

NIST Special Publication 1800-7C

Situational Awareness For Electric Utilities

Volume C:
How-To Guides

Jim McCarthy

National Cybersecurity Center of Excellence
Information Technology Laboratory

Otis Alexander

Sallie Edwards

Don Faatz

Chris Peloquin

Susan Symington

Andre Thibault

John Wiltberger

Karen Viani

The MITRE Corporation
McLean, VA

February 2017

DRAFT

This publication is available free of charge from:

https://nccoe.nist.gov/projects/use_cases/situational_awareness



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, 149 pages (February 2017)
CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: energy_nccoe@nist.gov.

Public comment period: February 16, 2017 through April 17, 2017

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
Mailstop 2002

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 or broad, cross-sector technology challenges. Working with 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 Cyber Security 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://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 (comprised 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 (OT), including industrial control systems, 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) 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 industrial control systems, IT resources, 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 industrial control systems (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 remediate 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 to 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 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 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

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

ACKNOWLEDGMENTS

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

Name	Organization
Robert Lee	Dragos
Justin Cavinee	Dragos
Jon Lavender	Dragos
Gregg Garbesi	Engie
Steve Roberts	HPE
Bruce Oehler	HPE
Gil Kroyzer	ICS2
Gregory Ravikovich	ICS2
Robert Bell	ICS2
Fred Hintermeister	NERC
Paul J. Geraci	OSIsoft
Mark McCoy	OSIsoft
Stephen J. Sarnecki	OSIsoft
Paul Strasser	PPC
Matt McDonald	PPC
Steve Sage	PPC
T.J. Roe	Radiflow
Ayal Vogel	Radiflow
Dario Lobizzo	Radiflow
Dave Barnard	RS2
Ben Smith	RSA, a Dell Technologies business
Tarik Williams	RSA, a Dell Technologies business
David Perodin	RSA, a Dell Technologies business
George Wrenn	Schneider Electric
Michael Pyle	Schneider Electric
AJ Nicolosi	Siemens
Jeff Foley	Siemens
Bill Johnson	TDi

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 Griffie	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 vendors who participated in this build submitted their capabilities in response to a notice in the Federal Register. Companies with relevant products 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	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

Technology Partner/Collaborator	Build Involvement
TDi Technologies	ConsoleWorks
Waratek	Waratek Runtime Application Protection
Waterfall Security Solutions	Unidirectional Security Gateway, Secure Bypass

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; PPC (Project Performance Company), for their dedication in assisting the NCCoE with the very challenging and complex integration in this build; and the NCCoE EPC (Energy Provider Community), for their patience, support, and guidance throughout the lifecycle of this project.

Contents

1	Introduction	1
1.1	Practice Guide Structure	2
1.2	Build Overview	3
1.3	Typographical Conventions	3
1.4	Logical Architecture Summary	4
1.5	Wiring Diagrams	5
2	Product Installation Guides	7
2.1	Cisco 2950 (O15).....	8
2.1.1	Cisco 2950 (O15) Installation Guide	8
2.2	Dragos Security CyberLens (E8, O10)	11
2.2.1	Dragos Security CyberLens Server (E8) Environment Setup	11
2.2.2	Dragos Security CyberLens Server (E8) Installation and Configuration Guide	12
2.2.3	Dragos Security CyberLens Sensor (O10) Installation Guide.....	13
2.3	HPE ArcSight (E12)	13
2.3.1	HPE ArcSight (E12) Installation Guide	14
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)	18
2.4.1	Environment Setup	18
2.4.2	Install Vendor Software.....	19
2.4.3	Install OnGuard System.....	20
2.5	IXIA Full-Duplex Tap (O16).....	22
2.6	OSIsoft Pi Historian (E4, O8).....	23
2.6.1	OSIsoft Pi Historian (E4) Installation Guide	23
2.6.2	OSIsoft Pi Historian (O8) Installation Guide	28
2.7	OSIsoft Citect Interface (O13).....	29
2.7.1	OSIsoft Citect Interface (O13) Installation Guide	29
2.7.2	Configuration	30
2.8	RS2 Technologies Access It! Universal.NET(E7)	34
2.8.1	Environment Setup	34
2.8.2	Post-installation and configuration	35
2.9	RS2 Technologies Door Controller (O4).....	36
2.9.1	Hardware Installation	36
2.9.2	Connecting Hardware to Access It! Universal.NET	39
2.10	Radiflow 3180 (O14)	40
2.10.1	Radiflow 3180 (O14) Installation Guide	40
2.11	Radiflow iSID (O11)	41

2.11.1 Environment Setup	41
2.11.2 Product Installation	41
2.12 RSA Archer Security Operations Management (E13)	42
2.12.1 System Requirements	42
2.12.2 Pre-Installation.....	43
2.12.3 Installation.....	46
2.12.4 Post-Installation	47
2.12.5 Configuration of ArcSight ESM to RSA Archer Security Operations Management	50
2.12.6 Additional ArcSight Integration Configuration	51
2.12.7 Sample Use Case Demonstration	52
2.13 Schneider Electric Tofino Firewall (O3, O18, O20).....	55
2.13.1 Schneider Electric Tofino Firewall (O3) Installation Guide.....	55
2.13.2 Schneider Electric Tofino Firewall (O18) Installation Guide.....	57
2.13.3 Schneider Electric Tofino Firewall (O20) Installation Guide.....	63
2.14 Siemens RUGGEDCOM CROSSBOW (E9).....	63
2.14.1 Environment Setup	63
2.14.2 Installation Procedure	63
2.15 Siemens RUGGEDCOM RX1400 (E1).....	82
2.15.1 Environment Setup	82
2.15.2 Installation Procedure	82
2.16 Siemens RUGGEDCOM RX1501 (O1).....	85
2.16.1 Siemens RUGGEDCOM RX1501 (O1) Installation Guide.....	85
2.17 TDi Technologies ConsoleWorks (E6, O5, O9)	85
2.17.1 System Environment.....	85
2.17.2 Installation.....	86
2.17.3 Usage	87
2.17.4 TDi Technologies ConsoleWorks (E6) Installation Guide	89
2.17.5 TDi Technologies ConsoleWorks (O9) Installation Guide.....	95
2.18 Waterfall Technologies Unidirectional Security Gateway (O2)	96
2.18.1 Waterfall Technologies Unidirectional Security Gateway (O2) Installation Guide	96
2.19 Waterfall Secure Bypass (O17)	100
2.19.1 Waterfall Secure Bypass (O17) Installation Guide	100
2.20 Waratek Runtime Application Protection (E10)	101
2.20.1 System Environment.....	101
2.20.2 Waratek Runtime Application Protection (E10) for Java Installation	101
2.20.3 Usage	102
2.21 ArcSight Connector Guides	102
2.21.1 Dragos CyberLens Connector	102
2.21.2 ICS2 OnGuard	107
2.21.3 RS2 Access It! Universal.NET	112
2.21.4 Additional References.....	117
3 Test Cases/Alert Configurations	118

3.1 ArcSight Filters.....	119
3.1.1 Filter Creation	119
3.1.2 ArcSight Test Cases	125
3.2 Test Cases.....	134
3.2.1 SA-1 Event Correlation for OT and PACS	135
3.2.2 SA-2 Event Correlation for OT and IT.....	135
3.2.3 SA-3 Event Correlation for OT and IT / PACS and OT.....	136
3.2.4 SA-4 Data Infiltration Attempts	136
3.2.5 SA-5 Configuration Management	137
3.2.6 SA-6 Rogue Device Detection	138

List of Tables

Table 1.1 Typographical Conventions	3
Table 2.1 Centos Partitioning Scheme for ArcSight ESM Manager Server.....	14
Table 2.2 RSA Archer Configuration Settings	43
Table 2.3 IIS Components and .NET Framework	44

1 Introduction

2	1.1 Practice Guide Structure	2
3	1.2 Build Overview	3
4	1.3 Typographical Conventions	3
5	1.4 Logical Architecture Summary	4
6	1.5 Wiring Diagrams.....	5

7 The following guides show IT professionals and security engineers how we implemented this
8 example solution. We cover all of the products employed in this reference design. We do not
9 recreate the product manufacturers' documentation, which is presumed to be widely available.
10 Rather, these guides show how we incorporated the products together in our environment.

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

13 1.1 Practice Guide Structure

14 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and
15 provides users with the information they need to replicate this approach to mobile device
16 security. The reference design is modular and can be deployed in whole or in parts.

17 Depending on their roles in an organization, different people will use this guide in different
18 ways.

19 This guide contains three volumes:

- 20 ■ NIST SP 1800-7a: Executive Summary
- 21 ■ NIST SP 1800-7b: Approach, Architecture, and Security Characteristics--what we built and
22 why
- 23 ■ NIST SP 1800-7c: How-To Guides--instructions for building the example solution (you are
24 here)

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

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

- 28 ■ challenges enterprises face in maintaining cross-silo situational awareness
- 29 ■ example solution built at the NCCoE
- 30 ■ benefits of adopting the example solution

31 **Technology or security program managers** who are concerned with how to identify,
32 understand, assess, and mitigate risk will be interested in the Approach, Architecture, and
33 Security Characteristics part of the guide, NIST SP 1800-7b, which describes what we did and
34 why. The following sections will be of particular interest:

- 35 ■ Section 3.4.1, Assessing Risk Posture, provides a detailed description of the risk analysis we
36 performed.
- 37 ■ Section 3.4.2, Security Characteristics and Controls Mapping, maps the security
38 characteristics

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

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

49 This guide assumes that IT professionals have experience implementing security products
50 within the enterprise. While we have used a suite of commercial products to address this
51 challenge, this guide does not endorse these particular products. Your organization can adopt
52 this solution or one that adheres to these guidelines in whole, or you can use this guide as a
53 starting point for tailoring and implementing parts of a solution including PACS OT, IT systems,
54 and business processes. Your organization's security experts should identify the products that
55 will best integrate with your existing tools and IT system infrastructure. We hope you will seek
56 products that are congruent with applicable standards and best practices.

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

61 **1.2 Build Overview**

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

69 **1.3 Typographical Conventions**

70 The following table presents typographic conventions used in this volume.

71 **Table 1.1 Typographical Conventions**

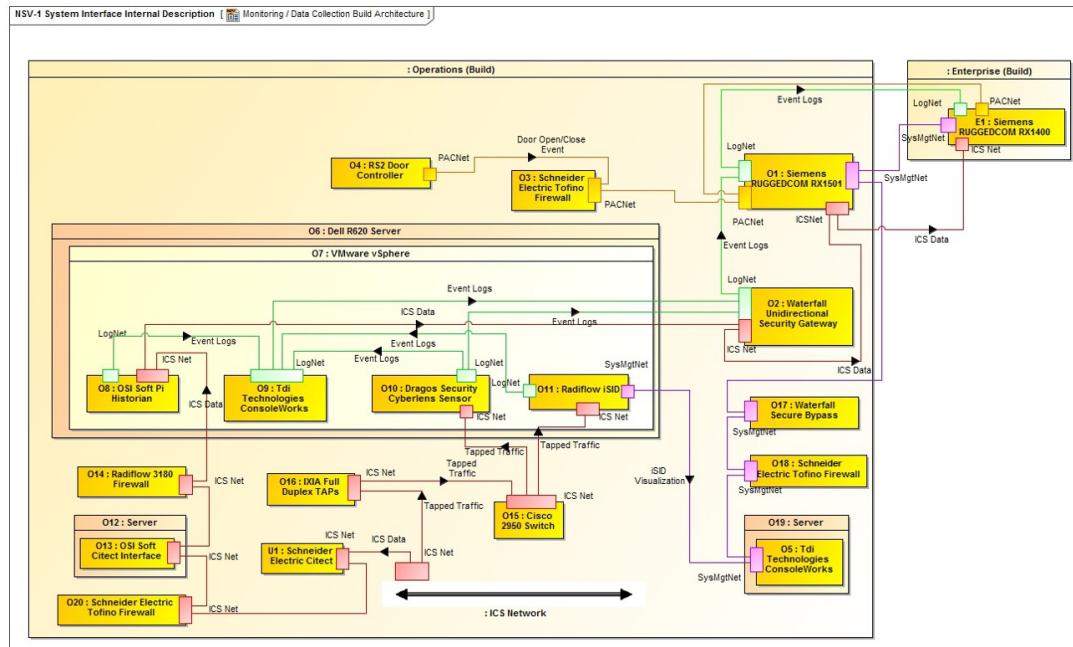
Typeface/Symbol	Meaning	Example
<i>Italics</i>	filenames and pathnames, references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit .
Monospace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

Table 1.1 Typographical Conventions

Typeface/Symbol	Meaning	Example
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 National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov

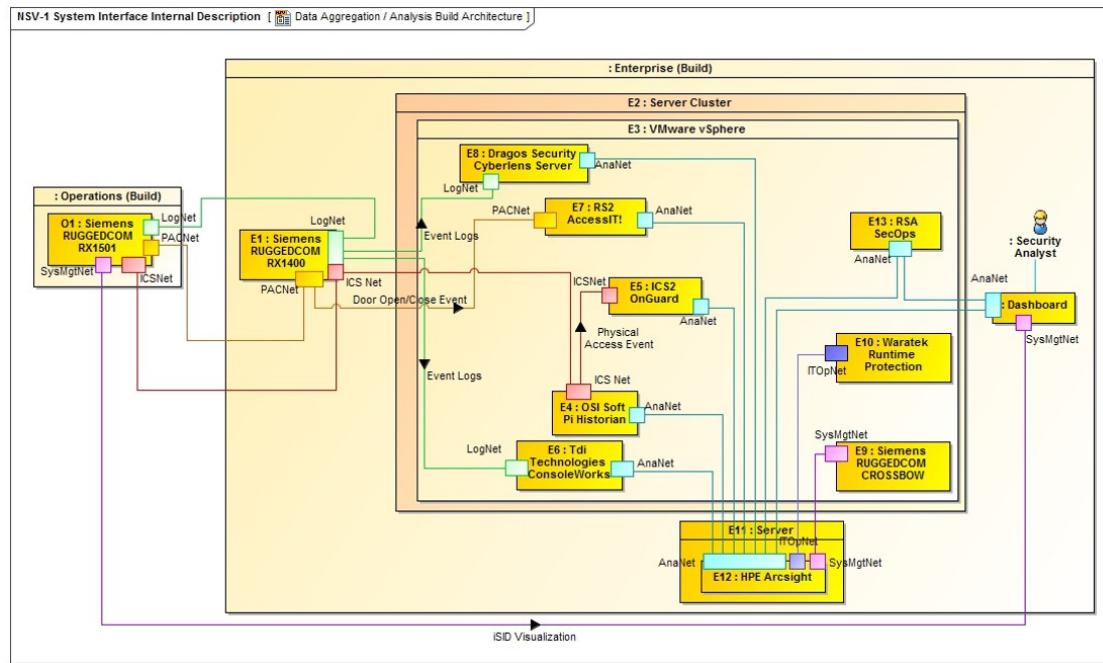
1.4 Logical Architecture Summary

NIST Special Publication 1800-7B (SP1800-7B) 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 ICS network by the monitoring / data collection component, and sent to the data aggregation / analysis component. SP1800-7B also presents an architecture for building and instance of the example solution using commercial products. That architecture is depicted in the [Figure 1.1](#) and [Figure 1.2](#) below.

Figure 1.1 Monitoring and Data Collection Lab Build Architecture

82

83

Figure 1.2 Data Aggregation and Analysis Lab Build Architecture

84

85
86
87

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 SP1800-7B Section 4, Architecture.

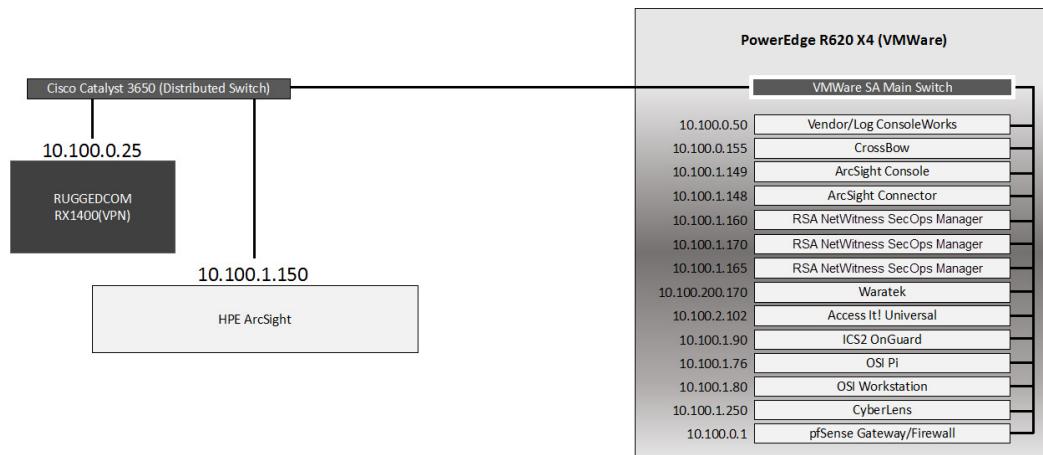
88

1.5 Wiring Diagrams

89
90
91

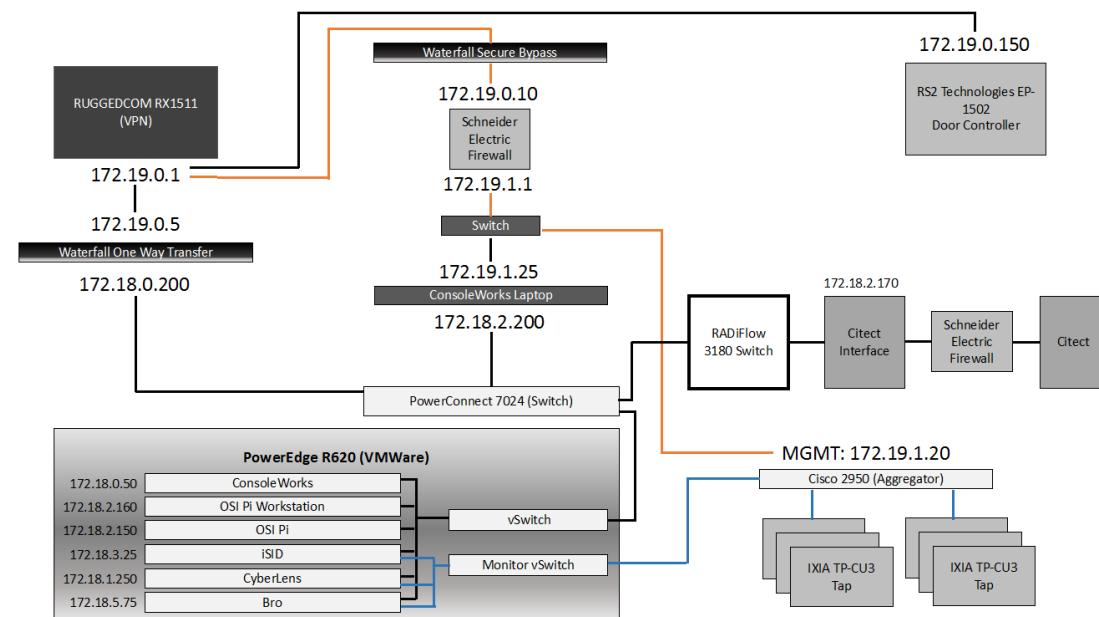
The architecture diagrams in the previous section present the logical connections needed among the products used to build an instance of the example solution. This section describes the physical wiring that implements those logical connections.

92

Figure 1.3 Enterprise Lab Wiring Diagram

93

94

Figure 1.4 Cogeneration Facility Lab Network Diagram

95

2 Product Installation Guides

2	2.1 Cisco 2950 (O15)	8
3	2.2 Dragos Security CyberLens (E8, O10).....	11
4	2.3 HPE ArcSight (E12).....	13
5	2.4 ICS2 OnGuard (E5).....	18
6	2.5 IXIA Full-Duplex Tap (O16)	22
7	2.6 OSIsoft Pi Historian (E4, O8)	23
8	2.7 OSIsoft Citect Interface (O13).....	29
9	2.8 RS2 Technologies Access It! Universal.NET(E7).....	34
10	2.9 RS2 Technologies Door Controller (O4).....	36
11	2.10 Radiflow 3180 (O14)	40
12	2.11 Radiflow iSID (O11).....	41
13	2.12 RSA Archer Security Operations Management (E13).....	42
14	2.13 Schneider Electric Tofino Firewall (O3, O18, O20)	55
15	2.14 Siemens RUGGEDCOM CROSSBOW (E9).....	63
16	2.15 Siemens RUGGEDCOM RX1400 (E1)	82
17	2.16 Siemens RUGGEDCOM RX1501 (O1).....	85
18	2.17 TDi Technologies ConsoleWorks (E6, O5, O9).....	85
19	2.18 Waterfall Technologies Unidirectional Security Gateway (O2)	96
20	2.19 Waterfall Secure Bypass (O17).....	100
21	2.20 Waratek Runtime Application Protection (E10).....	101
22	2.21 ArcSight Connector Guides.....	102

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:

- **En** identifies a product instance installed in the Enterprise portion of the build constructed in the NCCoE energy sector lab. For example, **E1** is the Siemens RUGGEDCOM RX1400 installed in the NCCoE lab.
- **On** identifies a product instance installed in the Operations portion of the build constructed in the build partner's cogeneration facility. For example, **O1** is the Siemens RUGGEDCOM RX1501 installed in the build partner's cogeneration facility.
- **Un** identifies a product instance that is an existing part of the build partner's cogeneration facility. For example, **U1** is the Citect SCADA controller that is part of the build partner's cogeneration facility control system.

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 E9 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
!
```

```
64    username admin privilege 15 secret 5 $1*.1Gz$nHZ.CVIlq28oMB46m2X8k/
65    ip subnet-zero
66    !
67    ip domain-name lab-mgmt
68    ip ssh time-out 120
69    ip ssh authentication-retries 3
70    ip ssh version 2
71    !
72    spanning-tree mode pvst
73    no spanning-tree optimize bpdu transmission
74    spanning-tree extend system-id
75    !
76    !
77    !
78    !
79    interface FastEthernet0/1
80    no keepalive
81    speed 100
82    !
83    interface FastEthernet0/2
84    no keepalive
85    speed 100
86    !
87    interface FastEthernet0/3
88    no keepalive
89    !
90    interface FastEthernet0/4
91    no keepalive
92    !
93    interface FastEthernet0/5
94    no keepalive
95    !
96    interface FastEthernet0/6
97    no keepalive
98    !
99    interface FastEthernet0/7
100   no keepalive
101   !
102   interface FastEthernet0/8
103   no keepalive
104   !
105   interface FastEthernet0/9
106   no keepalive
```

```
107      !
108      interface FastEthernet0/10
109      no keepalive
110      !
111      interface FastEthernet0/11
112      no keepalive
113      !
114      interface FastEthernet0/12
115      no keepalive
116      !
117      interface FastEthernet0/13
118      !
119      interface FastEthernet0/14
120      !
121      interface FastEthernet0/15
122      !
123      interface FastEthernet0/16
124      !
125      interface FastEthernet0/17
126      !
127      interface FastEthernet0/18
128      !
129      interface FastEthernet0/19
130      !
131      interface FastEthernet0/20
132      switchport mode trunk
133      !
134      interface FastEthernet0/21
135      !
136      interface FastEthernet0/22
137      !
138      interface FastEthernet0/23
139      !
140      interface FastEthernet0/24
141      switchport access vlan 1000
142      switchport mode access
143      !
144      interface FastEthernet0/25
145      !
146      interface FastEthernet0/26
147      !
148      interface Vlan1
149      no ip address
```

```
150      no ip route-cache
151      shutdown
152      !
153      interface Vlan1000
154      ip address 172.19.1.20 255.255.254.0
155      no ip route-cache
156      !
157      ip http server
158      !
159      line con 0
160      line vty 0 4
161      password -1pqla,zMXKSOW)@
162      transport input ssh
163      line vty 5 15
164      password -1pqla,zMXKSOW)@
165      transport input ssh
166      !
167      !
168      !
169      monitor session 1 source interface Fa0/1 - 12 rx
170      monitor session 1 destination interface Fa0/23
171      end
```

172 **2.2 Dragos Security CyberLens (E8, O10)**

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

175 **2.2.1 Dragos Security CyberLens Server (E8) Environment Setup**

176 The system that was set up to run this application was a fully updated (as of 5/20/2016) Ubuntu
177 14.04LTS Operating System with the following hardware specifications:

- 178 ■ 4Core Processor
- 179 ■ 8GB RAM
- 180 ■ 40GB HDD
- 181 ■ Other Requirements:
 - 182 ■ Sudo or Root privileges
 - 183 ■ CyberLens installer (cyberlens-<version>-linux-<architecture>-installer.run)
 - 184 ■ Valid CyberLens License file

185 2.2.2 Dragos Security CyberLens Server (E8) Installation and Configuration Guide

- 186 1. As Root:
 - 187 a. ./cyberlens-<version>-linux-<architecture>-installer.run
 - 188 b. Accept the agreement and select **Forward**.
 - 189 c. Select **Forward** for a randomly generated password for root on the MySQL server. You
190 can also specify your own password if you wish.
 - 191 d. Select **Forward** for a randomly generated password for CyberLens on the MySQL server.
192 As in the previous step, you can also specify your own password.
 - 193 e. Select **Forward** to accept the installation configuration.
 - 194 f. Choose a **Username**, **Password** (and Confirm Password), and **Email Address** for the
195 CyberLens login, then select **Forward**.
 - 196 g. Select **Localhost Access Only** (the files will be transferred across the Waterfall Security
197 Gateway), then select **Forward**.
 - 198 h. Select **Forward**. Do not check the box for Block Outbound Traffic.
 - 199 i. Click the **folder icon** to select the CyberLens license file, then select **Forward**.
 - 200 j. Select **Forward** to begin installation.
- 201 2. Configure:
 - 202 a. Open a browser and navigate to **http://localhost/**
 - 203 b. On the menu bar on the left, select **Server Console**.
 - 204 c. Click the **drop down arrow** next to **Options**, and check the box for **Use Sensor Files**.
 - 205 d. Click **Start** to start the server.
- 206 3. Set up FTP for transferring files across the Waterfall Security Gateway:
 - 207 a. First, set up the user login. We used the username “waterfall”.
 - 208 b. adduser waterfall
 - 209 c. Specify password.
 - 210 d. Add additional information if desired.
 - 211 e. Type **y** to accept information.
 - 212 f. apt-get install vsftpd
 - 213 g. Edit /etc/vsftpd.conf
 - 214 h. Ensure anonymous_enable=NO
 - 215 i. Ensure local_enable=YES
 - 216 j. Set write_enable=YES
 - 217 k. service vsftpd restart
 - 218 l. ln -s /var/www/html/cyberlens/lib/file_link/ /home/waterfall/
- 219 4. Permissions error: When files are copied over, the permissions default to
220 **waterfall:waterfall**. Use the following steps to change the default to **www-data:www-data**.

- 221 a. sudo apt-get install incrontab
 222 b. sudo vi /etc/incron.allow
 223 i. Add root to file, then save and exit.
 224 c. sudo incrontab -u root -e
 225 i. Add /var/www/html/cyberlens/lib/file_link IN_CREATE /bin/chown
 226 -R www-data:www-data /var/www/html/cyberlens/lib/file_link then
 227 save and exit.

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

The screenshot shows the CyberLens dashboard with the following sections:

- Server Controls:** Shows Elapsed Time (15d:21h:50m:20s), Listening Port (1337), and a "Running" status bar. Includes a "Stop" button.
- Database Controls:** A green box containing a trash can icon and text: "This action wipes all data in the database, but by default the devices are not erased." It has checkboxes for "Delete Devices" (checked) and "Delete Snapshots". A "Clear" button is also present.
- Session Manager:** A table with columns "Session Name" and "Actions". A note says: "Provide a name for the current project and then hit submit. This will allow you to be able to load the same graph with all the supporting metadata in the future." A "Save" button is at the top right of the table.
- Import Manager:** A section for importing device names. It includes "Import Device Names" help text, "Address Type" radio buttons for "IP Address" (selected) and "MAC Address", a "Delimiter" input field with ", (comma)", and a "Select a File" section with "Browse", "Click Browse to Select a File", and "Upload" buttons.

230

231 2.2.3 Dragos Security CyberLens Sensor (O10) Installation Guide

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

234 2.3 HPE ArcSight (E12)

235 HPE ArcSight is used as a central SIEM (Security Information and Event Management) platform,
 236 collecting alerts from all across the build and aggregating them in one central location.

237 For more information, visit

238 <http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/>

240 2.3.1 HPE ArcSight (E12) Installation Guide

241 2.3.1.1 ArcSight ESM Manager Server Environment Setup

242 The following configuration matched requirements for the product relative to the use in the
 243 Situational Awareness Use Case.

- 244 1. The base Operating System used is Centos 7. The following partition scheme was used for
 245 the install.

246 **Table 2.1 Centos Partitioning Scheme for ArcSight ESM Manager Server**

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

a. It is recommended to use XFS for /opt in lieu of ext4.

- 247 2. Ensure /tmp is larger than 3GB, otherwise ESM will fail to install
 248 3. Ensure the installation of X Windows and 'compatibility libraries' are installed as well; ESM
 249 requires them.
 250 4. Modification of user process limit may be required to ensure efficient thread usage
 251 a. If you do not already have a file /etc/security/limits.d/90-nproc.conf, create it (and the
 252 limits.d directory, if necessary).
 253 b. If the file already exists, delete all entries in the file.
 254 c. Add the following lines:
 255 * soft nproc 10240
 256 * hard nproc 10240
 257 5. Adjust networking items
 258 a. Set **IP address** to 10.100.1.150
 259 b. Set **Gateway** to 10.100.0.1
 260 c. Set **Subnet mask** to 255.255.0.0
 261 d. Add DNS server in **/etc/resolv.conf**
 262 10.97.74.8
 263 e. Add hostname in **/etc/hosts** as follows (or add to DNS):
 264 10.100.1.150 arcsight.es-sa-b1.test arcsight
 265 f. Set hostname in **/etc/sysconfig/network**

- 266 g. Set **ONBOOT** to **yes** in **/etc/sysconfig/network-scripts/ifcfg-eth0**
- 267 6. Ensure ports **8443, 9443, 9000** are open on server firewall (e.g. check via iptables -S or
268 iptables -L -n) If needed add the following (as root). Adjust 0.0.0.0/0 statements as needed.
269 iptables -I INPUT -p tcp --dport 8443 -s 0.0.0.0/0 -j ACCEPT
270 iptables -I INPUT -p tcp --dport 9443 -s 0.0.0.0/0 -j ACCEPT
271 iptables -I INPUT -p tcp --dport 9000 -s 0.0.0.0/0 -j ACCEPT
272 If using a SuperConnector/Forwarder (e.g. to RSA Archer) add the following (adjust for UDP
273 or TCP as needed):
274 iptables -I OUTPUT -p tcp -d 0.0.0.0/0 --dport 514 -j ACCEPT
- 275 7. Save the rules:
276 /sbin/service iptables save
- 277 8. Set Selinux to **permissive mode** (may set back to enforcing mode upon completion of
278 installation)
- 279 9. adduser arcsight
- 280 10. mkdir /opt/arcsight/
- 281 11. chown arcsight:arcsight /opt/arcsight/
- 282 12. Modify files to imitate RHEL 6.5 (For CentOS and newer Redhat versions)
- 283 a. Edit /etc/system-release
284 CentOS release 6.5 (Final)
- 285 b. Edit /etc/system-release-cpe
286 cpe:/o:centos:linux:6:GA
- 287 13. Ensure the time zone (tzdata) package is version 2014F or later. To install, use:
288 rpm -Uvh tzdata
289 or
290 yum update
- 291 14. Reboot

292 2.3.2 ArcSight ESM Manager Server Operating System Installation

- 293 1. Copy the ESM installation tar file (don't untar) to:
294 /home/arcsight/Desktop/ArcSight (create folder if it does not exist).
- 295 2. Copy the ESM zipped license file (don't unzip) into the folder from the previous step.
- 296 3. cd /home/arcsight/Desktop/ArcSight (su arcsight if not currently arcsight
297 user).
- 298 4. chown arcsight:arcsight <ESM Install File>
- 299 5. tar xvf <ESM Install File>

300 6. ./ArcSightESMSuite.bin -i console

301 Note: *Stop xwindows first if doing the installation with the -i console switch, this switch runs the*
302 *installation from the command line rather than a GUI. The command line install eases*
303 *troubleshooting.*

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

305 /opt/arcsight/manager/bin/arcsight firstbootsetup -boxster -soft -i
306 console

307 8. Settings in the wizard:

- 308 a. CORR-Engine (DB) password = _____
309 b. System Storage Size = 301GB
310 c. Event Storage Size = 361GB
311 d. Online Event Archive Size = 200GB (~1/6 minus 10% of total space...system reserves 10%
312 of space)
313 e. Retention Period (days) = 30
314 f. Manager host name = arcsight.es-sa-b1.test
315 g. Administrator user name = admin
316 h. Administrator password = _____

317 9. As user “root” run the following to install the ArcSight services onto the operating system:

318 10. Open a browser and navigate to ArcSight Command Center
319 (<https://arcsight.es-sa-b1.test:8443>). Set the manager java heap to 12288 (or another value
320 based on available RAM).

321 2.3.3 ArcSight Console Environment Setup

322 1. Microsoft Windows 7 64-bit with the following settings:

- 323 a. 1 vCPU
324 b. 4GB ram
325 c. 150GB storage

326 2. The guest OS IP information was set as follows:

- 327 a. IP address: 10.100.1.149
328 b. Gateway: 10.100.0.1?
329 c. Subnet mask: 255.255.0.0?
330 d. DNS: 10.97.74.8, 8.8.8.8, 8.8.4.4

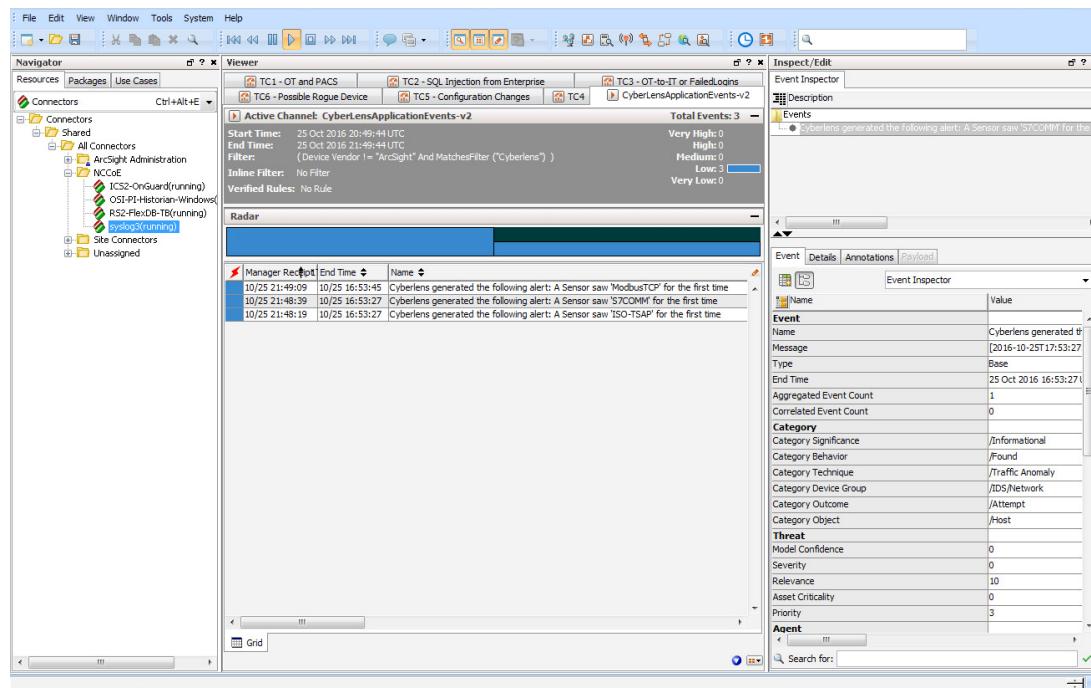
331 3. Installed VM Tools on guest OS to resolve missing mouse cursor issue.

332 4. Created OS user: arcsight, with password: _____

333 2.3.4 ArcSight Console Installation

- 334 1. Download ArcSight Console installation file (for Windows).
- 335 2. Run ArcSight Console installation file?
- 336 3. Add ArcSight Manager IP address to Windows OS host file (or add to DNS) at:
 - 337 a. C:\windows\system32\drivers\etc\hosts (edit this file as Administrator) by adding the following line:

