

Situational Awareness

For Electric Utilities

Volume C:
How-to Guides

Jim McCarthy

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Otis Alexander

Sallie Edwards

Don Faatz

Chris Peloquin

Susan Symington

Andre Thibault

John Wiltberger

Karen Viani

The MITRE Corporation
McLean, VA

August 2019

This publication is available free of charge from: <http://doi.org/10.6028/NIST.SP1800-7>

The first draft of this publication is available free of charge from:
<https://nccoe.nist.gov/sites/default/files/library/sp1800/es-sa-nist-sp1800-7-draft.pdf>

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor 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 1800-7C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-7C, 173 pages, (August 2019), 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 (FOIA).

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 IT 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 recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

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 Series 1800) 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

Through direct dialogue between NCCoE staff and members of the energy sector (composed mainly of electric power companies and those who provide equipment and/or services to them) it became clear that energy companies need to create and maintain a high level of visibility into their operating environments to ensure the security of their operational resources (operational technology [OT]), including industrial control systems (ICS), buildings, and plant equipment. However, energy companies, as well as all other utilities with similar infrastructure and situational awareness challenges, also need insight into their corporate or information technology (IT) systems and physical access control systems (PACS). The convergence of data across these three often self-contained silos (OT, IT, and PACS) can better protect power generation, transmission, and distribution.

Real-time or near-real-time situational awareness is a key element in ensuring this visibility across all resources. Situational awareness, as defined in this use case, is the ability to comprehensively identify and correlate anomalous conditions pertaining to ICS, IT resources, and access to buildings, facilities, and other business mission-essential resources. For energy companies, having mechanisms to capture, transmit, view, analyze, and store real-time or near-real-time data from ICS and related networking equipment provides energy companies with the information needed to deter, identify, respond to, and mitigate cyber attacks against their assets.

With such mechanisms in place, electric utility owners and operators can more readily detect anomalous conditions, take appropriate actions to remedy them, investigate the chain of events that led to the anomalies, and share findings with other energy companies. Obtaining real-time and near-real-time data from networks also has the benefit of helping demonstrate compliance with information security standards. This NCCoE project's goal is ultimately to improve the security of operational technology through situational awareness.

This NIST Cybersecurity Practice Guide describes our collaborative efforts with technology providers and energy sector stakeholders to address the security challenges that energy providers face in deploying a comprehensive situational awareness capability. It offers a technical approach to meeting the challenge and also incorporates a business value mind-set by identifying the strategic considerations involved in implementing new technologies. The guide provides a modular, end-to-end example solution that can be tailored and implemented by energy providers of varying sizes and sophistication. It shows energy providers how we met the challenge by using open-source and commercially available tools and technologies that are consistent with cybersecurity standards. The use case is based on an everyday business operational scenario that provides the underlying impetus for the functionality presented in the guide. Test cases were defined with industry participation to provide multiple examples of the capabilities necessary to provide situational awareness.

While the example solution was demonstrated with a certain suite of products, the guide does not endorse these products. Instead, it presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost effectively with an energy provider's existing tools and infrastructure.

KEYWORDS

correlated events; cybersecurity; energy sector; information technology; operational technology; physical access control systems; security information and event management; situational awareness

ACKNOWLEDGMENTS

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

Name	Organization
Pam Johnson	TDi
Clyde Poole	TDi
Eric Chapman	University of Maryland, College Park
David S. Shaughnessy	University of Maryland, College Park
Don Hill	University of Maryland, College Park
Mary-Ann Ibeziako	University of Maryland, College Park
Damian Griffe	University of Maryland, College Park
Mark Alexander	University of Maryland, College Park
Nollaig Heffernan	Waratek
James Lee	Waratek
John Matthew Holt	Waratek
Andrew Ginter	Waterfall
Courtney Schneider	Waterfall
Tim Pierce	Waterfall
Kori Fisk	The MITRE Corporation
Tania Copper	The MITRE Corporation

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

Technology Partner/Collaborator	Build Involvement
Dragos	CyberLens
Hewlett Packard Enterprise (HPE)*	ArcSight
ICS2	OnGuard
OSIsoft	PI Historian
Radiflow	iSIM
RS2 Technologies	Access It!, Door Controller
RSA, a Dell Technologies business	Archer Security Operations Management
Schneider Electric	Tofino Firewall
Siemens	RUGGEDCOM CROSSBOW
TDi Technologies	ConsoleWorks
Waratek	Waratek Runtime Application Protection
Waterfall Security Solutions	Unidirectional Security Gateway, Secure Bypass

**Please note: HPE in this project is now Micro Focus Government Solutions, which acquired the suite of products and solutions used by the NCCoE in this build.*

The NCCoE also wishes to acknowledge the special contributions of the University of Maryland for providing us with a real-world setting for the situational awareness build; Project Performance Company for its dedication in assisting the NCCoE with the very challenging and complex integration in this build; and the NCCoE Energy Provider Community for its patience, support, and guidance throughout the life cycle of this project.

Contents

1	Introduction.....	1
1.1	Practice Guide Structure	1
1.2	Build Overview.....	2
1.3	Typographic Conventions.....	3
1.4	Logical Architecture Summary	3
1.5	Wiring Diagrams.....	5
2	Product Installation Guides.....	6
2.1	Cisco 2950 (O15).....	7
2.1.1	Cisco 2950 (O15) Installation Guide	7
2.2	Dragos Security CyberLens (E8, O10)	10
2.2.1	Dragos Security CyberLens Server (E8) Environment Setup	10
2.2.2	Dragos Security CyberLens Server (E8) Installation and Configuration Guide	11
2.2.3	Dragos Security CyberLens Sensor (O10) Installation Guide.....	13
2.3	Hewlett Packard Enterprise (HPE) ArcSight (E12)	13
2.3.1	HPE ArcSight (E12) Installation Guide	13
2.3.2	ArcSight ESM Manager Server Operating System Installation	15
2.3.3	ArcSight Console Environment Setup.....	16
2.3.4	ArcSight Console Installation	17
2.4	ICS2 OnGuard (E5)	19
2.4.1	Environment Setup	20
2.4.2	Install Vendor Software	20
2.4.3	Install OnGuard System	22
2.5	IXIA Full-Duplex Tap (O16).....	25
2.6	OSIsoft PI Historian (E4, O8).....	26
2.6.1	OSIsoft PI Historian (E4) Installation Guide	26
2.6.2	OSIsoft PI Historian (O8) Installation Guide	33
2.7	OSIsoft Citect Interface (O13)	33
2.7.1	OSIsoft Citect Interface (O13) Installation Guide	33

2.7.2	Configuration	35
2.8	RS2 Technologies Access It! Universal.NET (E7)	39
2.8.1	Environment Setup	40
2.8.2	Post-Installation and Configuration	40
2.9	RS2 Technologies Door Controller (O4)	42
2.9.1	Hardware Installation	42
2.9.2	Connecting Hardware to Access It! Universal.NET	46
2.10	Radiflow 3180 (O14)	47
2.10.1	Radiflow 3180 (O14) Installation Guide	47
2.11	Radiflow iSID (O11)	49
2.11.1	Environment Setup	49
2.11.2	Product Installation	49
2.12	RSA Archer Security Operations Management (E13)	50
2.12.1	System Requirements	50
2.12.2	Preinstallation	50
2.12.3	Installation	54
2.12.4	Post-Installation	56
2.12.5	Configuration of ArcSight ESM to RSA Archer Security Operations Management	60
2.12.6	Additional ArcSight Integration Configuration	61
2.12.7	Sample Use Case Demonstration	63
2.13	Schneider Electric Tofino Firewall (O3, O18, O20)	67
2.13.1	Schneider Electric Tofino Firewall (O3) Installation Guide	67
2.13.2	Schneider Electric Tofino Firewall (O18) Installation Guide	69
2.13.3	Schneider Electric Tofino Firewall (O20) Installation Guide	77
2.14	Siemens RUGGEDCOM CROSSBOW (E9)	77
2.14.1	Environment Setup	77
2.14.2	Installation Procedure	77
2.15	Siemens RUGGEDCOM RX1400 (E1)	100
2.15.1	Environment Setup	101
2.15.2	Installation Procedure	101

2.16	Siemens RUGGEDCOM RX1501 (O1)	104
2.16.1	Siemens RUGGEDCOM RX1501 (O1) Installation Guide	104
2.17	TDi Technologies ConsoleWorks (E6, O5, O9)	104
2.17.1	System Environment	105
2.17.2	Installation	105
2.17.3	Usage	106
2.17.4	TDi Technologies ConsoleWorks (E6) Installation Guide	109
2.17.5	TDi Technologies ConsoleWorks (O9) Installation Guide	118
2.18	Waterfall Technologies Unidirectional Security Gateway (O2)	118
2.18.1	Waterfall Technologies Unidirectional Security Gateway (O2) Installation Guide ..	118
2.19	Waterfall Secure Bypass (O17)	124
2.19.1	Waterfall Secure Bypass (O17) Installation Guide	124
2.20	Waratek Runtime Application Protection (E10)	124
2.20.1	System Environment	125
2.20.2	Waratek Runtime Application Protection (E10) for Java Installation	125
2.20.3	Usage	126
2.21	ArcSight Connector Guides	126
2.21.1	Dragos CyberLens Connector	126
2.21.2	ICS2 OnGuard	131
2.21.3	RS2 Access It! Universal.NET	137
2.21.4	Additional References	143
3	Test Cases/Alert Configurations	144
3.1	ArcSight Filters	144
3.1.1	Filter Creation	144
3.1.2	ArcSight Test Cases	152
3.2	Test Cases	165
3.2.1	SA-1 Event Correlation for OT and PACS	165
3.2.2	SA-2 Event Correlation for OT and IT	166
3.2.3	SA-3 Event Correlation for OT and IT/PACS and OT	166
3.2.4	SA-4 Data Infiltration Attempts	167

3.2.5	SA-5 Configuration Management	168
3.2.6	SA-6 Rogue Device Detection	168
Appendix A List of Acronyms.....		170
Appendix B References		173

List of Figures

Figure 1-1	Monitoring and Data Collection Lab Build Architecture	4
Figure 1-2	Data Aggregation and Analysis Lab Build Architecture.....	4
Figure 1-3	Enterprise Lab Wiring Diagram	5
Figure 1-4	Cogeneration Facility Lab Network Diagram.....	6
Figure 2-1	OSIsoft PI Historian Connection	23
Figure 2-2	ApplicationSettings Syslog Configuration	24
Figure 2-3	IXIA TP-CU3 Network Tap	25
Figure 2-4	PI AF Server 2015 R2 Setup.....	27
Figure 2-5	Create New Data Source for SQL.....	28
Figure 2-6	Testing SQL Setup	29
Figure 2-7	PI SDK Setup	30
Figure 2-8	Configure New Interface	35
Figure 2-9	ICU — General Configuration.....	36
Figure 2-10	ICU — Citect ICU Control	37
Figure 2-11	ICU — Windows Service Setup.....	38
Figure 2-12	ICU — Unilnt Configuration	39
Figure 2-13	System Status	42
Figure 2-14	RS2 Door Controller Case.....	43
Figure 2-15	Inside of RS2 Door Controller Case.....	44
Figure 2-16	AC/DC Inverter.....	45
Figure 2-17	EP-1502 Door Controller Board	46

Figure 2-18 Radiflow iSID Web Dashboard	49
Figure 2-19 Web Server (IIS) Components Section	53
Figure 2-20 .NET Framework 4.5 Features Selection	54
Figure 2-21 Application Pools	59
Figure 2-22 RSA Archer User Login	60
Figure 2-23 Security Operations Management Tab	60
Figure 2-24 Multiple Security Alerts within the RSA Archer Console.....	63
Figure 2-25 Sample Message from ArcSight, Showing Raw Log Message/Alert and Parsing with Normalization	64
Figure 2-26 Sample Message Showing Alert Indicating New Device Detected at Substation	64
Figure 2-27 Sample Message Showing an Alert Indicating Badged Entry Detected at Substation	65
Figure 2-28 New Incident Response Workflow Record Started, Documented with Title, Summary, Details	65
Figure 2-29 Incident Record Alerts Tab, Showing the Association of Two Events Attached to This Incident Response Investigation Record.....	66
Figure 2-30 Incident Response Procedure with Two Related Tasks Assigned to the Incident Response Record	66
Figure 2-31 Incident Response Tasks with Status, Details, and Completion Status	67
Figure 2-32 Incoming Packet Configuration	68
Figure 2-33 Outgoing Packet Configuration	69
Figure 2-34 Create New Project	70
Figure 2-35 Administrator Password	70
Figure 2-36 Project Explorer Window.....	71
Figure 2-37 Tofino SA/MAC Address	71
Figure 2-38 Project Explorer	72
Figure 2-39 New Asset.....	73
Figure 2-40 Project Explorer Tofino SA Icon.....	74
Figure 2-41 Asset Rule Profiles.....	75
Figure 2-42 Apply Configuration Pane.....	76

Figure 2-43 CrossBow Server Configuration.....	79
Figure 2-44 CrossBow Server Configuration.....	81
Figure 2-45 CrossBow Server Configuration.....	82
Figure 2-46 MMC Snap-In	83
Figure 2-47 Preferences Dialogue Box.....	84
Figure 2-48 CxBClientOnlyCerts Snap-In	85
Figure 2-49 CrossBow Server Configuration.....	86
Figure 2-50 Preference Dialogue Box	87
Figure 2-51 CrossBow Server Configuration.....	88
Figure 2-52 Virtual Private Network (VPN) Certificate Form.....	90
Figure 2-53 VPN Private Key Form	91
Figure 2-54 Client Connection Info	92
Figure 2-55 SAC Connection List.....	93
Figure 2-56 Connection List	93
Figure 2-57 Certificates Info.....	94
Figure 2-58 Trigger Action	95
Figure 2-59 Status Log	95
Figure 2-60 Station Access Controller Properties	96
Figure 2-61 SAC Property Configuration — Identification.....	96
Figure 2-62 SAC Property Configuration — Connection.....	97
Figure 2-63 SAC Property Configuration — NERC CIP	97
Figure 2-64 Scheduling Push SAC Database	98
Figure 2-65 Application Selection Dialogue	100
Figure 2-66 RUGGEDCOM Web Login	101
Figure 2-67 Enable IPsec and NAT Traversal	102
Figure 2-68 Binding to Syslog.....	109
Figure 2-69 Server Management Bind Edit	110
Figure 2-70 Adding SYSLOG Console.....	110

Figure 2-71 Copying Plug-In to CWScript Directory	111
Figure 2-72 CWScript Upload	111
Figure 2-73 Browse for CWScript	112
Figure 2-74 Select CWScript XML	112
Figure 2-75 Review CWScript Settings.....	113
Figure 2-76 Modify Action and Parameter for CWScript.....	114
Figure 2-77 Add New Scan	115
Figure 2-78 Add New Event	116
Figure 2-79 Syslog Forwarding Action Config.....	116
Figure 2-80 Add Console to Syslog Forwarding Action Config.....	117
Figure 2-81 Review Event Settings	117
Figure 2-82 Waterfall Secure Bypass Interface	124
Figure 2-83 Set Up Syslog on CyberLens	127
Figure 2-84 ArcSight Configure	131
Figure 2-85 Program Parameters Setup.....	132
Figure 2-86 Request URL Configuration.....	132
Figure 2-87 Tool URL Verification.....	133
Figure 2-88 Access It! SQL Table.....	137
Figure 2-89 Access It! Application Window	138
Figure 2-90 Example Location	139
Figure 2-91 Example String/URL	141
Figure 2-92 Categorization File Fields.....	143
Figure 3-1 Create New Filter	145
Figure 3-2 Create Conditions (Logic).....	146
Figure 3-3 Bro Filter.....	147
Figure 3-4 Dragos CyberLens Filter.....	147
Figure 3-5 ICS2 On-Guard Filter.....	148
Figure 3-6 Windows Log Filter for OSI PI Historian.....	148

Figure 3-7 Radiflow iSID Filter.....	149
Figure 3-8 RS2 Access It! Filter	149
Figure 3-9 RSA Archer Filter	150
Figure 3-10 Waratek Filter	150
Figure 3-11 OT Cross-Boundary Filter	151
Figure 3-12 OT Inbound Filter	151
Figure 3-13 OT Outbound Filter	152
Figure 3-14 SA-1 - OT-Alerts Filter	152
Figure 3-15 SA-1 - OT and PACS Dashboard	153
Figure 3-16 SA-1 OT and PACS Active Channel	153
Figure 3-17 SA-2 - IT to OT AppAttack Filter	154
Figure 3-18 SA-2 OT-comms-with-non-OT Filter	154
Figure 3-19 SA-2 SQL Injection Dashboard.....	154
Figure 3-20 SA-2 SQL Injection Active Channel	155
Figure 3-21 SA-3 - FailedLogins Filter.....	155
Figure 3-22 SA-3 OT to IT or OT BadLogins Filter	156
Figure 3-23 SA-3 OT-to-IT or FailedLogins Dashboard	157
Figure 3-24 SA-3 OT-to-IT or FailedLogins Active Channel	158
Figure 3-25 SA-4 Anomaly Detection Filter	158
Figure 3-26 SA-4 Anomaly Detection Dashboard	159
Figure 3-27 Anomaly Detection Active Channel.....	159
Figure 3-28 SA-5 ConfigMgmt Filter	160
Figure 3-29 SA-5 ConfigMgmt Filter	160
Figure 3-30 SA-5 Master Filter	161
Figure 3-31 SA-5 Configuration Changes Dashboard	161
Figure 3-32 SA-5 Configuration Changes Active Channel	162
Figure 3-33 SA-6 RogueDevice Filter	163
Figure 3-34 SA-6 Rogue Device Dashboard	164

Figure 3-35 SA-6 Rogue Device Active Channel165

List of Tables

Table 2-1 CentOS Partitioning Scheme for ArcSight ESM Manager Server14

Table 2-2 RSA Archer Configuration Settings51

Table 2-3 IIS Components and .NET Framework52

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 recreate 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 approach to situational awareness. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-7A: *Executive Summary*
- NIST SP 1800-7B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-7C: *How-To Guides* – instructions for building the example solution (**you are here**)

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary* (NIST SP 1800-7A), which describes the following topics:

- challenges enterprises face in maintaining cross-silo situational awareness
- 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 1800-7B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.1, Risk, provides a description of the risk analysis we performed.
- Section 3.4.2, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary*, NIST SP 1800-7A, with your leadership team members to help them understand the importance of adopting a standards-based situational awareness solution.

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use the How-To portion of the guide, NIST SP 1800-7C, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution that includes physical access control systems (PACS) operational technology (OT), IT systems, and business processes. 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.

1.2 Build Overview

Energy sector colleagues shared that they need to know when cybersecurity events occur throughout the organization. Additionally, the information about such events must correlate data among various sources before arriving at a converged platform. Security staff need to be aware of potential or actual cybersecurity incidents in their IT and OT systems and PACS and to view these alerts on a single converged platform. Furthermore, the ability to drill down, investigate, and subsequently fully remedy or effectively mitigate a cybersecurity incident affecting any or all of the organization is essential.

1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit .
Monospace	command-line input, on-screen computer output, sample code examples, and status codes	<code>mkdir</code>
Monospace Bold	command-line user input contrasted with computer output	<code>service sshd start</code>
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

NIST Special Publication (SP) 1800-7B describes an example solution consisting of a monitoring/data collection component, which is deployed to operations facilities such as substations and generating plants; and a data aggregation/analysis component that is deployed as a single service for the enterprise. Data is collected from the industrial control systems (ICS) network by the monitoring/data collection component and sent to the data aggregation/analysis component. NIST SP 1800-7B also presents an architecture for building an instance of the example solution by using commercial products. That architecture is depicted in Figure 1-1 and Figure 1-2 below.

Figure 1-1 Monitoring and Data Collection Lab Build Architecture

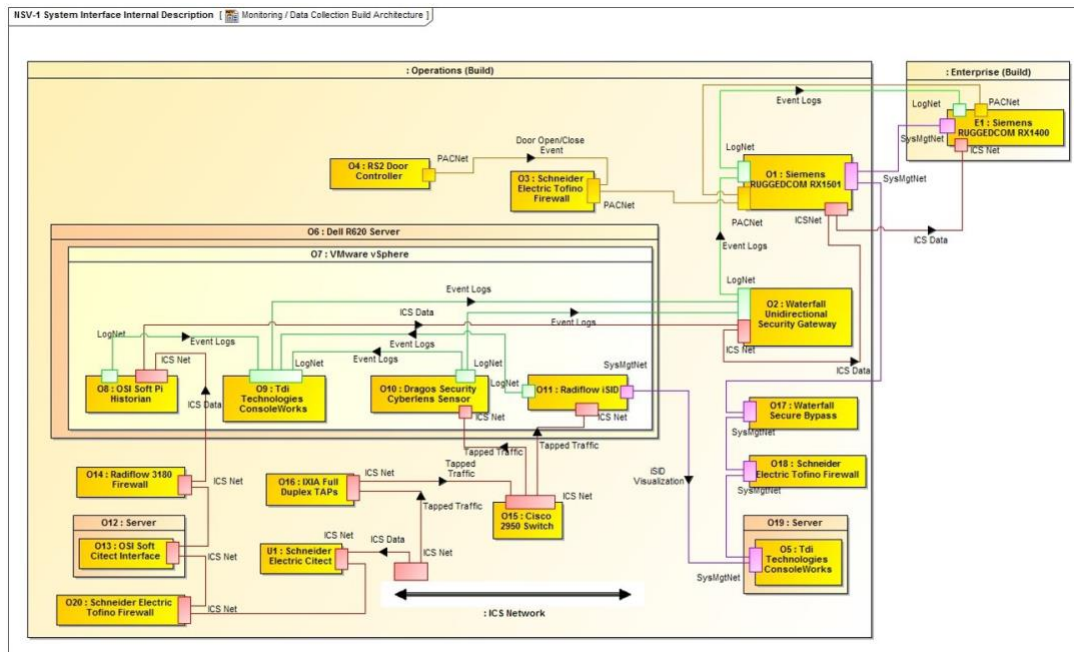
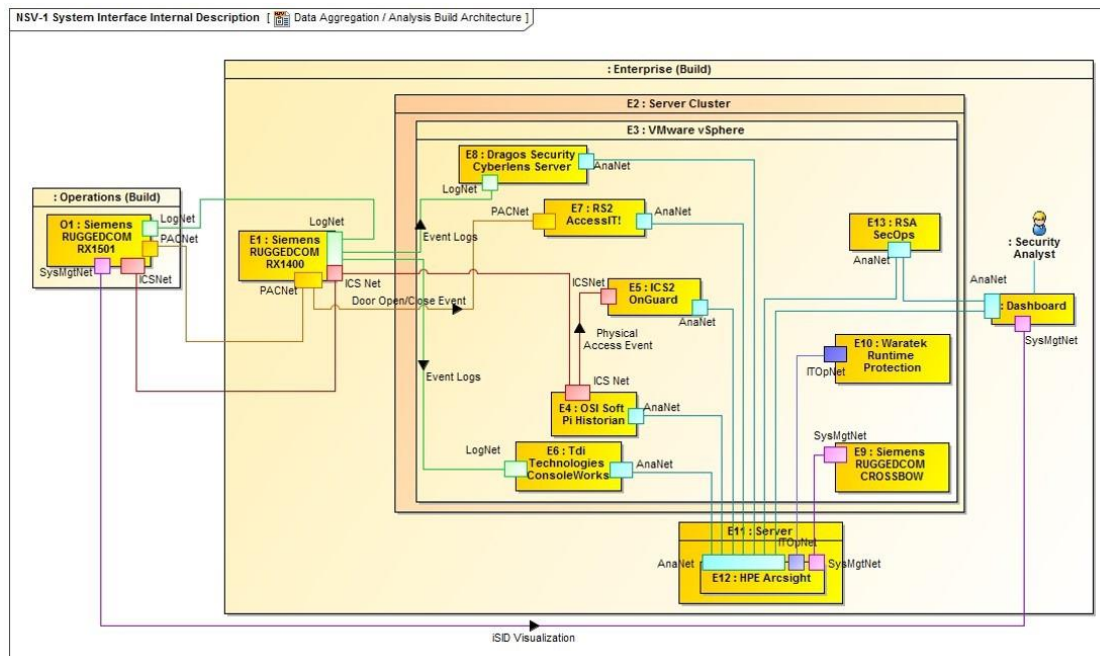


Figure 1-2 Data Aggregation and Analysis Lab Build Architecture

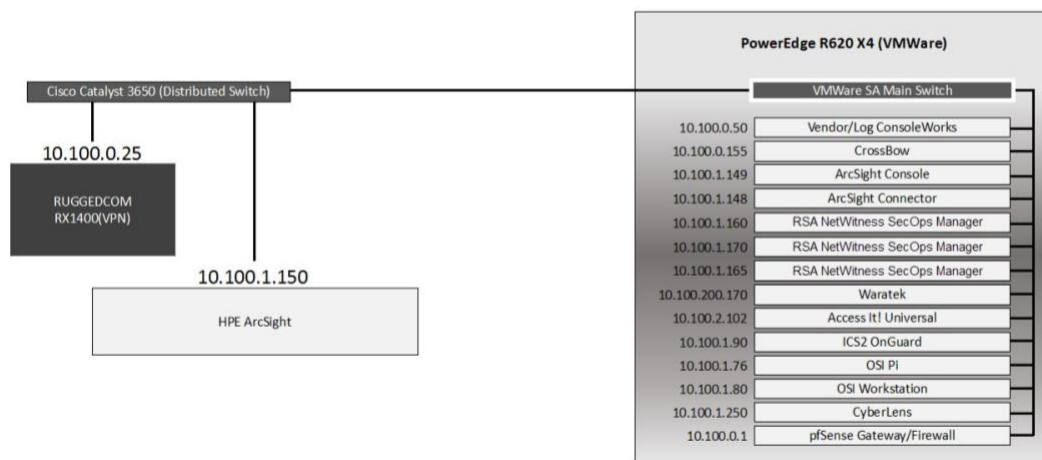


This practice guide provides detailed instructions on installing, configuring, and integrating the products used to build an instance of the example solution. The role of each product in the example solution is described in NIST SP 1800-7B, Section 4, Architecture.

1.5 Wiring Diagrams

The architecture diagrams in the previous section present the logical connections needed among the products used to build an instance of the example solution. This section describes the physical wiring that implements those logical connections.

Figure 1-3 Enterprise Lab Wiring Diagram



The diagram illustrates a complex network topology. At the top left, a **RUGGEDCOM RX1511 (VPN)** with IP **172.19.0.1** is connected to a **Waterfall One Way Transfer** (IP **172.19.0.5**) and a **Waterfall Secure Bypass** (IP **172.19.0.10**). The **Waterfall Secure Bypass** connects to a **Schneider Electric Firewall** (IP **172.19.1.1**), which in turn connects to a **Switch** (IP **172.19.1.25**). This switch is connected to a **ConsoleWorks Laptop** (IP **172.18.2.200**) and a **PowerConnect 7024 (Switch)**. The **PowerConnect 7024** connects to a **RADIFlow 3180 Switch**. The **RADIFlow 3180 Switch** connects to a **Citect Interface** (IP **172.18.2.170**), which connects to another **Schneider Electric Firewall**, and finally to a **Citect** system. A **MGMT: 172.19.1.20 Cisco 2950 (Aggregator)** is connected to the **RADIFlow 3180 Switch** and a group of **IXIA TP-CU3 Taps**. On the left, a **PowerEdge R620 (VMWare)** hosts several virtual machines: **ConsoleWorks** (172.18.0.50), **OSI PI Workstation** (172.18.2.160), **OSI PI** (172.18.2.150), **iSD** (172.18.3.25), **CyberLens** (172.18.1.250), and **Bro** (172.18.5.75). These VMs are connected to a **vSwitch** and a **Monitor vSwitch**, which connect to the **PowerConnect 7024** and the **RADIFlow 3180 Switch** respectively.

This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution. Product installation information is organized alphabetically by vendor with one section for each instance of the product. The section heading includes the unique product instance identifier used in the example solution architecture diagrams. Those identifiers have the form “Ln” where L is a letter and n is a number. Three different letters are used in the example solution architecture diagrams:

- If the build contains multiple instances of the same product installed in nominally the same way, the full installation instructions are presented for one instance. Only the differences in installation and

configuration are presented for the additional instances. For example, the build includes three instances of TDi Technologies ConsoleWorks (O5, O9, E6). Full installation instructions are provided for the E6 instance of TDi Technologies ConsoleWorks. The instructions provided for the O5 and O9 instances describe only the differences between those instances and the E6 instance.

2.1 Cisco 2950 (O15)

The Cisco 2950 switch is used to aggregate the IXIA network taps (O16). The configuration file is presented in the following subsection.

2.1.1 Cisco 2950 (O15) Installation Guide

Using 1904 out of 32768 bytes

```
!  
version 12.1  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname aggregator  
!  
aaa new-model  
enable secret 5 $1(s*tC$RHcpvnJts/adF.ONLSK32.  
enable password C1sc0  
!  
username admin privilege 15 secret 5 $1*.1Gz$nHZ.CVIlq28oMB46m2X8k/  
ip subnet-zero  
!  
ip domain-name lab-mgmt  
ip ssh time-out 120  
ip ssh authentication-retries 3  
ip ssh version 2  
!  
spanning-tree mode pvst  
no spanning-tree optimize bpdu transmission  
spanning-tree extend system-id  
!
```

```
!  
!  
!  
interface FastEthernet0/1  
no keepalive  
speed 100  
!  
interface FastEthernet0/2  
no keepalive  
speed 100  
!  
interface FastEthernet0/3  
no keepalive  
!  
interface FastEthernet0/4  
no keepalive  
!  
interface FastEthernet0/5  
no keepalive  
!  
interface FastEthernet0/6  
no keepalive  
!  
interface FastEthernet0/7  
no keepalive  
!  
interface FastEthernet0/8  
no keepalive  
!  
interface FastEthernet0/9  
no keepalive  
!  
interface FastEthernet0/10  
no keepalive  
!
```

```
interface FastEthernet0/11
no keepalive
!
interface FastEthernet0/12
no keepalive
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
switchport mode trunk
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
switchport access vlan 1000
switchport mode access
!
interface FastEthernet0/25
!
```

```

interface FastEthernet0/26
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
interface Vlan1000
ip address 172.19.1.20 255.255.254.0
no ip route-cache
!
ip http server
!
line con 0
line vty 0 4
password -lpqla,zMXKSOW)@
transport input ssh
line vty 5 15
password -lpqla,zMXKSOW)@
transport input ssh
!
!
!
monitor session 1 source interface Fa0/1 - 12 rx
monitor session 1 destination interface Fa0/23
end

```

2.2 Dragos Security CyberLens (E8, O10)

Dragos Security CyberLens software utilizes sensors placed within critical networks to identify assets and networks, building topologies and alerting on anomalies.

2.2.1 Dragos Security CyberLens Server (E8) Environment Setup

The system that was set up to run this application was a fully updated (as of 5/20/2016) Ubuntu 14.04 long-term support (LTS) operating system with the following hardware specifications:

- 4-core processor
- 8 gigabytes (GB) random access memory (RAM)

- 40 GB hard disk drive (HDD)

Other Requirements:

- Sudo or root privileges
- CyberLens installer (cyberlens-<version>-linux-<architecture>-installer.run)
- valid CyberLens license file

2.2.2 Dragos Security CyberLens Server (E8) Installation and Configuration Guide

1. As root:

- a. `./cyberlens-<version>-linux-<architecture>-installer.run`
- b. Accept the agreement and select **Forward**.
- c. Select **Forward** for a randomly generated password for root on the MySQL Server. A custom password can be specified if desired.
- d. Select **Forward** for a randomly generated password for CyberLens on the MySQL Server. As in the previous step, a custom password can be specified if desired.
- e. Select **Forward** to accept the installation configuration.
- f. Choose a **Username, Password** (and Confirm Password), and **Email Address** for the CyberLens login, then select **Forward**.
- g. Select **Localhost Access Only** (the files will be transferred across the Waterfall Security Gateway), then select **Forward**.
- h. Select **Forward**. Do not check the box for Block Outbound Traffic.
- i. Click the **folder icon** to select the CyberLens license file, then select **Forward**.
- j. Select **Forward** to begin installation.

2. Configure:

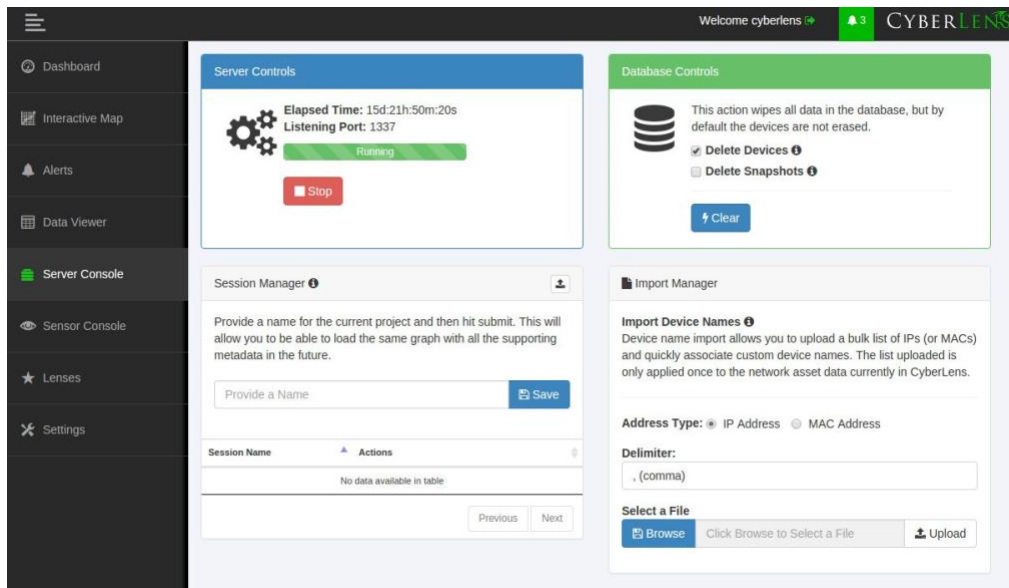
- a. Open a browser and navigate to *http://localhost/*
- b. On the menu bar on the left, select **Server Console**.
- c. Click the **drop-down arrow** next to **Options**, and check the box for **Use Sensor Files**.
- d. Click **Start** to start the server.

3. Set up file transfer protocol (FTP) for transferring files across the Waterfall Security Gateway:

- a. First, set up the user login. We used the username “waterfall.”

- b. `adduser waterfall`
 - c. Specify password.
 - d. Add additional information if desired.
 - e. Type **y** to accept information.
 - f. `apt-get install vsftpd`
 - g. Edit `/etc/vsftpd.conf`
 - h. Ensure `anonymous_enable=NO`
 - i. Ensure `local_enable=YES`
 - j. Set `write_enable=YES`
 - k. `service vsftpd restart`
 - l. `ln -s /var/www/html/cyberlens/lib/file_link/ /home/waterfall/`
4. Permissions error: When files are copied over, the permissions default to **waterfall:waterfall**. Use the following steps to change the default to **www-data:www-data**.
- a. `sudo apt-get install incrontab`
 - b. `sudo vi /etc/incron.allow`
 - i. Add `root` to file, then save and exit.
 - c. `sudo incrontab -u root -e`
 - i. Add `/var/www/html/cyberlens/lib/file_link IN_CREATE /bin/chown -R www-data:www-data /var/www/html/cyberlens/lib/file_link` then save and exit.

New files created in the directory should now automatically change permissions and be ingested.



2.2.3 Dragos Security CyberLens Sensor (O10) Installation Guide

For Dragos Security CyberLens Sensor, follow the steps in [Section 2.2.1](#) and [Section 2.2.2](#) for Dragos Security CyberLens Server. There is no need to fix the permissions error.

2.3 Hewlett Packard Enterprise (HPE) ArcSight (E12)

HPE ArcSight is used as a central security information and event management (SIEM) platform, collecting alerts from across the build and aggregating them in one central location.

(Please note: HPE in this project is now Micro Focus Government Solutions, which acquired the suite of products and solutions used by the NCCoE in this build.)

2.3.1 HPE ArcSight (E12) Installation Guide

2.3.1.1 ArcSight Enterprise Security Manager (ESM) Manager Server Environment Setup

The following configuration matched requirements for the product relative to the use in the situational awareness use case.

1. The base operating system is CentOS 7. The following partition scheme was used for the installation.

Table 2-1 CentOS Partitioning Scheme for ArcSight ESM Manager Server

Name	Size	Type
/	50 GB	ext4
/boot	1 GB	ext4
/home	22 GB	ext4
/tmp	40 GB	tmpfs
/opt	2126 GB	ext4 ^a

- a. It is recommended to use XFS for /opt in lieu of ext4.
2. Ensure /tmp is larger than 3 GB; otherwise, ESM will fail to install.
3. Ensure the installation of X Windows and “compatibility libraries” are installed as well; ESM requires them.
4. Modification of user process limit may be required to ensure efficient thread usage:
 - a. If there is not already a file /etc/security/limits.d/90-nproc.conf, create it (and the limits.d directory, if necessary).
 - b. If the file already exists, delete all entries in the file.
 - c. Add the following lines:

```
* soft nproc 10240
* hard nproc 10240
```
5. Adjust networking items:
 - a. Set **internet protocol (IP) address** to 10.100.1.150.
 - b. Set **Gateway** to 10.100.0.1.
 - c. Set **Subnet mask** to 255.255.0.0.
 - d. Add DNS server in **/etc/resolv.conf**.

```
10.97.74.8
```
 - e. Add host name in **/etc/hosts** as follows (or add to DNS):

```
10.100.1.150 arcsight.es-sa-b1.test arcsight
```
 - f. Set host name in **/etc/sysconfig/network**.

- g. Set **ONBOOT** to **yes** in **/etc/sysconfig/network-scripts/ifcfg-eth0**.
6. Ensure ports **8443**, **9443**, and **9000** are open on server firewall (e.g., check via `iptables -S` or `iptables -L -n`). If needed, add the following (as root). Adjust 0.0.0.0/0 statements as needed.
- ```
iptables -I INPUT -p tcp --dport 8443 -s 0.0.0.0/0 -j ACCEPT
iptables -I INPUT -p tcp --dport 9443 -s 0.0.0.0/0 -j ACCEPT
iptables -I INPUT -p tcp --dport 9000 -s 0.0.0.0/0 -j ACCEPT
```

If using a SuperConnector/Forwarder (e.g., to RSA Archer), add the following (adjust for user datagram protocol (UDP) or transmission control protocol (TCP) as needed):

```
iptables -I OUTPUT -p tcp -d 0.0.0.0/0 --dport 514 -j ACCEPT
```

7. Save the rules:

```
/sbin/service iptables save
```

8. Set Selinux to **permissive mode** (may set back to enforcing mode upon completion of installation).
9. `adduser arcsight`
10. `mkdir /opt/arcsight/`
11. `chown arcsight:arcsight /opt/arcsight/`
12. Modify files to imitate Red Hat Enterprise Linux (RHEL) 6.5 (for CentOS and newer Red Hat versions):
- a. Edit `/etc/system-release`  
`CentOS release 6.5 (Final)`
  - b. Edit `/etc/system-release-cpe`  
`cpe:/o:centos:linux:6:GA`

13. Ensure the time zone (tzdata) package is version 2014F or later. To install, use ...

```
rpm -Uvh tzdata
```

or

```
yum update
```

14. Reboot.

### 2.3.2 ArcSight ESM Manager Server Operating System Installation

1. Copy the ESM installation tar file (do not untar) to `/home/arcsight/Desktop/ArcSight` (create folder if it does not exist).

2. Copy the ESM zipped license file (do not unzip) into the folder from the previous step.
3. `cd /home/arcsight/Desktop/ArcSight (su arcsight if not currently arcsight user)`
4. `chown arcsight:arcsight <ESM Install File>`
5. `tar xvf <ESM Install File>`
6. `./ArcSightESMSuite.bin -i console`

***Note:** Stop xwindows first if doing the installation with the -i console switch. This switch runs the installation from the command line rather than from a graphical user interface (GUI). The command line installation eases troubleshooting.*

7. As user “arcsight” run the configuration wizard:

`/opt/arcsight/manager/bin/arcsight firstbootsetup -boxster -soft -i console`

8. Settings in the wizard:
  - a. CORR-Engine (DB) password = \_\_\_\_\_
  - b. System storage size = 301 GB
  - c. Event storage size = 361 GB
  - d. Online event archive size = 200 GB (~1/6 minus 10% of total space; system reserves 10% of space)
  - e. Retention period (days) = 30
  - f. Manager host name = arcsight.es-sa-b1.test
  - g. Administrator username = admin
  - h. Administrator password = \_\_\_\_\_
9. As user “root” run the following to install the ArcSight services onto the operating system:
10. Open a browser and navigate to ArcSight Command Center (<https://arcsight.es-sa-b1.test:8443>). Set the manager Java heap to 12288 (or another value based on available RAM).

