NIST SPECIAL PUBLICATION 1800-23

Energy Sector Asset Management

For Electric Utilities, Oil & Gas Industry

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

James McCarthy
Lauren Acierto
Glen Joy
Jason Kuruvilla
Titilayo Ogunyale
Nikolas Urlaub
John Wiltberger
Devin Wynne

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-23

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/library/energy-sector-asset-management-nist-sp-1800-23-practice-guide

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SPECIAL PUBLICATION 1800-23

Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry

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

James McCarthy
Glen Joy
National Cybersecurity Center of Excellence
Information Technology Laboratory

Lauren Acierto
Jason Kuruvilla
Titilayo Ogunyale
Nikolas Urlaub
John Wiltberger
Devin Wynne
The MITRE Corporation
McLean, Virginia

May 2020

U.S. Department of Commerce
Wilbur Ross, Secretary

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

NIST SPECIAL PUBLICATION 1800-23A

Energy Sector Asset Management

For Electric Utilities, Oil & Gas Industry

Volume A:
Executive Summary

James McCarthy
Glen Joy
National Cybersecurity Center of Excellence
Information Technology Laboratory

Lauren Acierto
Jason Kuruvilla
Titilayo Ogunyale
Nikolas Urlaub
John Wiltberger
Devin Wynne
The MITRE Corporation
McLean, Virginia

May 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-23

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/library/energy-sector-asset-management-nist-sp-1800-23-practice-guide

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Executive Summary

- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to demonstrate how energy organizations can strengthen their operational technology (OT) asset management practices by leveraging capabilities that may already exist within their operating environment or by implementing new capabilities.
- As electric utilities and the oil and gas industry are some of the nation's critical infrastructures, the incapacitation or destruction of assets, systems, and networks in the energy sector could have serious negative effects on the economy, public health, and safety.
- As industrial control systems (ICS) in the energy sector become more interconnected, vulnerabilities within OT assets and processes are targets for malicious actors.
- A challenge for energy organizations is maintaining an updated asset inventory. It is difficult to protect what is not seen or is not known. Without an effective asset management solution, organizations that are unaware of assets in their infrastructure may unnecessarily expose themselves to cybersecurity risks.
- This NIST Cybersecurity Practice Guide provides detailed steps on how energy organizations can identify and manage OT assets and detect cybersecurity risks associated with them.

CHALLENGE

Energy organizations may be a prime target of growing and evolving cybersecurity threats, given the criticality of their infrastructure to our nation. A cyber attack that disrupts OT processes or equipment can result in safety issues and the loss of power, as well as in significant productivity costs. Currently, many energy organizations rely on manual processes to manage their OT assets, which makes it challenging to quickly identify and respond to potential threats. Existing asset inventories may be static, one-time, or point-in-time snapshots of auditing activities conducted previously without a way to see the current status of those assets. As OT systems become interconnected and integrated with other information technology (IT) systems, organizations looking to modernize OT processes will have to find automated methods to strengthen their OT asset management capabilities.

SOLUTION

The NCCoE, in collaboration with experts from the energy sector and technology vendors, developed an asset management example solution that includes managing, monitoring, and baselining OT assets to reduce the risk of cybersecurity incidents. This practice guide outlines practical steps on how organizations can implement new asset management capabilities or leverage existing asset management capabilities, to enhance the security of OT assets.

The NCCoE sought existing technologies that provided the following capabilities:

- OT/ICS asset inventory (including devices using serial connections)
- high-speed communication mechanisms for remote asset management
- reliable/secure/encrypted communications

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-23.

- continuous asset monitoring
- log analysis and correlation
- cybersecurity event/attack detection
- patch-level information
- vulnerability awareness

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT/OT infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

The NCCoE's practice guide on Energy Sector Asset Management can help your energy organization:

- reduce cybersecurity risk and potentially reduce the impact of safety and operational risks such as power disruption
- develop and execute a strategy that provides continuous OT asset management and monitoring
- respond faster to security alerts through automated cybersecurity-event capabilities
- implement current cybersecurity standards and best practices, while maintaining the performance of energy infrastructures

SHARE YOUR FEEDBACK

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

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

TECHNOLOGY PARTNERS/COLLABORATORS

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

DRAGOS FORESCOUT FOXGUARD SOLUTIONS KORE splunk> tripwire tdi technologies

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

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

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

NIST SPECIAL PUBLICATION 1800-23B

Energy Sector Asset Management

For Electric Utilities, Oil & Gas Industry

Volume B:
Approach, Architecture, and Security Characteristics

James McCarthy
Glen Joy
National Cybersecurity Center of Excellence
Information Technology Laboratory

Lauren Acierto
Jason Kuruvilla
Titilayo Ogunyale
Nikolas Urlaub
John Wiltberger
Devin Wynne
The MITRE Corporation
McLean, Virginia

May 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-23

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/library/energy-sector-asset-management-nist-sp-1800-23-practice-guide

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-23B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-23B, 47 pages, (May 2020), CODEN: NSPUE2

FEEDBACK

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Industrial control systems (ICS) compose a core part of our nation's critical infrastructure. Energy sector companies rely on ICS to generate, transmit, and distribute power and to drill, produce, refine, and transport oil and natural gas. Given the wide variety of ICS assets, such as programmable logic controllers and intelligent electronic devices, that provide command and control information on operational technology (OT) networks, it is essential to protect these devices to maintain continuity of operations. These assets must be monitored and managed to reduce the risk of a cyber attack on ICS-networked environments. Having an accurate OT asset inventory is a critical component of an overall cybersecurity strategy.

The NCCoE at NIST is responding to the energy sector's request for an automated OT asset management solution. To remain fully operational, energy sector entities should be able to effectively identify, control, and monitor their OT assets. This document provides guidance on how to enhance OT asset management practices by leveraging capabilities that may already exist in an energy organization's operating environment as well as implementing new capabilities.

KEYWORDS

energy sector asset management; ESAM; ICS; industrial control system; malicious actor; monitoring; operational technology; OT; SCADA; supervisory control and data acquisition

ACKNOWLEDGMENTS

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

Name	Organization
Matt Cowell	Dragos, Inc.
Tom VanNorman	Dragos, Inc.
Andrew Dunham	Forescout Technologies, Inc.
Tim Jones	Forescout Technologies, Inc.
John Norsworthy	Forescout Technologies, Inc.
Lindsey Hale	FoxGuard Solutions, Inc.
Steve Boyd	KORE Wireless, Inc.
Brian Hicks	KORE Wireless, Inc.
Adam Cohn	Splunk Inc.
Bill Wright	Splunk Inc.
Ray Erlinger	TDi Technologies, Inc.
Bill Johnson	TDi Technologies, Inc.

Name	Organization
Samantha Pelletier	TDi Technologies, Inc.
Gabe Authier	Tripwire, Inc.
Steven Sletten	Tripwire, Inc.
Jim Wachhaus	Tripwire, Inc.

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

Technology Partner/Collaborator	Build Involvement
Dragos, Inc.	Dragos Platform v1.5
Forescout Technologies, Inc.	ForeScout CounterACT v8.0.1
FoxGuard Solutions, Inc.	FoxGuard Solutions Patch and Update Management Program v1
KORE Wireless Group, Inc.	KORE Wireless Cellular Connectivity with Cellular Gateway v2.0
Splunk, Inc.	Splunk Enterprise v7.1.3
TDi Technologies, Inc.	TDi Technologies ConsoleWorks v5.2-0u1
Tripwire, Inc.	Tripwire Industrial Visibility v3.2.1

Contents

List of Figures

List of Tables

1 Summary

Industrial control systems (ICS) compose a core part of our nation's critical infrastructure [1]. Energy-sector companies rely on ICS to generate, transmit, and distribute power and to drill, produce, refine, and transport oil and natural gas. Given the wide variety of ICS assets, such as programmable logic controllers (PLCs) and intelligent electronic devices (IEDs), which provide command and control information on operational technology (OT) networks, it is essential to protect these devices to maintain continuity of operations. Having an accurate OT asset inventory is a critical component of an overall cybersecurity strategy.

Energy companies own, operate, and maintain critical OT assets that possess unique requirements for availability and reliability. These assets must be monitored and managed to reduce the risk of cyber attacks on ICS-networked environments. Key factors in strengthening OT asset management capabilities are determining which tools can collect asset information and what type of communications infrastructure is required to transmit this information.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) is responding to the energy sector's request for an automated OT asset management solution. To remain fully operational, energy sector entities should be able to effectively identify, control, and monitor all of their OT assets. This document provides guidance on how to enhance OT asset management practices, by leveraging capabilities that may already exist in an energy organization's operating environment as well as implementing new capabilities.

The capabilities demonstrated in this guide were selected to address several key tenets of asset management: 1) establish a baseline of known assets, 2) establish a dynamic asset management platform that can alert operators to changes in the baseline, and 3) capture as many attributes about the assets as possible via the automated capabilities implemented.

In addition to these key tenets, this practice guide offers methods of asset management that address particular challenges in an OT environment, including the need to 1) account for geographically dispersed and remote assets, 2) have a consolidated view of the sum total of OT assets, and 3) be able to readily identify an asset's disposition, or level of criticality, in the overall operational environment.

The capabilities showcased in this guide may provide energy-sector entities with the means to establish a comprehensive OT asset management baseline that can be monitored over the life of the asset. Implementation of these capabilities provides an automated inventory that can be viewed in near real time and can alert designated personnel to changes to the inventory. This will prove useful from both a cybersecurity and operational perspective, as it can otherwise be difficult to quickly identify any anomalies due to a cyber attack or operational issues. This document concerns itself primarily with cybersecurity; however, it is possible that other operational benefits may be realized.

1.1 Challenge

Many energy-sector companies face challenges in managing their assets, particularly when those assets are remote and geographically dispersed. Organizations may not have the tools to provide a current account of their assets or may not be leveraging existing capabilities required to produce an adequate inventory. Existing asset inventories may be static, onetime, or point-in-time snapshots of auditing activities conducted previously without a way to see the current status of those assets. Adding to the challenge, asset inventories may be kept in documents or spreadsheets that may be difficult to manually maintain and update, especially considering that inventories can change frequently. Without an effective asset management solution, organizations that are unaware of any assets in their infrastructure may be unnecessarily exposed to cybersecurity risks. It is difficult to protect what cannot be seen or is not known.

1.2 Solution

This NCCoE Cybersecurity Practice Guide demonstrates how energy organizations can use commercially available technologies that are consistent with cybersecurity standards, to address the challenge of establishing, enhancing, and automating their OT asset management.

This project demonstrates an OT asset management solution that consists of the following characteristics:

- the ability to discover assets connected to a network
- the ability to identify and capture as many asset attributes as possible to baseline assets, such as manufacturer, model, operating system (OS), internet protocol (IP) addresses, media access control (MAC) addresses, protocols, patch-level information, and firmware versions, along with physical and logical locations of the assets
- continuous identification, monitoring, and alerting of newly connected devices, disconnected devices, and their connections to other devices (IP based and serial)
- the ability to determine disposition of an asset, including the level of criticality (high, medium, or low) and its relation and communication to other assets within the OT network
- the ability to alert on deviations from the expected operation of assets

Furthermore, this practice guide:

- maps security characteristics to standards, regulations, and best practices from NIST and other standards organizations
- provides a detailed architecture and capabilities that address asset management
- describes best practices and lessons learned
- provides instructions for implementers and security engineers to re-create the reference design

- is modular and uses products that are readily available and interoperable with existing energy infrastructures

1.2.1 Relevant Standards and Guidance

In developing our example implementation, we were influenced by standards and guidance from the following sources, which can also provide an organization with relevant standards and best practices:

- American National Standards Institute (ANSI)/International Society of Automation (ISA)-TR62443-2-3-2015, *Security for industrial automation and control systems Part 2-3: Patch management in the IACS environment*, 2015. https://www.isa.org/store/isa-tr62443-2-3-2015,-security-for-industrial-automation-and-control-systems-part-2-3-patch-management-in-the-iacs-environment/40228386
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*, 2013. https://www.isa.org/store/ansi/isa-62443-3-3-990303-2013-security-for-industrial-automation-and-control-systems-part-3-3-system-security-requirements-and-security-levels/116785
- ISA-62443-2-1-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.* https://www.isa.org/store/ansi/isa%E2%80%9362443-2-1-990201%E2%80%932009-security-for-industrial-automation-and-control-systems-establishing-an-industrial-automation-and-control-systems-security-program-/116731
- Center for Internet Security (CIS), Critical Security Controls V6.0. https://cisecurity.org/controls
- Information Systems Audit and Control Association (ISACA), Control Objectives for Information and Related Technology 5, https://www.isaca.org/cobit/pages/default.aspx
- NIST, Cryptographic Standards and Guidelines. https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines
- Department of Energy, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1,* February 2014. https://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf
- NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1, April 16, 2018. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11
- Internet Engineering Task Force (IETF) Request for Comments (RFC) 4254, *The Secure Shell (SSH) Connection Protocol*, January 2006. https://www.ietf.org/rfc/rfc4254.txt
- IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008. https://tools.ietf.org/html/rfc5246
- International Organization for Standardization (ISO) 55000:2014, *Asset Management—Overview, Principles and Terminology*, January 2014. https://www.iso.org/standard/55088.html

- ISO 55001:2014, *Asset Management—Management Systems—Requirements*, January 2014. https://www.iso.org/standard/55089.html
- ISO 55002:2014, *Asset Management—Management Systems—Guidelines for the Application of ISO 55001*, January 2014. https://www.iso.org/standard/55090.html
- ISO/International Electrotechnical Commission (IEC) 19770-1:2017, *Information Technology—IT Asset Management—Part 1: IT Asset Management Systems—Requirements,* December 2017. https://www.iso.org/standard/68531.html
- ISO/IEC 19770-5:2015, *Information Technology—IT Asset Management—Part 5: Overview and Vocabulary,* August 2015. https://www.iso.org/standard/68291.html
- ISO/IEC 27001:2013, *Information Technology—Security Techniques—Information Security Management Systems—Requirements*, October 2013. https://www.iso.org/standard/54534.html
- ISO/IEC 27019:2017, *Information Technology—Security Techniques—Information Security Controls for the Energy Utility Industry,* October 2017. https://www.iso.org/standard/68091.html
- NIST Special Publication (SP) 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*, July 2013. https://doi.org/10.6028/NIST.SP.800-40r3
- NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, August 2019. https://doi.org/10.6028/NIST.SP.800-52r2
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013. https://doi.org/10.6028/NIST.SP.800-53r4
- NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security,* May 2015. https://doi.org/10.6028/NIST.SP.800-82r2
- NIST SP 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, November 2016. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf
- NIST SP 1800-5 (DRAFT), *IT Asset Management*, 2014. https://nccoe.nist.gov/library/it-asset-management-nist-sp-1800-5-practice-guide
- NIST SP 1800-7 (DRAFT), *Situational Awareness for Electric Utilities*, 2017. https://nccoe.nist.gov/library/situational-awareness-electric-utilities-nist-sp-1800-7-practice-guide
- North American Electric Reliability Corporation (NERC), *Reliability Standards for the Bulk Electric Systems of North America,* last updated June 5, 2019. http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf

1.3 Benefits

This NCCoE practice guide can help your organization:

- reduce cybersecurity risk and potentially reduce the impact of safety and operational risks such as power disruption
- develop and execute a strategy that provides continuous OT asset management and monitoring
- respond faster to security alerts through automated cybersecurity event capabilities
- implement current cybersecurity standards and best practices, while maintaining the performance of energy infrastructures
- strengthen awareness of remote and geographically dispersed OT assets

Other potential benefits include:

- additional data for organizations to address business needs such as budget planning and technology updates
- improved situational awareness and strengthened cybersecurity posture

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the energy sector asset management (ESAM) solution that focuses on OT assets and does not include software inventory. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-23A: *Executive Summary*
- NIST SP 1800-23B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-23C: *How-To Guides* – instructions for building the example solution

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

Senior information technology (IT) executives, including chief information security and technology officers, will be interested in the *Executive Summary,* NIST SP 1800-23A, which describes the following topics:

- challenges that enterprises face in OT asset management
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-23B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk Assessment, provides a description of the risk analysis we performed.
- Section 3.4.4, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary,* NIST SP 1800-23A, with your leadership team members to help them understand the importance of adopting a standards-based solution to strengthen their OT asset management practices by leveraging capabilities that may already exist within their operating environment or by implementing new capabilities.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, NIST SP 1800-23C, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we integrated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of the ESAM solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.5,Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

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

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume. Acronyms used in figures can be found in Appendix A.

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

3 Approach

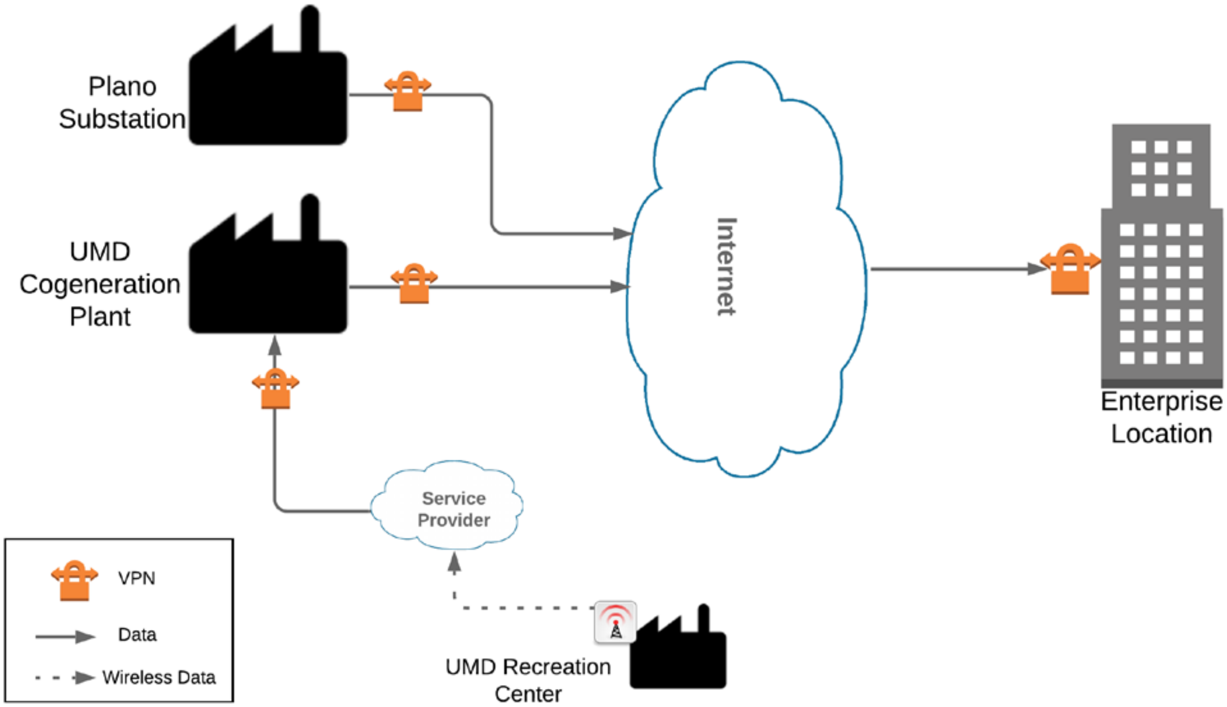
This practice guide highlights the approach the NCCoE used to develop the example implementation. The approach includes a risk assessment and analysis, logical design, example build development, testing, and security control mapping.

Based on discussions with cybersecurity practitioners in the energy sector, the NCCoE pursued the ESAM Project to illustrate the broad set of capabilities available to manage OT assets. ICS infrastructures consist of both IT and OT assets; however, this guide focuses primarily on OT devices due to their unique challenges.

The NCCoE collaborated with its Community of Interest members and participating vendors to produce an example architecture and example implementation. Vendors provided technologies that met project requirements and assisted in installing and configuring those technologies. This practice guide highlights the example architecture and example implementation, including supporting elements such as a functional test plan, security characteristic analysis, lessons learned, and future build considerations.

To reasonably replicate a live ICS environment, the project consists of three distinct geographic locations: 1) Plano, Texas; 2) College Park, Maryland; and 3) Rockville, Maryland. The Plano site is TDi Technology's lab and represents a substation. The College Park site is the University of Maryland's (UMD's) cogeneration plant. The Rockville site is the NCCoE' s energy lab and represents the enterprise location. The diagram in Figure 3-1 below visually represents the physical layout of the project.

Figure 3-1 High-Level Topology



Both the Plano substation and the UMD cogeneration plant are connected through the internet to the NCCoE energy lab as the enterprise location. Each site is connected via a multipoint, always-on virtual private network (VPN). This allows the NCCoE to aggregate data from multiple sites into a single location, emulating multisite deployments found within the energy sector. The UMD site also consists of a remote site connected via wireless technology. Each site is described in more detail in Section 4.

3.1 Audience

This guide is intended for individuals or entities responsible for cybersecurity of ICS and for those interested in understanding an example architecture demonstrating asset management capabilities for OT. It may also be of interest to anyone in industry, academia, or government who seeks general knowledge of an OT asset management solution for energy-sector organizations.

3.2 Scope

This document focuses on OT asset management, namely devices used to control, monitor, and maintain generation, transmission, and distribution of various forms of energy. These devices include PLCs, IEDs, engineering workstations, historians, and human-machine interfaces (HMIs). This document does not consider software inventories or other physical assets that may be used to support energy operations, such as buildings, trucks, and physical access control systems. The solution is designed to

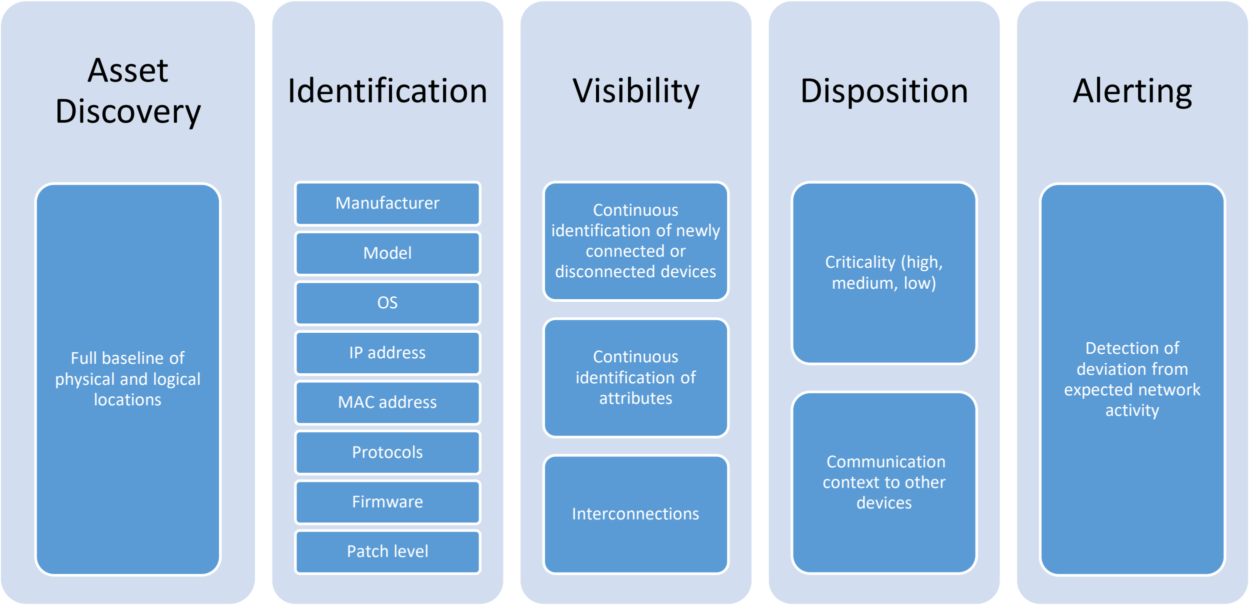
This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-23.

deliver an automated OT asset inventory that provides asset information in real or near real time and can alert personnel of any changes to the inventory. Additionally, we focus on OT asset management from a cybersecurity perspective. Although operational benefits can be obtained from implementation of one or more of the components of this guide, we propose OT asset management as a fundamental and core aspect of properly maintaining an adequate cybersecurity posture.

This project addresses the following characteristics of asset management:

- **Asset Discovery:** establishment of a full baseline of physical and logical locations of assets
- **Asset Identification:** capture of asset attributes, such as manufacturer, model, OS, IP addresses, MAC addresses, protocols, patch-level information, and firmware versions
- **Asset Visibility:** continuous identification of newly connected or disconnected devices and IP (routable and non-routable) and serial connections to other devices
- **Asset Disposition:** the level of criticality (high, medium, or low) of a particular asset, its relation to other assets within the OT network, and its communication (including serial) with other devices
- **Alerting Capabilities:** detection of a deviation from the expected operation of assets

Figure 3-2 Asset Management Characteristics


Asset Discovery
Full baseline of physical and logical locations
Identification
Manufacturer
Model
OS
IP address
MAC address
Protocols
Firmware
Patch level
Visibility
Continuous identification of newly connected or disconnected devices
Continuous identification of attributes
Interconnections
Disposition
Criticality (high, medium, low)
Communication context to other devices
Alerting
Detection of deviation from expected network activity

3.3 Assumptions

This project makes the following assumptions:

- The solution will scale to real-world operating environments.
- Some level of an asset management capability already exists within an organization.
- Although we differentiate between IT and OT asset inventories, there may be some overlap.
- All asset data sent to asset collection points has not been compromised.
- All OT assets within an organization’s infrastructure, especially those considered critical, need to be identified, tracked, and managed.
- OT networks are composed of numerous ICS devices (e.g., PLCs and IEDs) in addition to other vital components (e.g., engineering workstations, historians, and HMIs) that are typically installed on a Windows and/or Linux OS.
- NIST / NCCoE considers baseline asset monitoring an essential component of an overall comprehensive cybersecurity monitoring strategy. This guide provides guidance on the asset component of the strategy only, and is not intended to showcase a comprehensive cybersecurity monitoring capability which would likely include, but not be limited to: network and device vulnerabilities, behavioral anomaly detection capabilities, and intrusion detection.

3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* states that risk is “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence” [2]. The guide further defines risk assessment as “the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.”

The NCCoE recommends that any discussion of risk management, particularly at the enterprise-level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*—publicly-available material [3]. The Risk Management Framework guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide [4].

The basis for our assessment of the risks associated with the challenges in asset management for OT is derived from NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, Section 3. There are certain risks inherent in OT that are not found or that occur rarely in traditional IT environments, for example:

- the physical impact a cybersecurity incident could cause to an energy organization’s OT assets and to the larger energy grid

- the risk associated with non-digital control components within an OT environment and their lack of visibility within the organization

The NIST Cybersecurity Framework control mapping and related security controls found in this guide are based on these underlying risk concerns.

3.4.1 Threats

A threat is "any circumstance or event with the potential to adversely impact organizational operations" [5]. If an organization is not aware of its deployed OT assets, it is difficult to protect them and any other assets that may contain known or unknown vulnerabilities. Such lack of awareness increases the risk of exploitation of other networks, devices, and protocol-level vulnerabilities.

The Cybersecurity and Infrastructure Security Agency (CISA) ICS-Computer Emergency Readiness Team (CERT) defines cyber-threat sources to ICS as "persons who attempt unauthorized access to a control system device and/or network using a data communications pathway" [6]. Specifically, CISA ICS-CERT alongside NIST SP 800-82, *Guide to Industrial Control Systems Security* [1], identifies various malicious actors who may pose threats to ICS infrastructure [6]. These include:

- foreign intelligence services–national government organizations whose intelligence-gathering and espionage activities seek to harm U.S. interests
- criminal groups–such as organized crime groups that seek to attack for monetary gain
- hackers–regarded as the most widely publicized; however, they often possess very little tradecraft to produce large-duration attacks
- terrorists–adversaries of the U.S. who are less equipped in their cyber capabilities and therefore pose only a limited cyber threat

At the asset level, CISA ICS-CERT provides alerts and advisories when vulnerabilities for various OT assets are discovered that may pose a threat, if exploited, to ICS infrastructure [7].

The vulnerabilities are enumerated in the Common Vulnerabilities and Exposures vulnerability naming standard from the MITRE Corporation [8] and are organized according to severity by high, medium, and low, determined by the Common Vulnerability Scoring System standard from NIST. Common examples of such vulnerabilities include hard-coded credentials, unchanged default passwords, and encryption anomalies [9].

3.4.2 Vulnerabilities

CISA ICS-CERT defines a vulnerability as a defect that may allow a malicious actor to gain unauthorized access or interfere with normal operations of systems [10]. A vulnerability may exist inherently within a device or within the design, operation, and architecture of a system. This project does not address securing specific asset-based vulnerabilities at the device level. The key vulnerability addressed then in this guide is an organization not having visibility over its deployed assets.

NIST SP 800-82 categorizes ICS vulnerabilities into the following categories with examples [1]:

- Policy and Procedure–incomplete, inappropriate, or nonexistent security policy, including its documentation, implementation guides (e.g., procedures), and enforcement
- Architecture and Design–design flaws, development flaws, poor administration, and connections with other systems and networks
- Configuration and Maintenance–misconfiguration and poor maintenance
- Physical–lack of or improper access control, malfunctioning equipment
- Software Development–improper data validation, security capabilities not enabled, inadequate authentication privileges
- Communication and Network–nonexistent authentication, insecure protocols, improper firewall configuration

Knowledge of deployed assets is paramount in securing an organization's ICS infrastructure and mitigating risks associated with asset-based vulnerabilities. The knowledge of an asset's location and baselining of its behavior enable detection of anomalous behavior via network monitoring that may be the result of a successfully exploited vulnerability. The ability to reliably detect changes in asset behavior and knowing an asset's attributes are key in responding to potential cybersecurity incidents.

3.4.3 Risk

Information-system-related security risks are those risks that arise from loss of confidentiality, integrity, or availability of information or information systems and that reflect potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. For the energy sector, a primary risk concern to OT is a lack of awareness of the devices running on the infrastructure. If OT assets cannot be properly accounted for, they cannot be protected. The following are tactical risks associated with lack of an OT asset management solution:

- lack of knowledge of an existing asset, including its configuration and intended behavior
- lack of knowledge of the asset's physical and logical location
- lack of a near-real-time comprehensive asset inventory
- lack of knowledge of asset vulnerabilities and available patches
- lack of data visualization and analysis capabilities that help dispatchers and a security analyst view device security events

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-23.

3.4.4 Security Control Map

The NIST Cybersecurity Framework security Functions, Categories, and Subcategories that the reference design supports were identified through a risk analysis [11]. Table 3-1 below maps NIST SP 800-53 Rev. 4 Security and Privacy Controls [12], along with industry security references, to the NIST Cybersecurity Framework Subcategories addressed in this practice guide.

Table 3-1 Security Control Map

Informative References								
Function	Category	Subcategory	CIS CSC 2016	ISA 62443-2-1:2009	ISA 62443-3-3:2013	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	NERC CIP Standards
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	1	4.2.3.4	SR 7.8	A.8.1.1, A.8.1.2	CM-8 PM-5	CIP-002-5.1a:R1, R2 CIP-010-2:R1, R2

Informative References								
Function	**Category**	**Subcategory**	**CIS CSC 2016**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001:2013**	**NIST SP 800-53 Rev. 4**	**NERC CIP Standards**
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-2:** Threat and vulnerability information is received from information-sharing forums and sources.	4	4.2.3, 4.2.3.9, 4.2.3.12	A.6.14	A.6.1.4	SI-5, PM-15, PM-16	n/a
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-2:** Data-in-transit is protected.	13, 14	n/a	SR 3.1, SR 3.8, SR 4.1, SR 4.2	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	SC-8, SC-11, SC-12	CIP-005-5:R2 Part 2.2 CIP-011-2:R1 Part 1.2
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	2,3	n/a	SR 3.1, SR 3.3, SR 3.4, SR 3.8	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4	SC-16, SI-7	CIP-010-2:R1, R2, R3

Informative References								
Function	**Category**	**Subcategory**	**CIS CSC 2016**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001:2013**	**NIST SP 800-53 Rev. 4**	**NERC CIP Standards**
	Maintenance (PR.MA): Maintenance and repair of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools.	n/a	4.3.3.3.7	n/a	A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6	MA-2, MA-3, MA-5, MA-6	CIP-10-2:R1
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	3, 5	4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8	n/a	A.11.2.4, A.15.1.1, A.15.2.1	MA-4	CIP-010-2:R1

			Informative References					
Function	**Category**	**Subcategory**	**CIS CSC 2016**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001: 2013**	**NIST SP 800-53 Rev. 4**	**NERC CIP Standards**
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-4:** Communications and control networks are protected.	8, 12, 15	n/a	SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6	A.13.1.1, A.13.2.1, A.14.1.3	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	CIP-005-5:R1 Part 1.2
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner, and the	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is	1, 4, 6, 12, 13, 15, 16	4.4.3.3	n/a	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2	AC-4, CA-3, CM-2, SI-4	CIP-010-2:R1

Informative References								
Function	**Category**	**Subcategory**	**CIS CSC 2016**	**ISA 62443-2-1:2009**	**ISA 62443-3-3:2013**	**ISO/IEC 27001: 2013**	**NIST SP 800-53 Rev. 4**	**NERC CIP Standards**
	potential impact of events is understood.	established and managed.						
		DE.AE-3: Event data is aggregated and correlated from multiple sources and sensors.	1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16	n/a	SR 6.1	A.12.4.1, A.16.1.7	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	CIP-008-5:R1.4 CIP-010-2:R1

3.4.5 National Initiative for Cybersecurity Education Workforce Framework

This guide details the work roles needed to perform the tasks necessary to implement the cybersecurity Functions and Subcategories detailed in the reference design. The work roles are based on the National Initiative for Cybersecurity Education (NICE) Workforce Framework [13].

Table 3-2 maps the Cybersecurity Framework Categories implemented in the reference design to the NICE work roles. Note that the work roles defined may apply to more than one NIST Cybersecurity Framework Category.

For more information about NICE and other work roles, the NIST SP 800-181, *NICE Cybersecurity Workforce Framework*, is available at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf.

Table 3-2 NIST NICE Work Roles Mapped to the Cybersecurity Framework: ESAM

Work Role ID	Work Role	Work Role Description	Category	Specialty Area	Cybersecurity Framework Subcategory Mapping
OM-STS-001	Technical Support Specialist	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).	Operate and Maintain	Customer Service and Technical Support	ID.AM-1
PR-VAM-001	Vulnerability Assessment Analyst	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.	Protect and Defend	Vulnerability Assessment Management	ID.RA-2
OM-DTA-002	Information Systems	Examines data from multiple disparate sources, with the goal of providing security and privacy	Operate and Maintain	Data Administration	PR.DS-2

Work Role ID	Work Role	Work Role Description	Category	Specialty Area	Cybersecurity Framework Subcategory Mapping
	Security Developer	insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.			
PR-CDA-001	Cyber Defense Analyst	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments, to mitigate threats.	Protect and Defend	Cyber Defense Analysis	PR.DS-2
OM-DTA-001	Database Administrator	Administers databases and data management systems that allow secure storage, query, protection, and utilization of data.	Operate and Maintain	Data Administration	PR.DS-6
OM-ADM-001	System Administrator	Responsible for setting up and maintaining a system or specific components of a system (e.g., installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).	Operate and Maintain	Systems Administration	PR.MA-1
SP-TRD-001	Research & Develop-	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated.	Securely Provision	Technology R&D	PR.MA-2

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-23.

Work Role ID	Work Role	Work Role Description	Category	Specialty Area	Cybersecurity Framework Subcategory Mapping
	ment Specialist	Conducts comprehensive technology research to evaluate potential vulnerabilities in cyber space systems.			
SP-ARC-002	Security Architect	Ensures stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.	Securely Provision	Systems Architecture	PR.PT-4
SP-ARC-001	Enterprise Architect	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops IT rules and requirements that describe baseline and target architectures.	Securely Provision	Systems Architecture	DE.AE-1
CO-OPS-001	Cyber Operator	Conducts collection, processing, and geo-location of systems to exploit, locate, and track targets of interest. Performs network navigation and tactical forensic analysis and, when directed, executes on-net operations.	Collect and Operate	Cyber Operations	DE.AE-3

3.5 Technologies

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

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-23.

Table 3-3 Products and Technologies

Capability	Product	Project Role	Cybersecurity Framework Subcategories
Asset discovery and monitoring	Dragos Platform v1.5	Passive asset discovery, threat detection, and incident response for ICS networks	ID.AM-1, DE.AE-1, DE.AE-2
Data collection and inventory tool	ForeScout CounterACT v8.0.1	CounterACT appliance collects data from one location and reports back to the CounterACT Enterprise Manager on the enterprise network.	ID.AM-1, DE.AE-1, DE.AE-2
Asset identification, analysis, and baselining	FoxGuard Solutions Patch and Update Management Program v1	Patch availability reporting is an ICS security patch management report that consolidates patch sources into one source.	ID.RA-2
		Vulnerability Notification Report is curated specific to your asset list, putting critical security vulnerability data at your fingertips for your assets.	
		ICS Update Tool consumes monthly security-patch-availability reports and translates them into a dashboard of business analytics. This visualization of patch data provides near-real-time decision-making.	

Capability	Product	Project Role	Cybersecurity Framework Subcategories
Secure remote access	KORE Wireless, Inc. Cellular Connectivity with Cellular Gateway v2.0	Provide a secure bridge from remote devices via one or more long-term evolution (LTE) networks to the application server on the ICS network that gathers the data from the remote asset.	PR.DS-2, PR.MA-1
Analyzing and visualizing machine data	Splunk Enterprise v7.1.3	Provides capabilities for data collection, indexing, searching, reporting, analysis, alerting, monitoring, and visualization.	DE.AE-1, DE.AE-2
Data Collection, monitoring, and analysis	TDi Technologies, Inc. ConsoleWorks v5.2-0u1	Provides data collection and interfacing with serial conversion devices. Also provides analysis and reporting.	ID.AM-1, PR.DS-2
Anomaly detection	Tripwire Industrial Visibility v3.2.1	Passively scans the industrial control environments at two locations. Tripwire Industrial Visibility builds a baseline of assets and network traffic between those assets then alerts on anomalous traffic.	ID.AM-1, DE.AE-1, DE.AE-2

4 Architecture

The project architecture focuses on the key capabilities of asset management: asset discovery, identification, visibility, disposition, and alerting capabilities. When combined, these capabilities allow an organization to have a more robust understanding, not only of its device inventory and architecture but also of the current state of its devices and automated alerts for anomalous behavior of its assets.

This section presents a high-level architecture, a reference design, detailed topologies, and a visualization dashboard for implementing such a solution. The high-level architecture is a generic representation of the reference design. The reference design includes a broad set of capabilities available in the marketplace, to illustrate the ESAM capabilities noted above, that an organization may implement. Each topology depicts the physical architecture of the example solution. The asset management dashboard displays the network connectivity between devices and a list of known assets within the network. The NCCoE understands that an organization may not need all of the capabilities. An organization may choose to implement a subset of the capabilities, depending on its risk management decisions.