```
339 10.100.1.150 arcsight.es-sa-b1.test arcsight
```
- 340 4. Open ArcSight Console
- 341 5. Login 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`
- 342 6. At certificate related popup, click **Accept**.



344

345 2.3.4.1 ArcSight Connector Server Preparation

- 346 1. CentOS 7 host with the following VM settings:
 - 347 a. 1vCPU
 - 348 b. 12 GB ram
 - 349 c. 140 GB provisioned
- 350 2. Install CentOS using the following options:
 - 351 a. Server with GUI (Xwindows libraries are required in accordance with ArcSight guide)
 - 352 b. File and Storage (in case file-based log collection will be used)

353 c. Compatibility libraries
354 d. Development tools
355 3. Set guest hostname as follows: arcconn.es-sa-b1.test
356 4. Install VM Tools on guest OS
357 5. Set guest OS IP information as follows:
358 a. IP address: 10.100.1.148
359 b. Gateway: 10.100.0.1
360 c. Subnet mask: 255.255.0.0
361 d. DNS: 10.97.74.8, 8.8.8.8
362 6. Add hostnames in /etc/ hosts as follows (or add to DNS):
363 a. 10.100.1.148 arcconn.es-sa-b1.test arcconn
364 b. 10.100.1.150 arcsight.es-sa-b1.test arcsight
365 7. adduser arcsight
366 8. mkdir /opt/arcsight/
367 9. chown -r arcsight:arcsight /opt/arcsight/
368 10. As user arcsight, mkdir /opt/arcsight/connectors/syslog1
369 11. Ensure UDP port 514 is open inbound on server firewall and also that connector is allowed
370 outbound on port 8443. For example:
371 a. as root:
372 iptables -I INPUT -p udp --dport 514 -s 0.0.0.0/0 -j ACCEPT
373 iptables -I OUTPUT -p tcp -d 0.0.0.0/0 --dport 8443 -j ACCEPT
374 b. Save the rules:
375 /sbin/service iptables save
376 12. Disable firewall:
377 a. systemctl disable firewall
378 b. systemctl mask firewalld expressions
379 13. Disable OS native syslog service
380 a. systemctl disable rsyslog.service

381 2.4 ICS² OnGuard (E5)

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

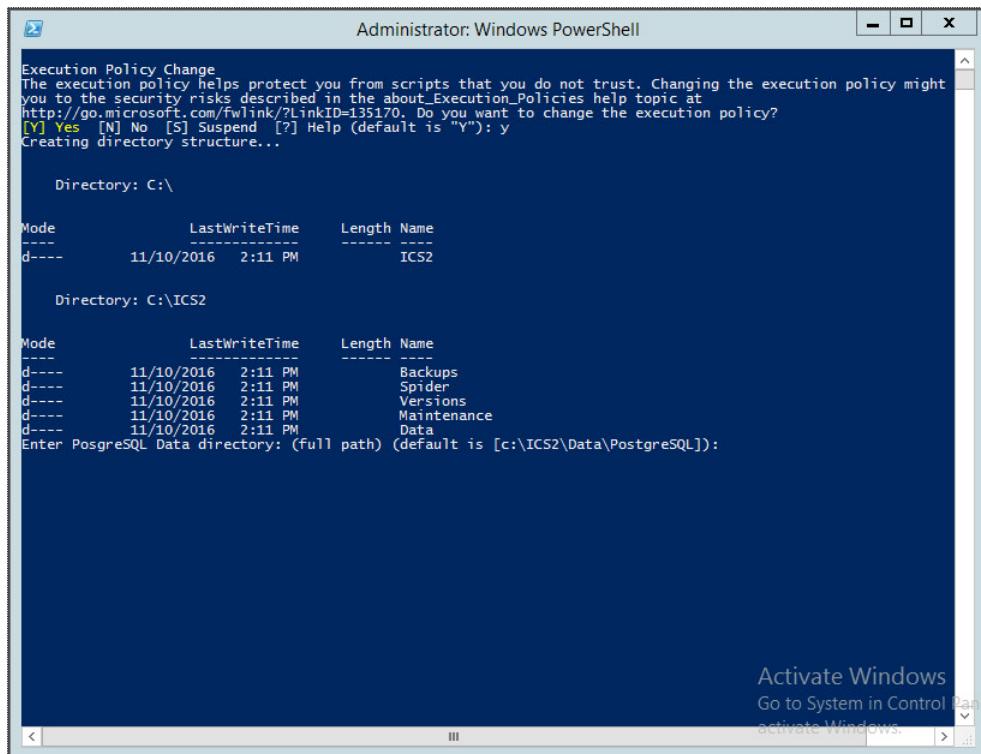
385 2.4.1 Environment Setup

386 The following configuration matched requirements for the product relative to the use in the
387 Situational Awareness build:

- 388 ■ Microsoft Windows Server 2012 R2
 389 ■ VM with CPU Quad Core 2.199GHz
 390 ■ VM with 16384MB of memory
 391 ■ Virtual Hard disk
 392 ■ OSISoft PI OLE DB Driver
 393 ■ ICS2_Installation_<version>.zip

394 2.4.2 Install Vendor Software

- 395 1. Open and extract the provided **ICS2_Installation_<version>.zip** file.
- 396 2. Open the **ICS2 Installation folder** created by extracting the .zip file.
- 397 3. Right-click the **ServerDeploy.PS1** file and select **Run with PowerShell**.
- 398 4. Press **Y** to change the execution policy.
- 399 5. Once the directory structure has been created, press **Enter** for the default PostgreSQL directory.



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". It displays the creation of directory structures. First, it shows the creation of the "ICS2" directory at the root of C:\. Then, it shows the creation of sub-directories within "ICS2": "Backups", "Spider", "Versions", "Maintenance", and "Data". Finally, it prompts the user to enter the PostgreSQL Data directory, defaulting to [c:\ICS2\Data\PostgreSQL].

```

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might
you to the security risks described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
Creating directory structure...

Directory: C:\

Mode          LastWriteTime    Length Name
----          -----          ---- 
d----
```

Mode	LastWriteTime	Length	Name
d----	11/10/2016 2:11 PM		ICS2

```

Directory: C:\ICS2

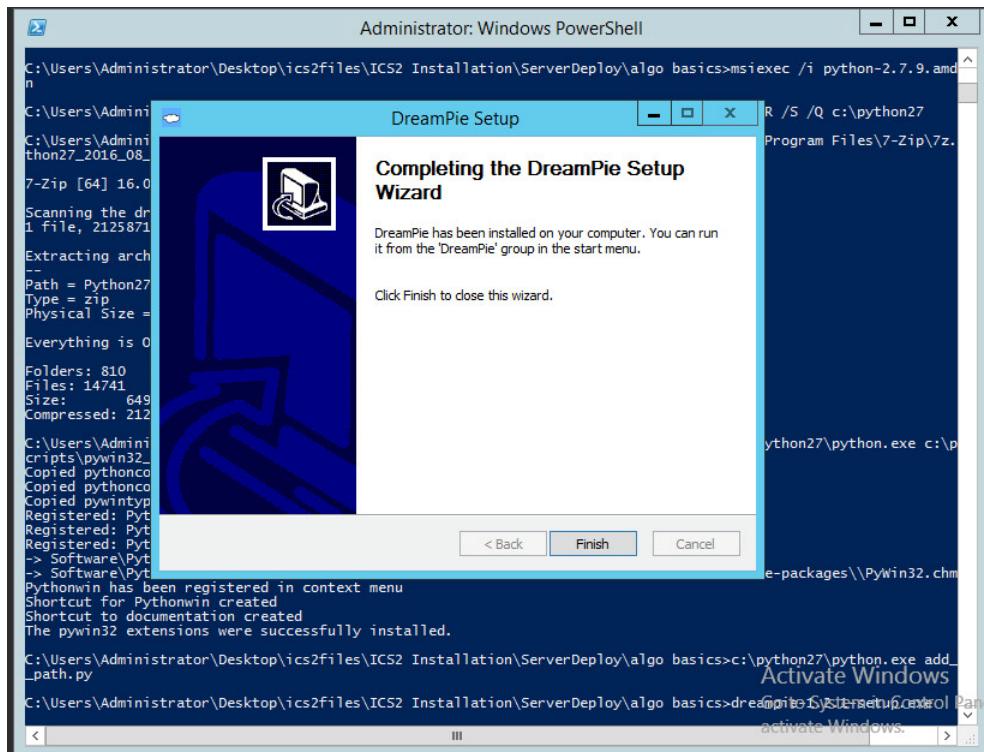
Mode          LastWriteTime    Length Name
----          -----          ---- 
d----
```

Mode	LastWriteTime	Length	Name
d----	11/10/2016 2:11 PM		Backups
d----	11/10/2016 2:11 PM		Spider
d----	11/10/2016 2:11 PM		Versions
d----	11/10/2016 2:11 PM		Maintenance
d----	11/10/2016 2:11 PM		Data

Enter PosgreSQL Data directory: (full path) (default is [c:\ICS2\Data\PostgreSQL]):

- 401 6. Press **Enter** for the default SQLServer directory.
 - 402 a. The installer will install multiple products, including Google Chrome and Notepad++.
- 403 7. When the DreamPie installer pops up, click **Next**.
- 404 8. Select **Install for anyone using this computer** and click **Next**.

- 406 9. Keep the default destination folder and click **Install**.
- 407 10. When the installation is complete, click **Next**.
- 408 11. Close the installer by clicking **Finish**.

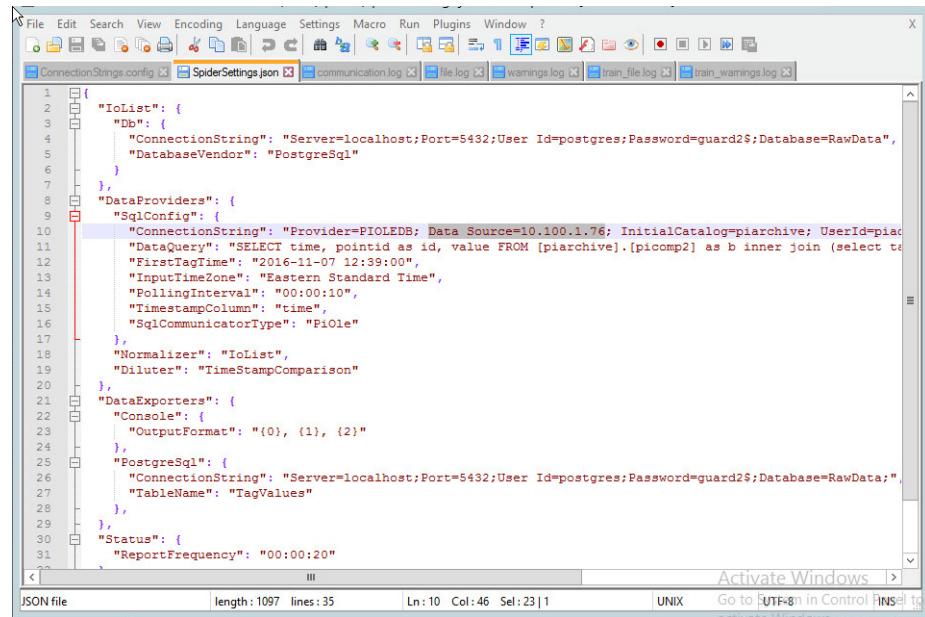


- 409 12. Once completed, PowerShell will close.

411 2.4.3 Install OnGuard System

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

418

Figure 2.1 OSisoft PI Historian Connection


```

1  {
2    "IoList": {
3      "Db": {
4        "ConnectionString": "Server=localhost;Port=5432;User Id=postgres;Password=guard2$;Database=RawData",
5        "DatabaseVendor": "PostgreSQL"
6      }
7    },
8    "DataProviders": {
9      "SqlConfig": {
10        "ConnectionString": "Provider=PIOLEDB; Data Source=10.100.1.76; InitialCatalog=piarchive; UserId=piacomp2; Password=guard2$",
11        "DataQuery": "SELECT time, pointid as id, value FROM [piarchive].[piocomp2] as b inner join (select ta.time, ta.id, ta.value, ta.tagname from [piarchive].[piocomp2] as ta where ta.tagname like 'TagValue%' and ta.time > '2016-11-07 12:39:00' and ta.value > 0) as c on b.id = c.id",
12        "InputTimeZone": "Eastern Standard Time",
13        "PollingInterval": "00:00:10",
14        "TimestampColumn": "time",
15        "SqlCommunicatorType": "PiOLE"
16      },
17      "Normalizer": "IoList",
18      "Diluter": "TimeStampComparison"
19    },
20    "DataExporters": {
21      "Console": {
22        "OutputFormat": "{0}, {1}, {2}"
23      }
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 }
34
35
36 
```

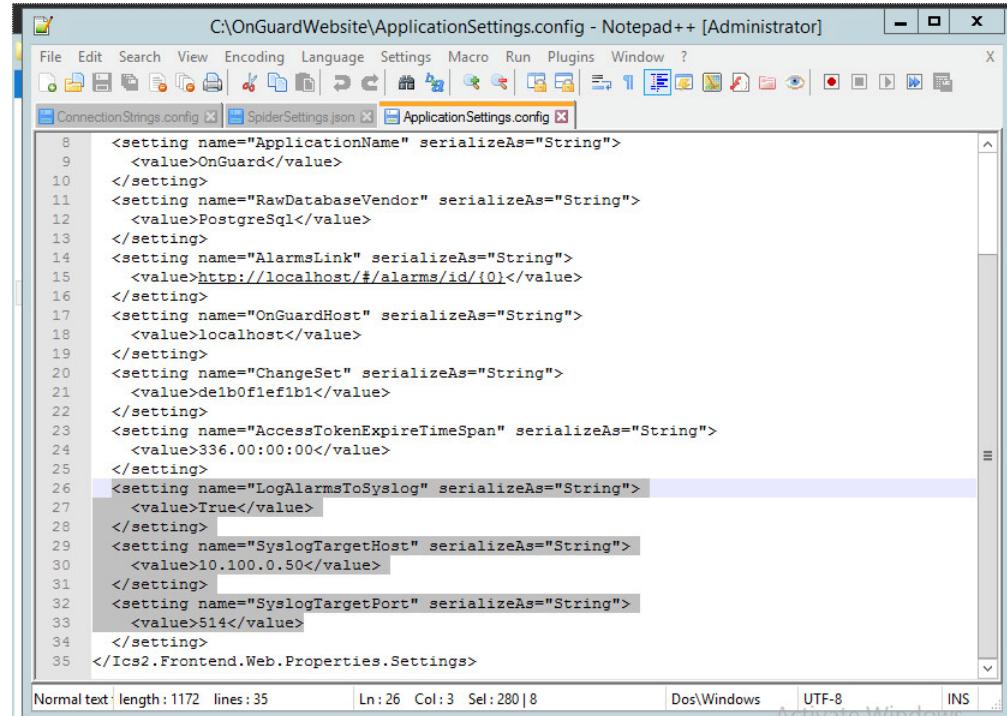
Activate Windows >

JSON file length: 1097 lines: 35 Ln: 10 Col: 46 Sel: 23 | 1 UNIX Go to UTF-8 in Control INS del to

419

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

423

Figure 2.2 ApplicationSettings Syslog Configuration


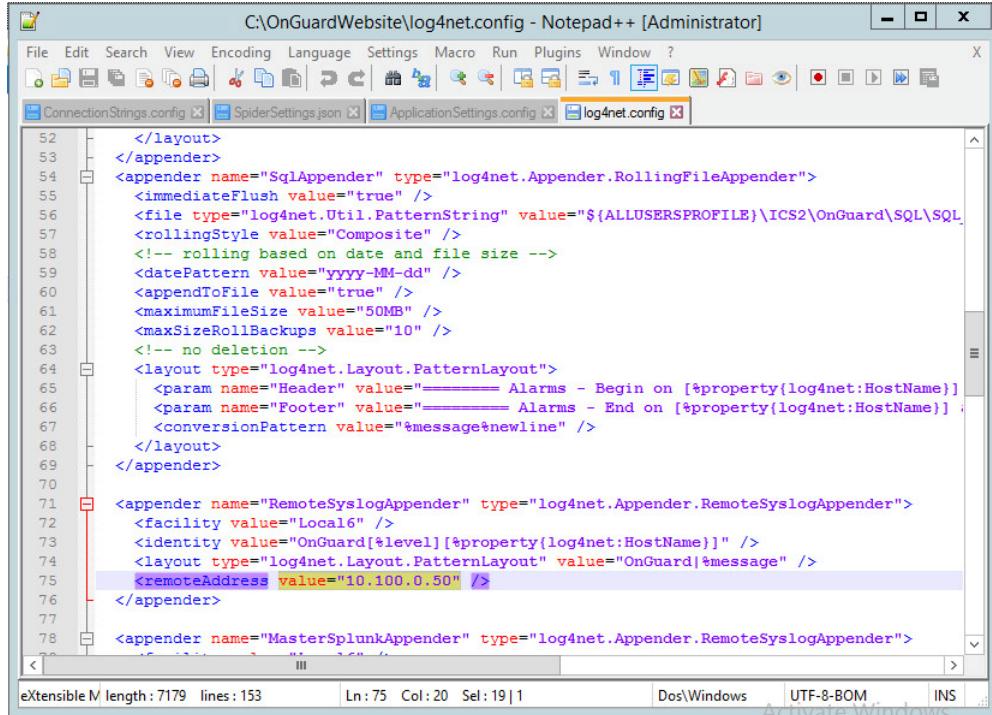
```

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}</value>
16   </setting>
17   <setting name="OnGuardHost" serializeAs="String">
18     <value>localhost</value>
19   </setting>
20   <setting name="ChangeSet" serializeAs="String">
21     <value>de1b0fe1fb1</value>
22   </setting>
23   <setting name="AccessTokenExpiresTimeSpan" 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>
36 
```

Normal text length: 1172 lines: 35 Ln: 26 Col: 3 Sel: 280 | 8 Dos\Windows UTF-8 INS del to

424

- 425 c. Open C:\OnGuardWebsite\log4net.config in Notepad++ and verify that the appender
 426 **RemoteSyslogAppender** has a **remoteAddress** value of the syslog server IP
 427 (10.100.0.50).



```

C:\OnGuardWebsite\log4net.config - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
ConnectionString.config SpiderSettings.json ApplicationSettings.config log4net.config

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%newline" />
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">
    ...
</appender>

```

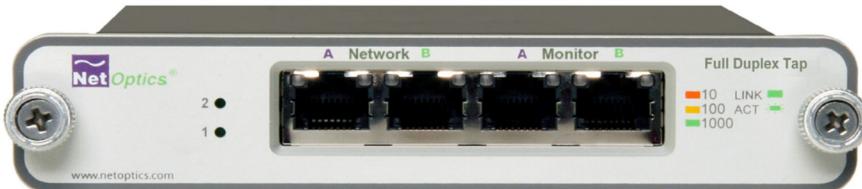
eXtensible M length : 7179 lines : 153 Ln : 75 Col : 20 Sel : 19 | 1 Dos\Windows UTF-8-BOM INS Activate Windows

- 428 4. Close Notepad++ and open Google Chrome to <http://localhost/> for the login screen.

430 2.5 IXIA Full-Duplex Tap (O16)

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

432 **Figure 2.3 IXIA TP-CU3 Network Tap**



- 433 1. Mount the tap to the rack.
 434 2. Utilize the supplied power cord to connect an outlet to the power jacks located on the rear
 435 of the tap.
 436 3. To connect to the network:
 437 a. Connect **Network Port A** to the Ethernet cable coming in from the control system
 438 network.
 439

- 440 b. Connect **Network Port B** to an Ethernet cable going out to the destination port of the
441 original Ethernet cable used in the previous step.
- 442 c. Verify that the link LEDs illuminate.
- 443 d. Connect **Monitor Port A** to the monitoring port of the device used to monitor the
444 ingress of **Network Port A**.
- 445 e. Connect **Monitor Port B** to the monitoring port of the device used to monitor the
446 ingress of **Network Port B**.
- 447 4. The tap installation and setup is complete.

448 2.6 OSIsoft Pi Historian (E4, O8)

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

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

454 2.6.1 OSIsoft Pi Historian (E4) Installation Guide

455 The following is the installation and configuration for the OSIsoft PI Historian located within the
456 Enterprise network.

457 2.6.1.1 Environment Setup

- 458 ■ Microsoft Windows Server 2012 R2
- 459 ■ 2.2Ghz Processor
- 460 ■ 8GB RAM
- 461 ■ 250GB storage
- 462 ■ SQL Server Express

463 2.6.1.2 Installation Instructions

- 464 1. Create admin user in windows: **Piadmin**
- 465 2. Create admin user in windows: **Afadmin**
- 466 3. Create standard user in windows: **Piuser**
- 467 4. Create new folder **C:\Download**
- 468 5. Install SQL Server 2014.
 - 469 a. Create instance:
 - 470 i. Name: **PIAFSQL**
 - 471 ii. Instance ID: **PIAF**

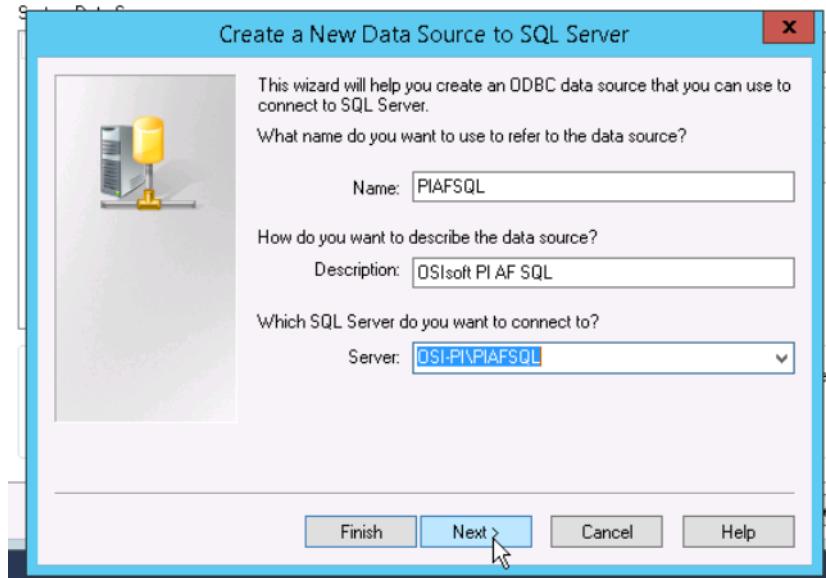
- 472 b. SQL Server Configuration Manager
473 i. Enable SWL Server Network Configuration -> Protocols for PIAFSQL -> {Shared
474 Memory, Named Pipes, TCP/IP}
475 6. Copy **PI-AF-Server_2015-R2_** to C:\Download and self-extract setup (run as administrator).
476 a. A reboot will be required.
477 b. After reboot, the Microsoft Visual C++ 2013 install window will appear.

478 **Figure 2.4 PI AF Server 2015 R2 Setup**



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

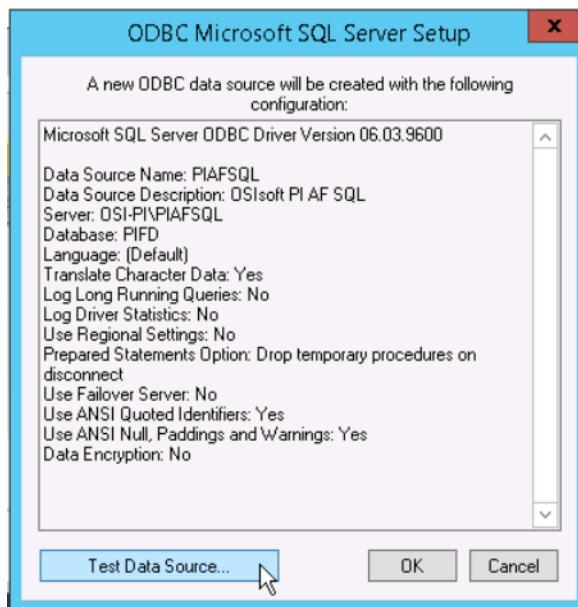
492

Figure 2.5 Create New Data Source for SQL

493

- 494 b. Click **Next**.
- 495 c. Click **Next**.
- 496 d. Check the **Change the default database to:** and select **PIFD**.
- 497 e. Click **Next**.
- 498 f. Click **Finish**.
- 499 g. Click **Test Data Source...**

500

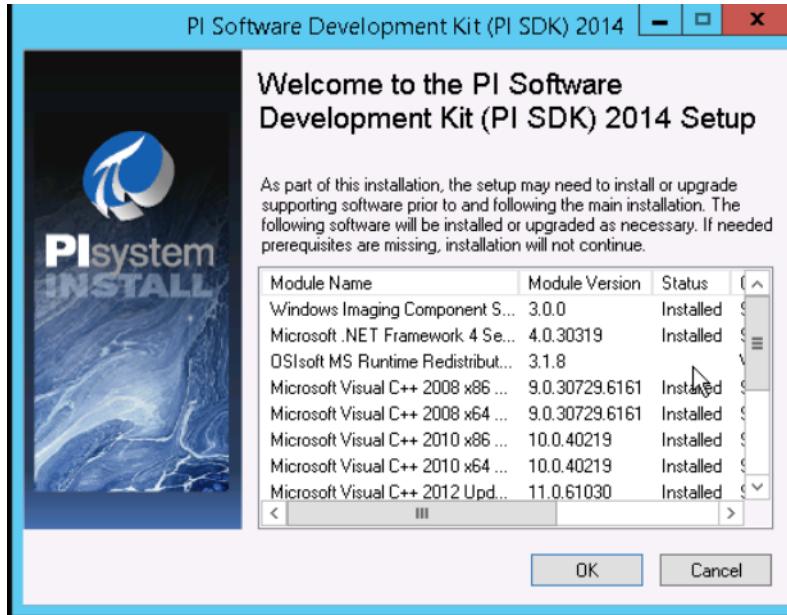
Figure 2.6 Testing SQL Setup

501

- 502 h. After a successful pass, click **OK** three times to close ODBC Data Sources.

- 503 8. Open Microsoft SQL Server Management Studio (as Administrator).
- 504 a. Ensure the settings are correct and click **Connect**.
- 505 b. In the left tab, select <hostname>\PIAFSQL > Databases > PFID > Tables and ensure
506 tables are listed.
- 507 c. Close Microsoft SQL Server Management Studio.
- 508 9. Copy **PISDK_2014_** and **PISMT_2015_R2_** to C:\Downloads.
- 509 10. Copy **PI-AF-Client_2015-R2_** to C:\Download and run as administrator.
- 510 a. Change the Extraction path to .\
- 511 b. When the PI AF Client 2015 R2 install screen starts up, click **OK**.
- 512 c. In the Default Data server input, type **piafsql** and click **Next**.
- 513 d. Click **Next** for the default PIHOME directory.
- 514 e. Wait for the installation to finish and click **Next**.
- 515 f. Select whether to participate in the Customer Experience Improvement and click **Next**.
- 516 g. Click **Next** for default features, then click **Install**.
- 517 h. Verify the Service Status screen shows all services started successfully, and click **Next**.
- 518 i. Click **Close**.
- 519 11. Run **PISDK_2014_** as administrator.
- 520 a. Change the Extraction path to .\
- 521 b. When the PI Software Development Kit install screen starts up, click **OK**.

522 **Figure 2.7 PI SDK Setup**



- 523 c. On the screen listing services that will be stopped, click **OK**.

- 525 d. Verify the Service Status screen shows all services started successfully, and click **Next**.
526 e. Click **Close**.
- 527 12. Run **PISMT_2015_R2_** as administrator.
- 528 a. Change the Extraction path to .\
529 b. When the install screen starts up, click **Next** twice.
530 c. On User Information, change the **Full Name** field to **Pladmin** and fill in **Organization**.
531 d. Click **Next**.
532 e. Click **Install**.
533 f. Click **Close**.
- 534 13. Run the **MSRunTimes** and **MSRunTimes_x64** applications to install the proper DLLs.
- 535 14. Run **OSIprerequisites-standalone_2.0.0.10_** as administrator.
- 536 a. Click **OK**.
537 b. Change Unzip folder to .\ and select **Unzip**.
538 c. When completed, click **Close**.
- 539 15. Run **OSIprerequisites-Patch_2.1.1_**
- 540 a. Change Unzip folder to .\ and select **Unzip**.
541 b. When completed, click **Close**.
- 542 16. Reboot your machine.
- 543 17. Create the following folders:
- 544 c. **C:\PI**
545 d. **C:\PI\Bin**
546 e. **C:\PI\Dat**
547 f. **C:\PI\License**
548 g. **C:\PI\Queue**
549 h. **C:\PI\Archive**
- 550 18. Copy a generated license file into **C:\PI\License** and name **pilicense.dat**.
- 551 19. Copy **PIServer_2012SP_x64_** to **C:\Downloads**.
- 552 20. Run **PIServer_2012SP_x64_** as Administrator.
- 553 a. Change the Unzip folder to .\ and click **Unzip**.
554 b. When the PI Server 2012 SP1 64-bit install screen starts up, click **OK**.
555 c. When showing what's installed, click **Close**.
556 d. On the welcome screen, click **Next**.
557 e. On licensing, click **Browse** and select **C:\PI\License**, then **Next**.
558 f. Verify the AF Server is the hostname, then click **Next**.

- 559 g. Ensure **No** is selected for **enabling PI Module Database** and click **Next**.
560 h. For PI Server Binaries, click **Browse** and select **C:\PI\Bin**.
561 i. For Event Queues, click **Browse** and select **C:\PI\Dat**.
562 j. For Archives, click **Browse** and select **C:\PI\Archive**.
563 k. Click **Next**.
564 l. Click **Next** to start installation.
565 m. When complete, click **Close**.
- 566 21. Open **PI System Management Tools**.
567 a. Under Servers on the left, select the **piafsql server**.
568 b. Close **PI System Management Tools**.
- 569 22. Reboot system.
- 570 23. Copy **C:\PI\Bin\admin\pisrvstart.bat** and **C:\PI\Bin\admin\pisrvstop.bat** to your **Desktop**.
- 571 24. Open **PISDKUtility**.
572 a. Under Tools, select **Add Server**.
573 i. Network Path/FQDN: <hostname>
574 ii. Click **OK**.
575 b. Under Default User Name for the new server, type **piadmin**.
576 c. Under Connections, select **Options**.
577 i. Set the Connection timeout to **30 seconds**.
578 ii. For Default Server, select <hostname>.
579 iii. Ensure the **Protocol Order** is:
580 **1. PI Trust**
581 **2. Default User**
582 **3. Windows Security**
583 iv. Click **OK**.
584 d. Under Connections, select **Aliases**.
585 i. Click **Add...**
586 ii. Under Alias, type the machine's **IP Address**.
587 iii. Click **OK**.
588 iv. Click **Close**.
589 e. Click **Save**.

590 2.6.2 OSIsoft Pi Historian (O8) Installation Guide

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

592 2.7 OSIsoft Citect Interface (O13)

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

595 2.7.1 OSIsoft Citect Interface (O13) Installation Guide

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