### 2.3.3 ArcSight Console Environment Setup

1. Microsoft Windows 7 64-bit with the following settings:
  - a. 1 virtual central processing unit (vCPU)
  - b. 4 GB RAM

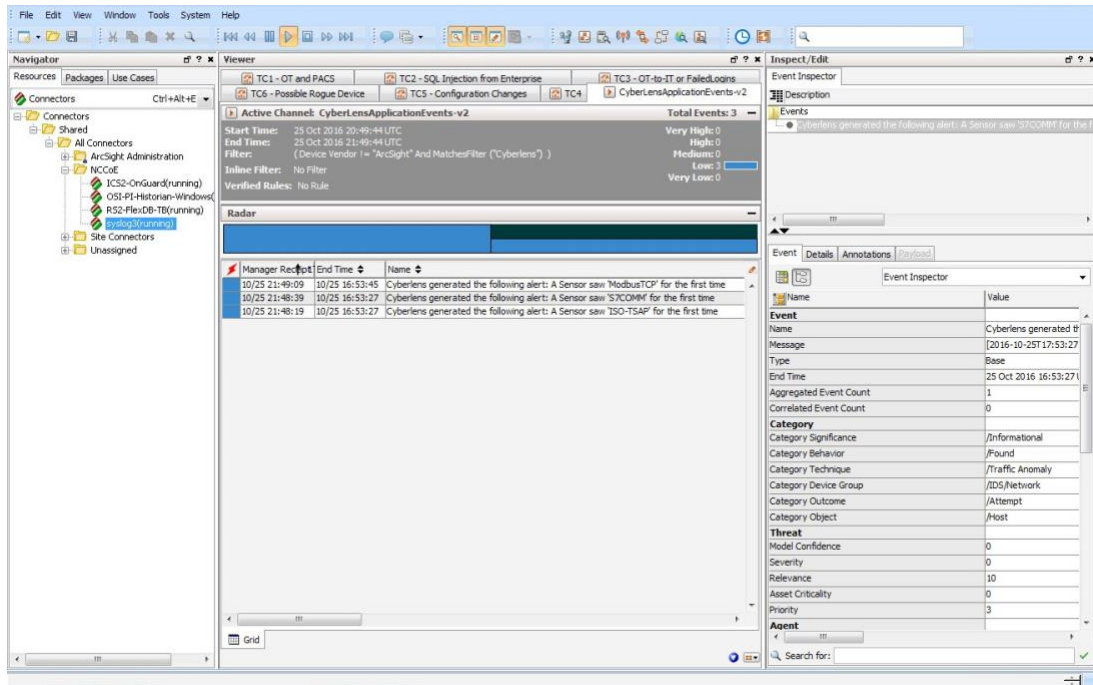
- c. 150 GB storage
- 2. The guest operating system (OS) IP information was set as follows:
  - a. IP address: 10.100.1.149
  - b. Gateway: 10.100.0.1?
  - c. Subnet mask: 255.255.0.0?
  - d. DNS: 10.97.74.8, 8.8.8.8, 8.8.4.4
- 3. Installed virtual machine (VM) Tools on guest OS to resolve missing mouse cursor issue.
- 4. Created OS user: arcsight, with password: \_\_\_\_\_

### 2.3.4 ArcSight Console Installation

- 1. Download ArcSight Console installation file (for Windows).
- 2. Run ArcSight Console installation file?
- 3. Add ArcSight Manager IP address to Windows OS host file (or add to DNS) at:

C:\windows\system32\drivers\etc\hosts (edit this file as Administrator) by adding the following line:

```
10.100.1.150 arcsight.es-sa-b1.test arcsight
```
- 4. Open ArcSight Console.
- 5. Log in to ArcSight Console with **user: arcsight, password: \_\_\_\_\_**, and in the **Manager** drop-down selection box type or select the server name: `arcsight.es-sa-b1.test`
- 6. At certificate-related pop-up, click **Accept**.



### 2.3.4.1 ArcSight Connector Server Preparation

1. CentOS 7 host with the following VM settings:
  - a. 1 vCPU
  - b. 12 GB RAM
  - c. 140 GB provisioned
2. Install CentOS using the following options:
  - a. Server with GUI Xwindows libraries are required in accordance with ArcSight guide.
  - b. File and Storage (in case file-based log collection will be used)
  - c. Compatibility libraries
  - d. Development tools
3. Set guest host name as follows: `arconn.es-sa-b1.test`
4. Install VM Tools on guest OS.
5. Set guest OS IP information as follows:
  - a. IP address: 10.100.1.148

- b. Gateway: 10.100.0.1
  - c. Subnet mask: 255.255.0.0
  - d. DNS: 10.97.74.8, 8.8.8.8
- 6. Add host names in `/etc/hosts` as follows (or add to DNS):  
`10.100.1.148 arconn.es-sa-b1.test arconn`
- 7. `10.100.1.150 arcsight.es-sa-b1.test arcsight adduser arcsight`
- 8. `mkdir /opt/arcsight/`
- 9. `chown -r arcsight:arcsight /opt/arcsight/`
- 10. As user `arcsight`, `mkdir /opt/arcsight/connectors/syslog1`
- 11. Ensure UDP port 514 is open inbound on server firewall and also that connector is allowed outbound on port 8443. For example: ...
  - a. As root:  
`iptables -I INPUT -p udp --dport 514 -s 0.0.0.0/0 -j ACCEPT`  
`iptables -I OUTPUT -p tcp -d 0.0.0.0/0 --dport 8443 -j ACCEPT`
  - b. Save the rules:  
`/sbin/service iptables save`
- 12. Disable firewall:
  - a. `systemctl disable firewall`
  - b. `systemctl mask firewalld expressions`
- 13. Disable OS native syslog service:  
`systemctl disable rsyslog.service`

## 2.4 ICS2 OnGuard (E5)

ICS2 OnGuard is used for behavioral analysis based on an extended model of historical historian information. Utilizing this information, OnGuard alerts to changes in historian activity based on deviations to original model.

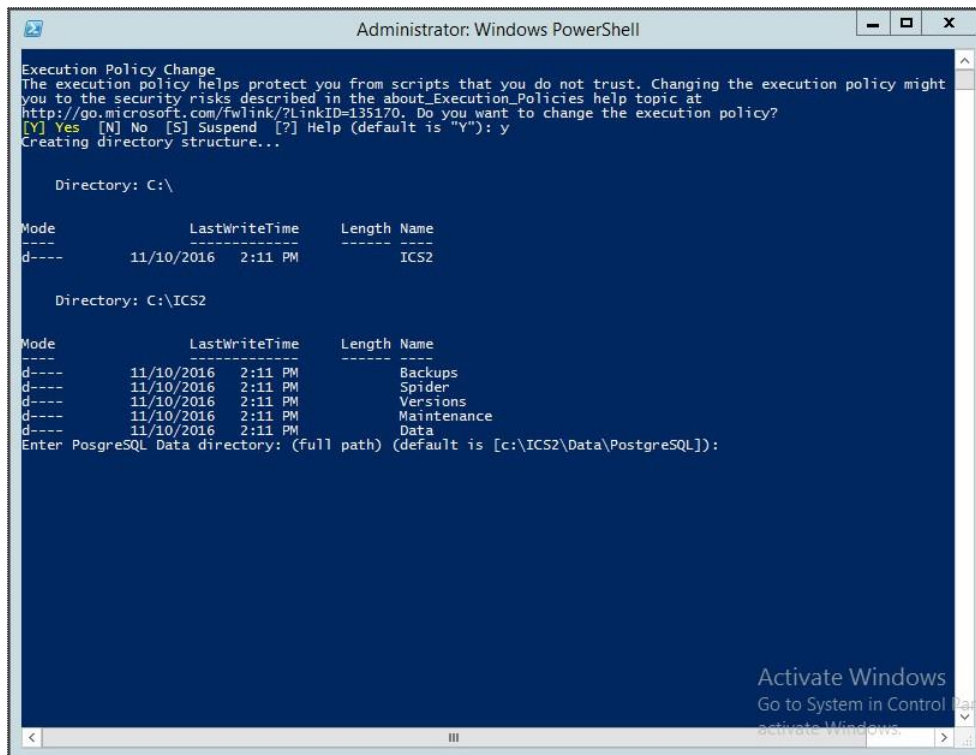
### 2.4.1 Environment Setup

The following configuration matched requirements for the product relative to the use in the situational awareness build:

- Microsoft Windows Server 2012 R2
- VM with CPU Quad Core 2.199 gigahertz (GHz)
- VM with 16,384 MB of memory
- virtual hard disk
- OS/soft PI OLE DB Driver
- ICS2\_Installation\_<version>.zip

### 2.4.2 Install Vendor Software

1. Open and extract the provided *ICS2\_Installation\_<version>.zip* file.
2. Open the **ICS2 Installation folder** created by extracting the .zip file.
3. Right-click the **ServerDeploy.PS1** file and select **Run with PowerShell**.
4. Press **Y** to change the execution policy.
5. Once the directory structure has been created, press **Enter** for the default PostgreSQL directory.

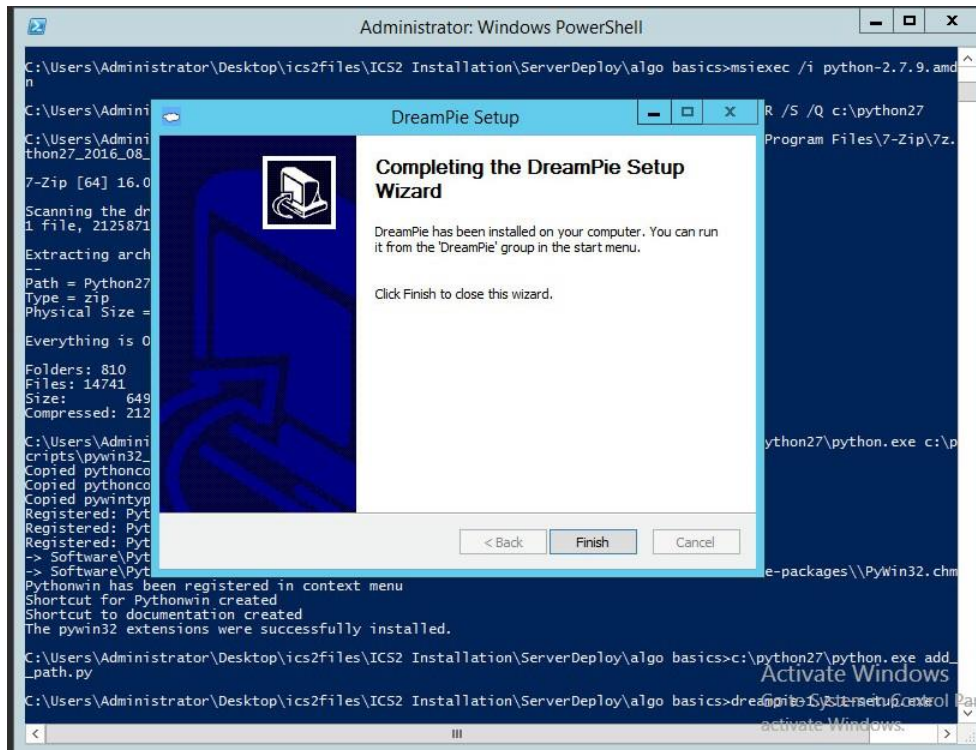


6. Press **Enter** for the default SQLServer directory.

The installer will install multiple products, including Google Chrome and Notepad++.

7. When the DreamPie installer pops up, click **Next**.
8. Select **Install for anyone using this computer** and click **Next**.
9. Keep the default destination folder and click **Install**.
10. When the installation is complete, click **Next**.
11. Close the installer by clicking **Finish**.



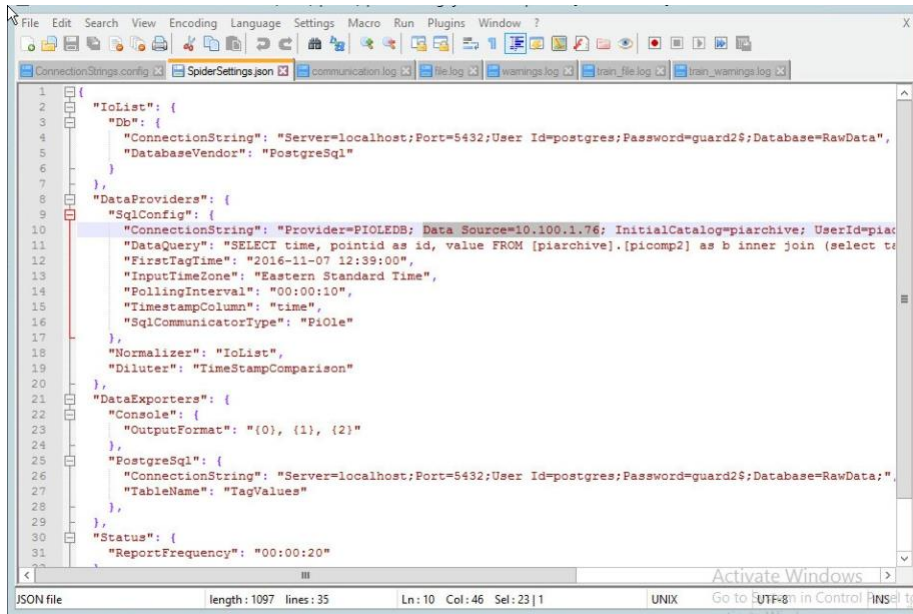


12. Once completed, PowerShell will close.

### 2.4.3 Install OnGuard System

1. Open the **Deploy OnGuard <version>** folder.
2. Double-click the **DeployOnGuard** Windows Batch File.
3. Verify that **ApplicationSettings.config**, **ConnectionStrings.config**, and **SpiderSettings.json** have been created.
  - a. If necessary, change the historian IP address (OSIsoft PI) in **SpiderSettings.json** to the appropriate IP address (the key is **DataProviders.SqlConfig.ConnectionString**).

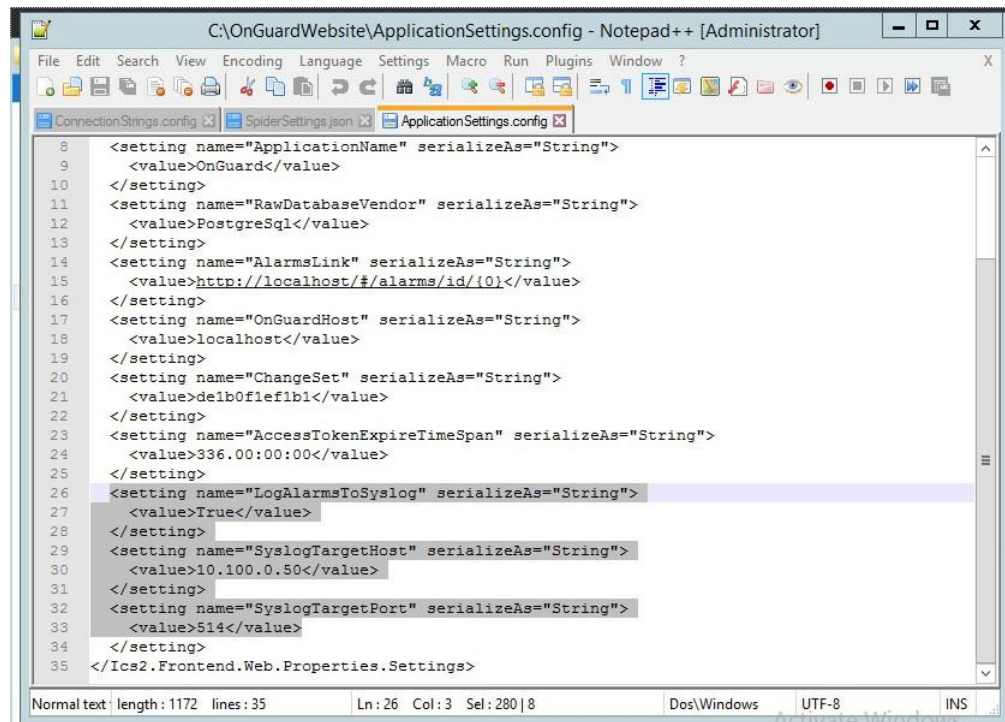
Figure 2-1 OSIsoft PI Historian Connection



```
1 {
2 "IoList": {
3 "Db": {
4 "ConnectionString": "Server=localhost;Port=5432;User Id=postgres;Password=guard2$;Database=RawData",
5 "DatabaseVendor": "PostgreSql"
6 }
7 },
8 "DataProviders": {
9 "SqlConfig": {
10 "ConnectionString": "Provider=PIOLEDB; Data Source=10.100.1.76; InitialCatalog=piarchive; UserId=piac",
11 "DataQuery": "SELECT time, pointid as id, value FROM [piarchive].[picomp2] as b inner join (select t",
12 "FirstTagTime": "2016-11-07 12:39:00",
13 "InputTimeZone": "Eastern Standard Time",
14 "PollingInterval": "00:00:10",
15 "TimestampColumn": "time",
16 "SqlCommunicatorType": "PiOLE"
17 },
18 "Normalizer": "IoList",
19 "Diluter": "TimeStampComparison"
20 },
21 "DataExporters": {
22 "Console": {
23 "OutputFormat": "{0}, {1}, {2}"
24 },
25 "PostgreSql": {
26 "ConnectionString": "Server=localhost;Port=5432;User Id=postgres;Password=guard2$;Database=RawData",
27 "TableName": "TagValues"
28 }
29 },
30 "Status": {
31 "ReportFrequency": "00:00:20"
32 }
33 }
```

- b. In ApplicationSettings.config, verify that settings LogAlarmsToSyslog is True, SyslogTargetHost is set to the syslog server IP (10.100.0.50), and the SyslogTargetPort is set to 514 (or whatever port syslog is listening on).

Figure 2-2 ApplicationSettings Syslog Configuration



```
8 <setting name="ApplicationName" serializeAs="String">
9 <value>OnGuard</value>
10 </setting>
11 <setting name="RawDatabaseVendor" serializeAs="String">
12 <value>PostgreSql</value>
13 </setting>
14 <setting name="AlarmsLink" serializeAs="String">
15 <value>http://localhost/#/alarms/id/{0}</value>
16 </setting>
17 <setting name="OnGuardHost" serializeAs="String">
18 <value>localhost</value>
19 </setting>
20 <setting name="ChangeSet" serializeAs="String">
21 <value>de1b0f1ef1b1</value>
22 </setting>
23 <setting name="AccessTokenExpireTimeSpan" serializeAs="String">
24 <value>336.00:00:00</value>
25 </setting>
26 <setting name="LogAlarmsToSyslog" serializeAs="String">
27 <value>True</value>
28 </setting>
29 <setting name="SyslogTargetHost" serializeAs="String">
30 <value>10.100.0.50</value>
31 </setting>
32 <setting name="SyslogTargetPort" serializeAs="String">
33 <value>514</value>
34 </setting>
35 </Ics2.Frontend.Web.Properties.Settings>
```

- c. Open **C:\OnGuardWebsite\log4net.config** in Notepad++ and verify that the appender **RemoteSyslogAppender** has a **remoteAddress** value of the syslog server IP (10.100.0.50).

```

52 </layout>
53 </appender>
54 <appender name="SqlAppender" type="log4net.Appender.RollingFileAppender">
55 <immediateFlush value="true" />
56 <file type="log4net.Util.PatternString" value="{ALLUSERSPROFILE}\ICS2\OnGuard\SQL\SQL
57 <rollingStyle value="Composite" />
58 <!-- rolling based on date and file size -->
59 <datePattern value="yyyy-MM-dd" />
60 <appendToFile value="true" />
61 <maximumFileSize value="50MB" />
62 <maxSizeRollBackups value="10" />
63 <!-- no deletion -->
64 <layout type="log4net.Layout.PatternLayout">
65 <param name="Header" value="===== Alarms - Begin on [{property{log4net:HostName}}
66 <param name="Footer" value="===== Alarms - End on [{property{log4net:HostName}}
67 <conversionPattern value="%message%n" />
68 </layout>
69 </appender>
70
71 <appender name="RemoteSyslogAppender" type="log4net.Appender.RemoteSyslogAppender">
72 <facility value="Local6" />
73 <identity value="OnGuard[{level}]{property{log4net:HostName}}" />
74 <layout type="log4net.Layout.PatternLayout" value="OnGuard|{message}" />
75 <remoteAddress value="10.100.0.50" />
76 </appender>
77
78 <appender name="MasterSplunkAppender" type="log4net.Appender.RemoteSyslogAppender">

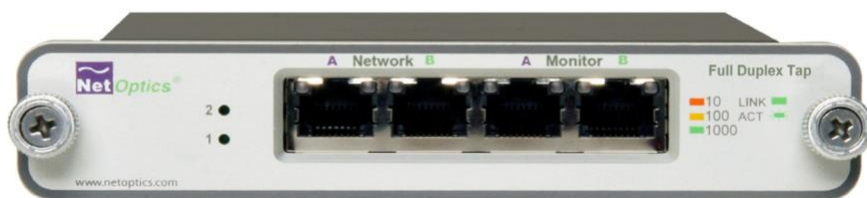
```

4. Close Notepad++ and open Google Chrome to *http://localhost/* for the login screen.

## 2.5 IXIA Full-Duplex Tap (O16)

The following is the installation for the IXIA TP-CU3 taps used in the lab.

Figure 2-3 IXIA TP-CU3 Network Tap



1. Mount the tap to the rack.
2. Utilize the supplied power cord to connect an outlet to the power jacks located on the rear of the tap.

3. To connect to the network ...

- a. Connect **Network Port A** to the Ethernet cable coming in from the control system network.
- b. Connect **Network Port B** to an Ethernet cable going out to the destination port of the original Ethernet cable used in the previous step.
- c. Verify that the link LEDs illuminate.
- d. Connect **Monitor Port A** to the monitoring port of the device used to monitor the ingress of **Network Port A**.
- e. Connect **Monitor Port B** to the monitoring port of the device used to monitor the ingress of **Network Port B**.

4. The tap installation and setup are complete.

## 2.6 OSIsoft PI Historian (E4, O8)

OSIsoft PI Historian is the primary historian type utilized in the build. The two instances serve as the main mirror of the control system's historian as well as a secondary historian located in the enterprise network. The secondary historian feeds the anomaly detection platform in the enterprise network.

For further information, visit <http://www.osisoft.com/federal/>.

### 2.6.1 OSIsoft PI Historian (E4) Installation Guide

The following are the installation and configuration for the OSIsoft PI Historian located within the enterprise network.

#### 2.6.1.1 Environment Setup

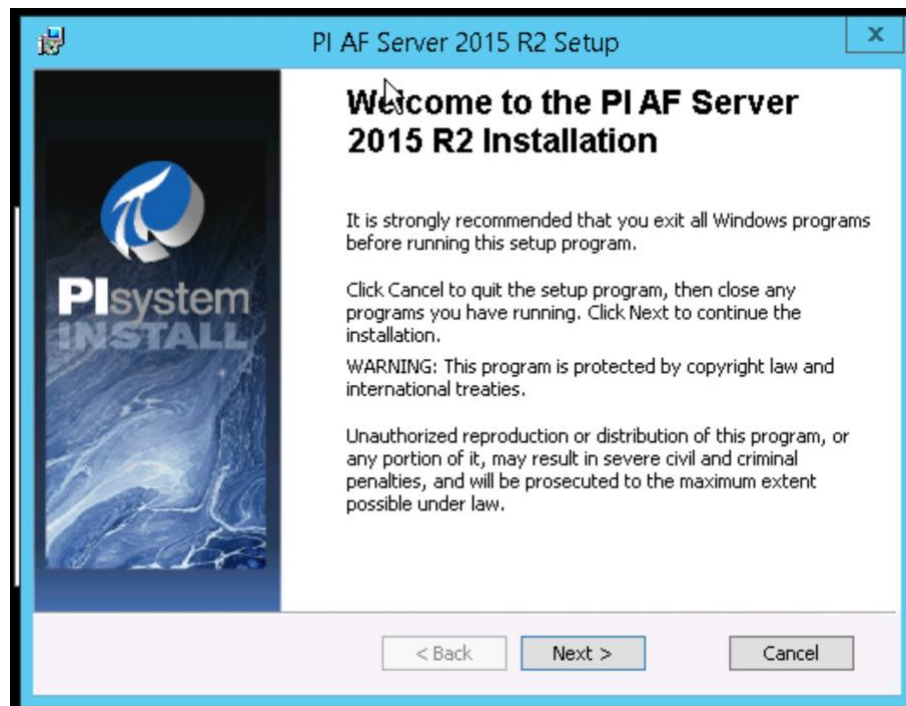
- Microsoft Windows Server 2012 R2
- 2.2 GHz processor
- 8 GB RAM
- 250 GB storage
- Structured Query Language (SQL) Server Express

#### 2.6.1.2 Installation Instructions

1. Create admin user in windows: **Piadmin**
2. Create admin user in windows: **Afadmin**

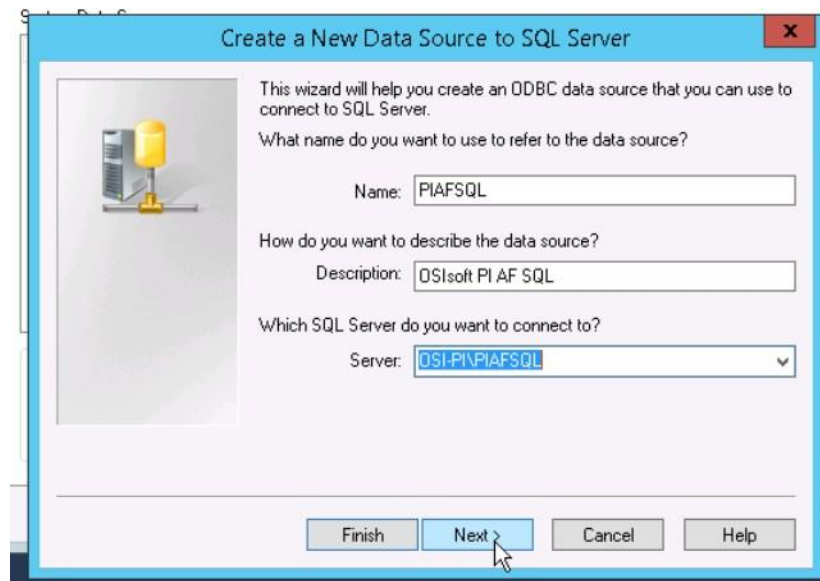
3. Create standard user in windows: **Piuser**
4. Create new folder **C:\Download**
5. Install SQL Server 2014.
  - a. Create instance:
    - i. Name: **PIAFSQL**
    - ii. Instance ID: **PIAF**
  - b. SQL Server Configuration Manager:
    - i. Enable SWL Server Network Configuration -> Protocols for PIAFSQL -> {Shared Memory, Named Pipes, TCP/IP}
6. Copy **PI-AF-Server\_2015-R2\_** to **C:\Download** and self-extract setup (run as administrator).
  - a. A reboot will be required.
  - b. After reboot, the Microsoft Visual C++ 2013 install window will appear.

Figure 2-4 PI AF Server 2015 R2 Setup



- c. On the “Welcome to the PI AF Server 2015 R2 Installation” screen ...
  - i. Click **Next**.
  - ii. Click **Next** to select default install directory.
  - iii. Click **Next** for default features.
  - iv. Select **Virtual User Account**.
  - v. Under SQL Server Connection, select **<hostname>\PIAFSQL** and click **Next**.
  - vi. Click **Install**.
- 7. Open **Open Database Connectivity (ODBC) Data Sources (64-bit)**.
  - a. Under System DSN, click **Add**.
    - i. Name: **PIAFSQL**
    - ii. Description: **OSIsoft PI AF SQL**
    - iii. Server: **<hostname>\PIAFSQL**

Figure 2-5 Create New Data Source for SQL

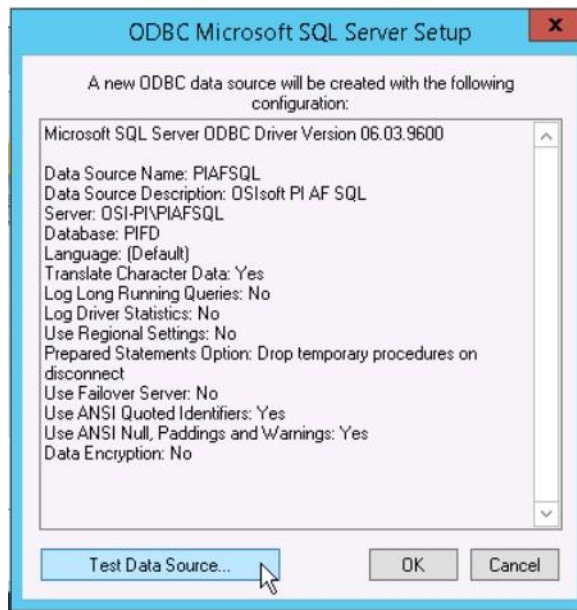


- b. Click **Next**.



- c. Click **Next**.
- d. Check the **Change the default database to:** and select **PIFD**.
- e. Click **Next**.
- f. Click **Finish**.
- g. Click **Test Data Source...**

Figure 2-6 Testing SQL Setup



- h. After a successful pass, click **OK** three times to close ODBC Data Sources.
8. Open Microsoft SQL Server Management Studio (as Administrator).
    - a. Ensure the settings are correct and click **Connect**.
    - b. In the left tab, select **<hostname>\PIAFSQL > Databases > PIFD > Tables** and ensure tables are listed.
    - c. Close Microsoft SQL Server Management Studio.
  9. Copy **PISDK\_2014\_** and **PISMT\_2015\_R2\_** to *C:\Downloads*.
  10. Copy **PI-AF-Client\_2015-R2\_** to *C:\Download* and run as administrator.



- a. Change the Extraction path to `.\`
  - b. When the PI AF Client 2015 R2 installation screen starts up, click **OK**.
  - c. In the Default Data server input, type `piafsql` and click **Next**.
  - d. Click **Next** for the default PIHOME directory.
  - e. Wait for the installation to finish and click **Next**.
  - f. Select whether to participate in the Customer Experience Improvement and click **Next**.
  - g. Click **Next** for default features, then click **Install**.
  - h. Verify that the Service Status screen shows all services started successfully, and click **Next**.
  - i. Click **Close**.
11. Run **PISDK\_2014\_** as administrator.
- a. Change the Extraction path to `.\`
  - b. When the PI Software Development Kit installation screen starts up, click **OK**.

Figure 2-7 PI SDK Setup



- c. On the screen listing services that will be stopped, click **OK**.
  - d. Verify that the Service Status screen shows all services started successfully, and click **Next**.
  - e. Click **Close**.
- 12. Run **PISMT\_2015\_R2\_** as administrator.
  - a. Change the Extraction path to **.\**
  - b. When the installation screen starts up, click **Next** twice.
  - c. On User Information, change the **Full Name** field to **Pladmin** and fill in **Organization**.
  - d. Click **Next**.
  - e. Click **Install**.
  - f. Click **Close**.
- 13. Run the **MSRuntimes** and **MSRuntimes\_x64** applications to install the proper DLLs.
- 14. Run **OSIprerequisites-standalone\_2.0.0.10\_** as administrator.
  - a. Click **OK**.
  - b. Change Unzip folder to **.\** and select **Unzip**.
  - c. When completed, click **Close**.
- 15. Run **OSIprerequisites-Patch\_2.1.1\_**
  - a. Change Unzip folder to **.\** and select **Unzip**.
  - b. When completed, click **Close**.
- 16. Reboot the machine.
- 17. Create the following folders:
  - a. **C:\PI**
  - b. **C:\PI\Bin**
  - c. **C:\PI\Dat**
  - d. **C:\PI\License**
  - e. **C:\PI\Queue**

- f. *C:\PI\Archive*
18. Copy a generated license file into *C:\PI\License* and name `pilicense.dat`.
  19. Copy *PIServer\_2012SP\_x64\_* to *C:\Downloads*.
  20. Run *PIServer\_2012SP\_x64\_* as Administrator.
    - a. Change the Unzip folder to *.\* and click **Unzip**.
    - b. When the PI Server 2012 SP1 64-bit installation screen starts up, click **OK**.
    - c. When it is showing what is installed, click **Close**.
    - d. On the welcome screen, click **Next**.
    - e. On licensing, click **Browse** and select *C:\PI\License*, then **Next**.
    - f. Verify that the AF Server is the host name, then click **Next**.
    - g. Ensure that **No** is selected for **enabling PI Module Database**, and click **Next**.
    - h. For PI Server Binaries, click **Browse** and select *C:\PI\Bin*.
    - i. For Event Queues, click **Browse** and select *C:\PI\Dat*.
    - j. For Archives, click **Browse** and select *C:\PI\Archive*.
    - k. Click **Next**.
    - l. Click **Next** to start installation.
    - m. When complete, click **Close**.
  21. Open **PI System Management Tools**.
    - a. Under Servers on the left, select the **piafsql server**.
    - b. Close **PI System Management Tools**.
  22. Reboot system.
  23. Copy *C:\PI\Bin\admin\pisrvstart.bat* and *C:\PI\Bin\admin\pisrvstop.bat* to the **Desktop**.
  24. Open **PISDKUtility**.
    - a. Under Tools, select **Add Server**.
      - i. Network Path/fully qualified domain name (FQDN): **<hostname>**
      - ii. Click **OK**.

- b. Under Default User Name for the new server, type **piadmin**.
- c. Under Connections, select **Options**.
  - i. Set the Connection time-out to **30 seconds**.
  - ii. For Default Server, select **<hostname>**.
  - iii. Ensure the **Protocol Order** is ...
    1. **PI Trust**
    2. **Default User**
    3. **Windows Security**
  - iv. Click **OK**.
- d. Under Connections, select **Aliases**.
  - i. Click **Add...**
  - ii. Under Alias, type the machine's **IP Address**.
  - iii. Click **OK**.
  - iv. Click **Close**.
- e. Click **Save**.

## 2.6.2 OSIsoft PI Historian (O8) Installation Guide

Follow the installation guide for OSIsoft PI Historian in [Section 2.6.1](#).

## 2.7 OSIsoft Citect Interface (O13)

The OSIsoft Citect Interface creates a connection for the OSIsoft PI Historian to interface with the SCADA server for aggregating historian data.

### 2.7.1 OSIsoft Citect Interface (O13) Installation Guide

1. Open the **pipc.ini** file located in **C:\Windows** (or the **%windir%** directory).
2. The file should contain the following info. If the file does not exist, create it and add the following lines:

```
[PIPC]

PIHOME=C:\Program Files (x86)\PIPC
```

3. Start the installation executable (**Citect\_#.#.#.#\_exe**).

4. This will install files in **PIHOME\Interfaces\Citect\**.
5. Copy the following files from the Citect machine's **Bin** directory into the **PIHOME\Interfaces\Citect\** directory.
  - a. **CtApi.dll**
  - b. **Ct\_ipc.dll**
  - c. **CtEng32.dll**
  - d. **CtRes32.dll**
  - e. **CtUtil32.dll**
  - f. **CiDebugHelp.dll**
6. To install the connector as a service, run **PI\_Citect.exe /install /auto /depend tcpip**. Test the connection between the interface node and the Citect node by using the **PI\_CitectTest.exe** connection tester.
7. Run the **interface configuration utility (ICU)**, and configure a new instance of this interface.
8. Define digital states.
9. **Cit\_Bad\_Conn** indicates communication problems with the Citect node.
10. Build input tags and, if desired, output tags for this interface by using the point builder utility **PI\_Citect\_PointBuilder.exe**. Important point attributes and their purposes are:
 

|                                           |                     |
|-------------------------------------------|---------------------|
| a. Location1 (interface instance ID):     | 1                   |
| b. Location2 (input/output parameter):    | 0 (input)           |
| c. Location3 (not used):                  | 0                   |
| d. Location4 (scan class):                | 1                   |
| e. Location5 (not used):                  | 0                   |
| f. ExDesc (optional, event-driven scans): | -                   |
| g. InstrumentTag:                         | [Citect point name] |
11. Start the interface interactively, and confirm its successful connection to the PI Server without buffering.
12. Confirm that the interface collects data successfully.

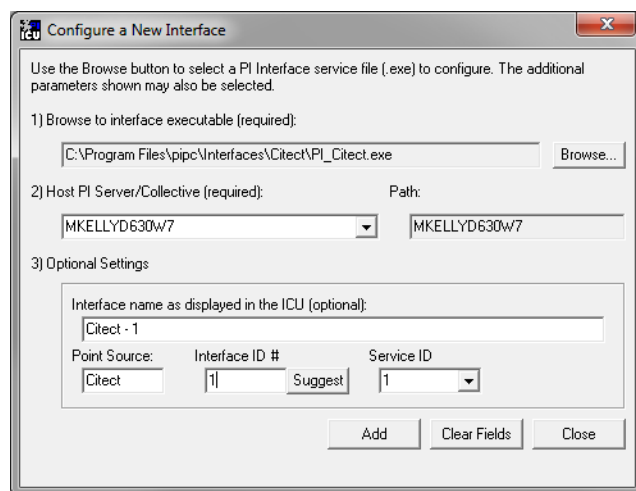
13. Stop the interface, and configure a buffering application (either Bufserv or PIBufss). When configuring buffering, use the ICU menu item **Tools > Buffering... > Buffering Settings** to make a change to the default value (32678) for the Primary and Secondary Memory Buffer Size (Bytes) to **2000000**. This will optimize the throughput for buffering and is recommended by OSIsoft.
14. Start the buffering application and the interface. Confirm that the interface works together with the buffering application by stopping the PI Server.
15. Configure the interface to run as an automatic service that depends on the PI Update Manager and PI Network Manager services.
16. Restart the interface node, and confirm that the interface and the buffering application restart.

## 2.7.2 Configuration

The PI Interface Configuration Utility provides a graphical user interface for configuring PI interfaces. If the interface is configured by the PI ICU, the batch file of the interface (PI\_Citect.bat) will be maintained by the PI ICU, and all configuration changes will be kept in that file and the module database. The procedure below describes the necessary steps for using PI ICU to configure the PI Citect interface.

1. From the PI ICU menu, select **Interface**, then **New Windows Interface Instance** from EXE..., and then **Browse** to the **PI\_Citect.exe** executable file. Then, enter values for **Host PI System**, **Point Source**, and **Interface ID#**. A window such as the following results:

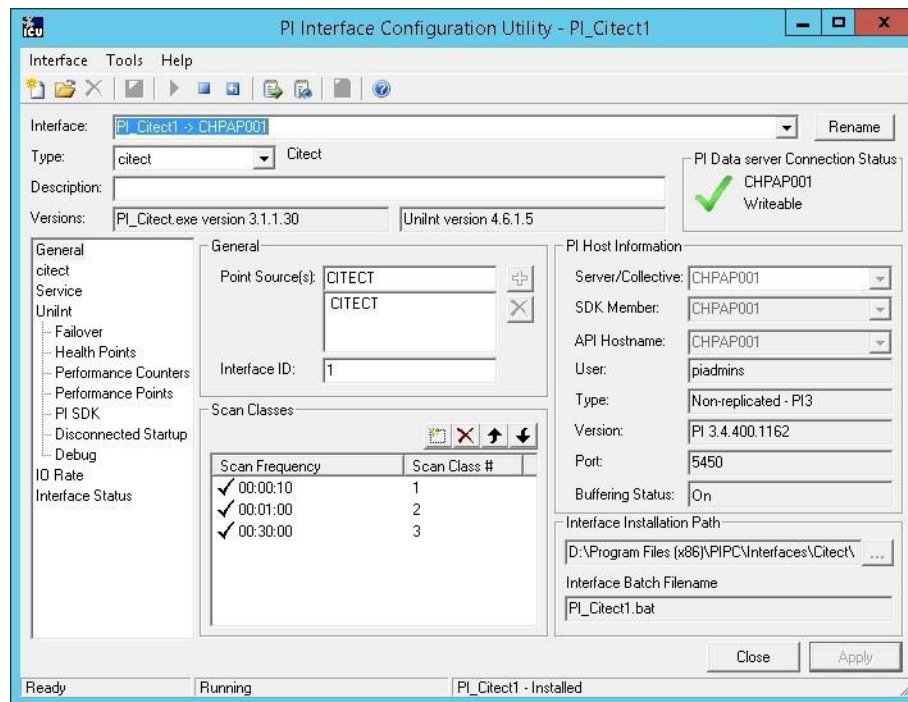
**Figure 2-8 Configure New Interface**



2. **Interface name as displayed in the ICU (optional)** will have PI- pre-pended to this name, and it will be the display name in the services menu.

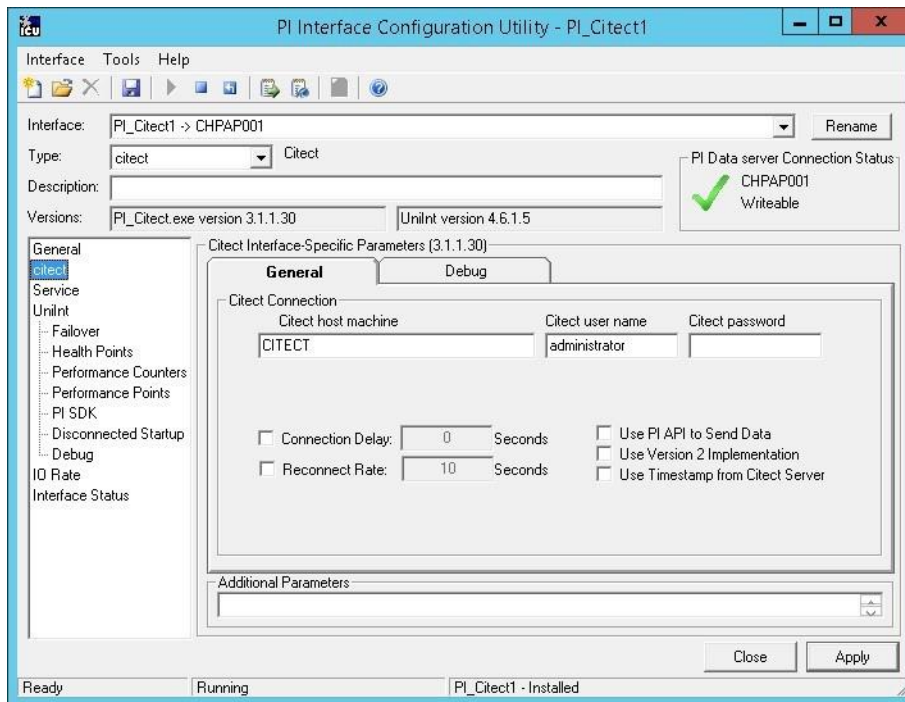
3. Click **Add**.
4. Once the interface is added to PI ICU, near the top of the main PI ICU screen, the interface **Type** should be **Citect**. If not, use the drop-down box to change the interface Type to be Citect.
5. Click on **Apply** to enable the PI ICU to manage this instance of the PI Citect interface.

**Figure 2-9 ICU — General Configuration**



6. Because the start-up file of the PI Citect interface is maintained automatically by the PI ICU, use the Citect page to configure the start-up parameters, and do not make changes in the file manually.