4.1 Architecture Description

4.1.1 High-Level Architecture

The ESAM solution is designed to address the Cybersecurity Framework Functions, Categories, and Subcategories described in Table 3-1 and is depicted in Figure 3-1.

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-23.

Figure 4-1 High-Level Architecture

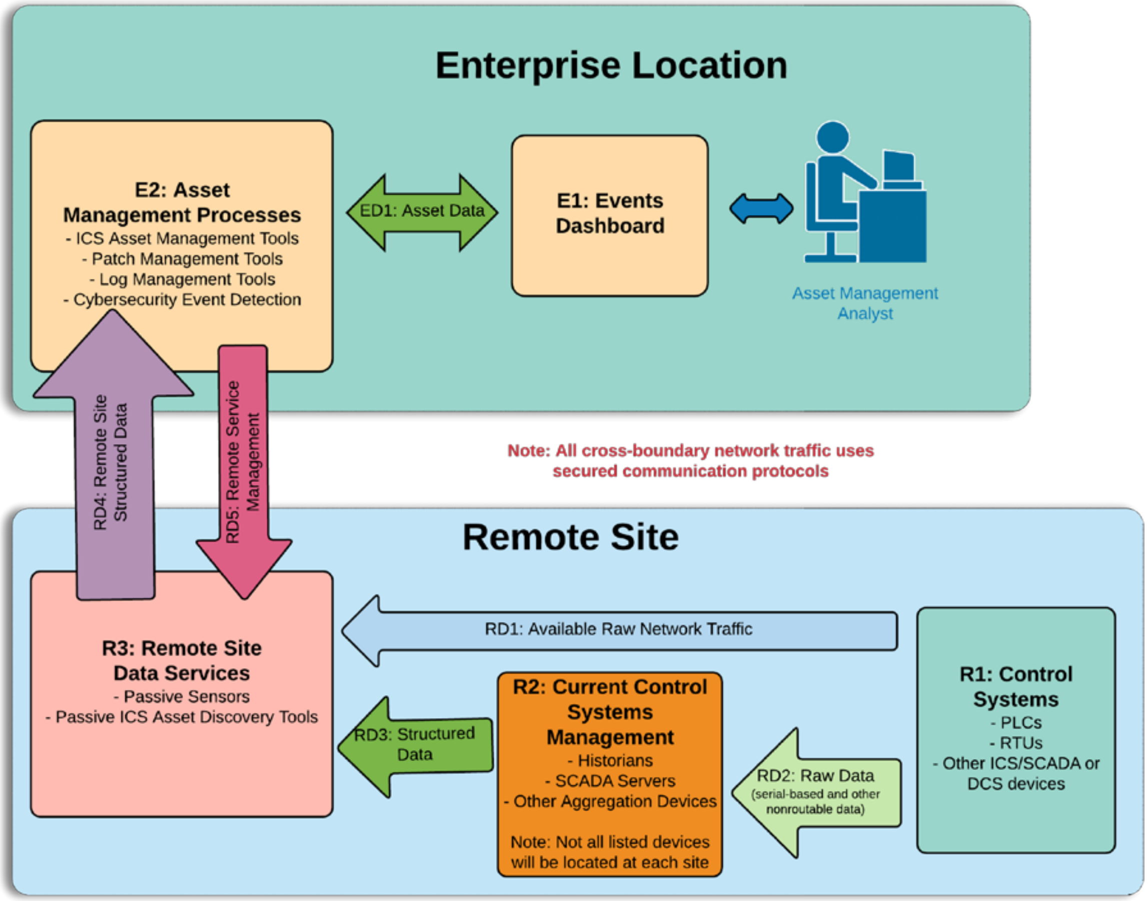

Enterprise Location
E2: Asset Management Processes
- ICS Asset Management Tools
- Patch Management Tools
- Log Management Tools
- Cybersecurity Event Detection
ED1: Asset Data
E1: Events Dashboard
Asset Management Analyst
RD4: Remote Site Structured Data
RD5: Remote Service Management
Note: All cross-boundary network traffic uses secured communication protocols
Remote Site
R3: Remote Site Data Services
- Passive Sensors
- Passive ICS Asset Discovery Tools
RD1: Available Raw Network Traffic
RD3: Structured Data
R2: Current Control Systems Management
- Historians
- SCADA Servers
- Other Aggregation Devices
Note: Not all listed devices will be located at each site
RD2: Raw Data
(serial-based and other nonroutable data)
R1: Control Systems
- PLCs
- RTUs
- Other ICS/SCADA or DCS devices

Figure 4-1 depicts the high-level architecture for monitoring ICS assets, including those located in remote sites. While one remote site is depicted, the architecture allows inclusion of multiple remote sites. This allows a repeatable and standard framework of deployment and strategy for multiple remotes sites, which can be tailored to individual site needs.

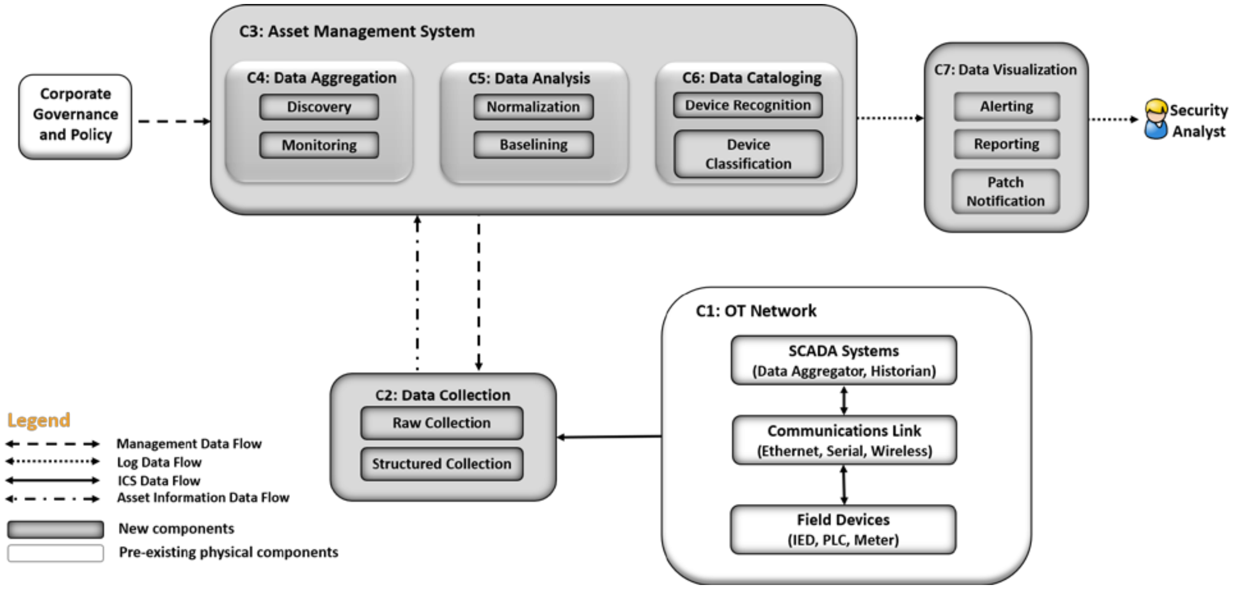
The high-level architecture (Figure 4-1) above is best described starting at the remote site control systems. Information at this level appears as raw ICS-based data (including serial communications), ICS-based network traffic (Distributed Network Protocol 3, Modbus, EtherIP, etc.), or raw networking data (Transmission Control Protocol [TCP]/User Datagram Protocol, internet control message protocol [ICMP], address resolution protocol [ARP], etc.). Serial communications are encapsulated in network protocols. All of this data is collected and stored by the remote site data servers (R3) object. These sensors are collecting ICS network traffic and raw IP networking data from the control systems (R1) and current control systems management (R2). Data collected by the remote site data servers (R3) is sent through a VPN tunnel to listening servers in the enterprise location. Once data arrives from the remote site at the enterprise-data-collection server, it is ingested into the assets management processes (E2). These tools aggregate the remote site structured data (RD4) from multiple sites, to build a holistic picture of the health and setup of the network. Next, both events and asset data from the asset management processes (E2) tools are sent directly to the events dashboard (E1). In the events dashboard (E1), events are displayed in an easily digestible format for an analyst.

In the event of needed configuration of remote site data servers (R3), remote service management connections can be established between the asset management processes (E2) and the remote site data servers (R3). This traffic is routed through the aforementioned VPN tunnel and is terminated inside the remote site data servers (R3). This allows configuration solely in the remote site data servers (R3), utilizing the established VPN tunnel for security, without allowing access to either the current control systems management (R2) or control systems (R3) devices.

4.1.2 Reference Architecture

The reference architecture shown in Figure 4-2 depicts the detailed ESAM design, including relationships among the included capabilities.

Figure 4-2 Reference Architecture



As indicated by the legend, different lines represent different types of data flowing into the various components. ICS data is depicted with solid lines. Management data flow is depicted with the dashed line. Asset information is depicted with a dot-dash line. Log data is depicted with a dotted line. Each of the clear shapes represents a preexisting or optional component. The OT network consists of devices composed of ICS-based data, ICS network traffic, or raw networking data. The example implementation includes the ICS devices in both the UMD cogeneration plant as well as TDi's lab in Plano, Texas, in the Reference Design OT Network categorization group.

Another component that utilizes the ESAM solution is corporate governance and policy. Corporate governance and policy may guide different aspects of the ESAM solution, such as how long records will be maintained, how to classify devices, and how often reports are run. Each organization's governance and policy will be determined by organizational risk tolerance and management decisions.

The components of the ESAM reference design, Figure 4-2, come together to form the asset management system. Each capability is described below:

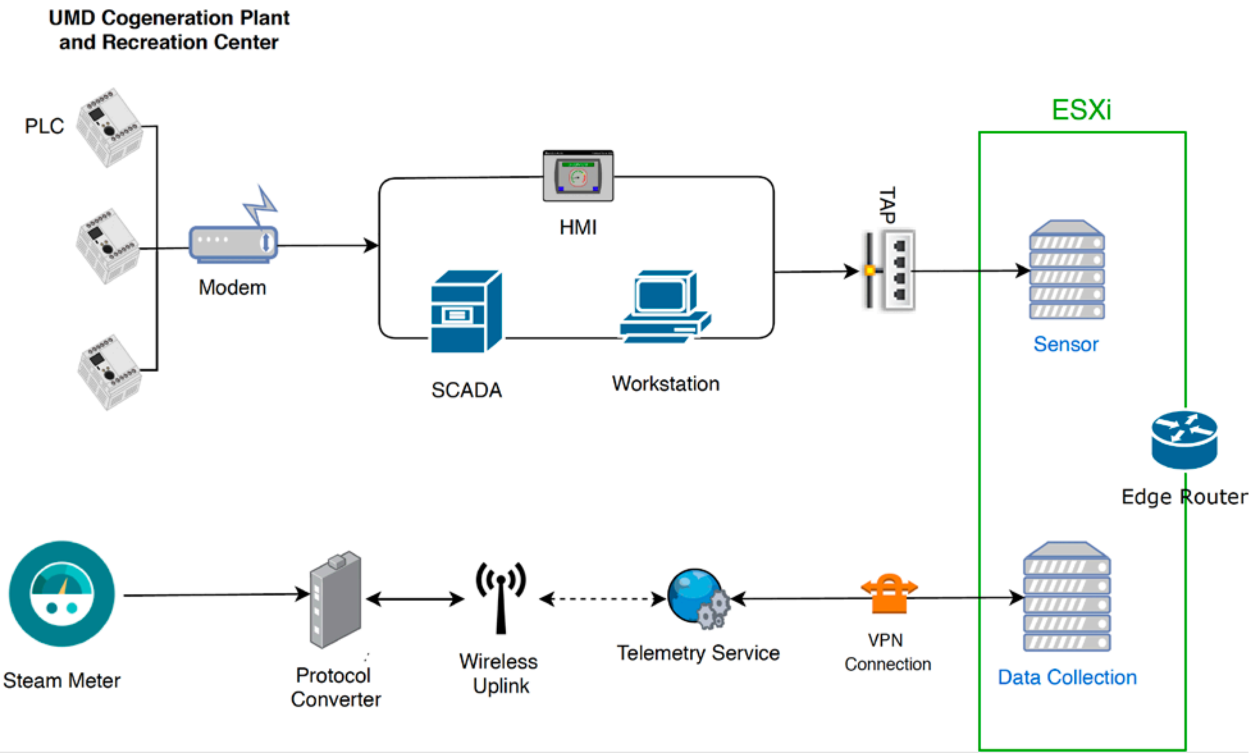
- The data collection capability captures the data from the in-place OT network. Data can be collected in raw packet capture form as well as any structured form that may come from tools or devices within the OT network. This capability can be configured through normal remote management channels, to ensure the most precise and policy-informed data ingestion needed for the organization.
- The data aggregation component ingests data from the data collection capability and utilizes both the discovery capability and monitoring capability. The monitoring capability tracks network activity collected from the OT network. After a training period, the discovery capability identifies new devices when new IP addresses and MAC addresses are communicating on the network.
- The data analysis capability utilizes both a normalization capability to bring in traffic from multiple sites into a single picture and a baselining capability to establish an informed standard of how an asset's network traffic should behave under normal operations.
- The device cataloging capability simultaneously uses information from the data collection component. The device recognition capability identifies different types of devices within the system. Devices are identified by MAC address to determine the manufacturer or by deep-packet inspection to determine the model, serial number, or both of a device if the raw ICS protocol contains such information. Figure 4-4 below depicts the option for determining the serial and model number of a device, when scanning is technically feasible. The organization should verify compliance with relevant regulations before deploying this aspect of the solution. Next, the device classification capability can determine the level of criticality for devices, both automatically as well as manually if requested.
- The data visualization capability displays data from components of the asset management system. Here, the alerting capability notifies analysts of incidents, including deviations to normal behaviors. This component also includes the reporting capability to generate timely reports needed in operations of the organization. One key feature of the reporting capability is the ability to report when a cybersecurity patch is available.

4.2 Example Solution

Below are topologies for three separate sites utilized for this project along with their asset management dashboard displays. The project employs network test access points (TAPs) that fail open, allowing network traffic to continue passing in the event of device failure. There are other examples of connectivity decisions used, including the use of Switched Port Analyzer (SPAN) ports, that are utilized specifically to facilitate the capture of data for the project. This approach represents one method to collect data.

4.2.1 UMD Site Topology

Figure 4-3 UMD In-Depth Topology



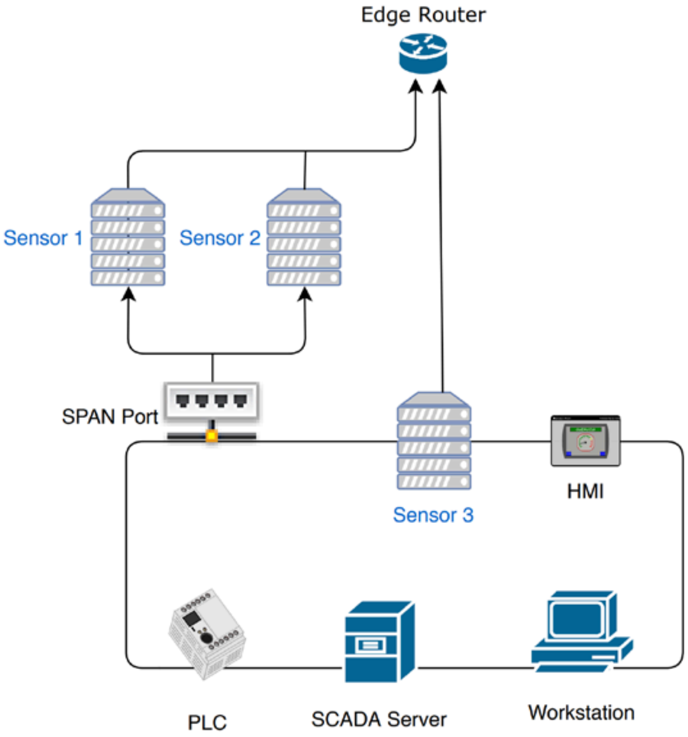
UMD's cogeneration plant was utilized as one of the remote sites for the project. At the site, the control system network consists of PLCs, networking equipment, operator workstations, HMIs, and Supervisory Control and Data Acquisition (SCADA) servers. The control system network is fitted with network TAPs to collect network traffic from the ICS network. This traffic feeds into a port on the ESXi server that is mapped to a virtual SPAN switch. Each sensor monitors traffic on the SPAN switch. The sensor collects the raw data, processes network packets, performs deep-packet inspection, and forwards structured data through the edge router to an asset management server, as shown above in Figure 4-3.

The UMD site topology also consists of a steam-meter asset in the solution. The steam meter utilizes highway addressable remote transducer (HART) communication protocol and is in a building separate from the cogeneration plant. The steam meter is wired to a protocol converter that converts HART communications to Ethernet. The wireless uplink is a cellular connection device providing wireless connectivity to the telemetry service provider. A VPN connection links the data collection server to the telemetry service provider, which allows data to be read from the steam meter.

Following collection of data from both the control system network and the steam meter to the VMware ESXi servers, the data is then sent through a VPN tunnel out of the edge router to the enterprise location. A description of the enterprise location is found in Section 4.2.3.

4.2.2 Plano Site Topology

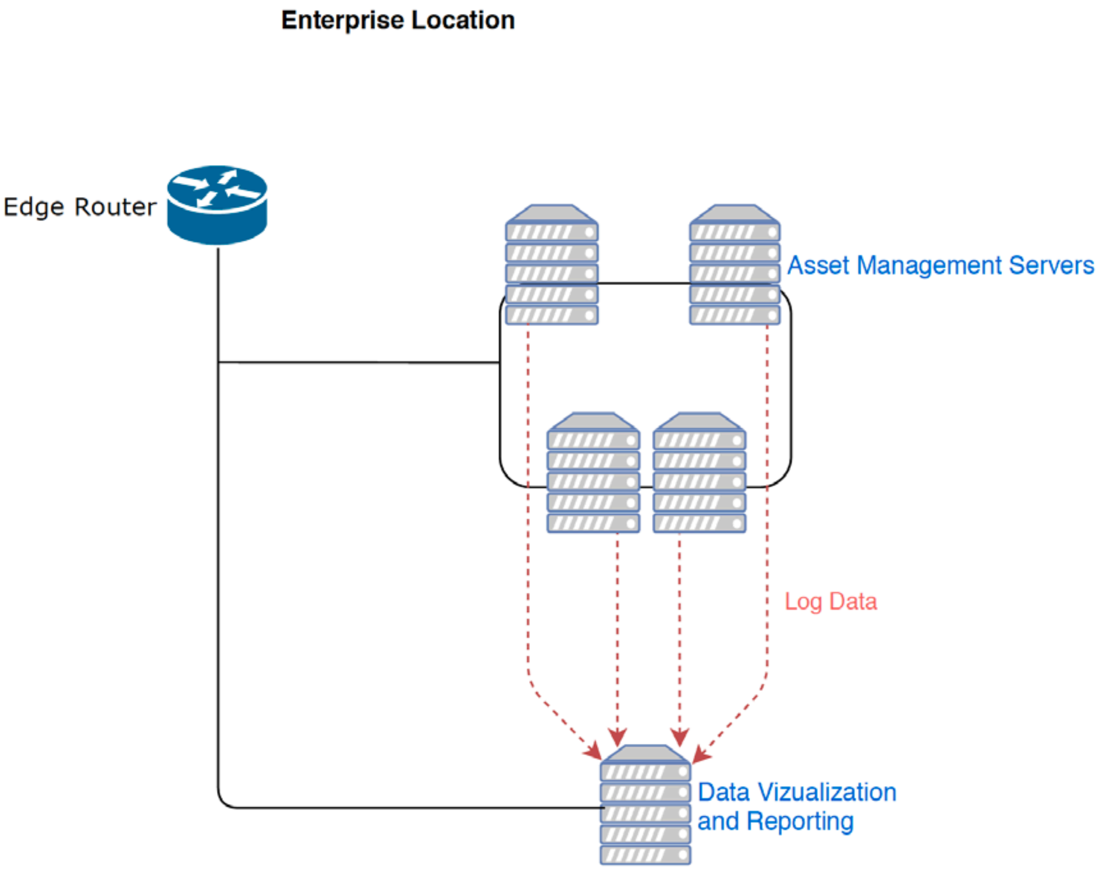
Figure 4-4 Plano In-Depth Topology



The lab in Plano, Texas, depicted in Figure 4-4, represents a second site and is set up to collect information from a variety of devices communicating on a network. The Plano site consist of PLCs, HMIs, SCADA servers, and workstations. Sensor 1 and Sensor 2 passively monitor devices via a SPAN port. Both sensors are collecting data. Sensor 3 has a network interface located on the control network, to demonstrate the ability to actively scan devices if desired. Actively scanning devices requires scripts to interrogate devices by using a method supported by the device. Methods may include using login credentials or combinations of commands to retrieve data from the device. Typically, similar devices from the same manufacturer can utilize similar scripts. Otherwise, most device types require unique scripts. Most devices can be scanned or polled to retrieve the model number, serial number, and more. All three sensors transfer their data, via the edge router, through a VPN to the enterprise location.

4.2.3 Enterprise Location Topology

Figure 4-5 Enterprise In-Depth Topology



The enterprise location in the NCCoE Lab (Rockville, Maryland), depicted in Figure 4-5, represents a central operations center for an organization. Data from both the Plano and UMD sites is sent to the enterprise location, for processing through the asset management servers.

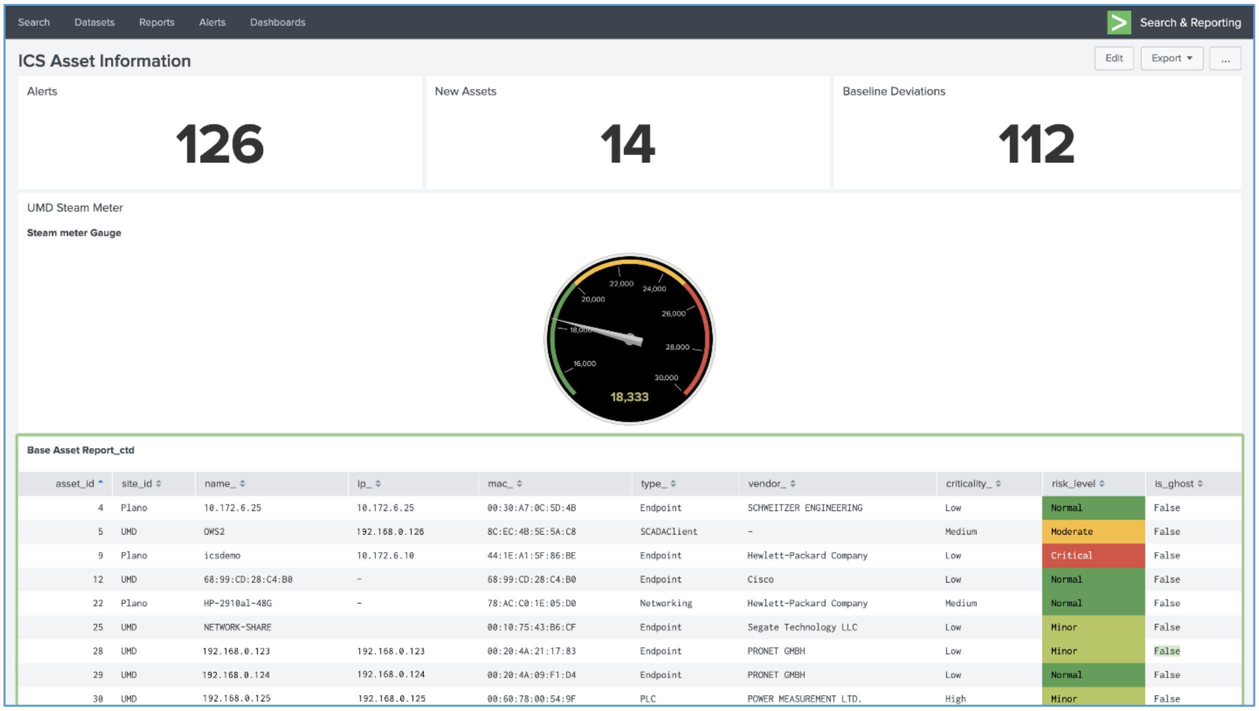
The asset management servers aggregate the data, analyze the data, and catalog the details about the assets currently on the network, incorporating both remote sites. Portions of this data are logged and forwarded to the data visualization and reporting server. First, alerts on new baselines and baseline deviations are forwarded via syslog. Alerts on asset changes, including new assets, changes in IP and

MAC addresses, and offline assets, are forwarded via syslog along with identified threats to those assets. Last, a comma-separated value (CSV) asset report is automatically forwarded on a regular basis to maintain an updated and near-real-time asset inventory.

4.2.4 Asset Management Dashboard

Note: IP addresses shown in the figures below have been sanitized.

Figure 4-6 Asset Dashboard: Asset Characteristics



ICS Asset Information

Alerts 126

New Assets 14

Baseline Deviations 112

UMD Steam Meter

Steam meter Gauge

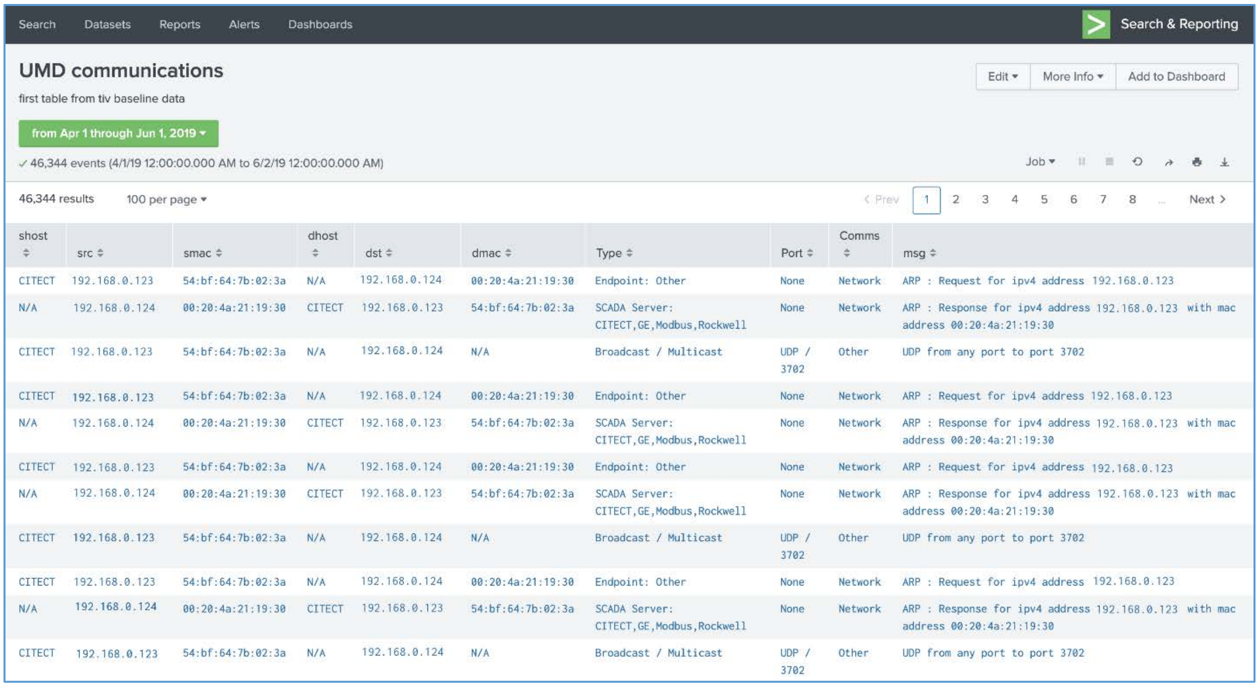
18,333

Base Asset Report_ctd

asset_id	site_id	name_	ip_	mac_	type_	vendor_	criticality_	risk_level	is_ghost
4	Plano	10.172.6.25	10.172.6.25	00:30:A7:0C:5D:4B	Endpoint	SCHWEITZER ENGINEERING	Low	Normal	False
5	UMD	OWS2	192.168.0.126	8C:EC:4B:5E:5A:C8	SCADAClient	-	Medium	Moderate	False
9	Plano	icsdemo	10.172.6.10	44:1E:A1:5F:86:BE	Endpoint	Hewlett-Packard Company	Low	Critical	False
12	UMD	68:99:CD:28:C4:B0	-	68:99:CD:28:C4:B0	Endpoint	Cisco	Low	Normal	False
22	Plano	HP-2910al-48G	-	78:AC:C0:1E:05:D0	Networking	Hewlett-Packard Company	Medium	Normal	False
25	UMD	NETWORK-SHARE		00:10:75:43:B6:CF	Endpoint	Segate Technology LLC	Low	Minor	False
28	UMD	192.168.0.123	192.168.0.123	00:20:4A:21:17:83	Endpoint	PRONET GMBH	Low	Minor	False
29	UMD	192.168.0.124	192.168.0.124	00:20:4A:09:F1:D4	Endpoint	PRONET GMBH	Low	Normal	False
30	UMD	192.168.0.125	192.168.0.125	00:60:78:00:54:9F	PLC	POWER MEASUREMENT LTD.	High	Minor	False

Figure 4-6 showcases how the asset management dashboard displays a list of known assets within the network. At the top of the dashboard, the total amount of alerts, number of new assets, and number of baseline deviations detected from both the Plano and UMD locations are listed. The gauge displays the meter reading from the Yokogawa steam meter at UMD. Information collected on each asset (including IP address, MAC address, asset type, criticality, and risk level) is displayed in the table.

Figure 4-7 Asset Dashboard: Asset Communications



UMD communications

first table from tiv baseline data

from Apr 1 through Jun 1, 2019 ▾

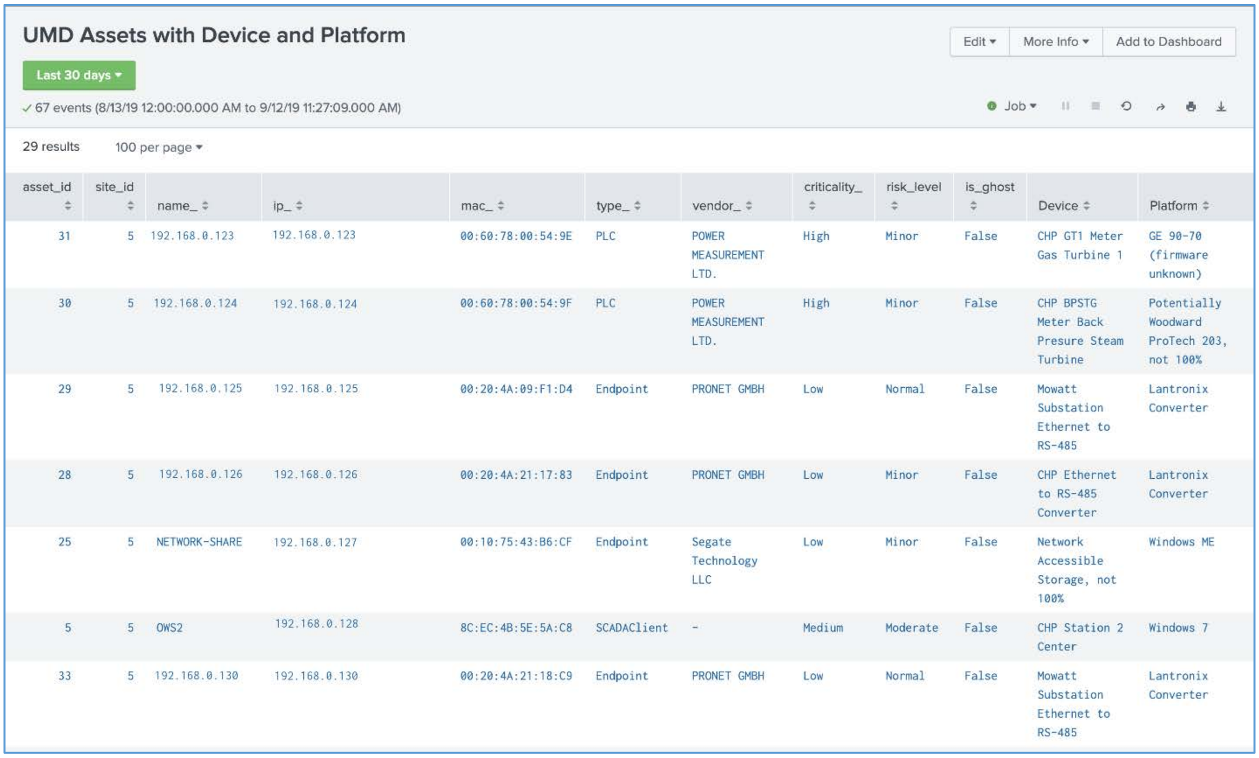
✓ 46,344 events (4/1/19 12:00:00.000 AM to 6/2/19 12:00:00.000 AM)

46,344 results   100 per page ▾

shost	src	smac	dhost	dst	dmac	Type	Port	Comms	msg
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	00:20:4a:21:19:30	Endpoint: Other	None	Network	ARP : Request for ipv4 address 192.168.0.123
N/A	192.168.0.124	00:20:4a:21:19:30	CITECT	192.168.0.123	54:bf:64:7b:02:3a	SCADA Server: CITECT,GE,Modbus,Rockwell	None	Network	ARP : Response for ipv4 address 192.168.0.123 with mac address 00:20:4a:21:19:30
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	N/A	Broadcast / Multicast	UDP / 3702	Other	UDP from any port to port 3702
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	00:20:4a:21:19:30	Endpoint: Other	None	Network	ARP : Request for ipv4 address 192.168.0.123
N/A	192.168.0.124	00:20:4a:21:19:30	CITECT	192.168.0.123	54:bf:64:7b:02:3a	SCADA Server: CITECT,GE,Modbus,Rockwell	None	Network	ARP : Response for ipv4 address 192.168.0.123 with mac address 00:20:4a:21:19:30
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	00:20:4a:21:19:30	Endpoint: Other	None	Network	ARP : Request for ipv4 address 192.168.0.123
N/A	192.168.0.124	00:20:4a:21:19:30	CITECT	192.168.0.123	54:bf:64:7b:02:3a	SCADA Server: CITECT,GE,Modbus,Rockwell	None	Network	ARP : Response for ipv4 address 192.168.0.123 with mac address 00:20:4a:21:19:30
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	N/A	Broadcast / Multicast	UDP / 3702	Other	UDP from any port to port 3702
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	00:20:4a:21:19:30	Endpoint: Other	None	Network	ARP : Request for ipv4 address 192.168.0.123
N/A	192.168.0.124	00:20:4a:21:19:30	CITECT	192.168.0.123	54:bf:64:7b:02:3a	SCADA Server: CITECT,GE,Modbus,Rockwell	None	Network	ARP : Response for ipv4 address 192.168.0.123 with mac address 00:20:4a:21:19:30
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	N/A	Broadcast / Multicast	UDP / 3702	Other	UDP from any port to port 3702

Figure 4-7 showcases the asset management dashboard visualization of network connectivity among devices. The visualization shows the interconnection among known assets, listing types of communications and messages.

Figure 4-8 Asset Dashboard: Asset Details, UMD



UMD Assets with Device and Platform

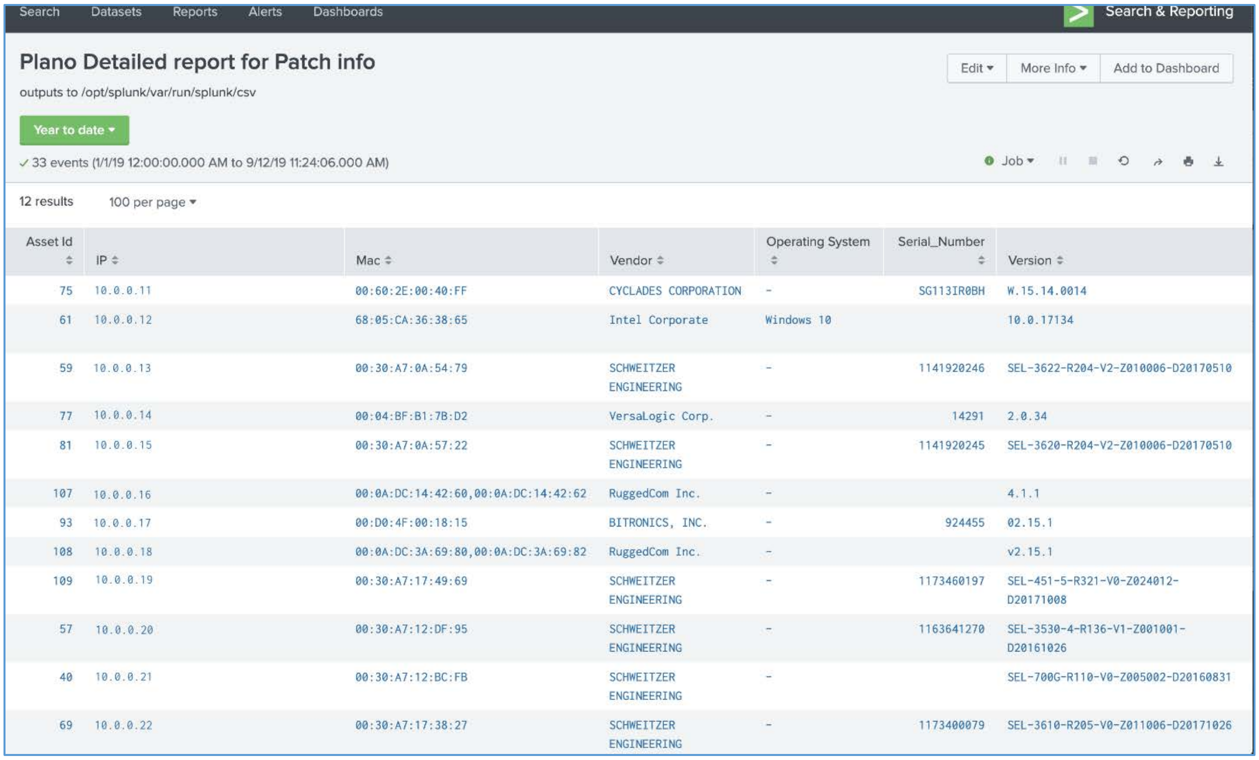
✓ 67 events (8/13/19 12:00:00.000 AM to 9/12/19 11:27:09.000 AM)

29 results 100 per page ▾

asset_id	site_id	name_	ip_	mac_	type_	vendor_	criticality_	risk_level	is_ghost	Device	Platform
31	5	192.168.0.123	192.168.0.123	00:60:78:00:54:9E	PLC	POWER MEASUREMENT LTD.	High	Minor	False	CHP GT1 Meter Gas Turbine 1	GE 90-70 (firmware unknown)
30	5	192.168.0.124	192.168.0.124	00:60:78:00:54:9F	PLC	POWER MEASUREMENT LTD.	High	Minor	False	CHP BPSTG Meter Back Presure Steam Turbine	Potentially Woodward ProTech 203, not 100%
29	5	192.168.0.125	192.168.0.125	00:20:4A:09:F1:D4	Endpoint	PRONET GMBH	Low	Normal	False	Mowatt Substation Ethernet to RS-485	Lantronix Converter
28	5	192.168.0.126	192.168.0.126	00:20:4A:21:17:83	Endpoint	PRONET GMBH	Low	Minor	False	CHP Ethernet to RS-485 Converter	Lantronix Converter
25	5	NETWORK-SHARE	192.168.0.127	00:10:75:43:B6:CF	Endpoint	Segate Technology LLC	Low	Minor	False	Network Accessible Storage, not 100%	Windows ME
5	5	OWS2	192.168.0.128	8C:EC:4B:5E:5A:C8	SCADAClient	-	Medium	Moderate	False	CHP Station 2 Center	Windows 7
33	5	192.168.0.130	192.168.0.130	00:20:4A:21:18:C9	Endpoint	PRONET GMBH	Low	Normal	False	Mowatt Substation Ethernet to RS-485	Lantronix Converter

Figure 4-8 showcases more detailed information about assets at the UMD location. The asset information is supplemented with known data about the devices.

