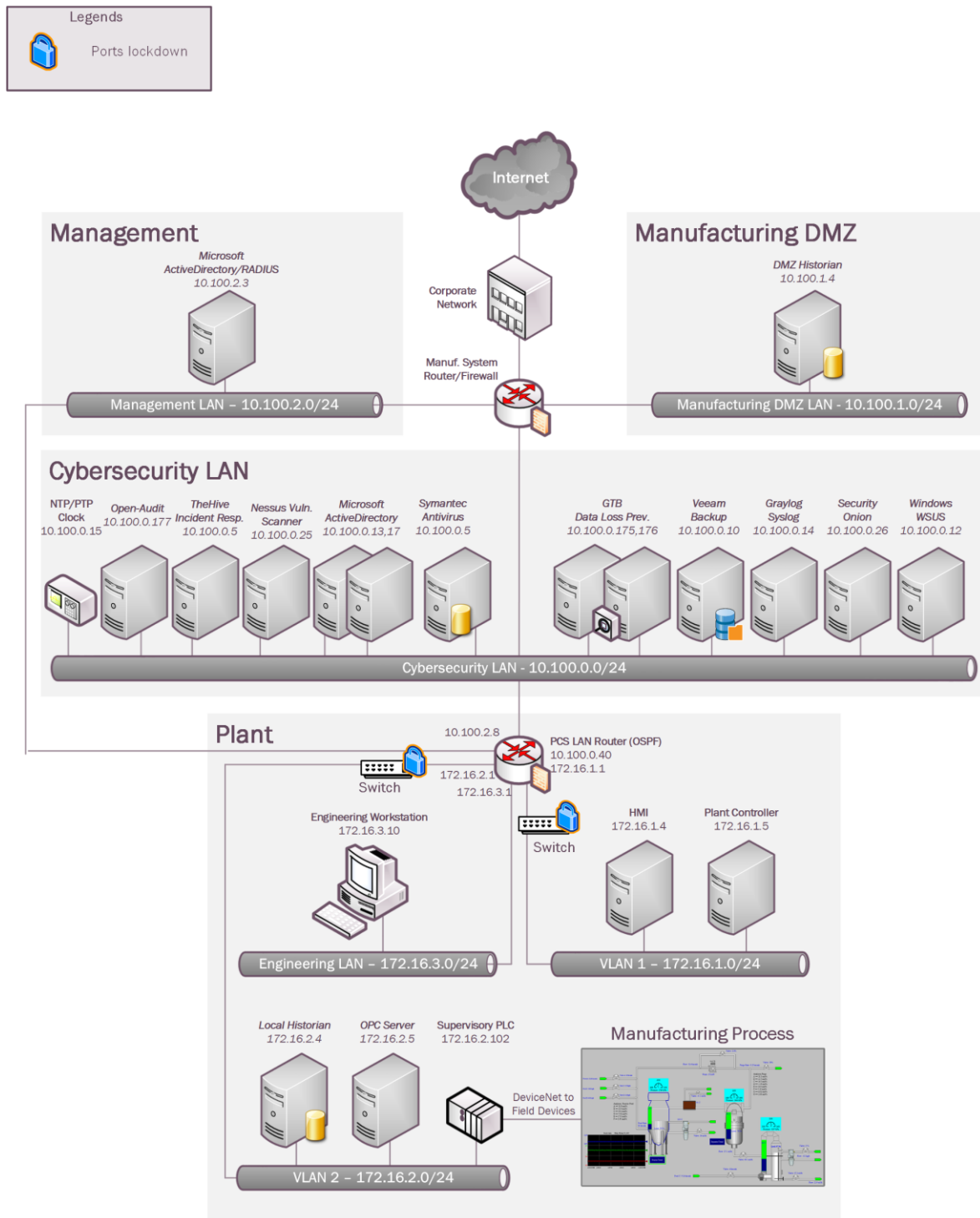
5758 **4.20.2 Technical Capabilities Provided by Solution**

5759 Managed Network Interfaces provides components of the following Technical Capabilities
5760 described in Section 6 of Volume 1:

- 5761 • Managed Network Interfaces

5762 **4.20.3 Subcategories Addressed by Implementing Solution**

5763 PR.AC-5

5764 **4.20.4 Architecture Map of Where Solution was Implemented**

5765

5766

5767 **4.20.5 Installation Instructions and Configurations**5768 **Managing Network Interface Instructions**5769 **Overview:**

5770 Port labeling provides ability for others to understand and know what network devices belong
 5771 where. Managing your switches with correct labeling and classification makes troubleshooting
 5772 simpler along with improving cybersecurity.

5773 **Labeling ports within switch:**5774 **Router/Switches within PCS: Allen-Bradley**5775 **Stratix 8300 (Router)** 172.16.3.15776 **Stratix 5700 (Switch)** Vlan1 172.16.1.3, Vlan2 172.16.2.2

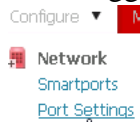
5777

5778

- Login to switch/router via web browser. <https://x.x.x.x>

5779

- Once logged in click on Configure→Port Settings



5780

5781

5782

- Select port that will be labeled and click edit.

5783

- A window will appear, now type into box next to Description and enter desired

5784

- label. Description | Engg Workstation

5784

- Click OK to save change and exit.

5785 **Same steps apply to Switches/Router within Process Control**

5786

5787 **Port Security Configuration for Process Control Enclave**5788 **Overview:**

5789 Port security prevents unauthorized devices from being plugged into a network switch while
 5790 trying to obtaining sensitive information, which could be used for mapping out network
 5791 connections for possible data exfiltration. When an unauthorized device is plugged into a
 5792 protected port a warning message is logged and sent to a syslog server if supported by switch
 5793 vendor.

5794

5795

5796 **Process Control Enclave:**

- 5797
- Enclave contains two different switches/routers.

5798

- Allen Bradley Router (8300)

5799

- Allen Bradley Switch (5700)

5800 **Allen Bradley Router 8300:** Has multiple ports which are individual configurable depending on
5801 desired network topology.

- 5802
- Ports Fa1/1, Fa1/2, Fa1/3(**Port Security Enabled**), Fa1/4, Gi1/1 = Enabled

- 5803
- Port Gi1/2 = Disabled

Physical Port Table Selected 0 | Total 6

Edit

	Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode
<input type="radio"/>	Fa1/1	Plant subn...		Auto-100Mb/s	Auto-Full	10/100BaseTX		routed	
<input type="radio"/>	Fa1/2	Manf- Vlan...		Auto-100Mb/s	Auto-Full	10/100BaseTX		routed	
<input type="radio"/>	Fa1/3	Engg Work...		Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	1	Access
<input type="radio"/>	Fa1/4	Uplink to L...		Auto-100Mb/s	Auto-Full	10/100BaseTX		routed	
<input type="radio"/>	Gi1/1	Mgmt		Auto-1000Mb/s	Auto-Full	AUTO-SELECT 10/10...	Static access	3	Access
<input type="radio"/>	Gi1/2			Auto	Auto	AUTO-SELECT Not Pr...	Down		Trunk

- 5804
- Enabling port security for connection are only allowed when configuring a switching
-
- 5805
- If a port has been configured for routing port security cannot be enabled.
-
- 5806

5807 **Allen Bradley 5700 (172.16.1.3):** Layer 2 switch (Vlan1)

- 5808
- Ports Fa1/1, Fa1/2, Fa1/5, Fa1/6, Gi1/1 are all configured for switching.

- 5809
- Ports Fa1/3, Fa1/4, Fa1/7, Fa1/8, Gi1/2 are currently disabled.