```
[PIPC]
PIHOME=C:\Program Files (x86)\PIPC
```
- 601 3. Start the installation executable (**Citect_#.#.#.#.exe**).
- 602 4. This will install files in **PIHOME\Interfaces\Citect**.
- 603 5. Copy the following files from the Citect machine's **Bin** directory into the
604 **PIHOME\Interfaces\Citect** directory.
 - 605 a. **CtApi.dll**
 - 606 b. **Ct_ipc.dll**
 - 607 c. **CtEng32.dll**
 - 608 d. **CtRes32.dll**
 - 609 e. **CtUtil32.dll**
 - 610 f. **CiDebugHelp.dll**
- 611 6. To install the connector as a service, run **PI_Citect.exe /install /auto /depend tcpip**. Test
612 the connection between the interface node and the Citect node using the **PI_CitectTest.exe**
613 connection tester.
- 614 7. Run the **ICU** and configure a new instance of this interface.
- 615 8. Define digital states.
- 616 9. **Cit_Bad_Conn** is an indicator of communication problems with the Citect node.
- 617 10. Build input tags and, if desired, output tags for this interface using the point builder utility
618 **PICitect_PointBuilder.exe**. Important point attributes and their purposes are:

619 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]

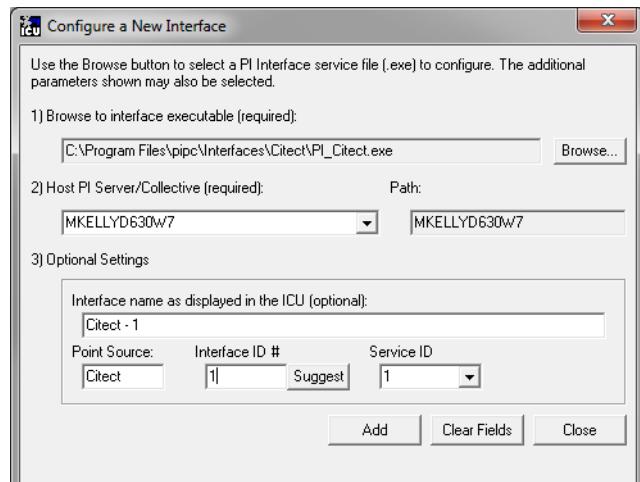
- 626 11. Start the interface interactively and confirm its successful connection to the PI Server
627 without buffering.
- 628 12. Confirm that the interface collects data successfully.
- 629 13. Stop the interface and configure a buffering application (either Bufserv or PIBufss). When
630 configuring buffering, use the ICU menu item **Tools > Buffering... > Buffering Settings** to
631 make a change to the default value (32678) for the Primary and Secondary Memory Buffer
632 Size (Bytes) to **2000000**. This will optimize the throughput for buffering and is
633 recommended by OSIsoft.
- 634 14. Start the buffering application and the interface. Confirm that the interface works together
635 with the buffering application by stopping the PI Server.
- 636 15. Configure the interface to run as an automatic service that depends on the PI Update
637 Manager and PI Network Manager services.
- 638 16. Restart the interface node and confirm that the interface and the buffering application
639 restart.

640 2.7.2 Configuration

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

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

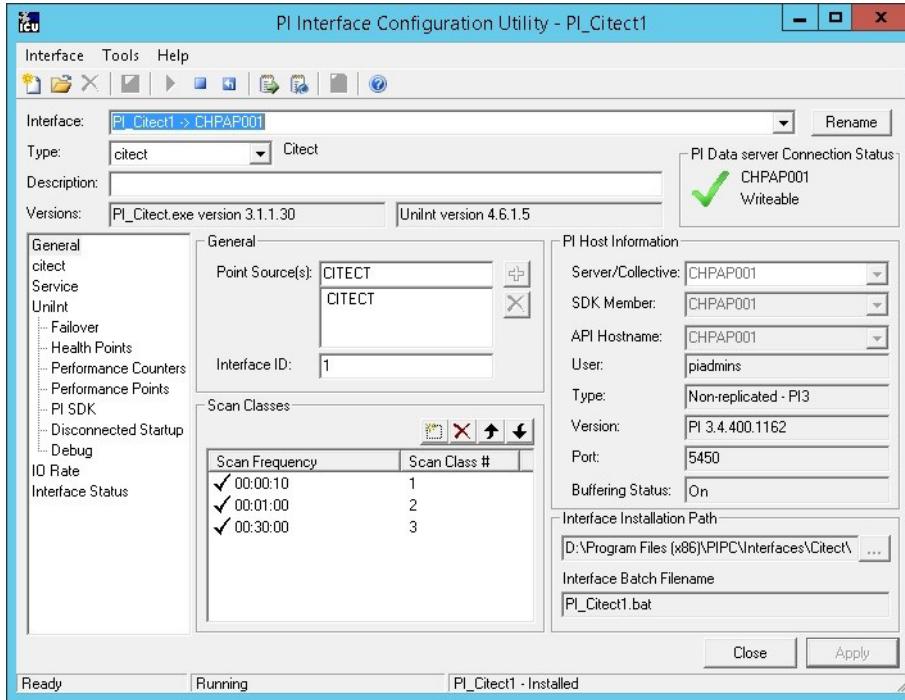
649 **Figure 2.8 Configure New Interface**



- 650 2. **Interface name as displayed in the ICU (optional)** will have PI- pre-pended to this name
651 and it will be the display name in the services menu.
652
- 653 3. Click **Add**.

- 654
- 655
- 656
- 657
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.

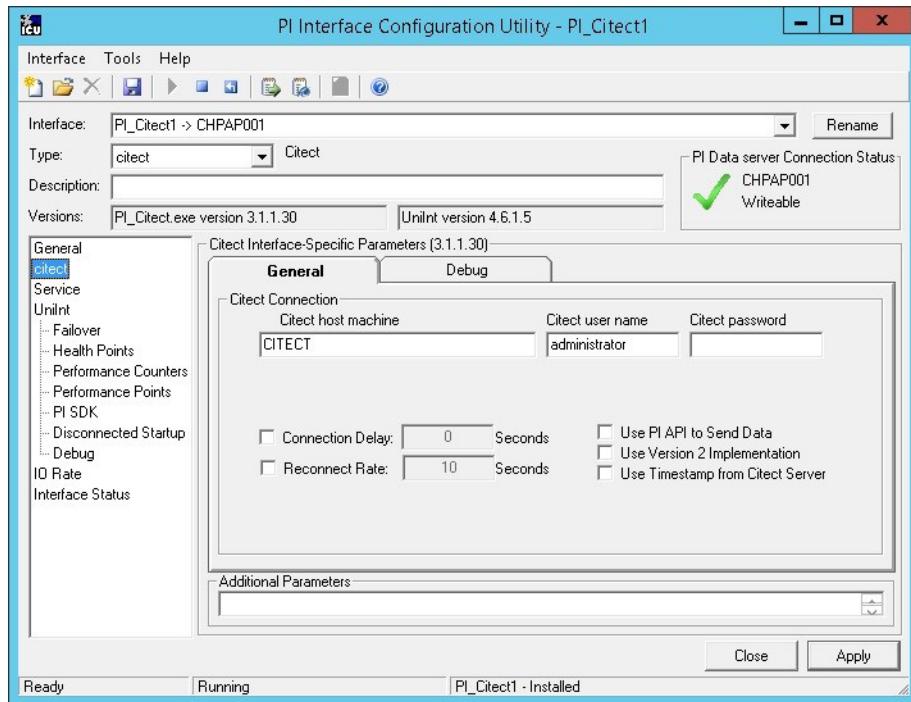
658 **Figure 2.9 PIU - General Configuration**



659

- 660
- 661
- 662
6. Since the startup file of the PI Citect interface is maintained automatically by the PI ICU, use the Citect page to configure the startup parameters and do not make changes in the file manually.

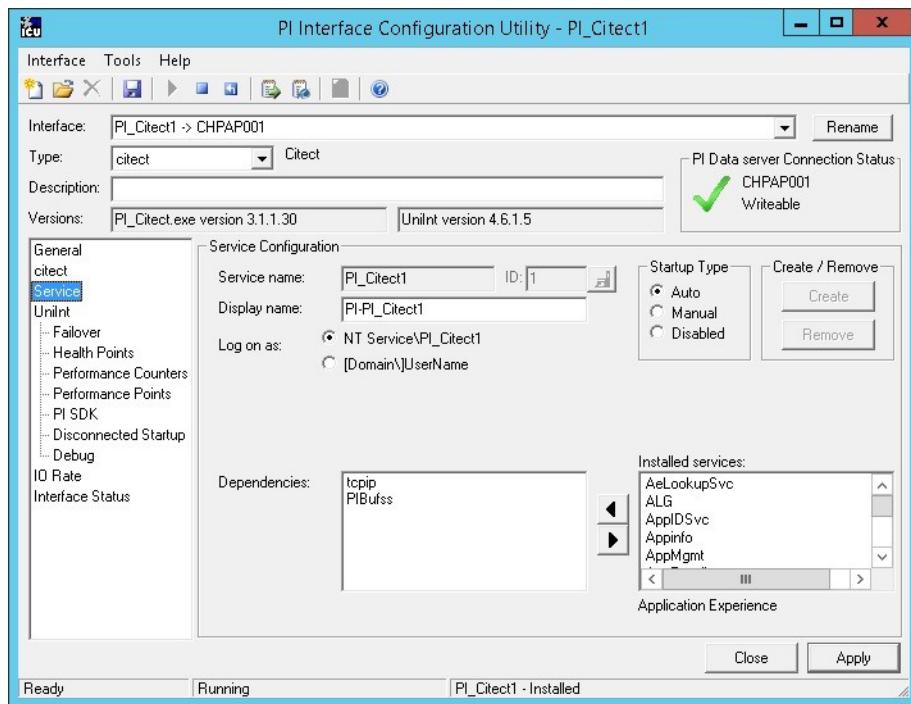
663

Figure 2.10 ICU - Citect ICU Control

664

- 665 7. Supply values for the fields in the Citect **General** tab as follows:
 - 666 a. Citect host machine - **CITECT**
 - 667 b. Citect user name - **administrator**
 - 668 c. Citect password - **<enter password here>**
 - 669 d. Connection Delay - **none (unchecked)**
 - 670 e. Reconnect Rate - **none (unchecked)**
 - 671 f. Use PI API data to Send Data - **(unchecked)**
 - 672 g. Use Version 2 Implementation - **(unchecked)**
 - 673 h. Use Timestamp from Citect Server - **(unchecked)**
- 674 8. Keep the defaults on the Citect **Debug** tab.
- 675 9. 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 the starting and stopping of the interface service. Keep the default values, as shown below.

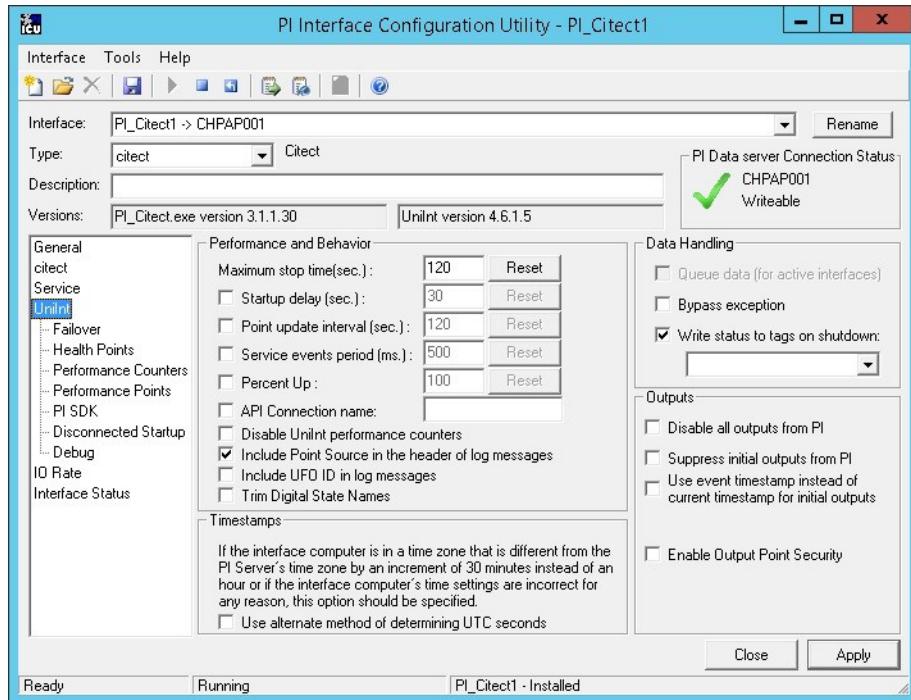
678

Figure 2.11 ICU - Windows Service Setup

679

- 680 10. Since the PI Citect interface is a UniInt-based interface, the UniInt page allows the user to
 681 access UniInt features through the PI ICU and to make changes to the behavior of the
 682 interface.

683

Figure 2.12 ICU - UniInt Configuration

684

- 685 11. Keep the default values, but check the following boxes:
686 a. **Include Point Source in the header log of messages**
687 b. **Write status to tags on shutdown**
688 12. Uncheck the following box:
689 a. **Suppress initial outputs from PI**

690 **2.8 RS2 Technologies Access It! Universal.NET(E7)**

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

694 **2.8.1 Environment Setup**

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

- 697 ■ Microsoft Windows Server 2012 R2
698 ■ VM with CPU Quad Core 2.199GHz
699 ■ VM with 8192MB of memory
700 ■ Virtual Hard Disk containing 240 GB of storage
701 ■ .NET Framework 3.5

702 **2.8.1.1 Product Installation**

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

718 2.8.2 Post-installation and configuration

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

- 722 1. Launch Access It! Universal.NET by selecting it from the **Start** menu.
- 723 2. Log in with the default user name **Admin**. Leave password blank.

724 2.8.2.1 Connecting Access It! Universal.NET

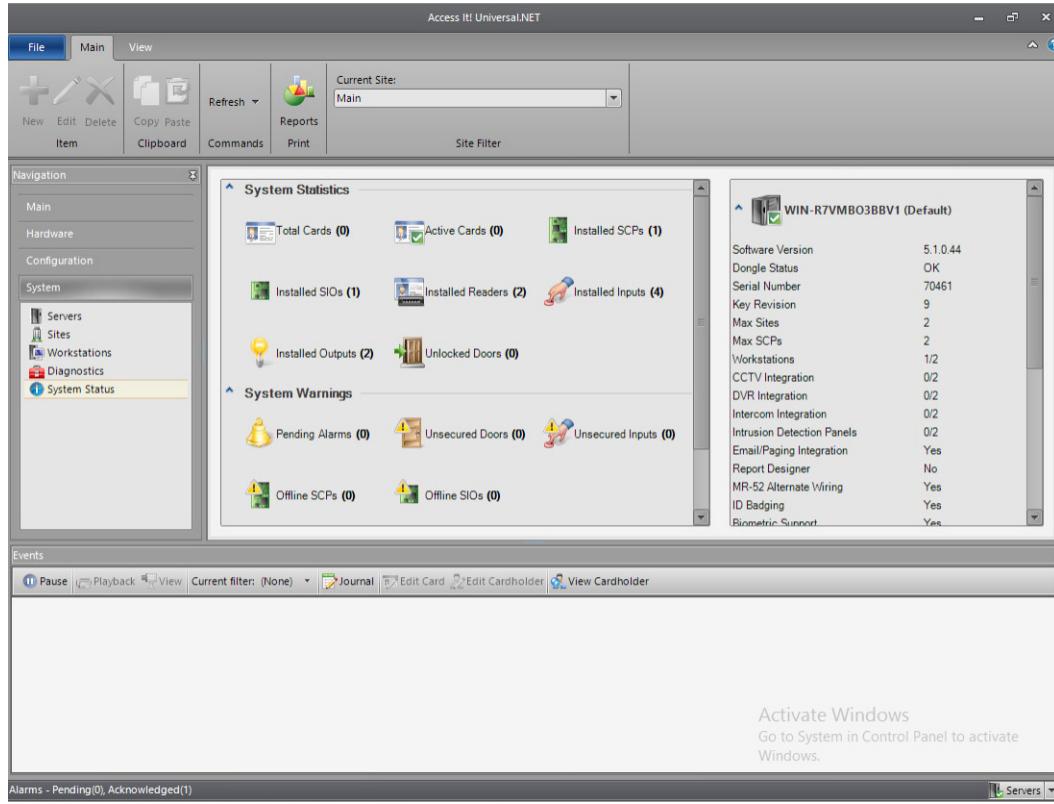
- 725 1. Select **Hardware** under the Navigation pane, then select the **Channels** pane.
- 726 2. Select the **green + sign** in the top left corner to create a new channel.
- 727 3. For Channel Type, select **IP server**.
- 728 4. Ensure Protocol Type is **SCP**.
- 729 5. Ensure **Channel Enabled** is checked.
- 730 6. Select **Save**.
- 731 7. Select **SCPs** under the Navigation pane on the left.
- 732 8. Select the **green + sign** in the top left corner to create a new SCP.
- 733 9. Under the **General** tab:
 - 734 a. Select **EP-1502** for Model.
 - 735 b. Ensure **Device installed** is checked.
 - 736 c. Set **SCP time zone** to the local time zone of the door controller.
- 737 10. Under the **Comm.** tab:
 - 738 a. Ensure that the channel created in the previous steps is listed.
 - 739 b. Set the IP address to **10.100.2.150**.
 - 740 c. Ensure the port number is set to **3001**.
 - 741 d. Ensure the Encryption Settings is set to **None**.
- 742 11. Select **Save**.

743 2.8.2.2 Enable TCP/IP for local SQL 2008 R2 Express Edition Server

- 744 1. Launch **Microsoft SQL Server Configuration Manager**.
- 745 2. Expand **SQL Server Network Configuration (32-bit)**.
- 746 3. Select **Protocols for AIUNIVERSAL**.
- 747 4. Right-click on **TCP/IP**, then select **Properties**.
- 748 5. Select the **IP Addresses** tab.
- 749 6. Under **IP1**, ensure that **IP Address** is set to **0.0.0.0**, and **TCP Port** is set to **1433**.
- 750 7. Under **IPALL**, ensure that **TCP Dynamic Ports** is set to **52839**, and **TCP Port** is set to **1433**.

- 751 8. Restart the SQL server. Select **SQL Server Services**, then right-click on **SQL Server**
 752 **(AIUNIVERSAL)** and select **Restart**.

753 **Figure 2.13 System Status**



755 **2.9 RS2 Technologies Door Controller (O4)**

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

759 **2.9.1 Hardware Installation**

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

- 761 1. The fully assembled and closed case:

762

Figure 2.14 RS2 Door Controller Case



763

764

2. The interior modules:

765

Figure 2.15 Inside of RS2 Door Controller Case



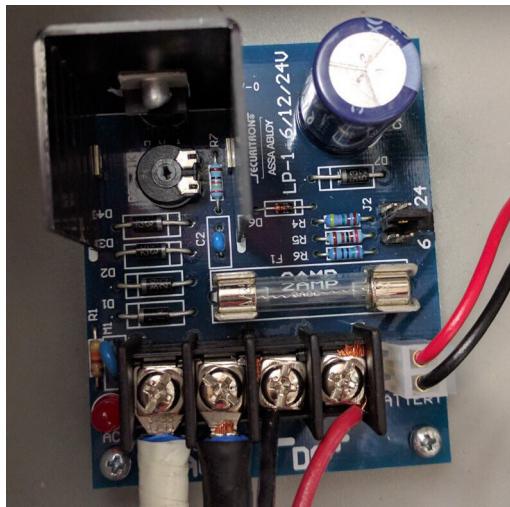
766

767
768

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

769

Figure 2.16 AC/DC Inverter



770

771
772
773

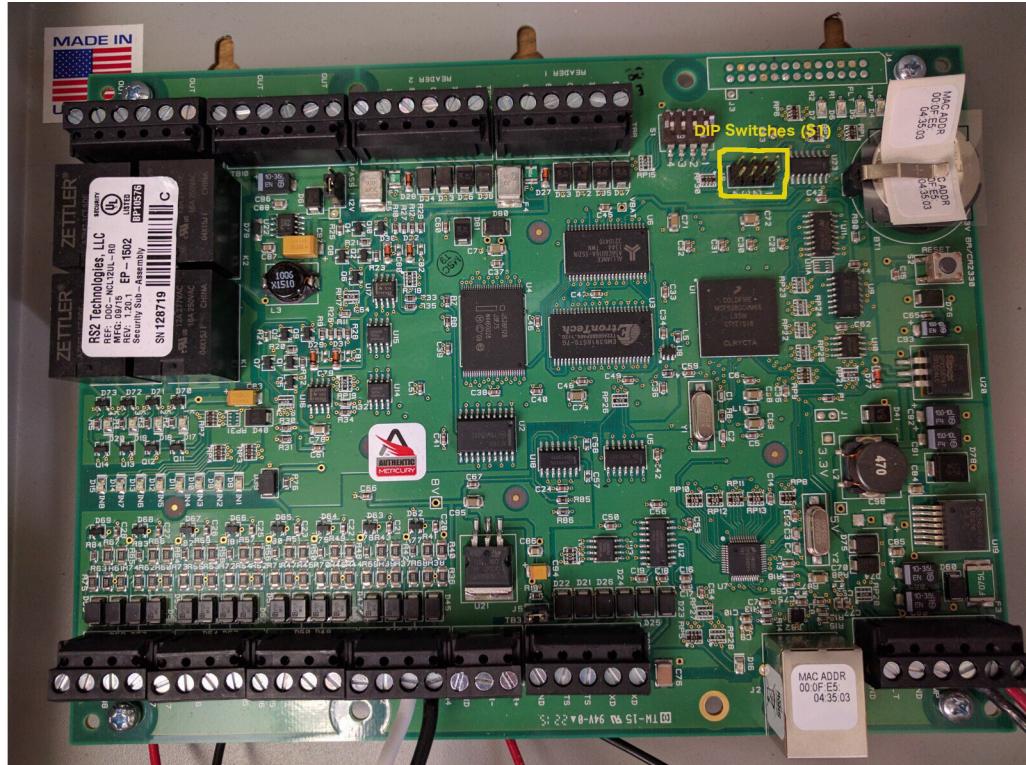
4. The two cables to the left are for positive and neutral input from a low voltage AC power supply. The ground (green) cable from the AC power supply attaches to a grounding nut on the case (pictured in the previous figure).

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

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

779 The larger EP-1502 board is pictured below:

780 **Figure 2.17 EP-1502 Door Controller Board**



781

- 782 5. The white and black wires on the bottom center of the figure go into **Door Contact 1 - IN1**,
783 and these connect to the physical door monitoring devices.
- 784 6. Power is supplied to the board via the bottom right corner posts, for 12 to 24VDC (max
785 500mA).

786 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.

- 790 1. Ensure that DIP Switch **DIP 2** is **ON** and **1, 3, & 4** are **OFF**.
- 791 2. Power on the EP-1502.
- 792 3. Manually configure a computer to **192.168.0.100**.
- 793 4. Using a crossover cable, connect the computer to the EP-1502 board.

- 794 5. Open a web browser and navigate to <http://192.168.0.251>.
- 795 6. Set DIP Switch **DIP 1 to ON**.
- 796 7. Select **Click Here to Login**.
- 797 8. Select **Continue to this website (not recommended)**.
- 798 9. Login with username: **admin** and password: **password**.
- 799 10. Select **Network** on the left-hand menu.
- 800 11. Select **Use Static IP configuration**.
- 801 a. IP Address: **172.18.3.50**
- 802 b. Subnet Mask: **172.18.0.0/16**
- 803 c. Default Gateway: **172.18.0.1**
- 804 12. Click **OK**.
- 805 13. Click **Apply Setting**.
- 806 14. Click **Apply, Reboot**.
- 807 15. Wait 60 seconds for the EP-1502 to reboot.
- 808 16. Remove power from the EP-1502.
- 809 17. Set **all DIP switches to OFF**.
- 810 18. Remove the crossover cable and connect to the network.
- 811 19. Apply power to the EP-1502 and follow the instructions in [Section 2.8.2, Post-installation and configuration](#).
- 812

813 **2.10 Radiflow 3180 (O14)**

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

817 **2.10.1 Radiflow 3180 (O14) Installation Guide**

- 818 1. Log in with the **su** user with the provided username and password.
- 819 2. Enter the following commands:
- 820 a. config terminal
- 821 b. ip access-list extended 1001
- 822 c. permit tcp host 172.16.2.170 eq 5450 host 172.18.2.150 eq 5450
823 priority 1
- 824 d. exit
- 825 e. interface fastethernet 0/1
- 826 f. ip access-group 1001 in
- 827 g. exit