Figure 4-9 Asset Dashboard: Asset Details, Plano



Plano Detailed report for Patch info

outputs to /opt/splunk/var/run/splunk/csv

✓ 33 events (1/1/19 12:00:00.000 AM to 9/12/19 11:24:06.000 AM)

12 results

Asset Id	IP	Mac	Vendor	Operating System	Serial_Number	Version
75	10.0.0.11	00:60:2E:00:40:FF	CYCLADES CORPORATION	-	SG113IR0BH	W.15.14.0014
61	10.0.0.12	68:05:CA:36:38:65	Intel Corporate	Windows 10		10.0.17134
59	10.0.0.13	00:30:A7:0A:54:79	SCHWEITZER ENGINEERING	-	1141920246	SEL-3622-R204-V2-Z010006-D20170510
77	10.0.0.14	00:04:BF:B1:7B:D2	VersaLogic Corp.	-	14291	2.0.34
81	10.0.0.15	00:30:A7:0A:57:22	SCHWEITZER ENGINEERING	-	1141920245	SEL-3620-R204-V2-Z010006-D20170510
107	10.0.0.16	00:0A:DC:14:42:60,00:0A:DC:14:42:62	RuggedCom Inc.	-		4.1.1
93	10.0.0.17	00:D0:4F:00:18:15	BITRONICS, INC.	-	924455	02.15.1
108	10.0.0.18	00:0A:DC:3A:69:80,00:0A:DC:3A:69:82	RuggedCom Inc.	-		v2.15.1
109	10.0.0.19	00:30:A7:17:49:69	SCHWEITZER ENGINEERING	-	1173460197	SEL-451-5-R321-V0-Z024012-D20171008
57	10.0.0.20	00:30:A7:12:DF:95	SCHWEITZER ENGINEERING	-	1163641270	SEL-3530-4-R136-V1-Z001001-D20161026
40	10.0.0.21	00:30:A7:12:BC:FB	SCHWEITZER ENGINEERING	-		SEL-700G-R110-V0-Z005002-D20160831
69	10.0.0.22	00:30:A7:17:38:27	SCHWEITZER ENGINEERING	-	1173400079	SEL-3610-R205-V0-Z011006-D20171026

Figure 4-9 showcases more detailed information about assets at the Plano location. The asset information is supplemented via automated scripts and manual entry. This report is normalized and then analyzed for patch notifications.

5 Functional Test Plan

5.1 Test Cases

The below test cases demonstrate integration of capabilities for use in the project. For reference, components of Figure 4-1 High-Level Architecture and Figure 4-2 Reference Architecture are included with their corresponding identifier tags in parenthesis.

5.1.1 ESAM-1: New Device Attached

Description	▪ Device attached to the network that has not appeared previously. ▪ ESAM solution will identify and alert on the new device.

Procedure	▪ Connect laptop to UMD-based Remote Site Data Server (R3) network. ▪ Request Dynamic Host Configuration Protocol for device, and generate minimal network traffic. ▪ Monitor Events Dashboard (E1) for identification of new device.
Architectural Requirements	▪ Raw network traffic appears on network at remote site. ▪ New device generates known network traffic with new connection (ARP/Reverse Address Resolution Protocol [RARP]), High-bandwidth Digital Content Protection, TCP connections, etc.). ▪ Network traffic is captured by sensors at Remote Site Data Servers (R3). ▪ Servers pass alerted data to enterprise location Asset Management Processes (E2). ▪ Alerts are aggregated and displayed to user in the Events Dashboard (E1).
Capabilities Requirements	▪ Network data collection via TAPs and SPAN ports on network device. ▪ Routing of network data through Asset Management (C3) sensors. ▪ Data Collection (C2) utilizing discovery and normalization processes for remote site asset information data flow. ▪ Alerting and analytics based on asset information data flow structured by the data collection capability presented to the analyst.
Expected Results	Events Dashboard (E1) will notify analyst via alerts for new devices.
Actual Results	▪ New device is created on network. ▪ Baseline monitoring system recognizes new device on network. ▪ Alert is created on Events Dashboard (E1).
Overall Result	PASS

5.1.2 ESAM-2: Vulnerability Notification

Description	▪ New vulnerability is released, affecting devices within the Control Systems (R1). ▪ ESAM solution can recognize affected devices and alert analysts to: • potential vulnerable devices • current status of devices • any potential patching for devices
Procedure	▪ Utilizing established asset list contained within the Asset Management Process (E2), create sanitized device list. ▪ Import device list to the Patch Management Tools inside the Asset Management Process (E2) for structuring. ▪ Submit structured device list to the Patch Management service. ▪ Ingest returned Patch Management report to Events Dashboard (E1) for alerting a reporting to analyst.
Architectural Requirements	▪ Assets cataloged within the Asset Management Process (E2), including vendor, device type, firmware version, and other pertinent information. ▪ Deliver device list with above information to the Patch Management tools. ▪ Deliver structured device list to the Patch Management service. ▪ Ingest report from the Patch Management service to Events Dashboard (E1).
Capabilities Requirements	▪ Data Cataloging (C6) components track asset-specific information. ▪ Vulnerability reports are compared with data included in submitted structured reports based on Data Cataloging (C6) information.
Expected Results	Analyst will receive reported information in Events Dashboard and will be able to identify potentially vulnerable devices.

Actual Results	▪ Device list is created and normalized. ▪ List is delivered to vendor for analysis. ▪ Vendor-delivered results added to dashboard. ▪ Events Dashboard notifies analyst of potentially vulnerable devices.
Overall Result	PASS

5.1.3 ESAM-3: Device Goes Offline

Description	▪ Device previously attached to the network no longer appears on the network. ▪ ESAM solution will identify and alert on the loss of device.
Procedure	▪ Option 1: • Determine control system device on Plano lab network that we can disconnect for test purposes. • Disconnect device from network. • Monitor Events Dashboard (E1) for changes and alerts. ▪ Option 2: • Determine which network TAP to disconnect from UMD network to the Remote Site Data Server (R3) network. • Disconnect selected TAP from network. • Monitor Events Dashboard (E1) for changes and alerts.
Architectural Requirements	▪ Established baselines generated from network and control system monitoring determine normalized system behavior. ▪ Lack of communication from a device triggers an anomaly in the Asset Management Process (E2). ▪ Events Dashboard (E1) is notified of anomalous activity and notifies analyst via an alert.
Capabilities Requirements	▪ Network and Serial TAPs capture data from OT Network (C1).

	- Asset Management System (C3) sensors monitor data to feed Data Collection (C2) capability. - Security incident and event management (SIEM) utilizes alerts from anomalous activity being transferred from data collection capabilities and presents them to the analyst.
Expected Results	Events Dashboard (E1) will notify analyst via alerts for loss of connection to device(s).
Actual Results	- Device is taken offline on control network. - Baseline monitoring system recognizes device is no longer online. - Alert is created on Events Dashboard.
Overall Result	PASS

5.1.4 ESAM-4: Anomalous Device Communication

Description	- Device begins communicating in ways that are not established in known baselines. - ESAM solution alerts to newly formed traffic patterns or device behaviors that do not correlate to determined device interaction baselines.
Procedure	- Utilizing devices within Plano network, begin communication with a device outside the established baseline. - Monitor Events Dashboard (E1) for newly created alerts signifying the departure from established baseline traffic and activity.
Architectural Requirements	- Established baselines generated from network and control system monitoring determine normalized system behavior. - Recognition of network anomaly and non-normal ICS activity (function codes, configuration changes, timing of commands, etc.) generate alerts in the Asset Management Processes (E2). - The Events Dashboard (E1) is notified of anomalous activity and notifies analyst via an alert.
Capabilities Requirements	- Network data collection via TAPs and SPAN ports on network device.

	▪ Routing of network data through Asset Management (C3) sensors. ▪ Data Collection (C2) utilizing discovery and normalization processes for remote site asset information data flow. ▪ Alerting and analytics based on asset information data flow structured by the data collection capability presented to the analyst.
Expected Results	Events Dashboard (E1) will notify analyst via alerts for anomalous device activity.
Actual Results	▪ Two devices start communicating in a way unseen before. ▪ Monitoring picks up new device communications, creates an alert. ▪ Events Dashboard delivers alert to analyst.
Overall Result	PASS

5.1.5 ESAM-5: Remote Devices with Cellular Connectivity

Description	▪ Devices located in areas without access to Ethernet-based networking for connection to outside internet. ▪ Utilizing cellular networks, these devices gain connectivity through specialized cellular modems not requiring a physical networking infrastructure.
Procedure	▪ Selected location will not be connected to main build network via normal Ethernet-based connections. ▪ Utilizing cellular-based networking, devices will connect to a VPN that has an upstream gateway connected through a cellular modem. ▪ These devices will be ingested into the build at the UMD Remote Site Data Servers (R3) then further cataloged through standard channels into the Events Dashboard (E1).
Architectural Requirements	▪ Cellular-based modem inside a subset of the Remote Site Data Servers (R3) that can be used to capture both Raw Network Traffic (RD1) and Structured Data (RD3).

	▪ VPN connectivity through cellular-based modem to a VPN concentrator, delivering data to the on-site Remote Site Data Servers (R3). ▪ The previous test cases apply once data from remote sites reach Remote Site Data Servers (R3).
Capabilities Requirements	▪ Communication links over cellular connections for the TAP capabilities. ▪ Routing of network data through Asset Management System (C3) sensors. ▪ Data Collection (C2) utilizing discovery and normalization processes for remote site asset information data flow. ▪ Alerting and analytics based on asset information data flow structured by the data collection capability presented to the analyst.
Expected Results	Devices in cellular-based remote sites will also show in the Events Dashboard (E1).
Actual Results	▪ Devices in location devoid of direct internet connection are connected to cellular-based modem. ▪ Cellular modem carries device communications to Asset Management servers. ▪ Device monitoring appears in Events Dashboard.
Overall Result	PASS

6 Security Characteristic Analysis

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of demonstrating asset management for OT. A key aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics it was intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment, by consulting the specific sections of each standard cited in reference to a Subcategory [14]. The cited sections provide validation points that the example solution would be expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

6.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

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

6.2 Analysis of the Reference Design's Support for Cybersecurity Framework Subcategories

This section analyzes the example implementation in terms of the specific Subcategories of the Cybersecurity Framework that they support. This enables an understanding of how the example implementation achieved the goals of the design when compared against a standardized framework. This section identifies the security benefits provided by each component of the example implementation and how those components support specific cybersecurity activities, as specified in terms of Cybersecurity Framework Subcategories.

6.2.1 ID.AM-1: Physical Devices and Systems Within the Organization Are Inventoried

The ESAM reference design employs multiple applications that keep inventory of devices. Using passive analysis of network communications as well as device polling, the design captures relevant data about each asset within the scope of the build, to give an asset owner insight into what devices are deployed.

The reference design notifies on device installation, updates, and removals, helping maintain an up-to-date, complete, accurate, and readily available inventory of system components. These processes are automated, allowing an organization to have a central repository for inventory of assets as well as for specifying roles played by those assets.

Some devices may prove difficult to inventory. If a device utilizes communications not initially monitored by the ESAM reference design, the device will not be captured in the inventory. The ESAM reference design employs an optional active scanning process that can resolve this situation.

6.2.2 ID.RA-2: Threat and Vulnerability Information Is Received from Information-Sharing Forums and Sources

The ESAM reference design implements a patch and vulnerability intelligence solution through vendor-provided reporting. Utilizing asset lists described above, patch and vulnerability information is provided by the vendor product, to relay system security alerts and advisories to analysts.

The reference design allows an organization to be aware of potential vulnerabilities that may be applicable in the network and to the organization's assets. The design informs an organization whether assets within its inventory have updates available, if any assets have vulnerabilities, and the criticality of those patches or vulnerabilities. This information is broken out into a per-device format, helping form a more informed decision on updates.

6.2.3 PR.DS-2: Data in Transit Is Protected

The ESAM reference design has multiple remote connections stemming from multiple remote sites. Data is constantly being transmitted across these connections, so protection of these connections is vital. The reference design utilizes VPN connections for all connections going out of an edge-network device.

The VPN connecting the three physically remote sites—namely the enterprise site; UMD; and Plano, Texas—utilizes an always-on, multipoint VPN connection. This connection is using TLS 1.2 and certificate authentication to ensure maximum security as well as maximum reliability.

6.2.4 PR.MA-1: Maintenance and Repair of Organizational Assets Are Performed and Logged in a Timely Manner with Approved and Controlled Tools

The ESAM reference design does not specifically track maintenance scheduling or approvals; however, predictive and preventive maintenance is supported by elements contained in the design. Patch and vulnerability information provided by vendors, combined with information from other sources, can be used by the organization to make informed cybersecurity-maintenance decisions.

This information supports any process that builds maintenance scheduling, allowing an organization to determine what assets should be included in preventive or predictive maintenance times. Although mainly software focused, asset information may include model numbers for devices, allowing an organization to locate and replace specific devices if needed.

6.2.5 PR.MA-2: Remote Maintenance of Organizational Assets Is Approved, Logged, and Performed in a Manner that Prevents Unauthorized Access

The ESAM reference design utilizes connections within the project to allow authenticated remote access to a system. This authentication is predicated on access to the enterprise network, forcing a potential user to first gain access to the asset management network before being able to remotely manage devices.

These connections are then wrapped within the established VPN tunnel, protecting systems from replay attacks or other attacks that require open, repeatable authentication techniques to gain access to a system. This allows a more secure remote management path for devices when manual configuration is required.

6.2.6 PR.PT-4: Communications and Control Networks Are Protected

The ESAM reference design is designed to protect critical devices located within the OT network. For the architecture, any connection pulling data from the control networks utilizes a one-way data connection (currently in the form of a SPAN port or a network TAP) to ensure no externally routable connectivity.

The active scanning device listed within the architecture in Section 4.2.2 is a selective aspect of the design. This would require a two-way connection with the OT network and should be implemented with due discretion. Each organization should verify compliance with the appropriate cybersecurity policies and relevant regulations before implementing this aspect of the solution.

6.2.7 DE.AE-1: A Baseline of Network Operations and Expected Data Flows for Users and Systems Is Established and Managed

The ESAM reference design utilizes passive and active scanning tools to scan the industrial control environments at the two remote locations. These tools build a baseline of assets and network traffic between those assets using machine learning, alerting to any anomalous behavior.

6.2.8 DE.AE-2: Detected Events Are Analyzed to Understand Attack Targets and Methods

The ESAM reference design utilizes discovery and monitoring tools to detect malicious activity from an established baseline of network activity. Any deviation from established baselines will notify organizational analysts to activity not recognized as normal behavior. The analyst will be informed what triggered the alert, allowing them to better respond to the incident.

Along with anomaly detection capabilities, the reference design employs alerting and reporting capabilities based on known attack tactics and techniques. Recognition of these threats also elicits an alert that is reported to the analyst.

6.3 Lessons Learned

Identifying and replicating the infrastructure(s) likely found in an OT operating environment is a challenge. The NCCoE ESAM Team did not limit this build to a lab environment. The team was able to demonstrate effective OT asset management in existing, real-world energy-sector environments with the support of collaborators who offered their infrastructure, resources, personnel, and assets.

While numerous automated capabilities are used to capture and maintain asset information, a significant manual effort will likely be needed to identify assets, especially those that are remote and not connected to an existing network infrastructure. Further, given the variety of assets deployed, we experienced instances where serial communication devices required conversion to IP-based communication protocols. It is critical to establish the necessary communication infrastructure to ensure these devices become part of the main, automated inventory that this project showcases.

While the technology we used is not complex, working through coordination and deployment of the supporting infrastructure and asset management technologies will be a rather large undertaking for any company looking to adopt this solution or any component of it. We highly recommend that executive management support be in place, whether the OT asset management solution is deployed to a specific site or across the entire enterprise.

7 Future Build Considerations

The Industrial Internet of Things, or IIoT, refers to the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport, energy, and industrial sectors. For the energy sector in particular, distributed energy resources (DERs), such as solar photovoltaic panels and wind turbines, introduce information exchanges between a utility's distribution control system and the DERs, to manage the flow of energy in the distribution grid. Moreover, the rate at which these IIoT devices are deployed in the energy sector is projected to increase and could introduce asset management and cybersecurity challenges for the sector. Expanding the architecture to include IIoT devices and using IIoT-generated data for near-real-time asset management could ensure secure deployment of these assets and may be explored in a future project.

Appendix A List of Acronyms

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
CERT	Computer Emergency Readiness Team
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CSV	Comma-Separated Value
DER	Distributed Energy Resource(s)
ESAM	Energy Sector Asset Management
HART	Highway Addressable Remote Transducer
HMI	Human-Machine Interface
ICMP	Internet Control Message Protocol
ICS	Industrial Control System(s)
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IP	Internet Protocol
ISA	International Society of Automation
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
LTE	Long-Term Evolution
MAC	Media Access Control
NCCoE	National Cybersecurity Center of Excellence
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OS	Operating System
OT	Operational Technology
PLC	Programmable Logic Controller
RARP	Reverse Address Resolution Protocol
RFC	Request for Comments
SCADA	Supervisory Control and Data Acquisition

SIEM	Security Information and Event Management
SP	Special Publication
SPAN	Switched Port Analyzer
TAP	Test Access Points
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UMD	University of Maryland
VPN	Virtual Private Network

Appendix B References

[1] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security,* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Revision 2, NIST, Gaithersburg, MD, May 2015. Available: https://doi.org/10.6028/NIST.SP.800-82r2.

[2] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST SP 800-30 Revision 1, NIST, Gaithersburg, MD, Sept. 2012. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[3] Joint Task Force, *Risk Management Framework for Information Systems and Organizations*, NIST SP 800-37 Revision 2, NIST, Gaithersburg, MD, Dec. 2018. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[4] NIST. *Risk Management Framework: Quick Start Guides*. [Online]. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides.

[5] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments,* NIST SP 800-30 Revision 1, NIST, Gaithersburg, MD, Sept. 2012. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[6] Cybersecurity and Infrastructure Security Agency (CISA) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Cyber Threat Source Descriptions. [Online].Available: https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions.

[7] CISA ICS-CERT. National Cyber Awareness System. Alerts. [Online]. Available: https://www.us-cert.gov/ncas/alerts.

[8] MITRE. Common Vulnerabilities and Exposures. [Online]. Available: https://cve.mitre.org/.

[9] NIST. National Vulnerability Database. Common Vulnerability Scoring System. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss.

[10] CISA ICS-CERT. National Cyber Awareness System. Report Incidents, Phishing, Malware, or Vulnerabilities. [Online]. Available: https://www.us-cert.gov/report.

[11] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Apr. 16, 2018. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[12] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations* NIST SP 800-53 Revision 4, NIST, Gaithersburg, MD, Apr. 2013. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[13] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,* NIST SP 800-181, NIST, Gaithersburg, MD, Aug. 2017. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf.

[14] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Apr. 16, 2018. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

NIST SPECIAL PUBLICATION 1800-23C

Energy Sector Asset Management

For Electric Utilities, Oil & Gas Industry

Volume C:
How-To Guides

James McCarthy
Glen Joy
National Cybersecurity Center of Excellence
Information Technology Laboratory

Lauren Acierto
Jason Kuruvilla
Titilayo Ogunyale
Nikolas Urlaub
John Wiltberger
Devin Wynne
The MITRE Corporation
McLean, Virginia

May 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-23

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/library/energy-sector-asset-management-nist-sp-1800-23-practice-guide

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-23C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-23C, 76 pages, (May 2020), CODEN: NSPUE2

FEEDBACK

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Industrial control systems (ICS) compose a core part of our nation's critical infrastructure. Energy sector companies rely on ICS to generate, transmit, and distribute power and to drill, produce, refine, and transport oil and natural gas. Given the wide variety of ICS assets, such as programmable logic controllers and intelligent electronic devices, that provide command and control information on operational technology (OT) networks, it is essential to protect these devices to maintain continuity of operations. These assets must be monitored and managed to reduce the risk of a cyber attack on ICS-networked environments. Having an accurate OT asset inventory is a critical component of an overall cybersecurity strategy.

The NCCoE at NIST is responding to the energy sector's request for an automated OT asset management solution. To remain fully operational, energy sector entities should be able to effectively identify, control, and monitor their OT assets. This document provides guidance on how to enhance OT asset management practices, by leveraging capabilities that may already exist in an energy organization's operating environment as well as by implementing new capabilities.

KEYWORDS

energy sector asset management; ESAM; ICS; industrial control system; malicious actor; monitoring; operational technology; OT; SCADA; supervisory control and data acquisition

ACKNOWLEDGMENTS

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

Name	Organization
Matt Cowell	Dragos, Inc.
Tom VanNorman	Dragos, Inc.
Andrew Dunham	Forescout Technologies, Inc.
Tim Jones	Forescout Technologies, Inc.
John Norsworthy	Forescout Technologies, Inc.
Lindsey Hale	FoxGuard Solutions, Inc.
Steve Boyd	KORE Wireless, Inc.
Brian Hicks	KORE Wireless, Inc.
Adam Cohn	Splunk Inc.
Bill Wright	Splunk Inc.
Ray Erlinger	TDi Technologies, Inc.
Bill Johnson	TDi Technologies, Inc.

Name	Organization
Samantha Pelletier	TDi Technologies, Inc.
Gabe Authier	Tripwire, Inc.
Steven Sletten	Tripwire, Inc.
Jim Wachhaus	Tripwire, Inc.

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

Technology Partner/Collaborator	Build Involvement
Dragos, Inc.	Dragos Platform v1.5
Forescout Technologies, Inc.	ForeScout CounterACT v8.0.1
FoxGuard Solutions, Inc.	FoxGuard Solutions Patch and Update Management Program v1
KORE Wireless Group, Inc.	KORE Wireless Cellular Connectivity with Cellular Gateway v2.0
Splunk, Inc.	Splunk Enterprise v7.1.3
TDi Technologies, Inc.	TDi Technologies ConsoleWorks v5.2-0u1
Tripwire, Inc.	Tripwire Industrial Visibility v3.2.1

Contents

List of Figures

List of Tables

1 Introduction

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

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

1.1 Practice Guide Structure

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this asset management solution in the energy sector. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-23A: *Executive Summary*
- NIST SP 1800-23B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-23C: *How-To Guides* – instructions for building the example solution **(you are here)**

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

Senior IT executives, including chief information security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-23A*, which describes the following topics:

- challenges that enterprises face in operational technology (OT) asset management
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in NIST SP 1800-23B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk Assessment, provides a description of the risk analysis we performed.
- Section 3.4.4, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary,* NIST SP 1800-23A, with your leadership team members to help them understand the importance of adopting a standards-based solution to strengthen their OT asset management practices, by leveraging capabilities that may already exist within their operating environment or by implementing new capabilities.

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, NIST SP 1800-23C, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of the energy sector asset management (ESAM) solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Volume B, Section 3.5, Technologies, lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

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

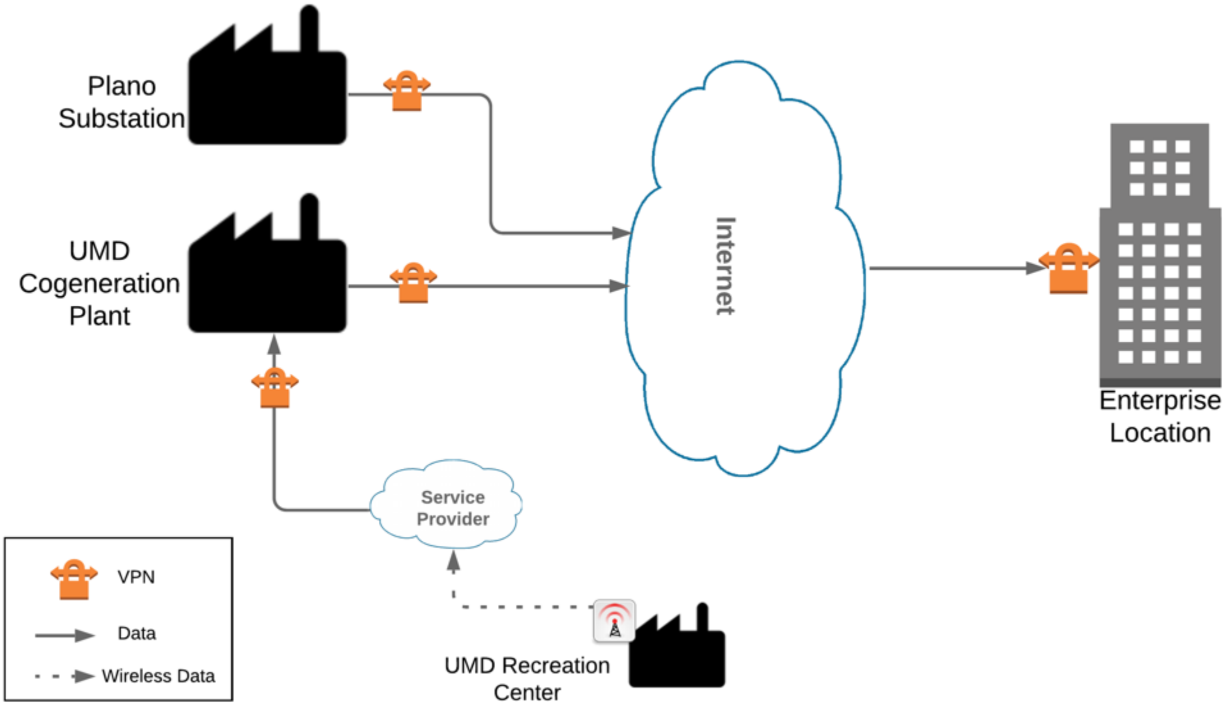
Acronyms used in figures can be found in the List of Acronyms appendix.

1.2 Build Overview

The example solution fulfills the need for an automated asset inventory. This example solution allows devices to be identified in multiple ways, depending on the needs of the organization. The architecture is intended as one solution.

The example solution makes use of two "remote" sites, while the National Cybersecurity Center of Excellence (NCCoE) serves as the enterprise location as shown in Figure 1 below. Having a central enterprise location provides flexibility to add multiple sites as well as the ability to collect all data in one place.

Figure 1-1 High-Level Topology



Different components in the build are installed at each location. However, some components preexist, including the OT assets, networks, routers, and protocol converters. This guide will describe the installation and configuration details of the components installed at each site but not preexisting components. A detailed topology and description of each site can be found in Volume B, Section 4.2, Example Solution.

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-23.

1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

1.4 Logical Architecture Summary

A logical architecture summary can be found in Volume B of this practice guide, Section 4.1, Architecture Description.

2 Product Installation Guides

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

2.1 ConsoleWorks

ConsoleWorks performs as a data collection server and a data analysis server. The data collection server is located at the University of Maryland (UMD) and reads data from a steam meter via protocol converters. The data analysis server resides at the NCCoE and normalizes data collected from security information and event management (SIEM) software, for processing by the patch analysis and reporting tool.

2.1.1 ConsoleWorks Configurations at the NCCoE

The following subsections document the software, hardware/virtual machine (VM), and network configurations for the ConsoleWorks server at the NCCoE.

2.1.1.1 VM Configuration

The ConsoleWorks VM is given the following resources:

- CentOS 7.5
- Central processing unit (CPU) cores
- 100 gigabyte (GB) hard disk
- 10 GB random access memory (RAM)
- 1 network interface controller/card (NIC)

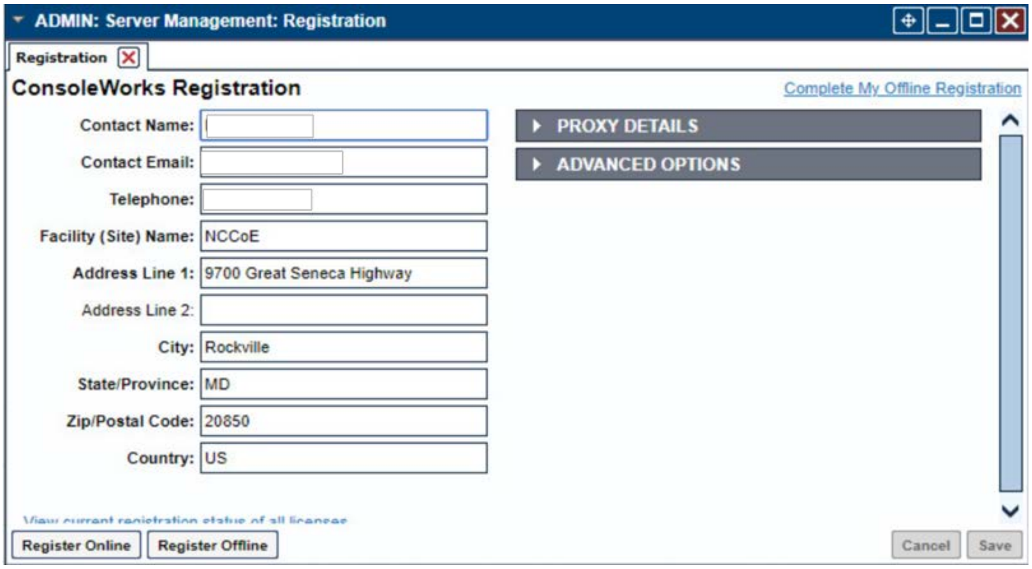
2.1.1.2 Network Configuration

- Dynamic Host Configuration Protocol (DHCP): disabled
- Internet protocol version (IPv)6: ignore
- IPv4: Manual
- IPv4 address: 10.100.100.6
- Netmask: 255.255.255.0

2.1.1.3 Installation

1. Download the installation kit from the http://support.tditechnologies.com website. A username and password are required, so contact TDi Support at support@tditechnologies.com to request them.
2. Create a directory to contain the ConsoleWorks installation files: `#mkdir temp/conworks`
3. Run the following command: `# yum local install consoleworksssssl-<version>_x86_64.rpm`
4. Extract the provided compressed license script to */tmp/conworks.*
5. Run the script from the extracted zip file.
6. Start ConsoleWorks with the following command: `# /opt/ConsoleWorks/bin/cw_start default`

7. Connect to the Console at *https://10.100.100.6:5176*. Log in using the default credentials.



ConsoleWorks Registration

Contact Name:

Contact Email:

Telephone:

Facility (Site) Name: NCCoE

Address Line 1: 9700 Great Seneca Highway

Address Line 2:

City: Rockville

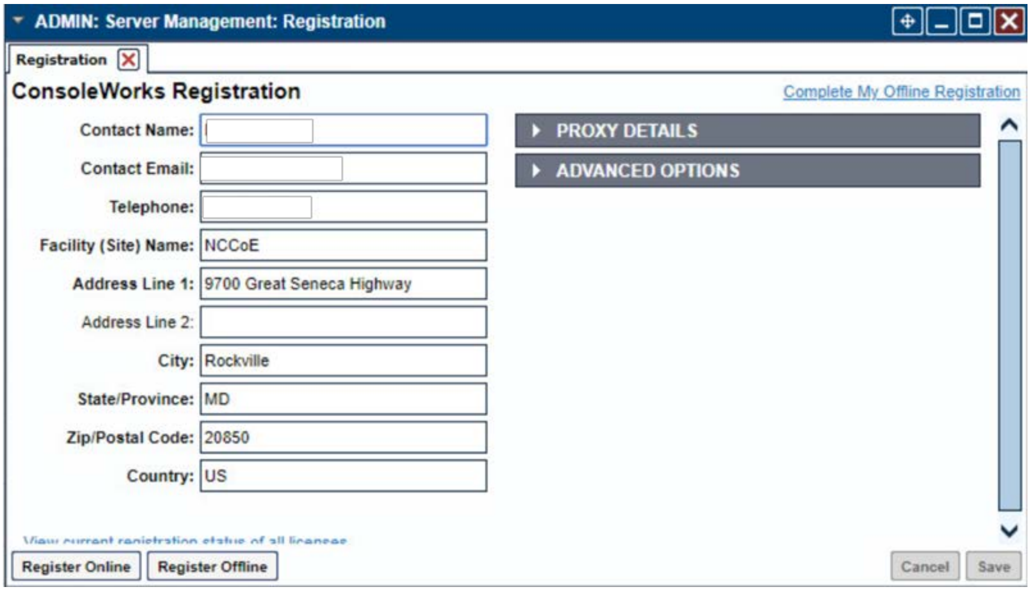
State/Province: MD

Zip/Postal Code: 20850

Country: US

View current registration status of all licenses

8. Fill in the details for Registration. Click **Register Online.** Click **Save.**



ConsoleWorks Registration

Contact Name:

Contact Email:

Telephone:

Facility (Site) Name: NCCoE

Address Line 1: 9700 Great Seneca Highway

Address Line 2:

City: Rockville

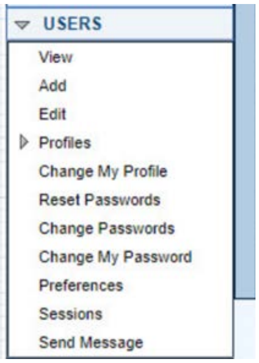
State/Province: MD

Zip/Postal Code: 20850

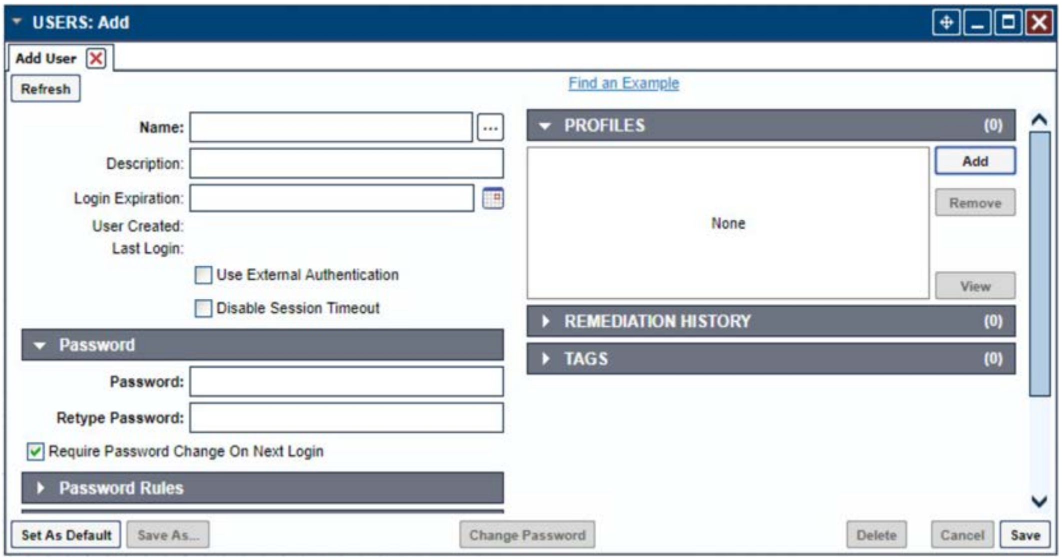
Country: US

View current registration status of all licenses

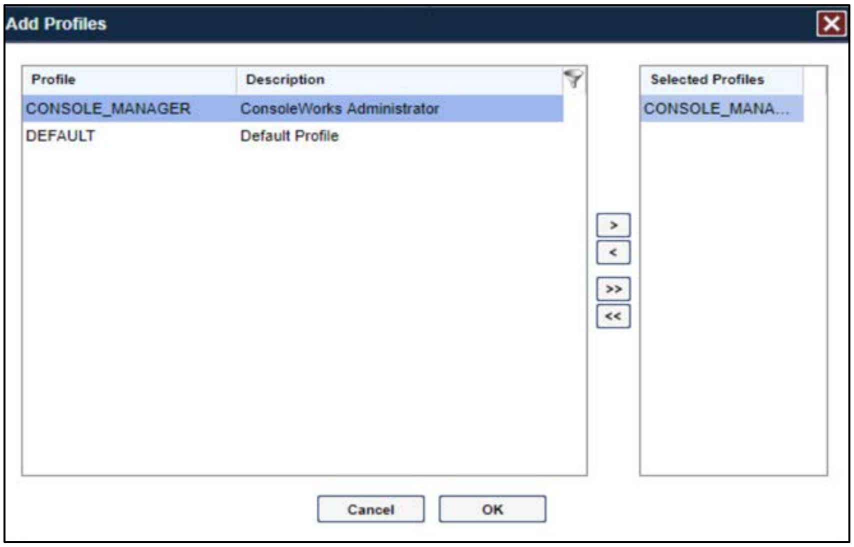
9. Create a new user. Navigate on the left to **Users > Add.**



10. Enter the **Name** and **Password.** Select **Add.**



11. Add **CONSOLE_MANAGER** as a selected profile, as shown in the screenshot below. Select **OK.**

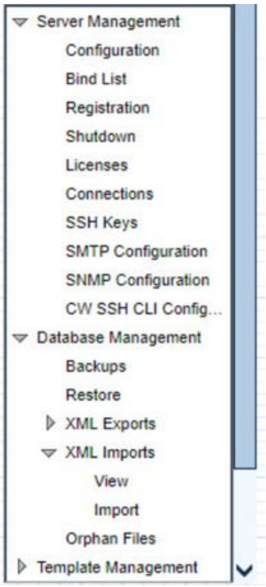


12. Click **Save.**

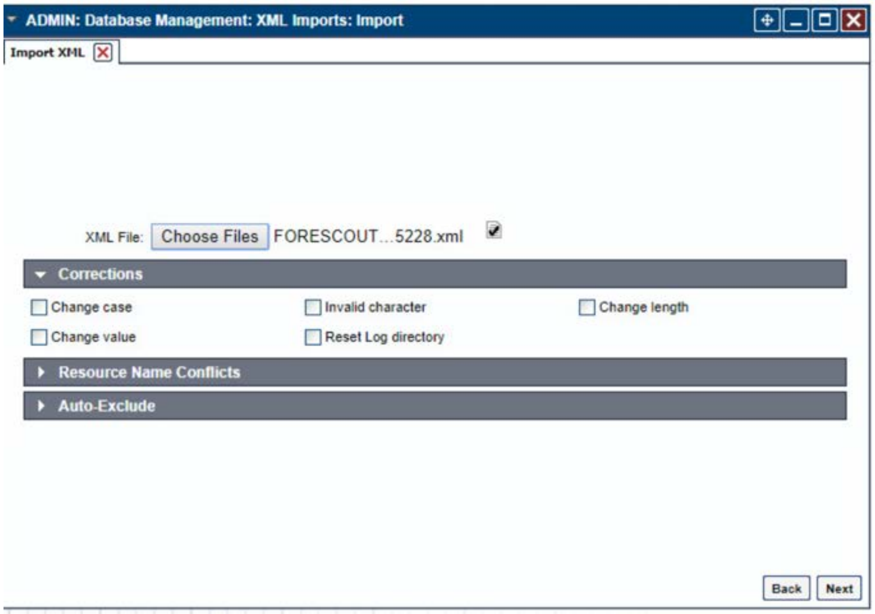
2.1.1.4 Configuration

ConsoleWorks provides the scripts to normalize data, for processing by FoxGuard Patch and Update Management Program (PUMP). The script provided is in extensible markup language (XML) format.