Physical Port Table Selected 0 | Total 10

Edit

	Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode
<input type="radio"/>	Fa1/1			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	101	Access
<input type="radio"/>	Fa1/2			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	101	Access
<input type="radio"/>	Fa1/3			Auto	Auto	10/100BaseTX	Down	101	Dynamic auto
<input type="radio"/>	Fa1/4			Auto	Auto	10/100BaseTX	Down	101	Dynamic auto
<input type="radio"/>	Fa1/5			Auto-10Mb/s	Auto-Full	10/100BaseTX	Static access	104	Access
<input type="radio"/>	Fa1/6			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	104	Access
<input type="radio"/>	Fa1/7			Auto	Auto	10/100BaseTX	Down	101	Dynamic auto
<input type="radio"/>	Fa1/8			Auto	Auto	10/100BaseTX	Down	101	Dynamic auto
<input type="radio"/>	Gi1/1			Auto-100Mb/s	Auto-Full	AUTO-SELECT 10/10...	Static access	101	Access
<input type="radio"/>	Gi1/2			Auto	Auto	AUTO-SELECT Not Pr...	Down	1	Dynamic auto

5810

5811 **Allen Bradley 5700 (172.16.2.2):** Layer 2 switch (Vlan2)

- 5812
- Ports Fa1/1, Fa1/4, Fa1/5, Fa1/6, Fa1/7, Gi1/1 are all configured for switching.

- 5813
- Ports Fa1/2, Fa1/3, Fa1/8, Gi1/2 are currently disabled.

Physical Port Table Selected 0 | Total 10

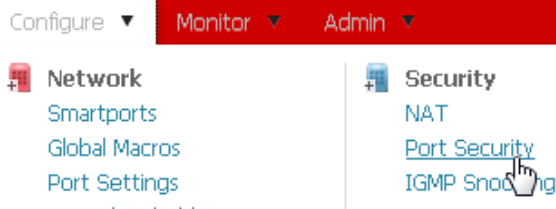
Edit

	Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode
<input type="radio"/>	Fa1/1			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	102	Access
<input type="radio"/>	Fa1/2			Auto	Auto	10/100BaseTX	Down	102	Access
<input type="radio"/>	Fa1/3			Auto	Auto	10/100BaseTX	Down	102	Dynamic auto
<input type="radio"/>	Fa1/4			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	102	Access
<input type="radio"/>	Fa1/5			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	102	Access
<input type="radio"/>	Fa1/6			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	102	Access
<input type="radio"/>	Fa1/7			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	102	Access
<input type="radio"/>	Fa1/8			Auto	Auto	10/100BaseTX	Down	102	Dynamic auto
<input type="radio"/>	Gi1/1			Auto-100Mb/s	Auto-Full	AUTO-SELECT 10/10...	Static access	102	Access
<input type="radio"/>	Gi1/2			Auto	Auto	AUTO-SELECT Not Pr...	Down	1	Dynamic auto

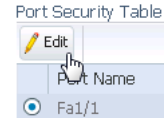
5814

5815 **Enable Port Security (Allen Bradley 5700 and 8300, switch ports only)**

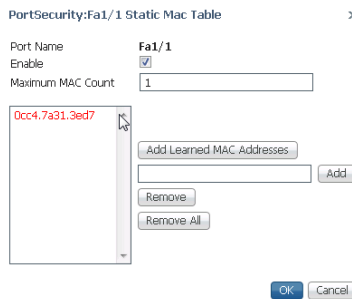
- 5816 • Login into Allen Bradley device via web browser.
- 5817 • Click, “**Configure→Security→Port Security**”



5818



- 5819 • Select desired port requiring security and click “**Edit**” button.
- 5820 • Place a check in box next to “**Enable**” and then click “**Add Learned MAC Addresses**”
- 5821 or add the Addresses manually.



5822

5823

5824

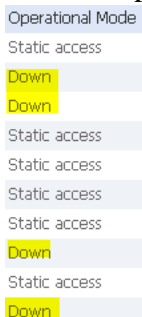
5825

5826

- Once MAC addresses have been added click “**OK**” to save changes.
- If more than one MAC addresses are required to be added change “**Maximum MAC Count**” to the required MACs being assigned to this port.

5827 **Disable unused ports**

- 5828 • While on the homepage select “**Configure→Port Settings**”
- 5829 • Find all Operational Mode labeled as down to identify ports being disabled.



5830

5831

5832

5833

- Now select one of the down ports and click on “**Edit**”
- Once “**Edit Physical Port**” window appears remove check for enable from Administrative and click OK.

Administrative ☐ Enable

- 5834 • Port now is disabled. Any device plugged into this port or other disabled ports will not
5835 work.

5836 **Lessons Learned**

- 5837 • A Router don't allow Port Security via MAC on a routed port. This is because a routed
5838 port uses IP Address and not MAC Addresses.
- 5839 • When enabling Port Security turn on one port at a time to limit changes within the
5840 environment.

5841 Snippet from Allen Bradley Vlan1 Switch Running-Config File

```
interface FastEthernet1/1
switchport access vlan 101
switchport mode access
switchport port-security mac-address 0cc4.7a31.3ed7
switchport port-security
!
interface FastEthernet1/2
switchport access vlan 101
switchport mode access
switchport port-security mac-address 0cc4.7a31.4447
switchport port-security
!
interface FastEthernet1/3
switchport access vlan 101
shutdown
!
interface FastEthernet1/4
switchport access vlan 101
shutdown
!
interface FastEthernet1/5
switchport access vlan 104
switchport mode access
switchport port-security mac-address 0cc4.7a32.b300
switchport port-security
!
interface FastEthernet1/6
switchport access vlan 104
switchport mode access
switchport port-security mac-address 001d.9cbf.78b3
switchport port-security
!
interface FastEthernet1/7
switchport access vlan 101
shutdown
!
interface FastEthernet1/8
switchport access vlan 101
shutdown
!
```

5842

```
interface GigabitEthernet1/1
switchport access vlan 101
switchport mode access
switchport port-security mac-address e490.693b.c2c6
switchport port-security
!
interface GigabitEthernet1/2
shutdown
interface FastEthernet1/1
switchport access vlan 102
switchport mode access
switchport port-security mac-address 0cc4.7a32.b301
switchport port-security
!
interface FastEthernet1/2
switchport access vlan 102
switchport mode access
shutdown
!
interface FastEthernet1/3
switchport access vlan 102
shutdown
!
interface FastEthernet1/4
switchport access vlan 102
switchport mode access
switchport port-security mac-address fcaa.147a.aa42
switchport port-security
!
interface FastEthernet1/5
switchport access vlan 102
switchport mode access
switchport port-security mac-address 001d.9cc9.6d42
switchport port-security
!
interface FastEthernet1/6
switchport access vlan 102
switchport mode access
switchport port-security maximum 2
switchport port-security mac-address 0800.27ae.9958
switchport port-security mac-address 0cc4.7a31.44bd
switchport port-security
!
interface FastEthernet1/7
switchport access vlan 102
switchport mode access
switchport port-security mac-address 0060.3520.c156
switchport port-security
!
interface FastEthernet1/8
switchport access vlan 102
shutdown
```

```
interface GigabitEthernet1/1
switchport access vlan 102
switchport mode access
switchport port-security mac-address e490.693b.c2c7
switchport port-security
!
interface GigabitEthernet1/2
shutdown
!
interface Vlan1
no ip address
shutdown
```

Snippet from the Allen Bradley Boundary Router Running-Configuration file

```
interface FastEthernet1/3
description Engg LAN Workstation
switchport mode access
switchport port-security mac-address 40a8.f03d.48ae
switchport port-security
ip access-group EnggWkstn-ACL in
```

4.20.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the managed network interfaces due to their implementation method (i.e., manually disable unused network interfaces in configuration).

4.20.7 Link to Entire Performance Measurement Data Set

N/A

5857 4.21 Time Synchronization**5858 4.21.1 Technical Solution Overview**

5859 Ability to have all devices sync from a reliable time source. Time synchronization is vital for
5860 system logins, event tracking and all other time sensitive events occurring with a manufacturing
5861 system.