Figure 2-10 ICU — Citect ICU Control



7. Supply values for the fields in the Citect **General** tab as follows:

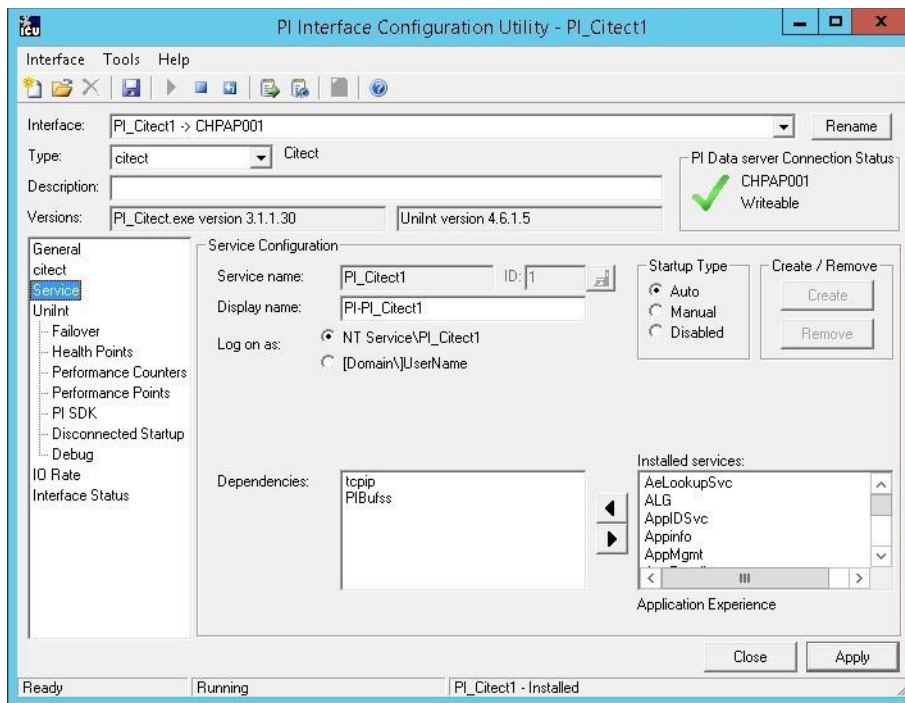
- a. Citect host machine — **CITECT**
- b. Citect username — **administrator**
- c. Citect password — **<enter password here>**
- d. Connection Delay — **none (unchecked)**
- e. Reconnect Rate — **none (unchecked)**
- f. Use PI API data to Send Data — **(unchecked)**
- g. Use Version 2 Implementation — **(unchecked)**
- h. Use Timestamp from Citect Server — **(unchecked)**

8. Keep the defaults on the Citect **Debug** tab.



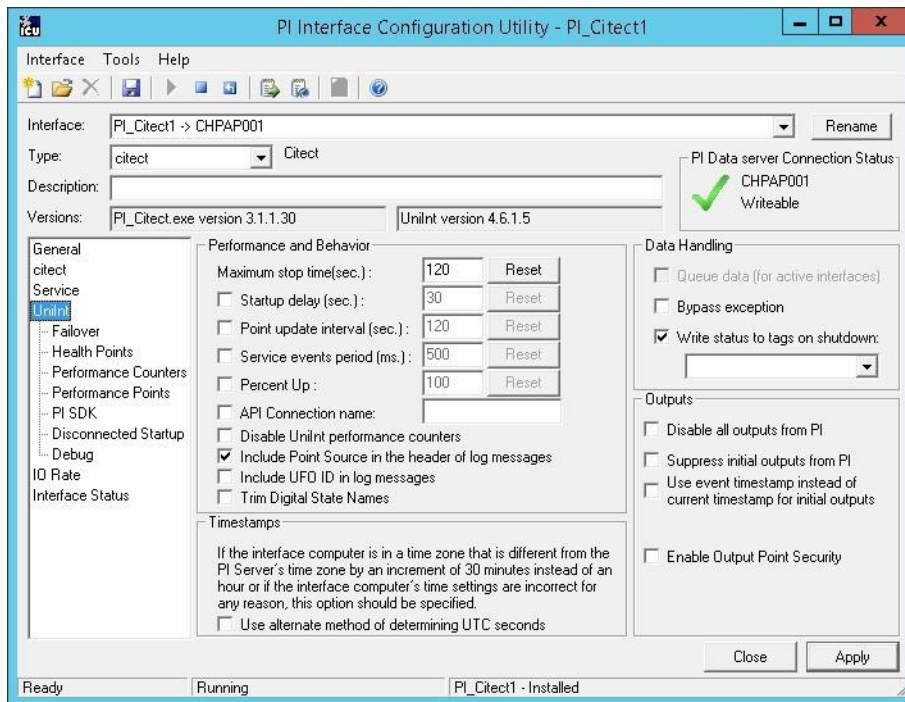
- To set up the interface as a Windows Service, use the **Service** page. This page allows configuration of the interface to run as a service as well as starting and stopping the interface service. Keep the default values, as shown below.

**Figure 2-11 ICU — Windows Service Setup**



- Because the PI Citect interface is a Unilnt-based interface, the Unilnt page allows the user to access Unilnt features through the PI ICU and to make changes to the behavior of the interface.

Figure 2-12 ICU — Unilnt Configuration



11. Keep the default values, but check the following boxes:

- a. **Include Point Source in the header log of messages**
- b. **Write status to tags on shutdown**

12. Uncheck the following box:

**Suppress initial outputs from PI**

## 2.8 RS2 Technologies Access It! Universal.NET (E7)

RS2 Technologies Access It! Universal.NET pairs with the RS2 Door Controller to monitor access into the lab utilized in the build. The software then alerts the SIEM for any access into the facility, allowing the SIEM to correlate network events with physical access events.

## 2.8.1 Environment Setup

The following configuration matched requirements for the product relative to the use in the example solution:

- Microsoft Windows Server 2012 R2
- VM with CPU Quad Core 2.199 GHz
- VM with 8,192 MB of memory
- virtual hard disk containing 240 GB of storage
- .NET Framework 3.5

### 2.8.1.1 Product Installation

1. Start the provided **AIUniversalNET51044CD.exe**.
2. Follow the prompts for installation:
  - a. Select **Stand-Alone/Server Installation**.
  - b. Select **I do not have a SQL Server Installed**.
  - c. When prompted to install SQL Server 2008 R2 Express Edition, select **Yes**.
  - d. Select **Install Access It! Universal.NET**.
  - e. When prompted to install a Stand-Alone Server version of Access It! Universal.NET, select **OK**.
  - f. Select **Next >**.
  - g. Read the license agreement and select **Next >** if the terms of the agreement are agreeable.
  - h. Use the default installation folder **C:\Program Files(x86)\RS2 Technologies\Access It! Universal.NET\**, then select **Next >**.
3. When the installer is ready, select **Next >** to continue.
4. Select **Close** to exit the installer.

## 2.8.2 Post-Installation and Configuration

Post-installation and configuration are partially dependent on installation and configuration of the RS2 Technologies Door Controller (O4). If that is not complete, please follow that guide first before attempting to complete the post-installation of Access It! Universal.NET (E7).

1. Launch Access It! Universal.NET by selecting it from the **Start** menu.

2. Log in with the default username **Admin**. Leave password blank.

### *2.8.2.1 Connecting Access It! Universal.NET*

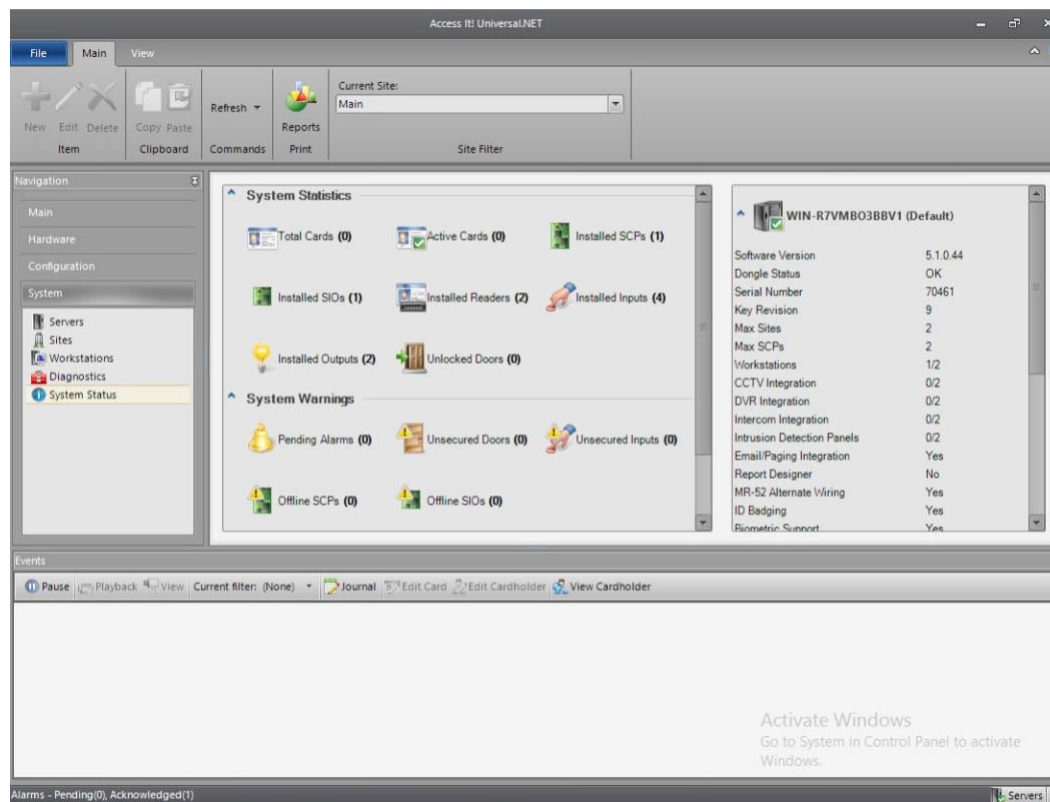
1. Select **Hardware** under the Navigation pane, then select the **Channels** pane.
2. Select the **green + sign** in the top left corner to create a new channel.
3. For Channel Type, select **IP server**.
4. Ensure Protocol Type is secure copy protocol (**SCP**).
5. Ensure **Channel Enabled** is checked.
6. Select **Save**.
7. Select **SCPs** under the Navigation pane on the left.
8. Select the **green + sign** in the top left corner to create a new SCP.
9. Under the **General** tab ...
  - a. Select **EP-1502** for Model.
  - b. Ensure **Device installed** is checked.
  - c. Set **SCP time zone** to the local time zone of the door controller.
10. Under the **Comm.** tab ...
  - a. Ensure that the channel created in the previous steps is listed.
  - b. Set the IP address to **10.100.2.150**.
  - c. Ensure the port number is set to **3001**.
  - d. Ensure the Encryption Settings is set to **None**.
11. Select **Save**.

### *2.8.2.2 Enable TCP/IP for Local SQL 2008 R2 Express Edition Server*

1. Launch **Microsoft SQL Server Configuration Manager**.
2. Expand **SQL Server Network Configuration (32-bit)**.
3. Select **Protocols** for **AIUNIVERSAL**.
4. Right-click on **TCP/IP**, then select **Properties**.

5. Select the **IP Addresses** tab.
6. Under **IP1**, ensure that **IP Address** is set to **0.0.0.0**, and **TCP Port** is set to **1433**.
7. Under **IPALL**, ensure that **TCP Dynamic Ports** is set to **52839**, and **TCP Port** is set to **1433**.
8. Restart the SQL Server. Select **SQL Server Services**, then right-click on **SQL Server (AIUNIVERSAL)** and select **Restart**.

**Figure 2-13 System Status**



## 2.9 RS2 Technologies Door Controller (O4)

The RS2 Technologies Door Controller is the physical piece to the Access It! Universal.NET product. This piece connects to the door itself, alerting the software to any access to the location.

### 2.9.1 Hardware Installation

The following instructions detail the hardware installation for the door controller:

1. The fully assembled and closed case:

Figure 2-14 RS2 Door Controller Case



2. The interior modules:

Figure 2-15 Inside of RS2 Door Controller Case



3. The battery is pictured in the lower right corner of the case. The smaller board (AC/DC inverter) is pictured below:

Figure 2-16 AC/DC Inverter



4. The two cables to the left are for positive and neutral input from a low voltage AC power supply. The ground (green) cable from the AC power supply attaches to a grounding nut on the case (pictured in the previous figure).

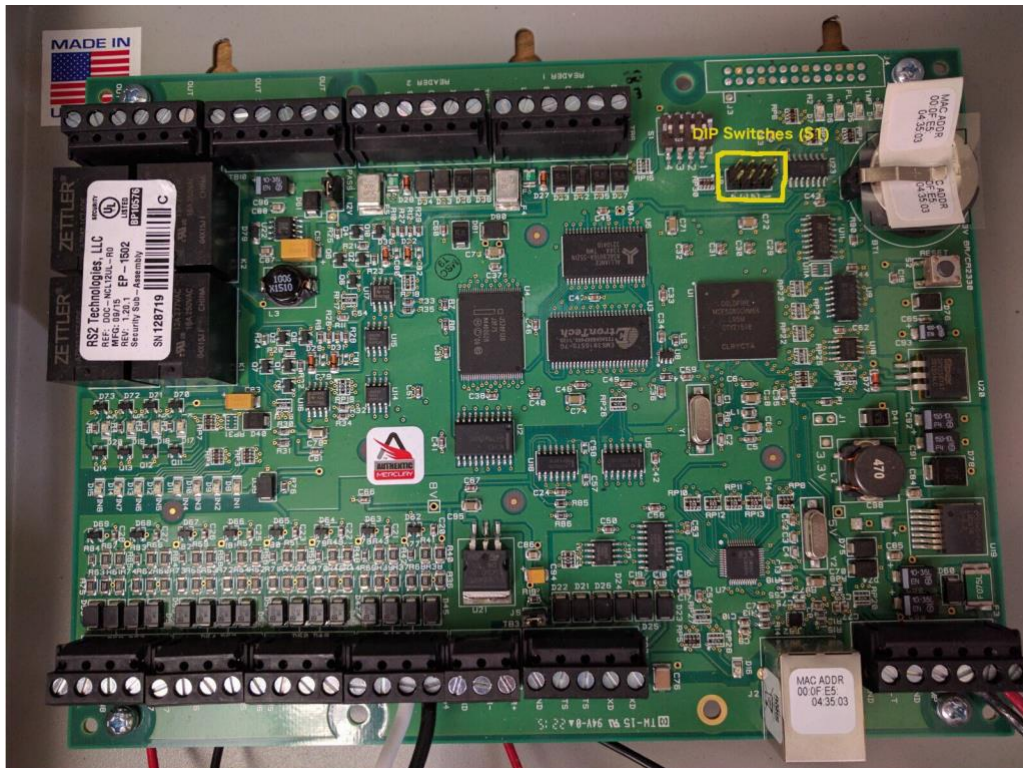
The black and red cables to the left of AC are the DC outputs. These supply power directly to the door controller EP-1502 board.

The other two black and red wires, connected to a harness, sit in the BATTERY port of the smaller board. These provide a trickle charge to the battery, which can be used in the event of a power outage.

The larger EP-1502 board is pictured below:



Figure 2-17 EP-1502 Door Controller Board



5. The white and black wires on the bottom center of the figure go into **Door Contact 1 - IN1**, and these connect to the physical door-monitoring devices.
6. Power is supplied to the board via the bottom right corner posts, for 12 to 24 VDC (max 500 mA).

### 2.9.2 Connecting Hardware to Access It! Universal.NET

Conduct the following steps to connect the EP-1502 Door Controller Board to the Access It! Universal.NET software. The DIP switches referenced in these steps apply to those highlighted in yellow in the figure above.

1. Ensure that DIP Switch **DIP 2** is **ON** and **1, 3, and 4** are **OFF**.
2. Power on the EP-1502.
3. Manually configure a computer to **192.168.0.100**.
4. Using a crossover cable, connect the computer to the EP-1502 board.
5. Open a web browser, and navigate to *http://192.168.0.251*.

6. Set DIP Switch **DIP 1** to **ON**.
7. Select Click Here to Login.
8. Select **Continue to this website (not recommended)**.
9. Log in with username **admin** and password **password**.
10. Select **Network** on the left-hand menu.
11. Select **Use Static IP configuration**.
  - a. IP Address: **172.18.3.50**
  - b. Subnet Mask: **172.18.0.0/16**
  - c. Default Gateway: **172.18.0.1**
12. Click **OK**.
13. Click **Apply Setting**.
14. Click **Apply, Reboot**.
15. Wait 60 seconds for the EP-1502 to reboot.
16. Remove power from the EP-1502.
17. Set **all DIP switches** to **OFF**.
18. Remove the crossover cable, and connect to the network.
19. Apply power to the EP-1502 and follow the instructions in [Section 2.8.2](#), Post-Installation and Configuration.

## 2.10 Radiflow 3180 (O14)

Radiflow's 3180 is a secure, ruggedized router used to handle connections between the OSIsoft Citect Interface and the OSIsoft PI Historian. This device ensures that proper communication is allowed while stopping any traffic that is not required.

### 2.10.1 Radiflow 3180 (O14) Installation Guide

1. Log in with the **su** user with the provided username and password.
2. Enter the following commands:
  - a. `config terminal`
  - b. `ip access-list extended 1001`

c. permit tcp host 172.16.2.170 eq 5450 host 172.18.2.150 eq 5450 priority 1

d. exit

e. interface fastethernet 0/1

f. ip access-group 1001 in

g. exit

h. ip access-list extended 1002

i. permit tcp host 172.16.2.150 eq 5450 host 172.18.2.170 eq 5450 priority 2

j. exit

k. interface fastethernet 0/2

l. ip access-group 1002 in

m. exit

n. ip access-list extended 2001

o. deny ip any any priority 51

p. exit

q. interface fastethernet 0/1

r. ip access-group 2001 in

s. exit

t. ip access-list extended 2002

u. deny ip any any priority 52

v. exit

w. interface fastethernet 0/2

x. ip access-group 2002 in

y. exit

z. write start

aa. reload

## 2.11 Radiflow iSID (O11)

Radiflow's iSID product is a software industrial intrusion detection system that monitors for anomalies within the control systems network and builds a network topology model.

### 2.11.1 Environment Setup

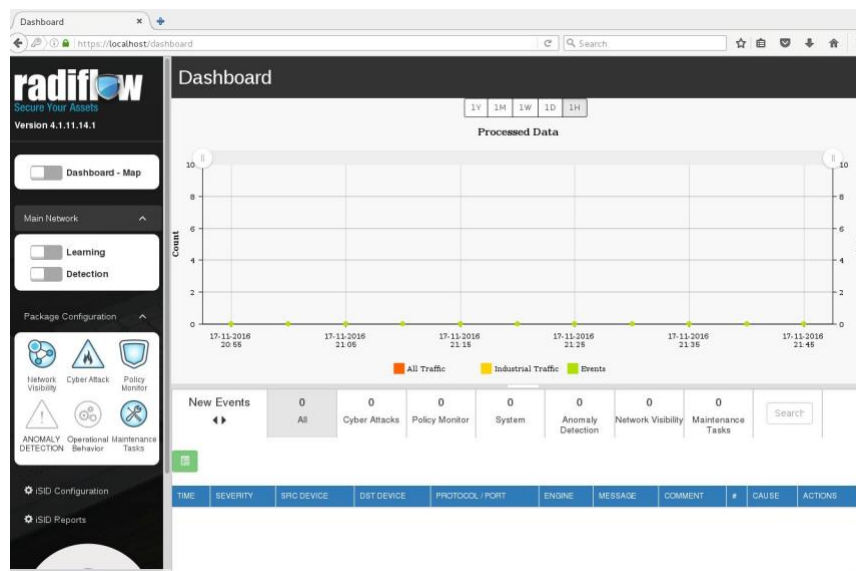
Radiflow supplies an open virtual appliance (OVA) to be deployed to a virtualized environment, so environment setup should be minimal.

### 2.11.2 Product Installation

1. After deploying the vendor-provided OVA on a virtualized platform, navigate to **/home/radiflow/isid**.
2. Modify the **server.conf** file to reflect the IP address of the syslog server:

```
rfids_remote_syslog_server=172.18.0.50
poco_source_dir=/home/radiflow/tools/poco
```
3. Run **sudo ./build\_install\_all.sh stop start install config bridge**.
4. Open a web browser, and navigate to **https://localhost/dashboard**.

Figure 2-18 Radiflow iSID Web Dashboard



5. Toggle the **Learning** switch on the left bar under Main Network.

Allow learning to take place for **5 to 7 days**.

6. Toggle the **Detection** switch on the left bar under Main Network.
7. Setup and configuration are now complete.

## 2.12 RSA Archer Security Operations Management (E13)

Governance, risk, and compliance (GRC) platforms allow an organization to link strategy and risk, adjusting strategy when risk changes, while remaining in compliance with laws, regulations, and security policies. RSA Archer Security Operations Management, based in part on the RSA Archer GRC platform, was used to perform the task of the Analysis Workflow Engine and Security Incident Response and Management.

For more information, visit ...

- <https://www.rsa.com/en-us/resources/rsa-netwitness-secops-manager>
- <https://www.rsa.com/en-us/products/threat-detection-and-response/rsa-netwitness-secops-manager>
- <https://www.rsa.com/en-us/products/threat-detection-and-response/network-monitoring-and-forensics>

### 2.12.1 System Requirements

This build installed a multihost RSA Archer GRC platform node on a VMware VM with the Microsoft Windows Server 2012R2 operating system to provide the Security Incident Response Management environment needed.

*Note: All components, features, and configurations presented in this guide reflect what we used based on vendors' best practices and requirements. Please refer to vendors' official documentation for complete instructions for other options.*

### 2.12.2 Preinstallation

We chose the multihost deployment option for installing and configuring the GRC platform on multiple VMs under the Microsoft Windows Server 2012R2 Operating System. The web application and services are running on one server, instance database/Microsoft SQL Server is running on one server, and integration components for Security Incident Response are running on a third server. Below are the preinstallation tasks that we performed prior the RSA Archer installation:

- Operating System: Windows Server 2012R2 Enterprise
- Database: Microsoft SQL Server 2012 Enterprise (x64)

Follow Microsoft's installation guidelines and steps to install the SQL Server Database Engine and SQL Server Management tools. Refer to [https://msdn.microsoft.com/en-us/library/bb500395\(v=sql.110\).aspx](https://msdn.microsoft.com/en-us/library/bb500395(v=sql.110).aspx) for additional details.

We used the following configuration settings during the installation and configuration process. We also created the required database instances and users for the RSA Archer installation. Test the database instances by using different users to verify the login permissions on all database instances and configuration databases to ensure that database owners have sufficient privileges and correct user mappings.

**Table 2-2 RSA Archer Configuration Settings**

| Setting                                                                                                                                          | Value                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Collation settings set to case insensitive for instance database                                                                                 | SQL_Latin1_general_CP1_CI_AS                                  |
| SQL compatibility level set appropriately                                                                                                        | SQL Server 2012 - 110                                         |
| Locale set                                                                                                                                       | English (United States)                                       |
| Database server time zone                                                                                                                        | EST                                                           |
| Platform language                                                                                                                                | English                                                       |
| Create both the instance and configuration databases within a single SQL Server instance. For migration, create only the configuration database. | Database names:<br><i>grc-content</i><br><i>grc-config</i>    |
| User Account set to Database Owner role                                                                                                          | <i>grc-content-archeruser</i><br><i>grc-config-archeruser</i> |
| Recovery Model                                                                                                                                   | Simple (configuration and instance databases)                 |
| Auto Shrink                                                                                                                                      | False (configuration database)                                |
| Auto-Growth                                                                                                                                      | Set it for (instance database)                                |
| Max Degree of Parallelism                                                                                                                        | 1 (configuration and instance databases)                      |

## Web and Services

- Microsoft Internet Information Services (IIS) 8
- Microsoft .NET Framework 4.5

Use Server Manager for installing IIS and .NET Framework, referring to <http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012> for detailed steps and corresponding screenshots.

First install IIS and then install the .NET Framework.

Table 2-3 below summarizes the required IIS components and .NET Framework features followed by the screenshots.

**Table 2-3 IIS Components and .NET Framework**

| Required Option             | Value                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IIS</b>                  |                                                                                                                                                    |
| Common (http) Features      | Default Document<br>Directory Browsing<br>http Errors<br>Static Content                                                                            |
| Health and Diagnostics      | http Logging                                                                                                                                       |
| Application Development     | .NET Extensibility 4.5<br>Active Server Pages (ASP) .NET 4.5<br>Internet Server Application Programming Interface (ISAPI) Extensions ISAPI Filters |
| Security                    | Request Filtering                                                                                                                                  |
| Management Tools            | IIS Management Console                                                                                                                             |
| <b>.NET Framework</b>       |                                                                                                                                                    |
| .NET Framework 4.5 Features | .NET Framework 4.5<br>ASP.NET 4.5                                                                                                                  |
| WCF Services                | http Activation TCP Port Sharing                                                                                                                   |

Figure 2-19 Web Server (IIS) Components Section

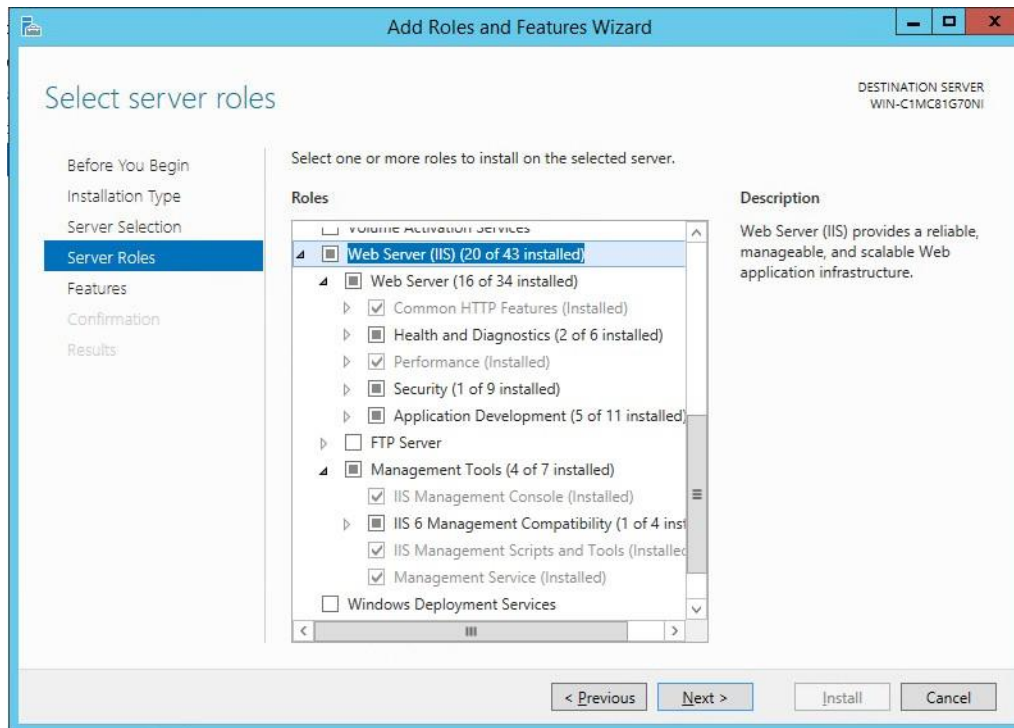
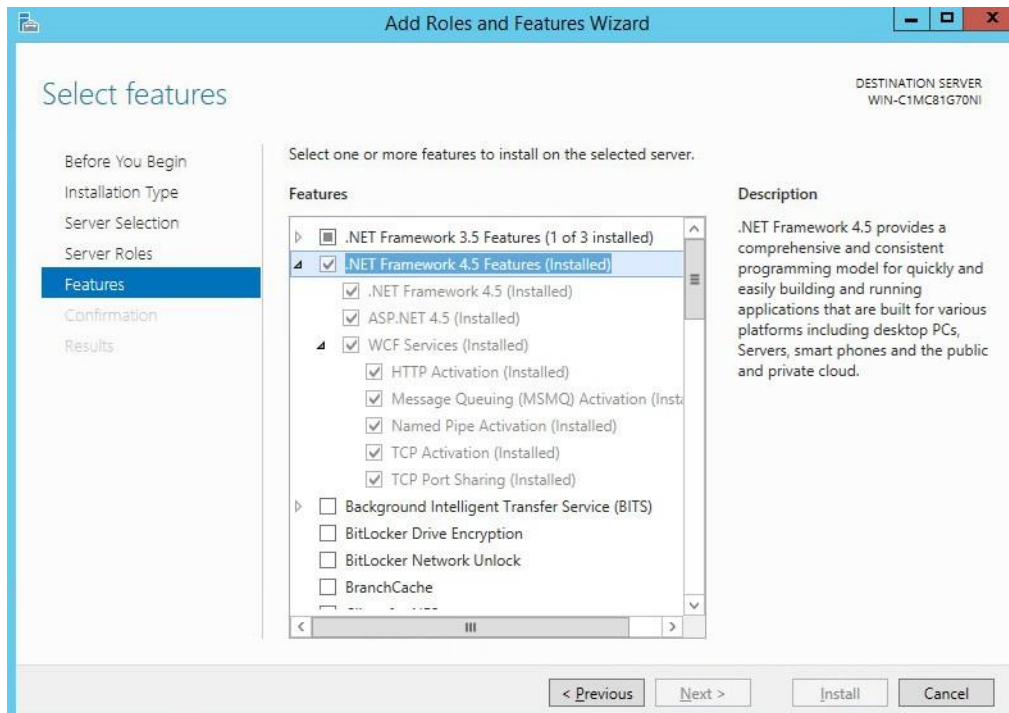




Figure 2-20 .NET Framework 4.5 Features Selection



### Microsoft Office 2013 Filter Pack

Download it from Microsoft website <http://www.microsoft.com/en-us/download/details.aspx?id=40229> and install it.

### Java Runtime Environment (JRE) 8

Download and install JRE 8. Refer to <http://www.oracle.com/technetwork/java/javase/install-windows-64-142952.html> for details.

**Note:** All preinstallation software must be installed and configured before installing RSA Archer.

### 2.12.3 Installation

1. Create folders **C:\ArcherFiles\Indexes** and **C:\ArcherFiles\Logging** (will be used later).
2. Obtain/Download the installer package from RSA; extract the installation package.
3. Run installer.
  - a. Open installation folder; right-click on **ArcherInstall.exe**.

- b. Select **Run as Administrator**.
- c. Click **OK** to run the installer.
- d. Follow the prompts from the installer for each step, set the value, and click **Next**.
- e. Select all components (Web Application, Services, Instance Database) for installation, then click **Next**.
- f. Specify the X.509 Certification by selecting it from the checklist (create new cert or use existing cert). We created a new cert.
- g. Set the Configuration Database options with the following properties:

|             |                                                                                                |
|-------------|------------------------------------------------------------------------------------------------|
| SQL Server: | <ip address of SQL Server>                                                                     |
| Login Name: | #####                                                                                          |
| Password:   | #####                                                                                          |
| Database:   | grc-config (This is the configuration database we created during the preinstallation process.) |
- h. Set the Configuration Web Application options with the following properties:

|                        |                                                                         |
|------------------------|-------------------------------------------------------------------------|
| Website:               | Default Website                                                         |
| Destination Directory: | Select Install in an IIS application option with RSAarcher as the value |
- i. Set Configuration of the Service Credentials.

Select **Use the Local System Account to Run All** from the checklist.
- j. Set the Services and Application Files paths with the following properties:
  - i. Services: use the default value **C:\Program Files\RSA Archer\Services\**.
  - ii. Application Files: use the default value **C:\Program Files\RSA Archer\**.
- k. Set the Log File Path to **C:\ArcherFiles\Logging**.
- l. Perform the installation by clicking **Install**, wait for the installer to complete installing all components, then click **Finish**. The RSA Archer Control Panel opens.

## 2.12.4 Post-Installation

### 2.12.4.1 *Configure the Installation Settings*

Verify and set the configurations for the following by clicking on **RSA Archer Control Panel > Installation Settings**, then select corresponding sections:

1. Logging Section
  - a. Path: **Archer Files\Logging**
  - b. Level: **Error**
2. Locale and Time Zone Section
  - a. Locale: **English (United States)**
  - b. Time Zone: **(UTC-05:00) Eastern Time (US & Canada)**
3. On the Toolbar, click **Save**.
4. Create the Default GRC Platform Instance.
  - a. Start the RSA Archer Queuing Service by doing the following steps:
    - i. Go to **Start**.
    - ii. Open **Server Manager**.
    - iii. Locate **RSA Archer Queuing** in the list under the **SERVICES** section.
    - iv. Right-click **RSA Archer Queuing**, and click **Start**.
  - b. Add a new instance by doing the following steps:
    - i. Open the **RSA Archer Control Panel**.
    - ii. In **Instance Management**, double-click **Add New Instance**.
    - iii. Enter **SituationalAwareness** as the **Instance Name**, then click **Go**.
    - iv. Complete the properties as needed.
  - c. Configure the Database Connection Properties by doing the following steps:
    - i. Open the **RSA Archer Control Panel**.
    - ii. In the **Database** tab, go to the **Connection Properties** section.
    - iii. In **Instance Management**, double-click the **SituationalAwareness** instance.

- d. In the **Database** tab, set up the following:
        - i. SQL Server: **<ip address of SQL Server>**
        - ii. Login name: **xxxxxx**
        - iii. Password: **xxxxxx**
        - iv. Database: **grc-content**
  5. Click on the **Test Connection** link to make sure the **Success** message appears.
  6. Configure the **General Properties** by doing the following steps:
    - a. Open **RSA Archer Control Panel**.
    - b. Go to **Instance Management**.
    - c. Under **All Instances**, click on **SituationalAwareness**.
    - d. In the **General** tab, set up the following:
      - i. **File Repository** section — Path **C:\ArcherFiles\Indexes**.
      - ii. **Search Index** section — **Content Indexing**: Check on Index design language only;  
Path: **C:\ArcherFiles\Indexes\SituationalAwareness**
  7. Configure the **Web Properties** by doing the following steps:
    - a. Open the **RSA Archer Control Panel**.
    - b. Go to **Instance Management**.
    - c. Under **All Instances**, click on **SituationalAwareness**.
    - d. In the **Web** tab, set up the following:
      - i. Base uniform resource locator (URL): *http://localhost/RSAArcher/*
      - ii. Authentication URL: **default.aspx**
  8. Change **SysAdmin** and **Service Account** passwords by doing the following steps:
    - a. Open the **RSA Archer Control Panel**.
    - b. Go to **Instance Management**.
    - c. Under **All Instances**, click on **SituationalAwareness**.
    - d. Select the **Accounts** tab.

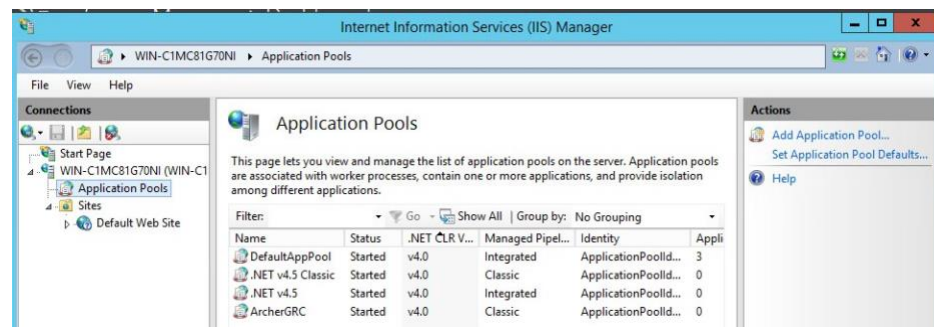
- e. Change the password on the page by using a strong password.
  - f. Complete the Default GRC Platform Instance Creation by clicking **Save** on the toolbar.
9. Register the Instance by doing the following steps:
- a. Open the **RSA Archer Control Panel**.
  - b. Go to **Instance Management**.
  - c. Under **All Instances**, right-click on **Situational Awareness**.
  - d. Select **Update Licensing**, enter the following information, then click on **Active**:
    - i. **Serial Number** (obtained from RSA)
    - ii. **Contact Info** (First Name, Last Name, Company, etc.)
    - iii. **Activation Method** (select Automated)
10. Activate the Archer Instance by doing the following steps:
- a. Start the **RSA Archer Services**.
  - b. On **Server Manager**, go to **Local Services** or **All Services**.
  - c. Locate the following services, right-click on each service, and click **Start**.
    - i. **RSA Archer Configuration**
    - ii. **RSA Archer Job Engine**
    - iii. **RSA Archer Lightweight Directory Access Protocol (LDAP) Synchronization**
  - d. Restart the **RSA Archer Queuing Service**.
    - i. Open **Server Manager**.
    - ii. Go to **Local Services** or **All Services**.
    - iii. Locate the **RSA Archer Queuing**.
    - iv. Right-click on **RSA Archer Queuing**, and click **Restart**.
  - e. Rebuild the Archer Search Index.
    - i. Open **RSA Archer Control Panel**.
    - ii. Go to **Instance Management**.

- iii. Under **All Instances**, right-click on **SituationalAwareness**, then click on **Rebuild Search Index**.

11. Configure and activate the Web Role (IIS).

- a. Set up **Application Pools** as shown in the screenshot.
  - i. Open **Server Manager**.
  - ii. Navigate to **Tools > IIS Manager > Application Pools** (in the left side bar).
  - iii. Right-click to add applications (.NET, ArcherGRC, etc.); example screenshot is below.

Figure 2-21 Application Pools



- b. Restart IIS.

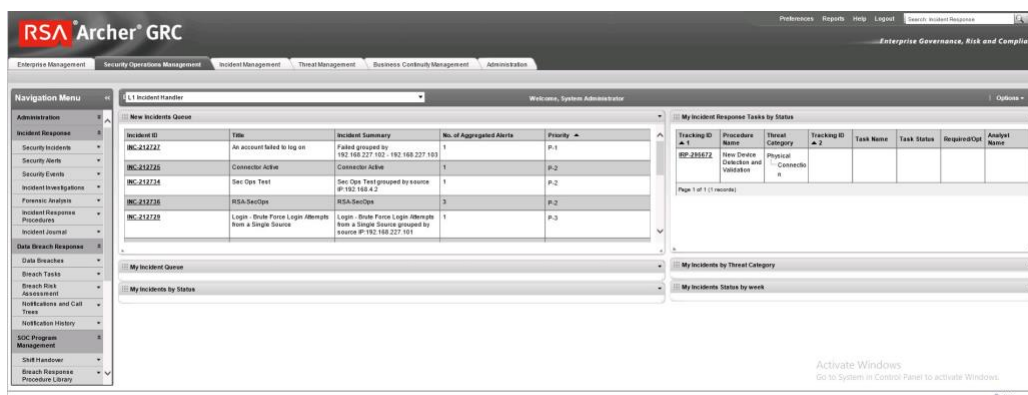
12. Verify that RSA Archer GRC is accessible by opening a browser and inserting the **Base** and **Authentication URL** from the Web tab of the RSA Archer Control Panel. The RSA Archer GRC Login screen appears as shown below.

Figure 2-22 RSA Archer User Login



13. Log in to **SituationalAwareness** Instance.

Figure 2-23 Security Operations Management Tab



## 2.12.5 Configuration of ArcSight ESM to RSA Archer Security Operations Management

After a base installation of RSA Archer and the associated RSA Archer Security Operations Management functionality, an additional configuration is required to connect the Security Incident Response use case to external data providers, such as ArcSight ESM. In this environment, this required an installation and

configuration of the RSA Archer Unified Collector Framework on the third Windows Server in the Archer multihost setup. For full details, please consult the installation and configuration guide for the RSA Collector Framework.

1. Create user within RSA Archer framework for the Collector Framework Web Services access. For testing, this user was granted appropriate privileges to read and write data for Security Alert Data originating from ArcSight.
2. Execute Archer Unified Collector Framework installer. When prompted, provide the Archer Collector Framework Web Services username and password created in step 1.
3. When prompted, follow the instructions for importing the Data Feed for the Unified Collector Framework (UCF).

### 2.12.6 Additional ArcSight Integration Configuration

Additional details for the ArcSight installation can be found in the RSA Archer Security Operations Management Implementation Guide from RSA. Below are the steps that were followed specifically for this environment to enable the connection to ArcSight.

1. Create ArcSight Forwarding Connector User.
  - a. From **ArcSight ESM Console**:
    - i. Create a new group under custom user groups and name as follows:  
**FwdConnector**
    - ii. Create a new user under that group and name as follows: **FwdConnectorUser**
    - iii. Set the user type to **Forwarding Connector**.
    - iv. For additional detail, see pages 7 – 9 of  
FwdConn\_ConfigGuide\_7.0.7.7286.0.pdf.
2. Install **SuperConnector** (also known as Forwarding Connector).
  - a. From the **ArcSight ESM Manager command line** ...
    - i. Su to **arcsight** user
    - ii. Find the install file **ArcSight-7.0.7.7286.0-Superconnector.bin**, and run the following command (to allow the installation to execute):  

```
chmod + x ArcSight-7.0.7.7286.0-Superconnector.bin
```
    - iii. Make a folder for the connector:  
  
e.g., 

```
mkdir /opt/arsight/superconnector
```



- iv. As **arcsight** user, execute the installation file:  
**./ArcSight-7.0.7.7286.0-Superconnector.bin**
- v. Choose to install to the folder that was just made:  
e.g., **/opt/arcsight/superconnector**
- vi. Accept defaults.
- vii. Choose **Don't Create Links**.
- viii. **Install**.
- ix. **Next**.
- x. Enter the ArcSight ESM Manager name: **[hostname]**
- xi. Enter the ArcSight ESM Manager port: **8443**
- xii. Enter the name of the user that was just created: **FwdConnectorUser**
- xiii. Enter the ArcSight Manager password: \_\_\_\_\_
- xiv. Import the manager certificate.
- xv. Select **CEF Syslog**.
- xvi. Enter the IP address of the RSA Archer UCF IP, Port: **514, TCP** (not UDP)
- xvii. Select **Next** twice, **Exit, Done**.
- xviii. As user **root**, install the service as follows:  

```
/opt/arcsight/superconnector/current/bin/arcsight agentsvc -i
-u arcsight
```
- xix. Start the service as follows:  

```
./etc/init.d/arc_superagent_ng start
```

Note: If another forwarding destination needs to be added, see page 32 of *FwdConn\_ConfigGuide\_7.0.7.7286.0.pdf*.

## 2.12.7 Sample Use Case Demonstration

For the use of the Security Incident Response use case and integration with ArcSight, the following sample use case was simulated:

### 1. Event 1

An individual enters a substation, an event that is detected by a door controller. This door reader is able to log its data or a SIEM, such as ArcSight, including identifying information (such as a badge ID or user).

### 2. Event 2

A new device appears on the substation network, detected by a tool (for example, CyberLens). This data is reported via a log event to a SIEM such as ArcSight.

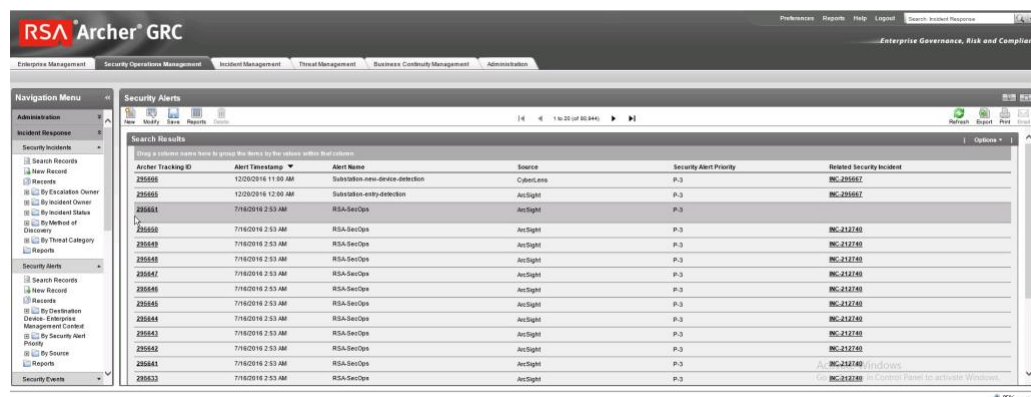
### 3. Action 1

An Alert/Correlation Rule appropriate for these events fires in ArcSight, triggering message delivery to RSA Archer Security Incident Response for review and possible action.