```
828     h. ip access-list extended 1002
829         i. permit tcp host 172.16.2.150 eq 5450 host 172.18.2.170 eq 5450
830             priority 2
831         j. exit
832         k. interface fastethernet 0/2
833         l. ip access-group 1002 in
834         m. exit
835         n. ip access-list extended 2001
836         o. deny ip any any priority 51
837         p. exit
838         q. interface fastethernet 0/1
839         r. ip access-group 2001 in
840         s. exit
841         t. ip access-list extended 2002
842         u. deny ip any any priority 52
843         v. exit
844         w. interface fastethernet 0/2
845         x. ip access-group 2002 in
846         y. exit
847         z. write start
848     aa. reload
```

2.11 Radiflow iSID (O11)

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

2.11.1 Environment Setup

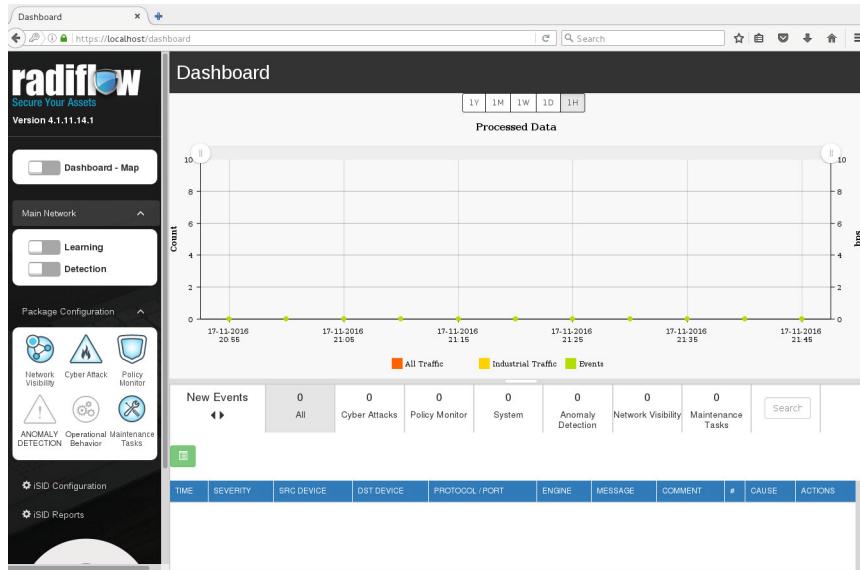
853 Radiflow supplies an OVA to be deployed to a virtualized environment, so environment setup
854 should be minimal.

2.11.2 Product Installation

- 856 1. After deploying the vendor-provided OVA on a virtualized platform, navigate to
857 **/home/radiflow/isid**.
- 858 2. Modify the **server.conf** file to reflect the IP Address of the syslog server:
859 rfids_remote_syslog_server=172.18.0.50
860 poco_source_dir=/home/radiflow/tools/poco
- 861 3. Run **sudo ./build_install_all.sh stop start install config bridge**.

862 4. Open a web browser and navigate to <https://localhost/dashboard>.

863 **Figure 2.18 Radiflow iSID Web Dashboard**



864

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

866 a. Allow learning to take place for **5-7 days**.

867 6. Toggle the **Detection** switch on the left bar under Main Network.

868 7. Setup and configuration is now complete.

869 2.12 RSA Archer Security Operations Management (E13)

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

875 For more information, visit:

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

881 2.12.1 System Requirements

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

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

888 2.12.2 Pre-Installation

889 We chose the multi-host deployment option for installing and configuring the GRC platform on
890 multiple VMs under the Microsoft Windows Server 2012R2 Operating System. The Web
891 application and services are running on one server, instance database / Microsoft SQL Server is
892 running on one server, and integration components for Security Incident Response are running
893 on a third server. Below are the pre-installation tasks that we performed prior the RSA Archer
894 installation:

- 895
 - Operating System: Windows Server 2012R2 Enterprise
 - 896 ■ Database: Microsoft SQL Server 2012 Enterprise (x64)

897 Follow Microsoft's installation guidelines and steps to install the SQL Server Database Engine
898 and SQL Server Management tools. Refer to
899 [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.

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

905 **Table 2.2 RSA Archer Configuration Settings**

Setting	Value
Collation settings set to case insensitive for instance database	SQL_Latin1_general_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: <i>grc-content</i> <i>grc-config</i>
User Account set to Database Owner role	<i>grc-content-archeruser</i> <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)

906 **Web and Services**

- 907 ■ Microsoft IIS 8
908 ■ Microsoft .NET Framework 4.5

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

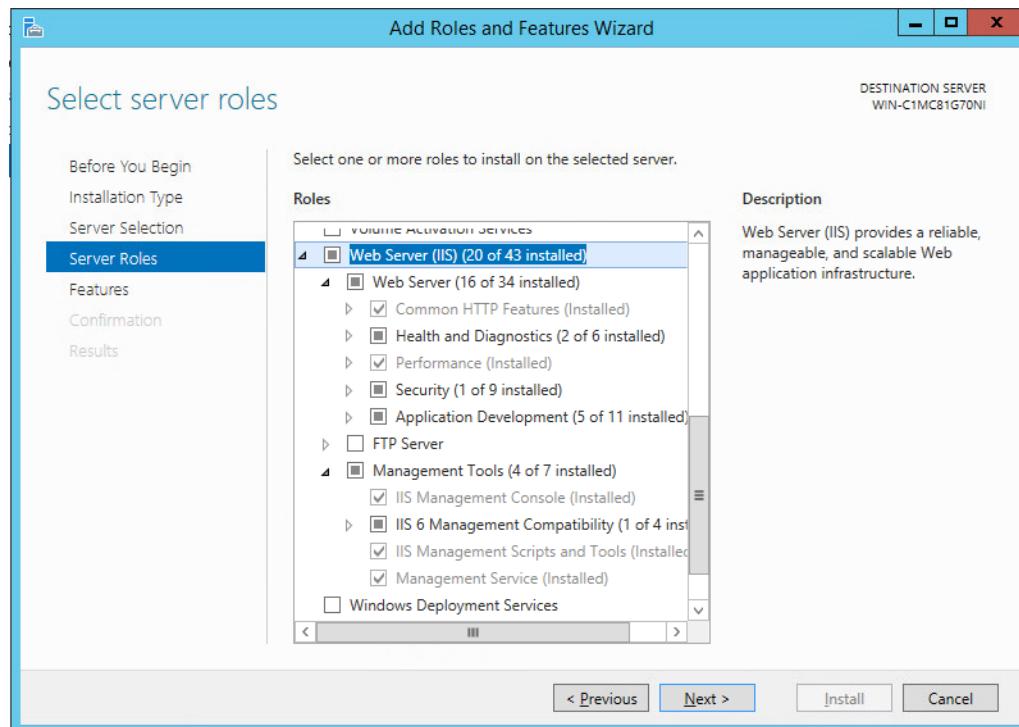
912 First install IIS and then install the .NET Framework.

913 **Table 2.3** below summarizes the required IIS components and .NET Framework features
914 followed by the screen shots.

915 **Table 2.3 IIS Components and .NET Framework**

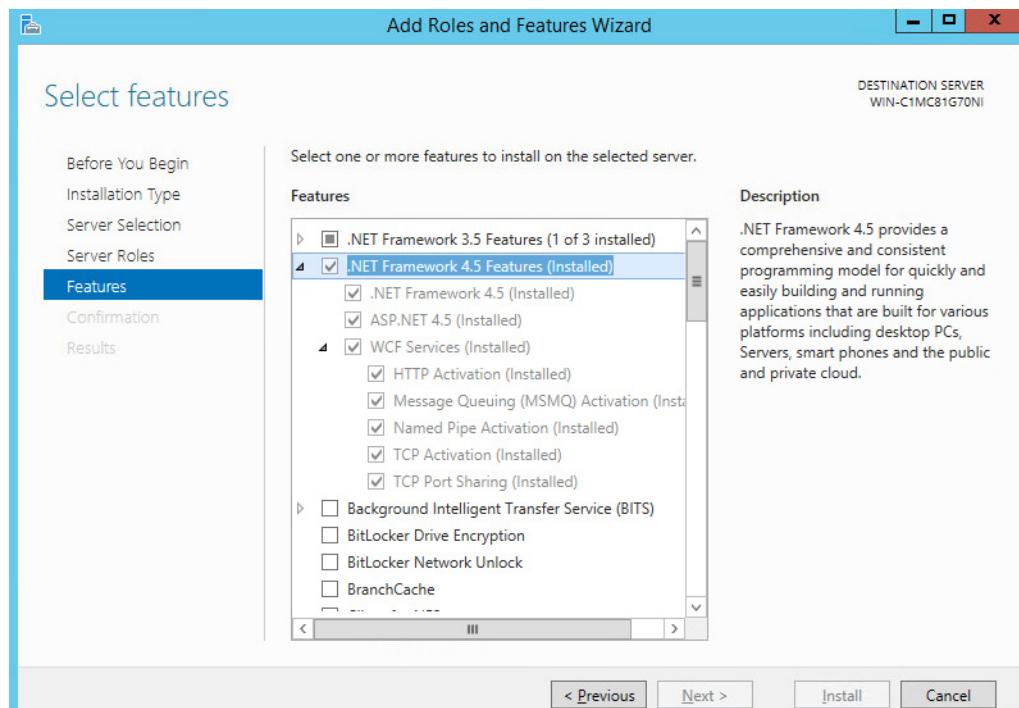
Required Option	Value
IIS	
Common HTTP Features	Default Document Directory Browsing HTTP Errors Static Content
Health and Diagnostics	HTTP Logging
Application Development	.NET Extensibility 4.5 ASP .NET 4.5 ISAPI Extensions ISAPI Filters
Security	Request Filtering
Management Tools	IIS Management Console
.NET Framework	
.NET Framework 4.5 Features	.NET Framework 4.5 ASP.NET 4.5
WCF Services	HTTP Activation TCP Port Sharing

916

Figure 2.19 Web Server (IIS) Components Section

917

918

Figure 2.20 .NET Framework 4.5 Features Selection

919

920

Microsoft Office 2013 Filter Pack

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

923 **Java Runtime Environment (JRE) 8**

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

926 Note: *All pre-installation software must be installed and configured before installing RSA Archer.*

927 **2.12.3 Installation**

- 928 1. Create folders **C:\ArcherFiles\Indexes** and **C:\ArcherFiles\Logging** (will be used later).
- 929 2. Obtain/Download the installer package from RSA; extract the installation package.
- 930 3. Run installer.
 - 931 a. Open installation folder, right-click on **ArcherInstall.exe**.
 - 932 b. Select **Run as Administrator**.
 - 933 c. Click **OK** to run the Installer.
 - 934 d. Follow the prompts from the installer for each step, set the value, and click **Next**.
 - 935 e. Select all components (Web Application, Services, Instance Database) for installation;
936 then click **Next**.
 - 937 f. Specify the X.509 Certification by selecting it from the checklist (create new cert or use
938 existing cert). We created a new cert.
 - 939 g. Set the Configuration Database options with the following properties:

940 SQL Server:	<ip address of SQL Server>
941 Login Name:	#####
942 Password:	#####
943 Database:	grc-config (this is the configuration database we created 944 during the pre-installation process)
 - 945 h. Set the Configuration Web Application options with the following properties:

946 Website:	Default Website
947 Destination Directory:	select Install in an IIS application option with RSAarcher as 948 the value
 - 949 i. Set the Configuration of the Service Credentials.
 - 950 i. Select **Use the Local System Account to Run All** from the checklist.
 - 951 j. Set the Services and Application Files paths with the following properties:
 - 952 i. Services: use the default value **C:\Program Files\RSA Archer\Services**.
 - 953 ii. Application Files: use the default value **C:\Program Files\RSA Archer**.
 - 954 k. Set the Log File Path to **C:\ArcherFiles\Logging**.

- 955 I. Perform the installation by clicking **Install**, wait for the installer to complete installing all
956 components, then click **Finish**. The RSA Archer Control Panel opens.

957 **2.12.4 Post-Installation**

958 **2.12.4.1 Configure the Installation Settings**

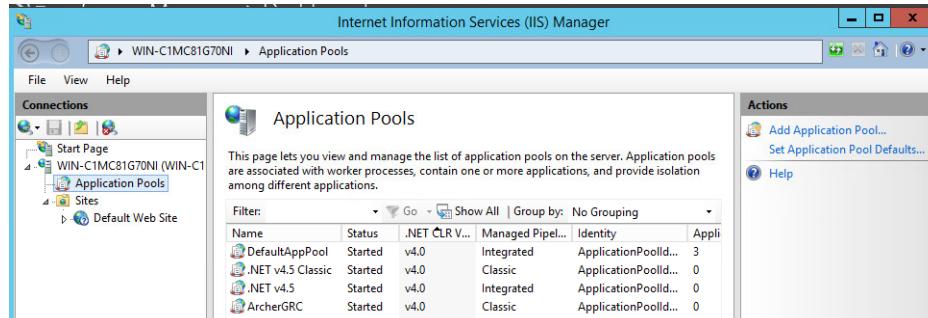
959 Verify and set the configurations for the following by clicking on **RSA Archer Control Panel >**
960 **Installation Settings**, then select corresponding sections:

- 961 1. Logging Section
 - 962 a. Path: **Archer Files\Logging**
 - 963 b. Level: **Error**
- 964 2. Locale and Time Zone Section
 - 965 a. Locale: **English (United States)**
 - 966 b. Time Zone: **(UTC-05:00) Eastern Time (US & Canada)**
- 967 3. On the Toolbar, click **Save**.
- 968 4. Create the Default GRC Platform Instance.
 - 969 a. Start the RSA Archer Queuing Service by doing the following steps:
 - 970 i. Go to **Start**.
 - 971 ii. Open **Server Manager**.
 - 972 iii. Locate **RSA Archer Queuing** in the list under the **SERVICES** section.
 - 973 iv. Right-click **RSA Archer Queuing** and click **Start**.
 - 974 b. Add a new instance by doing the following steps:
 - 975 i. Open the **RSA Archer Control Panel**.
 - 976 ii. In **Instance Management**, double-click **Add New Instance**.
 - 977 iii. Enter **SituationalAwareness** as the **Instance Name**, then click **Go**.
 - 978 iv. Complete the properties as needed.
 - 979 c. Configure the Database Connection Properties by doing the following steps:
 - 980 i. Open the RSA Archer Control Panel.
 - 981 ii. In the **Database** tab, go to the **Connection Properties** section.
 - 982 iii. In **Instance Management**, double-click the **SituationalAwareness** instance.
 - 983 d. In the **Database** tab, set up the following:
 - 984 i. SQL Server: **<ip address of SQL Server>**
 - 985 ii. Login name: **xxxxxx**
 - 986 iii. Password: **xxxxxx**
 - 987 iv. Database: **grc-content**

- 988 5. Click on the **Test Connection** link to make sure the **Success** message appears.
- 989 6. Configure the **General Properties** by doing the following steps:
 - 990 a. Open **RSA Archer Control Panel**.
 - 991 b. Go to **Instance Management**.
 - 992 c. Under **All Instances**, click on **SituationalAwareness**.
 - 993 d. In the **General** tab, set up the following:
 - 994 i. **File Repository** section - Path **C:\ArcherFiles\Indexes**.
 - 995 ii. **Search Index** section - **Content Indexing**: Check on Index design language only; Path: **C:\ArcherFiles\Indexes\SituationalAwareness**
- 997 7. Configure the **Web Properties** by doing the following steps:
 - 998 a. Open the **RSA Archer Control Panel**.
 - 999 b. Go to **Instance Management**.
 - 1000 c. Under **All Instances**, click on **SituationalAwareness**.
 - 1001 d. In the **Web** tab, set up the following:
 - 1002 i. Base URL: **http://localhost/RSAArcher/**
 - 1003 ii. Authentication URL: **default.aspx**
- 1004 8. Change **SysAdmin** and **Service Account** passwords by doing the following steps:
 - 1005 a. Open the **RSA Archer Control Panel**.
 - 1006 b. Go to **Instance Management**.
 - 1007 c. Under **All Instances**, click on **SituationalAwareness**.
 - 1008 d. Select the **Accounts** tab.
 - 1009 e. Change the password on the page by using a strong password.
 - 1010 f. Complete the Default GRC Platform Instance Creation by clicking **Save** on the toolbar.
- 1011 9. Register the Instance by doing the following steps:
 - 1012 a. Open the **RSA Archer Control Panel**.
 - 1013 b. Go to **Instance Management**.
 - 1014 c. Under **All Instances**, right-click on **SituationalAwareness**.
 - 1015 d. Select **Update Licensing**, enter the following information, then click on **Active**:
 - 1016 i. **Serial Number** (obtained from RSA)
 - 1017 ii. **Contact Info** (First Name, Last Name, Company, etc.)
 - 1018 iii. **Activation Method** (select Automated)
- 1019 10. Activate the Archer Instance by doing the following steps:
 - 1020 a. Start the **RSA Archer Services**.
 - 1021 b. On **Server Manager**, go to **Local Services** or **All Services**.

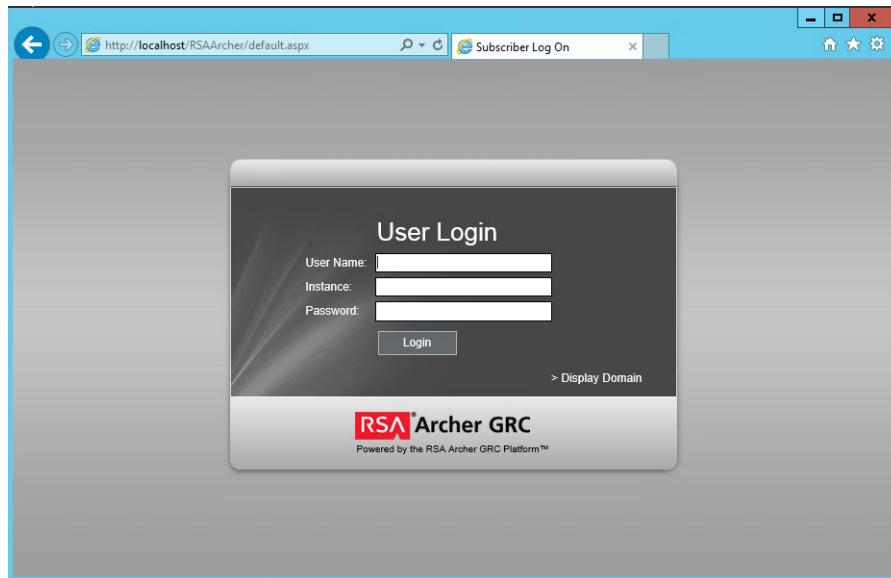
- 1022 c. Locate the following services, right-click on each service, and click **Start**.
- 1023 i. **RSA Archer Configuration**
- 1024 ii. **RSA Archer Job Engine**
- 1025 iii. **RSA Archer LDAP Synchronization**
- 1026 d. Restart the **RSA Archer Queuing Service**.
- 1027 i. Open **Server Manager**.
- 1028 ii. Go to **Local Services** or **All Services**.
- 1029 iii. Locate the **RSA Archer Queuing**.
- 1030 iv. Right-click on **RSA Archer Queuing** and click **Restart**.
- 1031 e. Rebuild the Archer Search Index.
- 1032 i. Open **RSA Archer Control Panel**.
- 1033 ii. Go to **Instance Management**.
- 1034 iii. Under **All Instances**, right-click on **SituationalAwareness**, then click on **Rebuild Search Index**.
- 1036 11. Configure and activate the Web Role (IIS).
- 1037 a. Set up **Application Pools** as shown in the screen shot.
- 1038 i. Open **Server Manager**.
- 1039 ii. Navigate to **Tools > IIS Manager > Application Pools** (in the left side bar).
- 1040 iii. Right-click to add applications (.NET, ArcherGRC, etc.), example screen shot below.

Figure 2.21 Application Pools



- 1043 b. Restart IIS.
- 1044 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.

1047

Figure 2.22 RSA Archer User Login

1048

1049

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

1050

Figure 2.23 Security Operations Management Tab

Incident ID	Title	Incident Summary	No. of Aggregated Alerts	Priority
INC-212222	An account failed to log on	Failed grouped by 192.168.227.192 - 192.168.227.103	1	P-1
INC-212223	Connector Active	Connector Active	1	P-2
INC-212234	Sec Ops Test	Sec Ops Test grouped by source IP 192.168.227.192	1	P-2
INC-212235	RSA-SecOps	RSA-SecOps	3	P-2
INC-212222	Login - Brute Force Login Attempts from a Single Source	Login - Brute Force Login Attempts from a Single Source grouped by source IP 192.168.227.101	1	P-3

1051

1052 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 multi-host 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.

- 1062 2. Execute Archer Unified Collector Framework installer. When prompted, provide the Archer
1063 Collector Framework Web Services username and password created in step 1.

1064 3. When prompted, follow the instructions for importing the Data Feed for the Unified
1065 Collector Framework (UCF).

1066 2.12.6 Additional ArcSight Integration Configuration

1067 Additional details for the ArcSight Installation can be found in the RSA Archer Security
1068 Operations Management Implementation Guide from RSA. Below are the steps that were
1069 followed specifically for this environment to enable the connection to ArcSight.

- 1070 1. Create ArcSight Forwarding Connector User.

1071 a. From **ArcSight ESM Console**:
1072 i. Create a new group under custom user groups and name as follows: **FwdConnector**
1073 ii. Create a new user under that group and name as follows: **FwdConnectorUser**
1074 iii. Set the user type to: **Forwarding Connector**
1075 iv. For additional detail, see page 7-9 of FwdConn_ConfigGuide_7.0.7.7286.0.pdf

1076 2. Install **SuperConnector** (AKA, Forwarding Connector).

1077 a. From the **ArcSight ESM Manager command line**:
1078 i. Su to **arcsight** user
1079 ii. Find the install file **ArcSight-7.0.7.7286.0-Superconnector.bin** and run the following
1080 command (in order to allow the install to execute):
1081 chmod + x ArcSight-7.0.7.7286.0-Superconnector.bin
1082 iii. Make a folder for the connector:
1083 e.g., mkdir /opt/arsight/superconnector
1084 iv. As **arcsight** user execute the installation file:
1085 ./ArcSight-7.0.7.7286.0-Superconnector.bin
1086 v. Choose to install to the folder that you just made:
1087 e.g., /opt/arcsight/superconnector
1088 vi. Accept defaults.
1089 vii. Choose **Don't Create Links**.
1090 viii. **Install**.
1091 ix. **Next**.
1092 x. Enter the ArcSight ESM Manager name: **[hostname]**
1093 xi. Enter the ArcSight ESM Manager port: **8443**
1094 xii. Enter the name of the user you just created: **FwdConnectorUser**
1095 xiii. Enter the ArcSight Manager password: _____

1096 xiv. Import the manager certificate.
1097 xv. Select **CEF Syslog**.
1098 xvi. Enter the IP address of the RSA Archer UCF IP, Port: **514, TCP** (not UDP)
1099 xvii. Select **Next** twice, **Exit, Done**.
1100 xviii. As user **root**, install the service as follows:
1101 /opt/arcsight/superconnector/current/bin/arcsight agentsvc -i
1102 -u arcsight
1103 xix. Start the service as follows:
1104 ./etc/init.d/arc_superagent_ng start

1105 Note: *If you need to add another forwarding destination, see page 32 of*
1106 *FwdConn_ConfigGuide_7.0.7.7286.0.pdf.*

1107 2.12.7 Sample Use Case Demonstration

1108 For the use of the Security Incident Response use case and integration with ArcSight, the
1109 following sample use case was simulated:

1110 1. Event 1

1111 An individual enters a substation, and event that is detected by a door controller. This door
1112 reader is able to log its data or a SIEM, such as ArcSight, including identifying information
1113 (such as a Badge ID or user)

1114 2. Event 2

1115 A new device appears on the substation network, detected by a tool (for example,
1116 CyberLens). This data is reported via a log event to a SIEM such as ArcSight.

1117 3. Action 1:

1118 An Alert/Correlation Rule appropriate for these events fires in ArcSight, triggering message
1119 delivery to RSA Archer Security Incident Response for review and possible action.

1120 Below are screen shots and narratives of this sample use case within the RSA Archer
1121 Security Operations Management Use Case.

1122 1. User is logged into the Archer Interface, and is examining the Security Alerts that have been
1123 delivered for review.

1124

Figure 2.24 Multiple Security Alerts within the RSA Archer Console

The screenshot shows the RSA Archer GRC interface with the title bar "RSA® Archer® GRC". The main menu includes "Enterprise Management", "Security Operations Management", "Incident Management", "Threat Management", "Business Continuity Management", and "Administration". The "Incident Response" section is expanded, showing "Security Incidents" with various filters like "Search Records", "New Record", "Records", "By Escalation Owner", "By Incident Owner", "By Incident Status", "By Method of Detection", "By Threat Category", "Reports", "Security Events", and "Search Results". The "Security Alerts" section is active, displaying a list of alerts with columns: "Archer Tracking ID", "Alert Timestamp", "Alert Name", "Source", "Security Alert Priority", and "Related Security Incident". There are 20 alerts listed, each with a unique tracking ID and timestamp ranging from 7/16/2016 11:59 AM to 7/16/2016 2:53 AM. The priority column shows P-3 for most alerts, except for one at P-1. The "Related Security Incident" column lists incidents such as INC-295667, INC-295662, INC-295661, INC-295660, INC-295659, INC-295658, INC-295657, INC-295656, INC-295655, INC-295654, INC-295653, INC-295652, INC-295651, INC-295650, INC-295649, INC-295648, INC-295647, INC-295646, INC-295645, INC-295644, INC-295643, INC-295642, INC-295641, and INC-295640. A tooltip for INC-295640 indicates "Control Panel to activate Windows". The bottom right corner shows a battery icon at 95%.

1125

1126
1127

Figure 2.25 Sample Message from ArcSight, showing raw log message/alert and parsing with normalization

The screenshot shows the RSA Archer GRC interface with the title bar "RSA® Archer® GRC". The main menu and navigation menu are similar to Figure 2.24. The "Security Alerts" section is active, showing a detailed view for "Security Alert: 295650". The "Alert Summary" tab is selected, displaying information like "Created On: 7/16/2016 6:42 PM", "Archer Tracking ID: 295650", "Alert Name: RSA-SetOps", "Source: ArcSight", "Alert Timestamp: 7/16/2016 2:53 AM", "Security Alert Priority: P-3", and "Severity Level: 0". The "Alert Metadata" tab is also visible. A large raw alert message is displayed below, containing complex log entries and normalization details. A tooltip for INC-295640 indicates "Control Panel to activate Windows". The bottom right corner shows a battery icon at 95%.

1128

1129

Figure 2.26 Sample message showing alert indicating new device detected at substation

The screenshot shows the RSA Archer GRC interface with the title bar "RSA® Archer® GRC". The main menu and navigation menu are similar to previous figures. The "Security Alerts" section is active, showing a detailed view for "Security Alert: 295666". The "Alert Summary" tab is selected, displaying information like "Created On: 12/20/2016 11:00 AM", "Archer Tracking ID: 295666", "Alert Name: Substation-new-device-detection", "Source: CyberLens", "Alert Timestamp: 12/20/2016 11:00 AM", "Security Alert Priority: P-3", "Number of Aggregated Security Events: 0", and "Severity Level: 1". The "Alert Metadata" tab is also visible. A large raw alert message is displayed below, containing log entries related to a new device detection at a substation. A tooltip for INC-295661 indicates "Control Panel to activate Windows". The bottom right corner shows a battery icon at 95%.

1130

1131

Figure 2.27 Sample message showing an alert indicating badged entry detected at substation

The screenshot shows the RSA Archer GRC interface. The top navigation bar includes links for Preferences, Reports, Help, Logout, and Search Incident Response. The main title is "Enterprise Governance, Risk and Compliance". The left sidebar has a "Navigation Menu" with sections like Administration, Incident Response, Security Incidents, Security Alerts, Security Events, Incident Investigations, Forensic Analysis, Incident Response Procedures, Incident Journal, Data Breach Response, Data Sources, and Batch Tasks. The main content area is titled "Security Alerts: 295665" and shows a single alert record. The alert summary details include: Created On: 12/26/2016 10:26 AM, Source: ArcSight, Alert Timestamp: 12/26/2016 12:00 AM, Security Alert Priority: P-3, Alert Name: Substation-entry-detection, Severity Level: 1. The alert metadata section shows Alert Category: RuleFire, Alert Action: None, Host: manual-national.arcsight, Raw Alert: CEF 1|ArcSight|ArcSight|8.0.1896.0|0|RSA-SecOps|Notification|RS2Open-close event|0203948|smith, and Service Type: notification.

1132

2. Based on rule or physical examination, these alerts are deemed Incident Investigation material and instantiate a full Incident Response Workflow.

1133

1134

Figure 2.28 New incident response workflow record started, documented with Title, Summary, Details

The screenshot shows the RSA Archer GRC interface. The top navigation bar includes links for Preferences, Reports, Help, Logout, and Search Incident Response. The main title is "Enterprise Governance, Risk and Compliance". The left sidebar has a "Navigation Menu" with sections like Administration, Incident Response, Security Incidents, Security Alerts, Security Events, Incident Investigations, Forensic Analysis, Incident Response Procedures, Incident Journal, Data Breach Response, and Data Sources. The main content area is titled "Security Incidents: INC-295667" and shows a new incident record. The incident summary details include: Incident ID: INC-295667, Title: Correlation Event - Multiple notifications from the ICS and physical security systems, Incident Summary: Physical Entry and introduction of new equipment into a substation detected within a defined period of time, and Incident Details: Based on rules that have been configured on the SIEM, a badged entry into a substation was detected, and within X hours a new device was detected in the same substation as detected by CyberLens. These events within a certain timeframe require additional examination for validity. The incident status section shows Threat Category: , Threat Actor: , Threat Vector: , Target Asset Type: , Threat Valid: Unknown.

1135

1136

Figure 2.29 Incident record alerts tab, showing the association of two events attached to this incident response investigation record

The screenshot shows the RSA Archer GRC interface. The top navigation bar includes links for Preferences, Reports, Help, Logout, and Search Incident Response. The main title is "Enterprise Governance, Risk and Compliance". The left sidebar has a "Navigation Menu" with sections like Administration, Incident Response, Security Incidents, Security Alerts, Security Events, Incident Investigations, Forensic Analysis, Incident Response Procedures, Incident Journal, Data Breach Response, and Data Sources. The main content area is titled "Security Incidents: INC-295667" and shows the alerts tab. It lists two events: 295665 (Alert Name: Substation-entry-detection, Alert Timestamp: 12/26/2016 12:00 AM, Security Alert Priority: P-3, Source: ArcSight) and 295666 (Alert Name: Substation-new-device-detection, Alert Timestamp: 12/26/2016 11:00 AM, Security Alert Priority: P-3, Source: CyberLens). The bottom right corner of the screen shows a message: "Activate Windows Go to System in Control Panel to activate Windows."

1137

1138

1139

3. 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

1143 procedure(s) outlines and maintained by an organization's security policy program and
 1144 response.

1145 **Figure 2.30 Incident response procedure with two related tasks assigned to the incident
 1146 response record**