5862 No additional cost since services are included.

5863 Ease of use simple

5864 Effort and time required = minimal

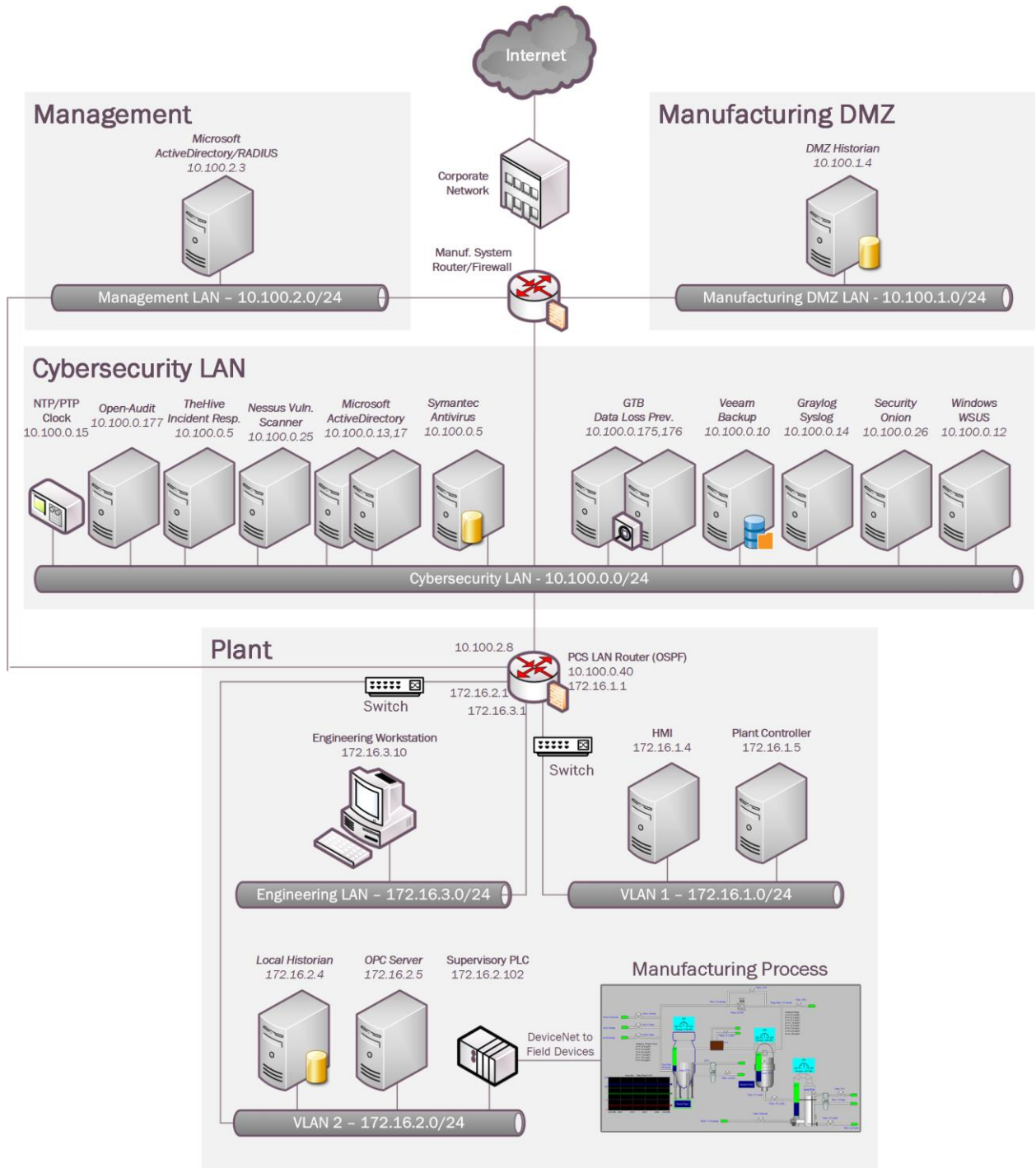
5865 4.21.2 Technical Capabilities Provided by Solution

5866 Time Synchronization provides components of the following Technical Capabilities described in
5867 Section 6 of Volume 1:

- 5868 • Time Synchronization

5869 4.21.3 Subcategories Addressed by Implementing Solution

5870 PR.PT-1

5871 **4.21.4 Architecture Map of Where Solution was Implemented**

5872

5873

4.21.5 Installation Instructions and Configurations

Details of the NTP server implemented:

Name	IP address	Purpose
Meinberg M9000 Lantime	10.100.0.15	NTP/PTP Clock

Computers:

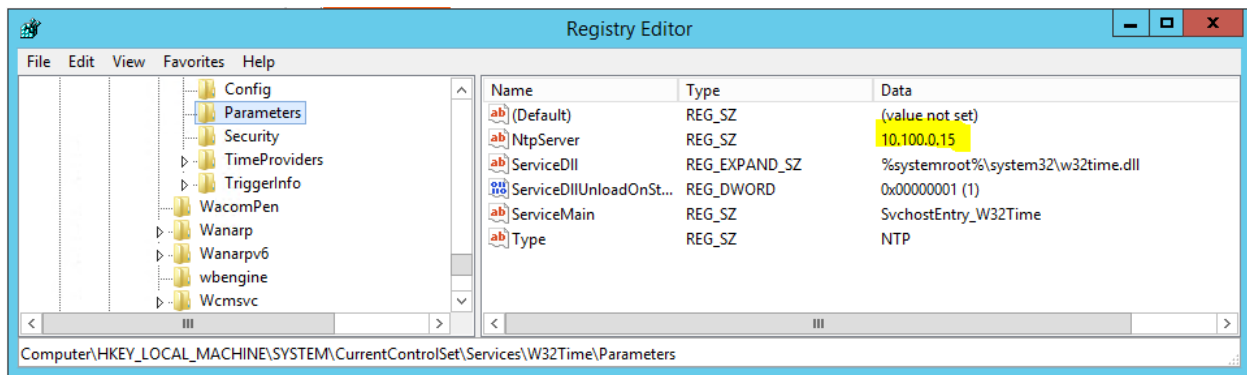
All windows computers within process control environment for Westman are joined to a domain.
Domain joined machines automatically update their time by contacting local domain controller.

Domain Controller:

Domain controller obtains time from Meinberg Lantime M900 device. W32tm.exe is used to configure Windows Time service settings. Change the following registry key on the Domain Controller to have w32Time sync its time from an external source IP address.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\NtpServer

The image below shows our Domain Controller pointing to the IP address of Meinberg LAN Time clock




**Other Devices:**

All other devices within manufacturing system contact Meinberg Lantime M900 using NTP to sync time.

Allen Bradley Boundary Router:

- Login to the web UI by browsing to <https://172.16.3.1>
- Click on Configure → NTP

- 5894
- Click Add button to add new time server.

<div>  Add  Edit  Delete </div>										
Status	Configured	IP Address	Prefer	Ref Clock	Stratum	When	Poll	Delay	Off Set	
<input type="radio"/> sys:peer	Yes	10.100.0.15	<input checked="" type="checkbox"/>	129.6.15.28	2	558	1024	0.767	-0.334	

- 5895
- 5896
- 5897
- Save change
 - Logout

5898 **Switches:**

- 5899
- Steps for switches **Vlan1 (172.16.1.3)** and **Vlan2 (172.16.2.2)** are the same as above.

5900 **Lesson Learned:** The master time reference selected should be as close to your physical location
5901 as possible. This should reduce the Off Set.

5902

5903 **4.21.6 Highlighted Performance Impacts**

5904 No performance measurement experiments were performed for time synchronization due to its
5905 installation in the system before the Manufacturing Profile implementation was initiated.

5906 **4.21.7 Link to Entire Performance Measurement Data Set**

5907 N/A

5908

5909 **4.22 System Use Monitoring**

5910 **4.22.1 Technical Solution Overview**

5911 System use monitor is accomplished by multiple tools to protect manufacturing system
5912 environment from harmful activities using data loss protection, auditing and syslog server for
5913 monitoring, store and auditing. Each tool provides a different level required to protect the
5914 manufacturing system.