Below are screenshots and narratives of this sample use case within the RSA Archer Security Operations Management Use Case.

1. User is logged into the Archer Interface and is examining the Security Alerts that have been delivered for review.

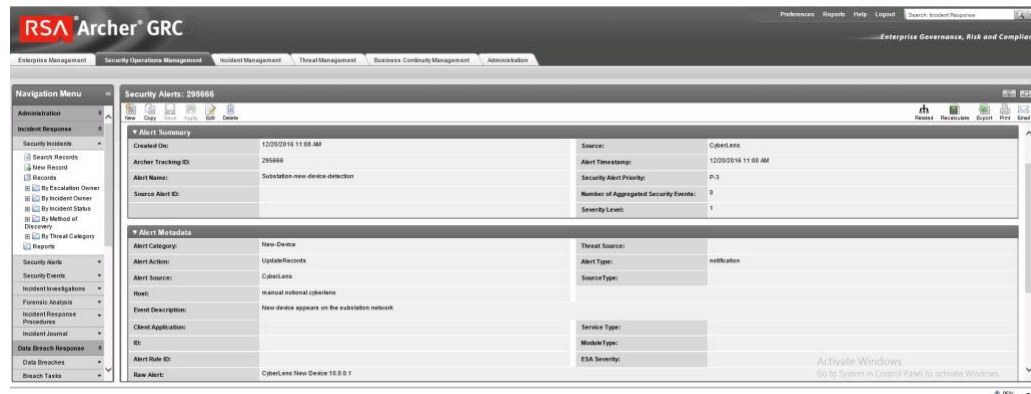
Figure 2-24 Multiple Security Alerts within the RSA Archer Console



**Figure 2-25 Sample Message from ArcSight, Showing Raw Log Message/Alert and Parsing with Normalization**



**Figure 2-26 Sample Message Showing Alert Indicating New Device Detected at Substation**



[Home](#)
[Help](#)
[Logout](#)
[Search Incident Response](#)

Enterprise Governance, Risk and Compliance

[Enterprise Management](#)
[Security Operations Management](#)
[Incident Management](#)
[Threat Management](#)
[Business Continuity Management](#)
[Administration](#)

Navigation Menu

Administration

Incident Response

Security Incidents

Security Alerts

Search Records

New Incident

Records

Destination

Device Categories

Alerts and Correlation

Security Alert Priority

My Source

Reports

Security Events

Incident Investigation

Process Analysis

Incident Response

Procedures

Incident Journal

Data Breach Response

Data Breaches

Breach Taxis

Security Alerts: 290565

New

Copy

Paste

Print

Export

Record 2 of 50,000

Printable

Export

Print

Send

Alert Summary

Alert Date

Attachments

About

Alert Summary

Created On:

12/20/2016 10:26 AM

Source:

ArtSight

Archer Tracking ID:

290565

Alert Timestamp:

12/20/2016 12:05 AM

Alert Name:

Subscription-entry-detection

Security Alert Priority:

P-3

Severity Level:

1

Alert Metadata

Alert Category:

BlueFire

Alert Action:

None

Alert Type:

notification

Host:

external.individual.artsight

Service Type:

Raw Alert:

CEP 1\src\Sight\srcSight8.0.1.1856.RD2015A-Service\srcSight\srcSight8.RS2Open-class-ws@2013042403-ws.xml

Session ID(s) (Optional)

Active Windows

Open Windows by process Name or window Name

- Figure 2-28 New Incident Response Workflow Record Started, Documented with Title, Summary, Details**

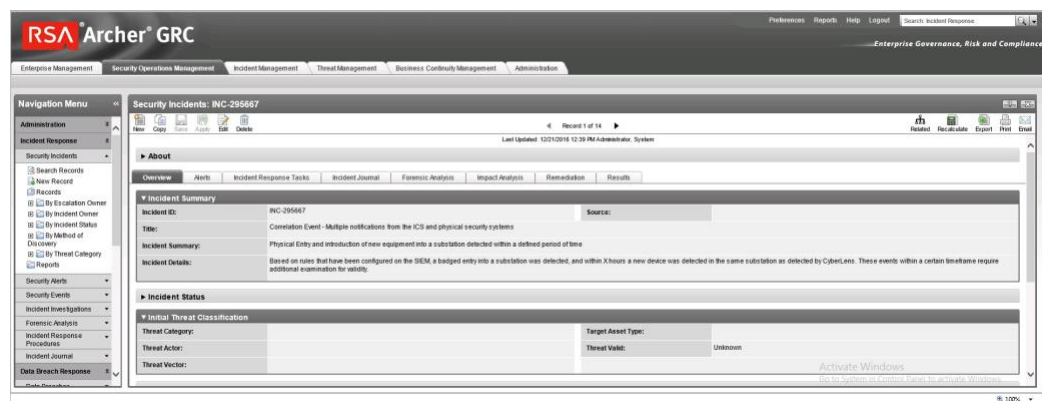
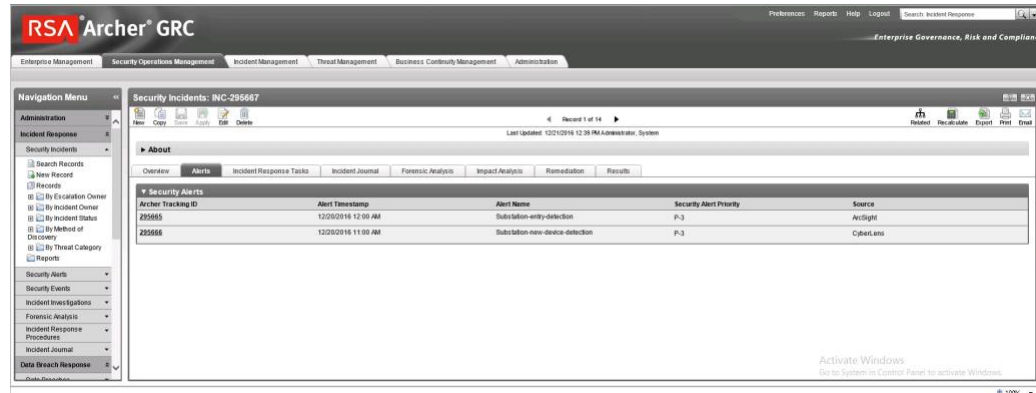


Figure 2-29 Incident Record Alerts Tab, Showing the Association of Two Events Attached to This Incident Response Investigation Record



- Based on Incident type, Appropriate Incident Response Procedure(s) and related tasks are assigned to the Record for completion. This directly represents the defined policy and procedure(s) outlines and maintained by an organization's security policy program and response.

Figure 2-30 Incident Response Procedure with Two Related Tasks Assigned to the Incident Response Record

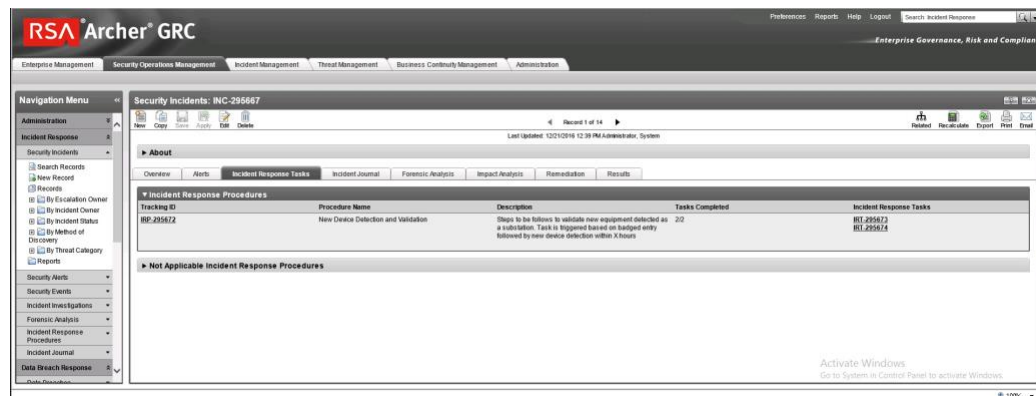
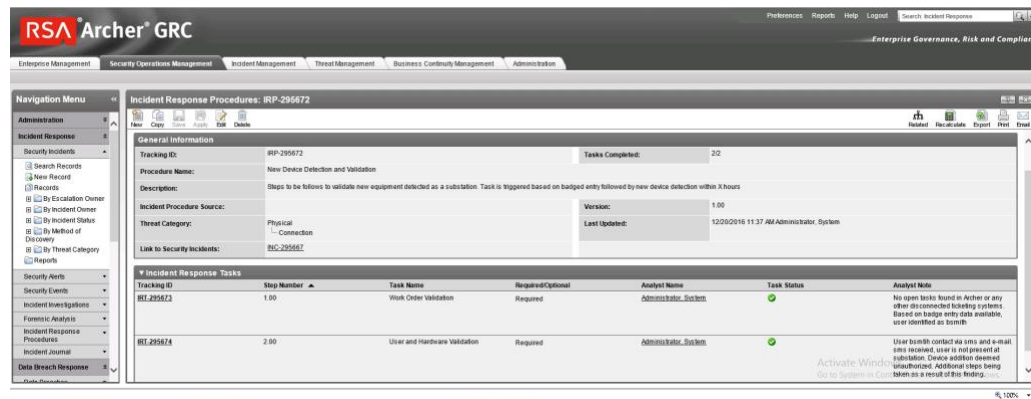


Figure 2-31 Incident Response Tasks with Status, Details, and Completion Status



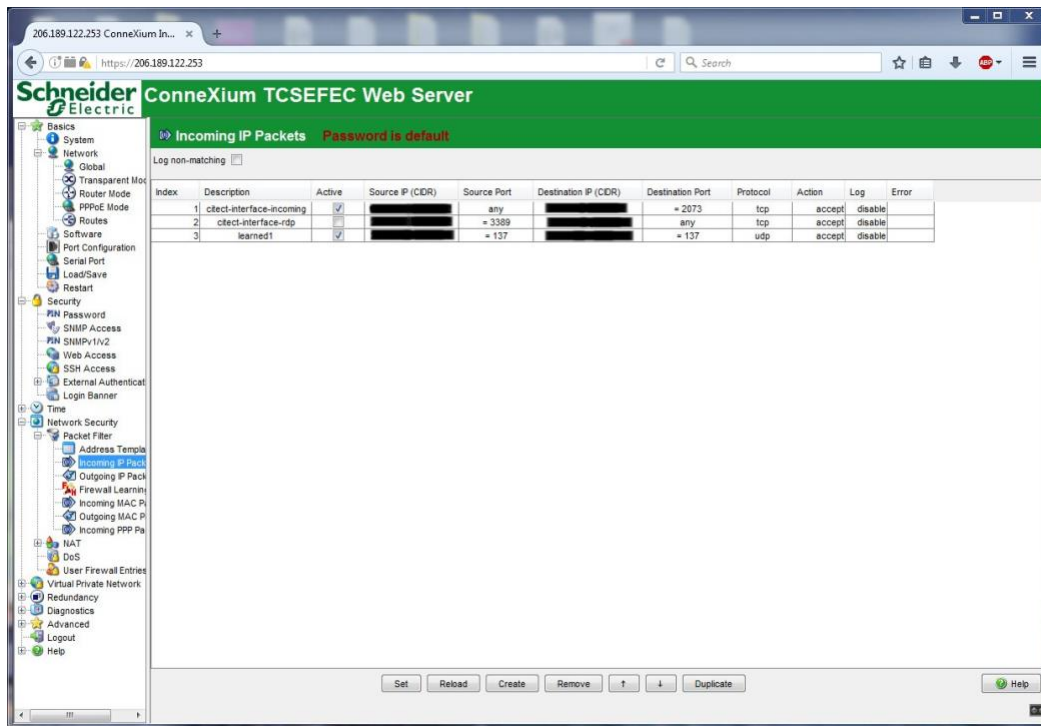
## 2.13 Schneider Electric Tofino Firewall (O3, O18, O20)

Schneider Electric Tofino Firewalls are used in multiple points throughout the build, supplying the necessary protection for network devices, including the door controller, the TDi ConsoleWorks operations management instance, and the connection between the OSIsoft Citect connector and the SCADA server.

### 2.13.1 Schneider Electric Tofino Firewall (O3) Installation Guide

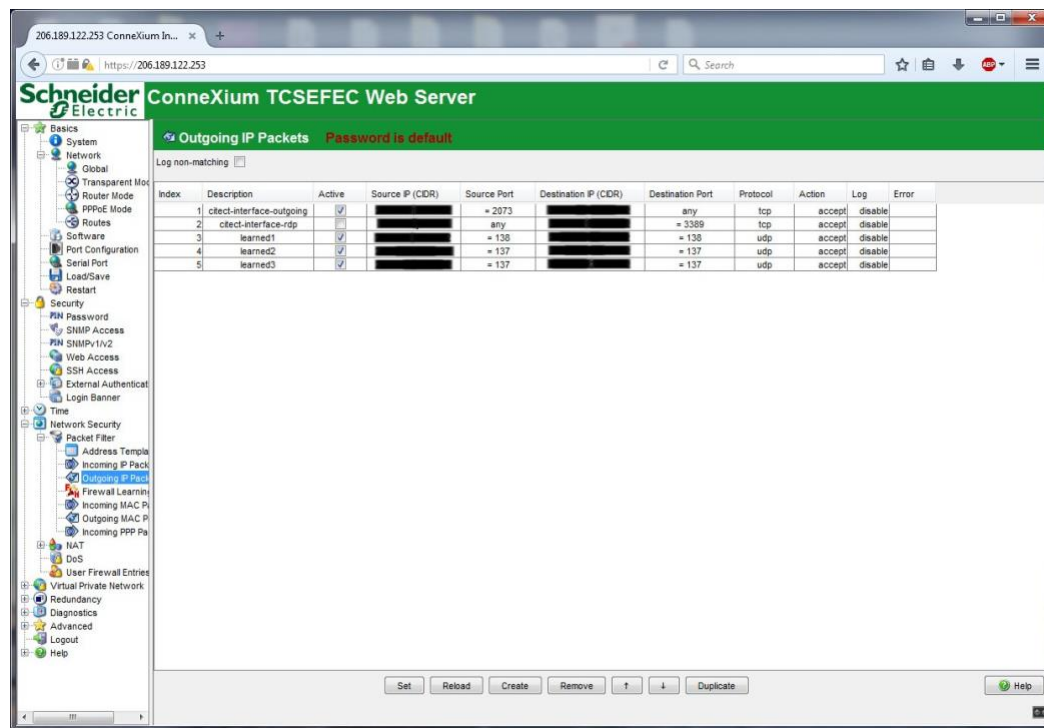
1. Log in to the web interface:
  - a. Open a browser and navigate to the IP address assigned to device.
  - b. Enter the username **admin** and password **private**.
2. For Login-Type, select **Administration**, then select **OK**.
3. From the menu on the left, select **Network Security** -> **Packet Filter** -> **Incoming IP Packets**. This is where the firewall rules will be created.
4. Click the **Create** button on the bottom of the main window.
5. Fill in the text fields for Description, Source IP (CIDR), Source Port, Destination IP (CIDR), Destination Port, Protocol, Action Log, and Error according to the rules needed for incoming packets.

Figure 2-32 Incoming Packet Configuration



6. From the menu on the left, select **Network Security -> Packet Filter -> Outgoing IP Packets**.
7. Follow the previous steps to create outgoing firewall rules.

Figure 2-33 Outgoing Packet Configuration



8. If necessary, configure the interface IP addresses from the menu on the left by selecting **Basics -> Network -> Transparent Mode**.

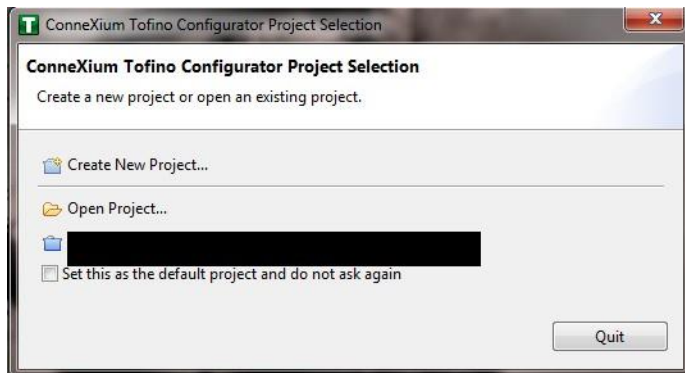
## 2.13.2 Schneider Electric Tofino Firewall (O18) Installation Guide

Install and Configure the Schneider Tofino Firewall:

1. Download the ConneXium software from the Schneider site as stated in the instructions accompanying the firewall, then start the ConneXium Tofino Configurator.
2. In the start-up screen, click **Create New Project...**

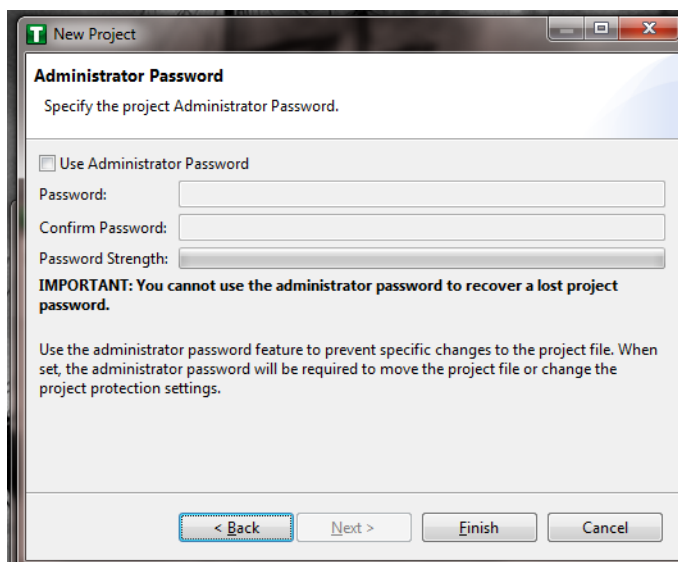


Figure 2-34 Create New Project



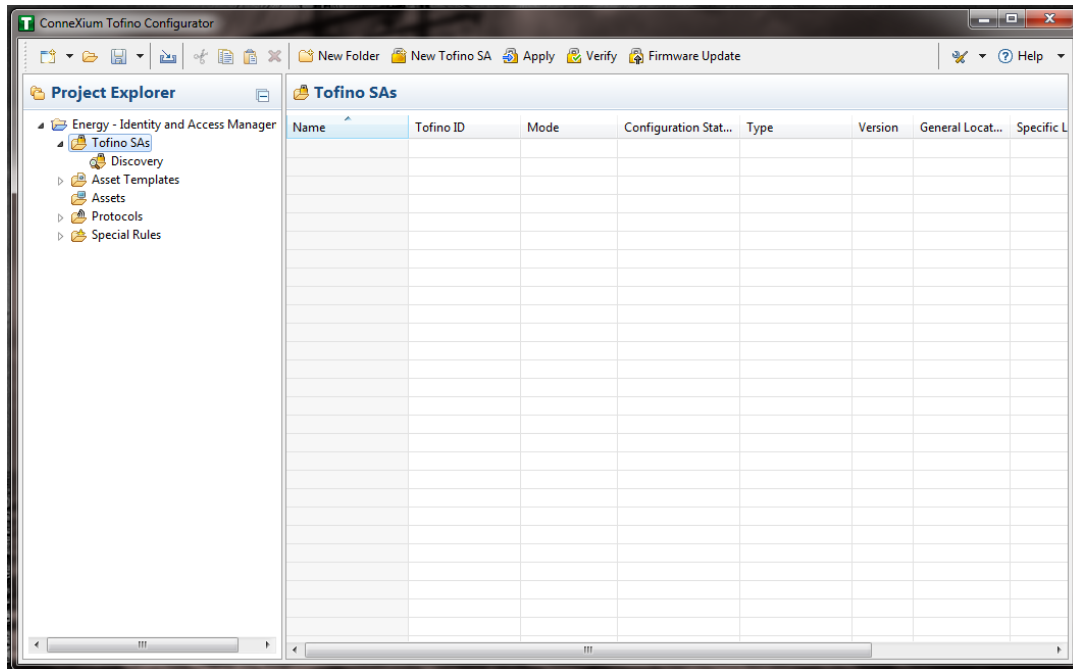
3. Enter the name for the project in the **Project name** field, the company name in the **Company** field, then click **Next**.
4. In the Project Protection screen, choose a password to protect the project, then click **Next**.

Figure 2-35 Administrator Password



5. In the Administrator Password screen, choose the administrator password, then click **Finish**.
6. In the Project Explorer window, right-click **Tofino SAs**, and select **New Tofino SA**. A folder can also be created for the SAs to help organize multiple areas.

Figure 2-36 Project Explorer Window



7. In the **Tofino ID** field, enter the MAC address listed on the firewall hardware sticker. Fill out the rest of the fields as necessary, then click **Finish**.

Figure 2-37 Tofino SA/MAC Address

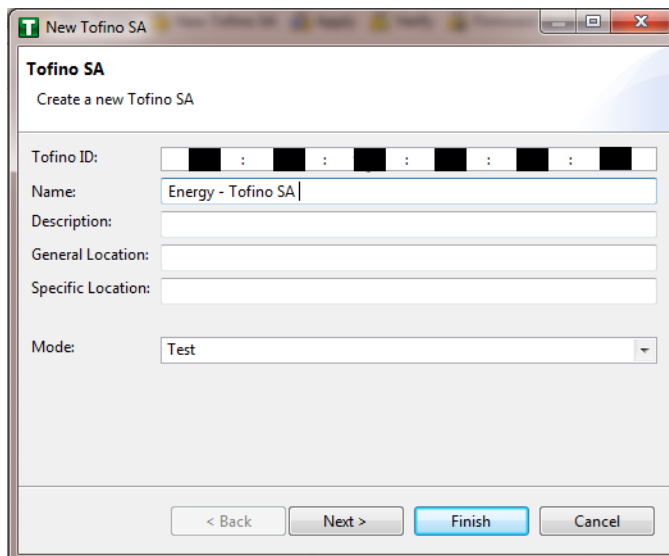
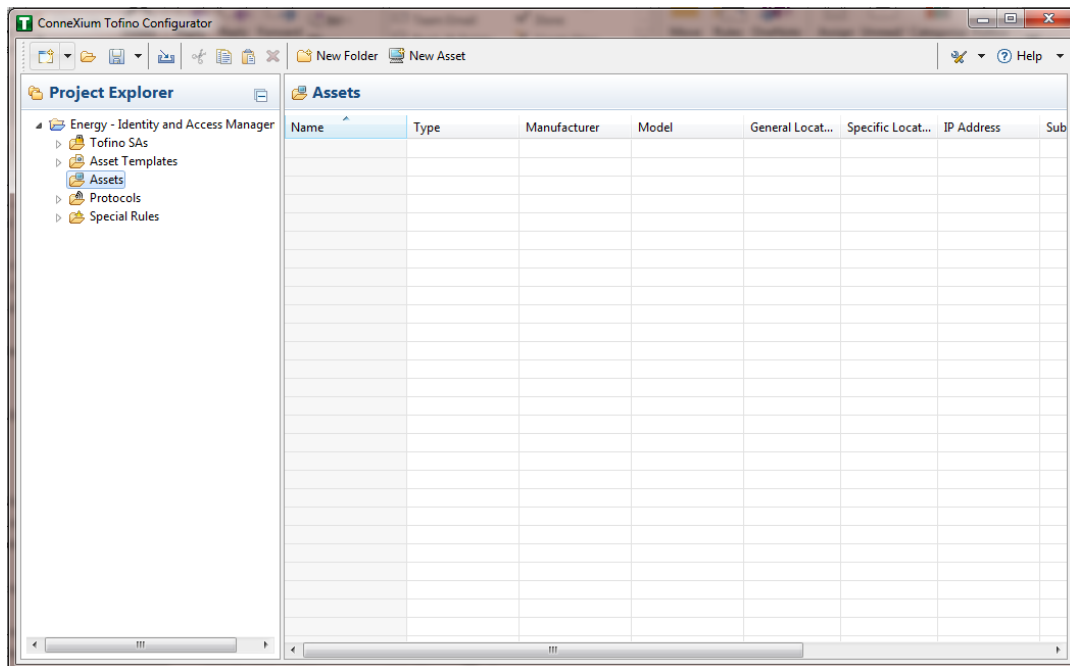
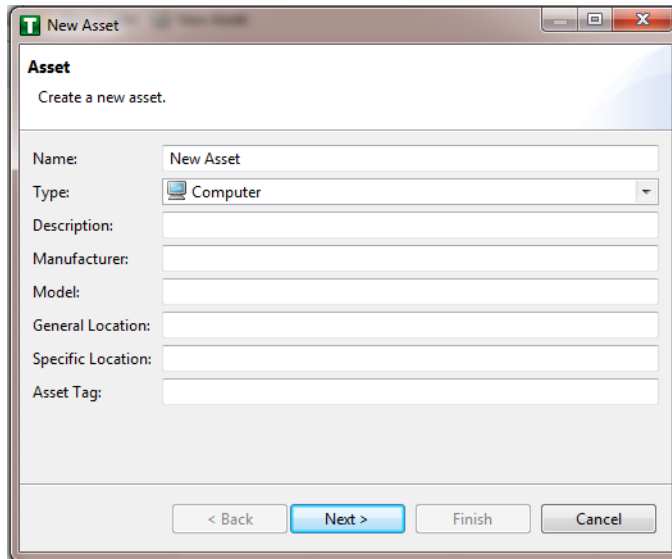


Figure 2-38 Project Explorer



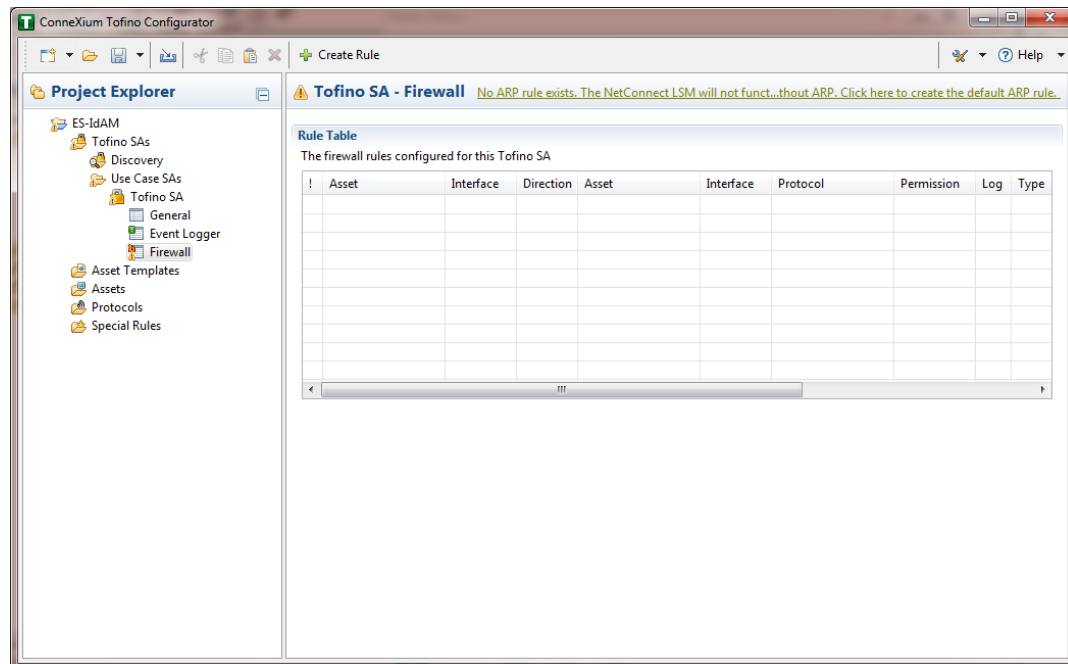
8. Right-click on the **Assets** icon in the Project Explorer frame, then click **New Asset**.
9. In the New Asset window, set the name and type of the device and all other fields as necessary, then click **Next**.

Figure 2-39 New Asset



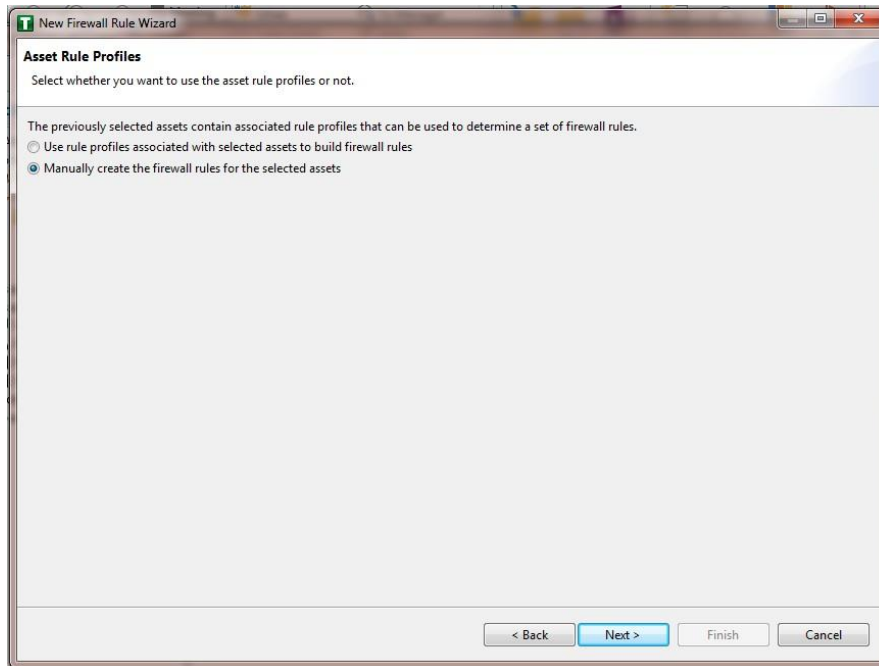
10. Fill in the **IP address** and/or the **MAC address** fields, then click **Finish**.
11. Repeat for all devices on the network. When they are configured, click on the **Assets** icon in the Project Explorer frame (if it is not already selected). There should be a list of all configured assets.
12. Under the Project Explorer frame, click the **drop-down arrow** next to Tofino SAs, then choose the SA created earlier. From there, click **Firewall** in the Project Explorer frame to display current firewall rules. This should currently be empty.

Figure 2-40 Project Explorer Tofino SA Icon



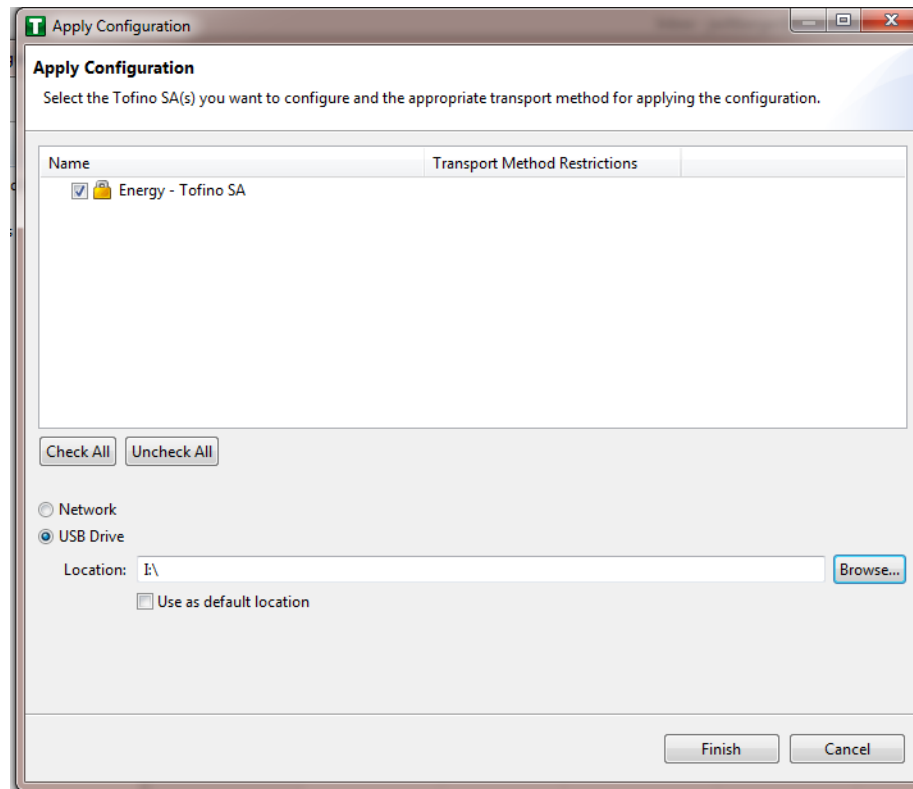
13. To create the first rule, click the **+ Create Rule** button above the Tofino SA-Firewall title. Then, ensure the **Standard rule** radio button is selected, and click **Next**.
14. On the next screen, choose the interface for **Asset 1**. This is where traffic originates before going into the device.  
  
Select a source asset and a destination asset from the radio buttons below. Set the direction of the traffic by using the arrow buttons in the middle. When finished, select **Next**.
15. In the Asset Rule Profiles window, select the **Manually create the firewall rules for the selected assets** radio button, then click **Next**.

Figure 2-41 Asset Rule Profiles



16. On the Protocol screen, choose the protocol to be checked against. Then choose the **Permission** on the right side of the screen, as well as whether to log, then click **Finish**.
17. After these steps are completed, the firewall rule should be listed in the **Rule Table**.
18. Repeat steps for the remainder of the rules needed.
19. Finally, click the **Save** button on the menu bar.
20. Place a FAT/FAT32 formatted Universal Serial Bus (USB) device into the computer running the ConneXium Tofino Configurator, then right-click **Tofino SAs** in the Project Explorer pane and select **Apply**. If the project asks that it be saved, click **OK**.

Figure 2-42 Apply Configuration Pane



21. In the Apply Configuration pane, ensure that the appropriate SA is selected in the table at the top and that the **USB Drive** radio button is selected. Browse to the top-level directory of the USB drive, then click **Finish**.
22. A pop-up will announce successful completion.
23. Ensure that the firewall has been powered on and has been running for at least one minute, then plug the USB device used to copy the Tofino configuration into the USB port on the back of the firewall.
24. Press the **Save/Load/Reset** button twice, setting it to the **Load** setting. (Pressing once should turn the indicator light to green pressing it again will change it from green to amber.) After a few seconds, the device will begin displaying lights that move from right to left across the LEDs on the back, indicating the configuration is being loaded.

25. Once the lights stop moving right to left, wait a few seconds to ensure that the **Fault** LED does not light up. Then remove the USB drive and place it back into the computer running the ConneXium Tofino Configurator software.
26. Right-click **Tofino SAs** in the Project Explorer pane and select **Verify**.
27. At the Verify Loaded Configuration window, select the **Tofino SA** in the table, and select the **USB Drive** radio button. Then select the USB drive by using the **Browse** button. Finally, click **Finish**.
28. A pop-up will announce successful verification, and configuration is complete.

### 2.13.3 Schneider Electric Tofino Firewall (O20) Installation Guide

Refer to the guide in [Section 2.13.2](#) on installing the Schneider Electric Tofino Firewall (O18).

## 2.14 Siemens RUGGEDCOM CROSSBOW (E9)

Siemens RUGGEDCOM CROSSBOW is a platform that allows remote connections and controls from the enterprise side of the lab to the control systems network lab. The product does require the Waterfall Secure Bypass to be in the closed position, however CROSSBOW also monitors the IXIA Network TAP aggregator Cisco switch for any configuration changes, which then prompts an alert to the centralized SIEM.

### 2.14.1 Environment Setup

- Microsoft Windows Server 2012 (64-bit)
- 4 GB RAM
- 4 cores
- 200 GB HDD
- Software:
  - Microsoft SQL Server 2012 (version 11.0.2100.60)

### 2.14.2 Installation Procedure

The following sections detail the installation procedure for the Siemens RUGGEDCOM CROSSBOW used in the build.

#### 2.14.2.1 Installing CROSSBOW Database

1. On the RUGGEDCOM CROSSBOW Server, extract the contents of **SQLScripts.zip** to RUGGEDCOMCROSSBOW install directory (e.g. **C:\ProgramFiles\RuggedCom\CrossBow**).
2. On a Microsoft SQL Server, launch **SQL Server Management Studio**, and connect to the SQL Server as a System Administrator (SA) or administrator.



3. In **Object Explorer**, expand the SQL Server.
4. Right-click **Databases**, and then click **New Database**. The New Database screen will appear.
5. In the **Database name** field, type the name of the new database (e.g. **CROSSBOW**).
6. Click .... and the **Select Database Owner** dialogue box will appear.
7. Select a user to be the RUGGEDCOM CROSSBOW database owner in the SQL Server. This grants the RUGGEDCOM CROSSBOW Server full access to the RUGGEDCOM CROSSBOW database.
8. If the desired account is unavailable, add a Windows domain user account for authenticating against the database. This account must be added to the database as an authorized user.
9. Click **OK**.
10. Optional: Further configure the database (such as the recovery model) as required based on the chosen database backup strategy. For more information, contact the local Database Administrator (if available) or visit the Microsoft Developer Network website (<https://msdn.microsoft.com/en-us/library/bb545450>).
11. Click **OK**.
12. In Object Explorer, expand the **Security** folder, followed by **Logins**.
13. Right-click the desired Windows domain account, and then click **Properties**. The **Login Properties** dialogue box will appear.
14. Under **Default database**, select the **CROSSBOW** database, then click **OK**.
15. Execute the following scripts in order:
  - a. Crossbow\_db\_create.sql
  - b. Crossbow\_db\_functions.sql
  - c. Crossbow\_db\_initial\_data.sql
  - d. Crossbow\_db\_scripts.sql
  - e. Crossbow\_db\_client\_queries.sql

#### **2.14.2.2**    *Installing CROSSBOW Server and Services*

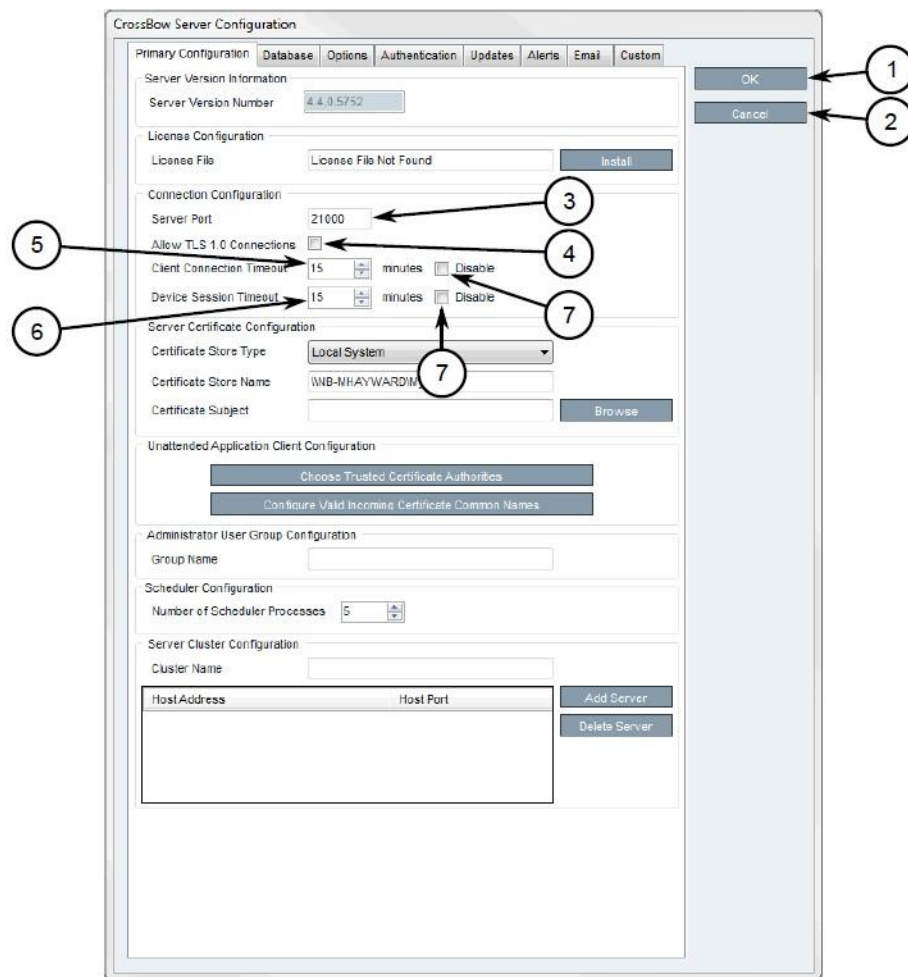
1. Contact Siemens Customer Support, and obtain a compressed zip file containing the latest CROSSBOW Server installer for RUGGEDCOM CROSSBOW v4.4.

2. Open the compressed zip file, and double-click **Server Strong Setup.msi**. The CROSSBOW Server with Strong Authentication Setup installation wizard will appear.
3. Follow the onscreen instructions to install CROSSBOW Server.

### 2.14.2.3 Configuring Server Host Connection

1. Access the RUGGEDCOM CROSSBOW Server, and launch CROSSBOW Server.
2. Make sure the **CROSSBOW Main Server** service is **stopped**.
3. Under **CrossBow Main Server**, click **Configure**. The CrossBow Server Configuration dialogue box will appear.

Figure 2-43 CrossBow Server Configuration



1. *OK Button*
  2. *Cancel Button*
  3. *Server Port Box*
  4. *Allow Transport Layer Security 1.0 Connections Check Box*
  5. *Client Connection Timeout Box*
  6. *Device Session Timeout Box*
  7. *Disable Check Box*
4. On the Primary Configuration tab, under **Connection Configuration**, type the TCP port number that the CROSSBOW Client application will use to connect to the CROSSBOW Server in the **Server Port** field. The default port number is 21000 but can be changed as needed.
  5. In the **Client Connection Timeout** field, type or select the maximum amount of time (in minutes) for the server to wait before disconnecting an inactive client. To disable this feature, select **Disable**.
  6. In the **Device Session Timeout** field, type or select the maximum amount of time (in minutes) for the server to wait before disconnecting an inactive remote device. To disable this feature, select **Disable**.
  7. Click **OK** to save changes.
  8. Start the CROSSBOW Main Server service.