The screenshot shows the RSA Archer GRC interface. The top navigation bar includes 'Enterprise Management', 'Security Operations Management', 'Incident Management' (selected), 'Threat Management', 'Business Continuity Management', and 'Administration'. The main content area is titled 'Security Incidents: INC-29567'. It displays an 'About' section and a table for 'Incident Response Procedures'. The table has columns for 'Tracking ID', 'Procedure Name', 'Description', 'Tasks Completed', and 'Incident Response Tasks'. One row is shown with tracking ID 'IRP-295672', procedure name 'New Device Detection and Validation', description 'Steps to be followed to validate new equipment detected as a substitution. Task is triggered based on badged entry followed by new device detection within X hours', tasks completed '2/2', and incident response tasks 'IRI-295672, IRI-295674'. Below the table is a section for 'Not Applicable Incident Response Procedures'. A status bar at the bottom right indicates 'Activate Windows' and 'Go to System in Control Panel to activate Windows'.

1147

1148 **Figure 2.31 Incident response tasks with status, details, and completion status**

This screenshot shows the 'Incident Response Procedures: IRP-295672' page. The left sidebar has a 'Navigation Menu' with 'Incident Response' selected. The main content area shows 'General Information' for the procedure and a table for 'Incident Response Tasks'. The table columns are 'Tracking ID', 'Step Number', 'Task Name', 'Required/Optional', 'Analyst Name', 'Task Status', and 'Analyst Note'. Two tasks are listed: 'IRI-295672' (Step 1.00, Task Name 'Work Order Validation', Required, Analyst 'Administrator, System', Status 'Completed') and 'IRI-295674' (Step 2.00, Task Name 'User and Hardware Validation', Required, Analyst 'Administrator, System', Status 'Completed'). A status bar at the bottom right indicates 'Activate Windows' and 'Go to System in Control Panel to activate Windows'.

1149

1150 **2.13 Schneider Electric Tofino Firewall (O3, O18, O20)**

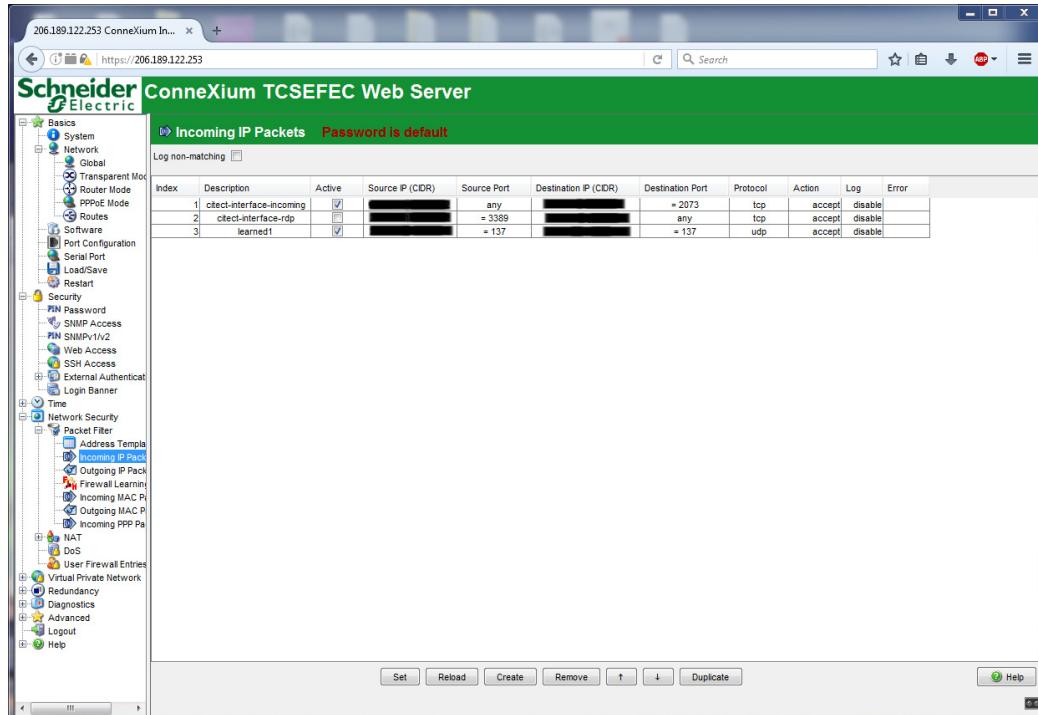
1151 Schneider Electric Tofino Firewalls are used in multiple points throughout the build, supplying
 1152 the necessary protection for network devices, including the door controller, the TDI
 1153 ConsoleWorks operations management instance, and the connection between the OSISoft
 1154 Citect connector and the SCADA server.

1155 **2.13.1 Schneider Electric Tofino Firewall (O3) Installation Guide**

- 1156 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**.
- 1157 2. For Login-Type, select **Administration**, then select **OK**.

- 1160 3. From the menu on the left, select **Network Security -> Packet Filter -> Incoming IP Packets**.
1161 This is where the firewall rules will be created.
- 1162 4. Click the **Create** button on the bottom of the main window.
- 1163 5. Fill in the text fields for **Description, Source IP (CIDR), Source Port, Destination IP (CIDR),**
1164 **Destination Port, Protocol, Action Log, and Error** according to the rules needed for
1165 incoming packets.

1166 **Figure 2.32 Incoming Packet Configuration**



- 1167 6. From the menu on the left, select **Network Security -> Packet Filter -> Outgoing IP Packets**.
1168 7. Follow the previous steps to create outgoing firewall rules.

1170

Figure 2.33 Outgoing Packet Configuration

The screenshot shows the ConneXium TCSEFEC Web Server interface. The left sidebar has a tree view with nodes like Basics, Network, Security, and Network Security. The main panel title is "Outgoing IP Packets". A table lists five entries:

Index	Description	Active	Source IP (CIDR)	Source Port	Destination IP (CIDR)	Destination Port	Protocol	Action	Log	Error
1	cfect-interface-outgoing	<input checked="" type="checkbox"/>	[REDACTED]	= 2073	[REDACTED]	any	tcp	accept	enable	
2	cfect-interface-rdp	<input checked="" type="checkbox"/>	[REDACTED]	any	[REDACTED]	= 3389	tcp	accept	enable	
3	learned1	<input checked="" type="checkbox"/>	[REDACTED]	= 138	[REDACTED]	= 138	udp	accept	enable	
4	learned2	<input checked="" type="checkbox"/>	[REDACTED]	= 137	[REDACTED]	= 137	udp	accept	enable	
5	learned3	<input checked="" type="checkbox"/>	[REDACTED]	= 137	[REDACTED]	= 137	udp	accept	enable	

Buttons at the bottom include Set, Reload, Create, Remove, and Duplicate.

1171

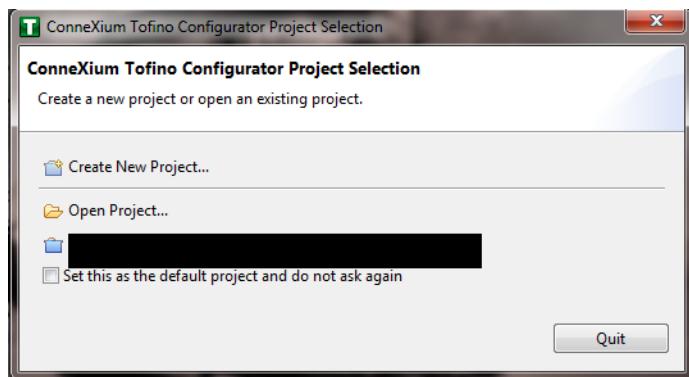
- 1172 8. If necessary, configure the interface IP addresses from the menu on the left by selecting
1173 **Basics -> Network -> Transparent Mode.**

1174 2.13.2 Schneider Electric Tofino Firewall (O18) Installation Guide

1175 Install and Configure the Schneider Tofino Firewall:

- 1176 1. Download the ConneXium software from the Schneider site as stated in the instructions
1177 accompanying the firewall, then start the ConneXium Tofino Configurator.
1178 2. In the startup screen, click **Create New Project...**

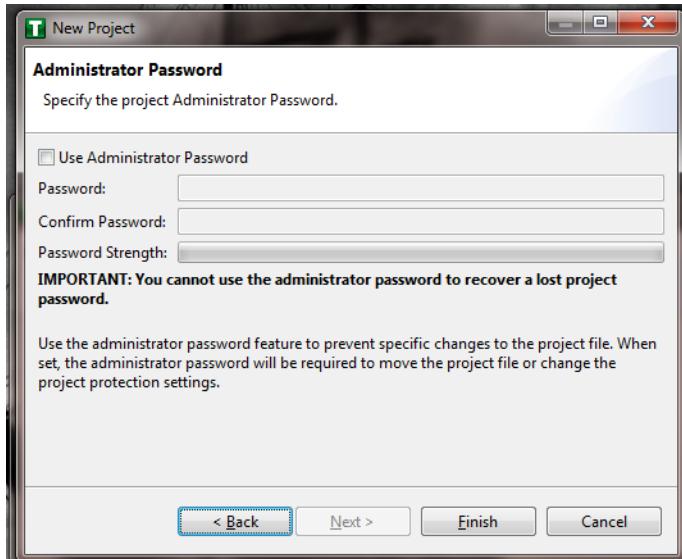
1179

Figure 2.34 Create New Project

1180

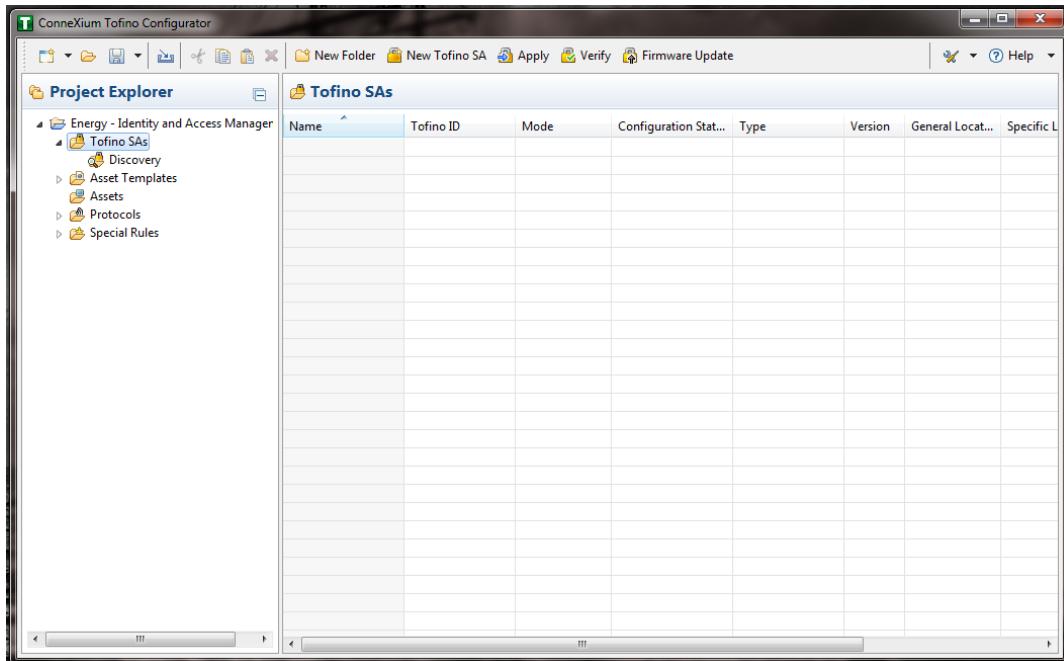
- 1181 3. Enter the name you would like to use for the project in the **Project name** field, and the
1182 company name in the **Company** field, then click **Next**.
- 1183 4. In the Project Protection screen, choose a password to protect the project, then click **Next**.

1184 **Figure 2.35 Administrator Password**



- 1185 5. In the Administrator Password screen, choose the administrator password, then click **Finish**.
- 1186 6. In the Project Explorer window, right-click **Tofino SAs** and select **New Tofino SA**. You can
1187 also choose to create a folder for the SAs to help organize multiple areas.

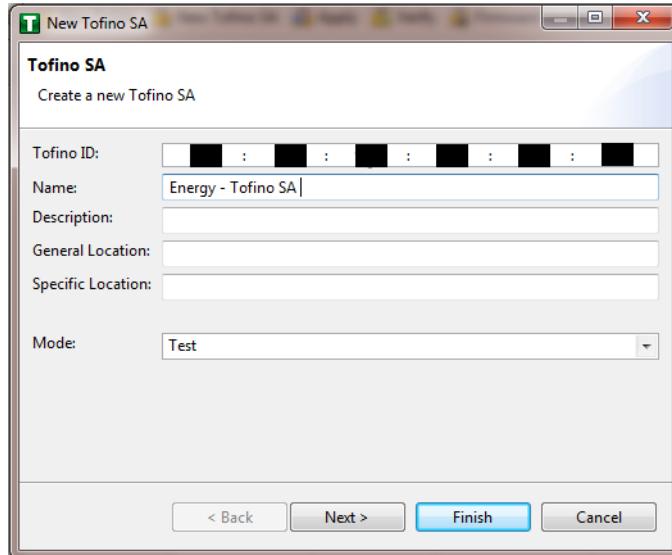
1188 **Figure 2.36 Project Explorer Window**



1190

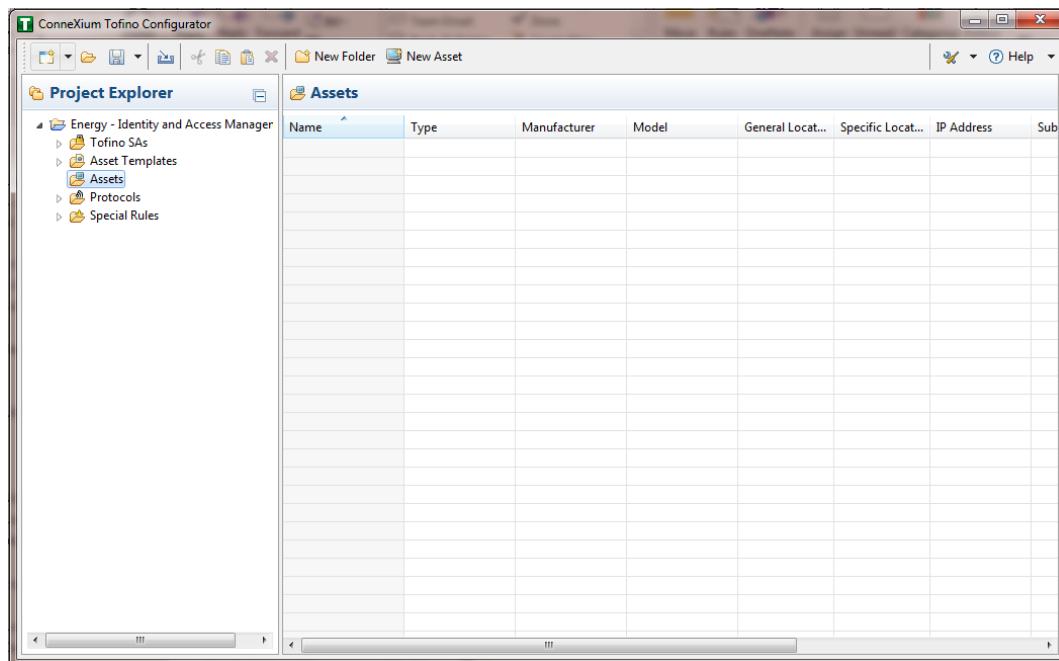
- 1191
1192 7. In the **Tofino ID** field, enter the MAC address listed on the firewall hardware sticker. Fill out the rest of the fields as necessary, then click **Finish**.

1193 **Figure 2.37 Tofino SA/MAC Address**



1194

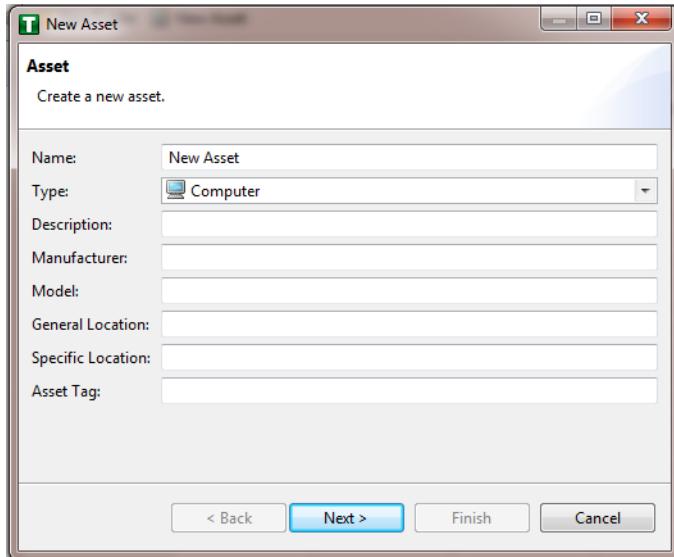
1195 **Figure 2.38 Project Explorer**



1196

- 1197 8. Right-click on the **Assets** icon in the Project Explorer frame, then click **New Asset**.
- 1198 9. In the New Asset window, set the name and type of the device, and all other fields as necessary, then click **Next**.
- 1199

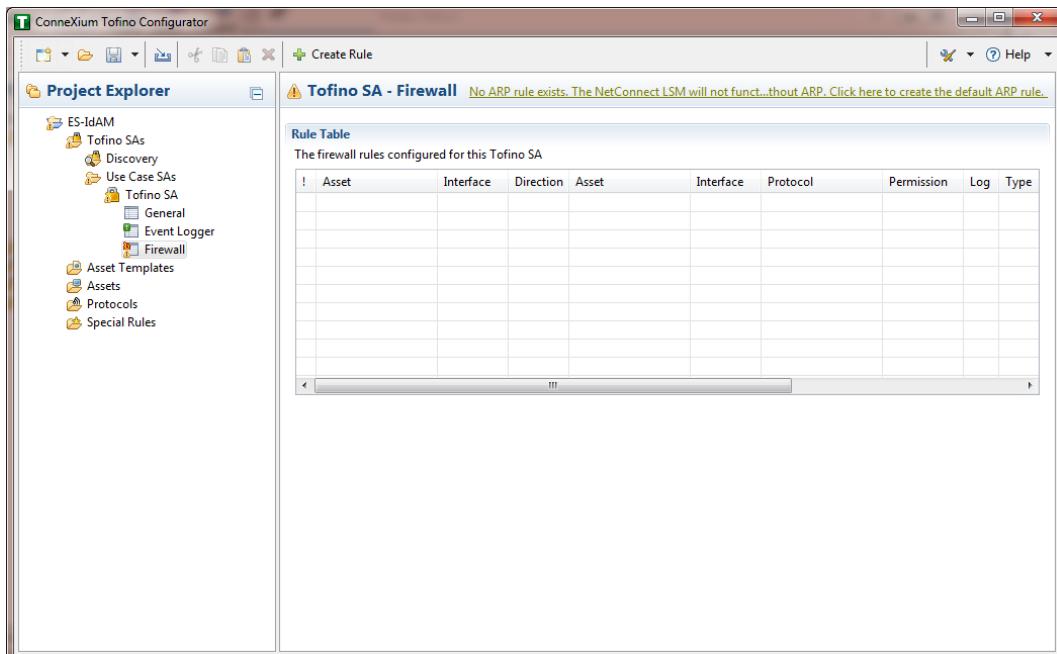
1200

Figure 2.39 New Asset

1201

- 1202 10. Fill in the **IP address** and/or the **MAC address** fields, then click **Finish**.
- 1203 11. Repeat for all devices on the network. When they are configured, click on the **Assets** icon in
- 1204 the Project Explorer frame (if it is not already selected). There should be a list of all
- 1205 configured assets.
- 1206 12. Under the Project Explorer frame, click the **dropdown arrow** next to Tofino SAs, then
- 1207 choose the SA created earlier. From there, click **Firewall** in the Project Explorer frame to
- 1208 display current firewall rules. This should currently be empty.

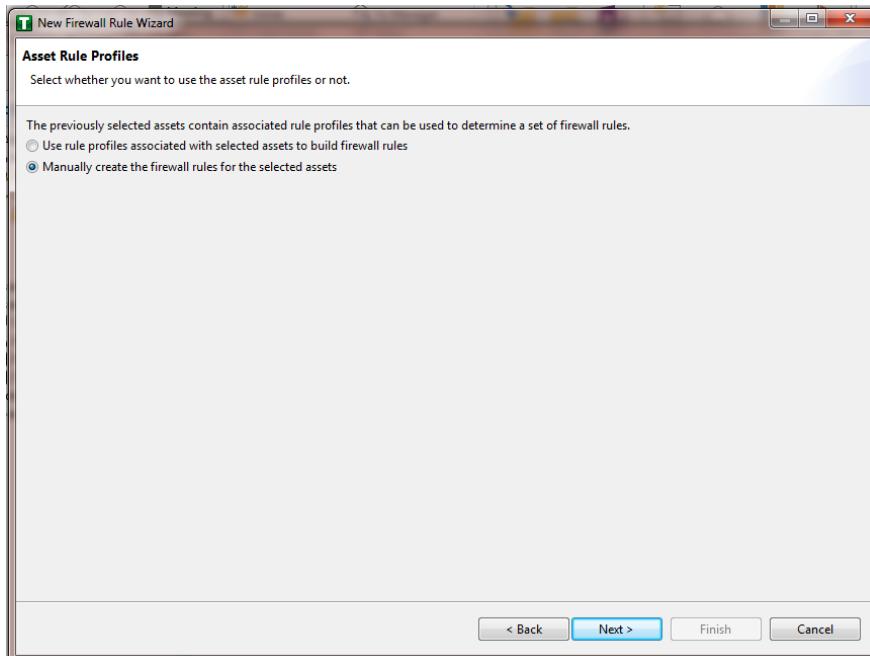
1209

Figure 2.40 Project Explorer Tofino SA Icon

1210

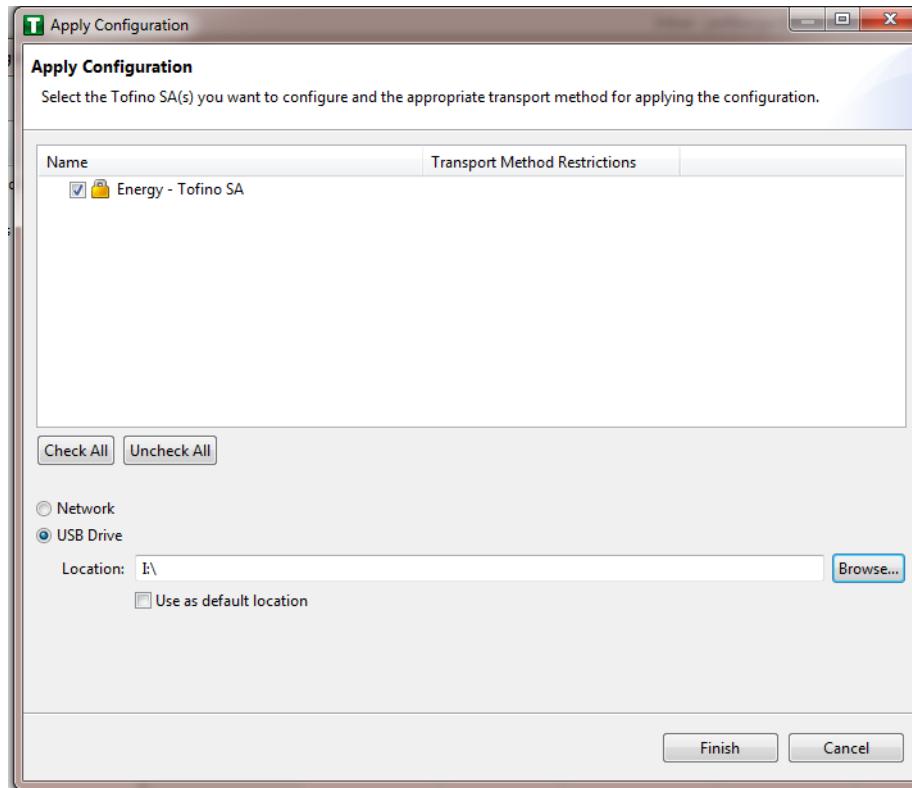
- 1211 13. To create the first rule, click the **+ Create Rule** button above the Tofino SA-Firewall title.
1212 Then, ensure the **Standard rule** radio button is selected and click **Next**.
- 1213 14. On the next screen, choose the interface for **Asset 1**. This is where traffic originates before
1214 going into the device.
- 1215 a. Select a source asset and a destination asset from the radio buttons below. Set the
1216 direction of the traffic using the arrow buttons in the middle. When finished, select
1217 **Next**.
- 1218 15. In the Asset Rule Profiles window, select the **Manually create the firewall rules for the**
1219 **selected assets** radio button, then click **Next**.

1220 **Figure 2.41 Asset Rule Profiles**



- 1221 16. On the Protocol screen, choose the protocol to be checked against. Then choose the
1222 **Permission** on the right side of the screen, as well as whether or not to log, then click
1223 **Finish**.
- 1224 17. After these steps are completed, the firewall rule should be listed in the **Rule Table**.
- 1225 18. Repeat steps for the remainder of the rules needed.
- 1226 19. Finally, click the **Save** button on the menu bar.
- 1227 20. Place a FAT/FAT32 formatted USB device into the computer running the ConneXium Tofino
1228 Configurator, then right-click **Tofino SAs** in the Project Explorer pane and select **Apply**. If the
1229 project asks you to save, click **OK**.

1231

Figure 2.42 Apply Configuration Pane

1232

- 1233 21. In the Apply Configuration pane, ensure that your SA is selected in the table at the top, and
1234 the **USB Drive** radio button is selected. Browse to the top-level directory of your USB drive,
1235 then click **Finish**.
- 1236 22. A popup will notify you of successful completion.
- 1237 23. Ensure the firewall has been powered on and has been running for at least one minute,
1238 then plug the USB device used to copy the Tofino configuration to into the USB port on the
1239 back of the firewall.
- 1240 24. Press the **Save/Load/Reset** button twice, setting it to the **Load** setting (Pressing once
1241 should turn the indicator light to green, pressing it again will change it from green to
1242 amber). After a few seconds, the device will begin displaying lights that move from right to
1243 left across the LEDs on the back, indicating the configuration is being loaded.
- 1244 25. Once the lights stop moving right to left, wait a few seconds to ensure that the **Fault** LED
1245 does not light up. Then remove the USB drive and place it back into the computer running
1246 the ConneXium Tofino Configurator software.
- 1247 26. Right-click **Tofino SAs** in the Project Explorer pane and select **Verify**.
- 1248 27. At the Verify Loaded Configuration window, select the **Tofino SA** in the table, and select the
1249 **USB Drive** radio button. Then select the USB drive using the **Browse** button. Finally, click
1250 **Finish**.
- 1251 28. A popup will notify you of successful verification, and configuration is complete.

2.13.3 Schneider Electric Tofino Firewall (O20) Installation Guide

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

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)
- 4GB RAM
- 4 cores
- 200GB 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 The **Select Database Owner** dialog 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.

- 1285 9. Click **OK**.
- 1286 10. [Optional] Further configure the database (such as the recovery model) as required based
1287 on the chosen database back-up strategy. For more information, contact the local Database
1288 Administrator (if available) or visit the Microsoft Developer Network website
1289 (<https://msdn.microsoft.com/en-us/library/bb545450>).
- 1290 11. Click **OK**.
- 1291 12. In Object Explorer, expand the **Security** folder, followed by **Logins**.
- 1292 13. Right-click the desired Windows domain account, and then click **Properties**. The **Login**
1293 **Properties** dialog box will appear.
- 1294 14. Under **Default database**, select the **CROSSBOW** database, then click **OK**.
- 1295 15. Execute the following scripts in order:
- 1296 a. Crossbow_db_create.sql
- 1297 b. Crossbow_db_functions.sql
- 1298 c. Crossbow_db_initial_data.sql
- 1299 d. Crossbow_db_scripts.sql
- 1300 e. Crossbow_db_client_queries.sql

1301 **2.14.2.2 Installing CROSSBOW Server and Services**

- 1302 1. Contact Siemens Customer Support and obtain a compressed zip file containing the latest
1303 CROSSBOW Server installer for RUGGEDCOM CROSSBOW v4.4.
- 1304 2. Open the compressed zip file and double-click **Server Strong Setup.msi**. The CROSSBOW
1305 Server with Strong Authentication Setup installation wizard will appear.
- 1306 3. Follow the on-screen instructions to install CROSSBOW Server.

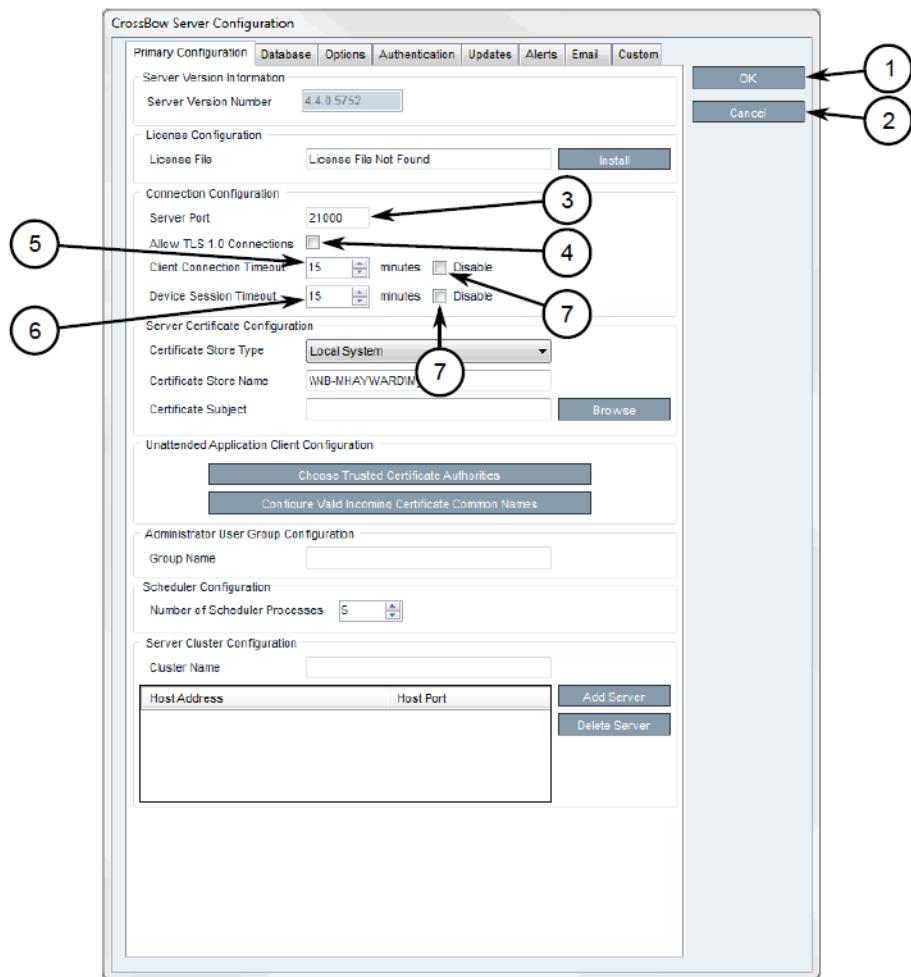
1307 **2.14.2.3 Configuring Server Host Connection**

- 1308 1. Access the RUGGEDCOM CROSSBOW server and launch CROSSBOW Server.
- 1309 2. Make sure the **CROSSBOW Main Server** service is **stopped**.
- 1310 3. Under **CrossBow Main Server**, click **Configure**. The CROSSBOW Server Configuration dialog
1311 box will appear.

1312

Figure 2.43 CrossBow Server Configuration

1313



1314

1. OK Button

1315

2. Cancel Button

1316

3. Server Port Box

1317

4. Allow TLS 1.0 Connections Check Box

1318

5. Client Connection Timeout Box

1319

6. Device Session Timeout Box

1320

7. Disable Check Box

1321

*4. On the Primary Configuration tab, under **Connection Configuration**, type the TCP port number 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.*

1322

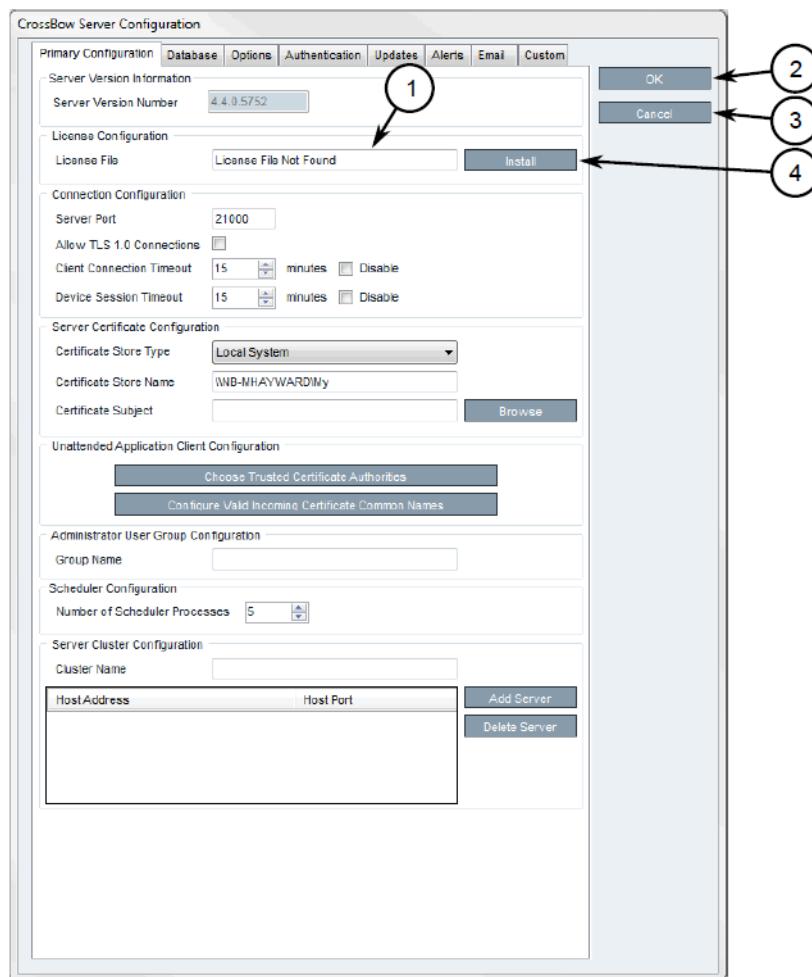
*5. In the **Client Connection Timeout** field, type or select the maximum amount of time (in minutes) for the server to wait before disconnecting an inactive client. To disable this feature, select **Disable**.*

- 1327 6. In the **Device Session Timeout** field, type or select the maximum amount of time (in
1328 minutes) for the server to wait before disconnecting an inactive remote device. To disable
1329 this feature, select **Disable**.
- 1330 7. Click **OK** to save changes.
- 1331 8. Start the CROSSBOW Main Server service

1332 2.14.2.4 Installing a License File

- 1333 1. Access the RUGGEDCOM CROSSBOW server and launch CROSSBOW Server.
- 1334 2. Make sure the **CROSSBOW Main Server** service is **stopped**.
- 1335 3. Under **CrossBow Main Server**, click **Configure**. The CrossBow Server Configuration dialog
1336 box will appear.

1337 **Figure 2.44** CrossBow Server Configuration



1338

1339 1. License File Box

1340

2. OK Button

1341 3. Cancel Button

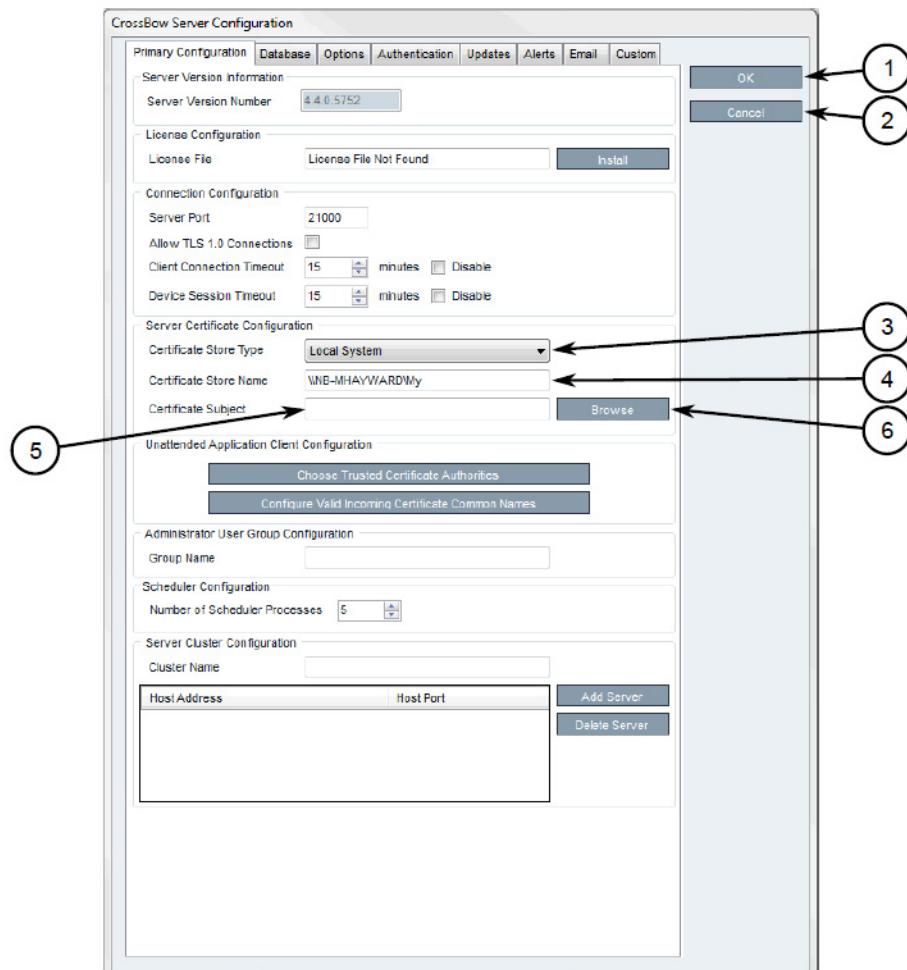
1342 4. Install Button

- 1343 4. On the **Primary Configuration** tab, under **License Configuration**, either type the name of
1344 the license file (including the system path) or click **Install** and select the desired file.
- 1345 5. Click **OK** to save changes.
- 1346 6. Start the CROSSBOW Main Server service.

1347 2.14.2.5 Selecting/Installing the CROSSBOW Server Certificate

- 1348 1. Access the RUGGEDCOM CROSSBOW server and launch CROSSBOW Server.
- 1349 2. Make sure the **CROSSBOW Main Server** service is **stopped**.
- 1350 3. Under **CrossBow Main Server**, click **Configure**. The CrossBow Server Configuration dialog
1351 box will appear.

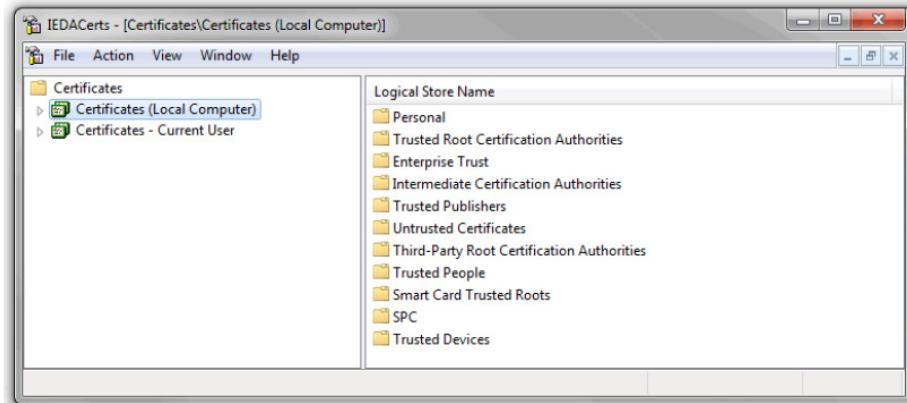
1352 Figure 2.45 CrossBow Server Configuration



1353

- 1354 1. *OK Button*
- 1355 2. *Cancel Button*
- 1356 3. *Certificate Store Type List*
- 1357 4. *Certificate Store Name Box*
- 1358 5. *Certificate Subject Box*
- 1359 6. *Browse Button*
- 1360 4. On the Primary Configuration tab, under **Server Certificate Configuration**, click **Browse**. The Select Server Certificate dialog box will appear.
- 1361 5. Click **Import**. A confirmation dialog box will appear.
- 1362 6. Click **Yes**. A confirmation dialog box will appear, as well as the Microsoft Management Console snap-in.

1365 Figure 2.46 MMC Snap-In

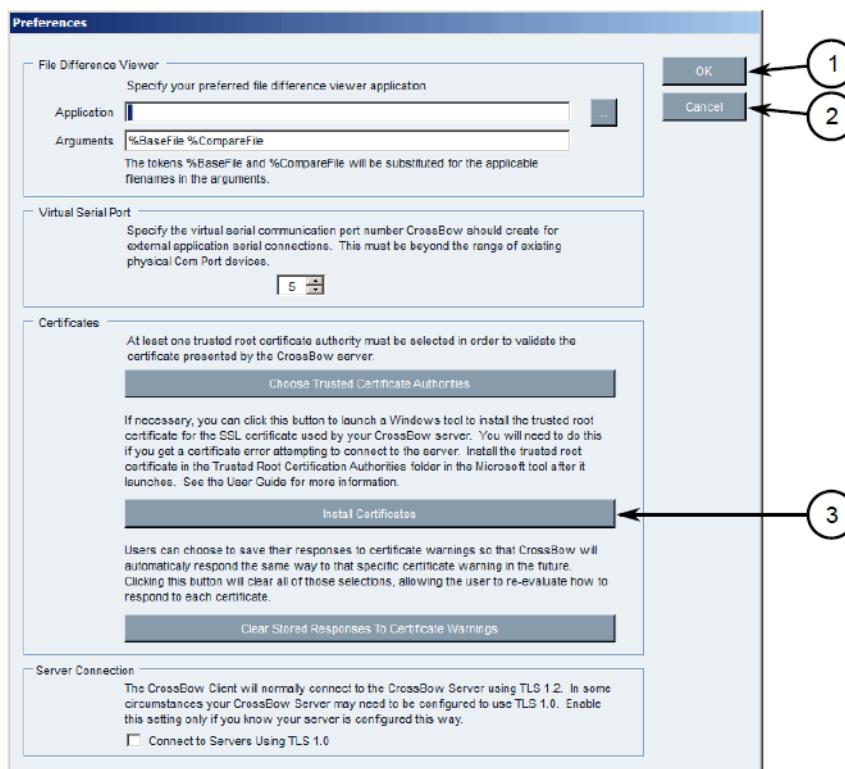


- 1366
- 1367 7. Expand **Certificates (Local Computer)**.
- 1368 8. Right-click either **Personal** or **Trusted Root Certification Authorities**, point to **All Tasks**, then click **Import**. The Certificate Import Wizard will appear.
- 1369 9. Follow the on-screen instructions to import the certificate.
- 1370 10. Close the Microsoft Management Console snap-in.
- 1371 11. Once the certificate is imported, Click **OK** to close the dialog box.
- 1372 12. On the Select Server Certificate dialog box, select the certificate from the list and click **OK**. The certificate name appears in the **Certificate Subject** field.
- 1373 13. Click **OK** to save changes.
- 1374 14. Start the CROSSBOW Main Server service.

1377 **2.14.2.6 Verifying/Installing the CROSSBOW Client CA Certificate**

- 1378 1. Launch CROSSBOW Client, but do not connect to the RUGGEDCOM CROSSBOW server.
- 1379 2. On the toolbar, click **File**, then click **Preferences**. The Preferences dialog box will appear.

1380

Figure 2.47 Preferences dialog box

1381

1. *OK* Button

1382

2. *Cancel* Button

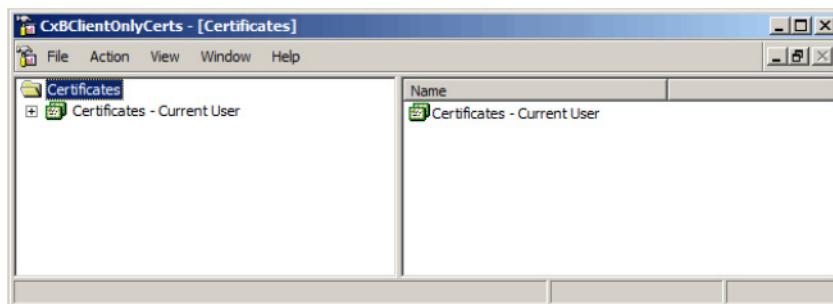
1383

3. *Install Certificates* Button

1384

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

1385

Figure 2.48 CxBClientOnlyCerts Snap-in

1386

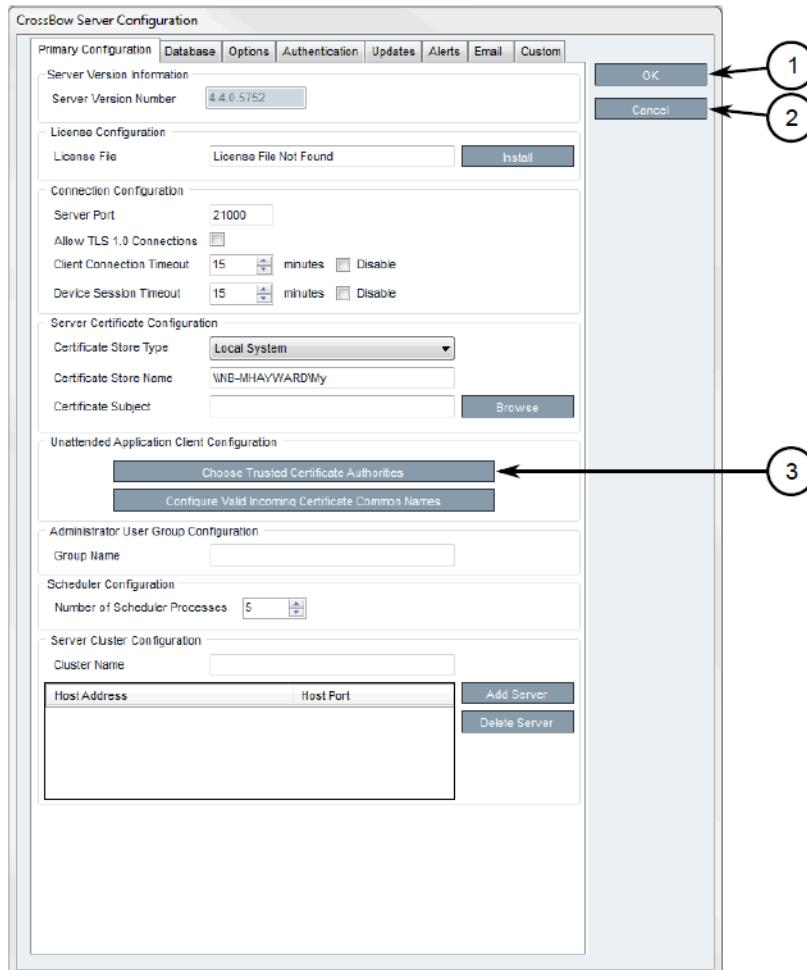
4. In the left pane, navigate to **Certificates - Current User ->Trusted Root Certification Authorities -> Certificates**.
5. Verify the appropriate CA certificate is listed in the right pane.
6. If the certificate is not listed, proceed to the next step.

- 1392 7. Right-click **Trusted Root Certification Authorities**, point to **All Tasks**, then click **Import**. The
1393 Certificate Import Wizard will appear.
- 1394 8. Follow the on-screen instructions to import a new CA certificate.
- 1395 9. Close the snap-in.

1396 **2.14.2.7 Select a Trusted CA for the CROSSBOW Server**

- 1397 1. Access the RUGGEDCOM CROSSBOW server and launch CROSSBOW Server.
- 1398 2. Make sure the **CROSSBOW Main Server** service is **stopped**.
- 1399 3. Under **CrossBow Main Server**, click **Configure**. The CrossBow Server Configuration dialog
1400 box will appear.

1401 **Figure 2.49 CrossBow Server Configuration**



1402

1403 1. *OK Button*

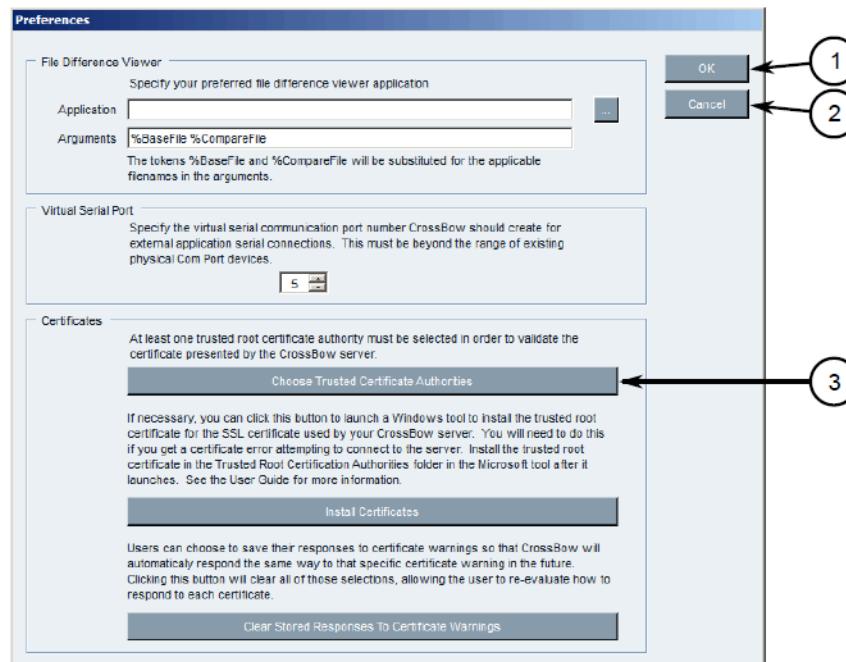
1404 2. *Cancel Button*

- 1405 3. *Choose Trusted Certificate Authorities Button*
- 1406 4. Click **Choose Trusted Certificate Authorities**. A dialog box will appear.
- 1407 5. [Optional] Filter the list of CAs by selecting either **Show Root Certificate Authorities**, **Show Intermediate Certificate Authorities** and/or **Show Third Party Certificate Authorities**.
- 1408
- 1409 6. Select one or more CAs from the list or select **Specify a certificate authority** and define the CA in the box below.
- 1410
- 1411 7. Click **OK** to save changes.
- 1412 8. Start the CROSSBOW Main Server service.

1413 2.14.2.8 Selecting a Trusted CA for a CROSSBOW Client

- 1414 1. Launch CROSSBOW Client, but do not connect to the RUGGEDCOM CROSSBOW server.
- 1415 2. On the toolbar, select **File**, then click **Preferences**. The Preferences dialog box will appear.

1416 **Figure 2.50 Preference dialog box**



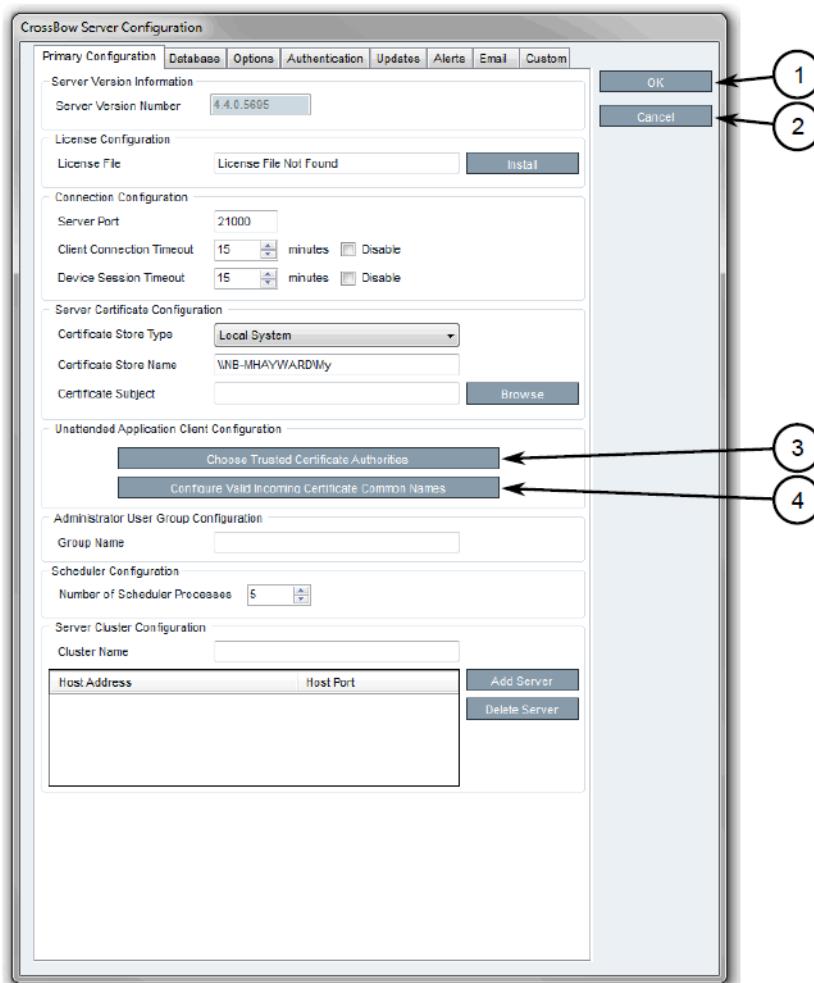
- 1417
- 1418 1. **OK Button**
- 1419 2. **Cancel Button**
- 1420 3. *Choose Trusted Certificate Authorities Button*
- 1421 3. Click **Choose Trusted Certificate Authorities**. A dialog box will appear.
- 1422 4. [Optional] Filter the list of CAs by selecting either **Show Root Certificate Authorities**, **Show Intermediate Certificate Authorities** and/or **Show Third Party Certificate Authorities**.

- 1424 5. Select one or more CAs from the list or select **Specify a certificate authority** and define the
1425 CA in the box below.
- 1426 6. Click **OK** to save changes.

1427 2.14.2.9 Adding a Common Name

- 1428 1. Access the RUGGEDCOM CROSSBOW server and launch CROSSBOW Server.
- 1429 2. Make sure the **CROSSBOW Main Server** service is **stopped**.
- 1430 3. Under **CROSSBOW Main Server**, click **Configure**. The CROSSBOW Server Configuration
1431 dialog box will appear.

1432 **Figure 2.51 CROSSBOW Server Configuration**



1433

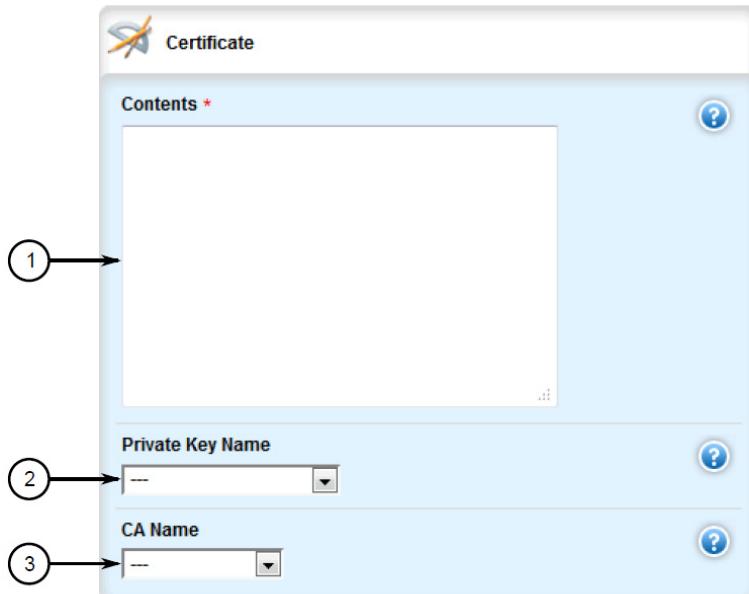
- 1434 1. *OK Button*
- 1435 2. *Cancel Button*
- 1436 3. *Choose Trusted Certificate Authorities Button*

- 1437 4. *Configure Valid Incoming Certificate Common Names Button*
- 1438 4. On the **Primary Configuration** tab, under **Unattended Application Client Configuration**,
1439 click **Configure Valid Incoming Certificate Common Names**. The Incoming Certificate
1440 Common Name dialog box will appear.
- 1441 5. Click **Add Name**. The Common Name dialog box will appear.
- 1442 6. In the **Common Name** box, type the common name, then click **OK** to close the dialog box.
- 1443 7. Click **OK**.
- 1444 8. Start the CROSSBOW Main Server service.

1445 2.14.2.10 Managing the RUGGEDCOM CROSSBOW Certificates and Keys

- 1446 The following references the RUGGEDCOM RX1400 and RX1511 web interface:
- 1447 1. Navigate to **security -> crypto -> ca** and click **<Add ca>**. The Key Settings form will appear.
- 1448 2. Configure the following parameter(s) as required:
- 1449 a. name
- 1450 3. Click **Add**. The CA form will appear.

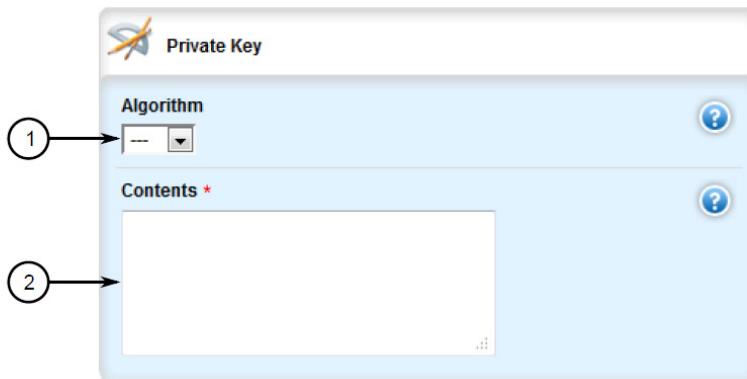
1451 Figure 2.52 VPN Certificate Form



- 1452
- 1453 1. *Contents Box*
- 1454 2. *Private Key Name List*
- 1455 3. *CA Certificate Name List*
- 1456 4. Copy the contents of the CA certificate into the **Key Cert Sign Certificate** field.
- 1457 5. Add the associated Certificate Revocation List (CRL).

- 1458 6. Navigate to **security -> crypto -> private-key** and click <**Add private-key**>. The Key Settings
1459 form will appear.
- 1460 7. In the Key Settings form, configure the following parameters as required:
- 1461 a. name
- 1462 8. Click **Add** to create the new private key. The Private Key form will appear.

1463 **Figure 2.53 VPN Private Key Form**



1464

1465 1. Algorithm List

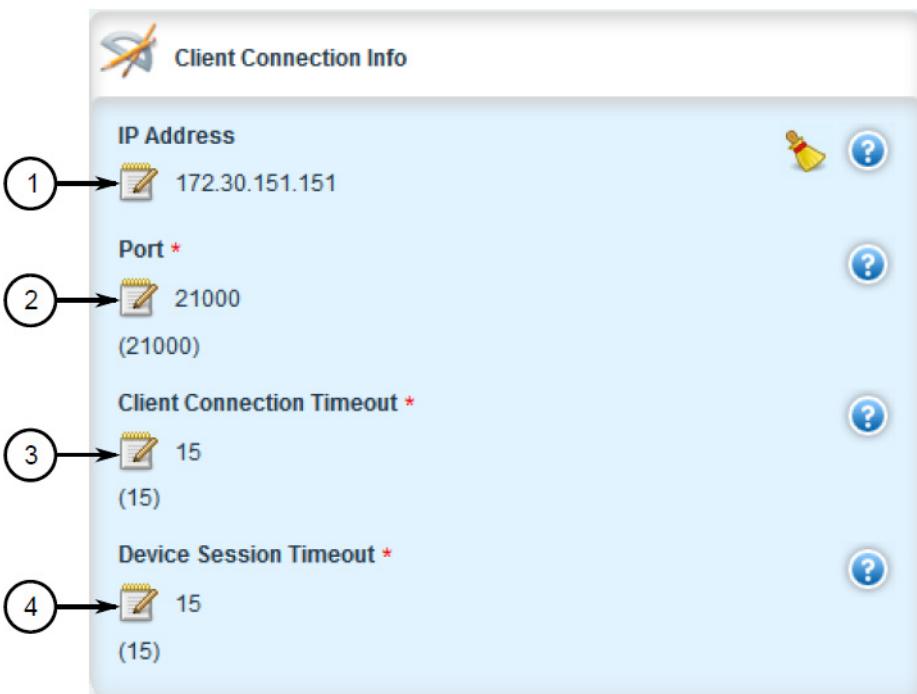
1466 2. Contents Box

- 1467 9. In the Private Key form, configure the following parameters as required:
- 1468 a. Algorithm
- 1469 b. Contents

1470 2.14.2.11 Managing the RUGGEDCOM CROSSBOW Application on RX1501

- 1471 To enable or disable communication with a RUGGEDCOM CROSSBOW system, do the following:
- 1472 1. Change the mode to **Edit Private** or **Edit Exclusive**.
- 1473 2. Navigate to **apps -> crossbow**. The CROSSBOW form will appear.
- 1474 3. Ensure that the **Enabled** checkbox is selected.
- 1475 4. Navigate to **apps -> crossbow -> client-connection**. The Client Connection Info form will
1476 appear.

1477

Figure 2.54 Client Connection Info

1478

1479 **1. IP Address Box**1480 **2. Port Box**

1481 5. Configure the following parameter(s) as required:

1482 a. ipaddr

1483 b. port

1484 6. Navigate to **apps -> crossbow -> sac-connection**. The SAC Connection List will appear.

1485

Figure 2.55 SAC Connection List

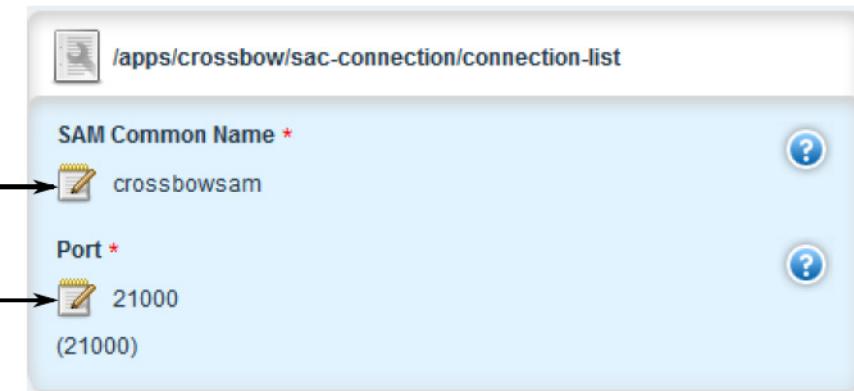
SAC Connection List			
IP Address	SAM Common Name	Port	
10.200.20.172	crossbowsam	21000	Edit Delete
10.200.22.232	crossbowserver	21000	Edit Delete
Add			

1486

1487 **1. Name Box**1488 **2. IP Address Box**1489 **3. Port Box**1490 7. Navigate to **apps -> crossbow -> sac-connection -> Add connection-list**. The Key Settings form will appear.
1491

- 1492 8. Configure the following parameter(s) as required:
- 1493 a. sam-ipaddr
- 1494 9. Click Add. The Connection List form will appear.

1495 **Figure 2.56 Connection List**



1496

1497 1. SAM Common Name Box

1498 2. Port Box

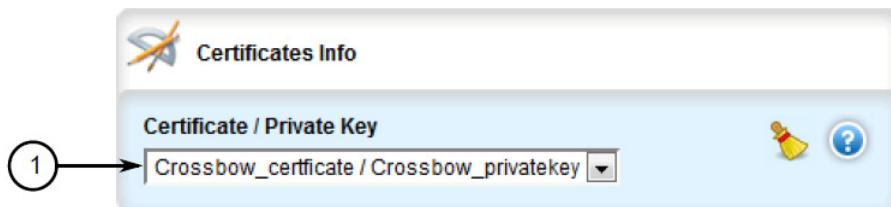
- 1499 10. Configure the following parameter(s) as required:

1500 a. sam-name

1501 b. sam-port

1502 11. Navigate to **apps -> crossbow -> certificate**. The Certificates Info forms will appear.

1503 **Figure 2.57 Certificates Info**



1504

1505 1. Certificate/Private Key List

- 1506 12. Configure the following parameters as required:

1507 a. cert

1508 b. cert-private-key

1509 13. Navigate to **apps -> crossbow -> certificate -> ca-cert-list** and click <Add ca-cert-list>. The Key Settings form will appear.

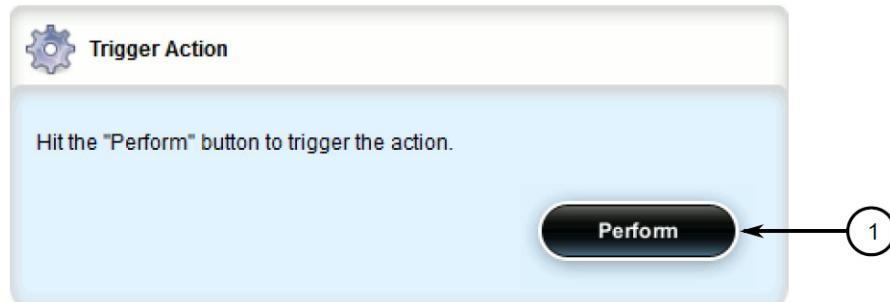
- 1511 14. Configure the following parameter(s) as required:

- 1512 a. name
- 1513 15. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box will
1514 appear. Click **OK** to proceed.
- 1515 16. Click **Exit Transaction** or continue making changes.

1516 2.14.2.12 Viewing the RUGGEDCOM CROSSBOW Log

- 1517 1. Navigate to **apps -> crossbow -> status** and click **log** in the menu. The Trigger Action form
1518 will appear.

1519 **Figure 2.58 Trigger Action**



1520

- 1521 1. **Perform Button**
- 1522 2. Click **Perform**. The Log form will appear.

1523 **Figure 2.59 Status Log**