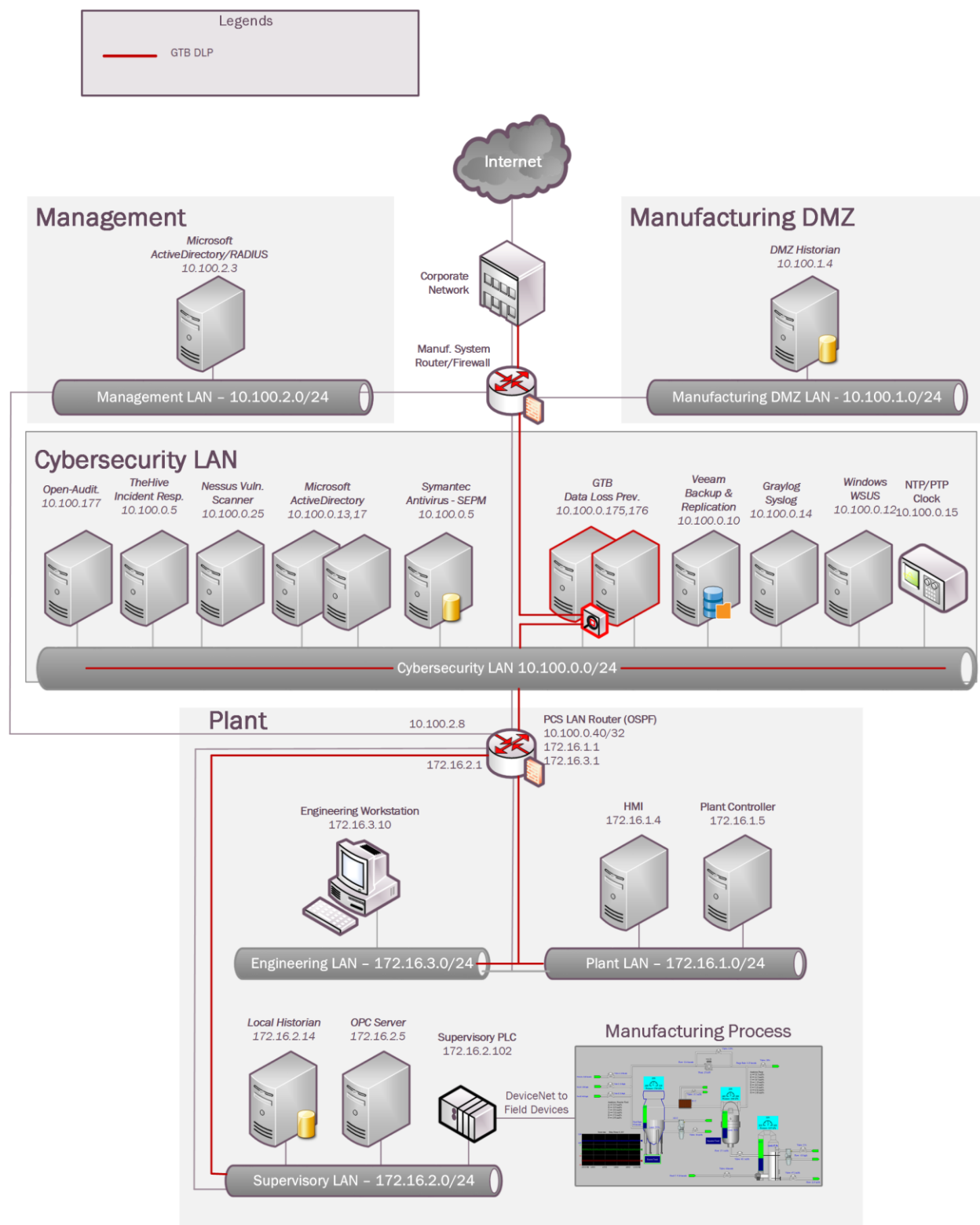
5915 Implementation effort is moderate requiring understanding of Linux and Windows systems, along
5916 with virtual machine experience. Time required to install and configure all components 10 to 20
5917 hours depending on skill level.

5918 **4.22.2 Technical Capabilities Provided by Solution**

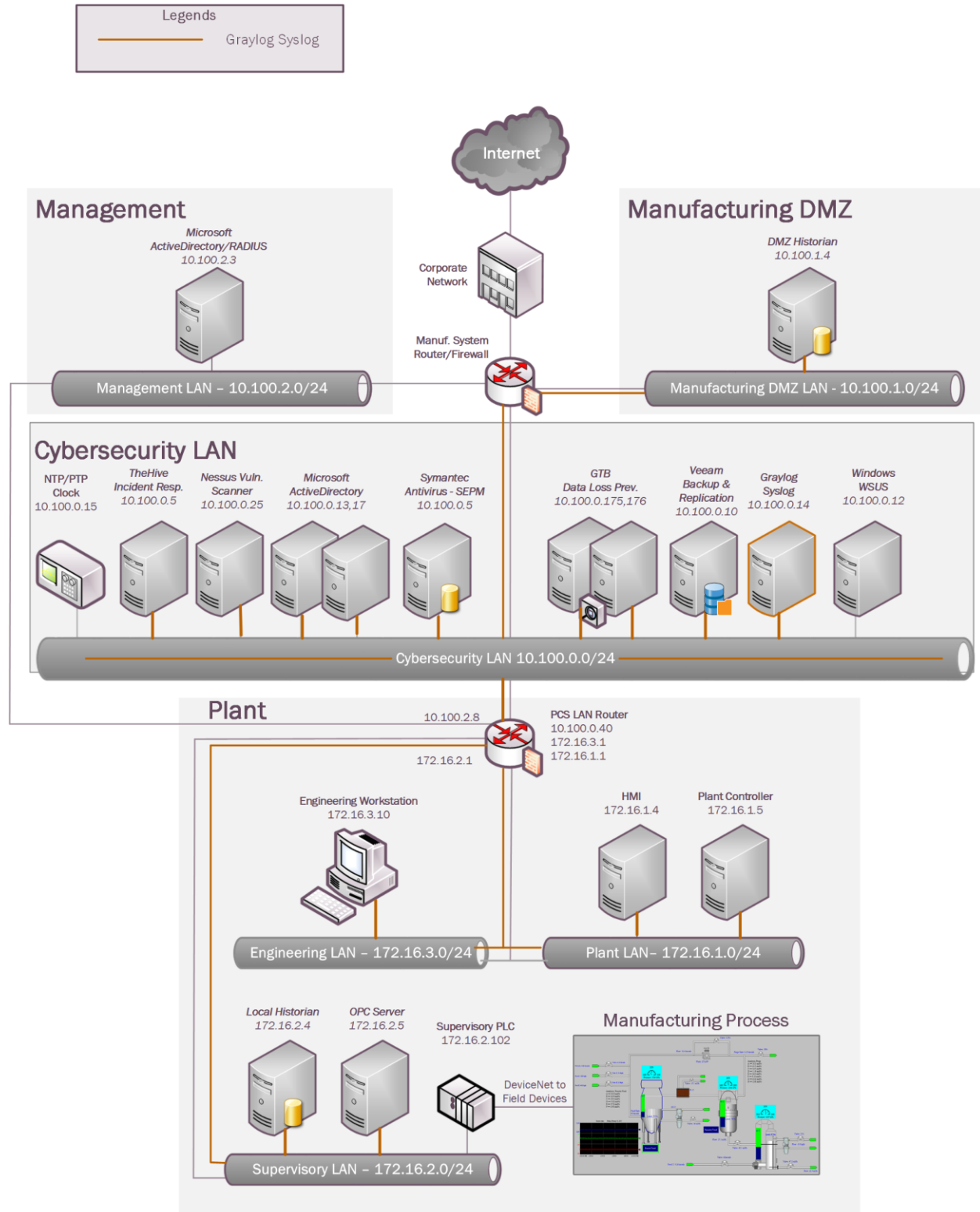
5919 System Use Monitoring was provided by GTB Inspector, Ports and Services Lockdown, and
5920 Graylog.

5921 **4.22.3 Subcategories Addressed by Implementing Solution**

5922 PR.AC-1, PR.DS-5, PR.MA-2, DE.CM-3

5923 **4.22.4 Architecture Map of Where Solution was Implemented**

5924



5925

5926

5927 **4.22.5 Installation Instructions and Configurations**

5928 System use monitoring was implemented using a combination of tools such as GTB Inspector,
5929 Graylog and native Windows Server Capabilities such as enabling Auditing, restricting
5930 administrative user accounts.