1. Import the provided XML file at **Admin > Database Management > XML Imports > Import.**



2. Click **Choose Files.** Locate the provided XML file. Select **Next.**

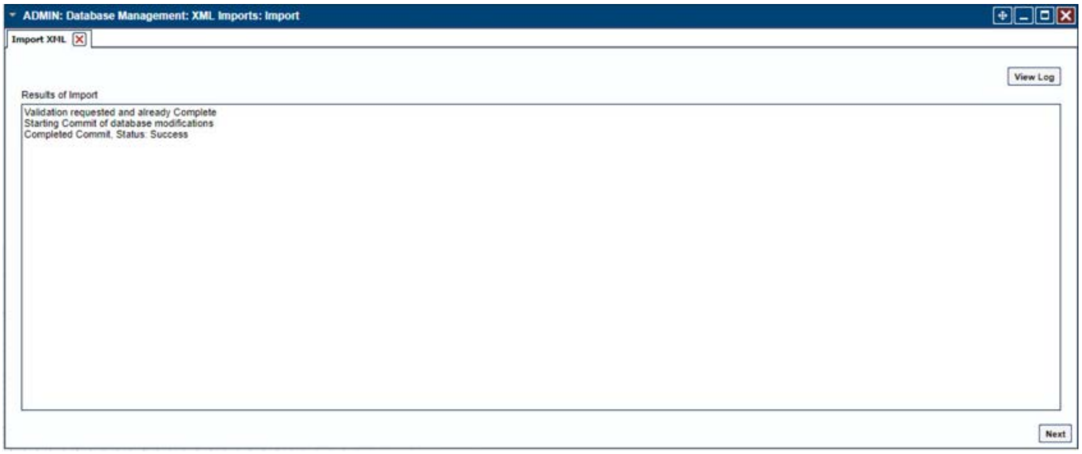


XML File: Choose Files FORESCOUT...5228.xml ☑

☐ Change case ☐ Invalid character ☐ Change length

☐ Change value ☐ Reset Log directory

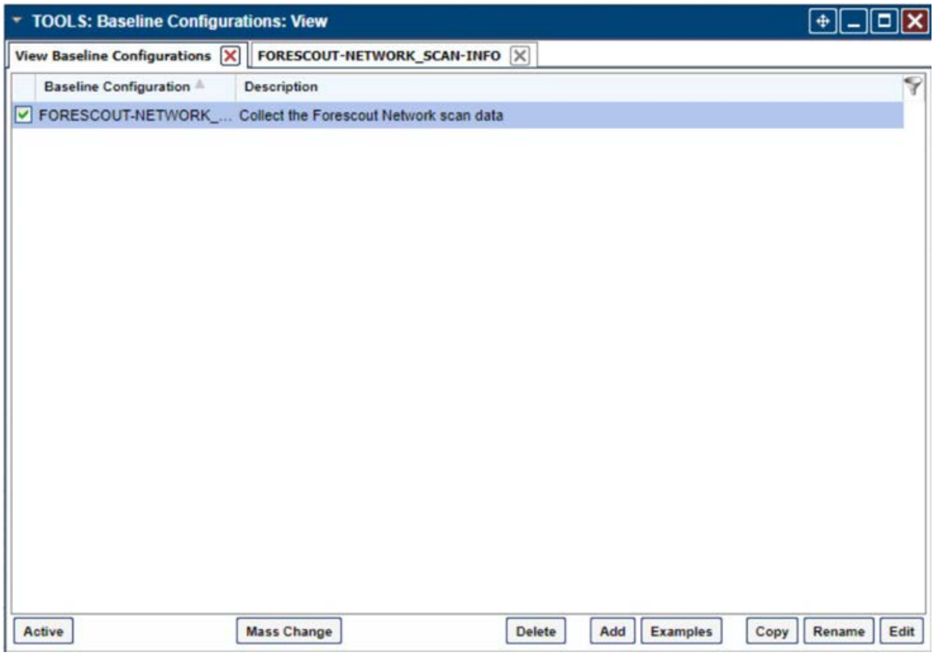
3. Select **Next.** The import is complete.



Results of Import

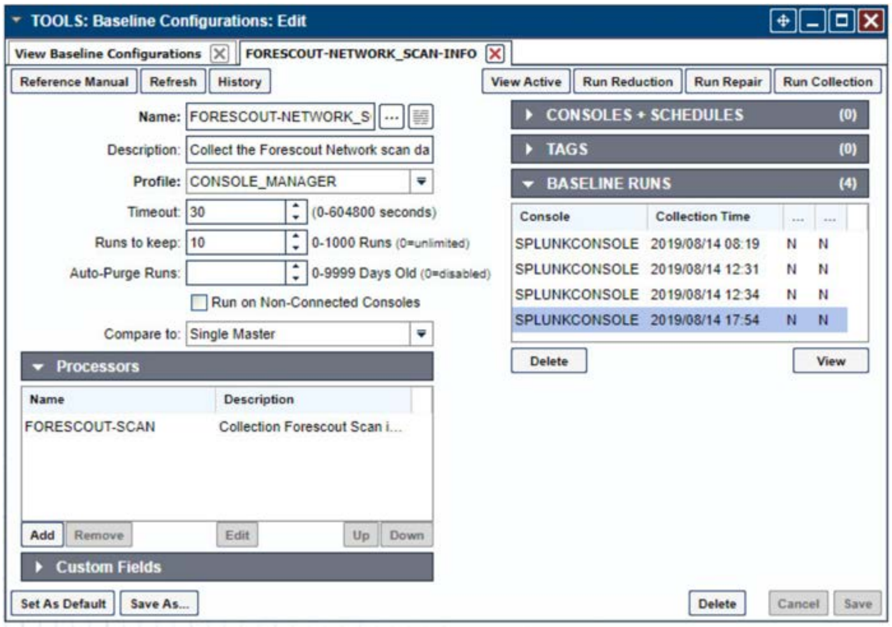
```
Validation requested and already Complete
Starting Commit of database modifications
Completed Commit, Status: Success
```

4. Open the baseline configuration at **Tools > Baseline Configurations > View.** Select **Edit.**


TOOLS: Baseline Configurations: View
View Baseline Configurations
FORESCOUT-NETWORK_SCAN-INFO
Active
Mass Change
Delete
Add
Examples
Copy
Rename
Edit

Baseline Configuration	Description
☑ FORESCOUT-NETWORK_...	Collect the Forescout Network scan data

5. Under **Processors,** select the scan, and click **Edit.**



Name: FORESCOUT-NETWORK_S

Description: Collect the Forescout Network scan da

Profile: CONSOLE_MANAGER

Timeout: 30 (0-604800 seconds)

Runs to keep: 10 0-1000 Runs (0=unlimited)

Auto-Purge Runs: 0-9999 Days Old (0=disabled)

□ Run on Non-Connected Consoles

Compare to: Single Master

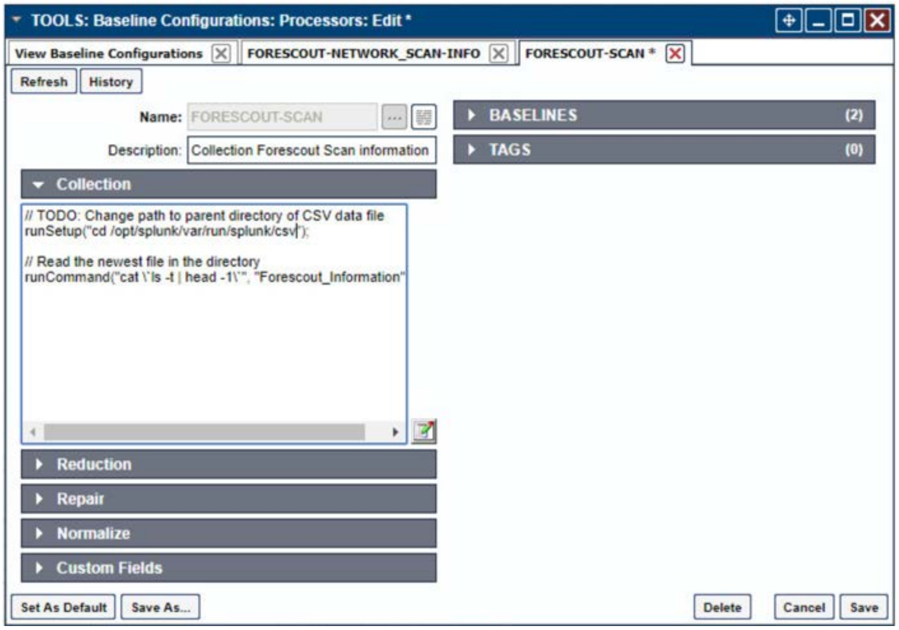
Name	Description
FORESCOUT-SCAN	Collection Forescout Scan i...

Console	Collection Time	...	...
SPLUNKCONSOLE	2019/08/14 08:19	N	N
SPLUNKCONSOLE	2019/08/14 12:31	N	N
SPLUNKCONSOLE	2019/08/14 12:34	N	N
SPLUNKCONSOLE	2019/08/14 17:54	N	N

6. Under **Collection,** update the path to match where Splunk saves the inventory, as shown in the screenshot.

```
// TODO: Change path to parent directory of CSV data file
```

```
runSetup("cd /opt/splunk/var/run/splunk/csv");

// Read the newest file in the directory

runCommand("cat \`ls -t | head -1\`", "Forescout_Information", 5);
```

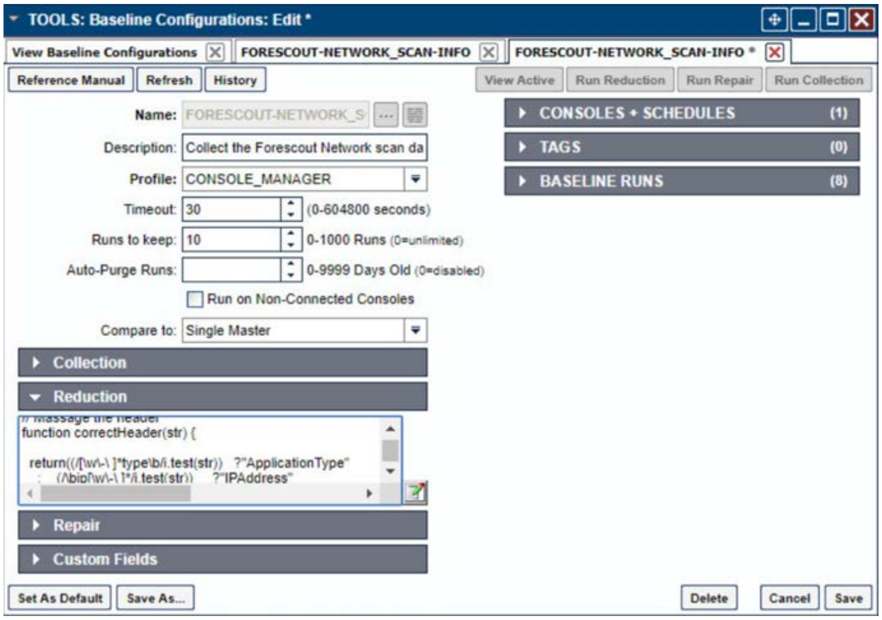


Name: FORESCOUT-SCAN

Description: Collection Forescout Scan information

```
// TODO: Change path to parent directory of CSV data file
runSetup("cd /opt/splunk/var/run/splunk/csv");

// Read the newest file in the directory
runCommand("cat \`ls -t | head -1\`", "Forescout_Information"
```

7. Under **Reduction,** enter the following script, as shown in the screenshot below.



Name: FORESCOUT-NETWORK_S

Description: Collect the Forescout Network scan da

Profile: CONSOLE_MANAGER

Timeout: 30 (0-604800 seconds)

Runs to keep: 10 0-1000 Runs (0=unlimited)

Auto-Purge Runs: 0-9999 Days Old (0=disabled)

□ Run on Non-Connected Consoles

Compare to: Single Master

```
// Massage the header
function correctHeader(str) {

  return((/[\w\-\ ]*type\b/i.test(str))   ?"ApplicationType"
    :    (/\bip[\w\-\ ]*/i.test(str))     ?"IPAddress"
```

```
include("UTIL");

include("UTIL_CUSTOM_FILE");

include("UTIL_JSON");

////////////////////////////////////////////////////////////////////////////////
//////////////////////////

// Massage the header

function correctHeader(str) {

return((/[\w\-\ ]*type\b/i.test(str))   ?"ApplicationType"

 :    (/\bip[\w\-\ ]*/i.test(str))    ?"IPAddress"

    :    (/\bmac[\w\-\ ]*/i.test(str))    ?"MACAddress"

    :    (/\bmodel[\w\-\ ]*/i.test(str))  ?"ModelNumber"

    :    (/\bpart[\w\-\ ]*/i.test(str))   ?"PartNumber"

    :    (/\basset.?id\b/i.test(str))    ?"PK"

:    (/\bproduct[\w\-\ ]*/i.test(str))?"ProductName"

    :    (/\bserial[\w\-\ ]*/i.test(str)) ?"SerialNumber"

    :    (/\bvendor/i.test(String(str)))  ?"VendorName"

    :    (/version/i.test(String(str)))   ?"VersionName"

    :                                String(str).replace(/[\W\_]+/g, "
").camelSpaced().toCapCase().replace(/\ +/g, ""));

}

////////////////////////////////////////////////////////////////////////////////
//////////////////////////

// ref: http://stackoverflow.com/a/1293163/2343

function CSVToArray(strData, strDelimiter) {

  // Check to see if the delimiter is defined. If not, then default to comma.

  strDelimiter=(typeof strDelimiter!='undefined')?strDelimiter:",";

  // Create a regular expression to parse the CSV values.

  //                      Delimiters                      Quoted fields
Standard fields.

  var objPattern=new
RegExp(("(\\"+strDelimiter+"|\\r?\\n|\\r|^)(?:\"([^\"]*(?:\"\"[^\"]*)*)\"|([^\"
\\"+strDelimiter+"\\r\\n]*))"), "gi");

  // Create an array to hold our data. Give the array a default empty first row.
  var arrData=[[]];

  // Create an array to hold our individual pattern matching groups.

  var arrMatches=null;

  // Keep looping over the regular expression matches until we can no longer
find a match.

  while(arrMatches=objPattern.exec(strData)) {

   // Get the delimiter that was found.

   var strMatchedDelimiter=arrMatches[1];

   // Check to see if the given delimiter has a length (is not the start of
string) and if it matches field delimiter.

   // If it does not, then we know that this delimiter is a row delimiter.

   if(strMatchedDelimiter.length && strMatchedDelimiter!==strDelimiter) {

    // Since we have reached a new row of data, add an empty row to our data
array.

    arrData.push([]);

   }

   var strMatchedValue;

   // Now that we have our delimiter out of the way, let's check to see which
kind of value we captured (quoted or unquoted).

   if(arrMatches[2]) {

    // We found a quoted value. When we capture this value, unescape any
double quotes.

    //strMatchedValue=arrMatches[2].replace(new RegExp( "\"\"", "g" ), "\"");

    strMatchedValue=arrMatches[2].replace(/\"{2}/g, '"');

   } else {

    // We found a non-quoted value.

    strMatchedValue=arrMatches[3];

   }

   // Now that we have our value string, let's add it to the data array.

   arrData[arrData.length-1].push(strMatchedValue);

  }

  // Return the parsed data.
```

```
  return(arrData);
}
///////////////////////////////////////////////////////////////////////////////
//////////////////////////
function procCSV(csv) {
  // Convert string to YYYYMMDD_HHMMSS for readability
  var outputDir="/FOXGUARD/"+(now.slice(0,8));
  var outputFile=""+outputDir+"/"+(now.slice(8,14));
  var result=[];
  // Default of negative feedback
  var tracker=false;
  if(typeof csv!='undefined' && csv.length>0) {
    try {
      var lines=CSVToArray(csv);
      lines.shift();
      if(lines.length>1) {
        try {
          // Header names
          var props=lines[0];
          if(props.length>0) {
            // Massage header names
            for(var k=0;k<props.length;k++) {
              if(props[k].length>0) {
                props[k]=correctHeader(props[k]);
              }
            }
            for(i=1;i<lines.length;i++) {
              var j=lines[i];
              if(j.length>0) {
                var obj={
                  "ApplicationType": "Firmware",
                  "ModelNumber": "unspecified",
                  "PartNumber": "unspecified",
                  "PK": "unspecified",
                  "ProductName": "unspecified",
                  "SerialNumber": "unspecified",
                 "VendorName": "unspecified",
                 "VersionName": "unspecified"
                };

   if(String(ServerConfig.getList()[0].conwrksinvo).split("/")[3]!="default") {

   obj.Site=String(ServerConfig.getList()[0].conwrksinvo).split("/")[3];
                 }
                 for(var k=0;k<props.length;k++) {
               if(Boolean(j[k]) && j[k]!="-") {
                 switch(props[k]) {
                  case "IPAddress":

//obj.IPAddress=(rEIPv4.test(j[k]))?j[k].match(rEIPv4)[1]:(rEIPv6.test(j[k]))?j[k].
match(rEIPv6)[1]:"unspecified";
                    break;
                  case "MACAddress":

//obj.MACAddress=(rEMAC.test(j[k]))?j[k].match(rEMAC)[1]:"unspecified";
                    break;
                  case "OperatingSystem":
                    obj.ApplicationType="Operating System";
                    obj.OperatingSystem=j[k];
                    obj.ProductName=j[k];
                    break;
                  case "VendorName":
                    if(obj.VendorName=="unspecified") {
```

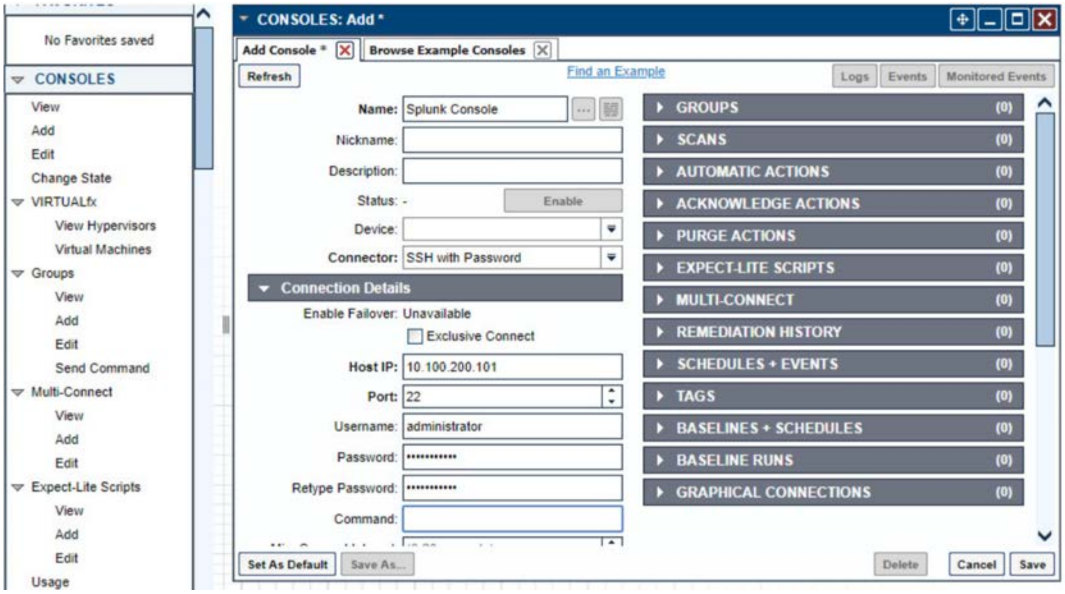
```
          obj.VendorName=j[k];
        }
        break;
      case "VersionName":
        obj.VersionName=j[k];
        if(rESEL.test(j[k])) {
          obj.ModelNumber=j[k].match(rESEL)[1];
          obj.VendorName="Schweitzer";
        }
        break;
      default:
        obj[props[k]]=j[k];
        break;
    }
  }
}
if(obj.hasOwnProperty('OperatingSystem')) {
  obj.OperatingSystemVersion=obj.VersionName;
  //delete obj.VersionName;
}
for(var p in obj) {
  // These are required properties
  if(["ProductName", "VendorName", "VersionName"].indexOf(p)<0) {
    // Not a required property, and no useful data, get rid of it!
    if(Boolean(obj[p])==false || obj[p]=="unspecified") {
      delete obj[p];
    }
  }
}
result.push({
```

```
                  "AssetIdentifiers": obj,
                  "FUI": null
                });
              }
            }
            try {
              setReduction("Forescout_Information", JSON.stringify(result, null, 2));
              makeDirectory(""+outputDir);
              // File for FoxGuard
              setCustomFileContents(""+outputFile+".txt", JSON.stringify(result,
null, 2));
              // Copy of original input
              //setCustomFileContents(""+outputFile+".csv", csv);
              // If everything goes great, return with positive feedback
              tracker=true;
            } catch(ex) {
              print("ERROR: "+ex);
            }
          } else {
            print("ERROR: Missing header data");
          }
        } catch(ex) {
          print("ERROR: "+ex);
        }
      } else {
        print("ERROR: Going to need more data than this");
      }
    } catch(ex) {
      print("ERROR: "+ex);
    }
  } else {
    print("ERROR: We got nothing!");
  }
  return(tracker);
}
////////////////////////////////////////////////////////////////////////////////////
//////////////////////
// value for TZ offset
var d=0;
try {
  d=new Date().getTimezoneOffset();
} catch(ex) {
  print("ERROR: "+ex);
}
// Create string of YYYYMMDDHHMMSS
var now=String(new Date(Date.now()-(d*60000)).toJSON()).replace(/\D/g,
"").slice(0,14);
// IPv4
var rEIPv4=/\b((?:(?:25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])\.){3}(?:25[0-
5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9]))\b/;
// IPv6
var rEIPv6=/\b([\da-fA-F]{1,4}(?:\:[\da-fA-F]{0,4}){2,6}[\da-fA-F]{1,4})\b/;
// MAC
var rEMAC=/\b((?:[\da-fA-F]{2}\:){5}[\da-fA-F]{2})\b/;
// SEL
var rESEL=/\b(SEL-.+)-R/;
try {
  procCSV(getOutput("Forescout_Information"));
} catch(ex) {
  print("ERROR: "+ex);
    }
```

8. Select **Save.**

9. Navigate to **Consoles > Add.**

10. Enter a name and connection details for the Splunk server. Select **Save.**



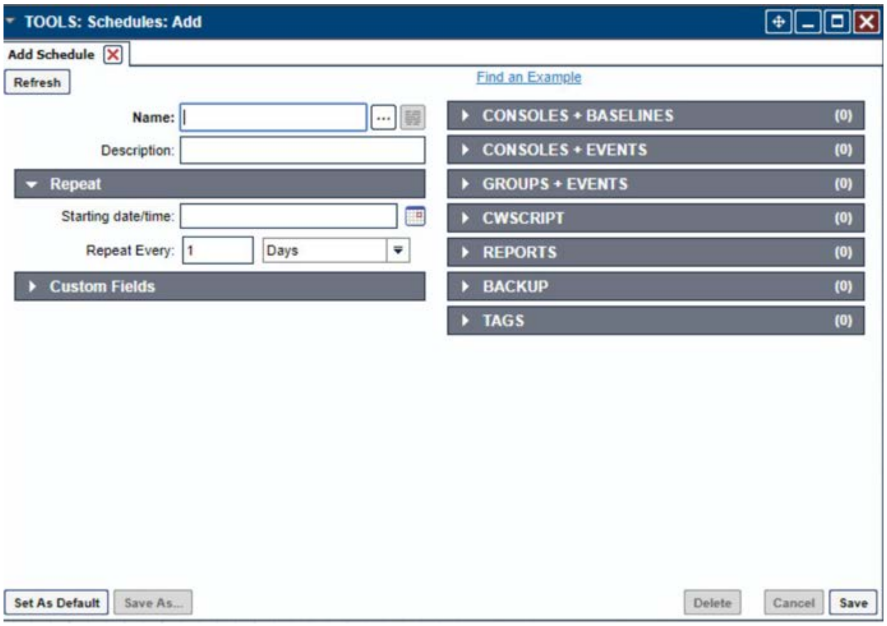
CONSOLES: Add *

Name: Splunk Console
Nickname:
Description:
Status: -
Device:
Connector: SSH with Password

Connection Details
Enable Failover: Unavailable
□ Exclusive Connect
Host IP: 10.100.200.101
Port: 22
Username: administrator
Password: ••••••••••
Retype Password: ••••••••••
Command:

11. Navigate to **Tools > Schedule.** Click **Add.**

12. Name the schedule. Set the time to run at an acceptable interval (this build set the interval to repeat daily). Under **CONSOLES + BASELINES,** click **Add.**

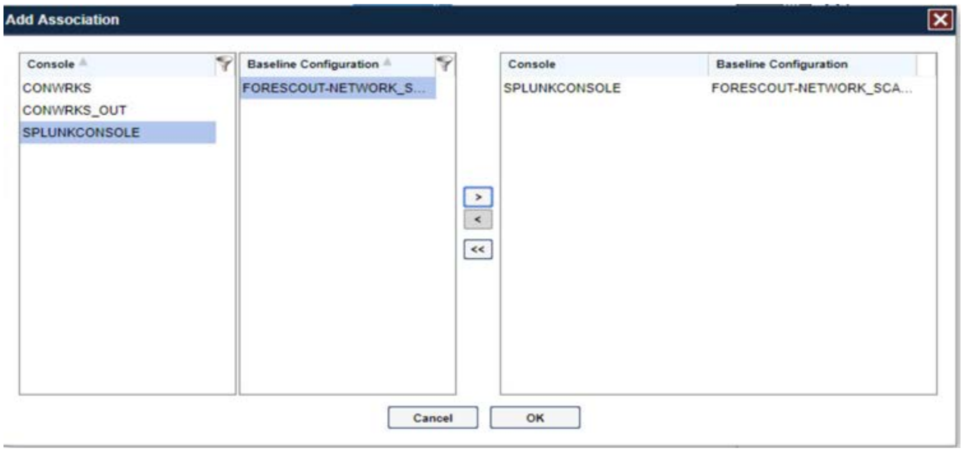


TOOLS: Schedules: Add

Name:
Description:

Repeat
Starting date/time:
Repeat Every: 1 Days

13. Select the previously created Splunk console and the imported baseline configuration. Click the arrow. Click **OK.**

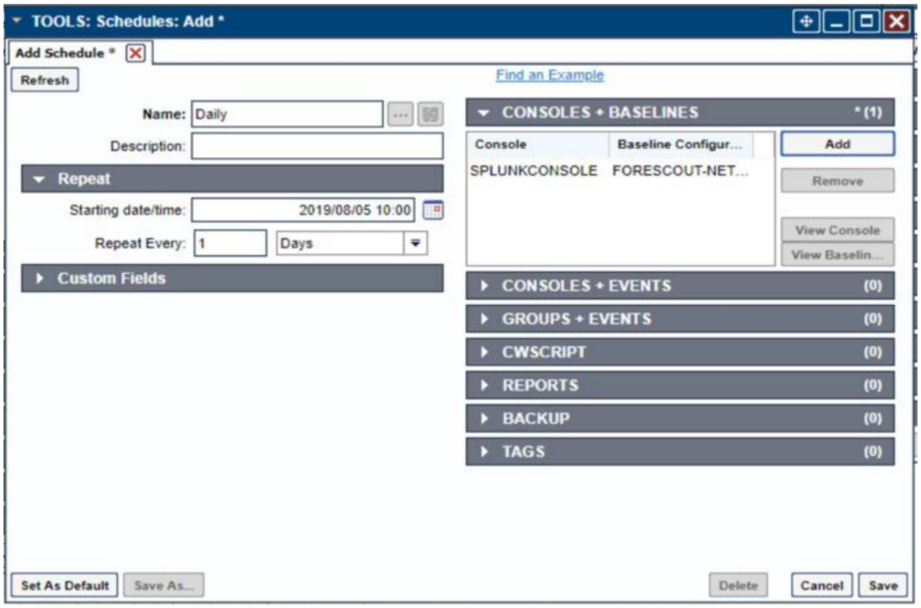


Console
CONWRKS
CONWRKS_OUT
SPLUNKCONSOLE

Baseline Configuration
FORESCOUT-NETWORK_S...

Console	Baseline Configuration
SPLUNKCONSOLE	FORESCOUT-NETWORK_SCA...

14. Click **Save.**



Name: Daily

Description:

Starting date/time: 2019/08/05 10:00

Repeat Every: 1 Days

Console	Baseline Configur...
SPLUNKCONSOLE	FORESCOUT-NET...

2.1.1.5 ConsoleWorks Configurations UMD

The following subsections document the software, hardware/VM, and network configurations for the ConsoleWorks server at UMD.

2.1.1.6 VM Configuration

The UMD ConsoleWorks VM is given the following resources:

- Windows Server 2016

- 2 CPU cores
- 100 GB hard Disks
- 12 GB RAM
- 2 NIC

2.1.1.7 Network Configuration

Network Configuration (Interface 1):

- DHCP: disabled
- IPv6: ignore
- IPv4: Manual
- IPv4 address: 10.100.1.6
- Netmask: 255.255.255.0

Network Configuration (Interface 2):

- DHCP: disabled
- IPv6: ignore
- IPv4: Manual
- IPv4 address: 172.16.2.82
- Netmask: 255.255.255.248

2.1.1.8 Installation

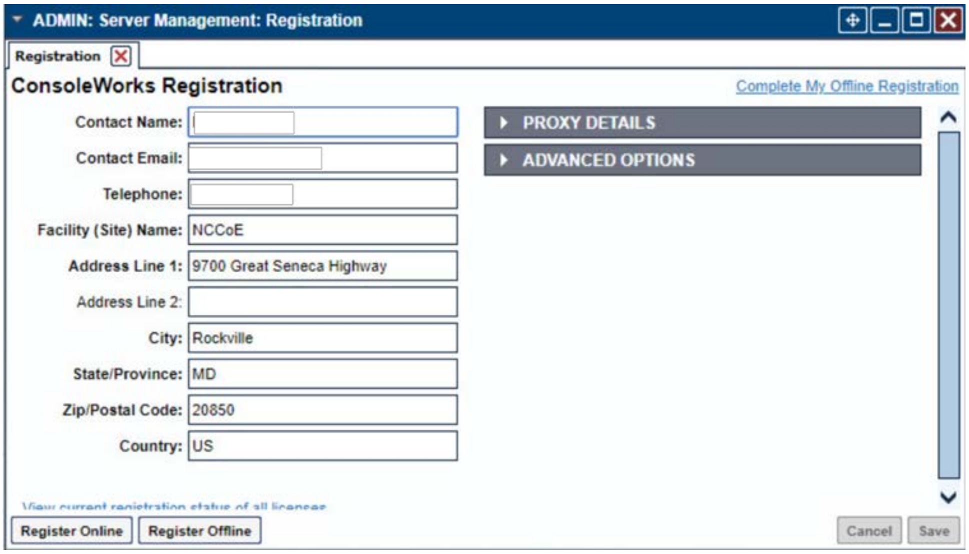
1. Download the installation kit from the http://support.tditechnologies.com website. A username and password are required, so contact TDi Support at support@tditechnologies.com to request them.

2. Run the installer *cw_server_<version>.exe.*

3. Download the Splunk universal forwarder installer from the https://www.splunk.com/en_us/download/universal-forwarder.html website. A username and password are required. An account can be created on the Splunk website.

4. Use the splunkforwarder-<version>-x64-release.msi installer to install the Splunk Universal Forwarder on the machine running the ConsoleWorks.

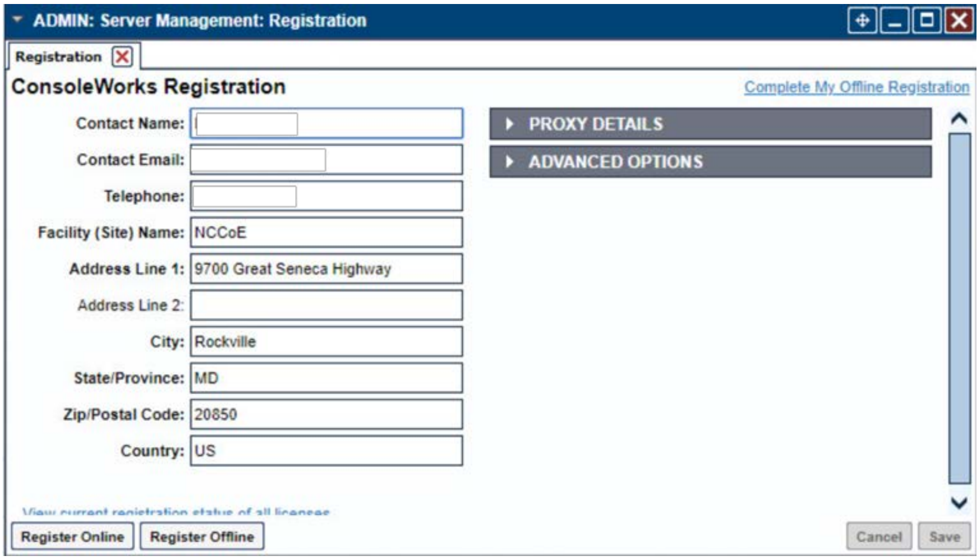
5. Connect to the Console at *https://10.100.1.6:5176*. Log in using the default credentials.


ADMIN: Server Management: Registration
Registration
Complete My Offline Registration
PROXY DETAILS
ADVANCED OPTIONS
View current registration status of all licenses
Register Online
Register Offline
Cancel
Save

ConsoleWorks Registration

Contact Name:
Contact Email:
Telephone:
Facility (Site) Name: NCCoE
Address Line 1: 9700 Great Seneca Highway
Address Line 2:
City: Rockville
State/Province: MD
Zip/Postal Code: 20850
Country: US

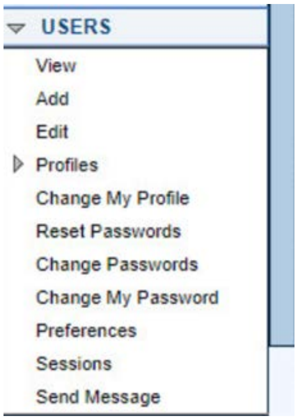
6. Fill in the details for **Registration**. Click **Register Online.** Click **Save.**


ADMIN: Server Management: Registration
Registration
Complete My Offline Registration
PROXY DETAILS
ADVANCED OPTIONS
View current registration status of all licenses
Register Online
Register Offline
Cancel
Save

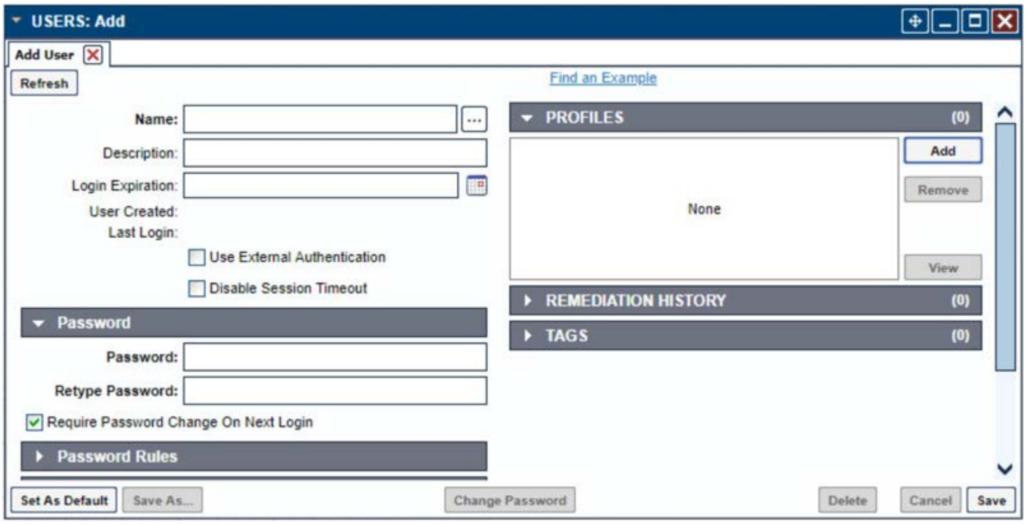
ConsoleWorks Registration

Contact Name:
Contact Email:
Telephone:
Facility (Site) Name: NCCoE
Address Line 1: 9700 Great Seneca Highway
Address Line 2:
City: Rockville
State/Province: MD
Zip/Postal Code: 20850
Country: US

7. Create a new user. Navigate on left to **Users > Add.**



8. Enter the name and password. Select **Add.**



Name:

Description:

Login Expiration:

User Created:

Last Login:

□ Use External Authentication

□ Disable Session Timeout

Password

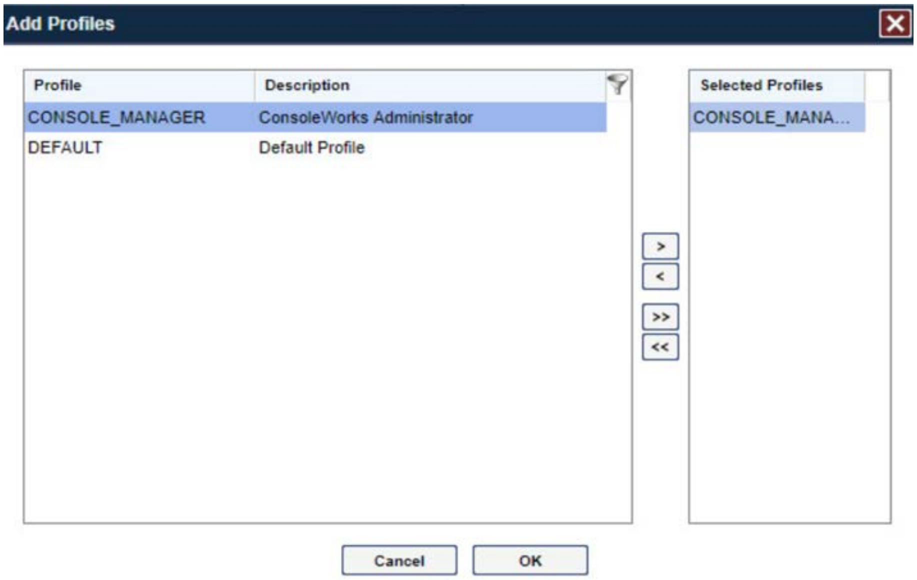
Password:

Retype Password:

☑ Require Password Change On Next Login

None

9. Add **CONSOLE_MANAGER** as a selected profile, as shown in the screenshot below. Select **OK.**



Profile	Description
CONSOLE_MANAGER	ConsoleWorks Administrator
DEFAULT	Default Profile

Selected Profiles
CONSOLE_MANA...