#### 2.14.2.4 *Installing a License File*

1. Access the RUGGEDCOM CROSSBOW Server, and launch CROSSBOW Server.
2. Make sure the **CROSSBOW Main Server** service is **stopped**.
3. Under **CrossBow Main Server**, click **Configure**. The CrossBow Server Configuration dialogue box will appear.

**Figure 2-44 CrossBow Server Configuration**

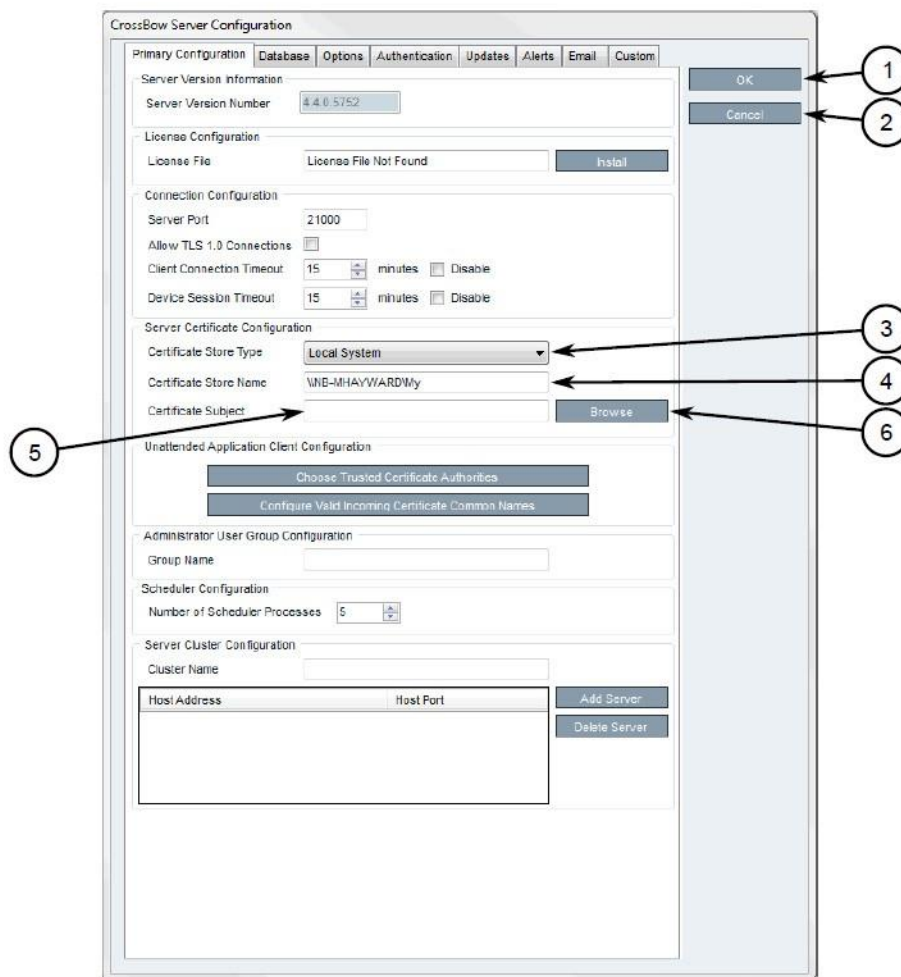
1. *License File Box*
2. *OK Button*
3. *Cancel Button*
4. *Install Button*

4. On the **Primary Configuration** tab, under **License Configuration**, either type the name of the license file (including the system path) or click **Install** and select the desired file.
5. Click **OK** to save changes.
6. Start the CROSSBOW Main Server service.

### 2.14.2.5 Selecting/Installing the CROSSBOW Server Certificate

1. Access the RUGGEDCOM CROSSBOW Server, and launch CROSSBOW Server.
2. Make sure the **CROSSBOW Main Server** service is **stopped**.
3. Under **CrossBow Main Server**, click **Configure**. The CrossBow Server Configuration dialogue box will appear.

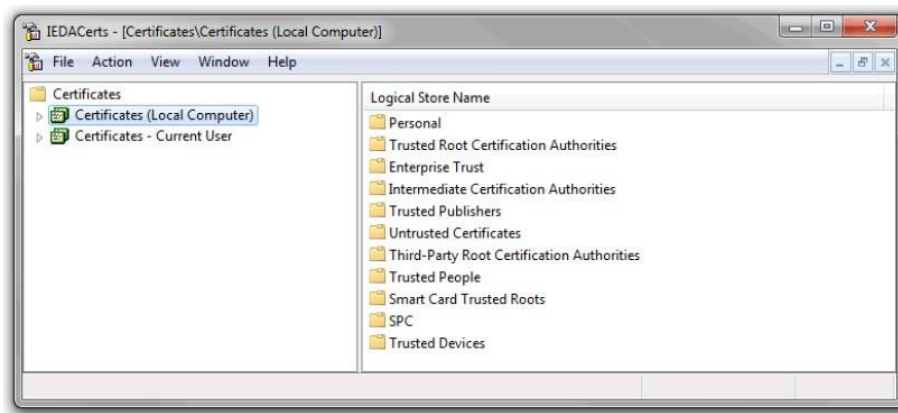
Figure 2-45 CrossBow Server Configuration



1. *OK Button*
2. *Cancel Button*
3. *Certificate Store Type List*

4. *Certificate Store Name Box*
  5. *Certificate Subject Box*
  6. *Browse Button*
4. On the Primary Configuration tab, under **Server Certificate Configuration**, click **Browse**. The Select Server Certificate dialogue box will appear.
  5. Click **Import**. A confirmation dialogue box will appear.
  6. Click **Yes**. A confirmation dialogue box will appear, as well as the Microsoft Management Console (MMC) snap-in.

Figure 2-46 MMC Snap-In

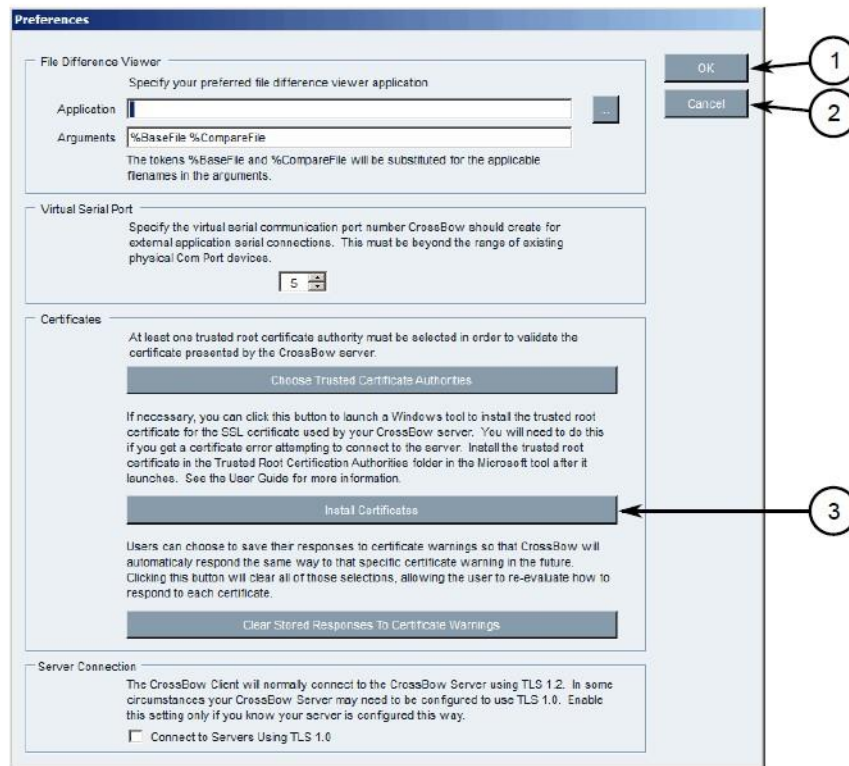


7. Expand **Certificates (Local Computer)**.
8. Right-click either **Personal** or **Trusted Root Certification Authorities**, point to **All Tasks**, then click **Import**. The Certificate Import Wizard will appear.
9. Follow the onscreen instructions to import the certificate.
10. Close the Microsoft Management Console snap-in.
11. Once the certificate is imported, click **OK** to close the dialogue box.
12. On the Select Server Certificate dialogue box, select the certificate from the list, and click **OK**. The certificate name appears in the **Certificate Subject** field.
13. Click **OK** to save changes.
14. Start the CROSSBOW Main Server service.

### 2.14.2.6 Verifying/Installing the CROSSBOW Client Certification Authority (CA) Certificate

1. Launch CROSSBOW Client, but do not connect to the RUGGEDCOM CROSSBOW Server.
2. On the toolbar, click **File**, then click **Preferences**. The Preferences dialogue box will appear.

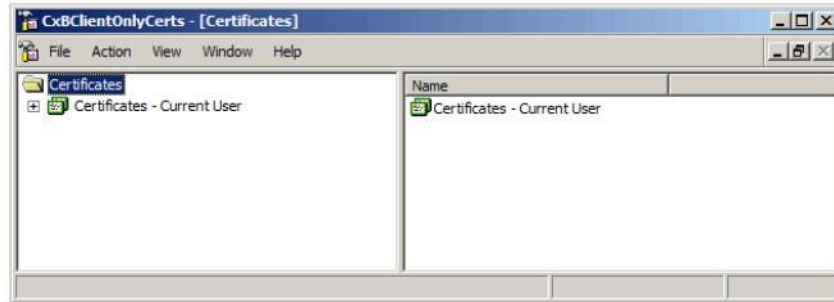
Figure 2-47 Preferences Dialogue Box



1. **OK Button**
2. **Cancel Button**
3. **Install Certificates Button**

3. Click **Install Certificates**. The CxBClientOnlyCerts snap-in will appear.

Figure 2-48 CxBClientOnlyCerts Snap-In



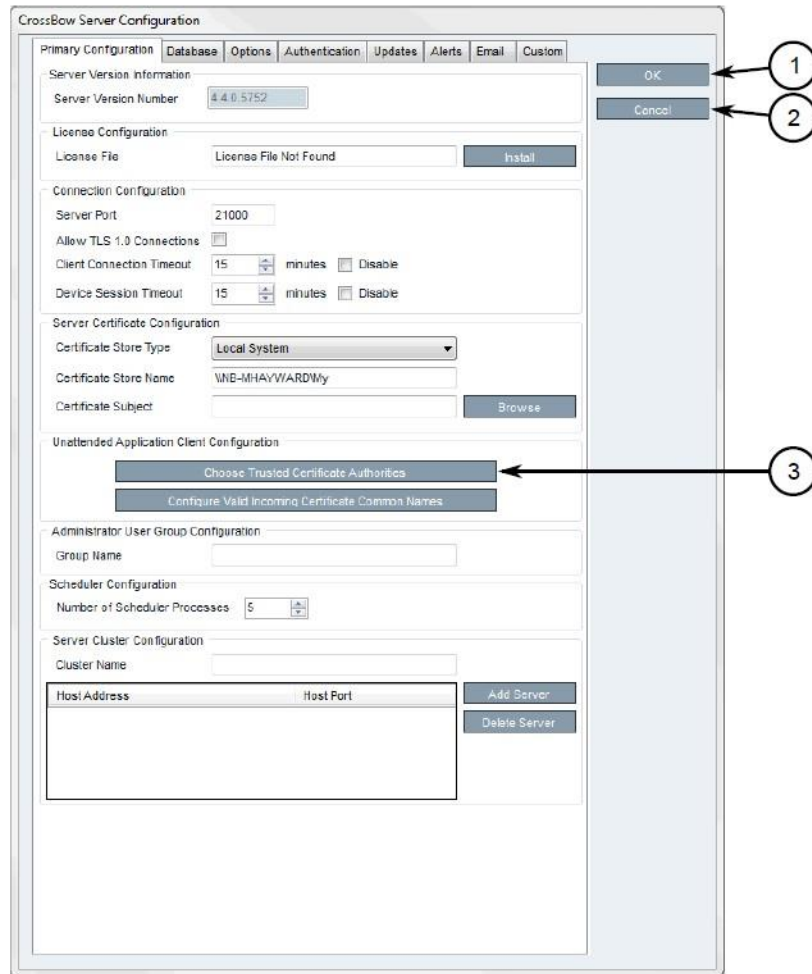
4. In the left pane, navigate to **Certificates — Current User ->Trusted Root Certification Authorities -> Certificates**.
5. Verify the appropriate CA certificate is listed in the right pane.
6. If the certificate is not listed, proceed to the next step.
7. Right-click **Trusted Root Certification Authorities**, point to **All Tasks**, then click **Import**. The Certificate Import Wizard will appear.
8. Follow the onscreen instructions to import a new CA certificate.
9. Close the snap-in.

#### *2.14.2.7 Select a Trusted CA for the CROSSBOW Server*

1. Access the RUGGEDCOM CROSSBOW Server, and launch CROSSBOW Server.
2. Make sure the **CROSSBOW Main Server** service is **stopped**.
3. Under **CrossBow Main Server**, click **Configure**. The CrossBow Server Configuration dialogue box will appear.



Figure 2-49 CrossBow Server Configuration



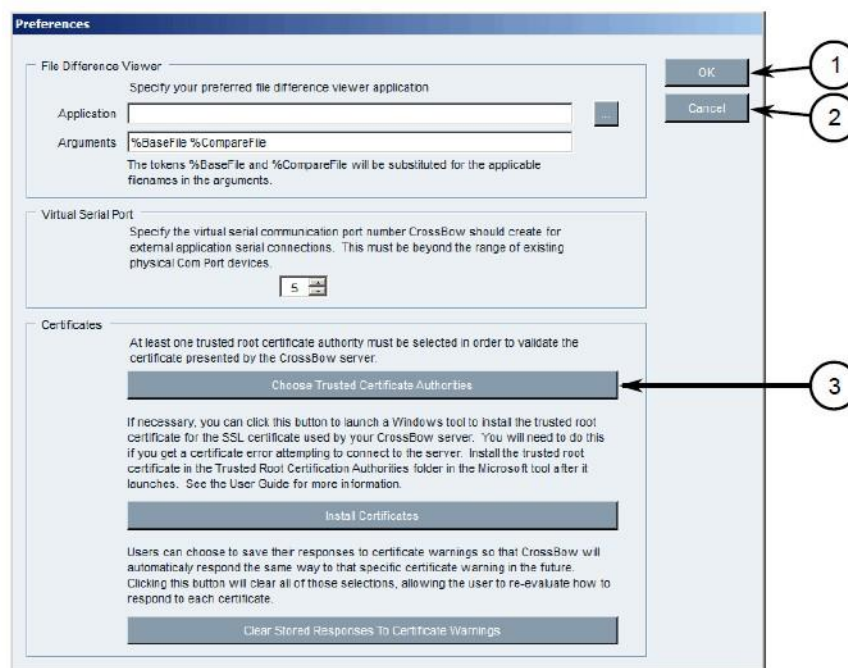
1. *OK Button*
2. *Cancel Button*
3. *Choose Trusted Certificate Authorities Button*
4. Click **Choose Trusted Certificate Authorities**. A dialogue box will appear.
5. Optional: Filter the list of CAs by selecting **Show Root Certificate Authorities**, **Show Intermediate Certificate Authorities**, and/or **Show Third Party Certificate Authorities**.
6. Select one or more CAs from the list, or select **Specify a certificate authority** and define the CA in the box below.

7. Click **OK** to save changes.
8. Start the CROSSBOW Main Server service.

#### 2.14.2.8 *Selecting a Trusted CA for a CROSSBOW Client*

1. Launch CROSSBOW Client, but do not connect to the RUGGEDCOM CROSSBOW Server.
2. On the toolbar, select **File**, then click **Preferences**. The Preferences dialogue box will appear.

**Figure 2-50 Preference Dialogue Box**



1. *OK Button*
2. *Cancel Button*
3. *Choose Trusted Certificate Authorities Button*

3. Click **Choose Trusted Certificate Authorities**. A dialogue box will appear.
4. Optional: Filter the list of CAs by selecting **Show Root Certificate Authorities**, **Show Intermediate Certificate Authorities**, and/or **Show Third Party Certificate Authorities**.
5. Select one or more CAs from the list, or select **Specify a certificate authority** and define the CA in the box below.
6. Click **OK** to save changes.

### 2.14.2.9 Adding a Common Name

1. Access the RUGGEDCOM CROSSBOW Server, and launch CROSSBOW Server.
2. Make sure the **CROSSBOW Main Server** service is **stopped**.
3. Under **CrossBow Main Server**, click **Configure**. The CrossBow Server Configuration dialogue box will appear.

Figure 2-51 CrossBow Server Configuration

The image shows the 'CrossBow Server Configuration' dialog box with the 'Primary Configuration' tab selected. The dialog box contains several sections: 'Server Version Information' (Server Version Number: 4.4.0.5695), 'License Configuration' (License File: License File Not Found, Install button), 'Connection Configuration' (Server Port: 21000, Client Connection Timeout: 15 minutes, Device Session Timeout: 15 minutes), 'Server Certificate Configuration' (Certificate Store Type: Local System, Certificate Store Name: VNB-MHAYWARDMy, Certificate Subject: [empty], Browse button), 'Unattended Application Client Configuration' (Choose Trusted Certificate Authorities, Configure Valid Incoming Certificate Common Names), 'Administrator User Group Configuration' (Group Name: [empty]), 'Scheduler Configuration' (Number of Scheduler Processes: 5), and 'Server Cluster Configuration' (Cluster Name: [empty], Host Address/Host Port table, Add Server/Delete Server buttons). On the right side, there are 'OK' and 'Cancel' buttons. Numbered callouts point to these buttons and the 'Choose Trusted Certificate Authorities' and 'Configure Valid Incoming Certificate Common Names' buttons.

1. OK Button

2. Cancel Button

3. Choose Trusted Certificate Authorities

4. Configure Valid Incoming Certificate Common Names

1. OK Button
2. Cancel Button

3. *Choose Trusted Certificate Authorities Button*
4. *Configure Valid Incoming Certificate Common Names Button*
4. On the **Primary Configuration** tab, under **Unattended Application Client Configuration**, click **Configure Valid Incoming Certificate Common Names**. The Incoming Certificate Common Name dialogue box will appear.
5. Click **Add Name**. The Common Name dialogue box will appear.
6. In the **Common Name** box, type the common name, then click **OK** to close the dialogue box.
7. Click **OK**.
8. Start the CROSSBOW Main Server service.

#### *2.14.2.10 Managing the RUGGEDCOM CROSSBOW Certificates and Keys*

The following references the RUGGEDCOM RX1400 and RX1511 web interface:

1. Navigate to **security -> crypto -> ca** and click **<Add ca>**. The Key Settings form will appear.
2. Configure the following parameter as required:
  - a. name
3. Click **Add**. The CA form will appear.

Figure 2-52 Virtual Private Network (VPN) Certificate Form

The image shows a web form titled "Certificate" with a blue header bar. Below the header, there is a section labeled "Contents \*" with a large, empty text area. To the left of this area, a circled number "1" has an arrow pointing to it. Below the "Contents" section, there are two dropdown menus. The first is labeled "Private Key Name" and has a circled number "2" with an arrow pointing to it. The second is labeled "CA Name" and has a circled number "3" with an arrow pointing to it. Each dropdown menu has a small blue question mark icon to its right.

1. *Contents Box*
2. *Private Key Name List*
3. *CA Certificate Name List*

4. Copy the contents of the CA certificate into the **Key Cert Sign Certificate** field.
5. Add the associated Certificate Revocation List.
6. Navigate to **security -> crypto -> private-key** and click **<Add private-key>**. The Key Settings form will appear.
7. In the Key Settings form, configure the following parameter as required:
  - a. name
8. Click **Add** to create the new private key. The Private Key form will appear.

Figure 2-53 VPN Private Key Form

1. *Algorithm List*
2. *Contents Box*

9. In the Private Key form, configure the following parameters as required:

- a. Algorithm
- b. Contents

#### 2.14.2.11 Managing the RUGGEDCOM CROSSBOW Application on RX1501

To enable or disable communication with a RUGGEDCOM CROSSBOW system, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **apps -> crossbow**. The CROSSBOW form will appear.
3. Ensure that the **Enabled** check box is selected.
4. Navigate to **apps -> crossbow -> client-connection**. The Client Connection Info form will appear.

Figure 2-54 Client Connection Info

Client Connection Info

1 IP Address 172.30.151.151

2 Port \* 21000  
(21000)

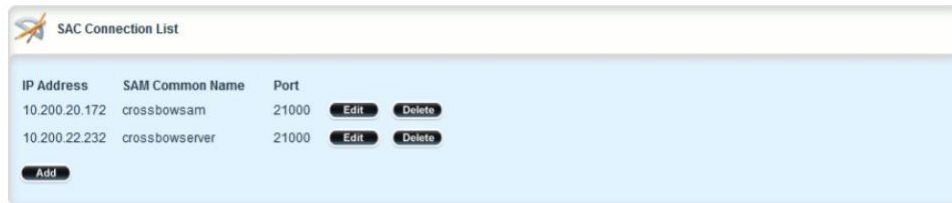
3 Client Connection Timeout \* 15  
(15)

4 Device Session Timeout \* 15  
(15)

1. IP Address Box
2. Port Box
3. (Keep default)
4. (Keep default)

5. Configure the following parameters as required:
  - a. ipaddr
  - b. port
6. Navigate to **apps -> crossbow -> sac-connection**. The station access controller (SAC) Connection List will appear.

Figure 2-55 SAC Connection List

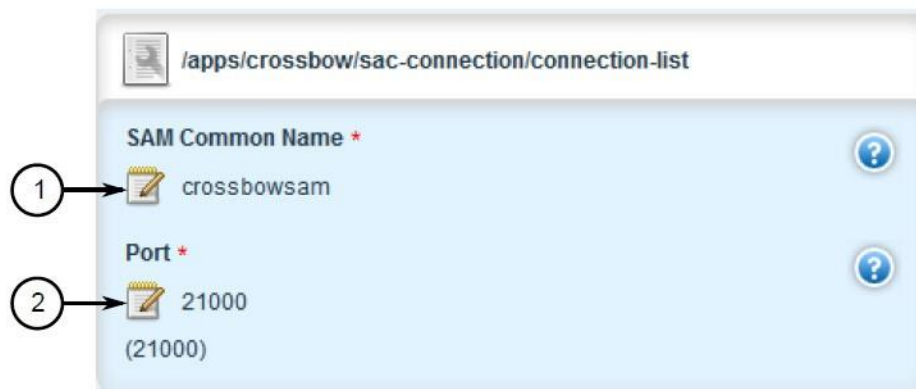


| IP Address    | SAM Common Name | Port  |      |        |
|---------------|-----------------|-------|------|--------|
| 10.200.20.172 | crossbowsam     | 21000 | Edit | Delete |
| 10.200.22.232 | crossbowserver  | 21000 | Edit | Delete |

Add

7. Navigate to **apps -> crossbow -> sac-connection -> Add connection-list**. The Key Settings form will appear.
8. Configure the following parameter(s) as required:
  - a. sam-ipaddr
9. Click **Add**. The Connection List form will appear.

Figure 2-56 Connection List



/apps/crossbow/sac-connection/connection-list

1 → SAM Common Name \* crossbowsam

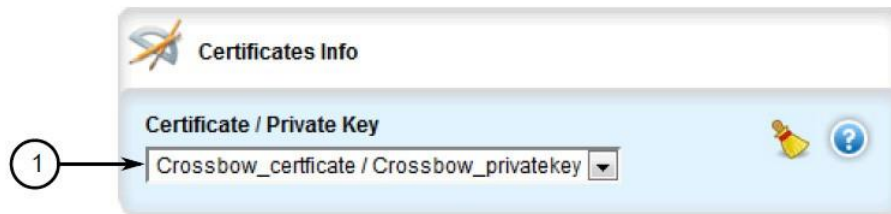
2 → Port \* 21000 (21000)

1. SAM Common Name Box
2. Port Box

10. Configure the following parameters as required:
  - a. sam-name
  - b. sam-port
11. Navigate to **apps -> crossbow -> certificate**. The Certificates Info forms will appear.



Figure 2-57 Certificates Info



1. *Certificate/Private Key List*

12. Configure the following parameters as required:

- a. cert
- b. cert-private-key

13. Navigate to **apps -> crossbow -> certificate -> ca-cert-list** and click **<Add ca-cert-list>**. The Key Settings form will appear.

14. Configure the following parameter as required:

- a. name

15. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialogue box will appear. Click **OK** to proceed.

16. Click **Exit Transaction**, or continue making changes.

#### 2.14.2.12 Viewing the RUGGEDCOM CROSSBOW Log

1. Navigate to **apps -> crossbow -> status** and click **log** in the menu. The Trigger Action form will appear.

Figure 2-58 Trigger Action



1. *Perform Button*
2. Click **Perform**. The Log form will appear.

Figure 2-59 Status Log



### 2.14.2.13 Managing SACs

1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and log in as a user with the necessary administrative privileges. The Field Layout tab appears by default.
2. In the right pane, right-click the associated facility or gateway, and click **Add Station Access Controller**. The Station Access Controller Properties dialogue box will appear.

Figure 2-60 Station Access Controller Properties

The screenshot shows the 'Station Access Controller Properties' dialog box with the 'Identification' tab selected. The dialog has four tabs: 'Identification', 'Connection', 'Login', and 'NERC CIP'. The 'Identification' tab contains a text box for 'Name' with the value 'New Station Access Controller 1', an empty text box for 'Description', a dropdown menu for 'Status' set to 'In Service', and a table for 'Custom Fields' with columns 'Line #', 'Test', and 'Voltage'. The 'Line #' column is highlighted. On the right side of the dialog are 'OK' and 'Cancel' buttons.

1. Name Box
2. Description Box
3. Status List
4. Custom Fields
5. OK Button
6. Cancel Button

3. Configure the identification properties (e.g., name, description) for the SAC.

Figure 2-61 SAC Property Configuration — Identification

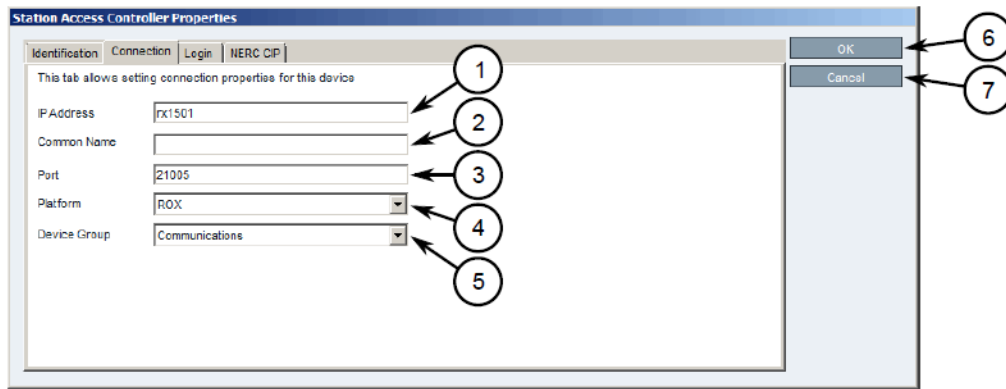
This screenshot is similar to Figure 2-60 but with specific data and numbered callouts. The 'Name' field contains 'Barker RX1501 SAC', the 'Status' dropdown is set to 'Out Of Service', and the 'Line #' column in the 'Custom Fields' table is highlighted. Numbered callouts (1-6) point to the following elements: 1. Name Box, 2. Description Box, 3. Status List, 4. Custom Fields, 5. OK Button, and 6. Cancel Button.

1. Name Box
2. Description Box
3. Status List
4. Custom Fields

5. *OK Button*
6. *Cancel Button*

4. Configure the connection properties (e.g., IP address, port, platform) for the SAC.

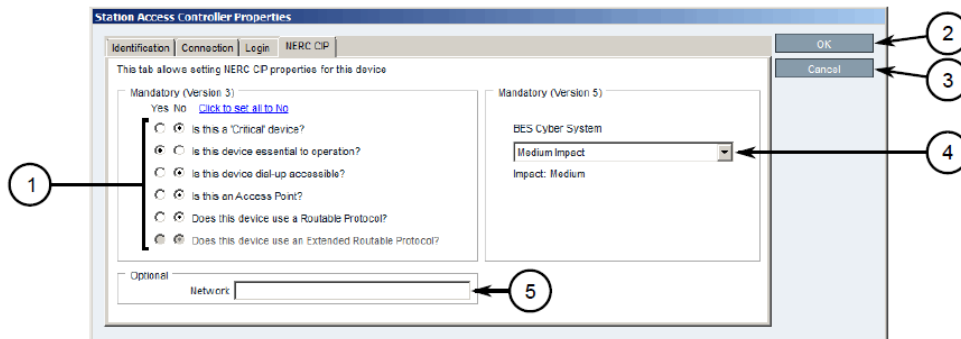
**Figure 2-62 SAC Property Configuration — Connection**



1. *IP Address Box*
2. *Common Name Box*
3. *Port Box*
4. *Platform List*
5. *Device Group*
6. *OK Button*
7. *Cancel Button*

5. Configure the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) properties for the SAC.

**Figure 2-63 SAC Property Configuration — NERC CIP**

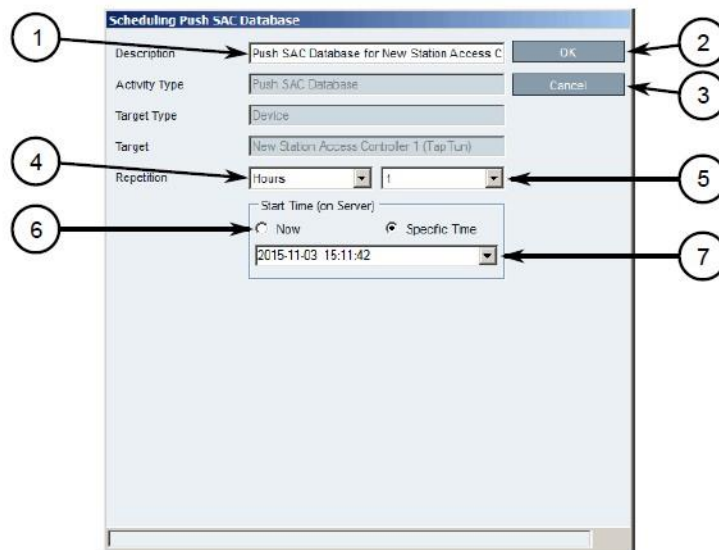


1. Questions
2. Network Box
3. OK Button
4. Cancel Button
5. BES Cyber System List

#### 2.14.2.14 Updating the SAC Database

1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and log in as a user with the necessary administrative privileges. Make sure to enter the host name and port number for the SAC during the login process.
2. Search for the SAC's device family on the **Devices** tab.
3. Right-click the **Station Access Controller** device family, point to **Special Operations**, then click **Push SAC Database**. The Scheduling Push SAC Database dialogue box will appear.

Figure 2-64 Scheduling Push SAC Database



1. Description Box
2. OK Button
3. Cancel Button
4. Repetition Lists
5. Start Time Options
6. Start Time Box

4. Optional: Under **Description**, type a description for the operation. Include details such as the affected target, the purpose of the operation, etc. This description will appear in the list of scheduled operations.
5. Under **Repetition**, select the interval and value (if applicable).
6. Under **Start Time (On Server)**, select **Now** or **Specific Time**.
7. Click **OK** to save changes. The operation will commence at the selected time.

#### *2.14.2.15 Managing Devices and Gateways*

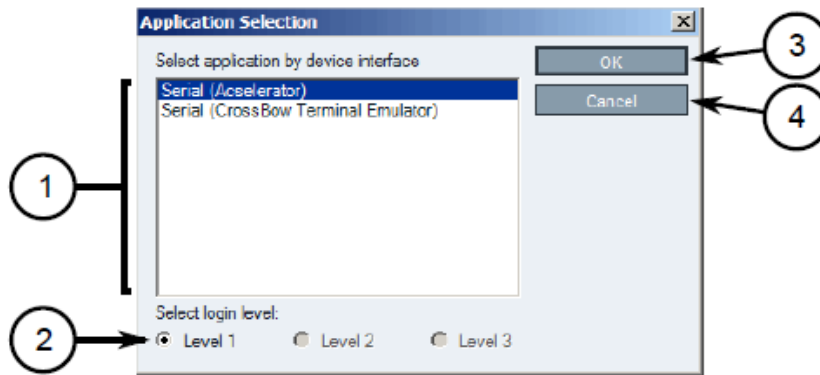
1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and log in as a user with the necessary administrative privileges.
2. On the **Field Layout** tab, right-click the desired facility or gateway, and click **Add Device**, **Add Gateway**, or **Add Subordinate Gateway (gateways only)**. The Device Properties or Gateway Properties dialogue box will appear.
3. Configure the identification properties (e.g., name, description) for the device/gateway.
4. Configure the connection properties (e.g., host name, user names, passwords) for the device/gateway.
5. Configure the interfaces available for the device/gateway.
6. Enable or disable the applications available for the device/gateway.
7. Configure the NERC CIP properties for the device/gateway.
8. Configure any advanced parameters associated with the device/gateway.
9. Click **OK** to save changes.

#### *2.14.2.16 Connecting to a Device/Gateway*

1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and log in as a user with the necessary administrative privileges.
2. If connecting to the device/gateway via a Station Access Controller, make sure to enter the host name and port number for the SAC during the login process. Otherwise, provide the host name and port number for the RUGGEDCOM CROSSBOW Server.
3. Search for the desired device/gateway on the **Field Layout** or **Devices** tab by either facility or device type.

4. Right-click the device/gateway, and then click either **Connect (devices)** or **Connect to Gateway (gateways)**. The Application Selection dialogue box will appear.

Figure 2-65 Application Selection Dialogue



1. Available Applications
2. Select Login Level Options
3. OK Button
4. Cancel Button

5. Select an application to connect to the device's interface.
6. Under **Select login level**, select the login level to use when connecting to the device.
7. Click **OK**. RUGGEDCOM CROSSBOW will attempt to connect to the device. Review the Messages pane for details.
8. Once connected, the device/gateway and the connection status are displayed in the **Device Connection History** pane.
9. When the application launches, if required, enter the local host IP address or the real IP address of the end-device or gateway, followed by the port number.

## 2.15 Siemens RUGGEDCOM RX1400 (E1)

The Siemens RUGGEDCOM RX1400 device is used on the enterprise side of the lab and creates an always-on VPN connection to the Siemens RUGGEDCOM RX1501, located on the boundary of the control network lab.

### 2.15.1 Environment Setup

Requirements for installation:

- personal computer/laptop with Ethernet port
- CAT5 or higher Ethernet cables
- RUGGEDCOM VPN device
- any type of terminal emulator
- web browser
- When connecting the device to the network, the NCCoE used switch.0001 as the wide area network (WAN) port and switch.0010 as the local area network port connected to the local network.

### 2.15.2 Installation Procedure

1. After powering on the device, connect to the IP address that the device supplies itself via a web browser. The connection will most likely require an interim switch for connecting, but this varies between cases.
2. The following screen should appear:

Figure 2-66 RUGGEDCOM Web Login

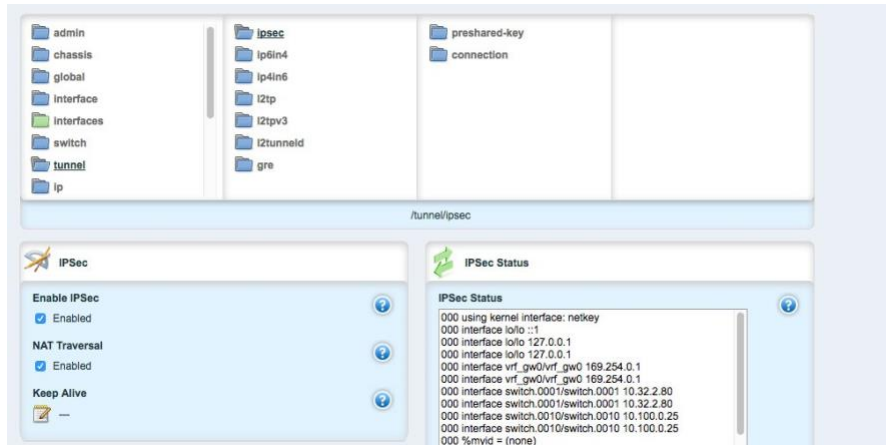


3. Once logged in, click the link for **Edit Private** to go into Edit mode.



4. Navigate to **tunnel -> ipsec**, and check the boxes for **Enable IP security (IPSec)** and network address translator (NAT) Traversal.

Figure 2-67 Enable IPSec and NAT Traversal



5. Click **preshared-key**, then **<Add preshared-key>**.
6. In the **Remote Address** field, type the remote IP address (the cogeneration plant's IP address).
7. In the **Local Address** field, type the local IP address (the enterprise network).
8. Click **Add**.
9. Click the newly created entry under the preshared-key folder.
10. Under **Secret Key**, create a new secret key that will be shared between devices.
11. Under **ipsec->connection**, click **<Add connection>** to create a new connection.
12. Fill in a name for **Connection Name**, then click **Add**.
13. Click on the new connection, and click the **Enable** check box for **Dead Peer Detect**.
14. Ensure that the settings under **Dead Peer Detect** are:
  - a. Interval: **30**
  - b. Timeout: **120**
  - c. Action: **Restart**
15. Under **Connection**, set the following parameters:

- a. Startup Operation: **start**
  - b. Authenticate By: **secret**
  - c. Connection Type: **tunnel**
  - d. Address-family: **ipv4**
  - e. Perfect Forward Secrecy: **yes**
  - f. SA Lifetime: **default**
  - g. IKE Lifetime: **default**
  - h. L2TP: **Unchecked (disabled)**
  - i. Monitor Interface: **switch.0001**
16. In the top window row, select the folder **ike**, and click **<Add algorithm>**.
17. Under **Key settings**, ensure the following parameters and click **Add**:
- a. Cipher Algorithm: **aes256**
  - b. Hash Method: **sha2**
  - c. Modpgroup: **modp8192**
18. Going back to the top window row, select the **esp** folder directly underneath **ike**, then select **algorithm** and click **<Add algorithm>**.
19. Under **Key settings**, ensure the following parameters and click **Add**:
- a. Cipher Algorithm: **aes256**
  - b. Hash Method: **sha2**
20. Going back to the top window row, select **left** under **esp**.
21. Under **Public IP Address**, ensure **Type** is **address**, then type the IP address into the **Hostname** or **IP Address** field.
22. Going back to the top window row, select **subnet**, and click **<Add subnet>**.
23. Under **Key Settings**, in the **Subnet Address** field, type the local subnet on the inside of the RX1400 in the box (lab used 10.100.0.0/16) and click **Add**.
24. Going back to the top window row, select **right** under **left**.

25. Under **Public IP Address**, ensure **Type** is **address**, then type the remote VPN IP Address into the **Hostname** or **IP Address** field.
26. Under the **Right** heading, for **NAT Traversal Negotiation Method**, select **rfc-3947**.
27. Going back to the top window row, select **subnet**, then click **<Add subnet>**.
28. Under **Key Settings**, in the **Subnet Address** field, type the remote subnet on the inside of the remote VPN in the box (lab used 172.19.0.0/16) and click **Add**.
29. Going back to the beginning of the top row, ensure that **interfaces->ip->switch.0001->ipv4** contains a folder named after the externally facing network IP address.
30. Ensure that **interface->ip->switch.0010->ipv4** contains a folder named after the internal network (lab used 10.100.0.0/16).

## 2.16 Siemens RUGGEDCOM RX1501 (O1)

The Siemens RUGGEDCOM RX1501 device is used on the boundary of the control network lab and creates an always-on VPN connection to the Siemens RUGGEDCOM RX1400, located on the inside of the enterprise network lab.

### 2.16.1 Siemens RUGGEDCOM RX1501 (O1) Installation Guide

The instructions for installation of the RUGGEDCOM RX1501 are very similar to those in [Section 2.15](#), with the following additional information:

1. Ensure that the shared key used in this installation is the same as the one used in the previous installation.
2. The remote IPs and local IPs will be different for this installation as they are relative to the device.
3. **NAT Traversal Negotiation Method** will be on the **left** menu option (as opposed to the **right** listed earlier) and must be the same value (e.g., rfc-3947).

## 2.17 TDi Technologies ConsoleWorks (E6, O5, O9)

TDi Technologies ConsoleWorks creates multiple consoles (both GUI- and terminal-based) that allow connections through a web interface to internal devices, utilizing a protocol break to separate connections. ConsoleWorks is also utilized to normalize syslogs from the control network before sending them to the SIEM.

### 2.17.1 System Environment

The system that was set up to run this application was a fully updated (as of 4/20/2016) CentOS 7 Operating System with the following hardware specifications:

- 4 GB RAM
- 500 GB HDD
- 2 network interface controllers (NICs)
- This installation required a preconfigured network where one NIC was located on the WAN side (connected to the Waterfall Secure Bypass) and the other was connected to the Dell R620 ESXi server.

Other requirements:

- ConsoleWorks install media (a CD was used in the build)
  - ConsoleWorksSSL-<version>.rpm
  - ConsoleWorks\_gui\_gateway-<version>.rpm
- ConsoleWorks license keys (TDI\_Licenses.tar.gz)
- software installation command:

```
yum install uuid libpng12 libvncserver
```

### 2.17.2 Installation

As Root:

1. Place ConsoleWorks Media into the system (assuming from here on that the media is in the form of a CD).
2. `mount /dev/sr0 /mnt/cdrom`
3. `mkdir /tmp/consoleworks`
4. `cp /mnt/cdrom/consolew.rpm /tmp/consoleworks/consolew.rpm`
5. `rpm -ivh /tmp/consoleworks/ConsoleWorksSSL-<version>.rpm`
6. `mkdir /tmp/consoleworkskeys/`
7. Copy ConsoleWorks keys to `/tmp/consoleworkskeys/`
8. `cd /tmp/consoleworkskeys/`
9. `tar xzf TDI_Licenses.tar.gz`
10. `cp /tmp/consoleworkskeys* /etc/TDI_licenses/`

11. `/opt/ConsoleWorks/bin/cw_add_invo`
12. **Accept** the License Terms.
13. Press **Enter** to continue.
14. Name the instance of ConsoleWorks.
15. Press **Enter** to accept default port (5176).
16. Press **N** to deny SYSLOG listening.
17. Press **Enter** to accept parameters entered.
18. Press **Enter** to return to `/opt/ConsoleWorks/bin/cw_add_invo`.
19. `rpm -ivh /tmp/consoleworks/ConsoleWorks_gui_gateway-version>.rpm`
20. `/opt/gui_gateway/install_local.sh`
21. `/opt/ConsoleWorks/bin/cw_start <invocation name created early>`
22. `service gui_gatewayd start`

### 2.17.3 Usage

1. Open a browser and navigate to `https://<ConsoleWorksIP>:5176`.
2. Log in with Username **console\_manager**, Password **Setup**.
3. Change the default password.
4. Choose **Register Now**.