```

Crossbowd-log
/var/log/syslog:Jan 31 15:06:28 ruggedcom crossbowd[23714]: ssl2tcp (ClientConn)[1208114224], elan_init_ctx():179: Unable to load cert chain file '/etc/certs/cxb_test_generated_cert.pem'.
/var/log/syslog:Jan 31 15:06:28 ruggedcom crossbowd[23714]: ssl2tcp (ClientConn)[1208114224], gethostbyname() failed using ip= -> Resource temporarily unavailable
/var/log/syslog:Jan 31 15:06:28 ruggedcom crossbowd[23714]: ssl2tcp (ClientConn)[1208114224], Create socket error: :21000 ->Resource temporarily unavailable
/var/log/syslog:Jan 31 15:06:28 ruggedcom crossbowd[23714]: ssl2tcp (ClientConn)[1208114224], main():193: Could not create SERVER R Socket (errno 11: Resource temporarily unavailable); fd: -1, bailing.
/var/log/syslog:Jan 31 15:06:29 ruggedcom crossbowd[23715]: ssl2tcp (MutualAuth)[1208114224], Log Level set to 2
/var/log/syslog:Jan 31 15:06:29 ruggedcom crossbowd[23715]: ssl2tcp (MutualAuth)[1208114224], elan_init_security():100: Unable to load random seed file.
/var/log/syslog:Jan 31 15:06:29 ruggedcom crossbowd[23715]: ssl2tcp (MutualAuth)[1208114224], elan_init_ctx():179: Unable to load cert chain file '/etc/certs/cxb_test_generated_cert.pem'.
/var/log/syslog:Jan 31 15:06:29 ruggedcom crossbowd[23715]: ssl2tcp (MutualAuth)[1208114224], gethostbyname() failed using ip= -> Resource temporarily unavailable
/var/log/crossbowd.log:Jan 31 15:06:29 ruggedcom crossbowd[23715]: ssl2tcp (MutualAuth)[1208114224], Create socket error: :21000 ->Resource temporarily unavailable

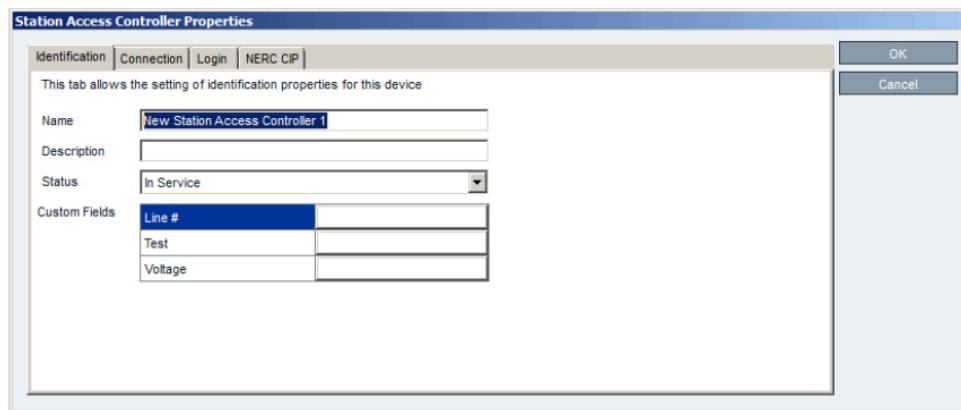
```

1524

1525 2.14.2.13 Managing Station Access Controllers (SACs)

- 1526 1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and
1527 login as a user with the necessary administrative privileges. The Field Layout tab appears by
1528 default.
- 1529 2. In the right pane, right-click the associated facility or gateway and click **Add Station Access
1530 Controller**. The Station Access Controller Properties dialog box will appear.

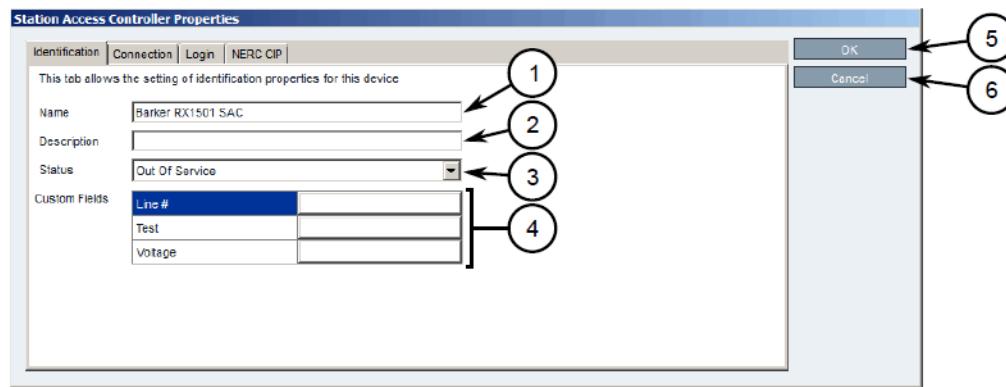
1531

Figure 2.60 Station Access Controller Properties

1532

- 1533 **1. Name Box**
- 1534 **2. Description Box**
- 1535 **3. Status List**
- 1536 **4. Custom Fields**
- 1537 **5. OK Button**
- 1538 **6. Cancel Button**
- 1539 3. Configure the identification properties (e.g. name, description, etc.) for the SAC.

1540

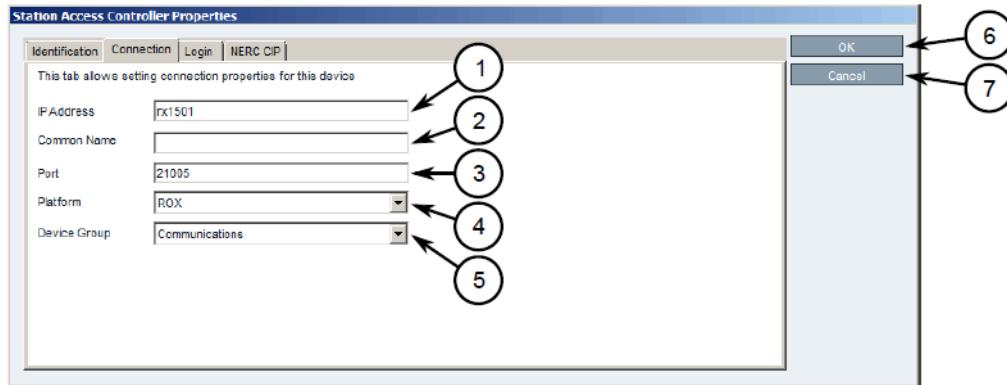
Figure 2.61 SAC Property Configuration - Identification

1541

- 1542 **1. Name Box**
- 1543 **2. Description Box**
- 1544 **3. Status List**
- 1545 **4. Custom Fields**
- 1546 **5. OK Button**
- 1547 **6. Cancel Button**

1548 4. Configure the connection properties (e.g. IP address, port, platform, etc.) for the SAC.

1549 **Figure 2.62 SAC Property Configuration - Connection**



1550

1551 1. *IP Address Box*

1552 2. *Common Name Box*

1553 3. *Port Box*

1554 4. *Platform List*

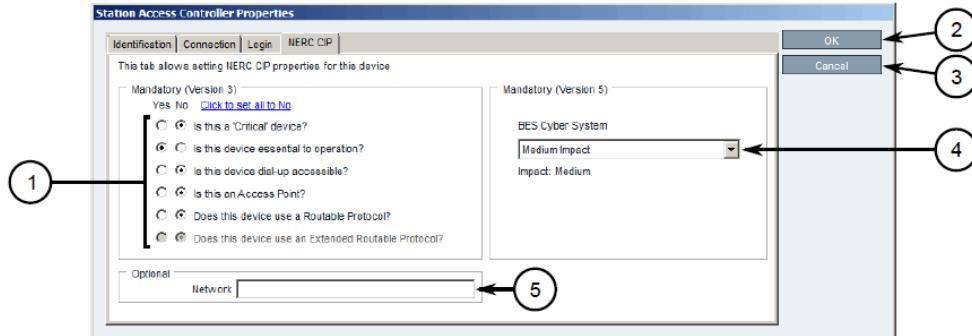
1555 5. *Device Group*

1556 6. *OK Button*

1557 7. *Cancel Button*

1558 5. Configure the NERC CIP properties for the SAC.

1559 **Figure 2.63 SAC Property Configuration - NERC CIP**



1560

1561 1. *Questions*

1562 2. *Network Box*

1563 3. *OK Button*

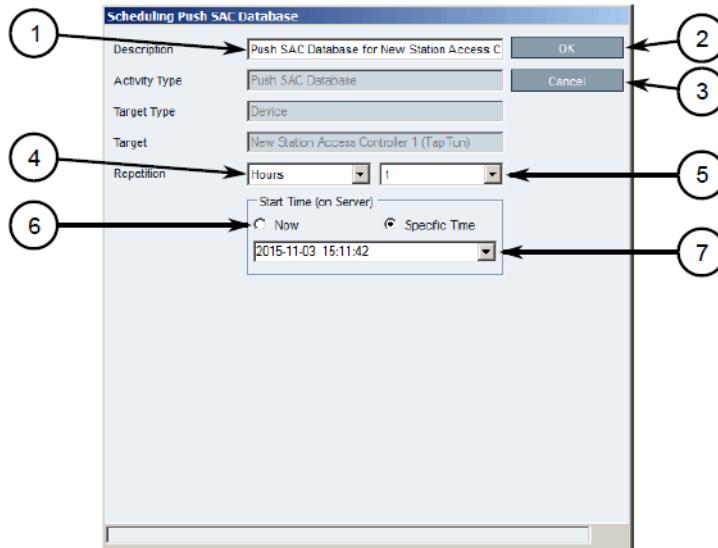
1564 4. *Cancel Button*

1565 5. *BES Cyber System List*

1566 2.14.2.14 Updating the SAC Database

- 1567 1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and
1568 login as a user with the necessary administrative privileges. Make sure to enter the host
1569 name and port number for the SAC during the login process.
- 1570 2. Search for the SAC's device family on the **Devices** tab.
- 1571 3. Right-click the **Station Access Controller** device family, point to **Special Operations**, then
1572 click **Push SAC Database**. The Scheduling Push SAC Database dialog box will appear.

1573 **Figure 2.64 Scheduling Push SAC Database**



1574

- 1575 1. *Description Box*
- 1576 2. *OK Button*
- 1577 3. *Cancel Button*
- 1578 4. *Repetition Lists*
- 1579 5. *Start Time Options*
- 1580 6. *Start Time Box*

- 1581 4. [Optional] Under **Description**, type a description for the operation. Include such details as
1582 the affected target, the purpose of the operation, etc. This description will appear in the list
1583 of scheduled operations.
- 1584 5. Under **Repetition**, select the interval and value (if applicable).
- 1585 6. Under **Start Time (On Server)**, select **Now** or **Specific Time**.
- 1586 7. Click **OK** to save changes. The operation will commence at the selected time.

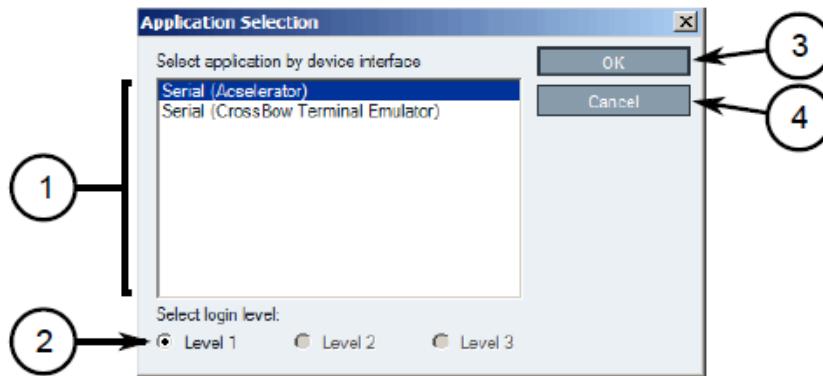
2.14.2.15 Managing Devices and Gateways

1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and login as a user with the necessary administrative privileges.
2. On the **Field Layout** tab, right-click the desired facility or gateway and click either **Add Device**, **Add Gateway**, or **Add Subordinate Gateway (gateways only)**. The Device Properties or Gateway Properties dialog box will appear.
3. Configure the identification properties (e.g. name, description, etc.) for the device/gateway.
4. Configure the connection properties (e.g. host name, user names, passwords, etc.) 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 login 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 dialog box will appear.

Figure 2.65 Application Selection dialog



1. Available Applications

- 1614 2. *Select Login Level Options*
- 1615 3. *OK Button*
- 1616 4. *Cancel Button*
- 1617 5. Select an application to connect to the device's interface.
- 1618 6. Under **Select login level**, select the login level to use when connecting to the device.
- 1619 7. Click **OK**. RUGGEDCOM CROSSBOW will attempt to connect to the device. Review the
1620 Messages pane for details.
- 1621 8. Once connected, the device/gateway and the connection status are displayed in the **Device
1622 Connection History** pane.
- 1623 9. When the application launches, if required, enter the localhost IP address or the real IP
1624 address of the end-device or gateway, followed by the port number.

1625 **2.15 Siemens RUGGEDCOM RX1400 (E1)**

1626 The Siemens RUGGEDCOM RX1400 device is used on the enterprise side of the lab, and creates
1627 an always-on VPN connection to the Siemens RUGGEDCOM RX1501, located on the boundary
1628 of the control network lab.

1629 **2.15.1 Environment Setup**

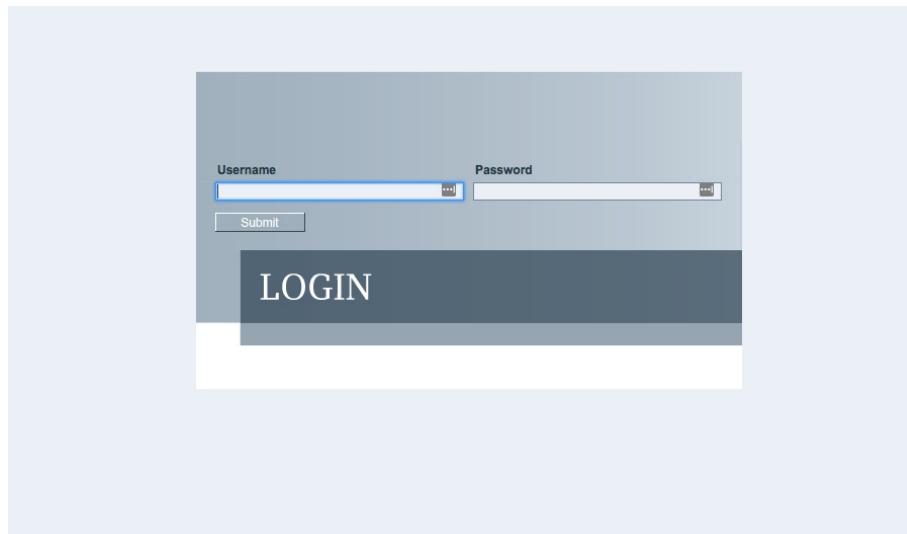
1630 Requirements for installation:

- 1631 ■ PC/laptop with Ethernet port
- 1632 ■ CAT5 or higher Ethernet cables
- 1633 ■ RUGGEDCOM VPN Device
- 1634 ■ Any type of terminal emulator
- 1635 ■ Web browser
- 1636 ■ When connecting the device to the network, the NCCoE used switch.0001 as the WAN port
1637 and switch.0010 as the LAN port connected to the local network

1638 **2.15.2 Installation Procedure**

- 1639 1. After powering on the device, connect to the IP address the device supplies itself via a web
1640 browser. The connection will most likely require an interim switch for connecting, but this
1641 varies between cases.
- 1642 2. You should be presented with the following screen:

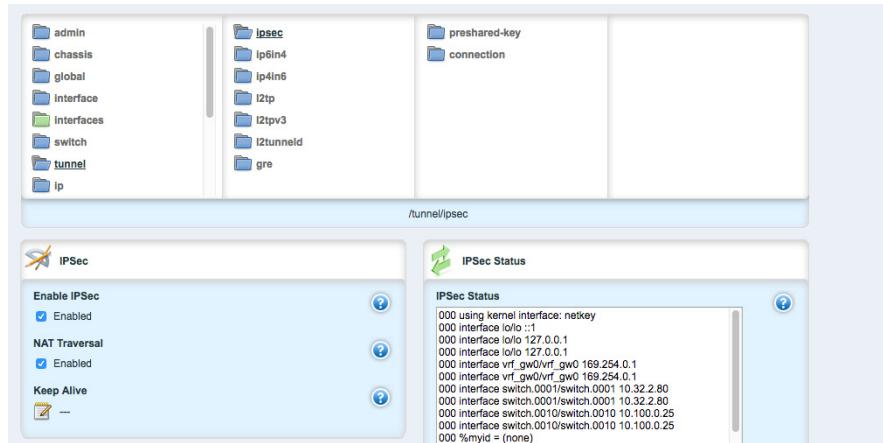
1643

Figure 2.66 RUGGEDCOM Web Login

1644

- 1645 3. Once logged in, click the link for **Edit Private** to go into Edit mode.
- 1646 4. Navigate to **tunnel -> ipsec** and check the boxes for **Enable IPSec** and **NAT Traversal**.

1647

Figure 2.67 Enable IPSec and NAT Traversal

1648

- 1649 5. Click **preshared-key**, then <**Add preshared-key**>.
- 1650 6. In the **Remote Address** field, type the remote IP address (the cogeneration plant's IP address).
- 1651 7. In the **Local Address** field, type the local IP address (the enterprise network).
- 1652 8. Click **Add**.
- 1653 9. Click the newly created entry under the preshared-key folder.
- 1654 10. Under **Secret Key**, create a new secret key that will be shared between devices.
- 1655 11. Under **ipsec->connection**, click <**Add connection**> to create a new connection
- 1656 12. Fill in a name for **Connection Name**, then click **Add**.

- 1658 13. Click on the new connection, and click the **Enable** checkbox for **Dead Peer Detect**.
- 1659 14. Ensure that the settings under **Dead Peer Detect** are:
- 1660 a. Interval: **30**
- 1661 b. Timeout: **120**
- 1662 c. Action: **Restart**
- 1663 15. Under **Connection**, set the following parameters:
- 1664 a. Startup Operation: **start**
- 1665 b. Authenticate By: **secret**
- 1666 c. Connection Type: **tunnel**
- 1667 d. Address-family: **ipv4**
- 1668 e. Perfect Forward Secrecy: **yes**
- 1669 f. SA Lifetime: **default**
- 1670 g. IKE Lifetime: **default**
- 1671 h. L2TP: **Unchecked (disabled)**
- 1672 i. Monitor Interface: **switch.0001**
- 1673 16. In the top window row, select the folder **ike** and click <**Add algorithm**>.
- 1674 17. Under **Key settings**, ensure the following parameters and click **Add**:
- 1675 a. Cipher Algorithm: **aes256**
- 1676 b. Hash Method: **sha1**
- 1677 c. Modpgroup: **modp8192**
- 1678 18. Going back to the top window row, select the **esp** folder directly underneath **ike**, then select **algorithm** and click <**Add algorithm**>.
- 1679
- 1680 19. Under **Key settings**, ensure the following parameters and click **Add**:
- 1681 a. Cipher Algorithm: **aes256**
- 1682 b. Hash Method: **sha1**
- 1683 20. Going back to the top window row, select **left** under **esp**.
- 1684 21. Under **Public IP Address**, ensure **Type** is **address**, then type the IP address into the **Hostname or IP Address** field.
- 1685
- 1686 22. Going back to the top window row, select **subnet** and click <**Add subnet**>.
- 1687 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**.
- 1688
- 1689 24. Going back to the top window row, select **right** under **left**.
- 1690 25. Under **Public IP Address**, ensure **Type** is **address**, then type the remote VPN IP Address into the **Hostname or IP Address** field.
- 1691
- 1692 26. Under the **Right** heading, for **NAT Traversal Negotiation Method**, select **rfc-3947**.

- 1693 27. Going back to the top window row, select **subnet**, then click <**Add subnet**>.
- 1694 28. Under **Key Settings**, in the **Subnet Address** field, type the remote subnet on the inside of
1695 the remote VPN in the box (lab used 172.19.0.0/16) and click **Add**.
- 1696 29. Going back to the beginning of the top row, ensure that **interfaces->ip->switch.0001->ipv4**
1697 contains a folder named after the externally facing network IP address.
- 1698 30. Ensure that **interface->ip->switch.0010->ipv4** contains a folder named after the internal
1699 network (lab used 10.100.0.0/16).

1700 **2.16 Siemens RUGGEDCOM RX1501 (O1)**

1701 The Siemens RUGGEDCOM RX1501 device is used on the boundary of the control network lab,
1702 and creates an always-on VPN connection to the Siemens RUGGEDCOM RX1400, located on the
1703 inside the enterprise network lab.

1704 **2.16.1 Siemens RUGGEDCOM RX1501 (O1) Installation Guide**

1705 The instructions for the installation of the RUGGEDCOM RX1501 are very similar to those in
1706 [Section 2.15](#), with the following additional information:

- 1707 1. Ensure that the shared key used in this installation is the same as the one used in the
1708 previous installation.
- 1709 2. The remote IPs and local IPs will be different for this installation, as they are relative to the
1710 device.
- 1711 3. **NAT Traversal Negotiation Method** will be on the **left** menu option (as opposed to the **right**
1712 listed earlier), and must be the same value (e.g., rfc-3947).

1713 **2.17 TDi Technologies ConsoleWorks (E6, O5, O9)**

1714 TDi Technologies ConsoleWorks creates multiple consoles (both GUI- and terminal-based) that
1715 allow connections through a web interface to internal devices, utilizing a protocol break to
1716 separate connections. ConsoleWorks is also utilized to normalize syslogs from the control
1717 network before sending them to the SIEM.

1718 For further information, see <https://www.tditechnologies.com/products/consoleworks-server>.

1719 **2.17.1 System Environment**

1720 The system that was set up to run this application was a fully updated (as of 4/20/2016) CentOS
1721 7 Operating System with the following hardware specifications:

- 1722 ■ 4GB RAM
- 1723 ■ 500GB HDD
- 1724 ■ 2 NICs

- 1725 ■ This install required a preconfigured network where one NIC was located on the WAN side
1726 (connected to the Waterfall Secure Bypass) and the other was connected to the Dell R620
1727 ESXi server

1728 Other requirements:

- 1729 ■ ConsoleWorks install media (a CD was used in the build)
1730 • ConsoleWorksSSL-<version>.rpm
1731 • ConsoleWorks_gui_gateway-<version>.rpm
1732 ■ ConsoleWorks license keys (TDI_Licenses.tar.gz)
1733 ■ Software installation command:
1734