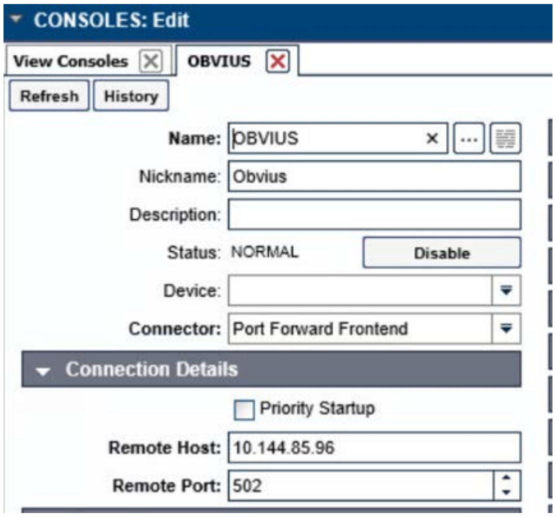
10. Click **Save.**

2.1.1.9 Configuration

ConsoleWorks provides the scripts to query the Modbus server. The script provided is in XML format.

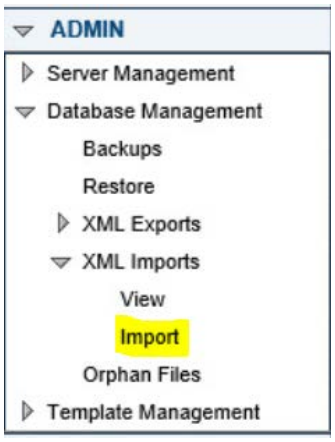
1. Navigate to **Consoles > Add.**

2. Enter a name and connection details that will be used to connect to the Obvius data acquisition server. Select **Save.**

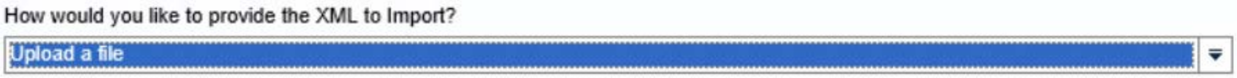


Name: OBVIUS
Nickname: Obvius
Description:
Status: NORMAL
Device:
Connector: Port Forward Frontend
□ Priority Startup
Remote Host: 10.144.85.96
Remote Port: 502

3. Navigate to **Admin > Database Management > XML Imports > Import.**



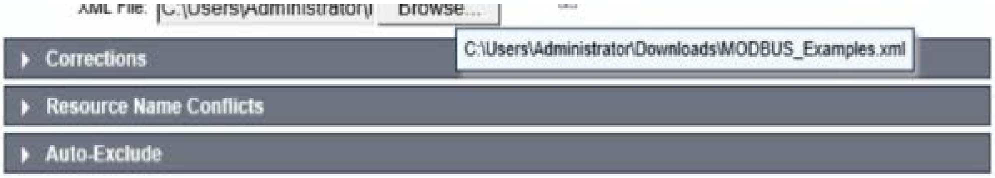
4. Select **Upload a file,** then click **Next.**



How would you like to provide the XML to Import?

Upload a file

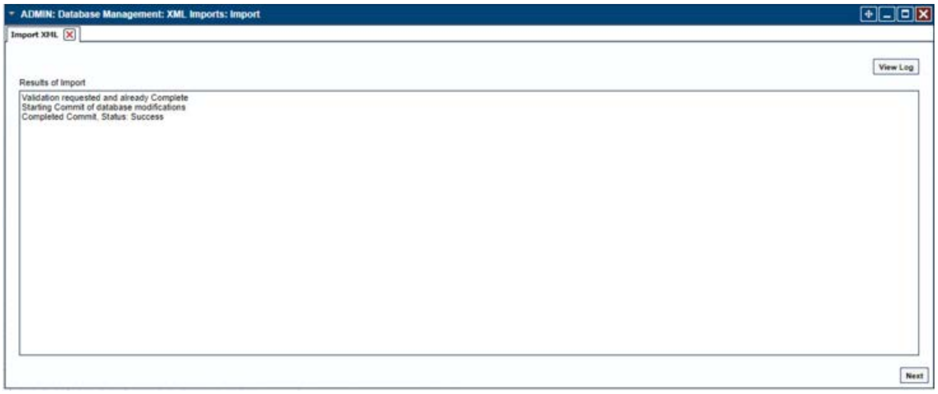
5. Click **Browse,** then find the XML file.



XML File: C:\Users\Administrator\ Browse...

C:\Users\Administrator\Downloads\MODBUS_Examples.xml

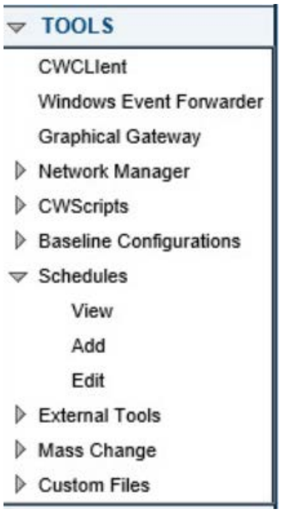
6. Click **Next.** ConsoleWorks will import the two CWScripts: *UTIL_MODBUS* and *UTIL_MODBUS_GE.*



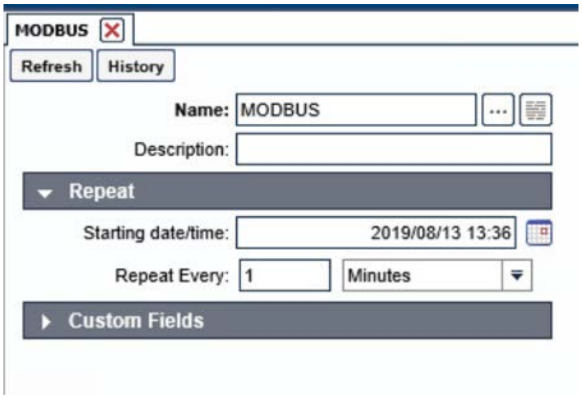
Results of Import

```
Validation requested and already Complete
Starting Commit of database modifications
Completed Commit, Status: Success
```

7. Navigate to **Tools > Schedule.** Click **Add.**



8. Name the schedule. Set the time to run at an acceptable interval, then **save.**



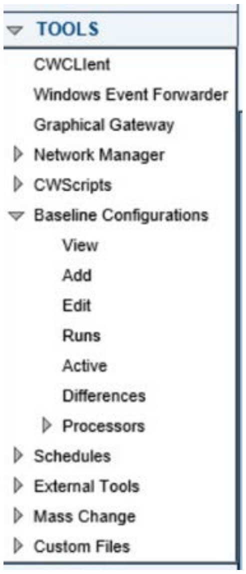
Name: MODBUS

Description:

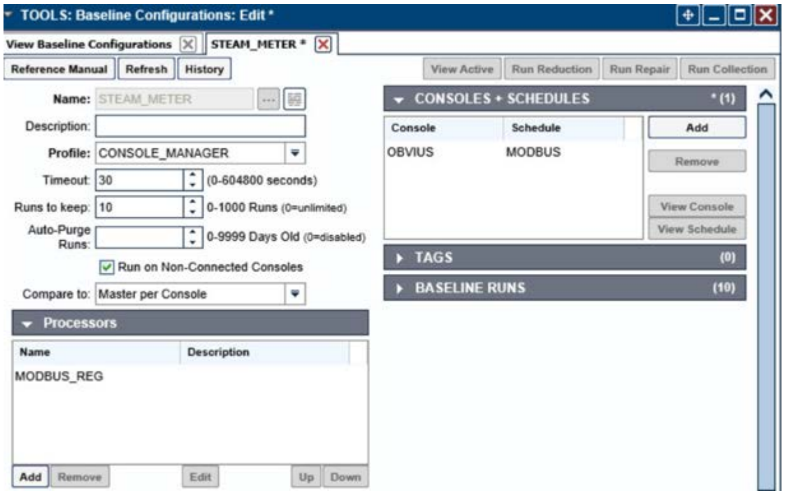
Starting date/time: 2019/08/13 13:36

Repeat Every: 1 Minutes

9. Navigate to **Tools > Baseline Configurations > Add.**



10. Name the baseline, and set the Profile to **CONSOLE_MANAGER.**



Name: STEAM_METER

Description:

Profile: CONSOLE_MANAGER

Timeout: 30 (0-604800 seconds)

Runs to keep: 10 0-1000 Runs (0=unlimited)

Auto-Purge Runs: 0-9999 Days Old (0=disabled)

☑ Run on Non-Connected Consoles

Compare to: Master per Console

Processors

Name	Description
MODBUS_REG	

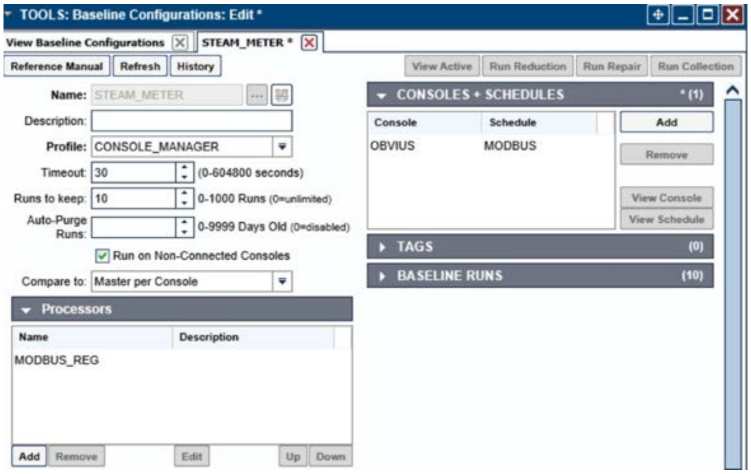
CONSOLES + SCHEDULES * (1)

Console	Schedule
OBVIUS	MODBUS

TAGS (0)

BASELINE RUNS (10)

11. Create a Processor to collect the information from the OBVIUS server. Click **Add** under **Processors.**

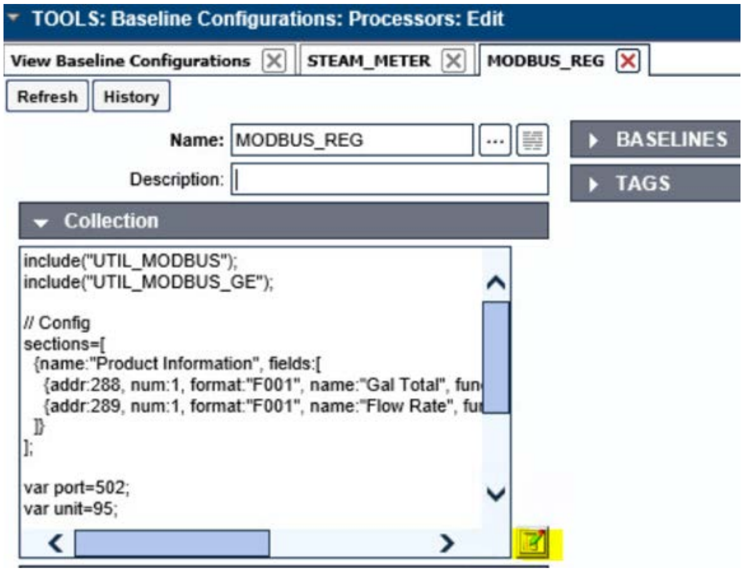


Name: STEAM_METER
Description:
Profile: CONSOLE_MANAGER
Timeout: 30 (0-604800 seconds)
Runs to keep: 10 0-1000 Runs (0=unlimited)
Auto-Purge Runs: 0-9999 Days Old (0=disabled)
☑ Run on Non-Connected Consoles
Compare to: Master per Console

Console	Schedule
OBVIUS	MODBUS

Name	Description
MODBUS_REG	

12. Name the Processor, then click the highlighted button. Enter the text that follows, then click **Save.**


TOOLS: Baseline Configurations: Processors: Edit
View Baseline Configurations
STEAM_METER
MODBUS_REG
Refresh
History
BASELINES
TAGS
Collection

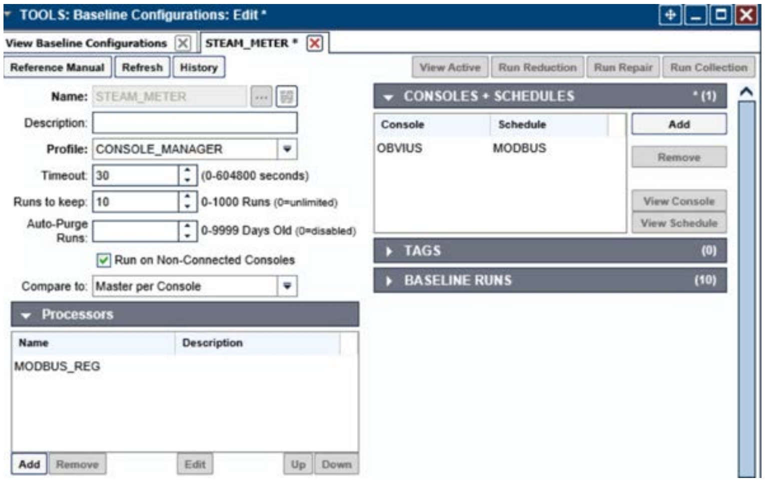
Name: MODBUS_REG
Description:

```
include("UTIL_MODBUS");
include("UTIL_MODBUS_GE");

// Config
sections=[
  {name:"Product Information", fields:[
    {addr:288, num:1, format:"F001", name:"Gal Total", fun
    {addr:289, num:1, format:"F001", name:"Flow Rate", fu
  ]}
];

var port=502;
var unit=95;
```

```
include("UTIL_MODBUS");
include("UTIL_MODBUS_GE");

// Config
sections=[
  {name:"Product Information", fields:[
    {addr:288, num:1, format:"F001", name:"Gal Total", functionName:
readHoldingRegisters},
    {addr:289, num:1, format:"F001", name:"Flow Rate", functionName:
readHoldingRegisters},
  ]}
];
```

```
var port=502;
var unit=95;

// Execute
var server=console.port;

for(var s=0;s<sections.length;s++) {
  setOutput(sections[s].name, formatGEOutput(modbusConnection(server, port, unit,
sections[s].fields)));
  log("SPLUNK",formatGEOutput(modbusConnection(server, port, unit,
sections[s].fields)));
}
```

13. Return the **Baseline Configuration**, then under **CONSOLE + SCHEDULES**, select **Add.**



Name: STEAM_METER

Description:

Profile: CONSOLE_MANAGER

Timeout: 30 (0-604800 seconds)

Runs to keep: 10 0-1000 Runs (0=unlimited)

Auto-Purge Runs: 0-9999 Days Old (0=disabled)

☑ Run on Non-Connected Consoles

Compare to: Master per Console

Processors

Name	Description
MODBUS_REG	

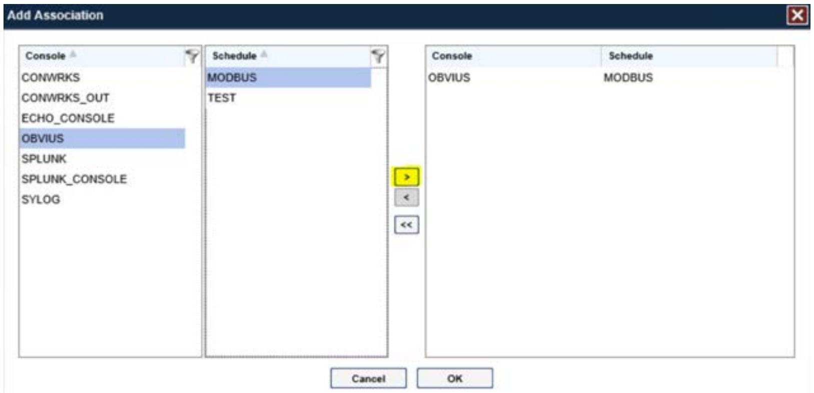
CONSOLES + SCHEDULES * (1)

Console	Schedule
OBVIUS	MODBUS

TAGS (0)

BASELINE RUNS (10)

14. Under **Console**, select **OBVIUS,** and select **MODBUS**, then click **>.**

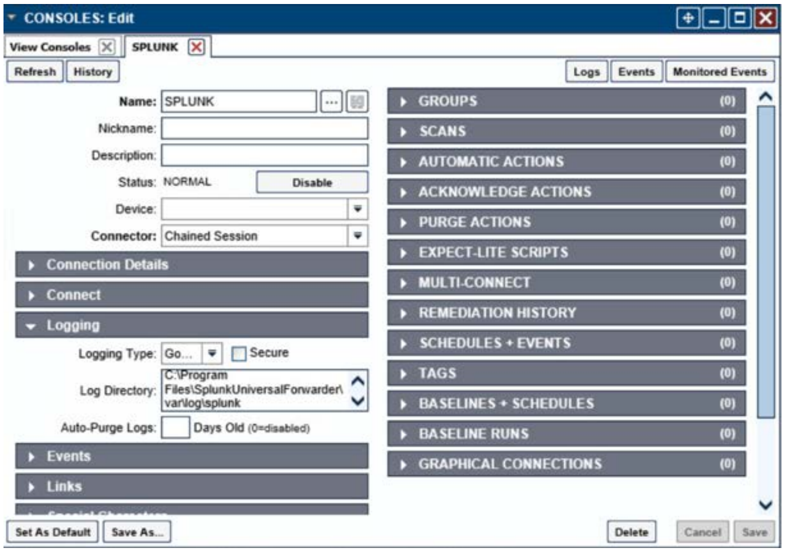


Console
CONWRKS
CONWRKS_OUT
ECHO_CONSOLE
OBVIUS
SPLUNK
SPLUNK_CONSOLE
SYLOG

Schedule
MODBUS
TEST

Console	Schedule
OBVIUS	MODBUS

15. Create the SPLUNK console to log the collected Modbus registers at **Console > Add.**



Name: SPLUNK

Nickname:

Description:

Status: NORMAL

Device:

Connector: Chained Session

Logging Type: Go... □ Secure

Log Directory: C:\Program Files\SplunkUniversalForwarder\var\log\splunk

Auto-Purge Logs: Days Old (0=disabled)

16. Name the **Console**, and set the connector to **Chain Session**, the log type to **Governed**, and the Log Directory to the below location:

    ```
    C:\Program Files\SplunkUniversalForwarder\log\splunk
    ```

17. Navigate to *C:\Program Files\SplunkUniversalForwarder\etc\system\local\*

18. Add the following lines to the *outputs.conf* file:

    ```
    [tcpout:default-autolb-group]

    server = 10.100.200.101:9997

    [tcpout-server://10.100.200.101:9997]
    ```

19. Add the following lines to the *inputs.conf* file:

    ```
    [monitor://$SPLUNK_HOME\var\log\splunk\SPLUNK.LOG*]

    index = modbus
    ```

2.2 Forescout CounterACT

Forescout CounterACT is used as a data collection and inventory tool. The CounterACT appliance actively collects data from the ICS lab in Plano, Texas. The appliance reports back to the CounterACT Enterprise Manager on the enterprise network in Rockville, Maryland. Once installed, the appliance is configured and managed through the enterprise manager.

Forescout CounterACT can be deployed on virtual or physical appliances. For virtualized environments, VMware ESXi, Microsoft Hyper-V, and KVM hypervisors are supported. Large networks that require multiple physical or virtual appliances can be centrally managed by the Enterprise Manager.

https://www.forescout.com/platform/specifications/#virtual-appliance

Note: Some network-related information has been redacted.

2.2.1 CounterACT Enterprise Manager Configuration

2.2.1.1 VM Configuration

The CounterACT Enterprise Manager is configured as follows:

- Red Hat Enterprise Linux 7
- CPU cores
- 16 GB of RAM
- 200 GB of storage
- 1 NIC

2.2.1.2 Network

Network Configuration (Interface 1):

- IPv4: Manual
- IPv6: disabled
- IPv4 address: 10.100.100.33
- Netmask: 255.255.255.0
- Gateway: 10.100.100.1

2.2.1.3 Installation

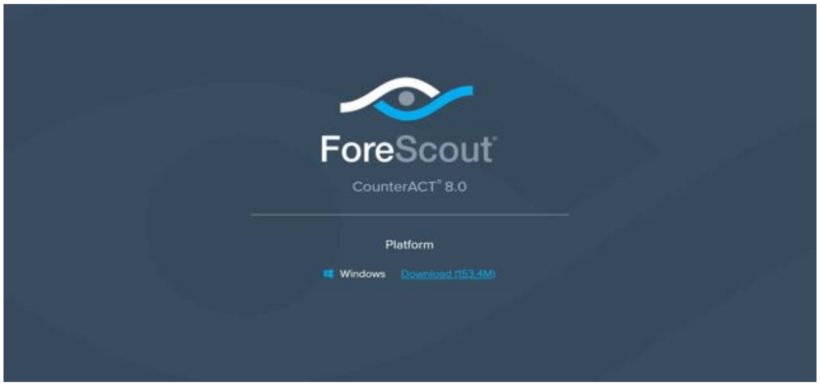
To install CounterACT Enterprise Manager, refer to the installation guide available at https://www.forescout.com/company/resources/forescout-installation-guide-8-1/.

2.2.1.4 Configuration

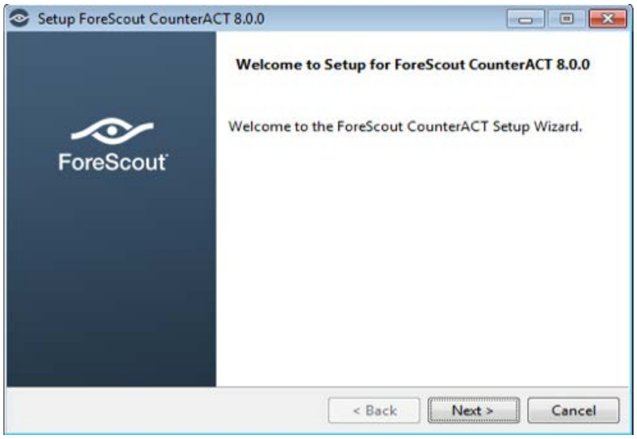
The following steps contain configuration instructions for scanning devices at the Plano location. For additional CounterACT configuration details, refer to the administration guide at https://www.forescout.com/wp-content/uploads/2018/11/counteract-administration-guide-8.0.1.pdf.

The CounterACT Enterprise Manager and CounterACT Appliance can be managed through the CounterACT console. Complete the following steps to install the console on a Windows desktop:

1. Download the executable from a Forescout portal.
2. Select the CounterACT Console Setup file. The CounterACT Console software download screen opens.



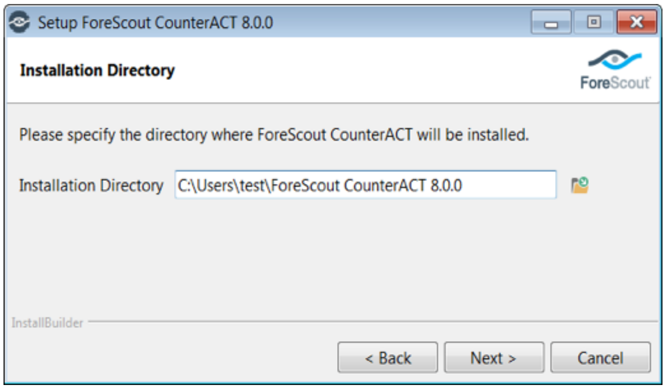
3. Select the download link required, and save the EXE file.
4. Select and run the file to begin the installation. The **Setup Wizard** opens. Select **Next.**



Welcome to Setup for ForeScout CounterACT 8.0.0

Welcome to the ForeScout CounterACT Setup Wizard.

5. Use the default installation directory. Click **Next.**



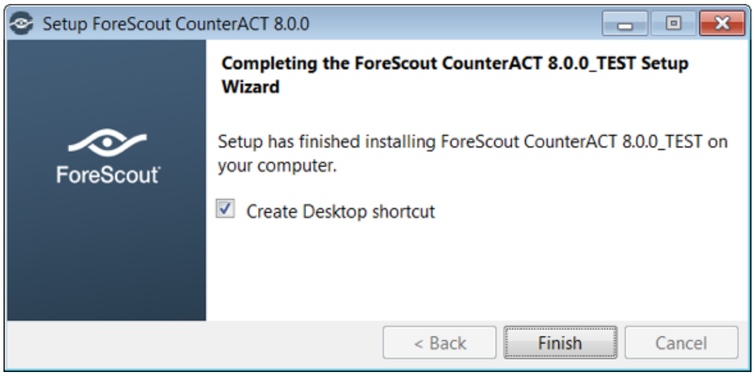
Installation Directory

Please specify the directory where ForeScout CounterACT will be installed.

Installation Directory C:\Users\test\ForeScout CounterACT 8.0.0

6. Click **Next.**

7. The installation begins. When completed, click **Finish.**

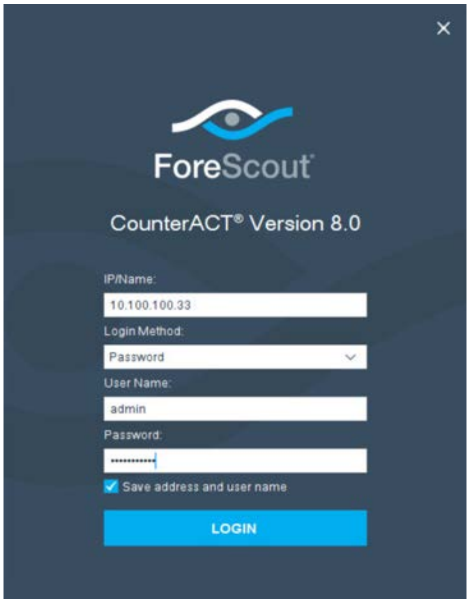


Completing the ForeScout CounterACT 8.0.0_TEST Setup Wizard

Setup has finished installing ForeScout CounterACT 8.0.0_TEST on your computer.

☑ Create Desktop shortcut

8. Connect to the Enterprise Manager with the Console and the password used during the CounterACT Enterprise Manager installation.



IP/Name: 10.100.100.33

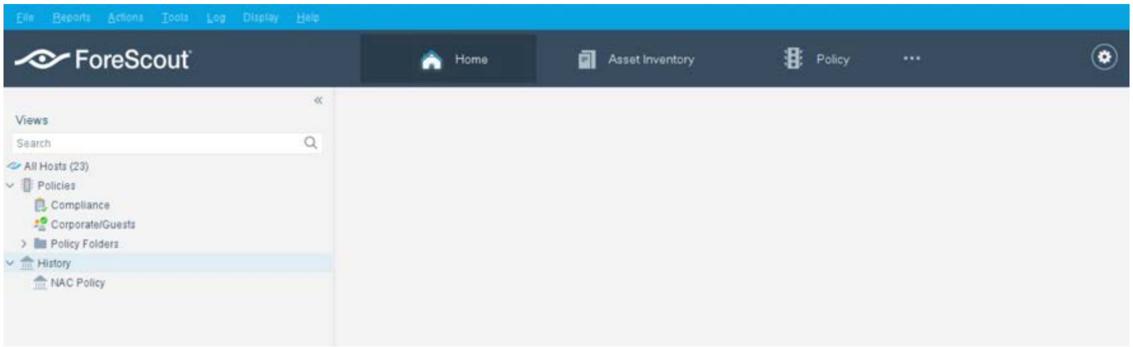
Login Method: Password

User Name: admin

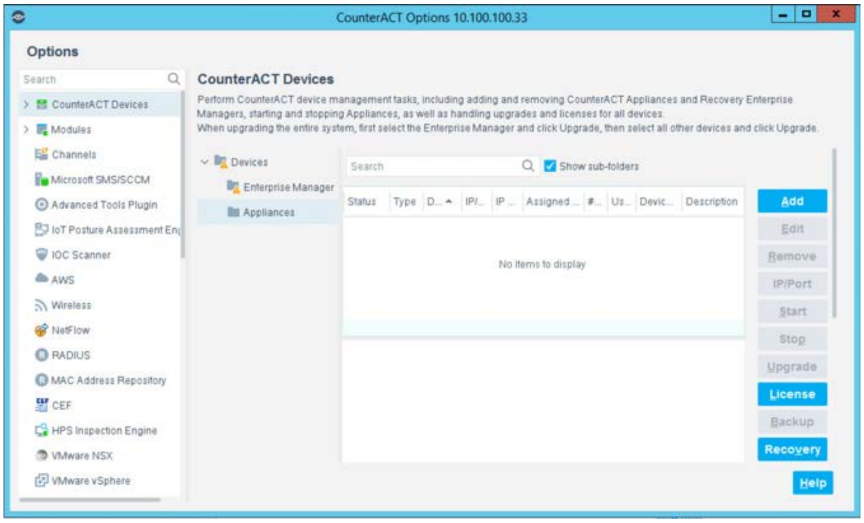
Password: ••••••••••

☑ Save address and user name

9. Select the gear icon in the top right of console.



10. Select **Add.**



CounterACT Options 10.100.100.33

CounterACT Devices

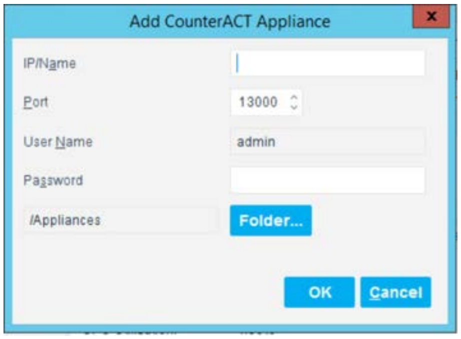
Perform CounterACT device management tasks, including adding and removing CounterACT Appliances and Recovery Enterprise Managers, starting and stopping Appliances, as well as handling upgrades and licenses for all devices.
When upgrading the entire system, first select the Enterprise Manager and click Upgrade, then select all other devices and click Upgrade.

☑ Show sub-folders

No items to display

11. Enter the internet protocol (IP) address of the appliance, and the admin password used in setup.

12. Select **OK.**



Add CounterACT Appliance

IP/Name

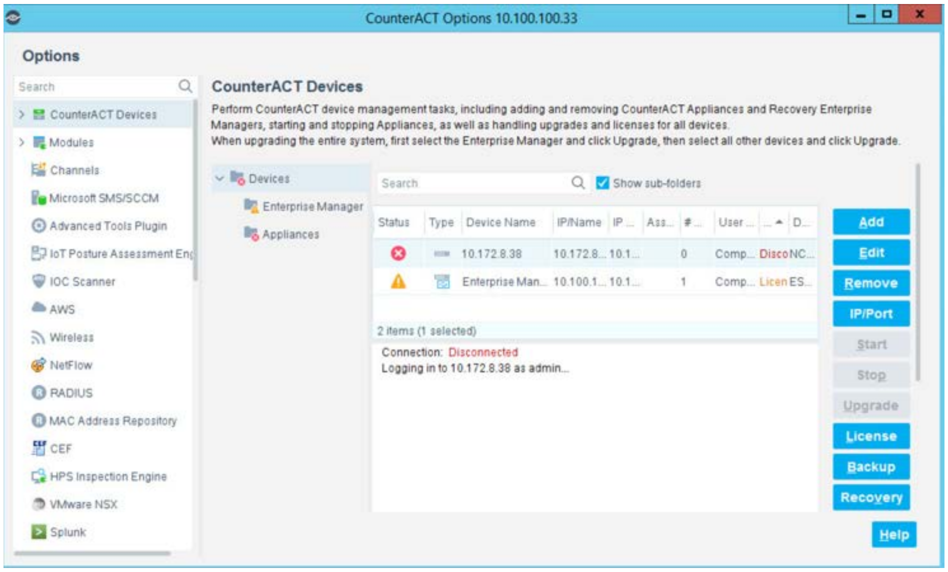
Port 13000

User Name admin

Password

/Appliances

13. Highlight the new appliance, and select **License.**



CounterACT Devices

Perform CounterACT device management tasks, including adding and removing CounterACT Appliances and Recovery Enterprise Managers, starting and stopping Appliances, as well as handling upgrades and licenses for all devices.
When upgrading the entire system, first select the Enterprise Manager and click Upgrade, then select all other devices and click Upgrade.

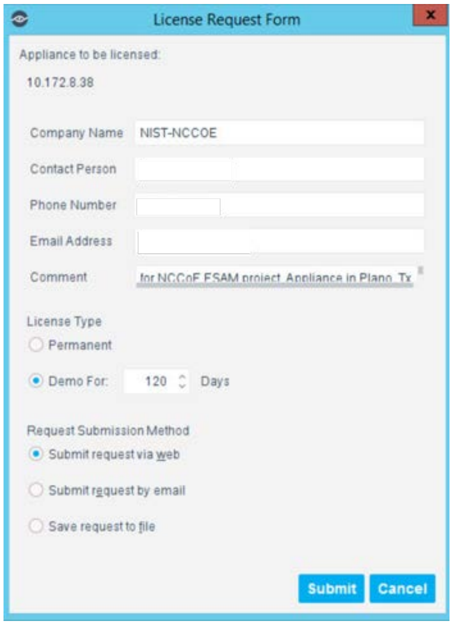
☑ Show sub-folders

Status	Type	Device Name	IP/Name	IP ...	Ass...	# ...	User ...	... ▲	D...
☒		10.172.8.38	10.172.8...	10.1...		0	Comp...	Disco	NC...
⚠		Enterprise Man...	10.100.1...	10.1...		1	Comp...	Licen	ES...

2 items (1 selected)

Connection: Disconnected
Logging in to 10.172.8.38 as admin...

14. Enter the required information. Select **Submit.**



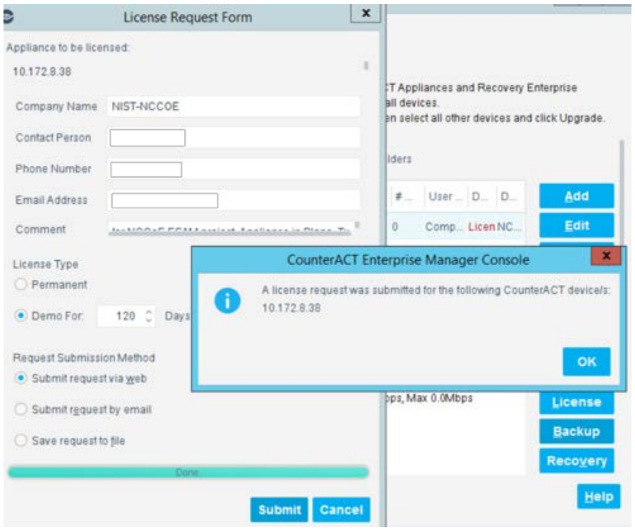
Appliance to be licensed:
10.172.8.38

Company Name NIST-NCCOE
Contact Person
Phone Number
Email Address
Comment for NCCoE ESAM project Appliance in Plano, Tx

License Type
○ Permanent
● Demo For: 120 Days

Request Submission Method
● Submit request via web
○ Submit request by email
○ Save request to file

15. Select **OK.**



Appliance to be licensed:
10.172.8.38

Company Name: NIST-NCCOE

Contact Person:

Phone Number:

Email Address:

Comment:

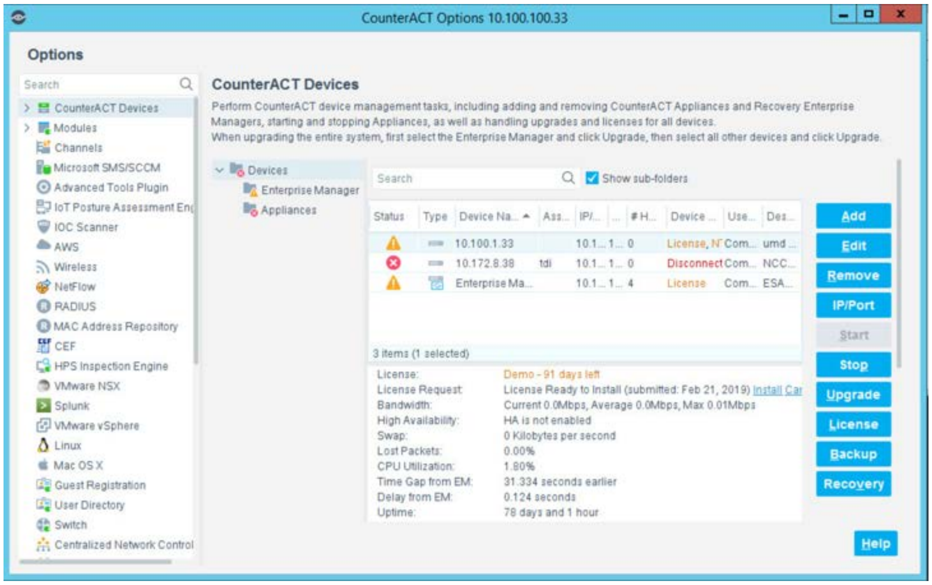
License Type
○ Permanent
● Demo For: 120 Days

Request Submission Method
● Submit request via web
○ Submit request by email
○ Save request to file

A license request was submitted for the following CounterACT device/s:
10.172.8.38

2.2.1.4.1 Appliance Interfaces Configurations

1. Under **Options**, highlight the appliance, and select **Edit.**



CounterACT Devices

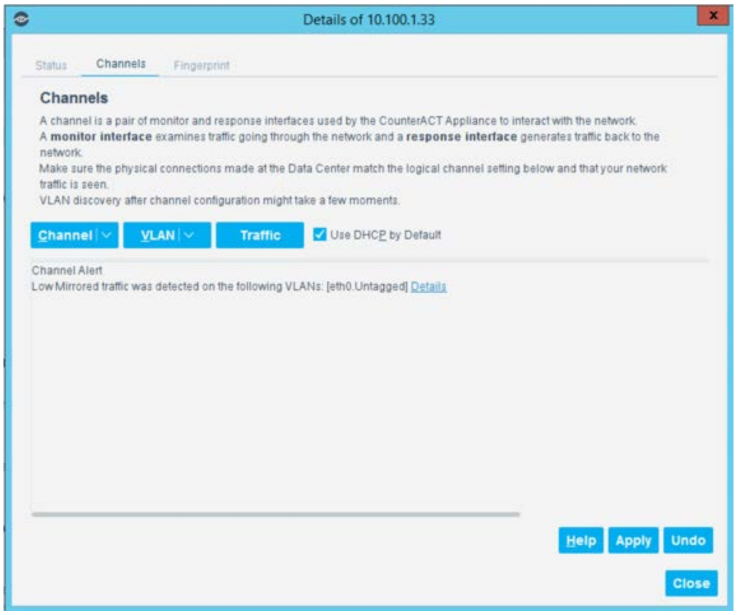
Perform CounterACT device management tasks, including adding and removing CounterACT Appliances and Recovery Enterprise Managers, starting and stopping Appliances, as well as handling upgrades and licenses for all devices.
When upgrading the entire system, first select the Enterprise Manager and click Upgrade, then select all other devices and click Upgrade.