#### 2.17.3.1 Initial Configuration

All instructions below start with a menu on the sidebar.

1. Tags

##### **Security > Tags > Add**

- i. Set **Name**.
- ii. Click **Save**.

2. Profiles

##### **Users > Profiles > Add**

- i. Set **Name**.

- ii. Select **Tag**.
- iii. Click **Save**.

### 3. Users

#### **Users->Add**

- i. Set **Name**.
- ii. Set **Password**.
- iii. Set **Profile**.
- iv. Set **Tag**.
- v. Click **Save**.

#### *2.17.3.2 Graphical Connections*

Use the following steps to set up graphical connections (specifically virtual network computing (VNC)):

##### 1. Graphical Gateway:

- a. **Graphical->Gateways->Add**
- b. Set a name, then set Host as **Localhost** and port as **5172**.
- c. Check the **Enabled** check box and click **Save**.
- d. Verify that it works by clicking **Test** in the top left corner.

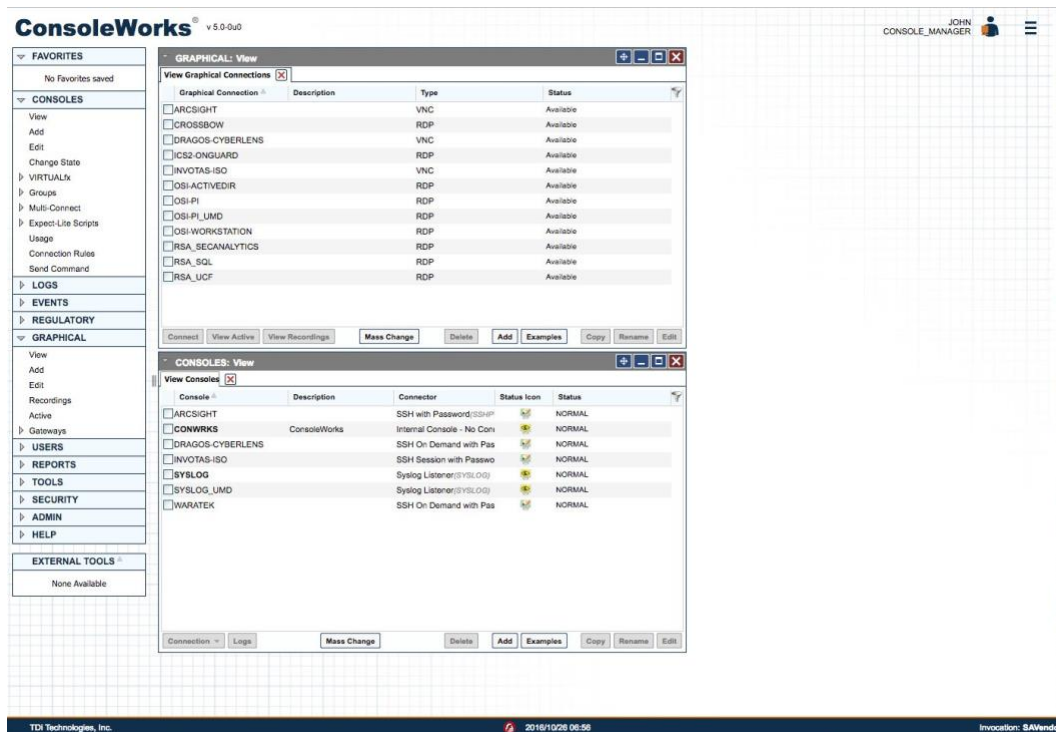
##### 2. Add a graphical connection (We will use VNC.):

- a. **Graphical->Add**
- b. Set **Name**.
- c. Set the **Type** (VNC/remote desktop protocol (RDP)).
- d. Set the **Hostname/IP**.
- e. If recordings are desired, set **Directory** and **Recordings**.
- f. Set the **Authentication**.
- g. Add **Graphical Gateway**.
- h. Add **Tags**.

### 3. Access Controls

- a. **Security->Access Control->Add**
- b. Set **Name**.
- c. Check **Enabled**.
- d. Set **Priority**.
- e. Set **ALLOW**.
- f. Set **Component Type** to **Graphical Connection**.
- g. The following will appear under **Profile Selection**:
  - i. Property Profile Equals \*Profile Name\* <join>
  - ii. The correct profile should appear in the box on right.
- h. The following will appear under **Resource Selection**:
  - i. Associate With a Tag that
  - ii. Property Tag Equals \*Tag name\* <join>
  - iii. The correct Graphical Console should appear in the box on right.
- i. Under **Privileges**, check ...
  - i. **Aware**
  - ii. **View**
  - iii. **Connect**
  - iv. **Enable**
  - v. **Monitor**
- j. Click **Save**.

Figure 2-68 Binding to Syslog



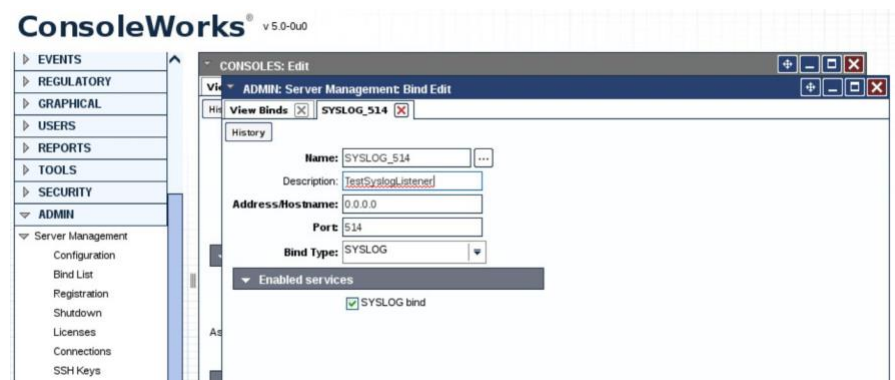
## 2.17.4 TDi Technologies ConsoleWorks (E6) Installation Guide

Follow the guide above on installing ConsoleWorks instance (O5), however, do not follow [Section 2.17.3.1](#), Initial Configuration; or [Section 2.17.3.2](#), Graphical Connections.

1. Navigate to **Server Management > Bind List > Add**.
2. Enter a name for **Binding** (e.g. SYSLOG\_514).
3. Leave **Address** as default (0.0.0.0).
4. Set **Port** to **514**.
5. Set Bind type to **SYSLOG** and **Enable**.

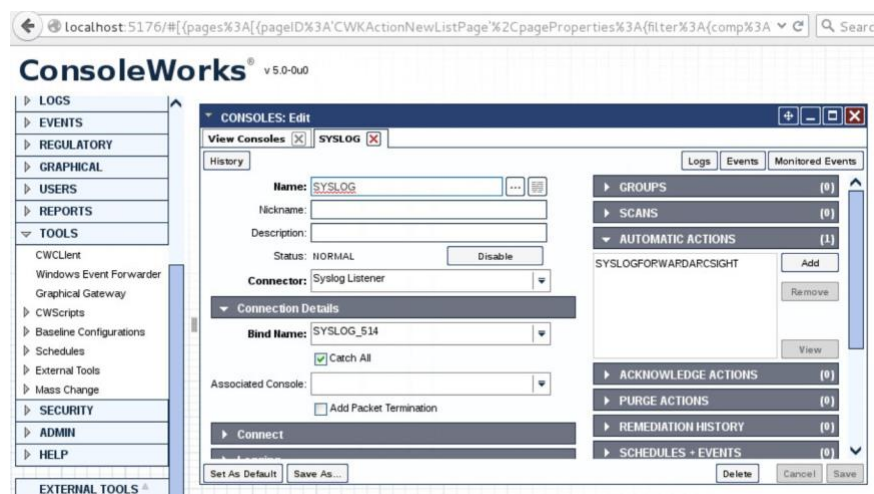


Figure 2-69 Server Management Bind Edit



6. Navigate to **Consoles > Add**.
7. Add **Console** and set a name (e.g., SYSLOG).
8. In the **Connector** field, click the drop-down menu, and select **Syslog Listener**.
9. Under **Connection Details**, click the drop-down menu, and select the **Binding** that was created above (e.g., SYSLOG\_514).
10. Check the **Catch All** check box.

Figure 2-70 Adding SYSLOG Console



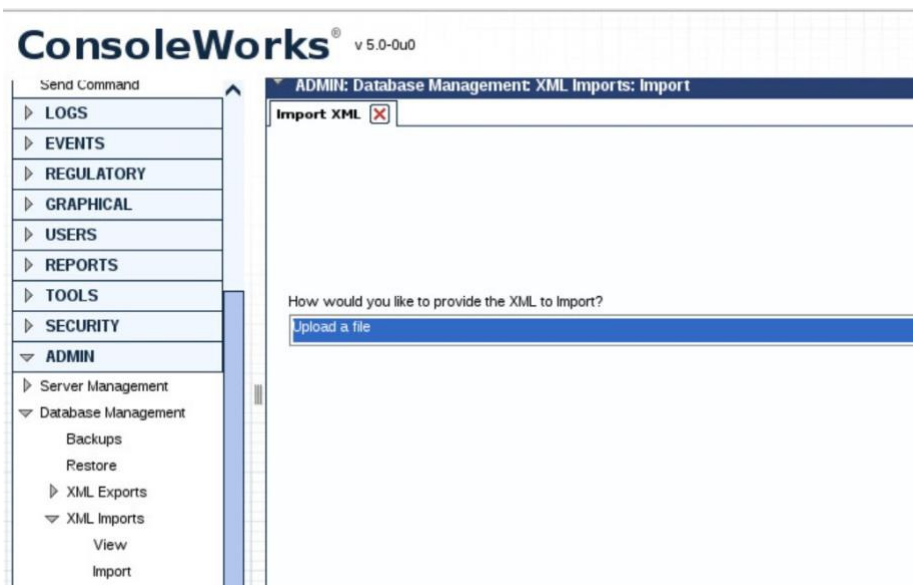
11. Copy the socket plug-in to the **cwscript** directory under the ConsoleWorks instance directory.

Figure 2-71 Copying Plug-In to CWScript Directory

```
[user@localhost bin]$ pwd
/opt/ConsoleWorks/bin
[user@localhost bin]$ sudo cp ./libPISocket.so /opt/ConsoleWorks/SAVendor/cwscript/
```

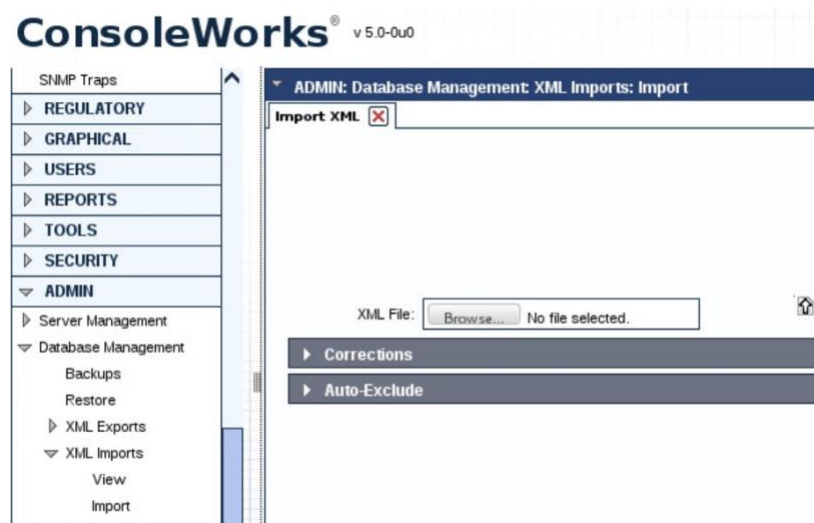
12. Navigate to **Admin > Database Management > XML Imports > Import > Upload a file**, then click **Next**.

Figure 2-72 CWScript Upload



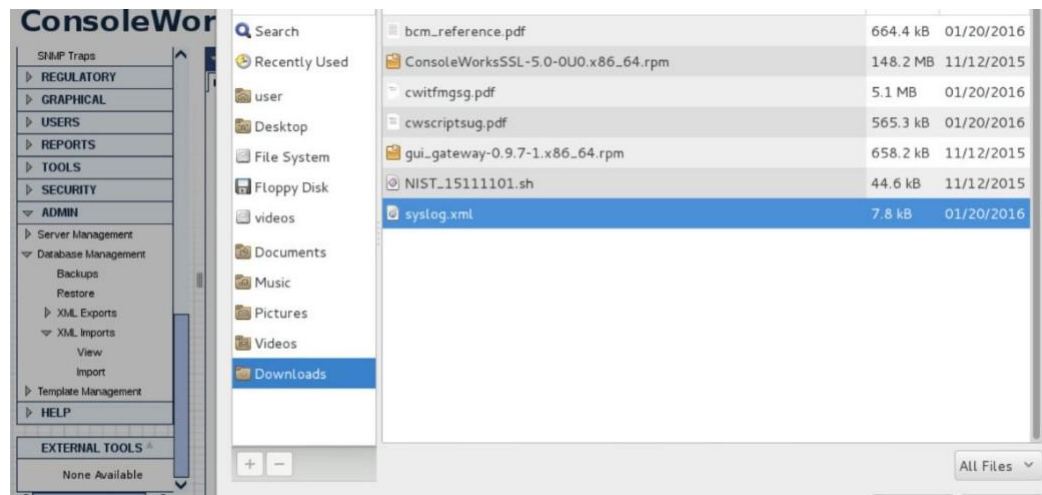
13. Click **Browse**.

Figure 2-73 Browse for CWScript



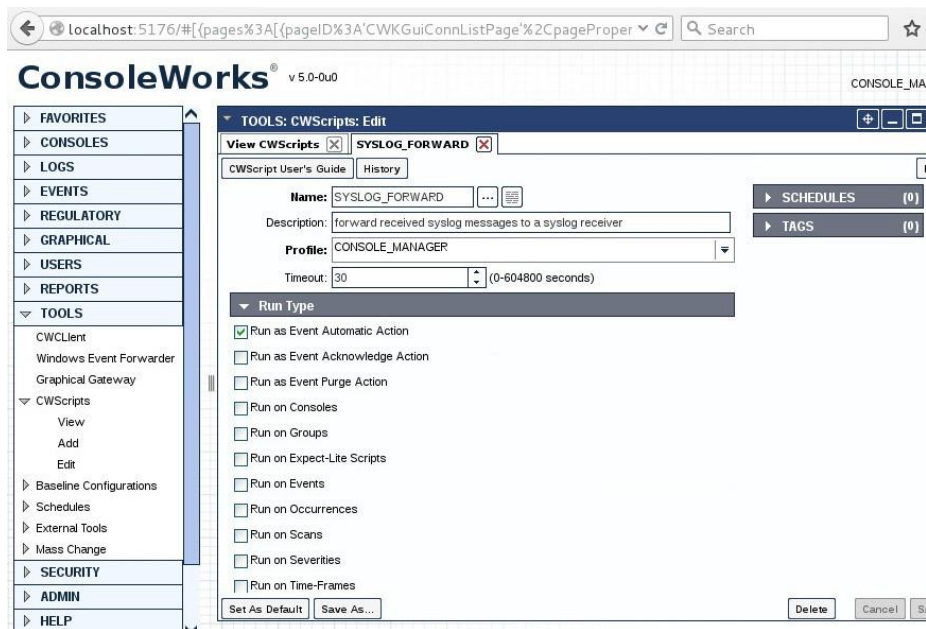
14. Select the **syslog.xml** file, then click **Next**.

Figure 2-74 Select CWScript XML



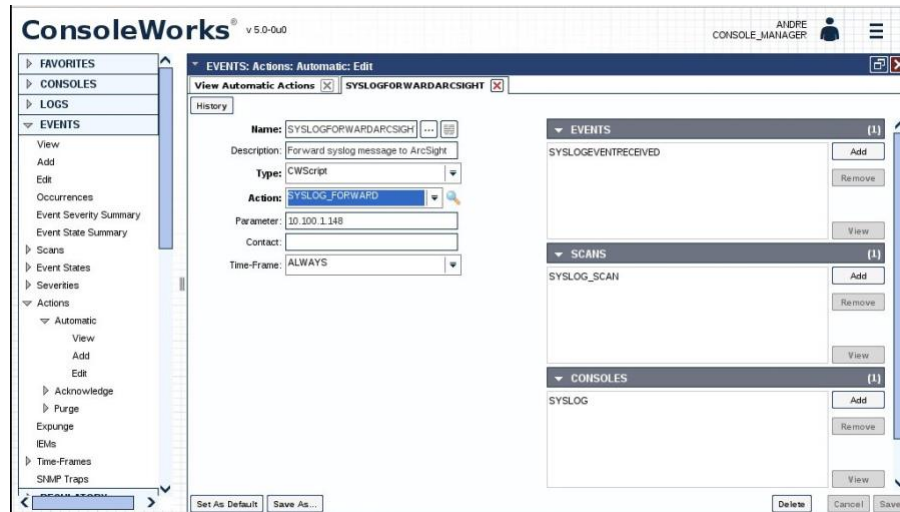
15. Navigate to **Tools > CWScripts > Select SYSLOG\_FORWARD > Review Settings**.

Figure 2-75 Review CWScript Settings



16. Navigate to **Actions > Automatic > Add**.
17. Set **Name**.
18. Set Type to **CWScript**.
19. In the **Action** field, click the drop-down menu, and select **SYSLOG\_FORWARD**.
20. In the **Parameter** field, enter the IP address (or FQDN) of the Syslog target.

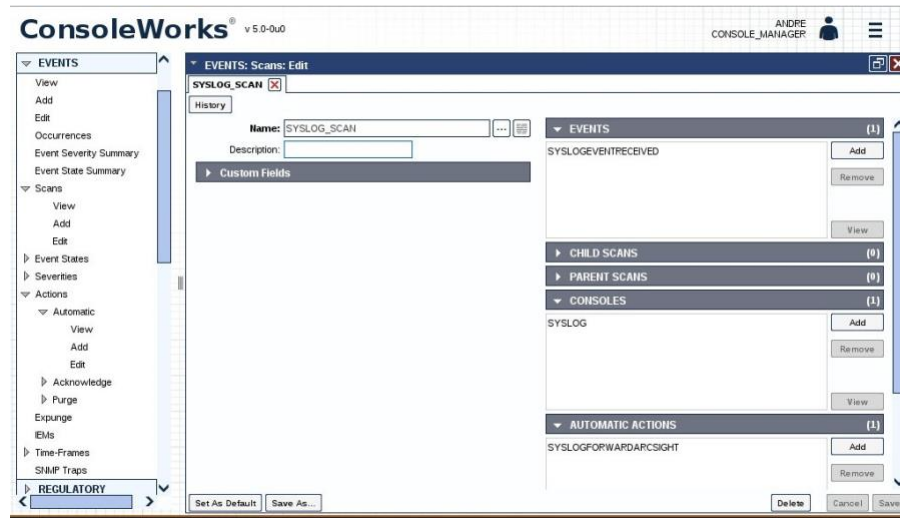
Figure 2-76 Modify Action and Parameter for CWScript



21. Navigate to **Scans**, then select **Add**.
22. Set **Name**.
23. In the **Consoles** field, add/select the Console defined in the previous steps.
24. In the **Automatic Action** field, add/select the Action defined in the previous steps.

Note: *The Events field will be updated later.*

Figure 2-77 Add New Scan



25. Navigate to **Events**, then select **Add**.
26. **Name** the Event.
27. Set the **Severity** level.
28. In the **Pattern** fields, line 1, type in a character pattern that matches the syslog data. Set **Wildcarding** to **Standard Wildcards**.
29. In the context **Lines Below** field, enter **1**.
30. In the **Scans** field, click **Add**, then select the name of the Scan that was defined in the previous steps.
31. In the **Automatic Actions** field, click **Add**, then select the name of the Action that was defined in the previous steps.

Figure 2-78 Add New Event

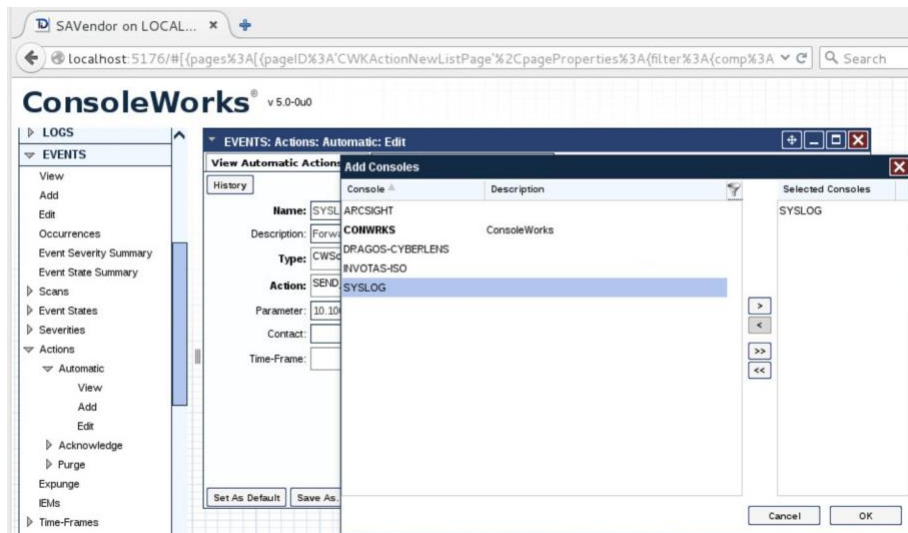
32. Navigate back to **Actions > Automatic**, then edit the Action defined in the previous steps.

33. In the **Event** field, confirm that the Event that was just created is selected.

Figure 2-79 Syslog Forwarding Action Config

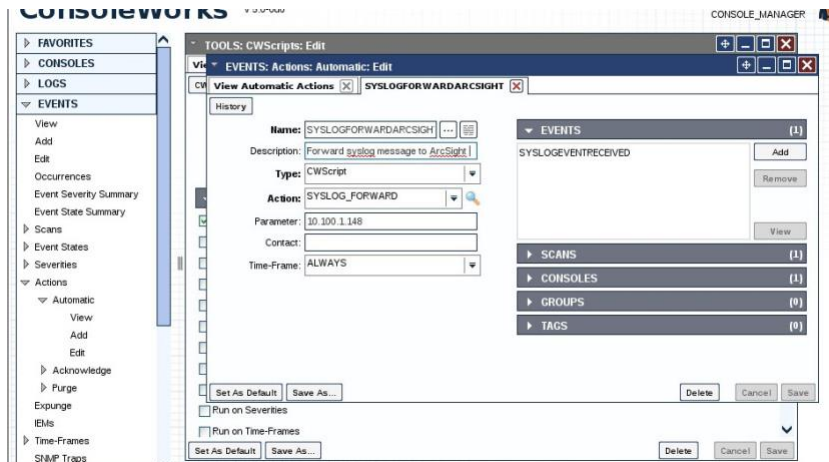
34. In the **Console** field, select the Syslog Console that was defined in previous steps.

Figure 2-80 Add Console to Syslog Forwarding Action Config



35. Review settings.

Figure 2-81 Review Event Settings



36. Add rules to ConsoleWorks host OS firewall:

```
iptables -I INPUT -p udp --dport 514 -s 0.0.0.0/0 -j ACCEPT
iptables -I OUTPUT -p udp -s 0.0.0.0/0 --dport 514 -j ACCEPT
```



37. Save the rules:

```
/sbin/service iptables save
```

### 2.17.5 TDi Technologies ConsoleWorks (O9) Installation Guide

Follow the guide for ConsoleWorks (E6) in [Section 2.17.4](#).

## 2.18 Waterfall Technologies Unidirectional Security Gateway (O2)

Waterfall's Unidirectional Security Gateway delivers a security gateway solution for replicating servers and emulating devices from the control system lab to the enterprise system lab. The replication occurs through hardware that is physically able to transmit information in only one direction and physically unable to transmit any information or attack in the reverse connection. The Unidirectional Gateway's combination of hardware and software supports many kinds of replications, including process historians, many open platform communication (OPC) variants, syslog, FTP, and others.

### 2.18.1 Waterfall Technologies Unidirectional Security Gateway (O2) Installation Guide

The Unidirectional Security Gateway was shipped to the NCCoE as an appliance in a 1U server chassis. The chassis contains two Host Modules, each running Microsoft Windows 8. The chassis also contains a Transmit (TX) Module and a Receive (RX) Module, linked by a short fiber-optic cable. The TX Module is physically able to send information/light to the fiber but is unable to receive any signal from the fiber. Conversely, the RX Module is able to receive information from the fiber but has no transmitter and so is physically unable to send any information to the fiber. In this guide, we will refer to the Windows Host Module connected to the TX Module as the Tx host, and the Windows Host Module connected to the RX Module as the Rx host.

#### 2.18.1.1 Rx Configuration

1. Open the **Waterfall RX Configuration** utility located in the **Start** menu.

##### 2.18.1.1.1 FTP Stream

1. Expand **wfStreamRx** from the left sidebar.
2. Expand **Files**.
3. From the sidebar, select **Local Folder**.
4. Under **Channels**, select **Add**. Ensure that the **Active** check box is checked.
5. Fill out the **Channel Name** field, and make a note of the **Channel ID** in parenthesis.
6. From the sidebar, select **NCFTP**.
7. Under **Channels**, select **Add**. Ensure that the **Active** check box is checked.

8. Select the **Automatically Bind to Local Folder with ID** radio button. Ensure that the ID for the Local Folder is selected by using the same ID that was automatically generated for the Local Folder that was just created.
9. Fill out the correct values for the following form fields:
  - a. FTP folder: **/file\_link**
  - b. FTP host: **10.100.1.250**
  - c. FTP port: **21**
  - d. Username: **waterfall**
  - e. Password: **<insert password here>**
10. For **Transfer mode**, select the **Passive** radio button.
11. For **Transfer type**, select the **Binary** radio button.
12. Ensure that the **Enable recursive transfer** check box is checked.
13. Ensure that the **File pattern** check box is checked and that the form field contains this value: **\***.

#### 2.18.1.1.2 OSI Pi Streams

1. Digital
  - a. Expand **wfStreamRxPI\_D** from the left sidebar.
  - b. Expand **SME** from the left sidebar.
  - c. Expand **PiPoint** from the left sidebar.
  - d. Ensure that the **Active** check box is checked.
  - e. Fill out the correct values for the following form fields:
    - i. Channel name: **PiPt Digital**
    - ii. Server IP: **10.100.1.76**
    - iii. Points type: **Digital**
    - iv. Snapshots/Sec limit: **5000**
    - v. Snapshots/Sec warning: **500**
2. Numeric
  - a. Expand **wfStreamRxPI\_N** from the left sidebar.

- b. Expand **SME** from the left sidebar.
- c. Expand **PiPoint** from the left sidebar.
- d. Ensure that the **Active** check box is checked.
- e. Fill out the correct values for the following form fields:
  - i. Channel name: **PiPt Numeric**
  - ii. Server IP: **10.100.1.76**
  - iii. Points type: **Numeric**
  - iv. Snapshots/Sec limit: **5000**
  - v. Snapshots/Sec warning: **5000**

### 3. String

- a. Expand **wfStreamRxPI\_S** from the left sidebar.
- b. Expand **SME** from the left sidebar.
- c. Expand **PiPoint** from the left sidebar.
- d. Ensure that the **Active** check box is checked.
- e. Fill out the correct values for the following form fields:
  - i. Channel name: **PiPt String**
  - ii. Server IP: **10.100.1.76**
  - iii. Points type: **String**
  - iv. Snapshots/Sec limit: **5000**
  - v. Snapshots/Sec warning: **5000**

#### 2.18.1.1.3 Syslog Streams

1. Expand **wfStreamRx** from the left sidebar.
2. Expand **IT Monitoring** from the left sidebar.
3. Select **Syslog UDP** from the left sidebar.
4. Under **Channels**, select **Add**. Ensure that the **Active** check box is checked.
5. Fill out the correct values for the following form fields:

Channel name: **Syslog 1**

Send report every: **500**

6. Under **Target Addresses**, select **Add**, and set the IP address to **10.100.0.50** and port to **514**.

### 2.18.1.2 TX Configuration

Open the **Waterfall TX Configuration** utility located in the **Start** menu.

#### 2.18.1.2.1 FTP Stream

1. Expand **wfStreamTx** from the left sidebar.
2. Expand **Files**.
3. From the sidebar, select **Local Folder**.
4. Under **Channels**, select **Add**. Ensure that the **Active** check box is checked.
5. Fill out the **Channel name** field, and make a note of the **Channel ID** in parenthesis.
6. From the sidebar, select **NCFTP**.
7. Under **Channels**, select **Add**. Ensure that the **Active** check box is checked.
8. Select the **Automatically Bind to Local Folder with ID** radio button. Select the ID that was automatically generated for the Local Folder created in the previous steps.
9. Fill out the correct values for the following form fields:
  - a. FTP folder: **/file\_link**
  - b. FTP host: **172.18.1.250**
  - c. FTP port: **21**
  - d. Username: **root**
  - e. Password: **<insert password here>**
10. For **Transfer mode**, select the **Passive** radio button.
11. For **Transfer type**, select the **Binary** radio button.
12. Ensure that the **Enable recursive transfer** check box is checked.
13. Ensure that the **File pattern** check box is checked and that the field contains this value: **\***.

#### 2.18.1.2.2 OSI Pi Streams

##### 1. Digital

- a. Expand **wfStreamTxPI\_D** from the left sidebar.
- b. Expand **SME** from the left sidebar.
- c. Expand **PiPoint** from the left sidebar.
- d. Ensure that the **Active** check box is checked.
- e. Fill out the correct values for the following form fields:
  - i. Channel name: **PiPt Digital**
  - ii. Server IP: **172.18.2.150**
  - iii. Points type: **Digital**
  - iv. Snapshots/Sec limit: **5000**
  - v. Snapshots/Sec warning: **5000**
  - vi. APS port: **3010**

##### 2. Numeric

- a. Expand **wfStreamTxPI\_N** from the left sidebar.
- b. Expand **SME** from the left sidebar.
- c. Expand **PiPoint** from the left sidebar.
- d. Ensure that the **Active** check box is checked.
- e. Fill out the correct values for the following form fields:
  - i. Channel name: **PiPt Numeric**
  - ii. Server IP: **172.18.2.150**
  - iii. Points type: **Numeric**
  - iv. Snapshots/Sec limit: **5000**
  - v. Snapshots/Sec warning: **5000**
  - vi. APS port: **3000**

### 3. String

- a. Expand **wfStreamTxPI\_S** from the left sidebar.
- b. Expand **SME** from the left sidebar.
- c. Expand **PiPoint** from the left sidebar.
- d. Ensure that the **Active** check box is checked.
- e. Fill out the correct values for the following form fields:
  - i. Channel name: **PiPt String**
  - ii. Server IP: **172.18.2.150**
  - iii. Points type: **String**
  - iv. Snapshots/Sec limit: **5000**
  - v. Snapshots/Sec warning: **5000**
  - vi. APS port: **3020**

#### 2.18.1.2.3 Syslog Streams

1. Expand **wfStreamTx** from the left sidebar.
2. Expand **IT Monitoring** from the left sidebar.
3. Select **Syslog UDP** from the left sidebar.
4. Under **Channels**, select **Add**. Ensure that the **Active** check box is checked.
5. Fill out the correct values for the following form fields:
  - a. Channel name: **Syslog 1**
  - b. Send report every: **500**
  - c. Port: **514**
  - d. IP (Listening): **0.0.0.0**
6. Under **target addresses**, select **Add**. Set the IP address to **10.100.0.50** and port to **514**.

## 2.19 Waterfall Secure Bypass (O17)

Waterfall Secure Bypass is used as a secure connection solution that allows bidirectional communication into the product lab at the control system. It is solely dependent on a person turning a physical key, and it has an automated time-out of two hours.

### 2.19.1 Waterfall Secure Bypass (O17) Installation Guide

The Waterfall Secure Bypass Solution is installed directly between the Siemens RUGGEDCOM RX1501 (O1) and a Schneider Electric Tofino Firewall (O18).

1. Connect an Ethernet cable from the RX1501 to the **Ext** interface of the Secure Bypass.
2. Connect an Ethernet cable from the WAN interface of the Tofino to the **Int** interface of the Secure Bypass.
3. When the key is fully turned clockwise, the Secure Bypass will allow bidirectional traffic between the Tofino and the RX1501.
4. When the key is fully turned counterclockwise, the Secure Bypass will block all traffic between the Tofino and the RX1501.
5. If the key is left fully turned clockwise for more than two hours (time was configured at Waterfall location prior to receiving the device), the Secure Bypass will block all traffic between the Tofino and the RX1501. To allow for traffic to pass again, the user must fully turn the key counterclockwise and then clockwise again.

Figure 2-82 Waterfall Secure Bypass Interface



## 2.20 Waratek Runtime Application Protection (E10)

Waratek Runtime Application Protection is a software agent plug-in for monitoring and protecting user interactions with enterprise applications. In the build, Waratek is monitoring a database application for any attempts the user may undertake to pull unauthorized data from the database (mainly through SQL injection).

For further information, see <http://www.waratek.com/solutions/> or <http://www.waratek.com/runtime-application-self-protection-rasp/>.

### 2.20.1 System Environment

A CentOS 7 Operating System (fully updated as of 4/20/2016) was set up to run this application. Other requirements:

Web application that demonstrates protection capabilities (this build used Spiracle, Waratek's demo application: <https://github.com/waratek/spiracle>).

- web application server (This build used Apache Tomcat 9.)
- SQL database (can be MSSQL, MySQL, or Oracle. In the build, we used MySQL.)

### 2.20.2 Waratek Runtime Application Protection (E10) for Java Installation

1. Download JDK 8 from the Oracle site, and unzip in **/opt** directory (e.g. **/opt/jdk1.8.0\_121**).
2. To configure for apache tomcat (or other web server), in `$CATALINA_HOME/bin/Catalina.sh`, point `JAVA_HOME` to `/opt/<jdk version>`

3. Add the following line to `Catalina.sh`:

```
JAVA_OPTS="-javaagent:/opt/waratek/waratek.jar
-Dcom.waratekContainerHome=/opt/<jdk version>"
```

4. Change directories to **/opt**, and untar the **waratek\_home.tar.gz** package.
5. `cd waratek_home`
6. Create the **Rules** directory in the current directory.
7. Move the provided **LICENSE\_KEY** file from Waratek to **/var/lib/javad/**.

8. Create a rules file: **/opt/waratek-home/Rules/global.rules**

```
VERSION 1.0

SQL Injection Blocking sql:database:mysql:deny:warn
file:read:/opt/tomcat/*:allow:trace
```

9. Create a logging XML file: **/opt/waratek/mylogProps.xml**

```
<logProps-array>

<logProps>

 <logMode>BOTH</logMode>

 <logFile>SECURITYLOG</logFile>

 <fileName>/opt/waratek/alerts.log</fileName>

 <remoteHost>**INSERT REMOTE SYSLOG HERE (i.e.
 10.100.100.10:514)**</remoteHost>
```



```

 <patternLayout>%m</patternLayout>

 <priorityLevel>WARN</priorityLevel>

 </logProps>

</logProps-array>

```

10. Edit the **/opt/waratek\_home/setenv.sh** file as follows:

```

export WARATEK_OPTS="-Dcom.waratek.jvm.name=tomcat7
-Dcom.waratek.rules.local=/opt/waratek_home/Rules/jvc.rules
-Dcom.waratek.log.properties=/opt/waratek_home/logProps.xml
-Dcom.waratek.jmxh

```

### 2.20.3 Usage

To utilize the Runtime Protection for Java product, start the web application mentioned in [Section 2.20.1](#), System Environment. The web application server (Tomcat 9 in our case) should load the Runtime Protection JDK that was configured.

## 2.21 ArcSight Connector Guides

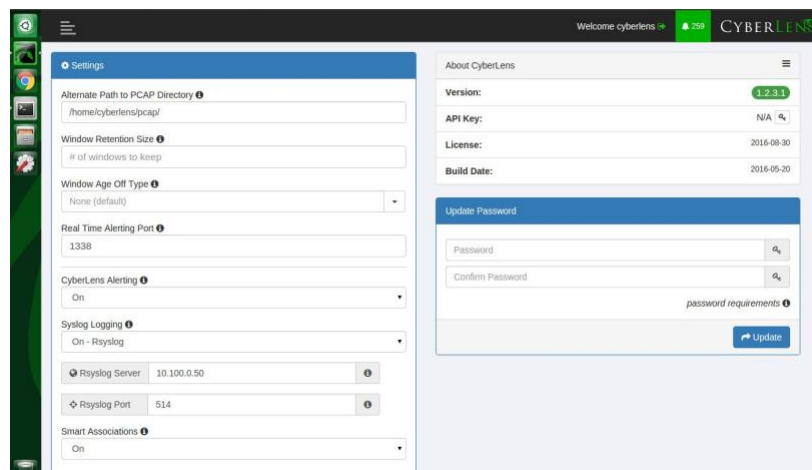
The following detail the custom configuration for the ArcSight connectors to individual monitoring and alerting products.

### 2.21.1 Dragos CyberLens Connector

#### 2.21.1.1 Configure Source Product

1. Connect to the CyberLens console.
2. In the CyberLens application, go to **Settings**.
3. In the **CyberLens Alerting** drop-down, select **On**.
4. In the **Syslog Logging** section ...
  - a. Select the drop-down for **On - Rsyslog**.
  - b. Enter the **IP address** of the syslog server, e.g.:  
 172.18.0.50
  - c. Enter the **port** of the syslog server, e.g.:  
 514

Figure 2-83 Set Up Syslog on CyberLens



5. From the command line, using the **cybersudo** account, check the OS firewall to see if it allows the syslog traffic by running **sudo ufw status**. **Add** and **save** the rule if needed.

*Note: Upon upgrading CyberLens software, the rsyslog settings may be lost. Be sure to check and update these settings as needed after any upgrades.*

### 2.21.1.2 Install/Configure Custom ArcSight FlexConnector

1. Follow ArcSight's instructions for installing a Linux-based syslog SmartConnector [1].
2. Copy the custom FlexConnector configuration files to the appropriate locations.
3. Start the Connector service:

```
/etc/init.d/arc_<connectorName> start
```

### 2.21.1.3 Custom Parser — ArcSight FlexConnector Parser

1. Create a file containing the text below, and copy this file to **/opt/arcsight/connectors/<connector directory>/current/user/agent/flexagent/cyberlens.subagent.sdkrfilereader.properties**

```
#::
Syslog custom subagent regex properties file: for CyberLens rsyslog
#
raw syslog example:
"Sep 6 16:04:48 ubuntu CyberLensApp: I, [2016-09-06T16:04:48.839937
#65401] INFO -- : Cyberlens generated the following alert: A Sensor
saw 'S7COMM' for the first time"
```

```
#
#::

without double slashes
regex=(CyberLensApp):\sI, ([\d+-\d\d-\d\d\S\d\d:\d\d:\d\d.\d+
#\d+]) (\D+) -- : (.*)\n?Source IP: (\d+.\d+.\d+.\d+)\n?(.*)
with double slashes and newline
regex=(CyberLensApp):\sI,
([\\[\d+-\\d\\d-\\d\\d\\S\\d\\d:\\d\\d:\\d\\d.\d+ #\\d+]) (\\D+) -- :
(.*)\\n?Source IP: (\\d+\\.\\d+\\.\\d+\\.\\d+)\\n?(.*)

token.count=6 token[0].name=Application
token[1].name=Message
token[2].name=Severity
token[3].name=Name
token[4].name=SourceIP
token[4].type=IPAddress
token[5].name=CatchAnyDoubledLines

event.name=Name
event.deviceProduct= stringConstant("CyberLens")
event.deviceVendor= stringConstant("DragosSecurity")
event.deviceSeverity=Severity
event.message=Message event.deviceProcessName=Application
event.deviceAddress=SourceIP
event.deviceCustomString1=CatchAnyDoubledLines

severity.map.veryhigh.if.deviceSeverity=1,2
severity.map.high.if.deviceSeverity=3,4
severity.map.medium.if.deviceSeverity=5,6
severity.map.low.if.deviceSeverity=INFO
```

#### 2.21.1.4 *ArcSight agent.properties File*

1. Modify the agent.properties file settings as needed based on the example below:

**`/opt/arcsight/connectors/<connector directory>/current/user/agent/agent.properties`**

2. Modify the **customsubagent** list as needed for the environment.

### 3. Replace the **IP address** to suit the environment.

```
#ArcSight Properties File
#Fri Mar 18 17:37:10 GMT 2016

agents.maxAgents=1
agents[0].aggregationcachesize=1000

agents[0].customsubagentlist=cyberlens.subagent.sdkrfilereader.properties_syslog|cyberlensPREFIX.subagent.sdkrfilereader.properties_syslog|sourcefire_syslog|ciscovpnios_syslog|apache_syslog|ciscovpnnoios_syslog|ciscorouter_syslog|pf_syslog|nagios_syslog|cef_syslog|ciscorouter_nonios_syslog|catos_syslog|symantecnetworksecurity_syslog|snare_syslog|mcafeesig_syslog|symantecendpointprotection_syslog|citrix_syslog|linux_auditd_syslog|vmwareesx_syslog|citrixnetscaler_syslog|vmwareesx_4_1_syslog|pulseconnectsecure_syslog|pulseconnectsecure_keyvalue_syslog|flexagent_syslog|generic_syslog

#agents[0].customsubagentlist=sourcefire_syslog|ciscorouter_syslog|pf_syslog|cef_syslog|ciscorouter_nonios_syslog|catos_syslog|symantecnetworksecurity_syslog|symantecendpointprotection_syslog|linux_auditd_syslog|vmwareesx_syslog|vmwareesx_4_1_syslog|flexagent_syslog|generic_syslog g
agents[0].destination.count=1

agents[0].destination[0].agentid=3R9bQilMBABCIy6NStvvaDA\=\=
agents[0].destination[0].failover.count=0

agents[0].destination[0].params=<?xml version\="1.0" encoding\="UTF-8"?>\n<ParameterValues>\n
<Parameter Name\="aupmaster" Value\="false"/>\n
<Parameter Name\="port" Value\="8443"/>\n
<Parameter Name\="fipsciphers" Value\="fipsDefault"/>\n
<Parameter Name\="host"
Value\="arcsight.es-sa-bl.test"/>\n
<Parameter Name\="filterevents"
Value\="false"/>\n</ParameterValues>\n
agents[0].destination[0].type=http
agents[0].deviceconnectionalertinterval=60000
agents[0].enabled=true
agents[0].entityid=0WbNilMBABCAAoBJrJmUOw\=\=
agents[0].fcp.version=0
agents[0].filequeuemaxfilecount=100
agents[0].filequeuemaxfilesize=10000000
agents[0].forwarder=false agents[0].forwardmode=true
agents[0].id=3R9bQilMBABCIy6NStvvaDA\=\=
```

```

agents[0].ipaddress=10.100.1.148
agents[0].overwriteraevent=false
agents[0].persistenceinterval=0
agents[0].port=514 agents[0].protocol=UDP
agents[0].rawloginterval=-1
agents[0].rawlogmaxsize=-1
agents[0].tcpbindretrytime=5000
agents[0].tcpbuffersize=10240
agents[0].tcpcleanupdelay=-1
agents[0].tcpmaxbuffersize=1048576
agents[0].tcpmaxidletime=-1
agents[0].tcpmaxsockets=1000
agents[0].tcppeerclosedchecktimeout=-1
agents[0].tcpsetsocketlinger=false
agents[0].tcpsleeptime=50
agents[0].type=syslog
agents[0].unparsedevents.log.enabled=true
agents[0].usecustomsubagentlist=true
agents[0].usefilequeue=true
remote.management.ssl.organizational.unit=HzjHilMBABCAAWiRlATijw

```

### 2.21.1.5 Map File

1. Create a file containing the text below, and copy this file to **/opt/arcsight/<connector directory>/current/user/agent/map/map.1.properties**

**Note:** *If an existing map.1.properties file exists, increment the suffix as needed (e.g., map.2.properties).*

```

!Flags,CaseSens-,Overwrite
regex.event.name,set.event.deviceVendor,set.event.deviceProduct
.*Cyberlens.*,DragosSecurity,CyberLens

```

### 2.21.1.6 Categorization File

1. Create a .csv file containing the text below, and copy this file to **/opt/arcsight/<connector directory>/current/user/agent/acp/categorizer/current/<deviceproduct>/deviceproduct.csv**

|         |            |            |            |             |              |            |
|---------|------------|------------|------------|-------------|--------------|------------|
| event.  | set.event. | set.event. | set.event. | set.event.  | set.event.   | set.event. |
| device  | category   | category   | category   | category    | category     | category   |
| Product | Object     | Behavior   | Technique  | DeviceGroup | Significance | Outcome    |

CyberLens /Host /Found /Traffic /IDS/Network /Informational /attempt  
Anomaly

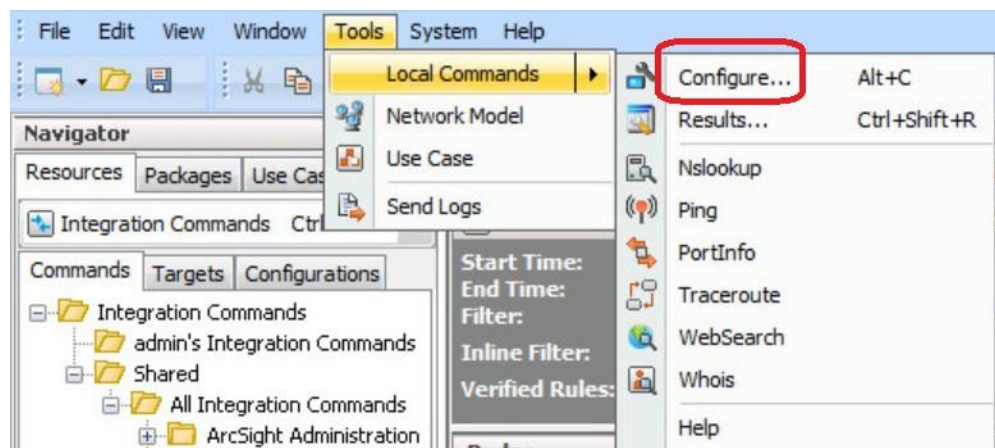
## 2.21.2 ICS2 OnGuard

### 2.21.2.1 Integration Setup

This will allow a user to right-click on a URL in an event to spawn OnGuard with the URL passed as a parameter.