```
yum install uuid libbpng12 libvncserver
```

1735 2.17.2 Installation

1736 As Root:

- 1737 1. Place ConsoleWorks Media into the system (assuming from here on that the media is in the
1738 form of a CD).
- 1739 2. mount /dev/sr0 /mnt/cdrom
- 1740 3. mkdir /tmp/consoleworks
- 1741 4. cp /mnt/cdrom/consolew.rpm /tmp/consoleworks/consolew.rpm
- 1742 5. rpm -ivh /tmp/consoleworks/ConsoleWorksSSL-<version>.rpm
- 1743 6. mkdir /tmp/consoleworkskeys/
- 1744 7. Copy ConsoleWorks keys to /tmp/consoleworkskeys/
- 1745 8. cd /tmp/consoleworkskeys/
- 1746 9. tar xzf TDI_Licenses.tar.gz
- 1747 10. cp /tmp/consoleworkskeys* /etc/TDI_licenses/
- 1748 11. /opt/ConsoleWorks/bin/cw_add_invo
- 1749 12. **Accept the License Terms.**
- 1750 13. Press **Enter** to continue.
- 1751 14. Name the instance of ConsoleWorks.
- 1752 15. Press **Enter** to accept default port (5176).
- 1753 16. Press **N** to deny SYSLOG listening.
- 1754 17. Press **Enter** to accept parameters entered.
- 1755 18. Press **Enter** to return to /opt/ConsoleWorks/bin/cw_add_invo.
- 1756 19. rpm -ivh /tmp/consoleworks/ConsoleWorks_gui_gateway-<version>.rpm
- 1757 20. /opt/gui_gateway/install_local.sh
- 1758 21. /opt/ConsoleWorks/bin/cw_start <invocation name created early>
- 1759 22. service gui_gatewayd start

1760 2.17.3 Usage

- 1761 1. Open a browser and navigate to https://<ConsoleWorksIP>:5176.
- 1762 2. Log in with Username: **console_manager**, Password: **Setup**.
- 1763 3. Change the default password.
- 1764 4. Choose **Register Now**.

1765 2.17.3.1 Initial Configuration

1766 All instructions below start with a menu on the sidebar.

- 1767 1. Tags
 - 1768 a. **Security->Tags->Add**
 - 1769 i. Set **Name**.
 - 1770 ii. Click **Save**.
- 1771 2. Profiles
 - 1772 a. **Users->Profiles->Add**
 - 1773 i. Set **Name**.
 - 1774 ii. Select **Tag**.
 - 1775 iii. Click **Save**.
- 1776 3. Users
 - 1777 a. **Users->Add**
 - 1778 i. Set **Name**.
 - 1779 ii. Set **Password**.
 - 1780 iii. Set **Profile**.
 - 1781 iv. Set **Tag**.
 - 1782 v. Click **Save**.

1783 2.17.3.2 Graphical Connections

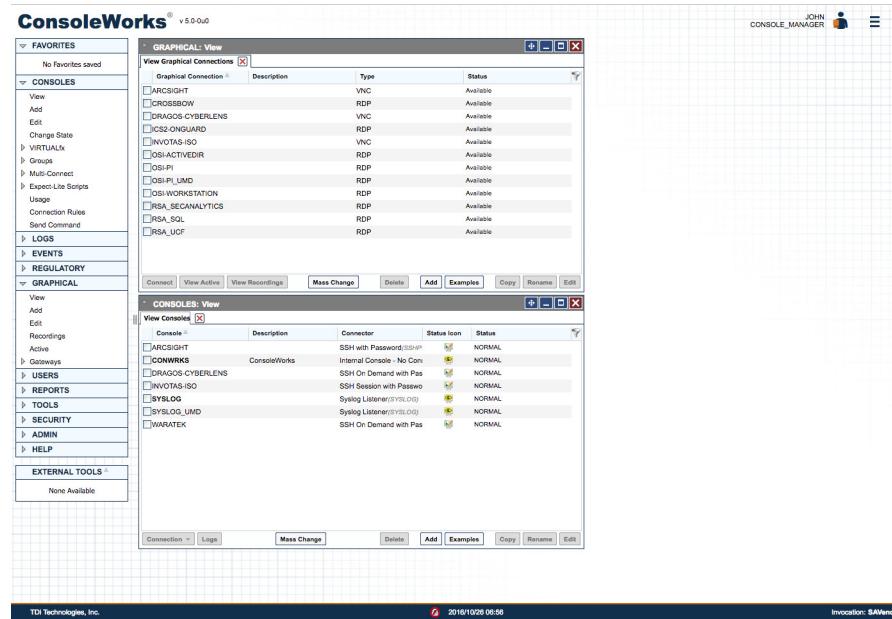
1784 Use the following steps to set up graphical connections (specifically VNC):

- 1785 1. Graphical Gateway:
 - 1786 a. **Graphical->Gateways->Add**
 - 1787 b. Set a name, then set Host as **localhost** and port as **5172**.
 - 1788 c. Check the **Enabled** checkbox and click **Save**.
 - 1789 d. Verify that it works by clicking **Test** in the top-left corner.
- 1790 2. Add a graphical connection (We'll use VNC):
 - 1791 a. **Graphical->Add**

- 1792 b. Set **Name**.
- 1793 c. Set the **Type** (VNC/RDP).
- 1794 d. Set the **Hostname/IP**.
- 1795 e. If you want recordings, set **Directory** and **Recordings**.
- 1796 f. Set the **Authentication**.
- 1797 g. Add **Graphical Gateway**.
- 1798 h. Add **Tags**.
- 1799 3. Access Controls
- 1800 a. **Security->Access Control->Add**
- 1801 b. Set **Name**.
- 1802 c. Check **Enabled**.
- 1803 d. Set **Priority**.
- 1804 e. Set **ALLOW**.
- 1805 f. Set **Component Type** to **Graphical Connection**.
- 1806 g. Under **Profile Selection**, you should see the following:
- 1807 i. Property Profile Equals *Profile Name* <join>
- 1808 ii. Correct Profile should appear in the box on right.
- 1809 h. Under **Resource Selection**, you should see the following:
- 1810 i. -Associate With a Tag that
- 1811 ii. Property Tag Equals *Tag name* <join>
- 1812 iii. Correct Graphical Console should appear in the box on right.
- 1813 i. Under **Privileges**, check:
- 1814 i. **Aware**
- 1815 ii. **View**
- 1816 iii. **Connect**
- 1817 iv. **Enable**
- 1818 v. **Monitor**
- 1819 j. Click **Save**.

1820

Figure 2.68 Binding to Syslog



1821

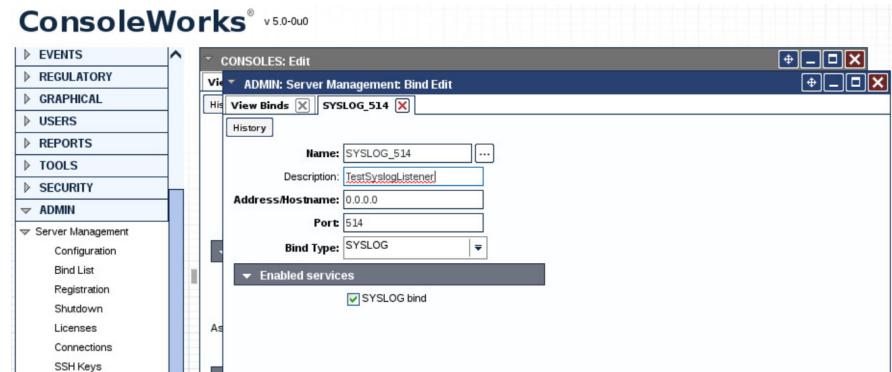
1822 2.17.4 TDI Technologies ConsoleWorks (E6) Installation Guide

1823 Follow the guide above on installing ConsoleWorks instance (O5), however, do not follow \
 1824 [Section 2.17.3.1, Initial Configuration](#) or [Section 2.17.3.2, Graphical Connections](#).

- 1825 1. Navigate to **Server Management > Bind List > Add**.
- 1826 2. Enter a name for **Binding** (e.g. **SYSLOG_514**).
- 1827 3. Leave **Address** as default (**0.0.0.0**).
- 1828 4. Set **Port** to **514**.
- 1829 5. Set **Bind type** to **SYSLOG** and **Enable**.

1830

Figure 2.69 Server Management Bind Edit

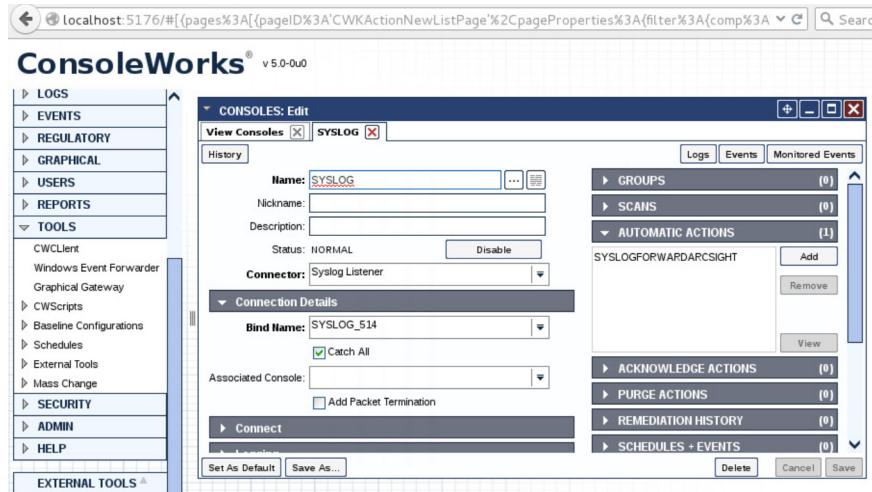


1831

- 1832 6. Navigate to **Consoles > Add**.
- 1833 7. Add **Console** and set a name (e.g. **SYSLOG**).

- 1834 8. In the **Connector** field, click the dropdown menu and select **Syslog Listener**.
- 1835 9. Under **Connection Details**, click the dropdown menu and select the **Binding** that you
1836 created above (e.g. SYSLOG_514).
- 1837 10. Check the **Catch All** checkbox.

1838 **Figure 2.70 Adding SYSLOG Console**



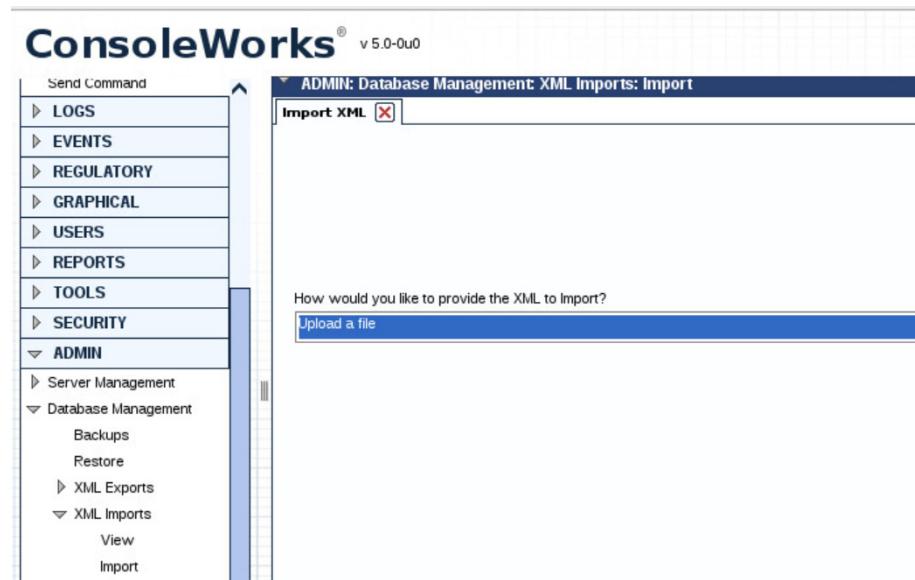
- 1839 11. Copy the socket plugin to the **cwscript** directory under your ConsoleWorks instance
1840 directory.

1841 **Figure 2.71 Copying Plugin to CWScript Directory**

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

- 1843 12. Navigate to **Admin > Database Management > XML Imports > Import > Upload a file**, then
1844 click **Next**.

1846

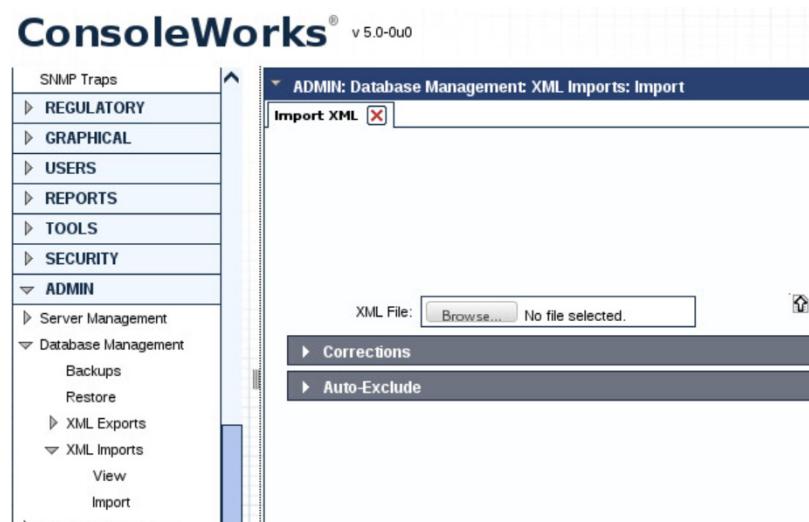
Figure 2.72 CWScript Upload

1847

1848

13. Click **Browse**.

1849

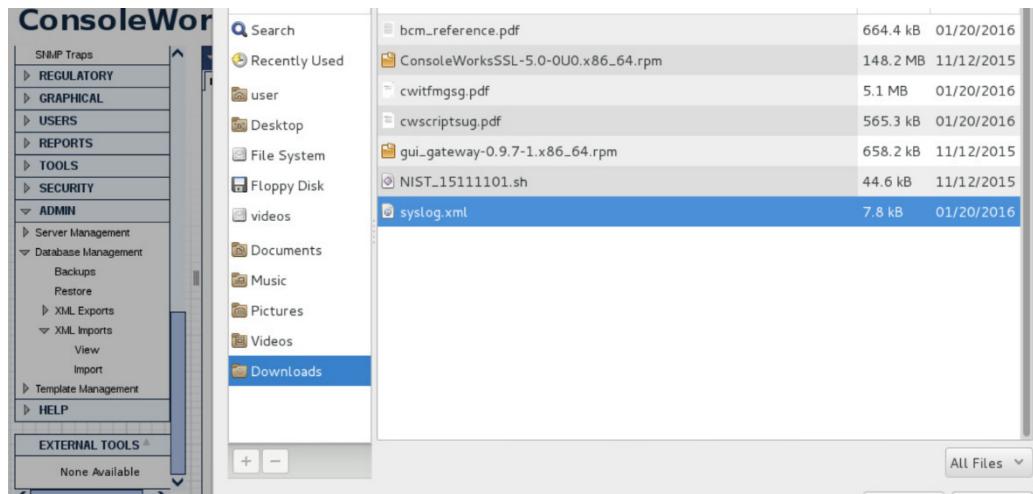
Figure 2.73 Browse for CWScript

1850

1851

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

1852

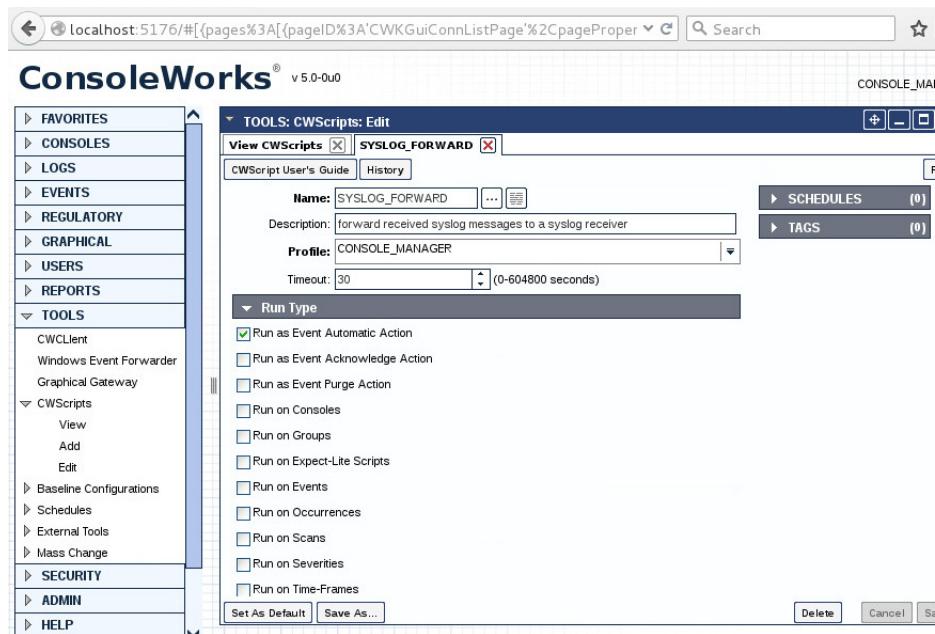
Figure 2.74 Select CWScript XML

1853

1854

15. Navigate to Tools > CWScripts > Select SYSLOG_FORWARD > Review Settings.

1855

Figure 2.75 Review CWScript Settings

1856

1857

16. Navigate to Actions > Automatic > Add.

1858

17. Set Name.

1859

18. Set Type to CWScript.

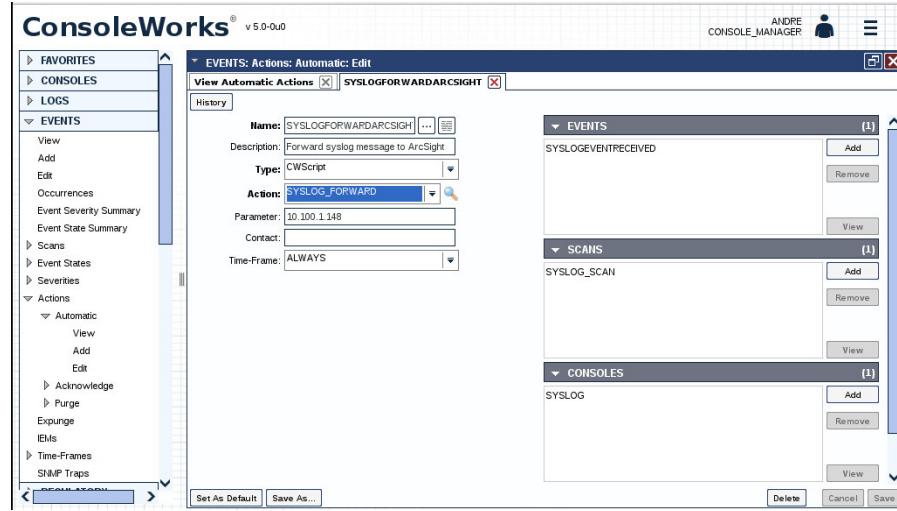
1860

19. In the Action field, click the dropdown menu and select SYSLOG_FORWARD.

1861

20. In the Parameter field enter the IP address (or FQDN) of the Syslog target.

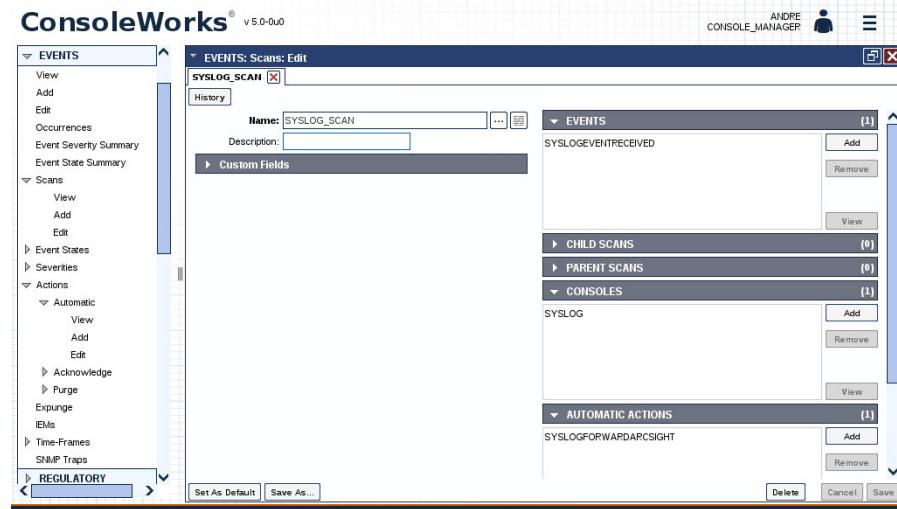
1862

Figure 2.76 Modify Action and Parameter for CWScript

1863

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

1864

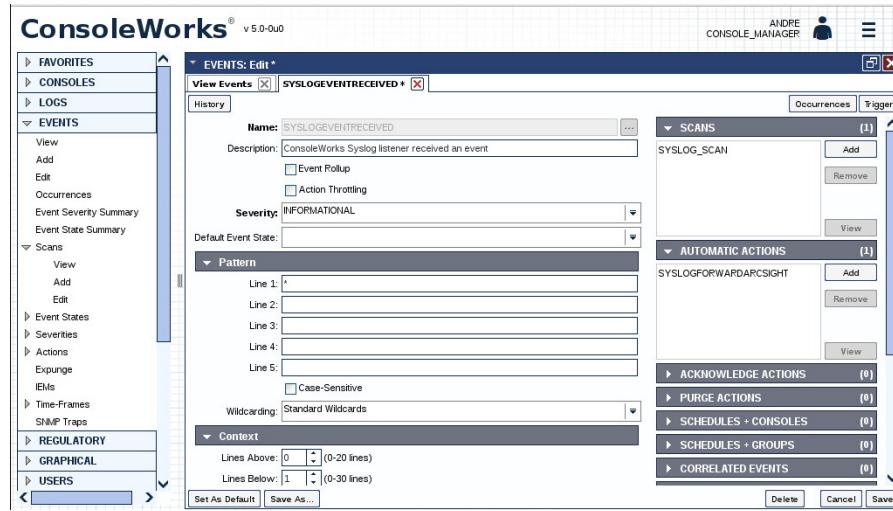
Figure 2.77 Add New Scan

1865

26. Navigate to **Events**, then select **Add**.
27. **Name** the Event.
28. Set the **Severity** level.
29. In the **Pattern** fields, Line 1, type in a character pattern that matches the syslog data. Set **Wildcarding to Standard Wildcards**.

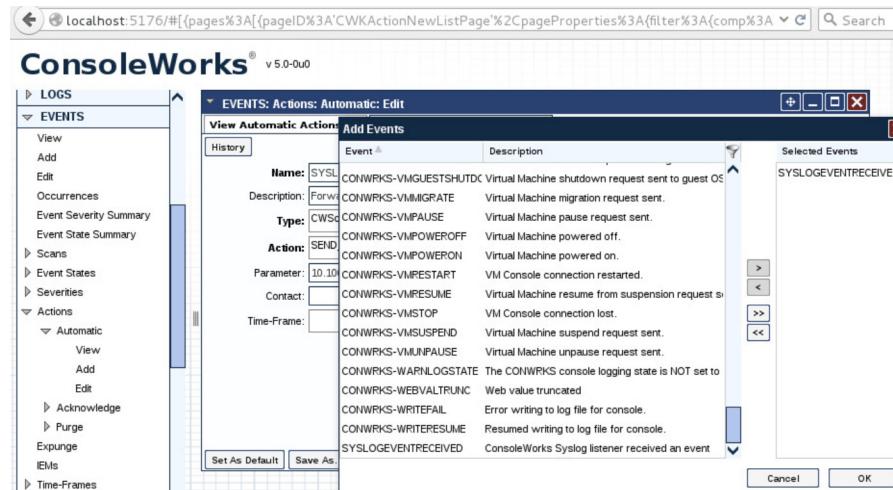
- 1876 30. In the context **Lines Below** field, enter **1**.
- 1877 31. In the **Scans** field, click **Add**, then select the name of the Scan that was defined in the
1878 previous steps.
- 1879 32. In the **Automatic Actions** field, click **Add**, then select the name of the Action that was
1880 defined in the previous steps.

1881 **Figure 2.78 Add New Event**



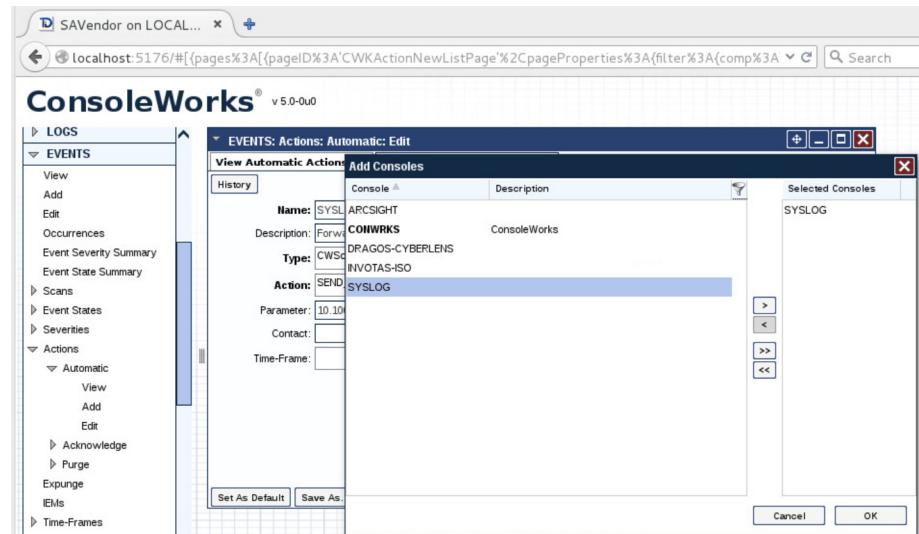
- 1882 33. Navigate back to **Actions > Automatic**, then edit the Action defined in the previous steps.
- 1883 34. In the **Event** field, confirm that the Event that you just created is selected.

1884 **Figure 2.79 Syslog Forwarding Action Config**



- 1885 35. In the **Console** field, select the Syslog Console that was defined in previous steps.

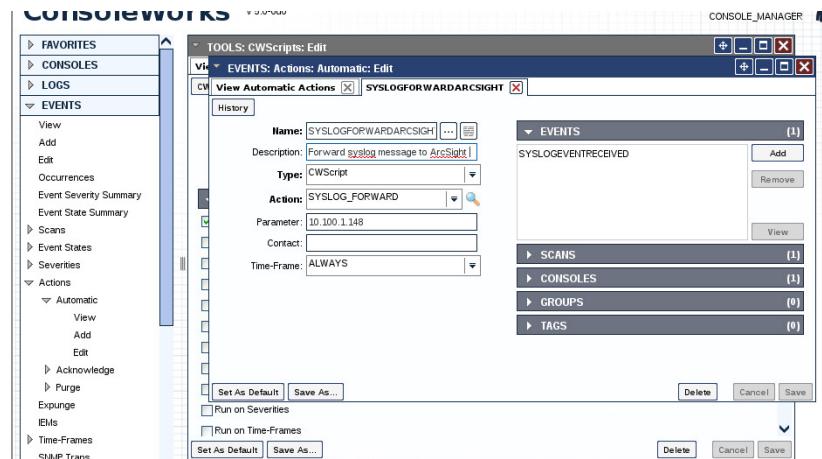
1888

Figure 2.80 Add Console to Syslog Forwarding Action Config

1889

36. Review settings.

1890

Figure 2.81 Review Event Settings

1892

37. Add rules to ConsoleWorks host OS firewall:

1893

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

1894

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

1895

38. Save the rules:

1896

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

1898 2.17.5 TDi Technologies ConsoleWorks (O9) Installation Guide

1899

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 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

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 the **Active** checkbox 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 the **Active** checkbox is checked.
8. Select the **Automatically Bind to Local Folder with ID** radio button. Ensure that you select the ID for the Local Folder using the same ID that was automatically generated for the Local Folder you 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**

- 1936 e. Password: <insert password here>
- 1937 10. For **Transfer mode**, select the **Passive** radio button.
- 1938 11. For **Transfer type**, select the **Binary** radio button.
- 1939 12. Ensure that the **Enable recursive transfer** checkbox is checked.
- 1940 13. Ensure that the **File pattern** checkbox is checked, and the form field contains the value: *.

1941 **2.18.1.1.2 OSI Pi Streams**

- 1942 1. Digital
- 1943 a. Expand **wfStreamRxPI_D** from the left sidebar.
- 1944 b. Expand **SME** from the left sidebar.
- 1945 c. Expand **PiPoint** from the left sidebar.
- 1946 d. Ensure the **Active** checkbox is checked.
- 1947 e. Fill out the correct values for the following form fields:
- 1948 i. Channel name: **PiPt Digital**
- 1949 ii. Server IP: **10.100.1.76**
- 1950 iii. Points type: **Digital**
- 1951 iv. Snapshots/Sec limit: **5000**
- 1952 v. Snapshots/Sec warning: **500**
- 1953 2. Numeric
- 1954 a. Expand **wfStreamRxPI_N** from the left sidebar.
- 1955 b. Expand **SME** from the left sidebar.
- 1956 c. Expand **PiPoint** from the left sidebar.
- 1957 d. Ensure the **Active** checkbox is checked.
- 1958 e. Fill out the correct values for the following form fields:
- 1959 i. Channel name: **PiPt Numeric**
- 1960 ii. Server IP: **10.100.1.76**
- 1961 iii. Points type: **Numeric**
- 1962 iv. Snapshots/Sec limit: **5000**
- 1963 v. Snapshots/Sec warning: **5000**
- 1964 3. String
- 1965 a. Expand **wfStreamRxPI_S** from the left sidebar.
- 1966 b. Expand **SME** from the left sidebar.
- 1967 c. Expand **PiPoint** from the left sidebar.
- 1968 d. Ensure the **Active** checkbox is checked.

- 1969 e. Fill out the correct values for the following form fields:
- 1970 i. Channel name: **PiPt String**
- 1971 ii. Server IP: **10.100.1.76**
- 1972 iii. Points type: **String**
- 1973 iv. Snapshots/Sec limit: **5000**
- 1974 v. Snapshots/Sec warning: **5000**

1975 **2.18.1.1.3 Syslog Streams**

- 1976 1. Expand **wfStreamRx** from the left sidebar.
- 1977 2. Expand **IT Monitoring** from the left sidebar.
- 1978 3. Select **Syslog UDP** from the left sidebar.
- 1979 4. Under **Channels**, select **Add**. Ensure the **Active** checkbox is checked.
- 1980 5. Fill out the correct values for the following form fields:
- 1981 a. Channel name: **Syslog 1**
- 1982 b. Send report every: **500**
- 1983 6. Under **Target Addresses**, select **Add** and set the IP address to **10.100.0.50**, and port to **514**.

1984 **2.18.1.2 TX Configuration**

1985 Open the **Waterfall TX Configuration** utility located in the **Start** menu.

1986 **2.18.1.2.1 FTP Stream**

- 1987 1. Expand **wfStreamTx** from the left sidebar.
- 1988 2. Expand **Files**.
- 1989 3. From the sidebar, select **Local Folder**.
- 1990 4. Under **Channels**, select **Add**. Ensure the **Active** checkbox is checked.
- 1991 5. Fill out the **Channel name** field and make a note of the **Channel ID** in parenthesis.
- 1992 6. From the sidebar, select **NCFTP**.
- 1993 7. Under **Channels**, select **Add**. Ensure the **Active** checkbox is checked.
- 1994 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.
- 1995 9. Fill out the correct values for the following form fields:
- 1996 a. FTP folder: **/file_link**
- 1997 b. FTP host: **172.18.1.250**
- 1998 c. FTP port: **21**
- 1999 d. Username: **root**

- 2001 e. Password: <insert password here>
- 2002 10. For **Transfer mode**, select the **Passive** radio button.
- 2003 11. For **Transfer type**, select the **Binary** radio button.
- 2004 12. Ensure that the **Enable recursive transfer** checkbox is checked.
- 2005 13. Ensure that the **File pattern** checkbox is checked, and the field contains the value: *.

2006 **2.18.1.2.2 OSI Pi Streams**

- 2007 1. Digital
- 2008 a. Expand **wfStreamTxPI_D** from the left sidebar.
- 2009 b. Expand **SME** from the left sidebar.
- 2010 c. Expand **PiPoint** from the left sidebar.
- 2011 d. Ensure the **Active** checkbox is checked.
- 2012 e. Fill out the correct values for the following form fields:
- 2013 i. Channel name: **PiPt Digital**
- 2014 ii. Server IP: **172.18.2.150**
- 2015 iii. Points type: **Digital**
- 2016 iv. Snapshots/Sec limit: **5000**
- 2017 v. Snapshots/Sec warning: **5000**
- 2018 vi. APS port: **3010**
- 2019 2. Numeric
- 2020 a. Expand **wfStreamTxPI_N** from the left sidebar.
- 2021 b. Expand **SME** from the left sidebar.
- 2022 c. Expand **PiPoint** from the left sidebar.
- 2023 d. Ensure the **Active** checkbox is checked.
- 2024 e. Fill out the correct values for the following form fields:
- 2025 i. Channel name: **PiPt Numeric**
- 2026 ii. Server IP: **172.18.2.150**
- 2027 iii. Points type: **Numeric**
- 2028 iv. Snapshots/Sec limit: **5000**
- 2029 v. Snapshots/Sec warning: **5000**
- 2030 vi. APS port: **3000**
- 2031 3. String
- 2032 a. Expand **wfStreamTxPI_S** from the left sidebar.
- 2033 b. Expand **SME** from the left sidebar.

- 2034 c. Expand **PiPoint** from the left sidebar.
- 2035 d. Ensure the **Active** checkbox is checked.
- 2036 e. Fill out the correct values for the following form fields:
- 2037 i. Channel name: **PiPt String**
- 2038 ii. Server IP: **172.18.2.150**
- 2039 iii. Points type: **String**
- 2040 iv. Snapshots/Sec limit: **5000**
- 2041 v. Snapshots/Sec warning: **5000**
- 2042 vi. APS port: **3020**

2043 **2.18.1.2.3 Syslog Streams**

- 2044 1. Expand **wfStreamTx** from the left sidebar.
- 2045 2. Expand **IT Monitoring** from the left sidebar.
- 2046 3. Select **Syslog UDP** from the left sidebar.
- 2047 4. Under **Channels**, select **Add**. Ensure the **Active** checkbox is checked.
- 2048 5. Fill out the correct values for the following form fields:
- 2049 a. Channel name: **Syslog 1**
- 2050 b. Send report every: **500**
- 2051 c. Port: **514**
- 2052 d. IP (Listening): **0.0.0.0**
- 2053 6. Under **target addresses**, select **Add**. Set the IP address to **10.100.0.50**, and port to **514**.

2054 **2.19 Waterfall Secure Bypass (O17)**

2055 Waterfall Secure Bypass is used as a secure connection solution that allows bidirectional
2056 communication into the product lab at the control system. It is solely dependent on a person
2057 turning a physical key, and has an automated timeout of two hours.

2058 **2.19.1 Waterfall Secure Bypass (O17) Installation Guide**

- 2059 The Waterfall Secure Bypass Solution is installed directly between the Siemens RUGGEDCOM
2060 RX1501 (O1) and a Schneider Electric Tofino Firewall (O18).
- 2061 1. Connect an Ethernet cable from the RX1501 to the **Ext** interface of the Secure Bypass.
- 2062 2. Connect an Ethernet cable from the WAN interface of the Tofino to the **Int** interface of the
2063 Secure Bypass.
- 2064 3. When the key is fully turned clockwise, the Secure Bypass will allow bi-directional traffic
2065 between the Tofino and the RX1501.

- 2066 4. When the key is fully turned counter-clockwise, the Secure Bypass will block all traffic
2067 between the Tofino and the RX1501.
- 2068 5. If the key is left fully turned clockwise for over 2 hours (time was configured at Waterfall
2069 location prior to receiving the device) the Secure Bypass will block all traffic between the
2070 Tofino and the RX1501. To allow for traffic to pass again, the user must fully turn the key
2071 counter-clockwise and then clockwise again.

2072 **Figure 2.82 Waterfall Secure Bypass Interface**



2.20 Waratek Runtime Application Protection (E10)

2075 Waratek Runtime Application Protection is a software agent plugin for monitoring and
2076 protecting user interactions with enterprise applications. In the build, Waratek is
2077 monitoring a database application for any attempts the user may undertake to pull
2078 unauthorized data from the database (mainly through the use of SQL Injection).

2079 For further information, see <http://www.waratek.com/solutions/> or
2080 <http://www.waratek.com/runtime-application-self-protection-rasp/>.

2.20.1 System Environment

2082 A CentOS 7 Operating System (fully updated as of 4/20/2016) was set up to run this application.
2083 Other Requirements:

2084 Web application that demonstrates protection capabilities (this build used Spiracle, Waratek's
2085 demo application: <https://github.com/waratek/spiracle>)

- 2086 ■ Web application server (this build used Apache Tomcat 9)
- 2087 ■ 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

- 2089 1. Download JDK 8 from Oracle site and unzip in /opt directory (e.g. /opt/jdk1.8.0_121)
- 2090 2. To configure for apache tomcat (or other web server), in
2091 \$CATALINA_HOME/bin/Catalina.sh, point JAVA_HOME to /opt/<jdk version>
- 2092 3. Add the following line to Catalina.sh:

2093 JAVA_OPTS="-javaagent:/opt/waratek/waratek.jar
2094 -Dcom.waratekContainerHome=/opt/<jdk version>"
- 2095 4. Change directories to /opt and untar the waratek_home.tar.gz package
- 2096 5. cd waratek_home