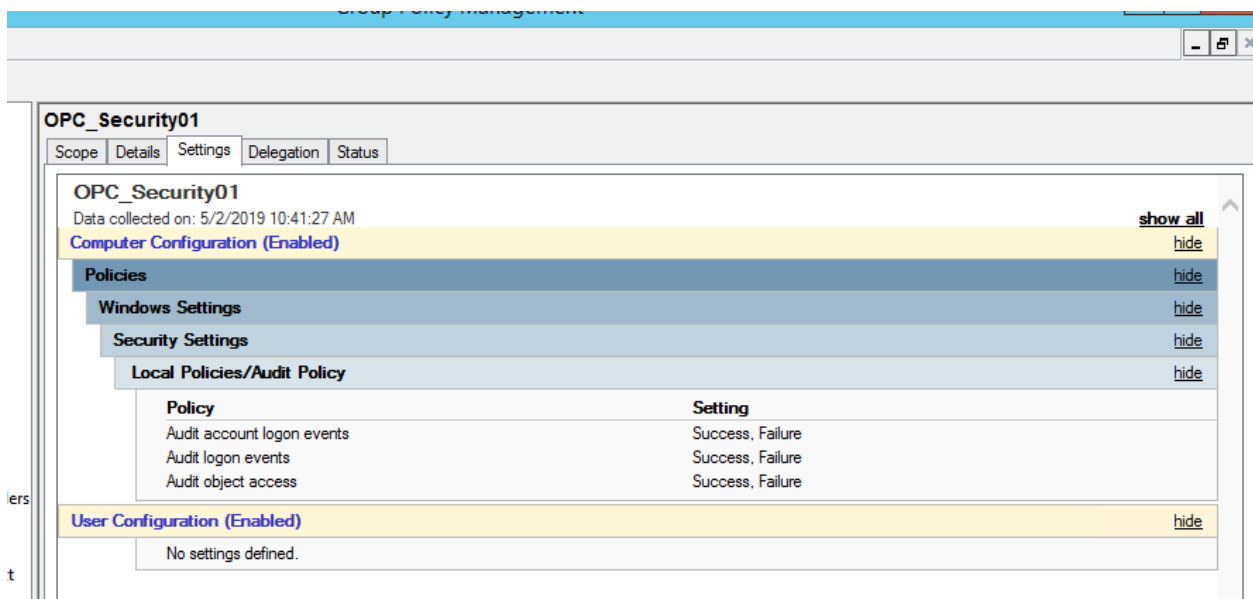
5931 **GTB DLP:** See Section 4.15.5 for instructions.

5932 **Graylog:** See Section 4.16.5 for instructions

5933 **Auditing Logon events:**

5934 Open Group Policy manager on domain controller.

5935 Right click on Group Policy and select edit.



5936

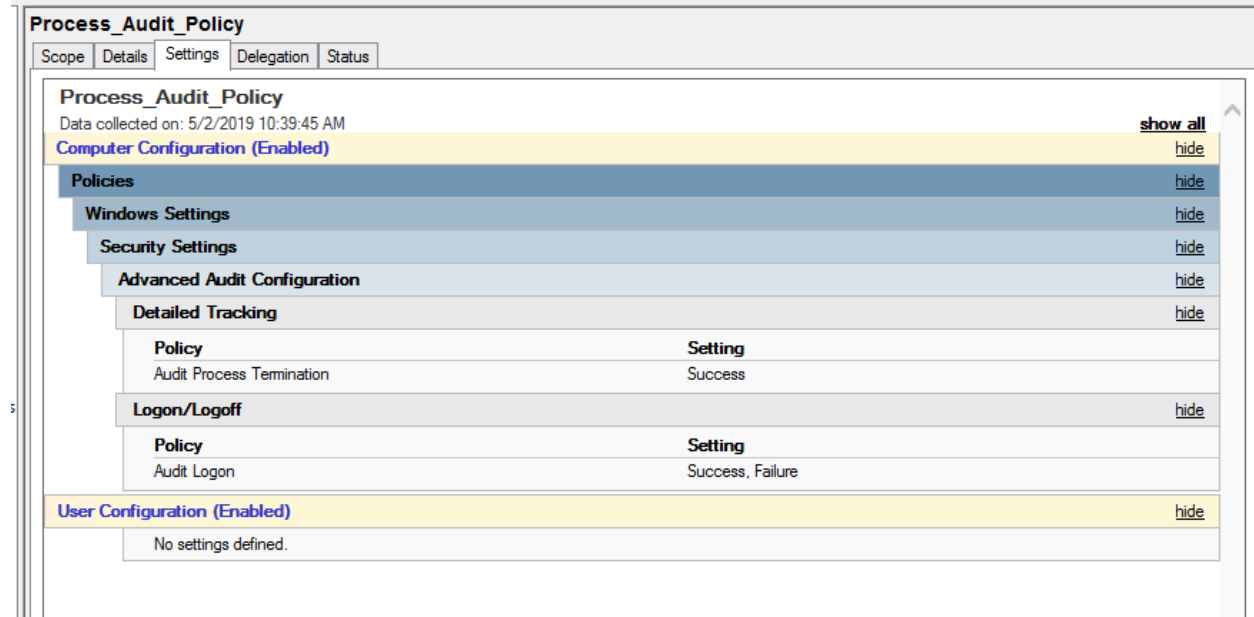
5937 Navigate to Computer Configuration→Policies→Windows Settings→Security Settings→Local
5938 Policies→Audit Policy

5939 Now change setting to reflect Success, Failure

5940 **Auditing Process Termination:**

5941 While in Group Policy manager navigate to Computer Configuration→Policies→Windows
5942 Settings→Security Settings→Advanced Audit Configuration→

5943 Change Detailed Tracking and Logon/Logoff to Success / Success, Failure (See Image)



5944

5945 **Restricting Administrative Users:**

5946 The local Administrators group on each system was reviewed and only those accounts that
 5947 needed to have Administrative privileges on the system were added to this group.

5948 For instance: An active directory user account “opc-admin” was created to run OPC-server
 5949 services and was granted Administrative privileges on the below 2 servers:

- 5950
- OPC Server
- 5951
- Controller Server

5952 Remote Access to PLC is only permitted through Engineering workstation.

5953 **4.22.6 Highlighted Performance Impacts**

5954 No performance measurement experiments were performed for the installation of GTB into the
 5955 PCS due to its location within the network topology. No manufacturing process components
 5956 across the boundary on a regular basis while the system is operational.

5957 No performance measurement experiments were performed for the use of the Graylog due to its
 5958 typical installation and usage location (i.e., external to the manufacturing system).

5959 **4.22.7 Link to Entire Performance Measurement Data Set**

5960 N/A

5961

5962 **4.23 Ports and Services Lockdown**

5963 **4.23.1 Technical Solution Overview**

5964 Ports and services lockdown solutions enable a manufacturer to discover and disable
5965 nonessential logical network ports and services. A logical port is a number assigned to a
5966 “logical” connection. Port numbers are assigned to a service, which is helpful to TCP/IP in
5967 identifying what ports it must send traffic to. Hackers use port scanners and vulnerability
5968 scanners to identify open ports on servers. By revealing which ports are open, the hacker can
5969 identify what kind of services are running and the type of system. Closing down unnecessary
5970 ports by uninstalling un-necessary programs considerably reduces the attack surface. These
5971 actions need to be performed manually.

5972
5973 Native OS capabilities, Open-Audit and Nessus scanner were leveraged to inventory list of ports
5974 and applications currently running on each device of the plant.