Status	Type	Device Na...	Ass...	IP/...	...	# H...	Device ...	Use...	Des...
⚠		10.100.1.33		10.1... 1...		0	License, N	Com...	umd ...
⊗		10.172.8.38	tdi	10.1... 1...		0	Disconnect	Com...	NCC...
⚠		Enterprise Ma...		10.1... 1...		4	License	Com...	ESA...

3 items (1 selected)

License:	Demo - 91 days left
License Request:	License Ready to Install (submitted: Feb 21, 2019) Install Ca
Bandwidth:	Current 0.0Mbps, Average 0.0Mbps, Max 0.01Mbps
High Availability:	HA is not enabled
Swap:	0 Kilobytes per second
Lost Packets:	0.00%
CPU Utilization:	1.80%
Time Gap from EM:	31.334 seconds earlier
Delay from EM:	0.124 seconds
Uptime:	78 days and 1 hour

2. Select the **Channels** tab.



Details of 10.100.1.33

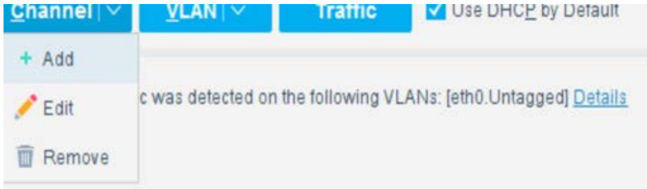
Channels

A channel is a pair of monitor and response interfaces used by the CounterACT Appliance to interact with the network.
A **monitor interface** examines traffic going through the network and a **response interface** generates traffic back to the network.
Make sure the physical connections made at the Data Center match the logical channel setting below and that your network traffic is seen.
VLAN discovery after channel configuration might take a few moments.

☑ Use DHCP by Default

Channel Alert
Low Mirrored traffic was detected on the following VLANs: [eth0.Untagged] Details

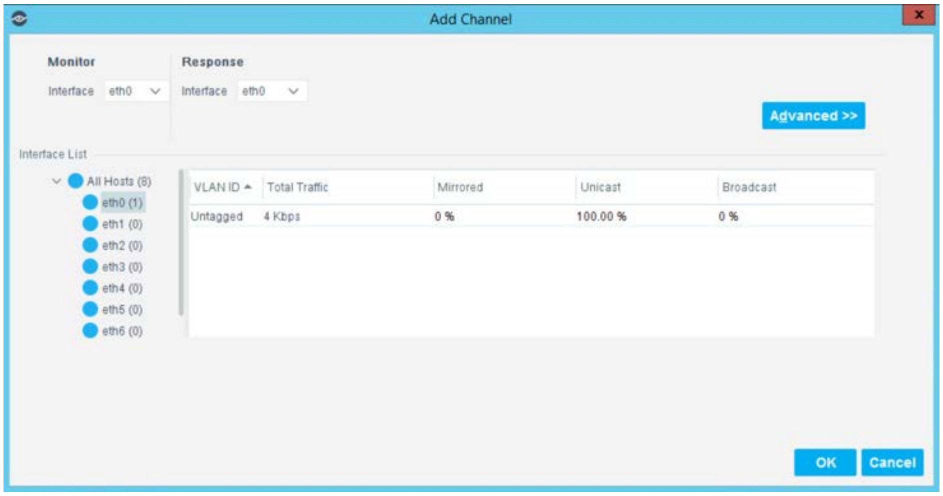
3. Under **Channel,** select **Add.**



☑ Use DHCP by Default

c was detected on the following VLANs: [eth0.Untagged] Details

4. Use the drop-down to select the interface listening on a switched port analyzer (SPAN) switch for both **Monitor** and **Response.** Select **OK.**



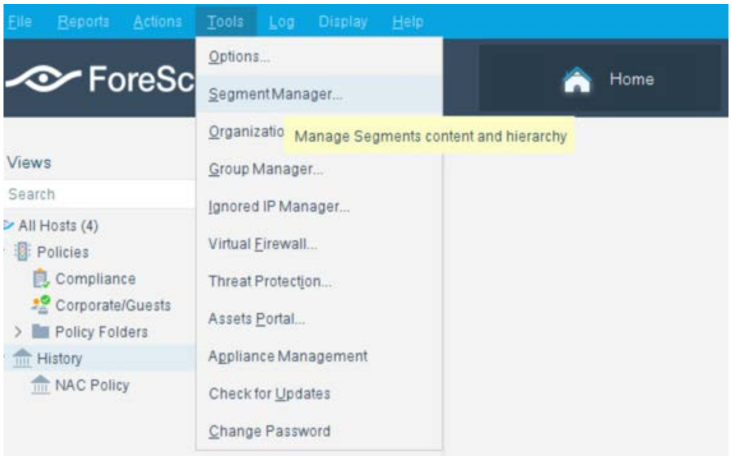
Add Channel

Monitor
Interface: eth0

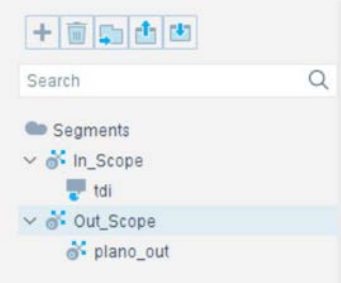
Response
Interface: eth0

VLAN ID	Total Traffic	Mirrored	Unicast	Broadcast
Untagged	4 Kbps	0 %	100.00 %	0 %

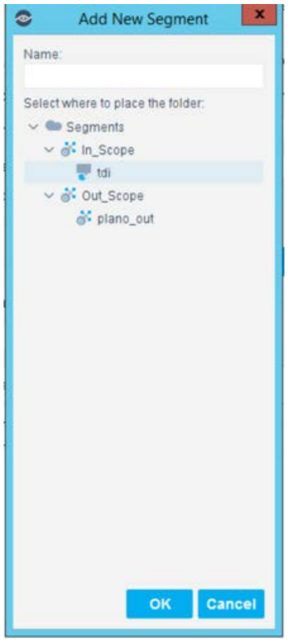
5. Under **Tools,** select **Segment Manager.**



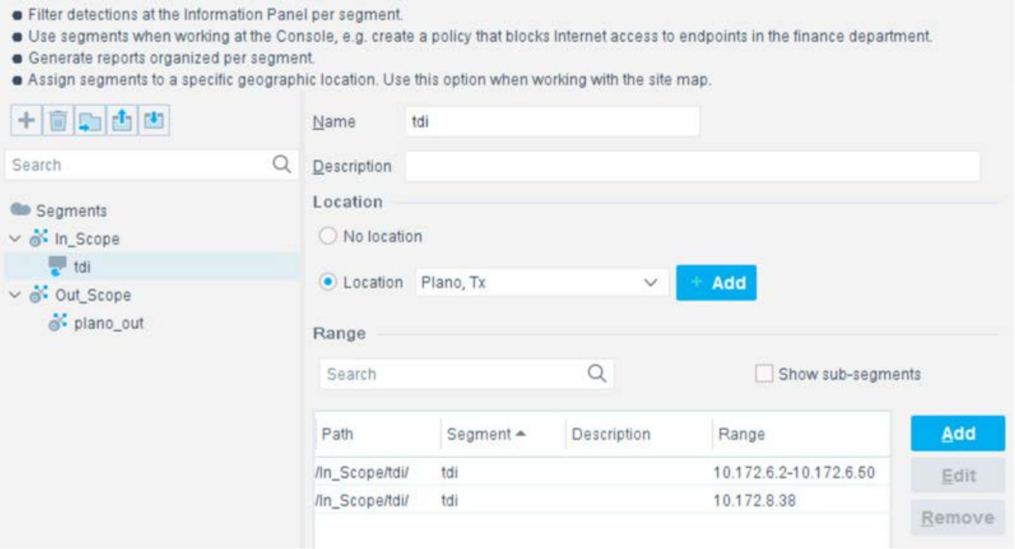
6. Select the **+** to add and name two segments called *In_Scope* and *Out_Scope*. Click **OK.** These will indicate which IP range should be scanned and which should not be scanned.



7. Select the plus icon again to add two subsegments shown in the screenshot below. Click **OK.**



8. Highlight the *tdi* segment. Click **Add** to add the range of IP addresses to scan. Click **OK.**



- Filter detections at the Information Panel per segment.
- Use segments when working at the Console, e.g. create a policy that blocks Internet access to endpoints in the finance department.
- Generate reports organized per segment.
- Assign segments to a specific geographic location. Use this option when working with the site map.

Name: tdi

Description:

Location

○ No location

● Location: Plano, Tx

Range

Path	Segment	Description	Range
/In_Scope/tdi/	tdi		10.172.6.2-10.172.6.50
/In_Scope/tdi/	tdi		10.172.8.38

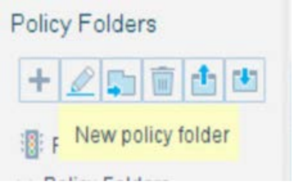
9. Repeat for the *plano_out* segment for IP address to not scan. Click **OK.**

2.2.1.4.2 Upload Network Scan Policies

Forescout network scan policies are prewritten and delivered as an XML file.

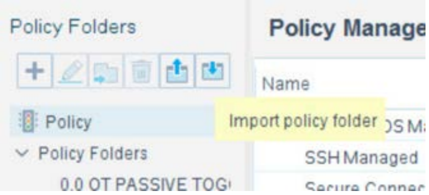
1. First, create a folder to house the polices. From the **Enterprise Manager** Console, select the **Policy** tab.

2. Select the plus icon to create a new folder.

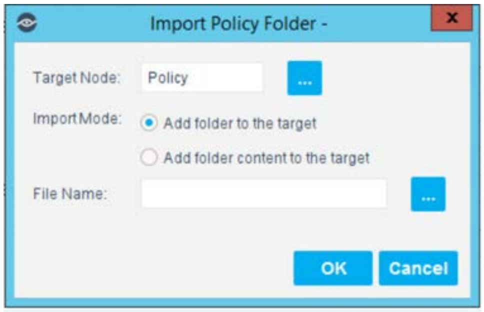
   

3. Name the folder. Click **OK.**

4. Select the **import policy** icon.

5. Select **…** to locate the XML file.

   Target Node: Policy

   Import Mode: ● Add folder to the target
   ○ Add folder content to the target

   File Name:

6. Select the XML file.

7. Select **OK.**

8. Repeat Steps 4 to 7 for each XML policy file.

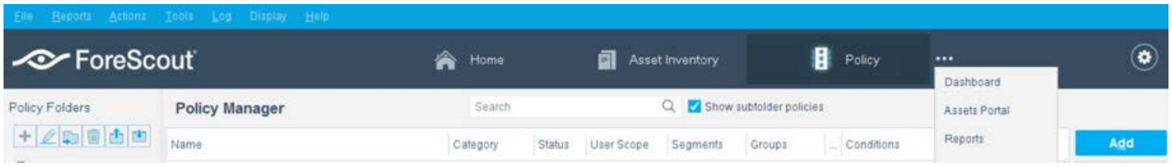
9. Select **Start.** Select **Apply** to start and apply the changes.

2.2.1.4.3 Splunk Integration

To complete Forescout Integration with Splunk, follow Forescout documentation found at https://www.forescout.com/platform/forescout-app-guide-splunk-2-7-0 and https://www.forescout.com/company/resources/extended-module-for-splunk-configuration-guide-2-8/.

2.2.1.4.4 Schedule Reporting

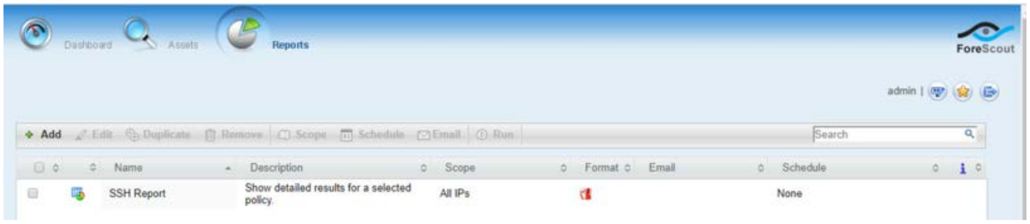
1. From the **Enterprise Manager** Console, select the ellipsis next to **Policy.** Select **Reports.**



2. Log in using the same credentials as the **Enterprise Manager** Console.

3. Select **Reports.**

4. Select **Add.**



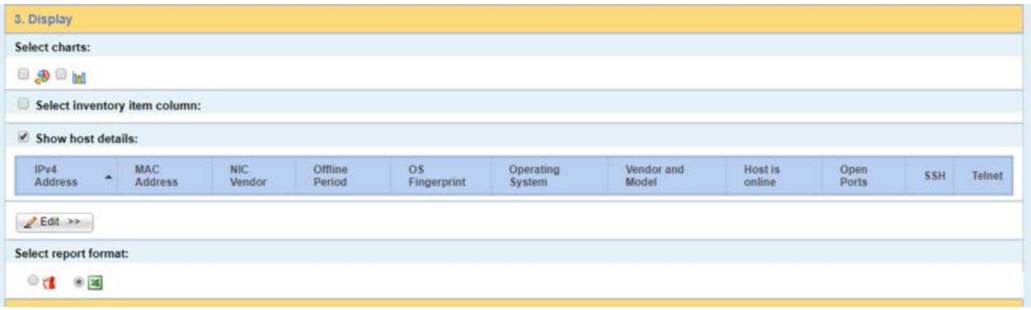
□		Name	Description	Scope	Format	Email	Schedule
□		SSH Report	Show detailed results for a selected policy.	All IPs			None

5. Select the **Asset Inventory** template. Click **Next.**

6. Name the report. Select the **All IPs** toggle**.**

7. Select only the **Show host details.**

8. Edit the host details to show the following properties:



☑ Show host details:

IPv4 Address	MAC Address	NIC Vendor	Offline Period	OS Fingerprint	Operating System	Vendor and Model	Host is online	Open Ports	SSH	Telnet

9. Set a schedule. Enter an email address. Select **Save.**

2.2.2 CounterACT Appliance Configuration

2.2.2.1 Host Configuration

The CounterACT Appliance is delivered on a Dell PowerEdge R640 server with version 8.0.0.

2.2.2.2 Network

Network Configuration (Interface 1):

- IPv4: Manual
- IPv6: disabled
- IPv4 address: 10.172.8.38
- Netmask: 255.255.255.0
- Gateway: 10.172.8.1

2.2.2.3 Installation

To install the CounterACT Appliance, follow the installation steps found at https://www.forescout.com/wp-content/uploads/2018/10/CounterACT_Installation_Guide_8.0.1.pdf.

2.2.2.4 Configuration

After the CounterACT Appliance is installed, follow the steps outlined in Section 2.2.1, to connect the appliance to the enterprise manager and complete the configuration.

2.3 Dragos Platform

The Dragos Platform is an industrial control system cybersecurity-monitoring platform based around threat-behavior analytics. It is being used in this build to provide asset discovery and monitoring. A Dragos Sitestore is installed at the NCCoE enterprise site, and a midpoint sensor is installed at the Plano site. The Dragos sensor is managed by the site store.

2.3.1 Dragos Sitestore Configuration

In the example implementation, Dragos Sitestore is deployed as a pre-built appliance from the vendor. The appliance was still configured with parameters necessary for our environment. Connect to the Dragos appliance by navigating the web browser to *https://<IP address>*.

2.3.1.1 Host Configuration

The Dragos Platform is delivered to the customer, preconfigured for the environment. The NCCoE received a Dell server utilizing iDRAC for virtualization. On the iDRAC server, VMware ESXi was installed and utilized for creating the server.

The VMs created to house the product have the following specifications:

- Operating system (OS) Version: CentOS 7 (64-bit)
- CPU: 48 cores

- Memory: 192 GB
- Hard disc drive (HDD) 1: 200 GB
- HDD 2: 10 terabytes (TB)

2.3.1.2 Network

Networking for the device included a single network within ESXi to which the VM was connected. The Dell iDRAC server housing the Dragos Sitestore Puppet Server was connected to the ESAM network with the following IP addresses:

- iDRAC: 10.100.200.6
- ESXi: 10.100.200.7
- Dragos Sitestore Puppet: 10.100.200.8

2.3.1.3 Installation

Installation began with setting up a VM. Utilizing the specifications in Section 2.3.1.1, Host Configuration, a VM was created for the Sitestore/Puppet server. Then the product ISO was added to the CD/DVD Drive 1 location (*DragosCustom-2019-06-18-CentOS-7-x86_64-Everything-1810.iso*).

1. Power on the VM, and open a console. The **Dragos installation** screen will start, allowing options to be selected for installation type.
2. With the Dell R730 server used for the NCCoE, select **Install Dragos Sitestore Kickstart.** The installer automatically installs the Dragos Platform without interaction from the user.

2.3.1.4 Configuration

Once the installation has completed, the Sitestore will be configured with the needed files listed in Table 2-1.

Table 2-1 Dragos Required Files

Dragos Files	
sitestore-orchestration-1.5.1.1-1.noarch.rpm.gpg	*midpoint-images-1.5.1.1-1.x86_64.rpm.gpg*
midpoint-configs-1.5.1.1-1.x86_64.rpm.gpg	*midpoint-manager-1.1.2-1.el7.x86_64.rpm.gpg*
midpoint-1.5.1.1-1.x86_64.rpm.gpg	*mms-cli-1.1.0-1.x86_64.rpm.gpg*
upgrade-1.5.1-3.tar.gz.gpg	*containerd.io-1.2.0-3.el7.x86_64.rpm*
container-selinux-2.68-1.el7.noarch.rpm	*docker-ce-18.09.0-3.el7.x86_64.rpm*
docker-ce-cli-18.09.0-3.el7.x86_64.rpm	

1. Upload these files to the Sitestore VM in */var/opt/releases/.*

2. Change directory to */var/opt/releases/* and run the command `gpg --decrypt-file *.gpg`. Enter the password supplied from Dragos for the installation. This will create all the files required for the installation.

3. Change directory to */root/* and, as root user, run `./puppet_server_setup.sh`

2.3.2 Dragos Midpoint Sensor

Dragos Midpoint Sensor is also deployed as a pre-built appliance from the vendor. Options for the midpoint sensor consist of configurations for small, medium, and large deployments. The appliance is configured with parameters necessary for our environment. The Dragos Midpoint Sensor can be managed from the Sitestore.

2.3.2.1 Network

The midpoint sensor has multiple interfaces. One interface will collect traffic via SPAN port. Another will serve as the management interface to communicate with the device.

Dragos Midpoint Sensor Management Interface:

- DHCP: disabled
- IPv6: ignore
- IPv4: Manual
- IPv4 address: 10.172.6.10
- Netmask: 255.255.255.0

2.3.2.2 Configuration

After the midpoint sensor is deployed and listening on the correct interface, the midpoint sensor can connect back to the Sitestore for further configurations.

2.3.3 Dragos Splunk Integration

The Dragos Splunk application allows data integration from the Dragos Sitestore into the Splunk dashboard. This allows Splunk to aggregate data from Dragos and other products into a central location for analyst visualization. This process assumes the reader has downloaded the Dragos Splunk application from https://splunkbase.splunk.com/app/4601/.

1. To begin, log in to the Splunk instance, and select the gear icon on the top left of the screen next to **Apps,** to configure the applications.

2. On the top right of the screen, select **Install app from the file.**

3. Follow the on-screen instructions to upload the downloaded application.
4. Restart Splunk (either prompted by the installation process or self-directed).
5. From the Splunk **Settings** menu on the top right, select the **Data Inputs** option.
6. Select **Add New** under **Local Inputs** for a transmission control protocol (TCP) listener. (User datagram protocol [UDP] is not recommended, because it will cut off longer messages.)
7. Set the port to the one that you want to transfer data on. (NCCoE build used **10514**.)
8. Select **Next** to configure the Input Settings.
9. Choose **dragos_alert** as the source type.
10. Set the **App Context** to **Dragos Splunk App.**
11. Set the **Index** to **dragos_alerts.** (Create a new index if it does not exist.)
12. Click **Submit.**

Once this process is completed, Splunk is ready to receive data from Dragos. The following instructions will be for configuring the Dragos Sitestore for sending information to Splunk:

1. Navigate to the **Servers** tab at https://<sitestore>/syslog/app/#/servers.
2. Click **+ Add Server** to create a new server.
3. Configure the connection information to point to the Splunk server configured previously.
4. Set the following options:
    a. Protocol: TCP
    b. Message Format: RFC 5424 Modern Syslog
    c. Message Delimiter: Use newline delimiter for TCP and transport layer security (TLS) streams.
5. Click **NEXT: SET TEMPLATE.**
6. Set the following value (must be on one line for Splunk to properly process) as **Message:**

```
{ "app": "dragos:platform", "body": "${content}", "category": "${summary}",
"created_at": "#{createdAt}", "dest": "${dest_asset_ip}",
"dest_dragos_id": "${dest_asset_id}", "dest_host":
"${dest_asset_hostname}", "dest_ip": "${dest_asset_ip}", "dest_mac":
"${dest_asset_mac}", "dest_name": "${dest_asset_domain}",
"dragos_detection_quad": "${detection_quad}", "dragos_detector_id":
"${detector_id}", "dvc": "${asset_ip}", "dvc_dragos_id":
"${dest_asset_id}", "dvc_host": "${dest_asset_hostname}", "dvc_ip":
"${asset_ip}", "dvc_mac": "${dest_asset_mac}", "dvc_name":
```

```
"${dest_asset_domain}", "id": "${id}", "ids_type": "network",
"occurred_at": "#{occurredAt}", "severity_id": "${severity}",
"signature": "${source}", "src": "${src_asset_ip}", "src_dragos_id":
"${src_asset_id}", "src_host": "${src_asset_hostname}", "src_ip":
"${src_asset_ip}", "src_mac": "${src_asset_mac}", "src_name":
"${src_asset_domain}", "subject": "${type}", "type": "alert",
"vendor_product": "Dragos Platform" }
```

7. Select **Save.**

2.4 FoxGuard Patch and Update Management Program

The solution utilizes the FoxGuard PUMP to provide patch availability and vulnerability notifications for identified assets. For this build, ConsoleWorks collects asset data from Splunk then converts that data into the JavaScript object notation (JSON) format required for PUMP. The resulting JSON file includes asset information such as vendor, product, and version, as well as serial and model information about devices from the asset inventory. Asset data often contains critical details. However, PUMP does not require sensitive data, such as asset location and IP address. The file is encrypted and provided to the PUMP team via secure delivery. FoxGuard's preferred method of file transfer is secure file transfer protocol and does not require direct access to an entities network.

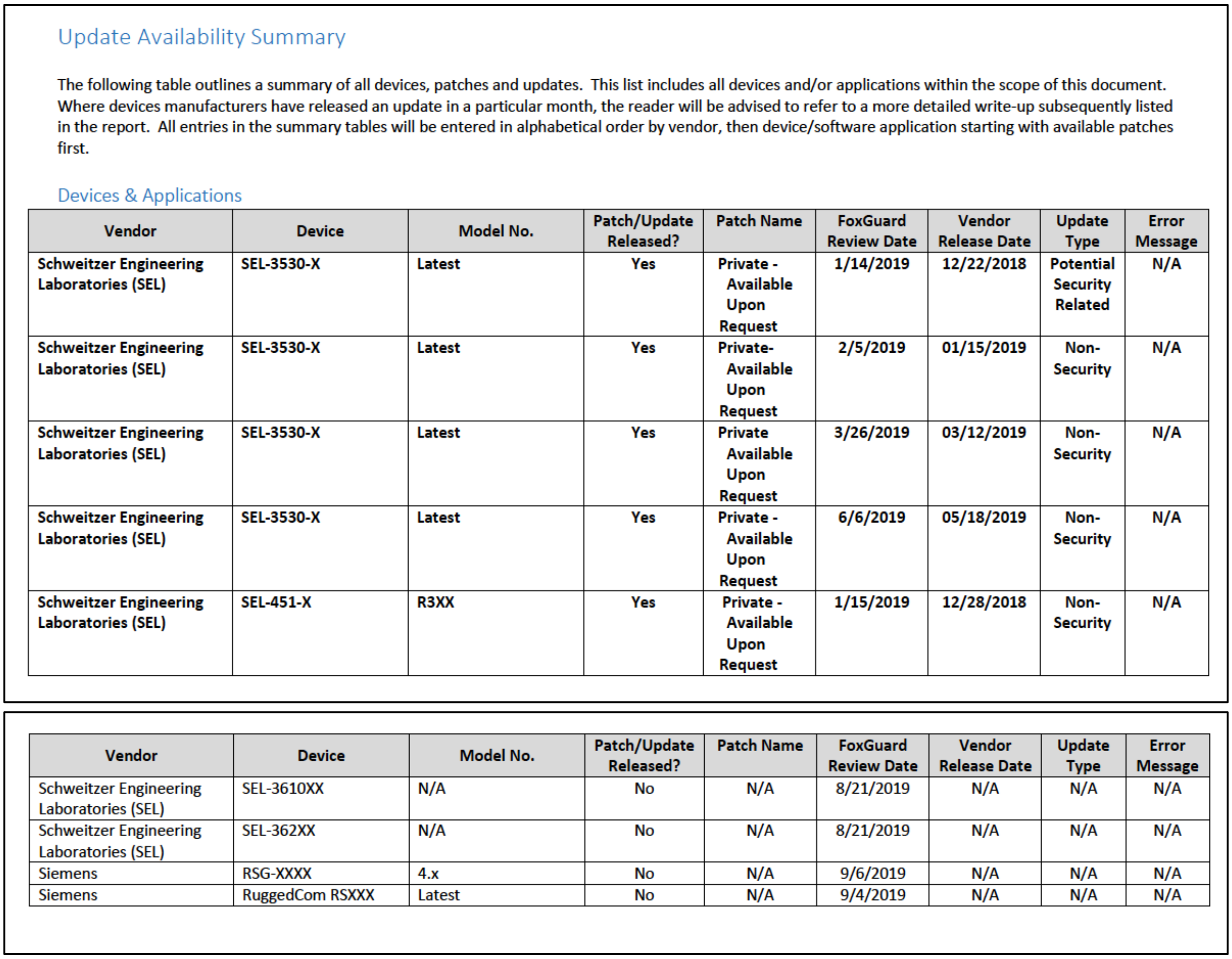
Once the asset data is received, the FoxGuard team analyzes the file for completeness. Any missing data, such as a serial number, version, or access to private patch data, is collected during the onboarding process with the end user. The final report is provided back to ConsoleWorks in a JSON file format and includes available patches and vulnerability notifications for each device. The data is then ingested back into Splunk for viewing and reporting. Reports are also available outside of the ConsoleWorks integration in portable document format (PDF) and comma separated value (CSV) format.

PUMP is a service managed by the FoxGuard team. The patch availability and vulnerability notification report does not require an installation. See Section 2.1 for configuring ConsoleWorks to automatically create the required JSON input file for the integration described in this guide.

2.4.1 Patch Report

Below are screenshots from the final patch report for this build.

Figure 2-1 Update Availability Summary



Update Availability Summary

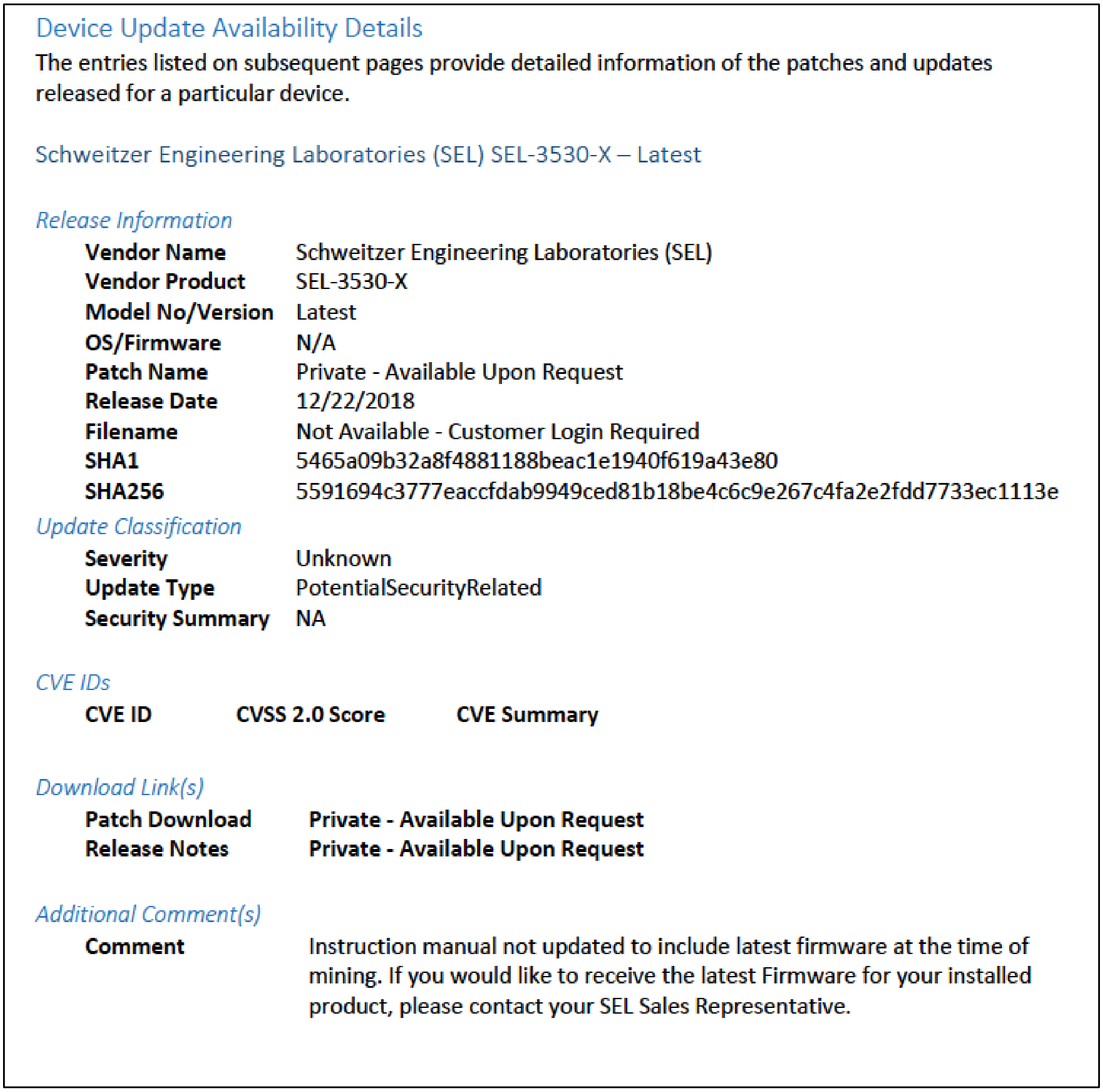
The following table outlines a summary of all devices, patches and updates. This list includes all devices and/or applications within the scope of this document. Where devices manufacturers have released an update in a particular month, the reader will be advised to refer to a more detailed write-up subsequently listed in the report. All entries in the summary tables will be entered in alphabetical order by vendor, then device/software application starting with available patches first.

Devices & Applications

Vendor	Device	Model No.	Patch/Update Released?	Patch Name	FoxGuard Review Date	Vendor Release Date	Update Type	Error Message
Schweitzer Engineering Laboratories (SEL)	**SEL-3530-X**	**Latest**	**Yes**	**Private - Available Upon Request**	**1/14/2019**	**12/22/2018**	**Potential Security Related**	**N/A**
Schweitzer Engineering Laboratories (SEL)	**SEL-3530-X**	**Latest**	**Yes**	**Private- Available Upon Request**	**2/5/2019**	**01/15/2019**	**Non-Security**	**N/A**
Schweitzer Engineering Laboratories (SEL)	**SEL-3530-X**	**Latest**	**Yes**	**Private Available Upon Request**	**3/26/2019**	**03/12/2019**	**Non-Security**	**N/A**
Schweitzer Engineering Laboratories (SEL)	**SEL-3530-X**	**Latest**	**Yes**	**Private - Available Upon Request**	**6/6/2019**	**05/18/2019**	**Non-Security**	**N/A**
Schweitzer Engineering Laboratories (SEL)	**SEL-451-X**	**R3XX**	**Yes**	**Private - Available Upon Request**	**1/15/2019**	**12/28/2018**	**Non-Security**	**N/A**

Vendor	Device	Model No.	Patch/Update Released?	Patch Name	FoxGuard Review Date	Vendor Release Date	Update Type	Error Message
Schweitzer Engineering Laboratories (SEL)	SEL-3610XX	N/A	No	N/A	8/21/2019	N/A	N/A	N/A
Schweitzer Engineering Laboratories (SEL)	SEL-362XX	N/A	No	N/A	8/21/2019	N/A	N/A	N/A
Siemens	RSG-XXXX	4.x	No	N/A	9/6/2019	N/A	N/A	N/A
Siemens	RuggedCom RSXXX	Latest	No	N/A	9/4/2019	N/A	N/A	N/A

Figure 2-2 Device Update Availability Details-1



Device Update Availability Details

The entries listed on subsequent pages provide detailed information of the patches and updates released for a particular device.

Schweitzer Engineering Laboratories (SEL) SEL-3530-X – Latest

Release Information

Vendor Name	Schweitzer Engineering Laboratories (SEL)
Vendor Product	SEL-3530-X
Model No/Version	Latest
OS/Firmware	N/A
Patch Name	Private - Available Upon Request
Release Date	12/22/2018
Filename	Not Available - Customer Login Required
SHA1	5465a09b32a8f4881188beac1e1940f619a43e80
SHA256	5591694c3777eaccfdab9949ced81b18be4c6c9e267c4fa2e2fdd7733ec1113e

Update Classification

Severity	Unknown
Update Type	PotentialSecurityRelated
Security Summary	NA

CVE IDs

CVE ID	**CVSS 2.0 Score**	**CVE Summary**

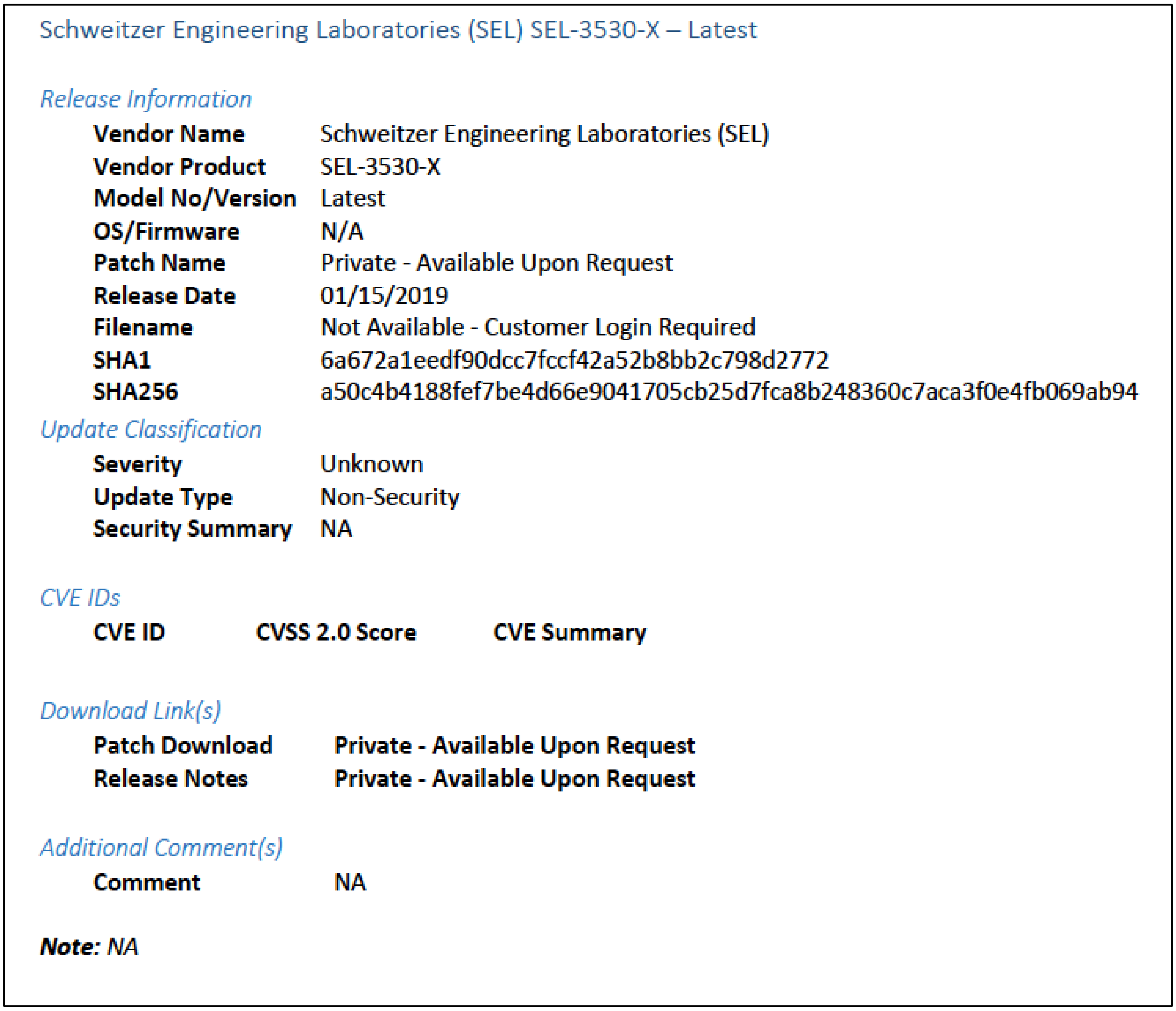
Download Link(s)

Patch Download	**Private - Available Upon Request**
Release Notes	**Private - Available Upon Request**

Additional Comment(s)

Comment	Instruction manual not updated to include latest firmware at the time of mining. If you would like to receive the latest Firmware for your installed product, please contact your SEL Sales Representative.