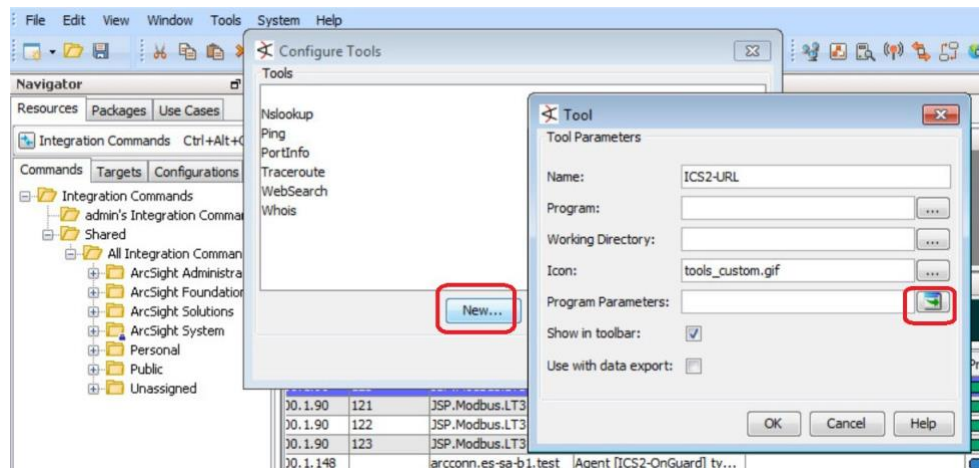
1. Select **Tools > Local Commands > Configure**.

Figure 2-84 ArcSight Configure



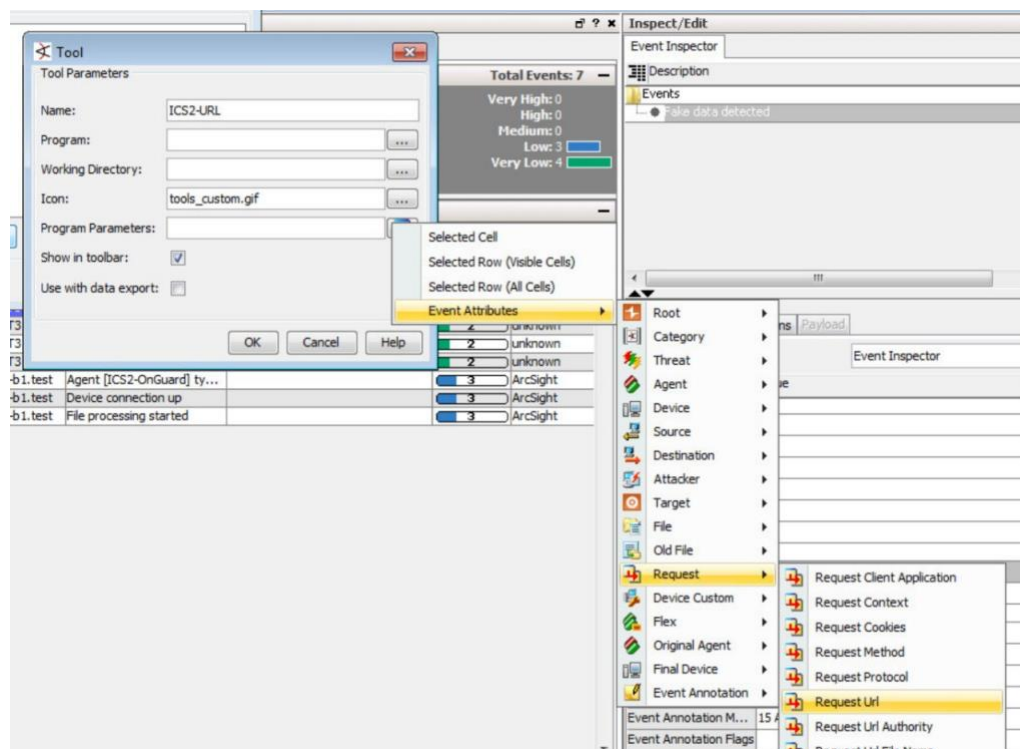
2. In the **name** field, type **ICS2-URL**, then select the **Program Parameters** browse button.

Figure 2-85 Program Parameters Setup



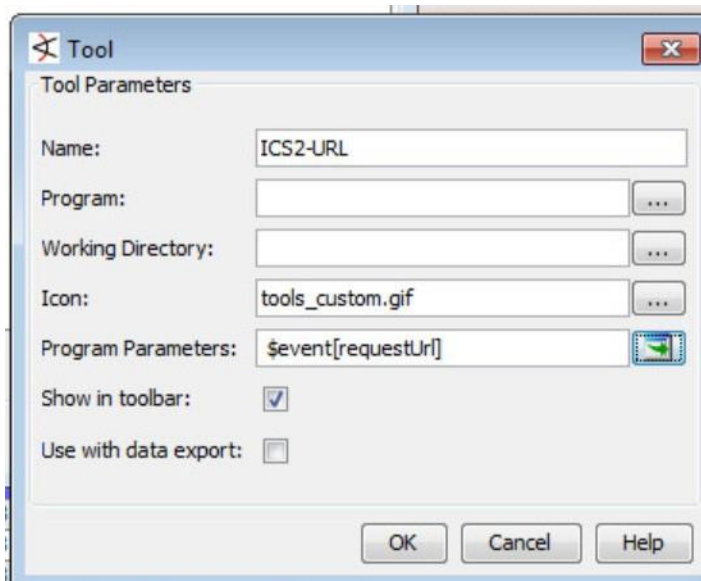
3. Select **Event Attributes > Request > Request URL**.

Figure 2-86 Request URL Configuration



4. Select **OK**.

Figure 2-87 Tool URL Verification



5. Right-click on a **URL** in an event, select **Tools**, and verify that the **ICS2-URL tool** appears in the menu.

#### 2.21.2.2 Install/Configure Custom ArcSight FlexConnector

1. Follow ArcSight's instructions for installing a Linux-based syslog SmartConnector.
2. Copy the custom FlexConnector configuration files to the appropriate locations.
  - a. See Sections 6-8 of cyberlens-syslog-configuration-v2\_3.docx.
3. Start the Connector service:

```
/etc/init.d/arc_[connectorName] start
```

#### 2.21.2.3 Custom Parser — ArcSight FlexConnector Parser

1. Create a file containing the text below, and copy the file to **/opt/arcsight/connectors/[connector-directory]/current/user/agent/flexagent/onguard.s dkrfilereader.properties**

```
#::
Syslog custom regex properties file
for ICS^2 OnGuard CEF syslog
```



```

delimiter=| text.qualifier="
comments.start.with=\#
trim.tokens=true
contains.empty.tokens=true

token.count=8

token[0].name=Token0 token[0].type=String
token[1].name=Token1 token[1].type=String
token[2].name=Token2 token[2].type=Integer
token[3].name=Token3 token[3].type=String
token[4].name=Token4 token[4].type=String
token[5].name=Token5
token[5].type=TimeStamp
token[5].format=yyyy-MM-dd HH\:mm\:ssz
token[6].name=Token6
token[6].type=TimeStamp
token[6].format=yyyy-MM-dd HH\:mm\:ssz
token[7].name=Token7 token[7].type=String
mappings
event.deviceCustomString1=Token0
event.deviceHostName=Token1
event.externalId=Token2
event.name=Token3 event.message=Token4
event.startTime=Token5
event.endTime=Token6
event.requestUrl=Token7
event.deviceVendor= stringConstant("ICS2")
event.deviceProduct= stringConstant("OnGuard")

#severity.map.veryhigh.if.deviceSeverity=1,2
severity.map.high.if.deviceSeverity=HIGH
severity.map.medium.if.deviceSeverity=MEDIUM
severity.map.low.if.deviceSeverity=LOW
severity.map.verylow.if.deviceSeverity=INFO

```

#### 2.21.2.4 ArcSight agent.properties File

Example, from the following directory: **/opt/arcsight/connectors/[connector directory]/current/user/agent/agent.properties**

```
#ArcSight Properties File
#Fri Apr 08 22:28:12 BST 2016
agents.maxAgents=1
agents[0].AgentSequenceNumber=0
agents[0].configfile=onguard
agents[0].destination.count=1
agents[0].destination[0].agentid=3dfzD91MBABDtvfjvZeFjZw\=\=
agents[0].destination[0].failover.count=0
agents[0].destination[0].params=<?xml version\="1.0"
encoding\="UTF-8"?>\n<ParameterValues>\n <Parameter Name\="host"
Value\="arcsight.es-sa-bl.test"/>\n <Parameter Name\="aupmaster"
Value\="false"/>\n <Parameter Name\="filterevents"
Value\="false"/>\n<Parameter
Name\="port" Value\="8443"/>\n
<Parameter Name\="fipsciphers"
Value\="fipsDefault"/>\n</ParameterValues>\n
agents[0].destination[0].type=http
agents[0].deviceconnectionalertinterval=60000
agents[0].enabled=true
agents[0].entityid=3dfzD91MBABDtvfjvZeFjZw\=\=
agents[0].extractfieldnames=
agents[0].extractregex=
agents[0].extractsource=File Name
agents[0].fcp.version=0
agents[0].fixedlinelength=-1
agents[0].followexternalrotation=true
agents[0].id=3dfzD91MBABDtvfjvZeFjZw\=\=
agents[0].internalevent.filecount.duration=-1
agents[0].internalevent.filecount.enable=false
agents[0].internalevent.filecount.minfilecount=-1
agents[0].internalevent.filecount.timer.delay=60
agents[0].internalevent.fileend.enable=true
```

```

agents[0].internalevent.filestart.enable=true
agents[0].logfilename=/opt/arcsight/connectors/syslogfiledata/OnGuardS
yslogExample.txt
agents[0].maxfilesize=-1
agents[0].onrotation=RenameFileInTheSameDirectory
agents[0].onrotationoptions=processed
agents[0].persistenceinterval=0
agents[0].preservedstatecount=10
agents[0].preservedstateinterval=30000
agents[0].preservestate=false
agents[0].rotationonlywheneventexists=false
agents[0].rotationdelay=30
agents[0].rotationscheme=None
agents[0].rotationsleeptime=10
agents[0].startatend=false
agents[0].type=sdkfilereader
agents[0].unparsedevents.log.enabled=true
agents[0].usealternaterotationdetection=false
agents[0].usefieldextractor=false
agents[0].usenonlockingwindowsfilereader=false
remote.management.second.listener.port=10051
remote.management.ssl.organizational.unit=vRTB91MBABCAASNGV81kQQ
server.base.url=https\://arcsight.es-sa-b1.test\:8443
server.registration.host=arcsight.es-sa-b1.test

```

## 2.21.2.5 Additional Configuration Files

### 2.21.2.5.1 Map File

Create a file containing the text below, and copy this file to **/opt/arcsight/connector directory]/current/user/agent/map/map.1.properties**

**Note:** *If an existing map.1.properties file exists, increment the suffix as needed (e.g., map.2.properties).*

```

!Flags,CaseSens-,Overwrite
regex.event.name,set.event.deviceVendor,set.event.deviceProduct
.*On-Guard.*,ICS2,OnGuard
.*OnGuard.*,ICS2,OnGuard

```

### 2.21.2.5.2 Categorization File

Create a .csv file containing the text below, and copy this file to **/opt/arcsight/connector directory]/current/user/agent/acp/categorizer/current/[deviceproduct]/ deviceproduct.csv**

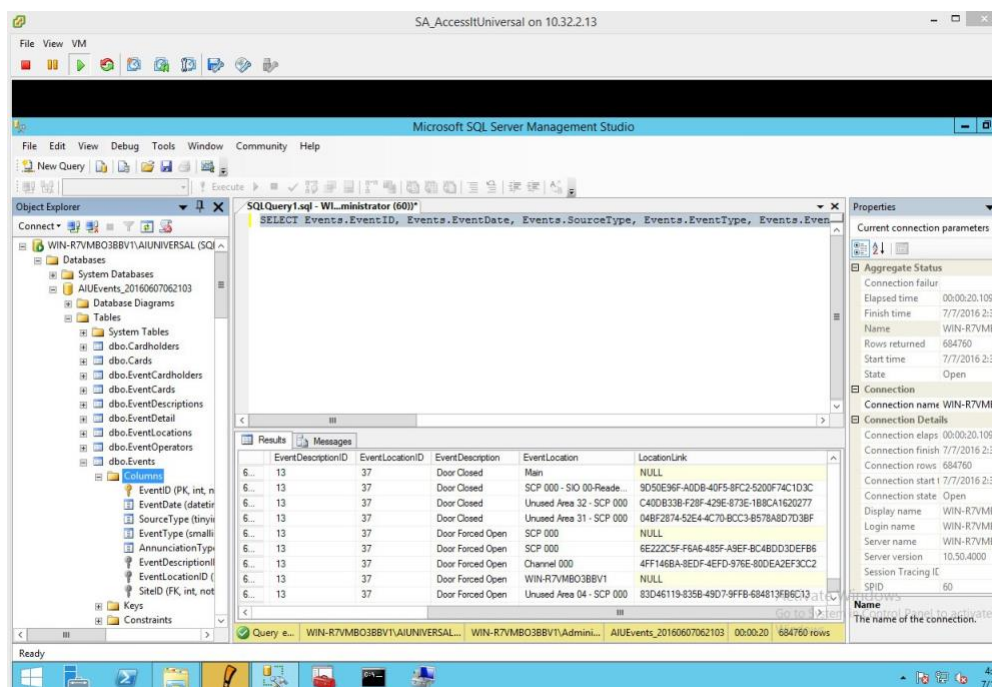
|         |            |            |            |              |                |            |
|---------|------------|------------|------------|--------------|----------------|------------|
| event.  | set.event. | set.event. | set.event. | set.event.   | set.event.     | set.event. |
| device  | category   | category   | category   | category     | category       | category   |
| Product | Object     | Behavior   | Technique  | DeviceGroup  | Significance   | Outcome    |
| OnGuard | /Host      | /Found     | /Traffic   | /IDS/Network | /Informational | /Attempt   |
|         |            |            | Anomaly    |              |                |            |

## 2.21.3 RS2 Access It! Universal.NET

### 2.21.3.1 Review Data Source

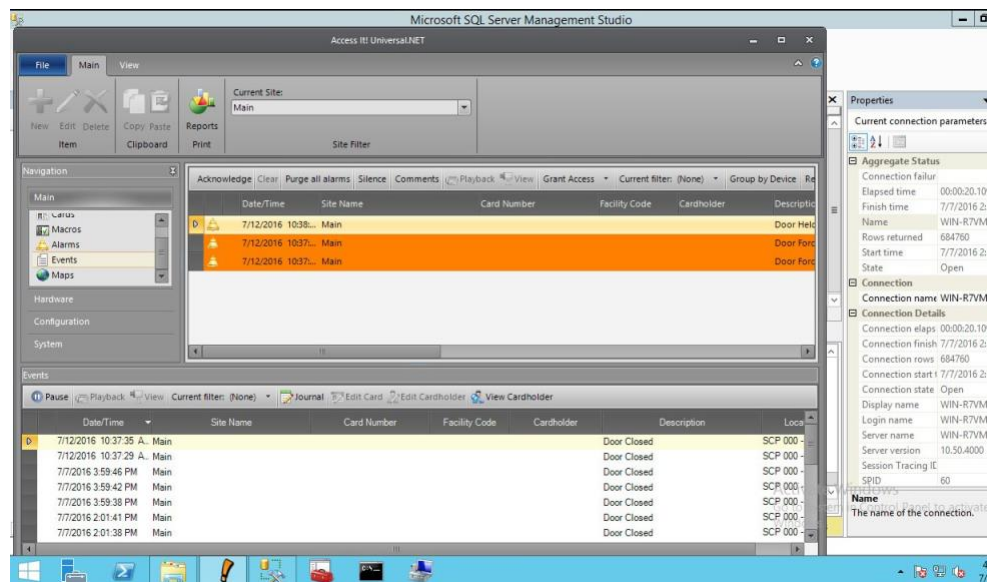
1. Review the relevant fields in Access It!'s Microsoft SQL Server Management Studio.

Figure 2-88 Access It! SQL Table



2. Review the data in RS2's Access It! application.

Figure 2-89 Access It! Application Window



### 2.21.3.2 Install/Configure Custom ArcSight FlexConnector

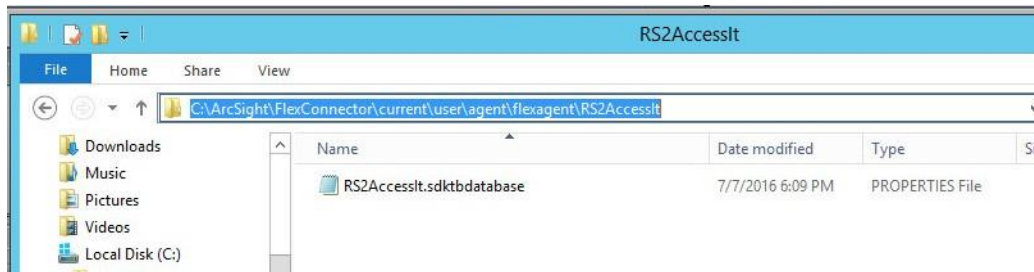
1. On the Access It! server, follow ArcSight's instructions for installing a Microsoft Windows-based Flex Connector, and specify the **Time Based Database** option [1].
2. Copy the custom FlexConnector configuration files to the appropriate locations. See Sections 6-8 of cyberlens-syslog-configuration-v2\_3.docx.
3. Start the Connector service via the **Windows Administrative Tools > Services** control panel item.

### 2.21.3.3 Custom Parser — ArcSight FlexConnector Parser

This parser will allow ArcSight to query the RS2 Access It! SQL database for door controller event data.

1. Create a file containing the text below, and copy this file to the connector installation directory.
2. Example location: **C:\ArcSight\FlexConnector\user\agent\flexagent\RS2AccessIt**

**Figure 2-90 Example Location**



```
Flex Connector for RS2 AccessIt Door Controller MS SQL Database
version.id=1.0
version.order=0
version.query=SELECT Max(EventDate) FROM Events

Pull events from which time period lastdate.query=SELECT
Max(EventDate) FROM Events

additionaldata.enabled=true

Database Query
query= SELECT Events.EventID, Events.EventDate, Events.SourceType,
Events.EventType, Events.EventDescriptionID, Events.EventLocationID,
EventDescriptions.EventDescription \
 FROM Events \
 LEFT OUTER JOIN EventDescriptions ON Events.EventDescriptionID =
EventDescriptions.EventDescriptionID \
 WHERE Events.EventDate > ? \ ORDER
 BY Events.EventDate

gets all the day's events once, and no new events
#timestamp.field=Events.EventDate

gets events every time a new event occurs timestamp.field=EventDate
uniqueid.fields=EventDescription,EventLocation,LocationLink

DB Column Mapping
event.deviceEventClassId= concatenate(EventDescription,":",EventID)
event.externalId=EventID
```

```

event.endTime=EventDate
event.name=EventDescription
#event.message=EventLocation
event.deviceCustomString1=SourceType
event.deviceCustomString2=EventType
event.deviceCustomString3=EventDescriptionID
event.deviceCustomString4=EventLocationID
#event.deviceCustomString5=LocationLink

Constants Mapping
event.deviceVendor= stringConstant (RS2) event.deviceProduct=
stringConstant (AccessIt) event.deviceCustomString1Label=
stringConstant (SourceType) event.deviceCustomString2Label=
stringConstant (EventType)
event.deviceCustomString3Label= stringConstant (EventDescriptionID)
event.deviceCustomString4Label= stringConstant (EventLocationID)
#event.deviceCustomString5Label= stringConstant (LocationLink)

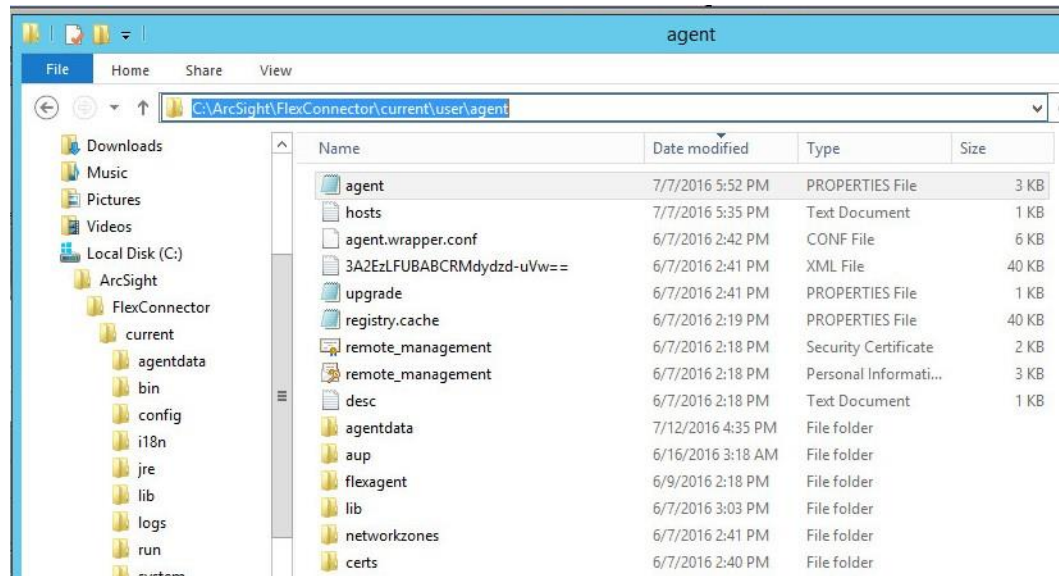
Severity Mapping event.deviceSeverity=EventDescription
severity.map.veryhigh.if.deviceSeverity=Door Forced Open,Door Held Open
severity.map.high.if.deviceSeverity=Power Loss,Comm Fail,Shutdown
severity.map.medium.if.deviceSeverity=Door Closed,Door Open,Startup
#severity.map.low.if.deviceSeverity=Low

```

#### 2.21.3.4 *ArcSight agent.properties File*

1. Modify the **agent.properties** file settings as needed based on the example below.
2. Replace the Database connection **string/url** (in bold below) to suit the environment (refer to section above).

Figure 2-91 Example String/URL



```
#ArcSight Properties File
#Thu Jul 28 17:02:44 EDT 2016
agents.maxAgents=1
agents[0].AgentSequenceNumber=0
agents[0].JDBCdriver=com.microsoft.sqlserver.jdbc.SQLServerDriver
agents[0].configfolder=RS2AccessIt
agents[0].database=Default
agents[0].dbcpcachestatements=false
agents[0].dbcpcheckouttimeout=600
agents[0].dbcpidletimeout=300
agents[0].dbcpmaxcheckout=-1
agents[0].dbcpmaxconn=5
agents[0].dbcpreap=300
agents[0].dbcprowprefetch=-1
agents[0].destination.count=1
```



```

agents[0].destination[0].agentid=3B+tGM1YBABDj2XjY9XWuyg\=\=

agents[0].destination[0].failover.count=0

agents[0].destination[0].params=<?xml version\="1.0" encoding\="UTF-
8"?>\n<ParameterValues>\n

<Parameter Name\="aupmaster"

Value\="false"/>\n

<Parameter Name\="port"

Value\="8443"/>\n

<Parameter Name\="fipsciphers"

Value\="fipsDefault"/>\n

<Parameter Name\="host"

Value\="arcsight.es-sa-bl.test"/>\n

<Parameter Name\="filterevents"

Value\="false"/>\n</ParameterValues>\n

agents[0].destination[0].type=http

agents[0].deviceconnectionalertinterval=60000

agents[0].enabled=true

agents[0].entityid=YdZKM1YBABCAAwkPuy5kNg\=\=

agents[0].fcp.version=0 agents[0].frequency=45

agents[0].id=3B+tGM1YBABDj2XjY9XWuyg\=\=

agents[0].initretrysleeptime=60000

agents[0].jdbcquerytimeout=-1

agents[0].jdbctimeout=240000

agents[0].loopingenabled=false

agents[0].password=OBFUSCATE.4.8.1\:tN7+FHjYvO5qkdFrnyHeng\=\=

agents[0].passwordchangeingcharactersets=UPPERCASE\=ABCDEFGHIJKLMNPNQR
STUVWXYZ,LOWERCASE\=abcdefghijklmnopqrstuvwxyz,NUMBER\=01234567890,SPECIAL\=+-
\!@#\$%&*()

agents[0].passwordchangingcharacterdelimiter=,

agents[0].passwordchangingenabled=false

```

```

agents[0].passwordchanginginterval=86400

agents[0].passwordchanginglength=16

agents[0].passwordchangingtemplate=UPPERCASE,NUMBER,SPECIAL,UPPERCASE|
LOWERCASE|NUMBER,UPPERCASE|LOWERCASE|NUMBER|SPECIAL

agents[0].persistenceinterval=1

agents[0].preservedstatecount=10

agents[0].preservedstateinterval=30000

agents[0].preservestate=true

agents[0].rotationtimeout=30000

agents[0].startatend=true

agents[0].type=sdktbdatabase

agents[0].unparsedevents.log.enabled=false

agents[0].url=jdbc\:sqlserver\://10.100.2.102\:1433;databasename\=AIUE
vents_20160607062103

agents[0].useconnectionpool=true

agents[0].user=OBFUSCATE.4.8.1\:LkwoJdKuWx8CDMiRZv4Qpg\=\=

remote.management.second.listener.port=10050

remote.management.ssl.organizational.unit=rE09M1YBABCAAQkPuy5kNg

```

### 2.21.3.5 Categorization File

1. Create a .csv file containing the fields below, and copy this file to the appropriate folder:  
**C:\ArcSight\<connector directory>\current\user\agent\acp\categorizer\current\rs2accessit\rs2accessit.csv**

**Figure 2-92 Categorization File Fields**

|   | A                | B                          | C                         | D                           | E                             |
|---|------------------|----------------------------|---------------------------|-----------------------------|-------------------------------|
| 1 | event.name       | set.event.categoryBehavior | set.event.categoryOutcome | set.event.categoryTechnique | set.event.categoryDeviceGroup |
| 2 | Door Forced Open | /Access                    | /Success                  | /Brute Force                | /PhysicalAccessSystem         |
| 3 | Door Held Open   | /Access                    | /Success                  | /Policy/Breach              | /PhysicalAccessSystem         |
| 4 |                  |                            |                           |                             |                               |

### 2.21.4 Additional References

1. HPE ArcSight SmartConnector User Guide <https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-SmartConnector-User-Guide-7-12-0/ta-p/1586784>

2. Syslog Guide <https://community.microfocus.com/t5/ArcSight-Connectors/SmartConnector-for-Raw-Syslog-Daemon/ta-p/1589006>
3. SmartConnector Quick Reference <https://community.microfocus.com/t5/ArcSight-User-Discussions/SmartConnector-Quick-Reference/td-p/1598927>
4. HPE ArcSight FlexConnector Developer's Guide <https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-FlexConnector-Developer-s-Guide/ta-p/1584874>
5. FlexConnector Quick Reference <https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-FlexConnector-Developer-s-Guide/ta-p/1584874>

## 3 Test Cases/Alert Configurations

This section shows filters used in ArcSight for the test cases as well as descriptions of test case alerts.

### 3.1 ArcSight Filters

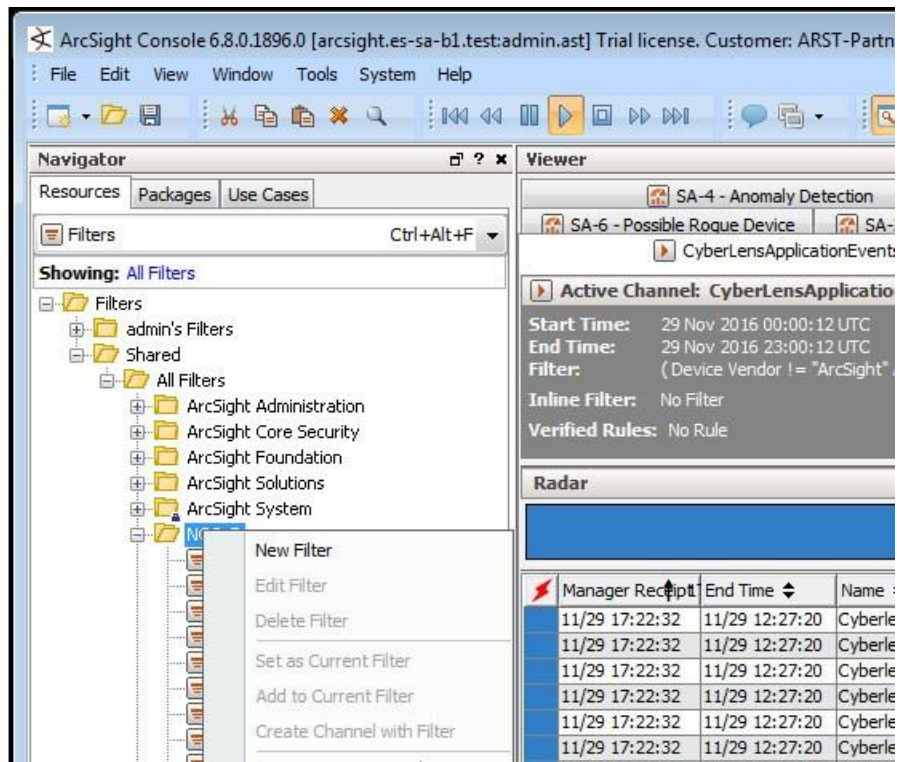
The following sections describe the creation of filters and what filters were used in the build.

#### 3.1.1 Filter Creation

ArcSight content is composed of many parts. A primary component in all content is the ArcSight filter. Use the following steps to create a filter:

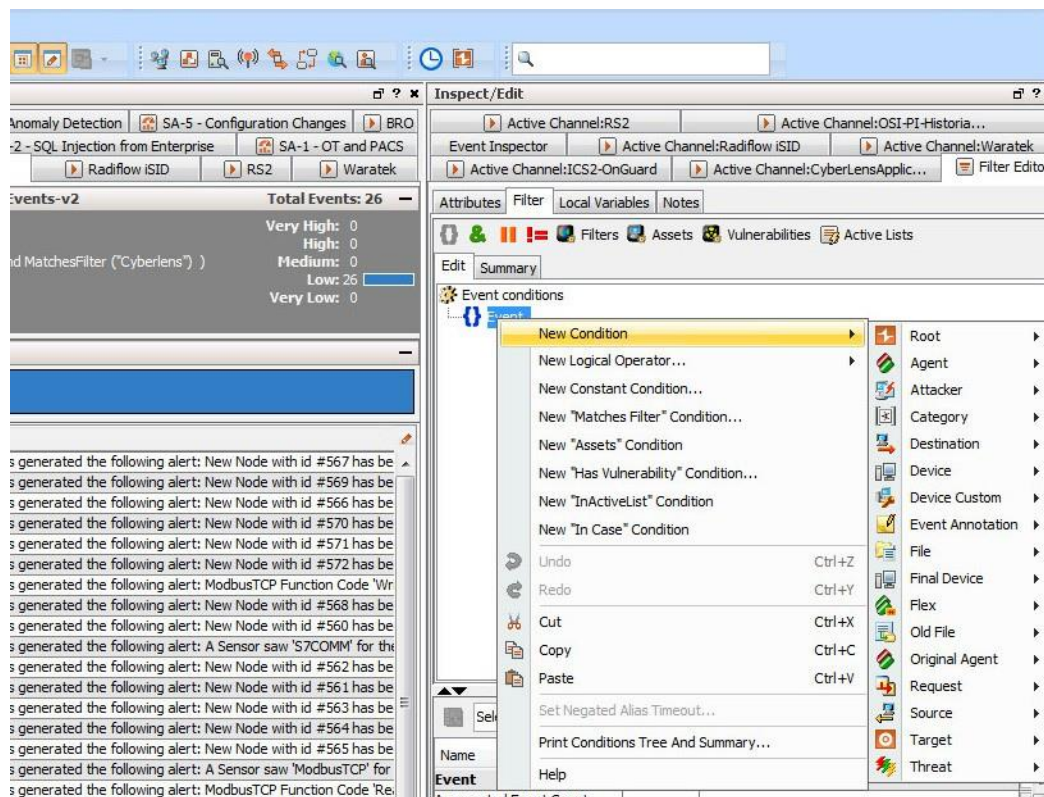
1. Go to the ArcSight navigation pane on the left.
2. Select **Filters** from the drop-down menu.
3. Right-click on a folder location.
4. Select **New Filter** from the pop-up menu.

Figure 3-1 Create New Filter



5. Right-click **Event** in the right pane of the Edit Window.
6. Select **New Condition** from the pop-up menu.

Figure 3-2 Create Conditions (Logic)



7. Next, begin constructing the conditions for which to query the ArcSight database.

*Note: It is customary to create a central folder to house ArcSight content and allow it to be shared by groups of users. Once content (such as filters) has been tested, it can then be copied or moved to the group (shared) folder. Permissions can be set on the folder to control access as needed.*

Shown below are ArcSight Filters that were created to support the Situational Awareness Test Cases.

Figure 3-3 Bro Filter



Figure 3-4 Dragos CyberLens Filter

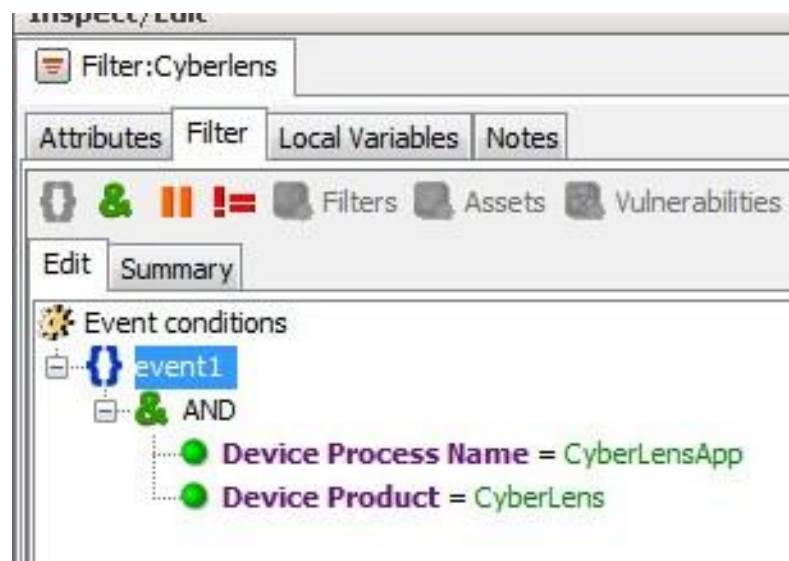


Figure 3-5 ICS2 On-Guard Filter



Figure 3-6 Windows Log Filter for OSI PI Historian

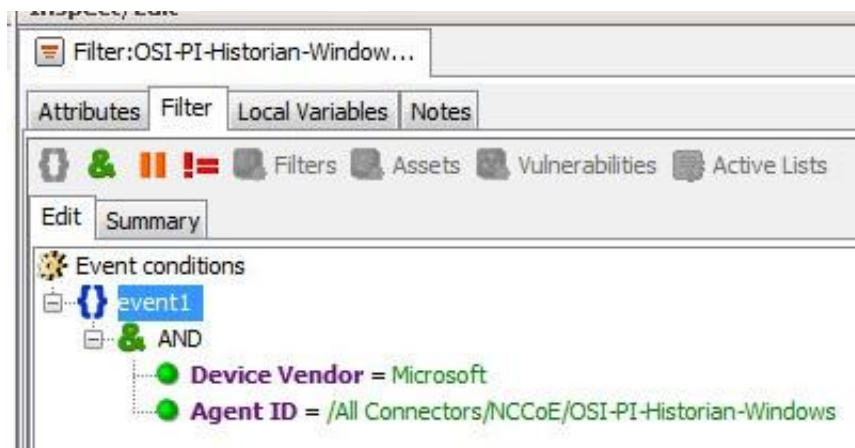


Figure 3-7 Radiflow iSID Filter



Figure 3-8 RS2 Access It! Filter

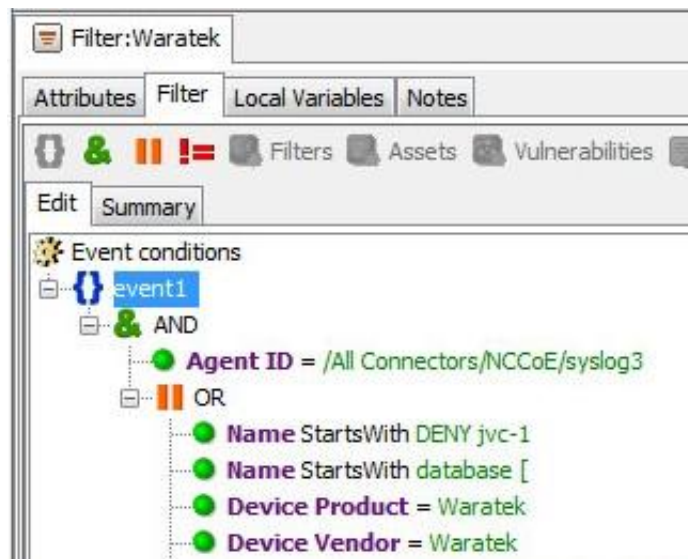




Figure 3-9 RSA Archer Filter



Figure 3-10 Waratek Filter



Below are filters that were created to match against conditions based on ...