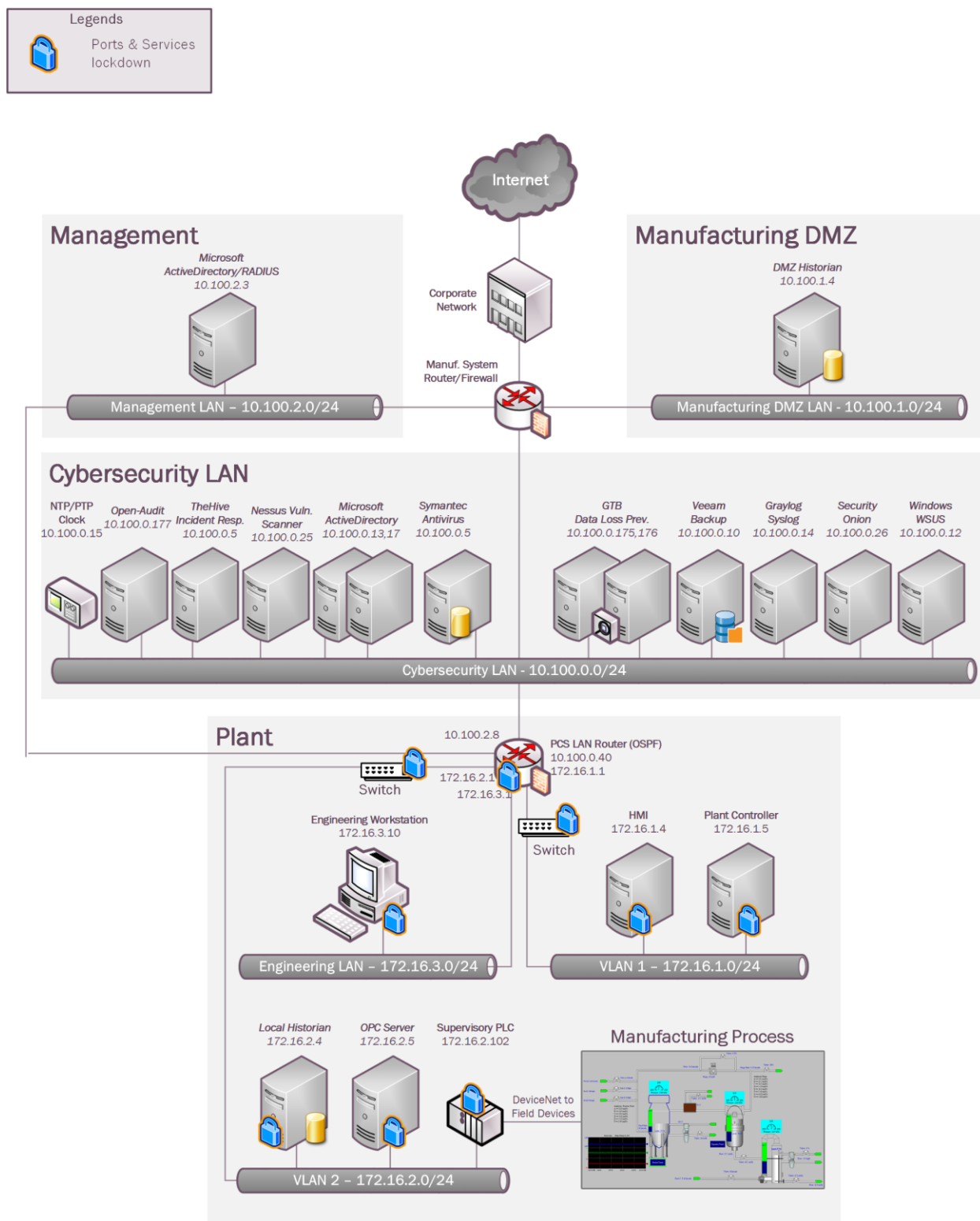
5975 5976 **4.23.2 Technical Capabilities Provided by Solution**

5977 Ports and Services Lockdown provides components of the following Technical Capabilities
5978 described in Section 6 of Volume 1:

- 5979
5980
 - Ports and Services Lockdown

5981 **4.23.3 Subcategories Addressed by Implementing Solution**

5982 PR.IP-1, PR.PT-3

5983 **4.23.4 Architecture Map of Where Solution was Implemented**

5984

5985 **4.23.5 Installation Instructions and Configurations**

5986 The following steps were performed on all Windows systems of the Plant

- 5987 • Removal of Un-wanted programs
- 5988 • Disable unsecure services

5989 Removal of Un-wanted programs:

5990 A software inventory of each system was performed using Open-Audit. The inventory reports

5991 were reviewed, and a list of unwanted programs were identified. These includes some software

5992 that's comes by default with the OS. These programs were then uninstalled.

5993 Netstat utility was used to gather information about which applications are running or using

5994 which TCP/IP ports on each system

5995 For instance: `netstat -aon | more` will generate a list of processes, PID

```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netstat -aon | more

Active Connections

  Proto Local Address           Foreign Address         State       PID
  TCP   0.0.0.0:135              0.0.0.0:0               LISTENING   976
  TCP   0.0.0.0:445              0.0.0.0:0               LISTENING   4
  TCP   0.0.0.0:1332             0.0.0.0:0               LISTENING   2552
  TCP   0.0.0.0:3060             0.0.0.0:0               LISTENING   3844
  TCP   0.0.0.0:3389             0.0.0.0:0               LISTENING   1412
  TCP   0.0.0.0:4241             0.0.0.0:0               LISTENING   2756
  TCP   0.0.0.0:5241             0.0.0.0:0               LISTENING   2812
  TCP   0.0.0.0:5357             0.0.0.0:0               LISTENING   4
  TCP   0.0.0.0:6000             0.0.0.0:0               LISTENING   1204
  TCP   0.0.0.0:6002             0.0.0.0:0               LISTENING   2892
  TCP   0.0.0.0:6160             0.0.0.0:0               LISTENING   8288
  TCP   0.0.0.0:6183             0.0.0.0:0               LISTENING   8532
  TCP   0.0.0.0:6185             0.0.0.0:0               LISTENING   8532
  TCP   0.0.0.0:7001             0.0.0.0:0               LISTENING   2856
  TCP   0.0.0.0:7002             0.0.0.0:0               LISTENING   2856
  TCP   0.0.0.0:8082             0.0.0.0:0               LISTENING   2664
  TCP   0.0.0.0:9395             0.0.0.0:0               LISTENING   8532

```

5996

5997 The PID from the above output can be used with Windows Task Manager for further analysis.

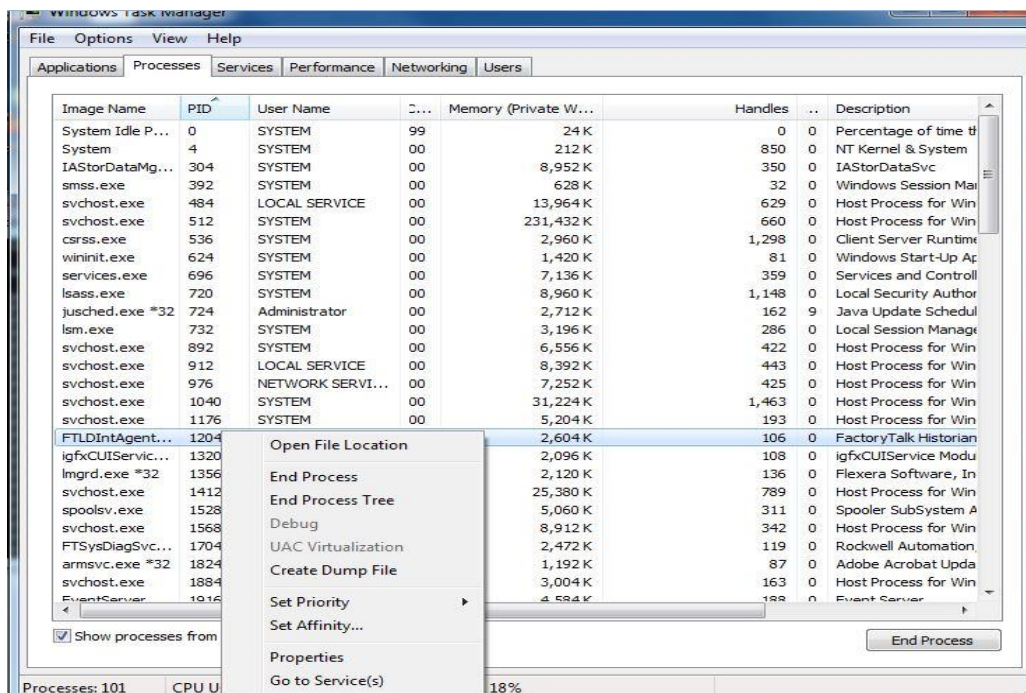
5998 Within Task Manager (Windows 7), enable the PID column by clicking on **View >> Select**

5999 **Columns.**

6000 Next, you might have to use the option to Show Processes for All Users, and then you'll be able

6001 to find the PID in the list. Once you're there, you can use the End Process, Open File Location,

6002 or Go to Service(s) options to control the process or stop it.