Figure 2-3 Device Update Availability Details-2



Schweitzer Engineering Laboratories (SEL) SEL-3530-X – Latest

Release Information

Vendor Name	Schweitzer Engineering Laboratories (SEL)
Vendor Product	SEL-3530-X
Model No/Version	Latest
OS/Firmware	N/A
Patch Name	Private - Available Upon Request
Release Date	01/15/2019
Filename	Not Available - Customer Login Required
SHA1	6a672a1eedf90dcc7fccf42a52b8bb2c798d2772
SHA256	a50c4b4188fef7be4d66e9041705cb25d7fca8b248360c7aca3f0e4fb069ab94

Update Classification

Severity	Unknown
Update Type	Non-Security
Security Summary	NA

CVE IDs

CVE ID	**CVSS 2.0 Score**	**CVE Summary**

Download Link(s)

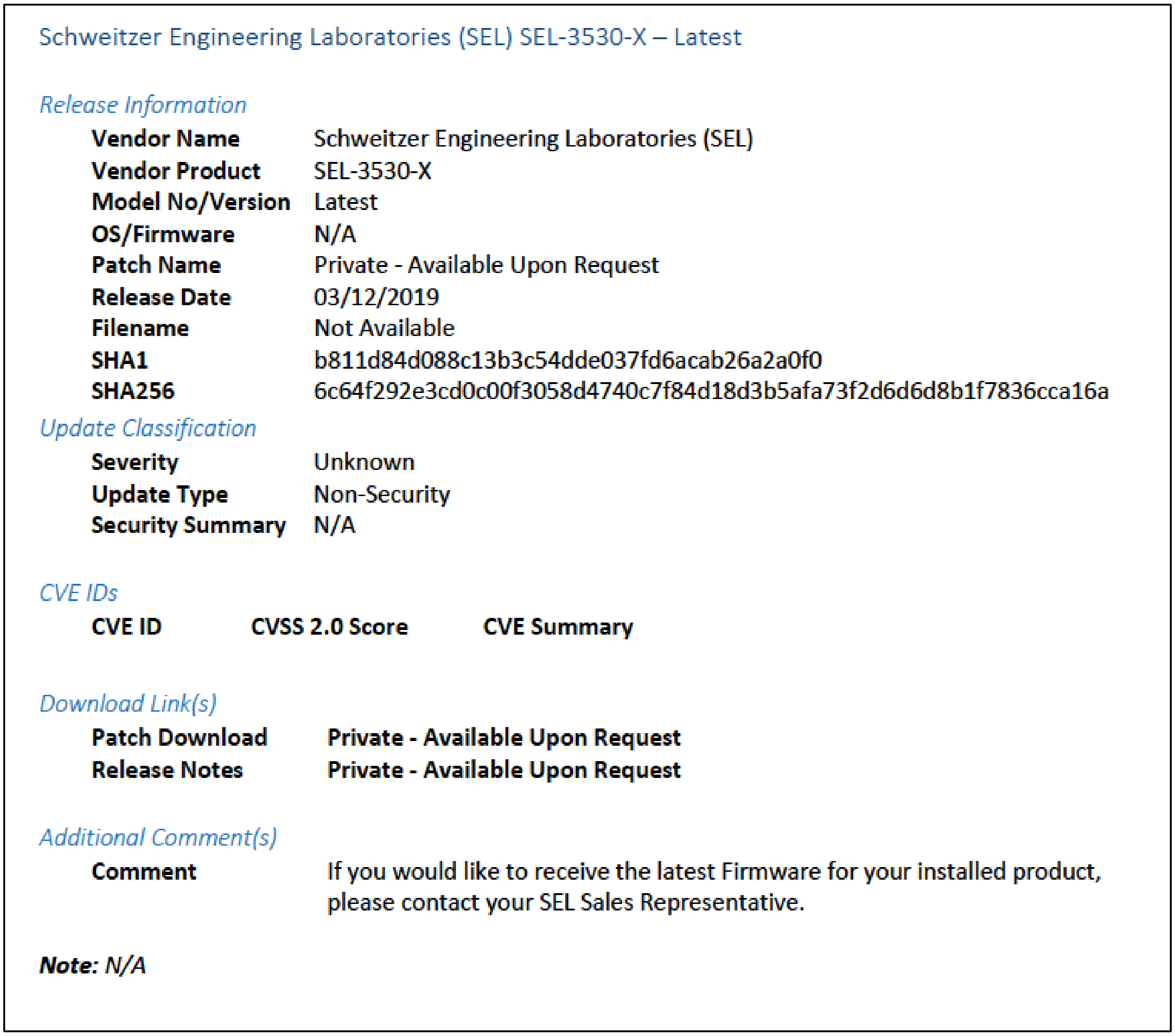
Patch Download	**Private - Available Upon Request**
Release Notes	**Private - Available Upon Request**

Additional Comment(s)

Comment	NA

***Note**: NA*

Figure 2-4 Device Update Availability Details-3



Schweitzer Engineering Laboratories (SEL) SEL-3530-X – Latest

Release Information

Vendor Name	Schweitzer Engineering Laboratories (SEL)
Vendor Product	SEL-3530-X
Model No/Version	Latest
OS/Firmware	N/A
Patch Name	Private - Available Upon Request
Release Date	03/12/2019
Filename	Not Available
SHA1	b811d84d088c13b3c54dde037fd6acab26a2a0f0
SHA256	6c64f292e3cd0c00f3058d4740c7f84d18d3b5afa73f2d6d6d8b1f7836cca16a

Update Classification

Severity	Unknown
Update Type	Non-Security
Security Summary	N/A

CVE IDs

CVE ID	CVSS 2.0 Score	CVE Summary

Download Link(s)

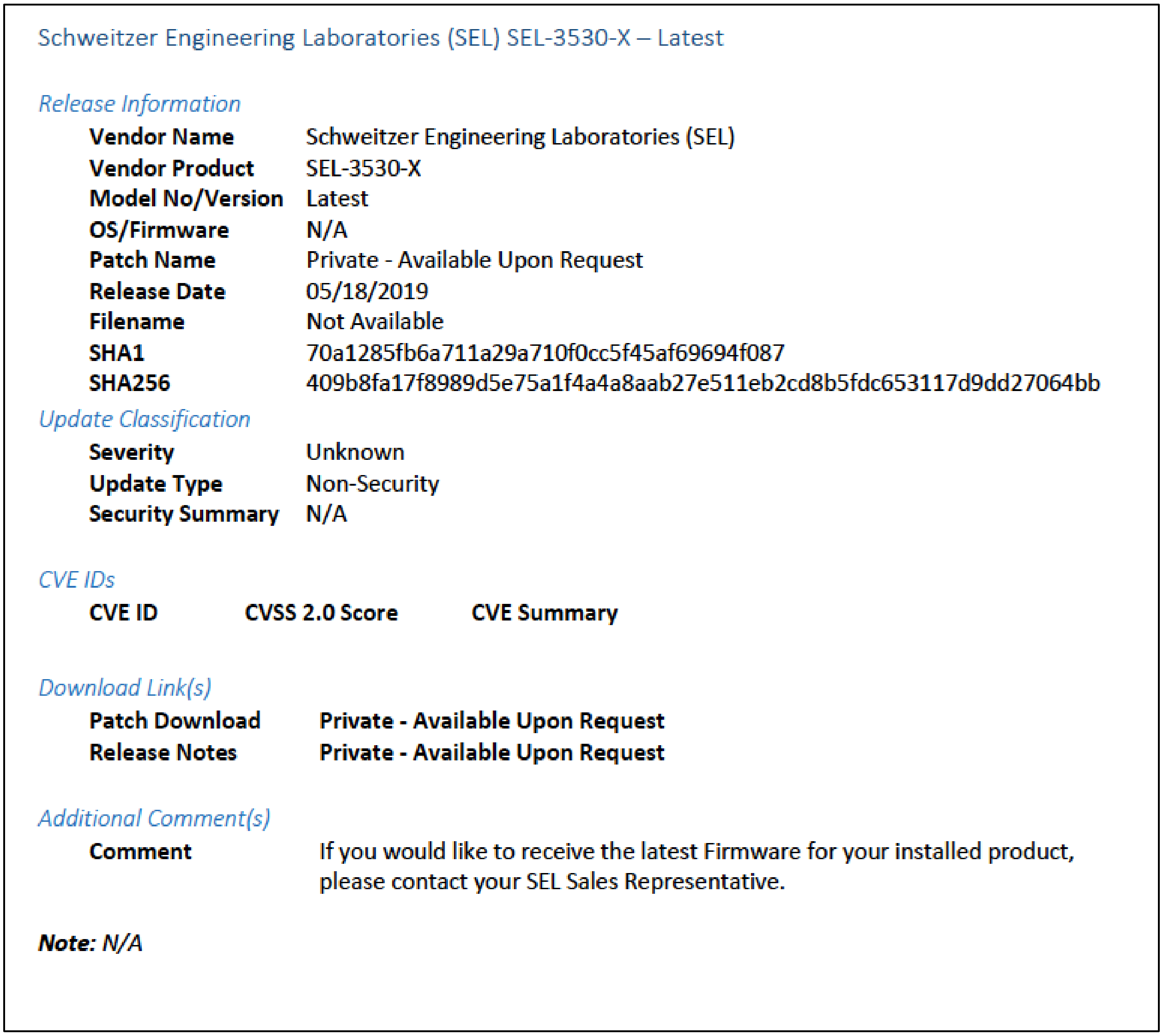
Patch Download	**Private - Available Upon Request**
Release Notes	**Private - Available Upon Request**

Additional Comment(s)

Comment	If you would like to receive the latest Firmware for your installed product, please contact your SEL Sales Representative.

Note: *N/A*

Figure 2-5 Device Update Availability Details-4



Schweitzer Engineering Laboratories (SEL) SEL-3530-X – Latest

Release Information

Vendor Name	Schweitzer Engineering Laboratories (SEL)
Vendor Product	SEL-3530-X
Model No/Version	Latest
OS/Firmware	N/A
Patch Name	Private - Available Upon Request
Release Date	05/18/2019
Filename	Not Available
SHA1	70a1285fb6a711a29a710f0cc5f45af69694f087
SHA256	409b8fa17f8989d5e75a1f4a4a8aab27e511eb2cd8b5fdc653117d9dd27064bb

Update Classification

Severity	Unknown
Update Type	Non-Security
Security Summary	N/A

CVE IDs

CVE ID	**CVSS 2.0 Score**	**CVE Summary**

Download Link(s)

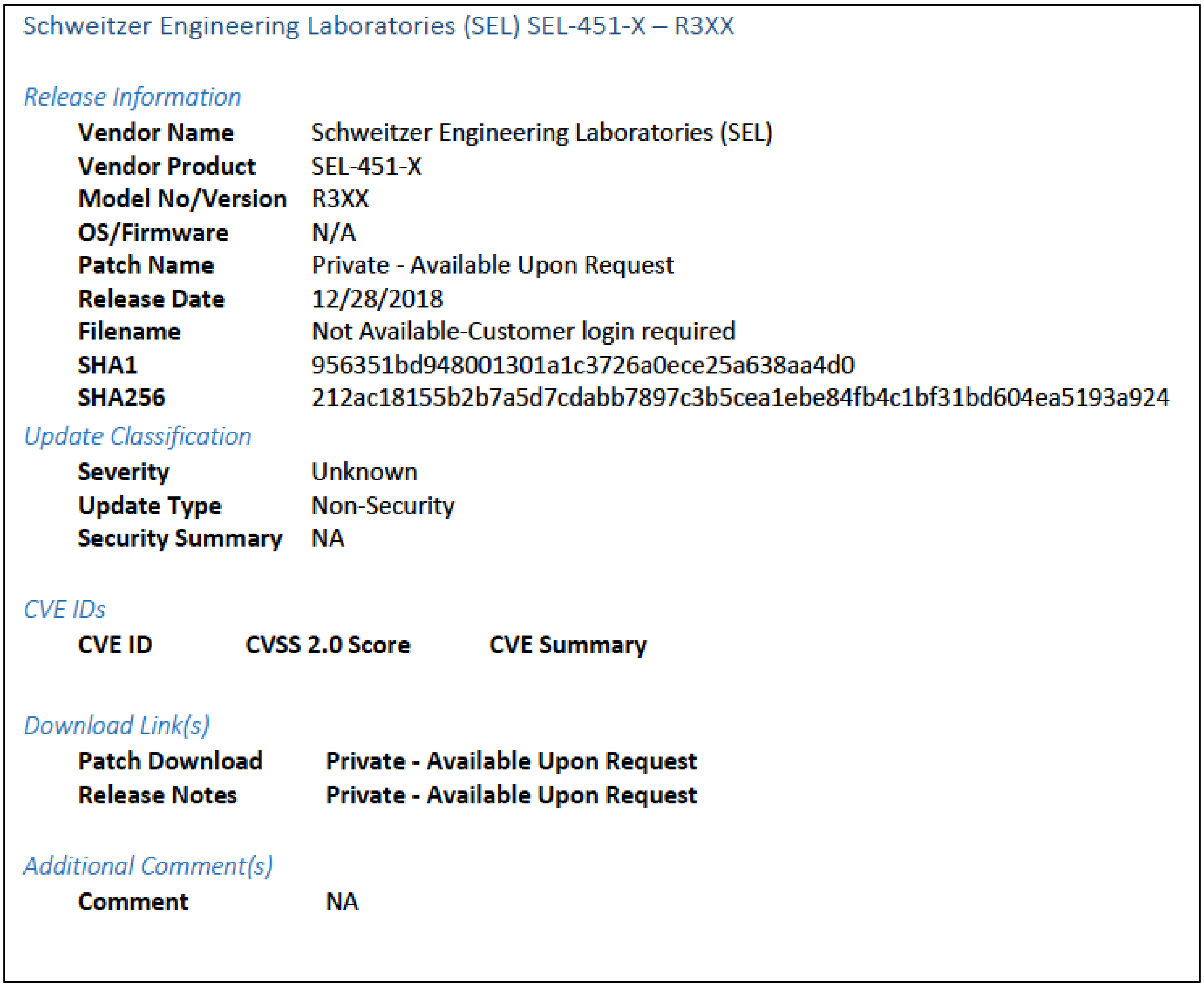
Patch Download	**Private - Available Upon Request**
Release Notes	**Private - Available Upon Request**

Additional Comment(s)

Comment	If you would like to receive the latest Firmware for your installed product, please contact your SEL Sales Representative.

Note: *N/A*

Figure 2-6 Device Update Availability Details-5



Schweitzer Engineering Laboratories (SEL) SEL-451-X – R3XX

Release Information

Vendor Name	Schweitzer Engineering Laboratories (SEL)
Vendor Product	SEL-451-X
Model No/Version	R3XX
OS/Firmware	N/A
Patch Name	Private - Available Upon Request
Release Date	12/28/2018
Filename	Not Available-Customer login required
SHA1	956351bd948001301a1c3726a0ece25a638aa4d0
SHA256	212ac18155b2b7a5d7cdabb7897c3b5cea1ebe84fb4c1bf31bd604ea5193a924

Update Classification

Severity	Unknown
Update Type	Non-Security
Security Summary	NA

CVE IDs

CVE ID	**CVSS 2.0 Score**	**CVE Summary**

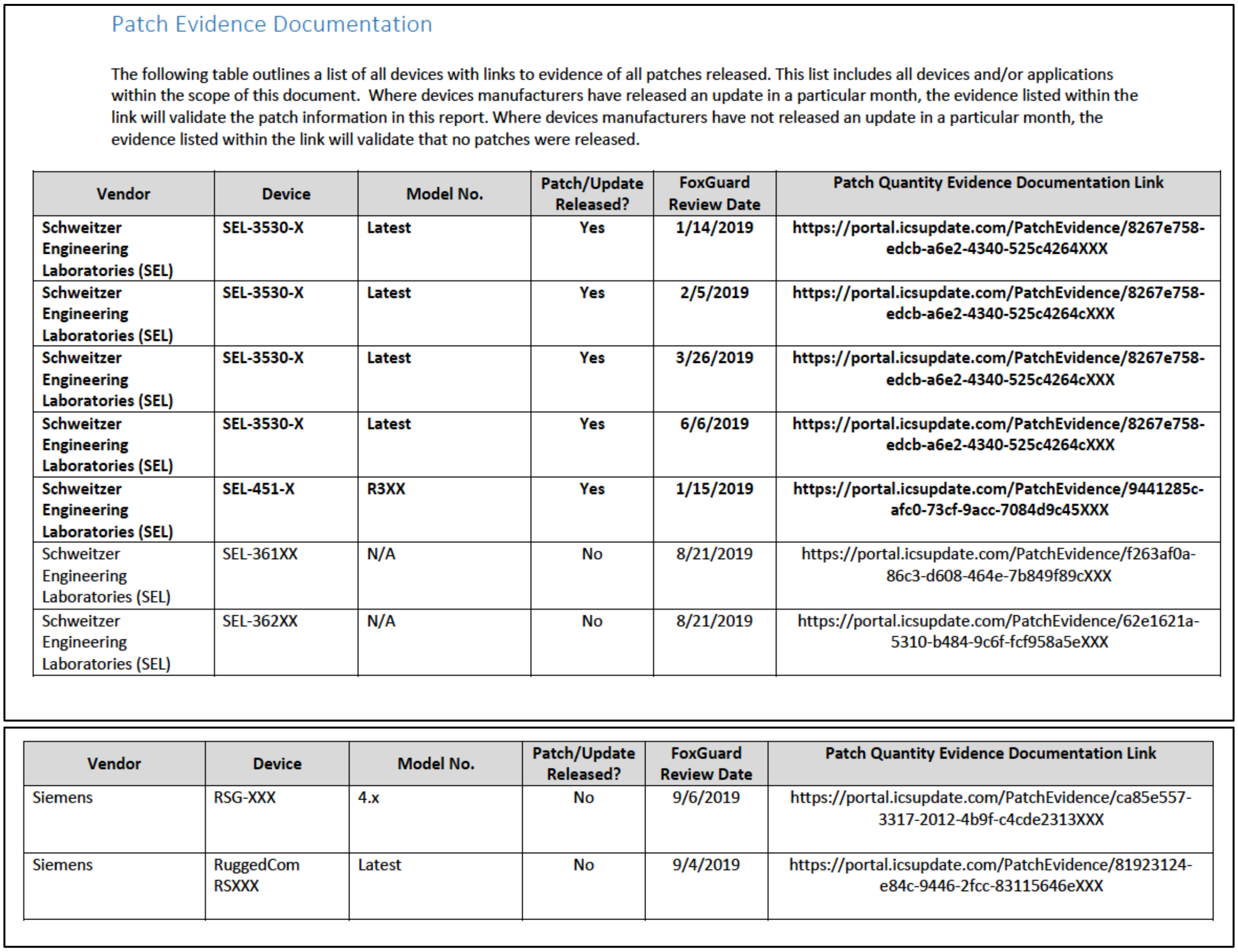
Download Link(s)

Patch Download	**Private - Available Upon Request**
Release Notes	**Private - Available Upon Request**

Additional Comment(s)

Comment	NA

Figure 2-7 Patch Evidence Documentation



Patch Evidence Documentation

The following table outlines a list of all devices with links to evidence of all patches released. This list includes all devices and/or applications within the scope of this document. Where devices manufacturers have released an update in a particular month, the evidence listed within the link will validate the patch information in this report. Where devices manufacturers have not released an update in a particular month, the evidence listed within the link will validate that no patches were released.

Vendor	Device	Model No.	Patch/Update Released?	FoxGuard Review Date	Patch Quantity Evidence Documentation Link
Schweitzer Engineering Laboratories (SEL)	**SEL-3530-X**	**Latest**	**Yes**	**1/14/2019**	**https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264XXX**
Schweitzer Engineering Laboratories (SEL)	**SEL-3530-X**	**Latest**	**Yes**	**2/5/2019**	**https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX**
Schweitzer Engineering Laboratories (SEL)	**SEL-3530-X**	**Latest**	**Yes**	**3/26/2019**	**https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX**
Schweitzer Engineering Laboratories (SEL)	**SEL-3530-X**	**Latest**	**Yes**	**6/6/2019**	**https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX**
Schweitzer Engineering Laboratories (SEL)	**SEL-451-X**	**R3XX**	**Yes**	**1/15/2019**	**https://portal.icsupdate.com/PatchEvidence/9441285c-afc0-73cf-9acc-7084d9c45XXX**
Schweitzer Engineering Laboratories (SEL)	SEL-361XX	N/A	No	8/21/2019	https://portal.icsupdate.com/PatchEvidence/f263af0a-86c3-d608-464e-7b849f89cXXX
Schweitzer Engineering Laboratories (SEL)	SEL-362XX	N/A	No	8/21/2019	https://portal.icsupdate.com/PatchEvidence/62e1621a-5310-b484-9c6f-fcf958a5eXXX

Vendor	Device	Model No.	Patch/Update Released?	FoxGuard Review Date	Patch Quantity Evidence Documentation Link
Siemens	RSG-XXX	4.x	No	9/6/2019	https://portal.icsupdate.com/PatchEvidence/ca85e557-3317-2012-4b9f-c4cde2313XXX
Siemens	RuggedCom RSXXX	Latest	No	9/4/2019	https://portal.icsupdate.com/PatchEvidence/81923124-e84c-9446-2fcc-83115646eXXX

2.5 Kore Wireless

This solution leverages a Kore Wireless virtual private network (VPN) to provide secure remote access to remote assets. In this case, the remote asset is an Obvius A8812 Data Acquisition Server that provides access to data from a Yokogawa flow meter.

Note: Some network information is excluded for security.

2.5.1 Bridge Configuration

2.5.1.1 Installation

1. Connect the MultiConnect eCell Ethernet port to the Ethernet port on the Obvius A8812 Data Acquisition Server.

2. Connect the Obvius A8812 RS485 to the multidrop Modbus network with the remote steam meter asset.

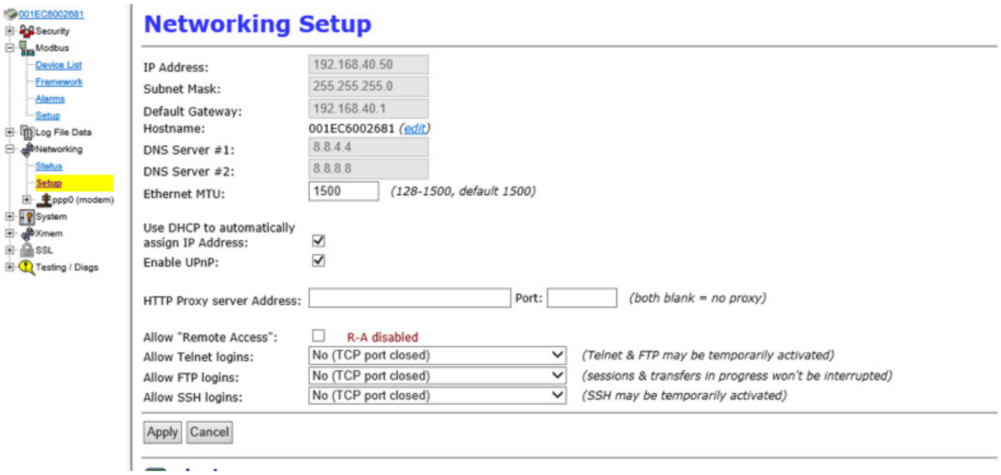
2.5.1.2 Network

1. Set Obvius A8812 to **DHCP.**

    a. Navigate the IP address of the Obvius A8812. Default is *192.168.40.50*.

    b. Open the **Networking** drop-down menu, and select **Setup**.

    c. Check the **Use DHCP to automatically assign IP Address** checkbox.



Networking Setup

IP Address: 192.168.40.50
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.40.1
Hostname: 001EC6002681 *(edit)*
DNS Server #1: 8.8.4.4
DNS Server #2: 8.8.8.8
Ethernet MTU: 1500 *(128-1500, default 1500)*

Use DHCP to automatically assign IP Address: ☑
Enable UPnP: ☑

HTTP Proxy server Address: Port: *(both blank = no proxy)*

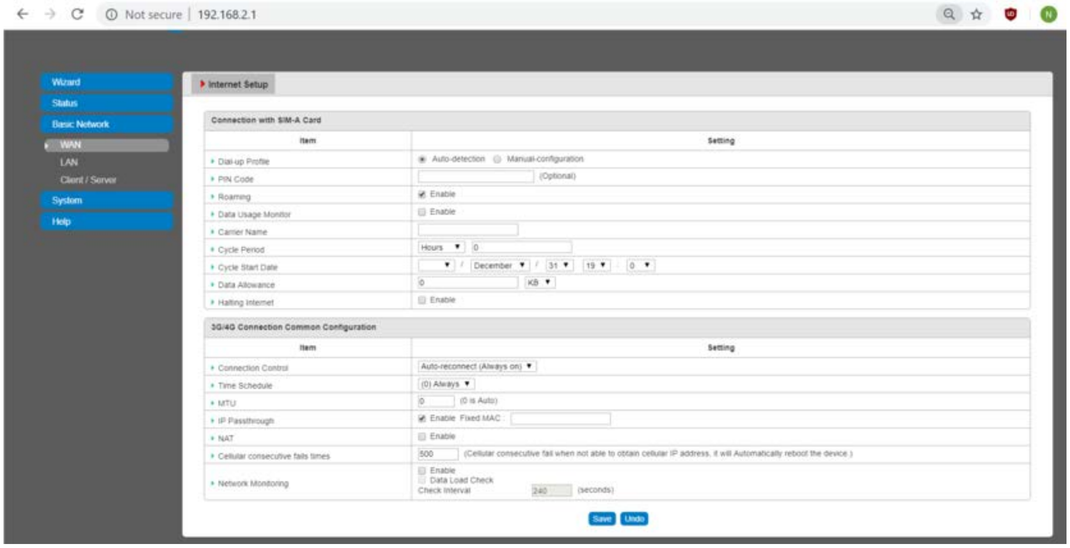
Allow "Remote Access": ☐ R-A disabled
Allow Telnet logins: No (TCP port closed) *(Telnet & FTP may be temporarily activated)*
Allow FTP logins: No (TCP port closed) *(sessions & transfers in progress won't be interrupted)*
Allow SSH logins: No (TCP port closed) *(SSH may be temporarily activated)*

2. Set MultiConnect eCell to Auto-detect Dialup profiles.

    a. Navigate the IP address of the MultiConnect eCell. Default is *192.168.40.50*.

    b. Open the **WAN** menu.

c. Set the Dial-up Profile to **Auto-detection.**



Connection with SIM-A Card

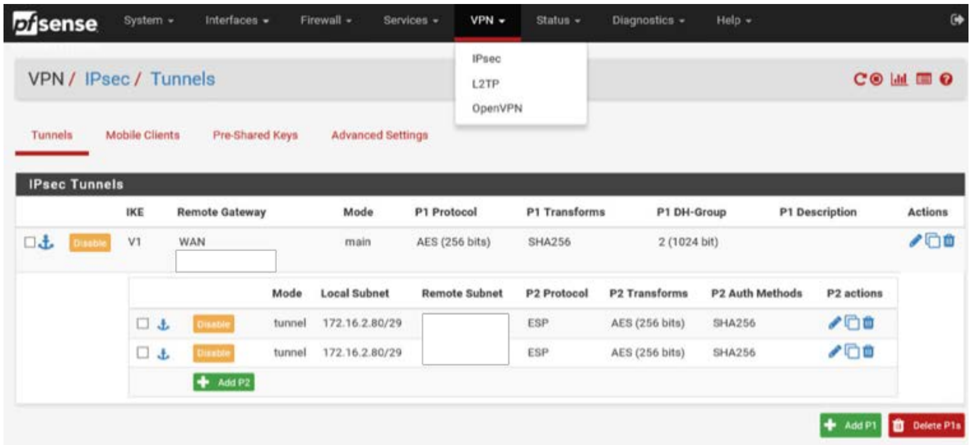
Item	Setting
Dial-up Profile	● Auto-detection ○ Manual-configuration
PIN Code	(Optional)
Roaming	☑ Enable
Data Usage Monitor	□ Enable
Carrier Name	
Cycle Period	Hours ▼ 0
Cycle Start Date	▼ / December ▼ / 31 ▼ 19 ▼ : 0 ▼
Data Allowance	0 KB ▼
Halting Internet	□ Enable

3G/4G Connection Common Configuration

Item	Setting
Connection Control	Auto-reconnect (Always on) ▼
Time Schedule	(0) Always ▼
MTU	0 (0 is Auto)
IP Passthrough	☑ Enable Fixed MAC :
NAT	□ Enable
Cellular consecutive fails times	500 (Cellular consecutive fail when not able to obtain cellular IP address, it will Automatically reboot the device)
Network Monitoring	□ Enable □ Data Load Check Check Interval 240 (seconds)

2.5.2 Virtual Private Network Configuration

1. Navigate to **VPN > IPsec** in pfsense.



IPsec Tunnels

		IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
□	Disable	V1	WAN	main	AES (256 bits)	SHA256	2 (1024 bit)		

		Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 actions
□	Disable	tunnel	172.16.2.80/29		ESP	AES (256 bits)	SHA256	
□	Disable	tunnel	172.16.2.80/29		ESP	AES (256 bits)	SHA256	

2. Click the **Add P1** button.

3. Set **Remote Gateway.**

4. Set **Authentication Method** to `Mutual PSK`.

5. Set **Pre-Shared Key.**

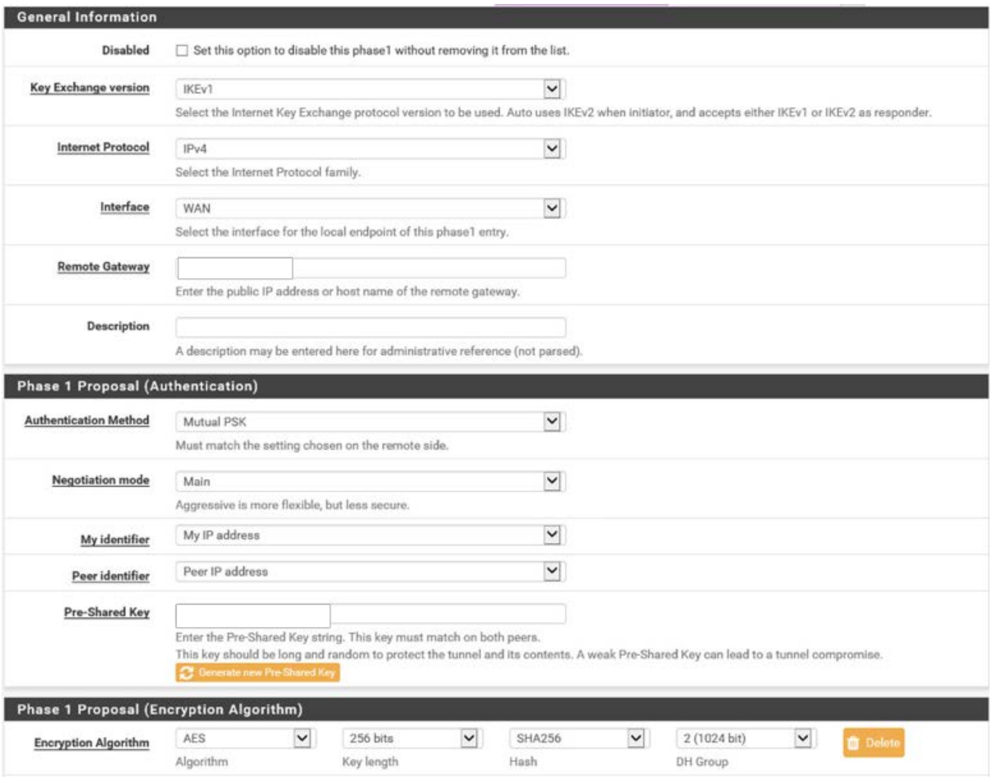
6. Set **Encryption Algorithm** settings:

a. **Algorithm:** AES

b. **Key Length:** `256 bits`

c. **Hash:** SHA256

d. **Diffie-Hellman Group:** `2 (1024 bit)`



General Information

Disabled	□ Set this option to disable this phase1 without removing it from the list.
Key Exchange version	IKEv1 Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.
Internet Protocol	IPv4 Select the Internet Protocol family.
Interface	WAN Select the interface for the local endpoint of this phase1 entry.
Remote Gateway	Enter the public IP address or host name of the remote gateway.
Description	A description may be entered here for administrative reference (not parsed).

Phase 1 Proposal (Authentication)

Authentication Method	Mutual PSK Must match the setting chosen on the remote side.
Negotiation mode	Main Aggressive is more flexible, but less secure.
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

Phase 1 Proposal (Encryption Algorithm)

	Algorithm	Key length	Hash	DH Group
Encryption Algorithm	AES	256 bits	SHA256	2 (1024 bit)

7. Return to **VPN > IPsec.**

8. Click the **Add P2** button.

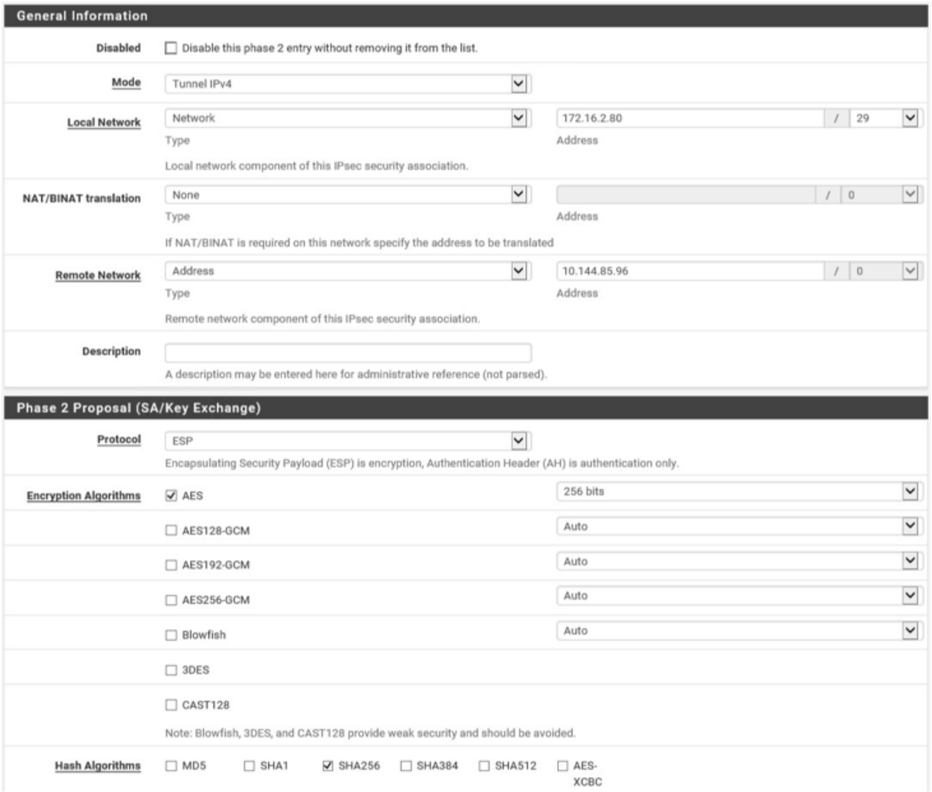
9. Set **Local Network** to `172.16.2.80/29`.

10. Set **Remote Network.**

11. Set **Protocol** to ESP.

12. Set **Encryption Algorithm** to `AE 256 bits`.

13. Set **Hash Algorithm** to `SHA256`.



General Information

Disabled: □ Disable this phase 2 entry without removing it from the list.

Mode: Tunnel IPv4

Local Network: Network (Type) 172.16.2.80 / 29 (Address)
Local network component of this IPsec security association.

NAT/BINAT translation: None (Type) / 0 (Address)
If NAT/BINAT is required on this network specify the address to be translated

Remote Network: Address (Type) 10.144.85.96 / 0 (Address)
Remote network component of this IPsec security association.

Description:
A description may be entered here for administrative reference (not parsed).

Phase 2 Proposal (SA/Key Exchange)

Protocol: ESP
Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.

Encryption Algorithms:
☑ AES — 256 bits
□ AES128-GCM — Auto
□ AES192-GCM — Auto
□ AES256-GCM — Auto
□ Blowfish — Auto
□ 3DES
□ CAST128
Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.

Hash Algorithms: □ MD5 □ SHA1 ☑ SHA256 □ SHA384 □ SHA512 □ AES-XCBC

2.6 pfSense VPN

pfSense is an open-source firewall/router used to create both site-to-site VPN tunnels. The following configuration file can be used to upload all configurations to the enterprise location edge router. Both the UMD and Plano edge routers are excluded for security purposes.

2.6.1 Plano and UMD VPN Configuration

To configure a site-to-site OpenVPN connection, refer to https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/index.html.

2.7 Splunk

Splunk is a security information and event management (SIEM) system that allows collecting and parsing logs and data from multiple systems.

2.7.1 Splunk Enterprise Configuration

2.7.1.1 VM Configuration

The Splunk VM is configured as follows:

- Ubuntu Mate 16.04.2
- 2 CPU cores
- 10 GB of RAM
- 2 TB of storage
- 1 NIC

2.7.1.2 Network

Network Configuration (Interface 1):

- IPv4: Manual
- IPv6: disabled
- IPv4 address: *10.100.200.101*
- Netmask: *255.255.255.0*
- Gateway: *10.100.200.1*

2.7.1.3 Installation

Note: A Splunk account will be needed to download Splunk Enterprise. The account is free and can be set up at https://www.splunk.com/page/sign_up.

Download Splunk Enterprise from https://www.splunk.com/en_us/download/splunk-enterprise.html. This build uses Version 7.1.3. Splunk can be installed on Windows, Linux, Solaris, and Mac OS X. Each of these installation instructions is provided at http://docs.splunk.com/Documentation/Splunk/7.1.3/Installation/Beforeyouinstall.

2.7.1.4 Universal Forwarder

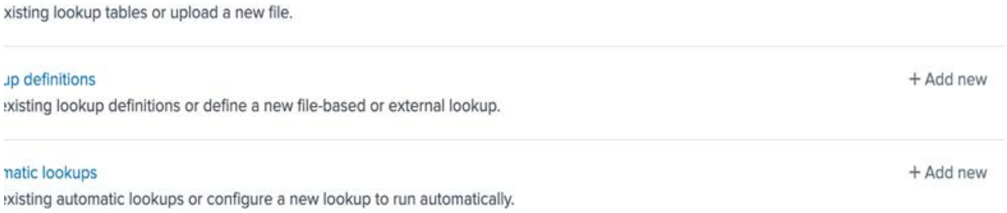
To install the universal forwarder, refer to documentation found at https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Installtheuniversalforwardersoftware.

Refer to each individual product to configure the universal forwarder or another means of integration with Splunk.