- direction of network activity
- awareness of Security Zones (OT versus non - OT)

Figure 3-11 OT Cross-Boundary Filter

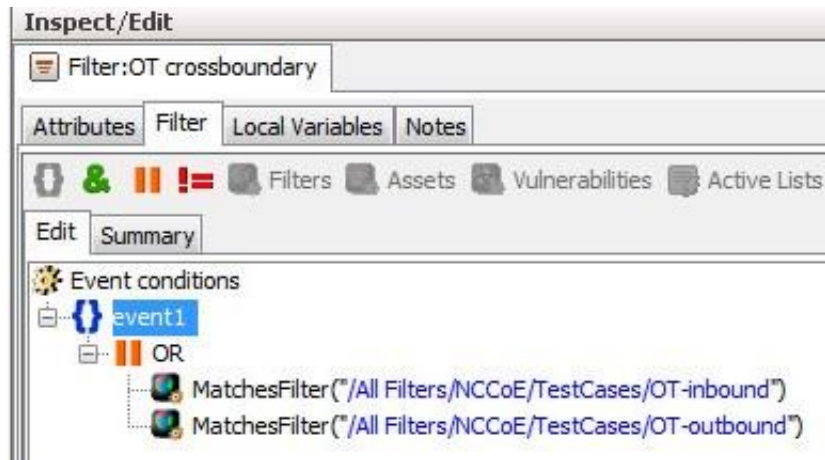


Figure 3-12 OT Inbound Filter

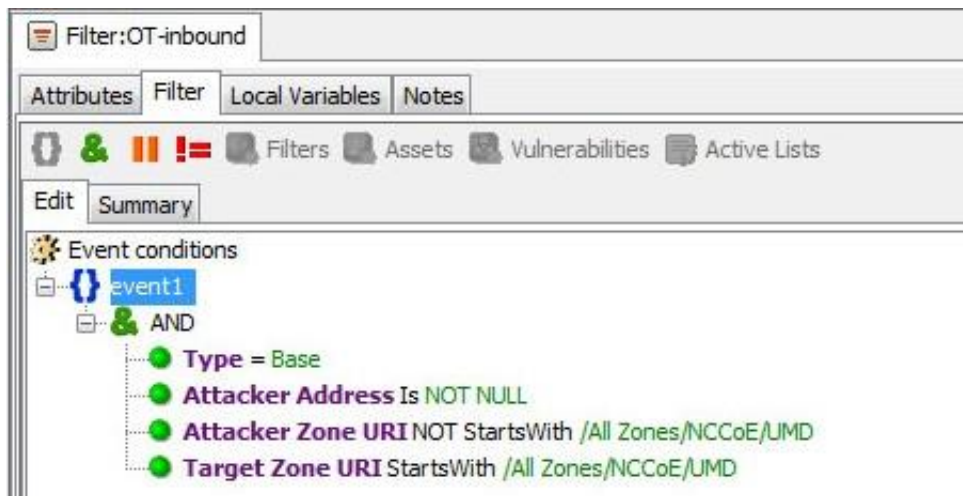
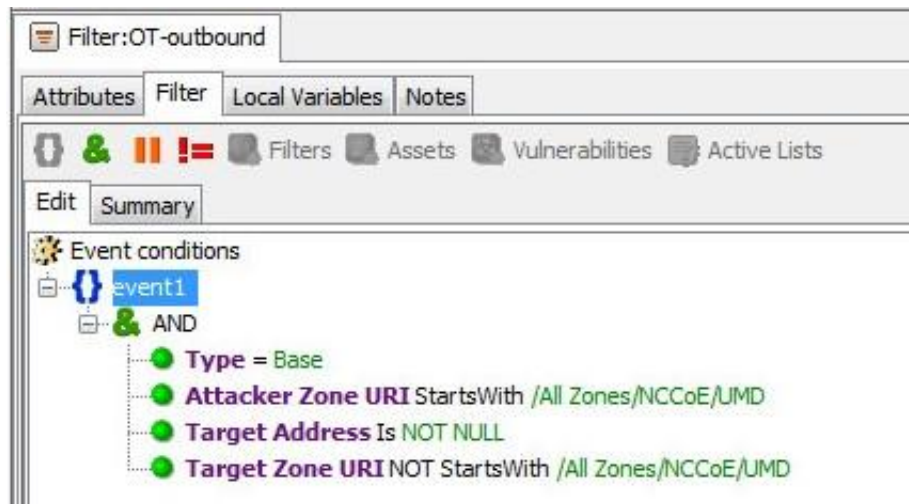


Figure 3-13 OT Outbound Filter



### 3.1.2 ArcSight Test Cases

Shown below are additional filters that were built to support the SA Test Cases. Also shown are examples of Dashboards and Data Monitors that use these filters.

Figure 3-14 SA-1 - OT-Alerts Filter



**Figure 3-15 SA-1 - OT and PACS Dashboard**

SA-1 - OT and PACS

SA-2 - SQL Injection from Enterprise

SA-3 - OT-to-IT or FailedLogins

SA-4 - Anomaly Detection

SA-5 - Configuration Changes

SA-6 - Possible Rogue Device

SA-1 - PACS Events - RS2 - last15

| End Time                 | Name             | Category Device Group | Device Vendor | Agent Zone Name            | Priority                 |
|--------------------------|------------------|-----------------------|---------------|----------------------------|--------------------------|
| 15 Dec 2016 03:18:00 UTC | Cleared Alarm    |                       | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 2 |
| 15 Dec 2016 03:17:00 UTC | Cleared Alarm    |                       | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 2 |
| 14 Dec 2016 22:57:00 UTC | Cleared Alarm    |                       | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 2 |
| 14 Dec 2016 21:29:00 UTC | Cleared Alarm    |                       | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 2 |
| 14 Dec 2016 21:28:00 UTC | Cleared Alarm    |                       | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 2 |
| 14 Dec 2016 17:30:07 UTC | Door Held Open   | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 8 |
| 14 Dec 2016 17:29:37 UTC | Door Forced Open | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 8 |
| 14 Dec 2016 17:29:36 UTC | Door Closed      | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 5 |
| 14 Dec 2016 17:29:35 UTC | Door Forced Open | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 8 |
| 14 Dec 2016 17:29:34 UTC | Door Closed      | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 5 |
| 14 Dec 2016 17:29:30 UTC | Door Forced Open | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 8 |
| 14 Dec 2016 17:29:29 UTC | Door Closed      | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 5 |
| 14 Dec 2016 17:29:28 UTC | Door Forced Open | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 8 |
| 14 Dec 2016 17:29:28 UTC | Door Closed      | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 5 |
| 13 Dec 2016 21:17:24 UTC | Door Held Open   | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | <div><div></div></div> 8 |

10/13 16:33:00 - 12/15 3:12:41

SA-1 - OT alerts - last15

| End Time | Name | Device Vendor | Device Product | Priority |
|----------|------|---------------|----------------|----------|
|----------|------|---------------|----------------|----------|

12/15 17:54:09 - 12/15 17:54:10

### Figure 3-16 SA-1 OT and PACS Active Channel

[illegible]

Figure 3-17 SA-2 - IT to OT AppAttack Filter



Figure 3-18 SA-2 OT-comms-with-non-OT Filter

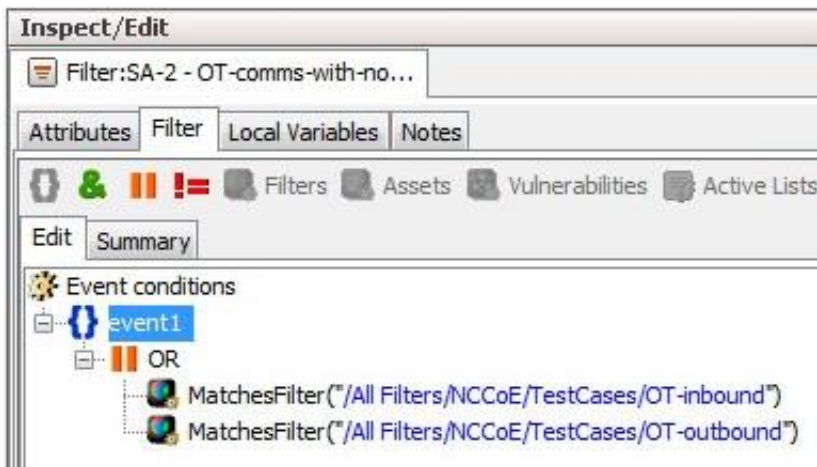


Figure 3-19 SA-2 SQL Injection Dashboard

SA-2 - IT to OT AppAttack

SA-2 - SQL Injection from Enterprise

SA-3 - OT-to-IT or FailedLogins

SA-2 - IT to OT AppAttack - last 15

| End Time                 | Name                                                                                                   | Device ... | Priority |
|--------------------------|--------------------------------------------------------------------------------------------------------|------------|----------|
| 8 Dec 2016 20:50:18 UTC  | DENY jvc-1 sql:database [mysql] - [1' OR 1=1-] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPat... | Waratek    | 2        |
| 8 Dec 2016 20:50:08 UTC  | database [mysql] - [1' OR 1=1-] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPath":"/MySQL_Get_... | Waratek    | 3        |
| 25 Oct 2016 18:00:57 UTC | DENY jvc-1 sql:database [mysql] - [1' OR 1=1-] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPat... | Waratek    | 2        |
| 25 Oct 2016 18:00:57 UTC | database [mysql] - [1' OR 1=1-] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPath":"/MySQL_Get_... | Waratek    | 3        |
| 25 Oct 2016 17:56:27 UTC | DENY jvc-1 sql:database [mysql] - [1' OR 1=1-] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPat... | waratek    | 2        |
| 25 Oct 2016 17:55:57 UTC | database [mysql] - [1' OR 1=1-] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPath":"/MySQL_Get_... | waratek    | 3        |
| 25 Oct 2016 17:46:07 UTC | DENY jvc-1 sql:database [mysql] - [1' OR 1=1-] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPat... | waratek    | 2        |
| 25 Oct 2016 17:46:07 UTC | database [mysql] - [1' OR 1=1-] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPath":"/MySQL_Get_... | waratek    | 3        |



Figure 3-20 SA-2 SQL Injection Active Channel

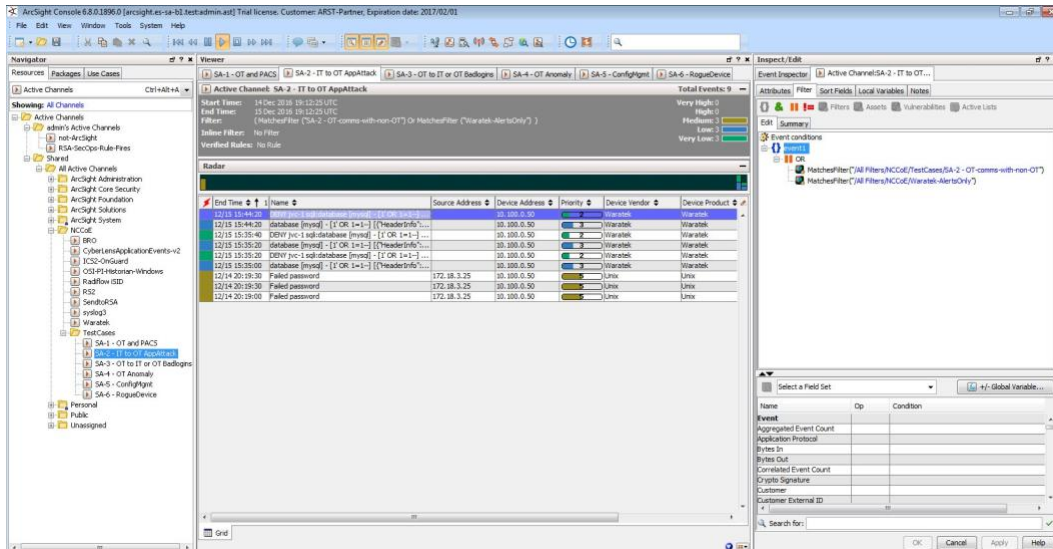


Figure 3-21 SA-3 - FailedLogins Filter



Figure 3-22 SA-3 OT to IT or OT BadLogins Filter



Figure 3-23 SA-3 OT-to-IT or FailedLogins Dashboard

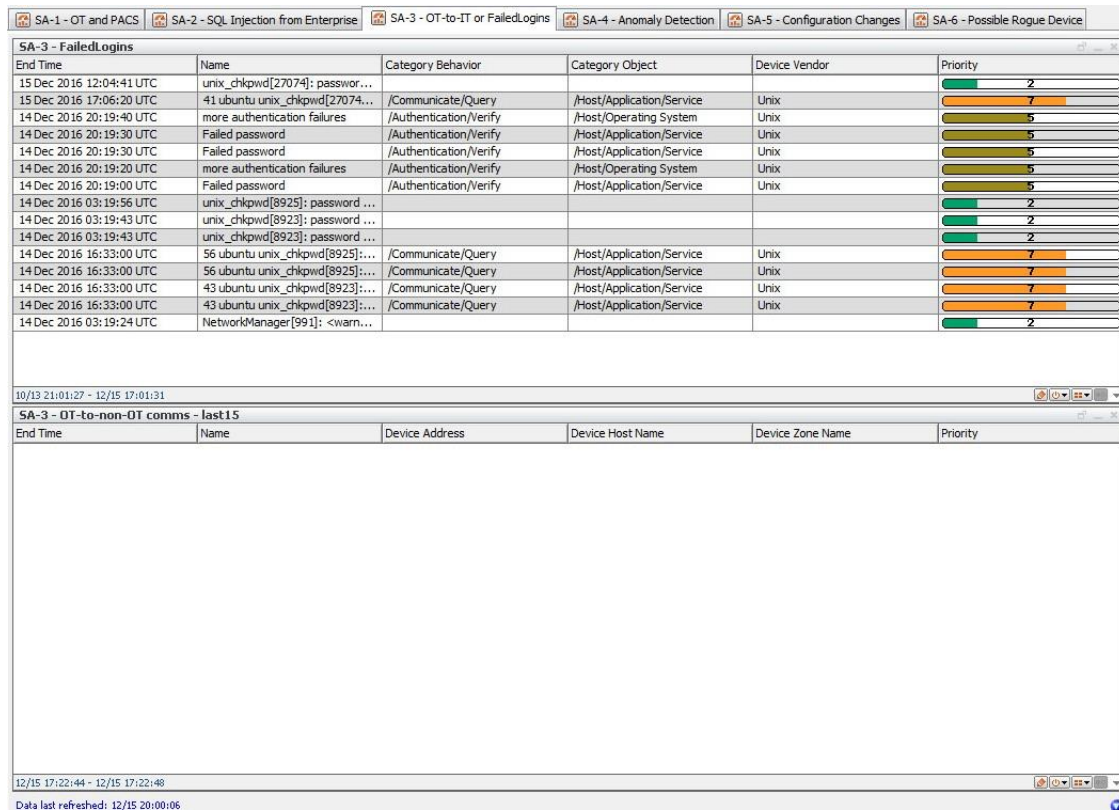




Figure 3-24 SA-3 OT-to-IT or FailedLogins Active Channel

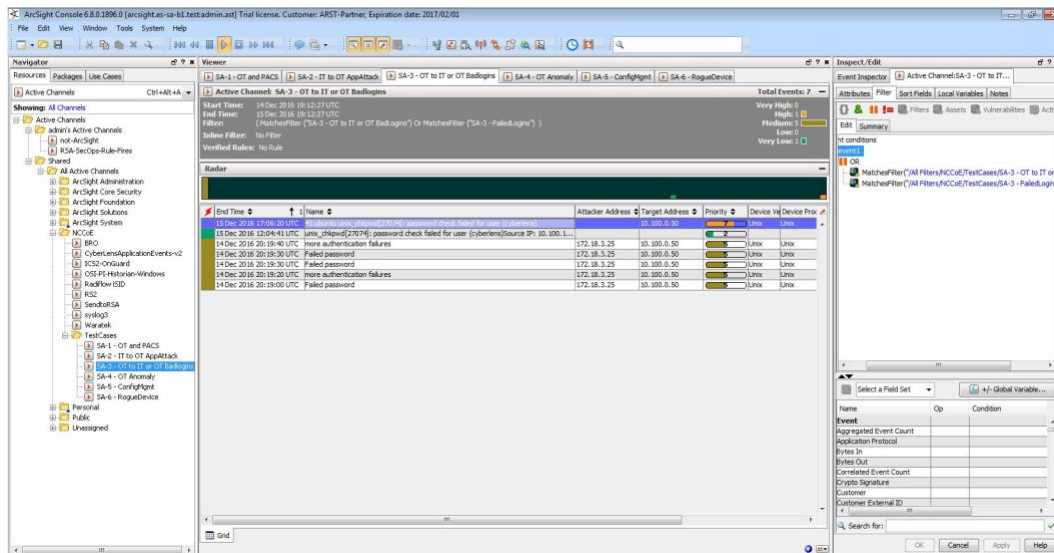


Figure 3-25 SA-4 Anomaly Detection Filter

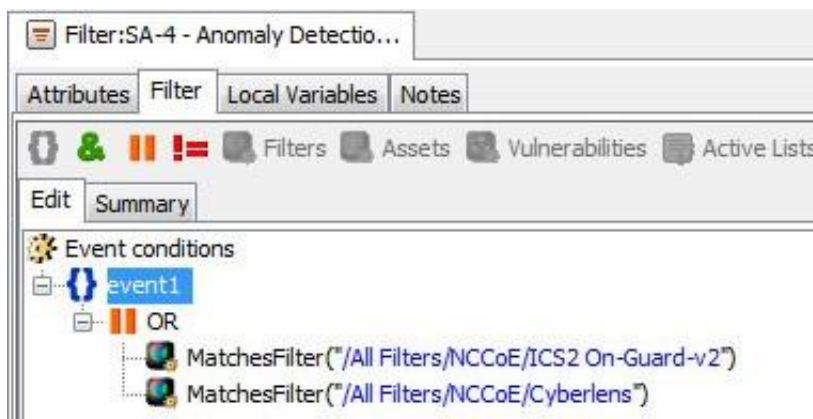


Figure 3-26 SA-4 Anomaly Detection Dashboard

| SA-4 - Anomaly Detection |                                                                                                                                     |              |            |          |  |  |  |  |  |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------|--------------|------------|----------|--|--|--|--|--|
| End Time                 | Name                                                                                                                                | Device Ve... | Device ... | Priority |  |  |  |  |  |
| 15 Dec 2016 20:00:40 UTC | 32.905463-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:59:40 UTC | 30.998907-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:58:40 UTC | 30.470453-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:57:50 UTC | 30.191992-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:56:50 UTC | 29.310588-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:55:40 UTC | 28.823047-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:54:30 UTC | 27.877579-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:53:30 UTC | 27.245086-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:52:30 UTC | 26.570606-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:51:30 UTC | 25.714121-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:50:30 UTC | 25.158658-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:49:30 UTC | 23.287124-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:48:30 UTC | 23.322682-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:47:30 UTC | 22.786209-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:46:30 UTC | 22.088000-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:45:30 UTC | 20.269199-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:44:30 UTC | 20.438768-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:43:30 UTC | 19.521282-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:42:30 UTC | 18.961810-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:41:20 UTC | 17.971327-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:40:20 UTC | 17.430855-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:39:20 UTC | 16.338352-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:38:20 UTC | 15.780880-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |
| 15 Dec 2016 19:37:20 UTC | 15.069412-05:00 WIN-S3PUD2U939R Ics2 OnGuard Alarm [localhost]243[ICS2.NUMBER OF TAGS WITH NEW DATA]No new data in DB for too lo... | ICS2         | OnGuard    | 3        |  |  |  |  |  |

Figure 3-27 Anomaly Detection Active Channel

The screenshot displays the ArcSight Console interface. The top navigation bar shows several tabs: SA-1 - OT and PACS, SA-2 - SQL Injection from Enterprise, SA-3 - OT-to-IT or Failed Logins, SA-4 - Anomaly Detection (selected), SA-5 - Configuration Changes, and SA-6 - Possible Rogue Device. The main window is divided into three sections:

- Navigator:** Located on the left, it shows a tree view of active channels. The 'Active Channels' section is expanded, showing 'SA-4 - OT Anomaly' as the selected channel.
- Event List:** The central pane displays a list of events. The 'End Time' column is sorted in descending order. The events are generated by 'CyberLens' and include various alerts such as 'A Sensor saw Multicast DNS (mDNS) for the first time', 'A Sensor saw Network Time Protocol (NTP) used for', and 'A Sensor saw Unhandled Protocol on port 155 for R...'. Each event entry includes a timestamp, a name, a device address, a priority, and a device vendor.
- Event Inspector:** Located on the right, it provides a detailed view of the selected event. It shows the event's attributes, filters, and conditions. The 'Event conditions' section is visible, showing a rule named 'MatchedFilter("All Filters:ACCE/TestCases/SA-4 - Anomaly Detection-v2")'.

Figure 3-28 SA-5 ConfigMgmt Filter

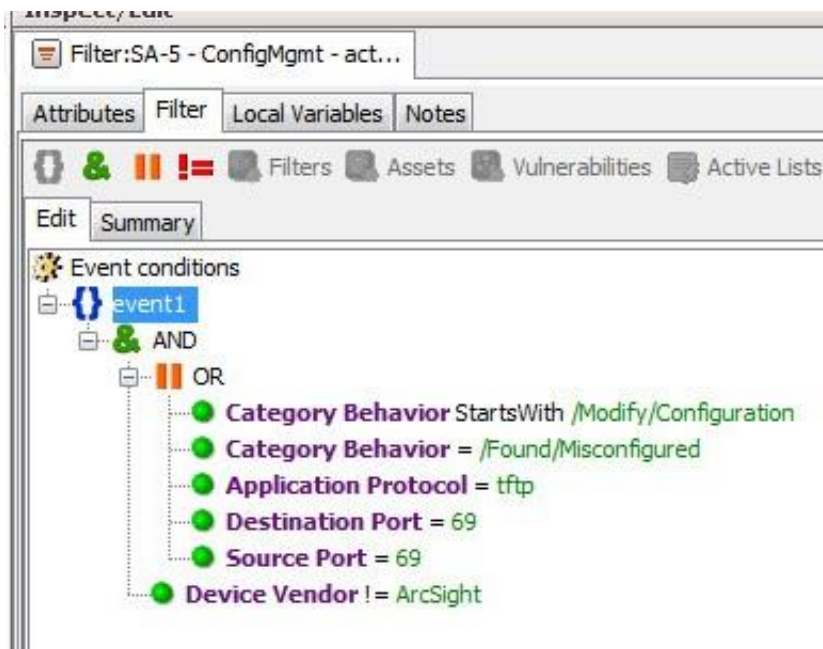


Figure 3-29 SA-5 ConfigMgmt Filter



Figure 3-30 SA-5 Master Filter

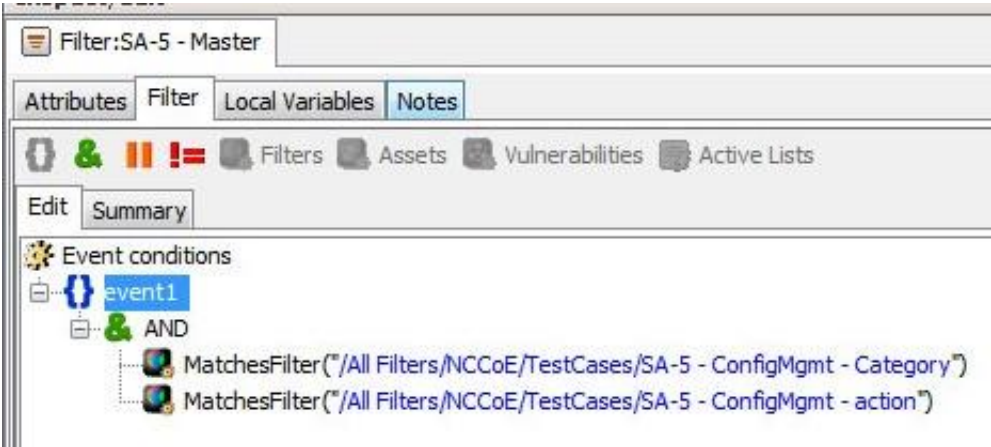


Figure 3-31 SA-5 Configuration Changes Dashboard

SA-5 - Configuration Changes

SA-6 - Possible Rogue Device

SA-5 - Configuration Changes - last15

| End Time | Name | Category Behavior | Category Device Group | Category Object | Category Outcome |
|----------|------|-------------------|-----------------------|-----------------|------------------|
|          |      |                   |                       |                 |                  |

Figure 3-32 SA-5 Configuration Changes Active Channel

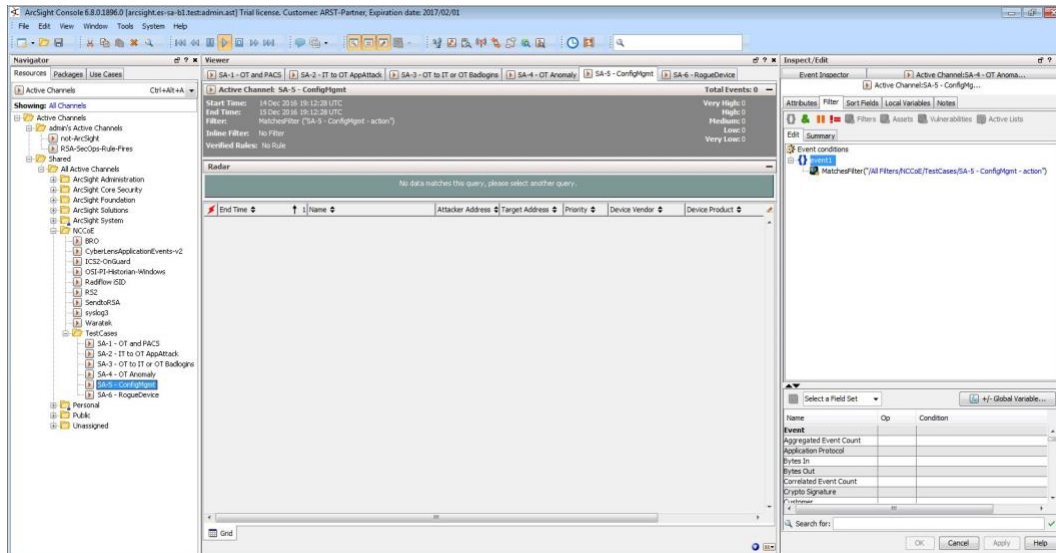




Figure 3-33 SA-6 RogueDevice Filter

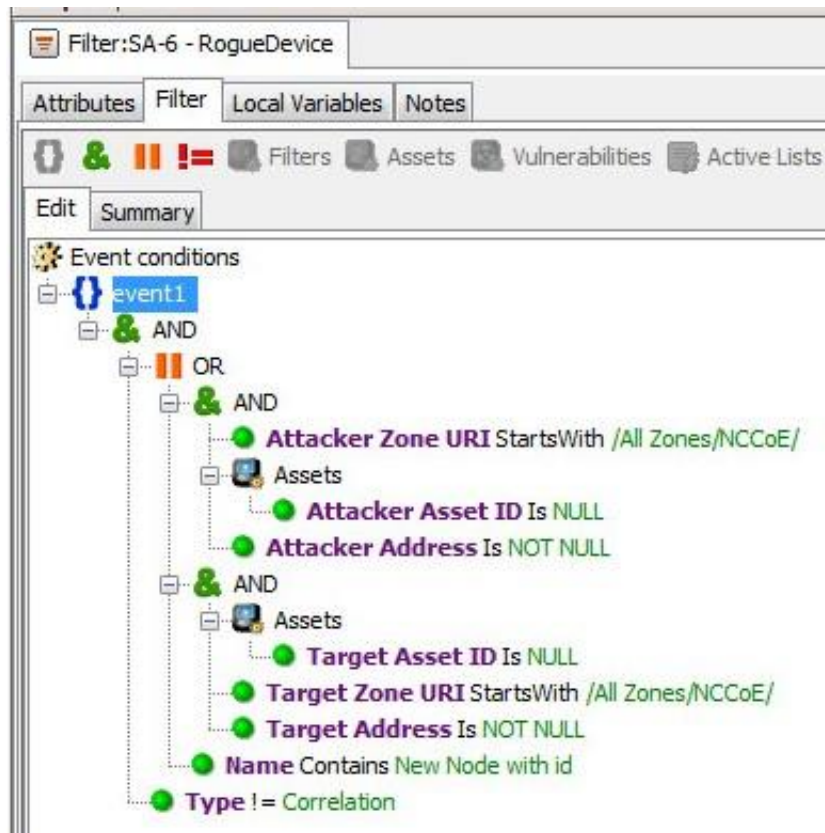


Figure 3-34 SA-6 Rogue Device Dashboard

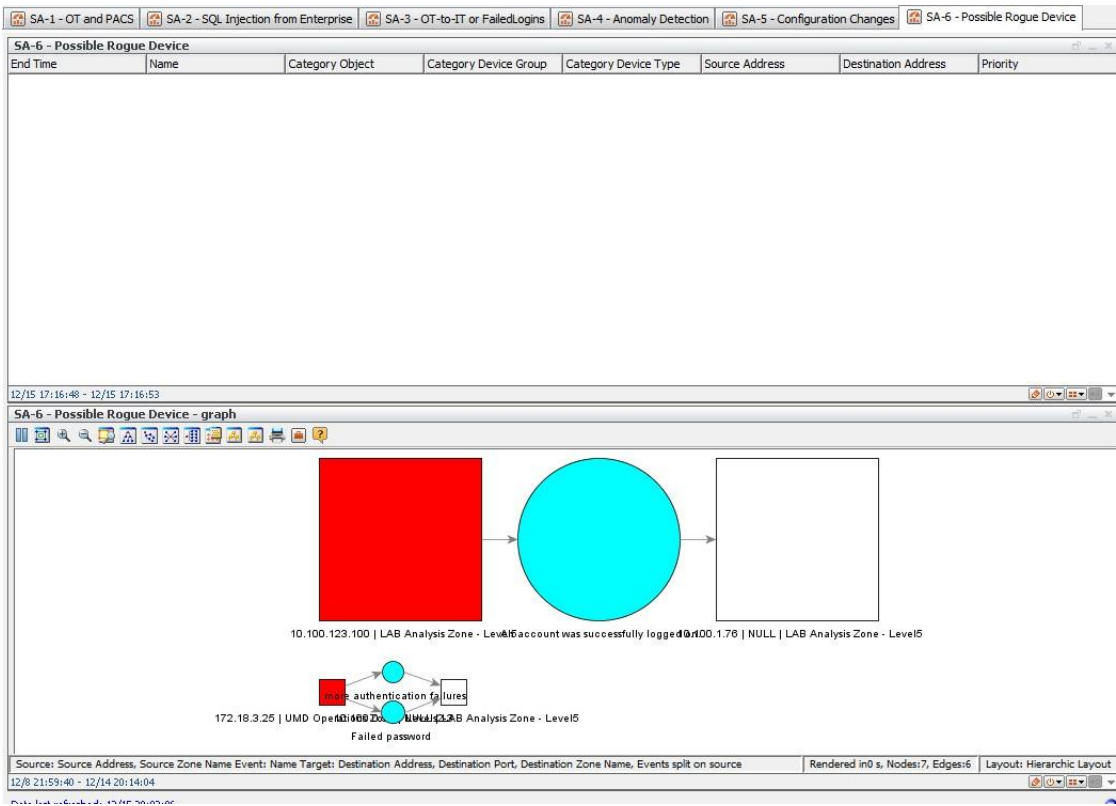
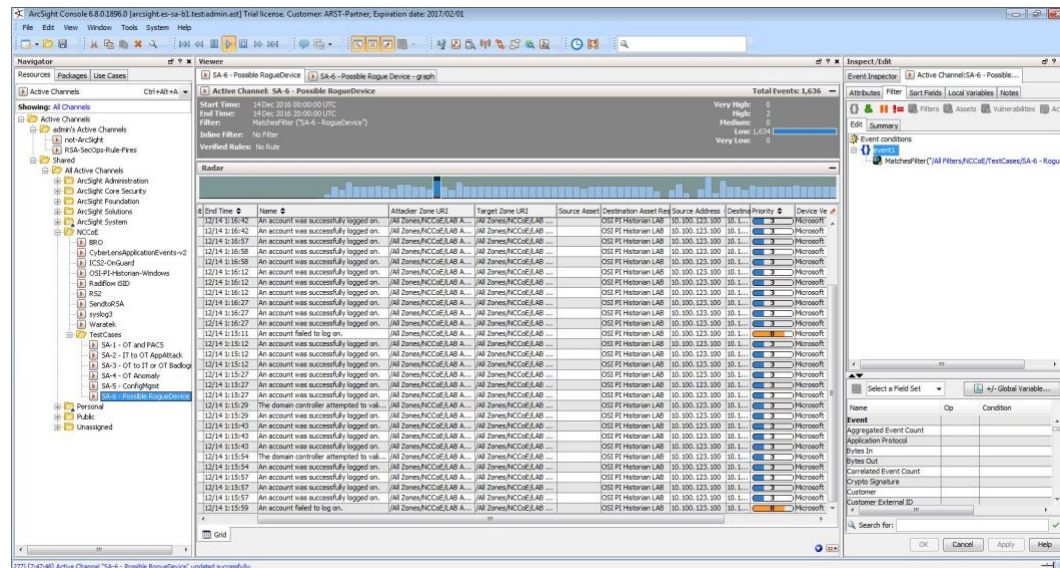


Figure 3-35 SA-6 Rogue Device Active Channel



## 3.2 Test Cases

Below are descriptions of test cases as matched to Section 3.6, Situational Awareness Test Cases, of NIST SP 1800-7B.

### 3.2.1 SA-1 Event Correlation for OT and PACS

This test case focuses on the possibility of correlated events occurring that involve OT and PACS and that might indicate compromised access.

#### 3.2.1.1 Events

1. Technician accesses substation/control station.
2. OT device goes down.

#### 3.2.1.2 Desired Outcome

Alert of anomalous condition and subsequent correlation to PACS to see who accessed facility

#### 3.2.1.3 ArcSight Content

1. OT network Zones
2. Filter for OT network Zones.



3. filters for OT/IT inbound, outbound, cross-boundary communications
4. filter for RS2 Door Controller events
5. filter for CyberLens or iSID events
6. Active List for RS2 Door Controller events with time threshold
7. rule to add RS2 Door Controller filter events to Active List
8. Data Monitor and Dashboard to display results of the above

### 3.2.2 SA-2 Event Correlation for OT and IT

The enterprise (IT) Java application communication with an OT device (historian) is used as a vector for SQL injection (SQLi), which also includes data exfiltration attempts.

#### 3.2.2.1 *Events*

Detection of SQLi attack on IT device interconnected with OT device

#### 3.2.2.2 *Desired Outcome*

Alert sent to SIEM on multiple SQLi attempts

#### 3.2.2.3 *ArcSight Content*

1. filter for Waratek events (intended to monitor for SQLi against the OSIsoft PI Historian)
2. filter to combine Waratek and OT/IT inbound communications filters
3. Data Monitor and Dashboard to display results of the above

### 3.2.3 SA-3 Event Correlation for OT and IT/PACS and OT

Unauthorized access attempts are detected, and alerts are triggered based on connection requests from a device on the SCADA network destined for an IP that is outside the SCADA IP range. This test case focuses on the possibility of a malicious actor attempting to gain access to an OT device via the enterprise (IT) network. This test case is also relevant in a PACS-OT scenario, in which someone has physical access to an OT device but lacks the necessary access to perform changes to the device, and alerts are sent based on numerous failed login attempts.

#### 3.2.3.1 *Events*

Inbound/outbound connection attempts from devices outside authorized and known inventory

### 3.2.3.2 *Desired Outcome*

Alert to SIEM showing IP of unidentified host attempting to connect, or of identified host attempting to connect to unidentified host

### 3.2.3.3 *ArcSight Content*

1. Use OT network Zones (as defined in SA-1 content).
2. Use filter for OT network Zones (as defined in SA-1 content).
3. Filter for events from OT network Zone to/from a different Zone
4. Filters for authorization, authentication failures
5. Filter for authorization, authentication failures, or outbound events
6. Data Monitor and Dashboard to display results of the above

## 3.2.4 SA-4 Data Infiltration Attempts

Examine the behavior of systems, and configure the SIEM to alert on behavior that is outside the normal baseline. Alerts can be created emanating from OT, IT, and PACS. This test case seeks alerting based on behavioral anomalies rather than recognition of IP addresses, and guards against anomalous or malicious inputs.

### 3.2.4.1 *Events*

Anomalous behavior falling outside defined baseline

### 3.2.4.2 *Desired Outcome*

Alert sent to SIEM on any event falling outside of what is considered normal activity based on historical data

### 3.2.4.3 *ArcSight Content*

1. Use OT network Zones.
2. Use Filter for OT network Zones.
3. Filter for ICS2 OnGuard events or events with a Category of Traffic Anomaly (e.g., as defined in Dragos Security CyberLens ArcSight FlexConnector/Categorizer files).
4. Data Monitor and Dashboard to display results of the above

### 3.2.5 SA-5 Configuration Management

An alert will be created to notify the SIEM of unauthorized (inadvertent or malicious) uploading of an ICS network device configuration. The detection method will be primarily based on inherent device capability (i.e., log files).

#### 3.2.5.1 *Events*

Configuration change on Tofino FW, Cisco 2950

#### 3.2.5.2 *Desired Outcome*

Alert will be created to notify SIEM that this has occurred.

#### 3.2.5.3 *ArcSight Content*

1. Filter for any of the following:
  - a. ArcSight Category events:
    - i. /Modify/Configuration
    - ii. /Found/Misconfigured
    - iii. tftp protocol
    - iv. tftp port
2. Filter for following ArcSight Category Device Groups:
  - a. /Firewall
  - b. /Network Equipment
  - c. /VPN
  - d. /IDS
  - e. or Category Object:
    - i. /Network
3. Data Monitor and Dashboard to display results of the above

### 3.2.6 SA-6 Rogue Device Detection

Alerts are triggered by the introduction of any device onto the ICS network that has not been registered with the asset management capability in the build.

#### *3.2.6.1 Events*

Unidentified device appears on ICS network.

#### *3.2.6.2 Desired Outcome*

Alert will be created to notify the SIEM that this has occurred.

#### *3.2.6.3 ArcSight Content*

1. Specific Asset definitions for all known ICS devices (grouped by OT Zones)
2. Filter to detect presence of any “non-ICS” devices (not in Asset lists).
3. Filter for CyberLens events alerting on “new” hosts.
4. Data Monitor and Dashboard to display results of the above

## Appendix A List of Acronyms

|              |                                                 |
|--------------|-------------------------------------------------|
| <b>ASP</b>   | Active Server Pages                             |
| <b>CA</b>    | Certificate Authority                           |
| <b>CRADA</b> | Cooperative Research and Development Agreement  |
| <b>E1</b>    | Siemens RUGGEDCOM RX1400                        |
| <b>E4</b>    | OSIsoft Pi Historian                            |
| <b>E5</b>    | OnGuard                                         |
| <b>E6</b>    | ConsoleWorks                                    |
| <b>E7</b>    | RS2 Access IT!                                  |
| <b>E8</b>    | CyberLens Server                                |
| <b>E9</b>    | Siemens RUGGEDCOM CROSSBOW                      |
| <b>E10</b>   | Waratek Runtime Protection                      |
| <b>E12</b>   | Hewlett Packard Enterprise ArcSight             |
| <b>E13</b>   | RSA SecOps                                      |
| <b>EACMS</b> | Electronic Access Control and Monitoring System |
| <b>ESM</b>   | Enterprise Security Manager                     |
| <b>FQDN</b>  | Fully Qualified Domain Name                     |
| <b>FTP</b>   | File Transfer Protocol                          |
| <b>HDD</b>   | Hard Disk Drive                                 |
| <b>HPE</b>   | Hewlett Packard Enterprise                      |
| <b>ICS</b>   | Industrial Control System(s)                    |
| <b>ICU</b>   | Interface Configuration Utility                 |
| <b>IDS</b>   | Intrusion Detection System                      |
| <b>IIS</b>   | Internet Information Services                   |
| <b>IP</b>    | Internet Protocol                               |
| <b>IPSec</b> | IP Security                                     |

|                 |                                                                                    |
|-----------------|------------------------------------------------------------------------------------|
| <b>ISAPI</b>    | Internet Server Application Programming Interface                                  |
| <b>IT</b>       | Information Technology                                                             |
| <b>LDAP</b>     | Lightweight Directory Access Protocol                                              |
| <b>LTS</b>      | Long-Term Support                                                                  |
| <b>NAT</b>      | Network Address Translator                                                         |
| <b>NCCoE</b>    | The National Cybersecurity Center of Excellence                                    |
| <b>NERC CIP</b> | North American Electric Reliability Corporation Critical Infrastructure Protection |
| <b>NIC</b>      | Network Interface Controller                                                       |
| <b>NIST</b>     | National Institute of Standards and Technology                                     |
| <b>O1</b>       | Siemens RUGGEDCOM RX1501                                                           |
| <b>O2</b>       | Waterfall Security Solutions, Ltd. Unidirectional Security Gateway                 |
| <b>O3</b>       | Schneider Electric Tofino Firewall                                                 |
| <b>O4</b>       | RS2 Door Controller                                                                |
| <b>O5</b>       | TDi Technologies ConsoleWorks                                                      |
| <b>O8</b>       | OSIsoft Pi Historian                                                               |
| <b>O9</b>       | TDi Technologies ConsoleWorks                                                      |
| <b>O10</b>      | CyberLens Sensor                                                                   |
| <b>O11</b>      | Radiflow iSID                                                                      |
| <b>O13</b>      | OSIsoft Citect Interface software                                                  |
| <b>O14</b>      | Radiflow 3180 Firewall                                                             |
| <b>O15</b>      | Cisco 2950 Network Switch                                                          |
| <b>O16</b>      | IXIA Full Duplex Taps                                                              |
| <b>O17</b>      | Waterfall Secure Bypass Switch                                                     |
| <b>O18</b>      | Schneider Electric Tofino Firewall                                                 |
| <b>O20</b>      | Schneider Electric Tofino Firewall                                                 |
| <b>ODBC</b>     | Open Database Connectivity                                                         |

|              |                                           |
|--------------|-------------------------------------------|
| <b>OPC</b>   | Open Platform Communication               |
| <b>OT</b>    | Operational Technology                    |
| <b>OVA</b>   | Open Virtual Appliance                    |
| <b>PAC</b>   | Physical Access Control                   |
| <b>PACS</b>  | Physical Access Control Systems           |
| <b>PDP</b>   | Policy Decision Point                     |
| <b>PEP</b>   | Policy Enforcement Point                  |
| <b>RDP</b>   | Remote Desktop Protocol                   |
| <b>RHEL</b>  | Red Hat Enterprise Linux                  |
| <b>RMF</b>   | Risk Management Framework                 |
| <b>SA</b>    | Situational Awareness                     |
| <b>SAC</b>   | Station Access Controller                 |
| <b>SCADA</b> | Supervisory Control and Data Acquisition  |
| <b>SCP</b>   | Secure Copy Protocol                      |
| <b>SIEM</b>  | Security Information and Event Management |
| <b>SP</b>    | Special Publication                       |
| <b>SQL</b>   | Structured Query Language                 |
| <b>SQLi</b>  | Structured Query Language Injection       |
| <b>U1</b>    | Citect SCADA System                       |
| <b>UDP</b>   | User Datagram Protocol                    |
| <b>UMD</b>   | University of Maryland                    |
| <b>vCPU</b>  | Virtual Central Processing Unit           |
| <b>VNC</b>   | Virtual Network Computing                 |
| <b>VPN</b>   | Virtual Private Network                   |
| <b>WAN</b>   | Wide Area Network                         |

## Appendix B    References

- [1]        Micro Focus. *HPE ArcSight SmartConnector User Guide – Hewlett Packard Software Community*. Available: <https://www.protect724.hpe.com/docs/DOC-2279>.