6003

6004 Other alternatives are using **Resource Monitor** (resmon.exe) and **TCPView** from SysInternals
 6005 [1].

6006 TCPView:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	Status	Sent Packets	Sent Bytes
RdcyHost.exe	2552	TCP	127.0.0.1	1332	127.0.0.1	49192	ESTABLISHED		
Rsvchost.exe	2812	TCP	127.0.0.1	5241	127.0.0.1	49193	ESTABLISHED		
Rsvchost.exe	2812	TCP	127.0.0.1	5241	127.0.0.1	65156	ESTABLISHED		
Rsvchost.exe	2812	TCP	127.0.0.1	5241	127.0.0.1	65157	ESTABLISHED		
Rsvchost.exe	2812	TCP	127.0.0.1	5241	127.0.0.1	65160	ESTABLISHED		
Rsvchost.exe	2812	TCP	127.0.0.1	5241	127.0.0.1	49174	ESTABLISHED		
Imgrd.exe	1356	TCP	127.0.0.1	27000	127.0.0.1	49172	ESTABLISHED		
nxlog.exe	2332	TCP	127.0.0.1	49166	127.0.0.1	49167	ESTABLISHED		
nxlog.exe	2332	TCP	127.0.0.1	49167	127.0.0.1	49166	ESTABLISHED		
flexsvr.exe	2404	TCP	127.0.0.1	49170	127.0.0.1	49171	ESTABLISHED		
flexsvr.exe	2404	TCP	127.0.0.1	49171	127.0.0.1	49170	ESTABLISHED		
flexsvr.exe	2404	TCP	127.0.0.1	49172	127.0.0.1	27000	ESTABLISHED		
RSLinxNG.exe	2756	TCP	127.0.0.1	49174	127.0.0.1	5241	ESTABLISHED		
RdcyHost.exe	2552	TCP	127.0.0.1	49192	127.0.0.1	1332	ESTABLISHED		
RdcyHost.exe	2552	TCP	127.0.0.1	49193	127.0.0.1	5241	ESTABLISHED		
mstsc.exe	4864	TCP	172.16.3.10	51955	172.16.1.4	3389	ESTABLISHED		
mstsc.exe	7996	TCP	172.16.3.10	51956	172.16.2.5	3389	ESTABLISHED		
WinSCP.exe	8732	TCP	172.16.3.10	58958	10.100.0.16	22	ESTABLISHED		
putty.exe	3456	TCP	172.16.3.10	60520	10.100.0.16	22	ESTABLISHED		
putty.exe	4944	TCP	172.16.3.10	60522	10.100.0.16	22	ESTABLISHED		
putty.exe	3884	TCP	172.16.3.10	60526	10.100.0.16	22	ESTABLISHED		
mstsc.exe	9052	TCP	172.16.3.10	64301	172.16.2.3	3389	ESTABLISHED		
mstsc.exe	8308	TCP	172.16.3.10	64317	172.16.2.4	3389	ESTABLISHED		
mstsc.exe	2296	TCP	172.16.3.10	64328	172.16.1.5	3389	ESTABLISHED		
EventClientMultiplexer.exe	3864	TCP	127.0.0.1	65156	127.0.0.1	5241	ESTABLISHED		
RndDirServer.exe	3844	TCP	127.0.0.1	65157	127.0.0.1	5241	ESTABLISHED		
RNADirMultiplexor.exe	4340	TCP	127.0.0.1	65160	127.0.0.1	5241	ESTABLISHED		
RdcyHost.exe	2552	TCP	172.16.3.10	65109	172.16.2.4	1332	SYN_SENT		

6007

6008

6009 The following steps were performed on all network devices of the Plant

- 6010 • Disabling unsecure services such as Telnet, SNMP (1 and 2)
- 6011 • If SNMP is required, change the default community string
- 6012 • Setting a password for enable

6013 Cisco commands to set a password for enable:

```
6014 router1(config)# enable
6015 router1(config)# configure terminal
6016 router1(config)# enable secret <password>
6017
```

- 6018 • Restrict ssh access to select machines.

6019 Cisco commands to restrict access [2]:

```
6020 router1(config)# enable
6021 router1(config)# configure terminal
6022 router1(config)# access-list 1 permit 172.16.0.0 0.0.255.255
6023 router1(config)# line vty 0 15
6024 router1(config-line)# access-class 1 in
6025
```

6026 The following steps were performed on the PLC

- 6027 • Disabled unsecure services such as Telnet, SNMP and HTTP
- 6028 • Remote Access to the PLC was permitted only through the Engineering Workstation.

6029 4.23.6 Highlighted Performance Impacts

6030 No performance measurement experiments were performed for the managed network interfaces
6031 due to their implementation method (i.e., manually disabled network ports and removed
6032 unwanted Windows programs and services).

6033 4.23.7 Link to Entire Performance Measurement Data Set

6034 N/A

6035 4.24 Media Protection**6036 4.24.1 Technical Solution Overview**

6037 Port locks provide a low-cost solution for protecting USB ports. Implementation and ease of use
6038 provide for quick install and easy removal. USB Port locks provide a simple yet effective
6039 solution to restrict USB use. Once USB Port lock has been inserted and engaged there is no way
6040 of removing lock device without damaging USB port unless key is used. Each USB Port lock can
6041 block up to two ports. These ports are the inserted port, and the port directly to either side
6042 depending on the blocking plate direction. USB Port Lock can be purchased with a collar that
6043 protects attached USB Mice and Keyboards from removal without prior approval.

6044 4.24.2 Technical Capabilities Provided by Solution

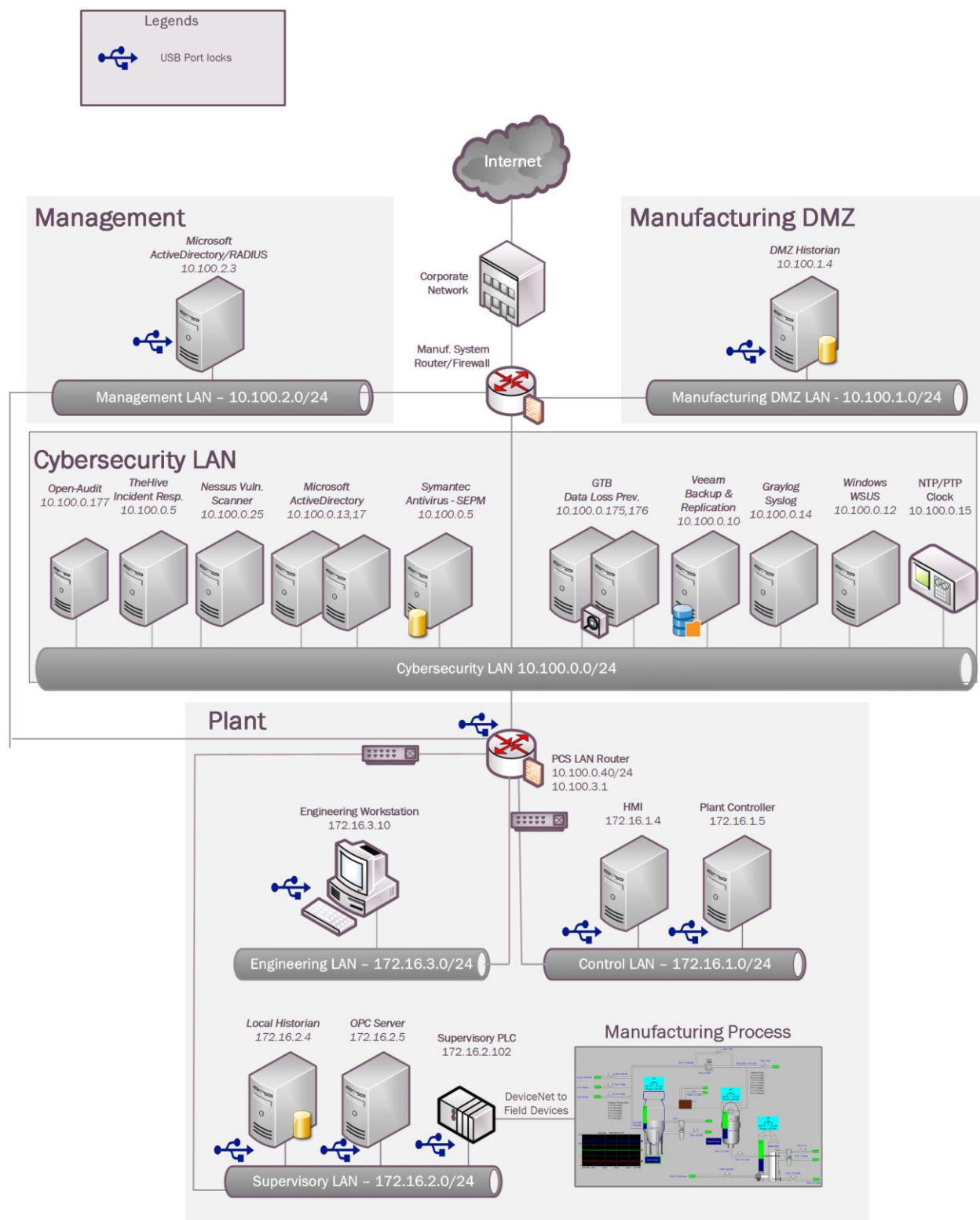
6045 Media Protection provides components of the following Technical Capabilities described in
6046 Section 6 of Volume 1:

- 6047
- 6048 • Media Protection

6049 4.24.3 Subcategories Addressed by Implementation

6050 PR.PT-2

6051

6052 **4.24.4 Architecture Map of Where Solution was Implemented**

6053

6054 **4.24.5 Installation Instructions and Configurations**6055 **• Products / Tools found to meet capability:**

- 6056
 - Kensington USB Port Locks
 - 6057 ○ Symantec Endpoint Protection (USB Policy Enforcement)
 - 6058 ○ Group Policy Management (GPO) Active Directory

6059 **• Product / Tools selected to be implemented in testbed:**

- 6060
 - Kensington USB Port Locks (Protects Linux Machines)
 - 6061 ○ Symantec Endpoint Protection (USB Policy Enforcement - Protects Windows
 - 6062 Machines)
 - 6063 ○ Group Policy (GPO) Active Directory (Protects Windows Machines)

6064 **• Products Overview:**

- 6065
 - USB Port locks from Kensington provide an alternative for small manufactures
 - 6066 that don't have the resources or primarily run Linux machines within their
 - 6067 environment to have a solution that protections from rogue USB devices being
 - 6068 used without approval.
 - 6069 ▪ **Pros:** Quick solution, Hardware only solution, inexpensive
 - 6070 ▪ **Cons:** Feels like having to force device into USB Port first few times

6071 Insert USB Port lock then push locking button in to secure. Kensington provides inserts to block
6072 multiple ports including locks designed for securing USB Keyboards and Mice.

6073 **Lessons learned:**

6074 Patience is required when using this product so as not to inadvertently damage USB port

6075 **4.24.6 Highlighted Performance Impacts**

6076 No performance measurement experiments were performed for the USB port locks due to their
6077 implementation method (i.e., physically restricting access to USB ports).

6078 **4.24.7 Link to Entire Performance Measurement Data Set**

6079 N/A

6080

6081

Appendix A - Acronyms and Abbreviations

Selected acronyms and abbreviations used in this document are defined below.

CSF	Cybersecurity Framework
FIPS	Federal Information Processing Standards
HMI	Human Machine Interface
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ISA	The International Society of Automation
IT	Information Technology
LAN	Local Area Network
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OT	Operational Technology
PLC	Programmable Logic Controller
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

6099 **Appendix B - Glossary**

6100 Selected terms used in in this document are defined below.

6101 **Business/Mission Objectives** - Broad expression of business goals. Specified target outcome
6102 for business operations.

6103
6104 **Capacity Planning** - Systematic determination of resource requirements for the
6105 projected output, over a specific period. [businessdictionary.com]
6106

6107 **Category** - The subdivision of a Function into groups of cybersecurity outcomes closely tied to
6108 programmatic needs and particular activities.

6109
6110 **Critical Infrastructure** - Essential services and related assets that underpin American society
6111 and serve as the backbone of the nation's economy, security, and health. [DHS]
6112

6113 **Criticality Reviews** - A determination of the ranking and priority of manufacturing system
6114 components, services, processes, and inputs in order to establish operational thresholds and
6115 recovery objectives.

6116
6117 **Critical Services** - The subset of mission essential services required to conduct manufacturing
6118 operations. Function or capability that is required to maintain health, safety, the environment and
6119 availability for the equipment under control. [62443]
6120

6121 **Cyber Risk** - Risk of financial loss, operational disruption, or damage, from the failure of the
6122 digital technologies employed for informational and/or operational functions introduced to a
6123 manufacturing system via electronic means from the unauthorized access, use, disclosure,
6124 disruption, modification, or destruction of the manufacturing system.

6125
6126 **Cybersecurity** - The process of protecting information by preventing, detecting, and responding
6127 to attacks. [CSF]
6128

6129 **Defense-in-depth** - The application of multiple countermeasures in a layered or stepwise manner
6130 to achieve security objectives. The methodology involves layering heterogeneous security
6131 technologies in the common attack vectors to ensure that attacks missed by one technology are
6132 caught by another. [62443 1-1]
6133

6134 **Event** - Any observable occurrence on a manufacturing system. Events can include
6135 cybersecurity changes that may have an impact on manufacturing operations (including mission,
6136 capabilities, or reputation). [CSF]
6137

6138 **Firmware** - Software program or set of instructions programmed on the flash ROM of a
6139 hardware device. It provides the necessary instructions for how the device communicates with
6140 the other computer hardware. [Techterms.com]
6141

Framework - The Cybersecurity Framework developed for defining protection of critical infrastructure. It provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. Includes activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes.

Function - Primary unit within the Cybersecurity Framework. Exhibits basic cybersecurity activities at their highest level.

Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [CSF]

Integrator - A value-added engineering organization that focuses on industrial control and information systems, manufacturing execution systems, and plant automation, that has application knowledge and technical expertise, and provides an integrated solution to an engineering problem. This solution includes final project engineering, documentation, procurement of hardware, development of custom software, installation, testing, and commissioning. [CSIA.com]

Manufacturing Operations - Activities concerning the facility operation, system processes, materials input/output, maintenance, supply and distribution, health, and safety, emergency response, human resources, security, information technology and other contributing measures to the manufacturing enterprise.

Network Access - any access across a network connection in lieu of local access (i.e., user being physically present at the device).

Operational technology - Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. [Gartner.com]

Programmable Logic Controller - A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing. [800-82]

Profile - A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories. [CSF]

- Target Profile - the desired outcome or 'to be' state of cybersecurity implementation
- Current Profile – the 'as is' state of system cybersecurity

Protocol - A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [800-82]

Remote Access - Access by users (or information systems) communicating external to an information system security perimeter. Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). [800-53]

Resilience Requirements - The business-driven availability and reliability characteristics for the manufacturing system that specify recovery tolerances from disruptions and major incidents.

Risk Assessment - The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. [800-82]

Risk Tolerance - The level of risk that the Manufacturer is willing to accept in pursuit of strategic goals and objectives. [800-53]

Router - A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets. [800-82]

Security Control - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data. [800-82]

Subcategory - The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.” [CSF]

Supporting Services - Providers of external system services to the manufacturer through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. Supporting services include, for example, Telecommunications, engineering services, power, water, software, tech support, and security. [800-53]

Switch - A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. [Whatis.com]

System Categorization - The characterization of a manufacturing system, its components, and operations, based on an assessment of the potential impact that a loss of availability, integrity, or confidentiality would have on organizational operations, organizational assets, or individuals. [FIPS 199]

6230 **Third-Party Relationships** - relationships with external entities. External entities may include,
6231 for example, service providers, vendors, supply-side partners, demand-side partners, alliances,
6232 consortiums, and investors, and may include both contractual and non-contractual parties.
6233 [DHS]

6234 **Third-party Providers** - Service providers, integrators, vendors, telecommunications, and
6235 infrastructure support that are external to the organization that operates the manufacturing
6236 system.

6237
6238 **Thresholds** - Values used to establish concrete decision points and operational control limits to
6239 trigger management action and response escalation.

Appendix C - References

1. Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. <https://www.govinfo.gov/app/details/FR-2013-02-19/2013-03915>
2. National Institute of Standards and Technology (2014) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), February 12, 2014. <https://doi.org/10.6028/NIST.CSWP.02122014>
3. Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-82r2>
4. Stouffer K, Zimmerman T, Tang CY, Lubell J, Cichonski J, McCarthy J (2017) Cybersecurity Framework Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8183, Includes updates as of May 20, 2019. <https://doi.org/10.6028/NIST.IR.8183>