2.7.1.5 Reports and Alerts

If desired, lookup tables can be used to cross-check automated detections with human knowledge of a device. Some properties are cross-checked with human knowledge at both the UMD and Plano sites. Patch information from PUMP also uses a lookup table to cross-check results with devices. To upload lookup tables:

1. Log in to Splunk.
2. Go to **Settings > Lookups.**
3. Select **+ Add New** under **Lookup table files.**



xisting lookup tables or upload a new file.

up definitions
:xisting lookup definitions or define a new file-based or external lookup.
+ Add new

natic lookups
:xisting automatic lookups or configure a new lookup to run automatically.
+ Add new

4. Choose **Search** as the **Destination App.**
5. Browse for the CSV file. Name the Lookup file. Select **Save.**

The UMD lookup CSV file contains the following fields:

```
Asset Id,IP,Device,Platform
```

The Plano lookup CSV file contains the following fields:

```
Asset Id,IP,Vendor,Product Name,Serial Number,Version
```

Once integrations are complete, the following Splunk queries will create the desired reports:

2.7.1.5.1 Asset Report for Both Sites

```
index=_* OR index=* sourcetype=CTD_csv | table asset_id site_id name_ ip_ mac_ type_
vendor_ criticality_ risk_level is_ghost | sort site_id | where isnum(asset_id)
```

2.7.1.5.2 Asset Report for UMD

```
index=_* OR index=* sourcetype=CTD_csv | where isnum(asset_id)  | table asset_id
site_id name_ ip_ mac_ type_ vendor_ criticality_ risk_level is_ghost Device Platform
| sort site_id | search ip_=206.189.122* | lookup umd_lookup.csv "Asset Id" AS
asset_id OUTPUT "Device" AS Device, Platform AS Platform
```

2.7.1.5.3 Asset Report for Plano (Static)

```
index=_* OR index=* sourcetype=CTD_csv | where isnum(asset_id)  | table asset_id
site_id name_ ip_ mac_ type_ vendor_ criticality_ risk_level is_ghost Serial_Number
Version | sort site_id | search ip_=10.172.6* | lookup plano_lookup.csv "Asset Id" AS
asset_id OUTPUT "Serial Number" AS Serial_Number, Version AS Version
```

2.7.1.5.4 Asset Report for Plano (Dynamic)

```
index=forescout
```

```
|table ip mac "host_properties.nmap_banner7{}.value" nbthost
"host_properties.nmap_def_fp5{}.value" "host_properties.user_def_fp{}.value"
"host_properties.server_session{}.value"
```

```
|stats
values(mac),values("host_properties.nmap_banner7{}.value"),values(nbthost),values("hos
t_properties.nmap_def_fp5{}.value"),values("host_properties.user_def_fp{}.value"),valu
es("host_properties.server_session{}.value") by ip
```

```
|rename values(mac) as mac_address, values(host_properties.nmap_banner7{}.value) as
ports_and_services, values(nbthost) as hostname,
values(host_properties.nmap_def_fp5{}.value) as device_footprints,
values(host_properties.user_def_fp{}.value) as device_footprints2,
values(host_properties.server_session{}.value) as server_session_properties
```

2.7.1.5.5 UMD Steam Meter Data

```
index=modbus |rex "CWScript BCM:(?<name>.\w+)" | rex field=_raw "Flow Rate :
(?<flowRate>.*)" | rex field=_raw "Gal Total : (?<GalTotal>.*)" | transaction
maxspan=30s | table name _time flowRate GalTotal
```

2.7.1.5.6 UMD Device Data Calls

```
(index=* OR index=_*) (index=main host="10.100.100.111" NOT "cs2=UP") | table shost
src smac dhost dst dmac cs6 cs3 cs7 cs8 msg
```

2.7.1.5.7 Patch Report for FoxGuard PUMP

```
index=test sourcetype="csv" | lookup plano_lookup.csv "Asset Id" AS Asset_Id OUTPUT
"Serial Number" AS Serial_Number, Version AS Version | table Asset_Id IP Mac Vendor
"Operating System" Serial_Number Version Criticality Protocols | join IP type=left
[search index=test sourcetype=CTD_csv_report] | fields "Asset Id" IP Mac Vendor
"Operating System" Serial_Number Version | where isnotnull(Serial_Number) OR
isnotnull(Version) | sort IP | outputcsv patchreport.csv
```

2.8 Tripwire Industrial Visibility

Tripwire Industrial Visibility is used to passively scan the industrial control environments at both the College Park and Plano locations in the build. Tripwire Industrial Visibility builds a baseline of assets and network traffic between those assets then alerts on anomalous activity. Logs and alerts are reported up to the SIEM.

Tripwire Industrial Visibility is installed at three locations: Plano, Texas (TDi); UMD; and the NCCoE. This section describes how to deploy Tripwire Industrial Visibility 3.0.0.

Tripwire Industrial Visibility taps into OT network communication by listening through the SPAN port of routers and switches connected to the network segment, opening data packets, and interpreting protocols without disrupting normal operations.

By reading network traffic, it isolates all assets on the network and maps the flow of traffic between them. This data is then used to create graphical network maps.

2.8.1 Tripwire Industrial Visibility Configuration UMD

The following subsections document the software, hardware/VM, and network configurations for the Tripwire Industrial Visibility servers.

2.8.1.1 VM Configuration

The Tripwire Industrial Visibility VM was given the following resources:

- CentOS 7.5
- 4 CPU cores
- 100 GB hard disk
- 32 GB RAM
- 2 NICs

2.8.1.2 Network Configuration

Network Configuration:

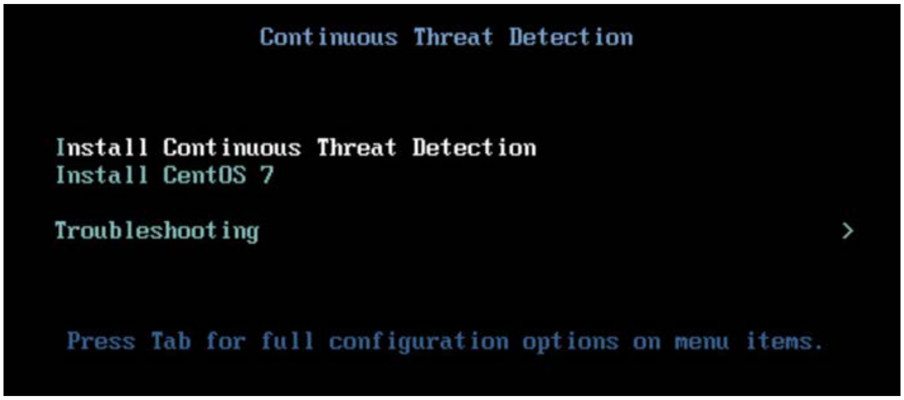
- DHCP: disabled
- IPv6: ignore
- IPv4: Manual
- IPv4 address: *10.100.100.111*
- Netmask: *255.255.255.0*
- Gateway: *10.100.100.1*

2.8.1.3 Installation

Tripwire supplied the Tripwire Industrial Visibility as an ISO installer. To configure TIV, use the ISO installer for each instance at Plano, UMD, and the NCCoE. Tripwire Industrial Visibility is configured in a sensor-server architecture. Plano and UMD instances act as sensors, and the NCCoE instance is the central server.

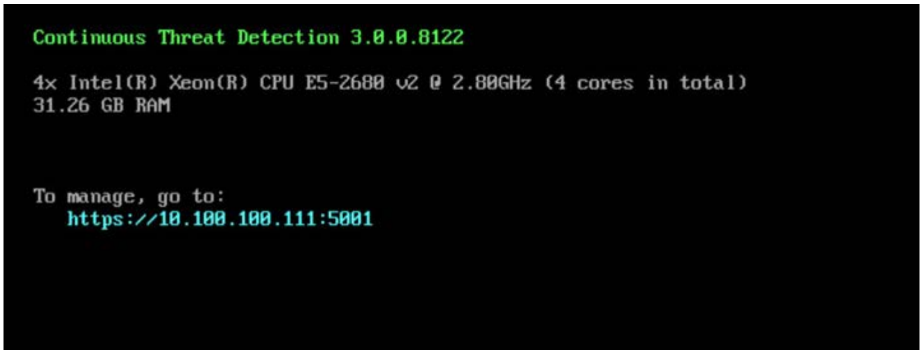
To begin installation, mount the provided image to the VM, and complete the following steps:

1. From the boot menu, select **Install Continuous Threat Detection.**



```
                  Continuous Threat Detection


  Install Continuous Threat Detection
  Install CentOS 7

  Troubleshooting                                          >


   Press Tab for full configuration options on menu items.
```

2. When the system is up, navigate to the configurator tool by using a browser.

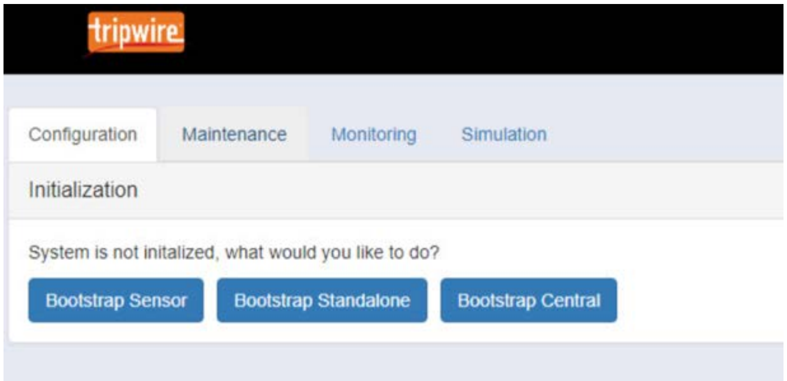


```
Continuous Threat Detection 3.0.0.8122

4x Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz (4 cores in total)
31.26 GB RAM


To manage, go to:
   https://10.100.100.111:5001
```

2.8.1.4 Configuration

Configure the Tripwire Industrial Visibility sensors.

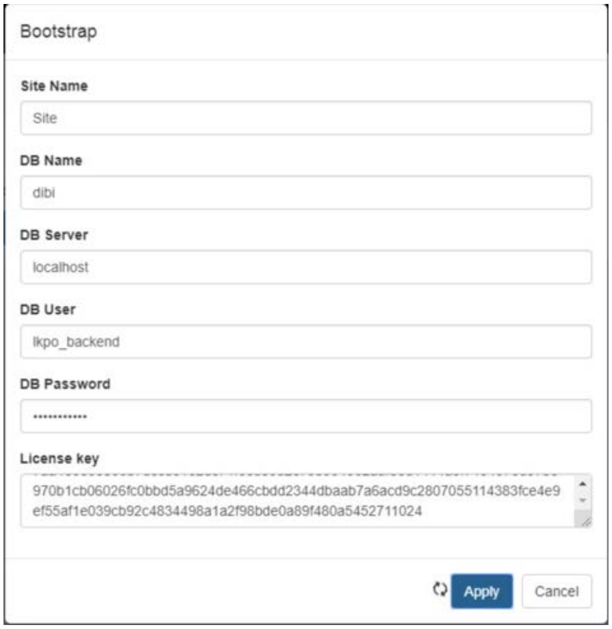
1. Connect to the configuration tool by entering the following URL into the browser: *https://10.100.100.11:5001.*
2. Enter the default credentials.
3. On the **Configuration** tab, the system will need to be initialized. Select **Bootstrap Sensor** (for Plan and UMD sites).



Initialization

System is not initalized, what would you like to do?

4. Enter the details and License Key. Select **Apply.**


Bootstrap

Site Name: Site

DB Name: dibi

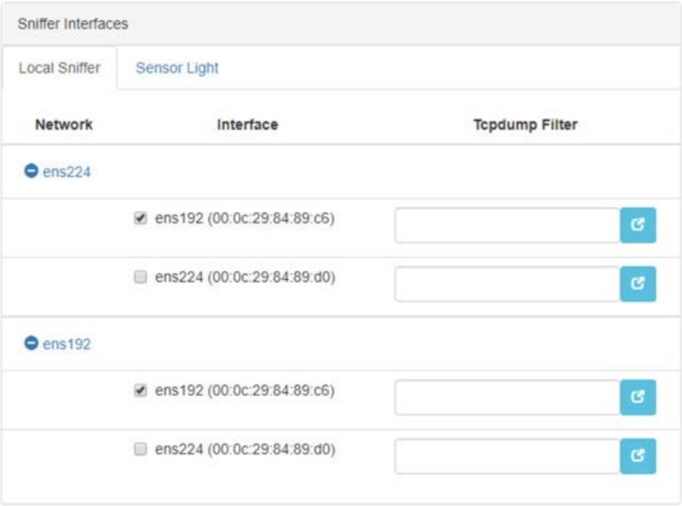
DB Server: localhost

DB User: lkpo_backend

DB Password: •••••••••••

License key:
970b1cb06026fc0bbd5a9624de466cbdd2344dbaab7a6acd9c2807055114383fce4e9
ef55af1e039cb92c4834498a1a2f98bde0a89f480a5452711024

5. Set the Sniffer Interface on the **Configuration** tab. Select the interfaced used as the SPAN port. Select **Apply.**

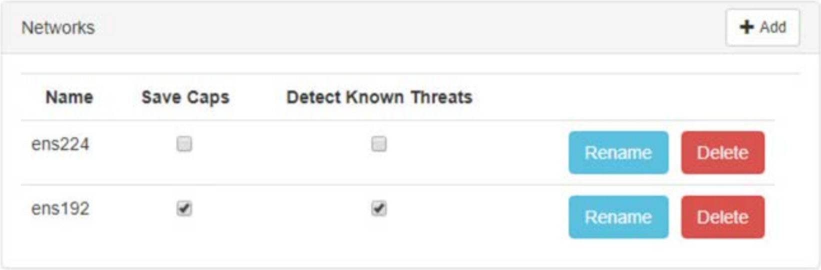


Sniffer Interfaces

Local Sniffer | Sensor Light

Network	Interface	Tcpdump Filter
● ens224		
	☑ ens192 (00:0c:29:84:89:c6)	
	□ ens224 (00:0c:29:84:89:d0)	
● ens192		
	☑ ens192 (00:0c:29:84:89:c6)	
	□ ens224 (00:0c:29:84:89:d0)	

6. Under **Networks,** select **Save Caps** and **Detect Known Threats** for the appropriate interface.

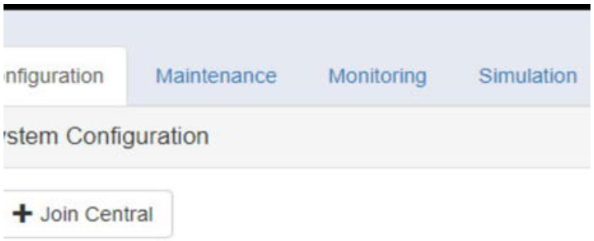


Networks

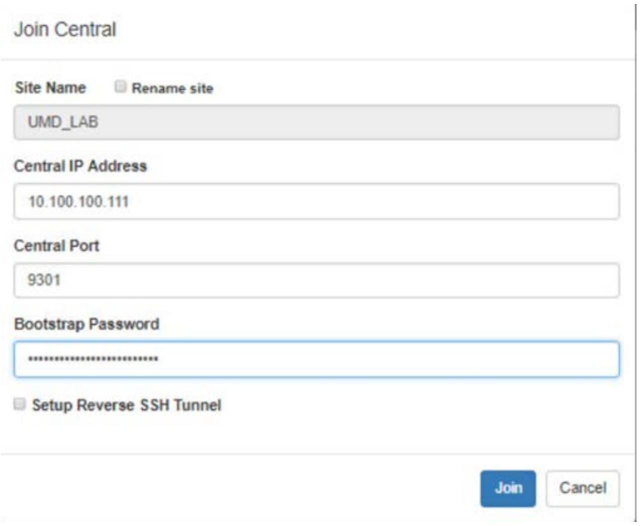
Name	Save Caps	Detect Known Threats	
ens224	□	□	Rename Delete
ens192	☑	☑	Rename Delete

7. Next, Join the Sensor to the Sensor Server. Set up the Central Server in Section 2.8.3 before completing these steps.

8. Select **Join Central,** from the **Configuration** tab.



9. Name the Sensor, and enter the IP address of the Central Server. Enter the Bootstrap password found on the Central Server. Select **Join.**



Join Central

Site Name □ Rename site

UMD_LAB

Central IP Address

10.100.100.111

Central Port

9301

Bootstrap Password

••••••••••••••••••••••••

□ Setup Reverse SSH Tunnel

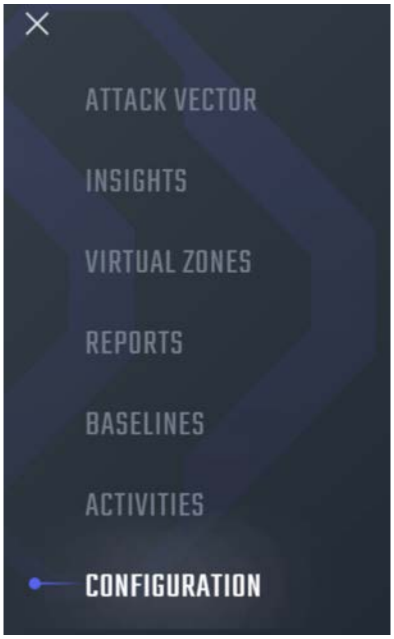
10. Connect to the continuous threat detection (CTD) Dashboard: *https://10.100.1.17:5000*.

The system is started in Training Mode. After an acceptable amount of time passes, place the system in Operational Mode. This build used one month as the training period.

1. Select the hamburger icon in the top left corner.

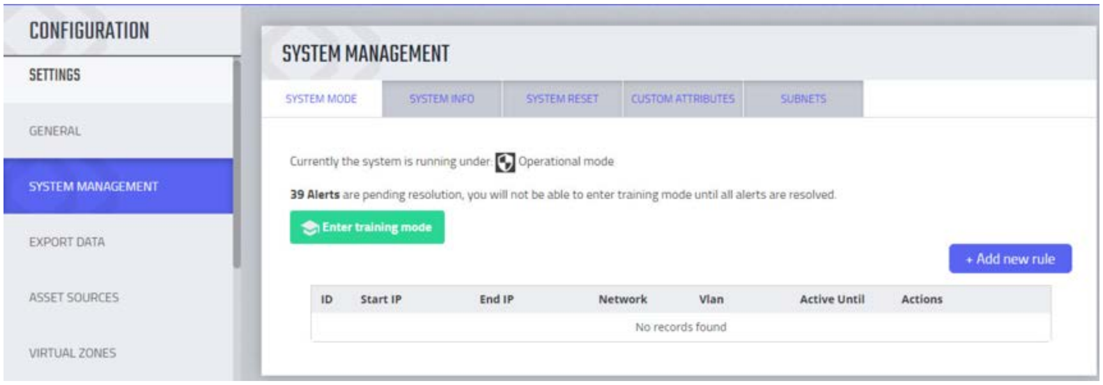
☰

2. Scroll down to select **Configuration**.



3. Select **System Management.**

4. Select the **System Mode** tab. Click **Enter Operational Mode.** Note: The screen will show **Enter Training Mode,** if the system is already in Operational Mode.

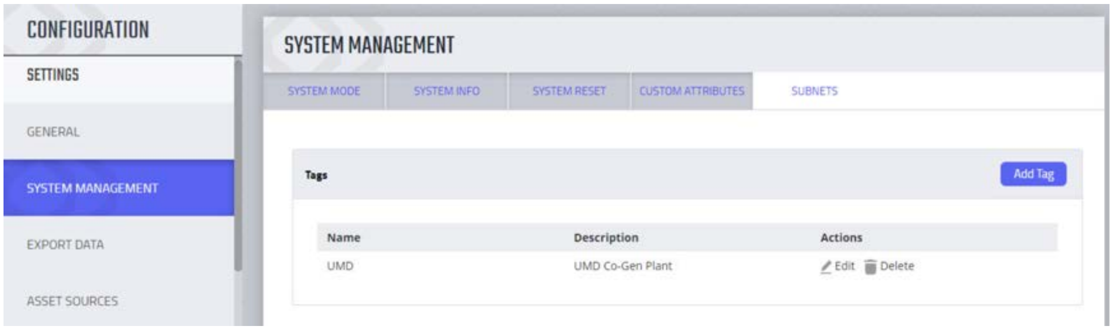


Currently the system is running under: Operational mode

39 Alerts are pending resolution, you will not be able to enter training mode until all alerts are resolved.

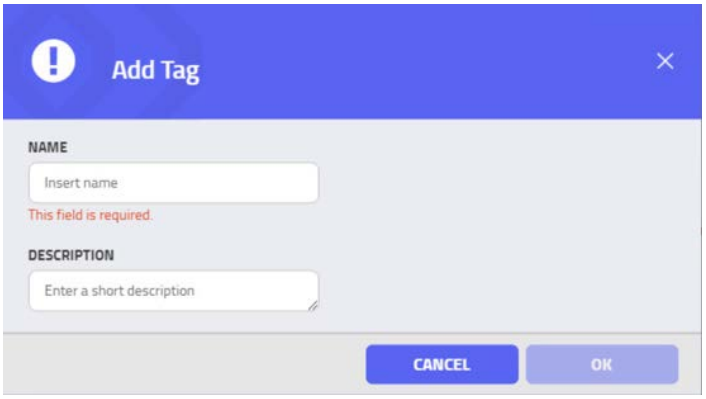
ID	Start IP	End IP	Network	Vlan	Active Until	Actions
No records found						

5. Select the **Subnets** tab. Click **Add Tag.**



Name	Description	Actions
UMD	UMD Co-Gen Plant	Edit Delete

6. Name a new Tag, and add the description. Select **OK.**



NAME

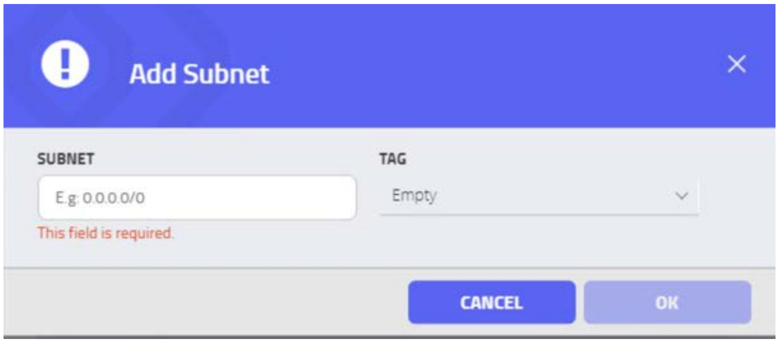
Insert name

This field is required.

DESCRIPTION

Enter a short description

7. Click **Add Subnet.** Enter the Subnet that the assets are on and the previously created TAG. Select **OK.**



This field is required.

8. Repeat Steps 16 and 17 for multiple subnets.

2.8.2 Tripwire Industrial Visibility Configuration Plano

The following subsections document the software, hardware/VM, and network configurations for the Tripwire Industrial Visibility servers.

2.8.2.1 VM Configuration

The Tripwire Industrial Visibility VM was given the following resources:

- CentOS 7.5
- 1 CPU Core
- 8 GB RAM
- 200 GB hard disk
- 3 NICs

2.8.2.2 Network Configuration

Network Configuration:

- DHCP: disabled
- IPv6: ignore
- IPv4: Manual
- IPv4 address: *10.100.100.111*
- Netmask: *255.255.255.0*
- Gateway: *10.100.100.1*

2.8.2.3 Installation

Repeat steps in Section 2.8.1.3.

2.8.2.4 Configurations

Repeat steps in Section 2.8.1.4.

2.8.3 Tripwire Industrial Visibility Configuration National Cybersecurity Center of Excellence

Tripwire Industrial Visibility at the NCCoE serves as the central server.

2.8.3.1 VM Configuration

The Tripwire Industrial Visibility VM was given the following resources:

- CentOS 7.5
- 4 CPU cores
- 80 GB hard disk
- 32 GB RAM
- 1 NIC

2.8.3.2 Network Configuration

Network Configuration:

- DHCP: disabled
- IPv6: ignore
- IPv4: Manual
- IPv4 address: *10.100.100.111*
- Netmask: *255.255.255.0*
- Gateway: *10.100.100.1*

2.8.3.3 Installation

Repeat steps in Section 2.8.1.3.

2.8.3.4 Configurations

Repeat Steps 1–4 in Section 2.8.1.4.

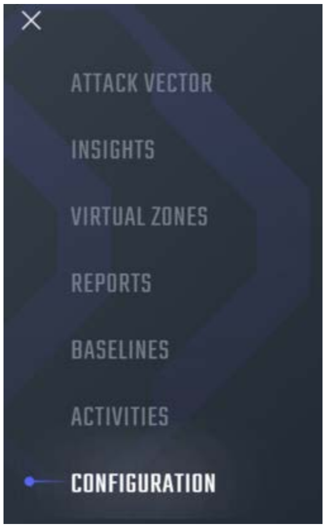
In Step 3, select **Bootstrap Central.**

To complete the configuration: set up syslog, schedule a report, and install the Claroty application on Splunk.

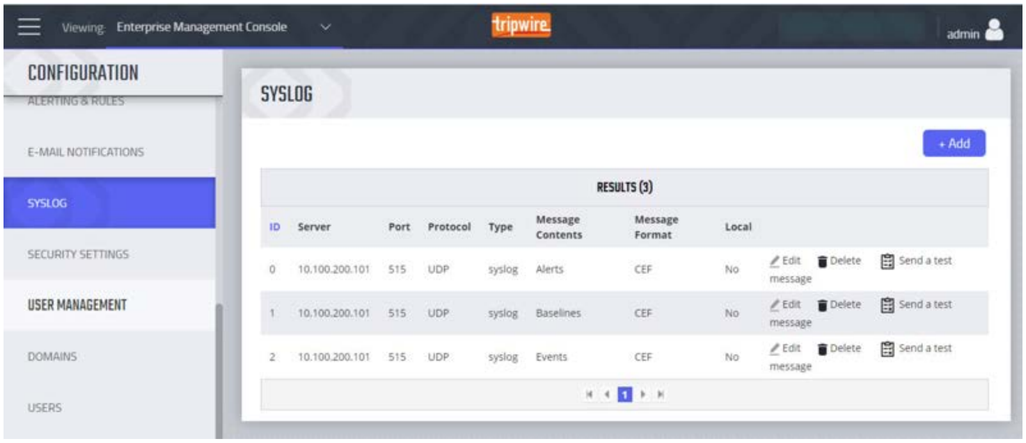
1. Connect to the CTD Dashboard: *https://10.100.100.1111:5000.*

2. Select the hamburger menu in the top left corner.

3. Scroll down to select **Configuration.**



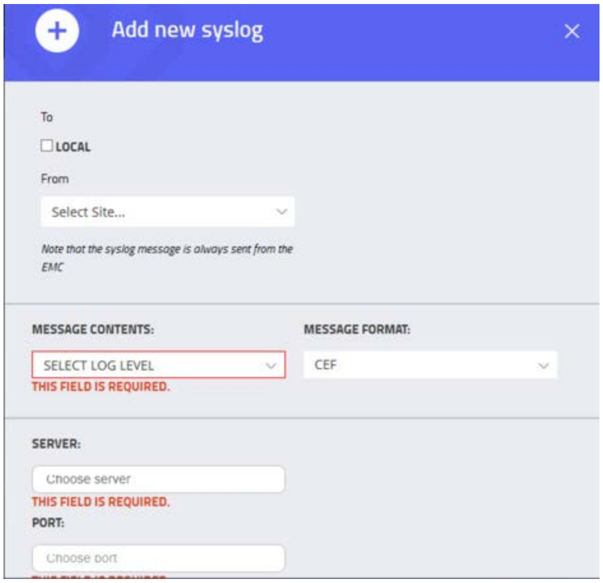
4. Select **Syslog.** Select **Add.**



RESULTS (3)

ID	Server	Port	Protocol	Type	Message Contents	Message Format	Local			
0	10.100.200.101	515	UDP	syslog	Alerts	CEF	No	Edit	Delete	Send a test message
1	10.100.200.101	515	UDP	syslog	Baselines	CEF	No	Edit	Delete	Send a test message
2	10.100.200.101	515	UDP	syslog	Events	CEF	No	Edit	Delete	Send a test message

5. Uncheck **Local.** Do not Select a Site.



Add new syslog

To

☐ LOCAL

From

Select Site...

Note that the syslog message is always sent from the EMC

MESSAGE CONTENTS: SELECT LOG LEVEL

THIS FIELD IS REQUIRED.

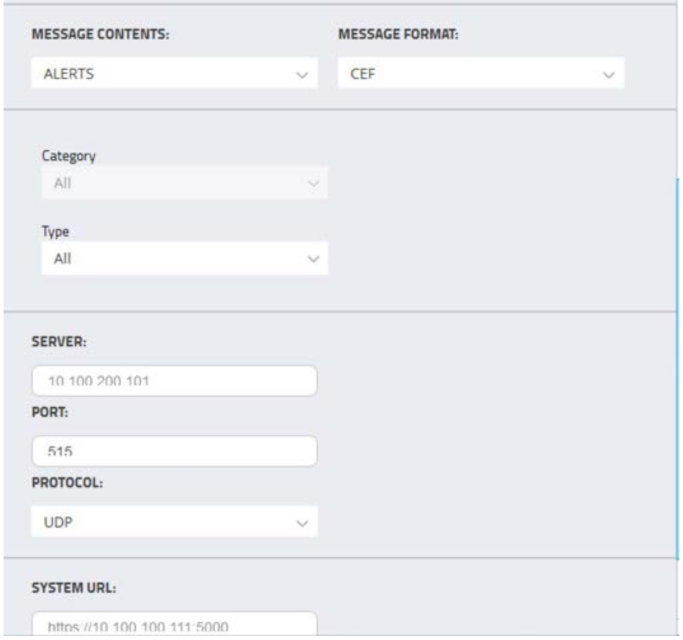
MESSAGE FORMAT: CEF

SERVER: Choose server

THIS FIELD IS REQUIRED.

PORT: Choose port

6. Select Alerts for the **Log Level.** Enter the IP address for the Splunk server under **Server.** Enter **Port** `515` and **Protocol** `UDP`**.** Select all boxes under **Category** and all boxes under **Type.** Leave the **System URL** and the **Message Format** as the default.



MESSAGE CONTENTS: ALERTS

MESSAGE FORMAT: CEF

Category: All

Type: All

SERVER: 10.100.200.101

PORT: 515

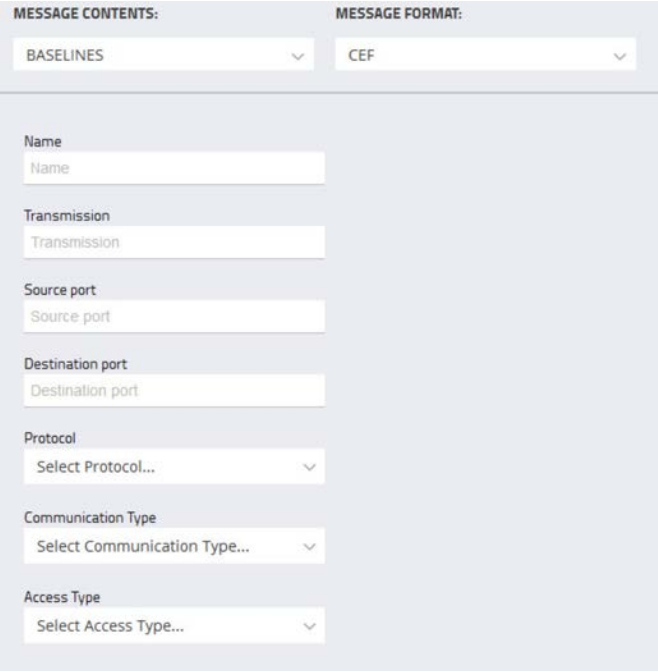
PROTOCOL: UDP

SYSTEM URL: https://10.100.100.111:5000

7. Select **Save**.

8. Select **Add** to add another.

9. Select **Baselines** under **Message Contents.**



MESSAGE CONTENTS: BASELINES

MESSAGE FORMAT: CEF

Name: Name

Transmission: Transmission

Source port: Source port

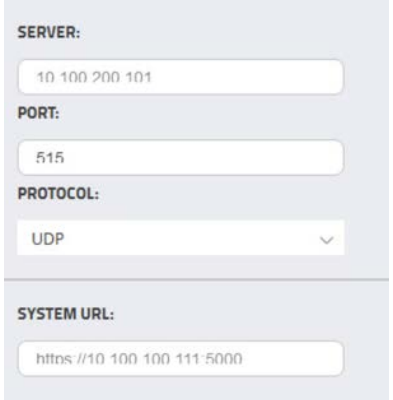
Destination port: Destination port

Protocol: Select Protocol...

Communication Type: Select Communication Type...

Access Type: Select Access Type...

10. Enter the Splunk IP for **Server, Port** 515, and **Protocol** UDP. Leave **System URL** as the default. Click **Save.**



SERVER: 10.100.200.101

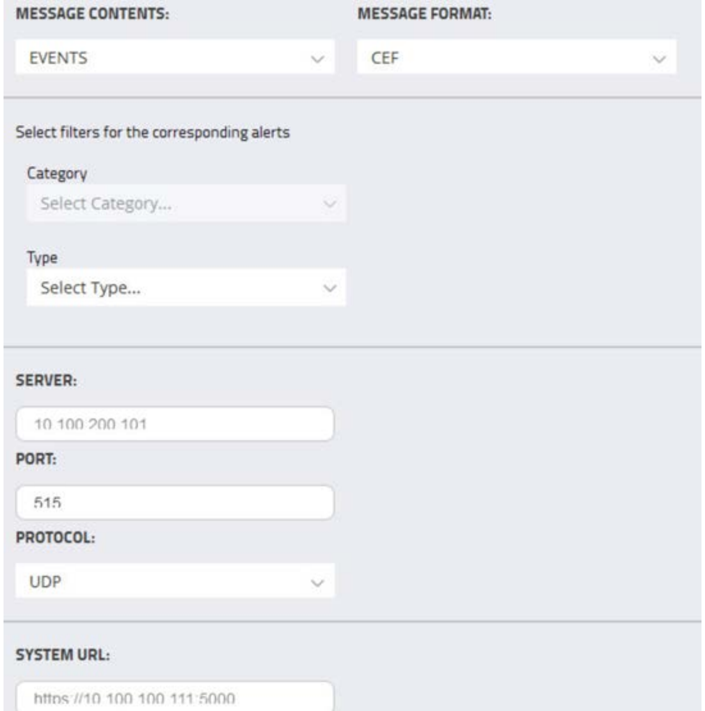
PORT: 515

PROTOCOL: UDP

SYSTEM URL: https://10.100.100.111:5000

11. Select **Add** to add another.

12. Select **EVENTS** for **Message Contents**. Enter the Splunk IP for **Server, Port** 515, and **Protocol** UDP. Leave the **System URL** as default.



MESSAGE CONTENTS: EVENTS

MESSAGE FORMAT: CEF

Select filters for the corresponding alerts

Category: Select Category...

Type: Select Type...

SERVER: 10.100.200.101

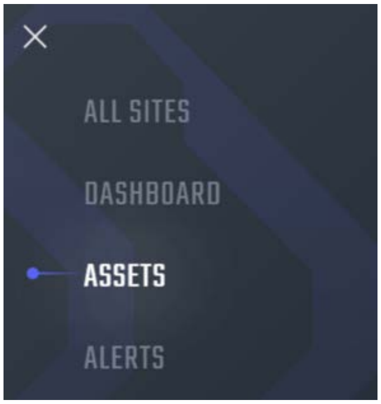
PORT: 515

PROTOCOL: UDP

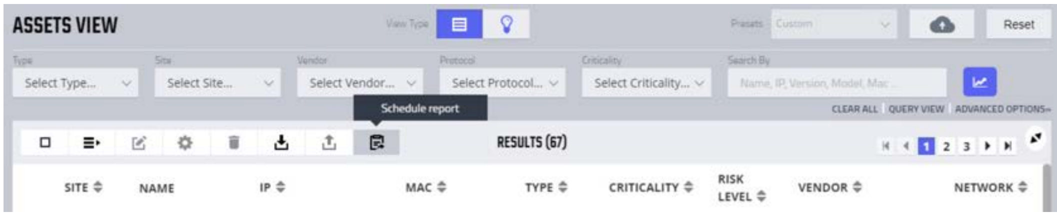
SYSTEM URL: https://10.100.100.111:5000

13. Click **Save.**

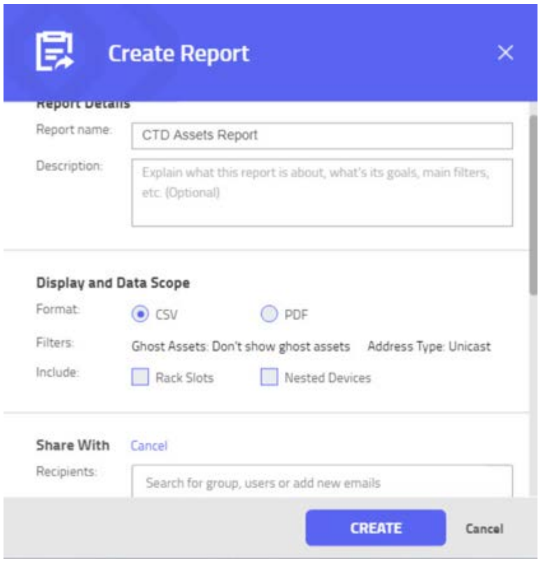
14. To configure Asset Reporting, select **Assets** from the hamburger menu.



15. From the **Assets** list, select the report icon in the menu bar, to schedule a report.



16. Name the report, and select **CSV** as the **Format.** Enter a recipient to receive and download the report. Schedule the report to run at an acceptable interval. This build scheduled the report to run daily. Click **Create.**



Report name: CTD Assets Report

Description: Explain what this report is about, what's its goals, main filters, etc. (Optional)

Format: ● CSV ○ PDF

Filters: Ghost Assets: Don't show ghost assets Address Type: Unicast

Include: □ Rack Slots □ Nested Devices

Recipients: Search for group, users or add new emails

2.8.3.5 Tripwire Splunk Integration

To integrate Tripwire with Splunk, install the Claroty Continuous Detection Application for Splunk. Additionally, install the Splunk Universal Forwarder to forward the CSV report.

1. Download the Claroty Continuous Detection Application for Splunk from https://splunkbase.splunk.com/app/4529/.
2. Log in to Splunk.
3. On the **Apps** menu, click **Manage Apps.**
4. Click **Install app** from file.
5. In the **Upload app** window, click **Choose File.**
6. Locate the downloaded *.tar.gz* file, and then click **Open** or **Choose.**
7. Click **Upload.**
8. Click **Restart Splunk,** and then confirm the restart.
9. To install Splunk Universal Forwarder, follow the steps in Section 2.7.1.4.
10. Place the following text in the */opt/splunkforwarder/etc/system/local/outputs.conf* file:

```
[tcpout]
defaultGroup = default-autolb-group
[tcpout:default-autolb-group]
Server = 10.100.200.101:9997
[tcpout-server://10.100.200.101:9997]
```

11. Place the following text in the */opt/splunkforwarder/etc/system/local/deploymentclient.conf* file:
12. `[target-broker:deploymentserver]`
13. `targetURI = 10.100.200.101:8089`
14. Log in to Splunk. Go to **Settings > Data Inputs > Files & Directories.**
15. Select **New Remote File & Directory.**
16. Select the host on which the forwarder is installed. Name the Server Class. Click **Next.**
17. Input the CSV file to monitor, i.e., /home/esam/attachments/report.csv.
18. Select **Next.**
19. Select **Review.**
20. Select **Submit.**

Appendix A List of Acronyms

CSV	Comma Separated Value
CPU	Central Processing Unit
CTD	Continuous Threat Detection
DHCP	Dynamic Host Configuration Protocol
DVD	Digital Versatile Disc
ESAM	Energy Sector Asset Management
ESP	Encapsulating Security Payload
GB	Gigabyte
HDD	Hard Disk Drive
IP	Internet Protocol
IPv	Internet Protocol version
ISO	Optical Disc Image
IT	Information Technology
NCCoE	National Cybersecurity Center of Excellence
NIC	Network Interface Controller/Card
NIST	National Institute of Standards and Technology
OS	Operating System
OT	Operational Technology
PUMP	Patch and Update Management Program
RAM	Random Access Memory
SIEM	Security Information and Event Management
SPAN	Switched Port Analyzer
TB	Terabyte
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UMD	University of Maryland
VM	Virtual Machine
VPN	Virtual Private Network
XML	Extensible Markup Language

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-23.