```

2097     6. Create the Rules directory in the current directory.
2098     7. Move the provided LICENSE_KEY file from Waratek to /var/lib/javad/.
2099     8. Create a rules file: /opt/waratek-home/Rules/global.rules

2100     VERSION 1.0
2101     # SQL Injection Blocking
2102     sqli:database:mysql:deny:warn
2103     file:read:/opt/tomcat/*:allow:trace
2104
2105     9. Create a logging XML file: /opt/waratek/mylogProps.xml
2106     <logProps-array>
2107         <logProps>
2108             <logMode>BOTH</logMode>
2109             <logFile>SECURITYLOG</logFile>
2110             <fileName>/opt/waratek/alerts.log</fileName>
2111             <remoteHost>**INSERT REMOTE SYSLOG HERE (i.e.
2112             10.100.100.10:514)**</remoteHost>
2113             <patternLayout>%m</patternLayout>
2114             <priorityLevel>WARN</priorityLevel>
2115         </logProps>
2116     </logProps-array>
2117     10. Edit the /opt/waratek_home/setenv.sh file as follows:
2118         export WARATEK_OPTS="-Dcom.waratek.jvm.name=tomcat7
2119         -Dcom.waratek.rules.local=/opt/waratek_home/Rules/jvc.rules
2120         -Dcom.waratek.log.properties=/opt/waratek_home/logProps.xml
2121         -Dcom.waratek.jmxh

```

2.20.3 Usage

To utilize the Runtime Protection for Java product, start up the web application mentioned in 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.

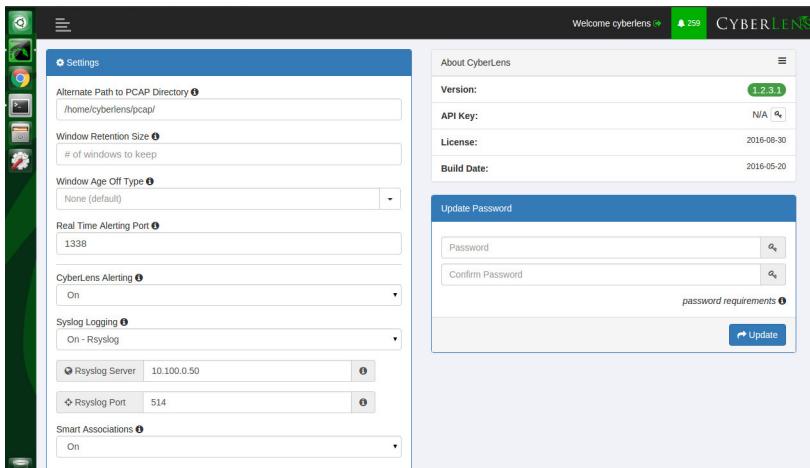
2.21.1 Dragos CyberLens Connector

2.21.1.1 Configure Source Product

1. Connect to the CyberLens console.

- 2131 2. In the CyberLens app, go to **Settings**.
- 2132 3. In the **CyberLens Alerting** dropdown, select **On**.
- 2133 4. In the **Syslog Logging** section:
- 2134 a. select the dropdown for **On - Rsyslog**.
- 2135 b. Enter the **IP address** of the syslog server, e.g.:
- 2136 172.18.0.50
- 2137 c. Enter the **port** of the syslog server, e.g.:
- 2138 514

2139 **Figure 2.83 Set Up Syslog on Cyberlens**



- 2140
- 2141 5. From the command line, using the **cybersudo** account, check the OS firewall to see if it
2142 allows the syslog traffic by running **sudo ufw status**. **Add** and **save** the rule if needed.
- 2143 6. *Note: upon upgrading Cyberlens software, the rsyslog settings may be lost. Be sure to check
2144 and update these settings as needed after any upgrades.*

2145 2.21.1.2 Install/Configure Custom ArcSight FlexConnector

- 2146 1. Follow ArcSight's instructions for installing a Linux-based syslog SmartConnector¹.
- 2147 2. Copy the custom FlexConnector configuration files to the appropriate locations.
- 2148 3. Start the Connector service:
- 2149 `/etc/init.d/arc_<connectorName> start`

1.HPE ArcSight SmartConnector User Guide - <https://www.protect724.hpe.com/docs/DOC-2279>

2.21.1.3 Custom Parser - ArcSight FlexConnector Parser

2151 Create a file containing the text below and copy this file to:
2152 **/opt/arcsight/connectors/<connector**
2153 **directory>/current/user/agent/flexagent/cyberlens.subagent.sdkrfilereader.properties**

2154
2155 **#:::::::::::::::::::**
2156 **# Syslog custom subagent regex properties file: for CyberLens rsyslog**
2157 **#**
2158 **# raw syslog example:**
2159 **# "Sep 6 16:04:48 ubuntu CyberLensApp: I, [2016-09-06T16:04:48.839937**
2160 **#65401] INFO -- : Cyberlens generated the following alert: A Sensor**
2161 **saw 'S7COMM' for the first time"**
2162 **#**
2163 **#:::::::::::::::::::**
2164
2165 **# without double slashes**
2166 **# regex=(CyberLensApp) :\sI, (\[\d+-\d\d-\d\d\s\d\d:\d\d:\d\d.\d+**
2167 **#\d+]) (\D+) -- : (.*)\n?Source IP: (\d+. \d+. \d+)\n?(.*)**
2168 **# with double slashes and newline**
2169 **regex=(CyberLensApp) :\sI,**
2170 **(\\[\d+-\\d\\d-\\d\\d\\d\\s\\d\\d:\\d\\d:\\d\\d.\\d+ #\\d+]) (\\D+) -- :**
2171 **(.*)\n?Source IP: (\\d+. \\d+. \\d+)\n?(.*)**

2172
2173 token.count=6
2174 token[0].name=Application
2175 token[1].name=Message
2176 token[2].name=Severity
2177 token[3].name=Name
2178 token[4].name=SourceIP
2179 token[4].type=IPAddress
2180 token[5].name=CatchAnyDoubledLines

2181
2182 event.name=Name
2183 event.deviceProduct=__stringConstant("CyberLens")
2184 event.deviceVendor=__stringConstant("DragosSecurity")
2185 event.deviceSeverity=Severity
2186 event.message=Message
2187 event.deviceProcessName=Application
2188 event.deviceAddress=SourceIP
2189 event.deviceCustomString1=CatchAnyDoubledLines

2190
2191 severity.map.veryhigh.if.deviceSeverity=1,2
2192 severity.map.high.if.deviceSeverity=3,4
2193 severity.map.medium.if.deviceSeverity=5,6

```
2194    severity.map.low.if.deviceSeverity=INFO
```

2.21.1.4 ArcSight agent.properties File

```
2196    1. Modify the agent.properties file settings as needed based on the example below:  
2197        /opt/arcsight/connectors/<connector directory>/current/user/agent/agent.properties  
2198    2. Modify the customsubagent list as needed for your environment.  
2199    3. Replace the IP address to suit your environment.  
2200  
2201 #ArcSight Properties File  
2202 #Fri Mar 18 17:37:10 GMT 2016  
2203 agents.maxAgents=1  
2204 agents[0].aggregationcachesize=1000  
2205 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  
2213 #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  
2218 agents[0].destination.count=1  
2219 agents[0].destination[0].agentid=3R9bQilMBABCiY6NStvvaDA\=\=  
2220 agents[0].destination[0].failover.count=0  
2221 agents[0].destination[0].params=<?xml version\="1.0"  
2222 encoding\="UTF-8"?>\n<ParameterValues>\n      <Parameter  
2223 Name\="aupmaster" Value\="false"/>\n      <Parameter Name\="port"  
2224 Value\="8443"/>\n      <Parameter Name\="fipsiphers"  
2225 Value\="fipsDefault"/>\n      <Parameter Name\="host"  
2226 Value\="arcsight.es-sa-b1.test"/>\n      <Parameter Name\="filterevents"  
2227 Value\="false"/>\n</ParameterValues>\n  
2228 agents[0].destination[0].type=http  
2229 agents[0].deviceconnectionalertinterval=60000  
2230 agents[0].enabled=true  
2231 agents[0].entityid=0WbNilMBABCiAoBJrJmUow\=\=  
2232 agents[0].fcp.version=0  
2233 agents[0].filequeueumaxfilecount=100  
2234 agents[0].filequeueumaxfilesize=10000000  
2235 agents[0].forwarder=false  
2236 agents[0].forwardmode=true  
2237 agents[0].id=3R9bQilMBABCiY6NStvvaDA\=\=
```

```

2238     agents[0].ipaddress=10.100.1.148
2239     agents[0].overwriterawevent=false
2240     agents[0].persistenceinterval=0
2241     agents[0].port=514
2242     agents[0].protocol=UDP
2243     agents[0].rawloginterval=-1
2244     agents[0].rawlogmaxsize=-1
2245     agents[0].tcpbindretrytime=5000
2246     agents[0].tcpbuffersize=10240
2247     agents[0].tcpcleanupdelay=-1
2248     agents[0].tcpmaxbuffersize=1048576
2249     agents[0].tcpmaxidletime=-1
2250     agents[0].tcpmaxsockets=1000
2251     agents[0].tcppeerclosedchecktimeout=-1
2252     agents[0].tcpsetsocketlinger=false
2253     agents[0].tcpsleepetime=50
2254     agents[0].type=syslog
2255     agents[0].unparsedevents.log.enabled=true
2256     agents[0].usecustomsubagentlist=true
2257     agents[0].usefilequeue=true
2258     remote.management.ssl.organizational.unit=HzjHilMBABCAAWiR1ATijw

```

2259 2.21.1.5 Map File

- 2260 1. Create a file containing the text below and copy this file to: **/opt/arcsight/<connector**
2261 **directory>/current/user/agent/map/map.1.properties**
 - 2262 2. *Note: if an existing map.1.properties file exists, increment the suffix as needed (e.g.*
2263 *map.2.properties)*
- ```

2264 !Flags,CaseSens-,Overwrite
2265 regex.event.name,set.event.deviceVendor,set.event.deviceProduct
2266 .*Cyberlens.* ,DragosSecurity,CyberLens

```

### 2267 2.21.1.6 Categorization File

2268 Create a .csv file containing the text below and copy this file to: **/opt/arcsight/<connector**  
2269 **directory>/current/user/agent/acp/categorizer/current/<deviceproduct>/deviceproduct.csv**

| event.<br>device<br>Product | set.event.<br>category<br>Object | set.event.<br>category<br>Behavior | set.event.<br>category<br>Technique | set.event.<br>category<br>DeviceGroup | set.event.<br>category<br>Significance | set.event.<br>category<br>Outcome |
|-----------------------------|----------------------------------|------------------------------------|-------------------------------------|---------------------------------------|----------------------------------------|-----------------------------------|
| CyberLens                   | /Host                            | /Found                             | /Traffic<br>Anomaly                 | /IDS/Network                          | /Informational                         | /attempt                          |

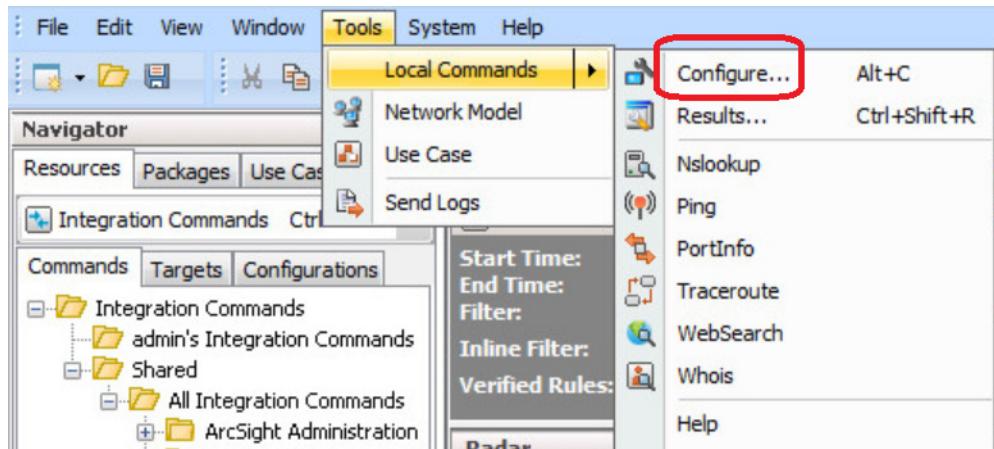
## 2.21.2 ICS<sup>2</sup> OnGuard

### 2.21.2.1 Integration Setup

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

1. Select Tools > Local Commands > Configure.

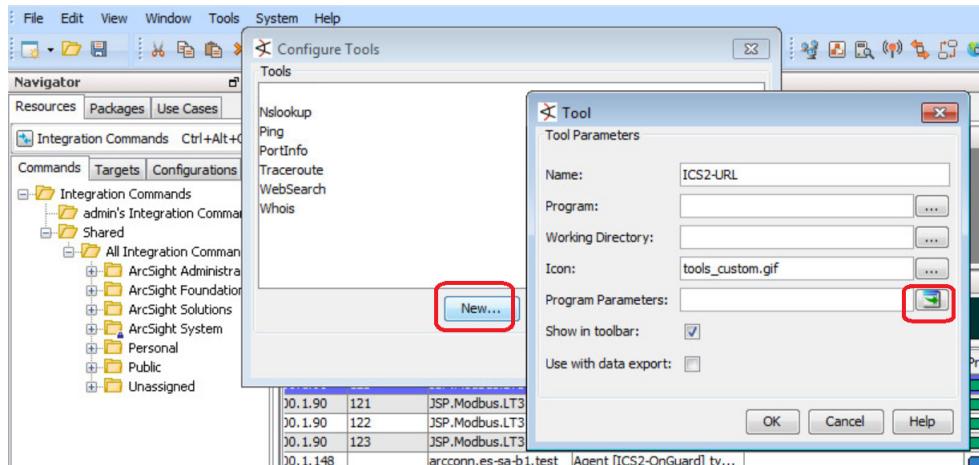
Figure 2.84 ArcSight Configure



2277

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

Figure 2.85 Program Parameters Setup

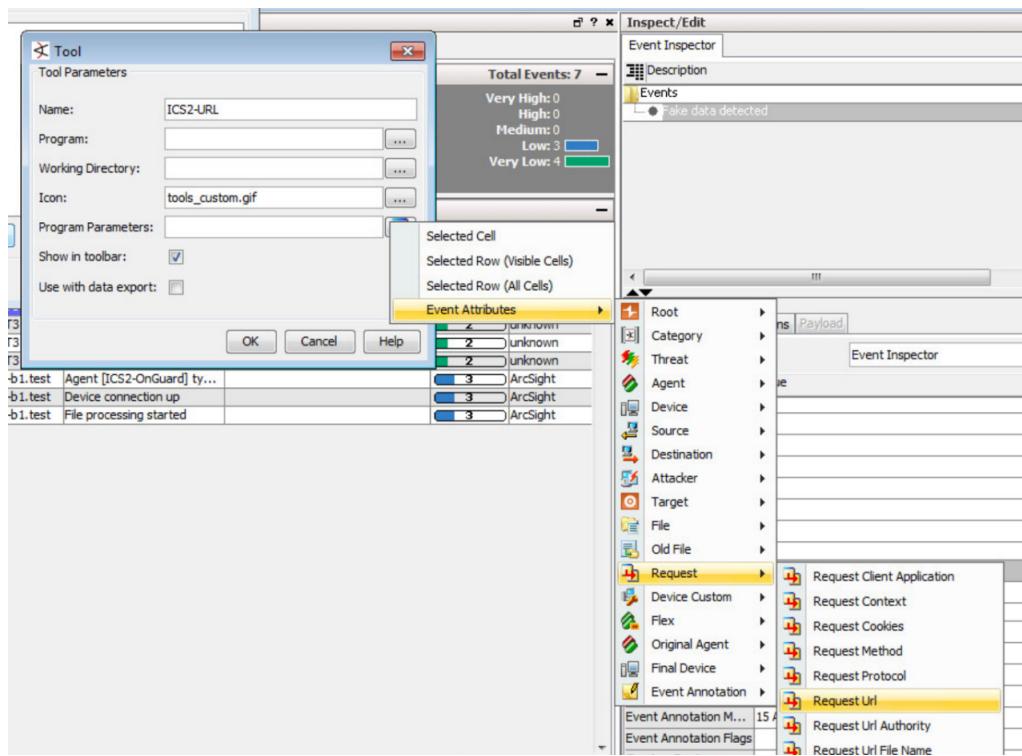


2280

3. Select Event Attributes > Request > Request URL.

2282

Figure 2.86 Request URL Configuration

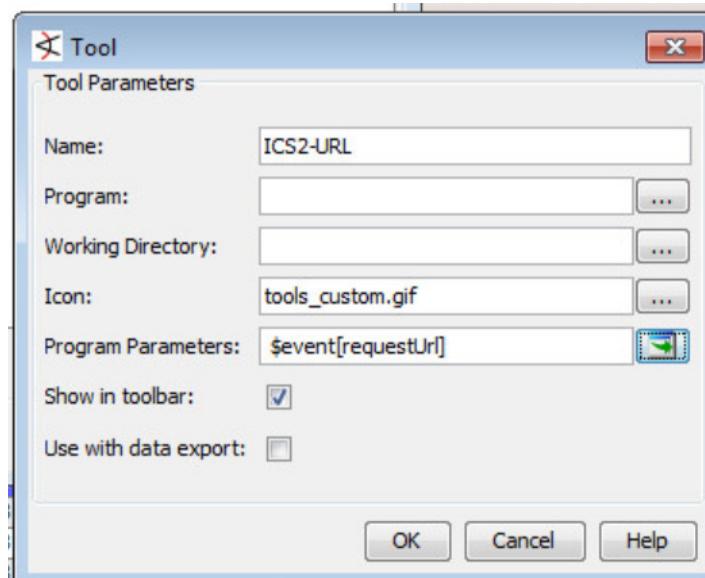


2283

- 2284 4. Select OK.

2285

Figure 2.87 Tool URL Verification



2286

- 2287 5. Right click on a **URL** in an event, select **Tools**, and verify that the **ICS2-URL tool** appears in the menu.

2289 **2.21.2.2 Install/Configure Custom ArcSight FlexConnector**

- 2290     1. Follow ArcSight's instructions for installing a Linux-based syslog SmartConnector.  
2291     2. Copy the custom FlexConnector configuration files to the appropriate locations.  
2292         a. See sections 6-8 of cyberlens-syslog-configuration-v2\_3.docx  
2293     3. Start the Connector service:  
2294         `/etc/init.d/arc_[connectorName] start`

2295 **2.21.2.3 Custom Parser - ArcSight FlexConnector Parser**

- 2296     1. Create a file containing the text below, and copy the file to:  
2297         **/opt/arcsight/connectors/[connector-directory]/current/user/agent/flexagent/onguard.s  
2298         dkrfileader.properties**
- 2299         `#:::::::::::::::::::::::::::::::::::`  
2300         `# Syslog custom regex properties file`  
2301         `# for ICS^2 OnGuard CEF syslog`  
2302  
2303         `delimiter=|`  
2304         `text.qualifier=""`  
2305         `comments.start.with=\#`  
2306         `trim.tokens=true`  
2307         `contains.empty.tokens=true`  
2308  
2309         `token.count=8`  
2310  
2311         `token[0].name=Token0`  
2312         `token[0].type=String`  
2313         `token[1].name=Token1`  
2314         `token[1].type=String`  
2315         `token[2].name=Token2`  
2316         `token[2].type=Integer`  
2317         `token[3].name=Token3`  
2318         `token[3].type=String`  
2319         `token[4].name=Token4`  
2320         `token[4].type=String`  
2321         `token[5].name=Token5`  
2322         `token[5].type=TimeStamp`  
2323         `token[5].format=yyyy-MM-dd HH\:mm\:ssz`  
2324         `token[6].name=Token6`  
2325         `token[6].type=TimeStamp`  
2326         `token[6].format=yyyy-MM-dd HH\:mm\:ssz`  
2327         `token[7].name=Token7`  
2328         `token[7].type=String`

```

2329
2330 # mappings
2331 event.deviceCustomString1=Token0
2332 event.deviceHostName=Token1
2333 event.externalId=Token2
2334 event.name=Token3
2335 event.message=Token4
2336 event.startTime=Token5
2337 event.endTime=Token6
2338 event.requestUrl=Token7
2339 event.deviceVendor=__stringConstant("ICS2")
2340 event.deviceProduct=__stringConstant("OnGuard")
2341
2342 #severity.map.veryhigh.if.deviceSeverity=1,2
2343 severity.map.high.if.deviceSeverity=HIGH
2344 severity.map.medium.if.deviceSeverity=MEDIUM
2345 severity.map.low.if.deviceSeverity=LOW
2346 severity.map.verylow.if.deviceSeverity=INFO

```

#### [2.21.2.4 ArcSight agent.properties File](#)

- 2348     1. Example, from the following directory: **/opt/arcsight/connectors/[connector**  
 2349       **directory]/current/user/agent/agent.properties**

```

2350 #ArcSight Properties File
2351 #Fri Apr 08 22:28:12 BST 2016
2352 agents.maxAgents=1
2353 agents[0].AgentSequenceNumber=0
2354 agents[0].configfile=onguard
2355 agents[0].destination.count=1
2356 agents[0].destination[0].agentid=3dfzD91MBABDtvfjvZeFjZw\=\
2357 agents[0].destination[0].failover.count=0
2358 agents[0].destination[0].params=<?xml version\="1.0"
2359 encoding\="UTF-8"?>\n<ParameterValues>\n <Parameter Name\="host"
2360 Value\="arcsight.es-sa-b1.test"/>\n <Parameter Name\="aupmaster"
2361 Value\="false"/>\n <Parameter Name\="filterevents"
2362 Value\="false"/>\n <Parameter Name\="port" Value\="8443"/>\n
2363 <Parameter Name\="fipsciphers"
2364 Value\="fipsDefault"/>\n</ParameterValues>\n
2365 agents[0].destination[0].type=http
2366 agents[0].deviceconnectionalertinterval=60000
2367 agents[0].enabled=true
2368 agents[0].entityid=3dfzD91MBABDtvfjvZeFjZw\=\
2369 agents[0].extractfieldnames=
2370 agents[0].extractregex=

```

```

2371 agents[0].extractsource=File Name
2372 agents[0].fcp.version=0
2373 agents[0].fixedlinelength=-1
2374 agents[0].followexternalrotation=true
2375 agents[0].id=3dfzD91MBABDtvfjvZeFjZw\=\=
2376 agents[0].internalevent.filecount.duration=-1
2377 agents[0].internalevent.filecount.enable=false
2378 agents[0].internalevent.filecount.minfilecount=-1
2379 agents[0].internalevent.filecount.timer.delay=60
2380 agents[0].internalevent.fileend.enable=true
2381 agents[0].internalevent.filestart.enable=true
2382 agents[0].logfilename=/opt/arcsight/connectors/syslogfiledata/OnGuards
2383 yslogExample.txt
2384 agents[0].maxfilesize=-1
2385 agents[0].onrotation=RenameFileInTheSameDirectory
2386 agents[0].onrotationoptions=processed
2387 agents[0].persistenceinterval=0
2388 agents[0].preservedstatecount=10
2389 agents[0].preservedstateinterval=30000
2390 agents[0].preservestate=false
2391 agents[0].roationonlywheneventexists=false
2392 agents[0].rotationdelay=30
2393 agents[0].rotationscheme=None
2394 agents[0].rotationsleepetime=10
2395 agents[0].startatend=false
2396 agents[0].type=sdkfilereader
2397 agents[0].unparsedevents.log.enabled=true
2398 agents[0].usealtermaterotationdetection=false
2399 agents[0].usefieldextractor=false
2400 agents[0].usenonlockingwindowsfilereader=false
2401 remote.management.second.listener.port=10051
2402 remote.management.ssl.organizational.unit=vRTB91MBABCASNGV81kQQ
2403 server.base.url=https\://arcsight.es-sa-b1.test\:8443
2404 server.registration.host=arcsight.es-sa-b1.test

```

## 2405 2.21.2.5 Additional Configuration Files

### 2406 2.21.2.5.1 Map File

- 2407 1. Create a file containing the text below and copy this file to: **/opt/arcsight/connector**  
**directory]/current/user/agent/map/map.1.properties**
- 2408 2. Note: if an existing map.1.properties file exists, increment the suffix as needed (e.g.  
**map.2.properties**)

```

2411 !Flags,CaseSens-,Overwrite
2412 regex.event.name,set.event.deviceVendor,set.event.deviceProduct
2413 .*On-Guard.*,ICS2,OnGuard
2414 .*OnGuard.*,ICS2,OnGuard

```

### 2.21.2.5.2 Categorization File

- 2416 1. Create a csv file containing the text below and copy this file to: **/opt/arcsight/connector**  
2417 **directory]/current/user/agent/acp/categorizer/current/[deviceproduct]/**  
2418 **deviceproduct.csv**

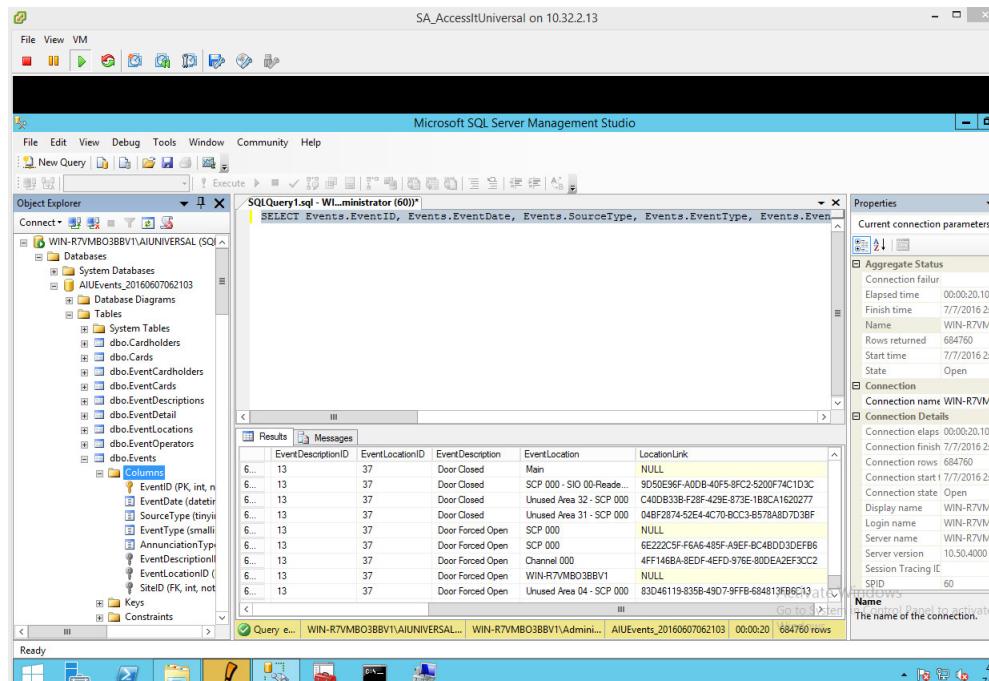
| event.<br>device<br>Product | set.event.<br>category<br>Object | set.event.<br>category<br>Behavior | set.event.<br>category<br>Technique | set.event.<br>category<br>DeviceGroup | set.event.<br>category<br>Significance | set.event.<br>category<br>Outcome |
|-----------------------------|----------------------------------|------------------------------------|--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

### 2.21.3 RS2 Access It! Universal.NET

#### 2.21.3.1 Review Data Source

- 2422 1. Review the relevant fields in Access It's Microsoft SQL Server Management Studio.

Figure 2.88

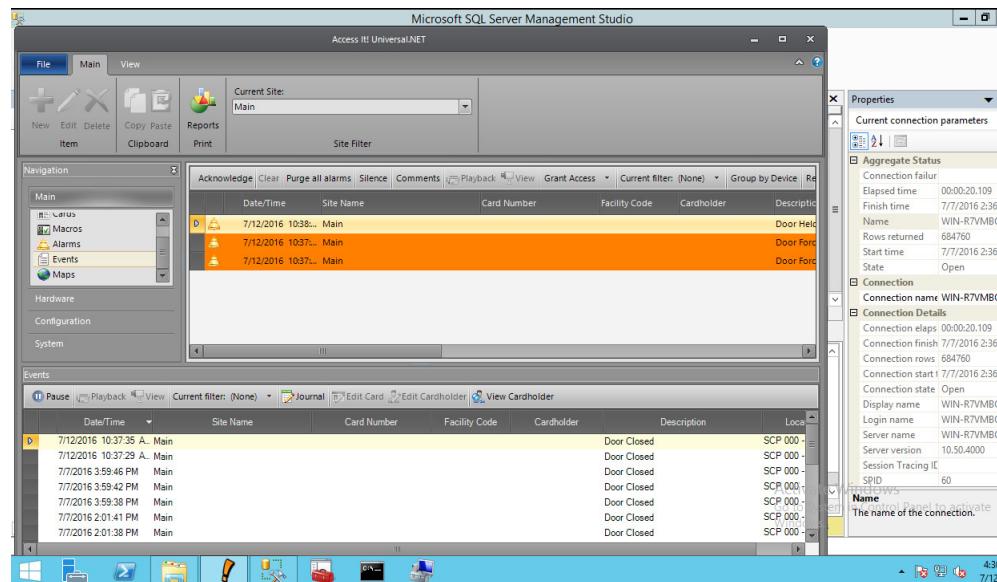


2424

- 2425 2. Review the data in RS2's Access It application.

2426

Figure 2.89



2427

### 2428 2.21.3.2 Install/Configure custom ArcSight FlexConnector

- 2429 1. On the Access It! server, follow ArcSight's instructions for installing a Microsoft
- 2430 Windows-based Flex Connector and specify the **Time Based Database** option.<sup>1</sup>
- 2431 2. Copy the custom FlexConnector configuration files to the appropriate locations
- 2432 a. See sections 6-8 of cyberlens-syslog-configuration-v2\_3.docx
- 2433 3. Start the Connector service via the **Windows Administrative Tools > Services** control panel
- 2434 item.

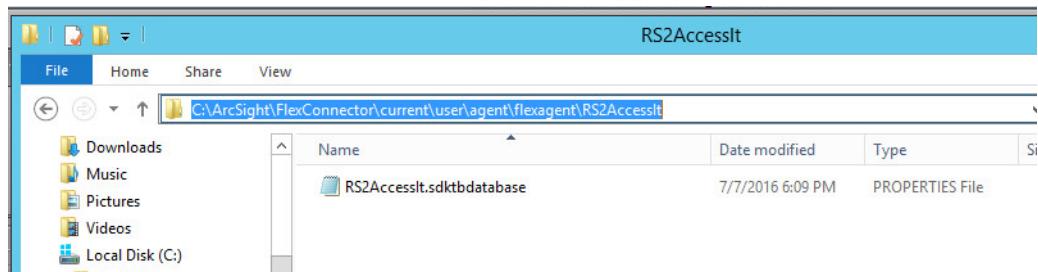
### 2435 2.21.3.3 Custom Parser - ArcSight FlexConnector Parser

2436 This parser will allow ArcSight to query the RS2 Access It SQL database for door controller event  
2437 data.

- 2438 1. Create a file containing the text below and copy this file to the connector installation  
2439 directory.
- 2440 2. Example location: C:\ArcSight\FlexConnector\user\agent\flexagent\RS2AccessIt

<sup>1</sup>HPE ArcSight SmartConnector User Guide - <https://www.protect724.hpe.com/docs/DOC-2279>

2441

**Figure 2.90 Example Location**

2442

```
2443 # Flex Connector for RS2 AccessIt Door Controller MS SQL Database
2444 version.id=1.0
2445 version.order=0
2446 version.query=SELECT Max(EventDate) FROM Events
2447
2448 # Pull events from which time period
2449 lastdate.query=SELECT Max(EventDate) FROM Events
2450
2451 additionaldata.enabled=true
2452
2453 # Database Query
2454 query= SELECT Events.EventID, Events.EventDate, Events.SourceType,
2455 Events.EventType, Events.EventDescriptionID, Events.EventLocationID,
2456 EventDescriptions.EventDescription \
2457 FROM Events \
2458 LEFT OUTER JOIN EventDescriptions ON Events.EventDescriptionID =
2459 EventDescriptions.EventDescriptionID \
2460 WHERE Events.EventDate > ? \
2461 ORDER BY Events.EventDate
2462
2463 # gets all the day's events once, and no new events
2464 #timestamp.field=Events.EventDate
2465 # gets events every time a new event occurs
2466 timestamp.field=EventDate
2467 uniqueid.fields=EventDescription,EventLocation,LocationLink
2468
2469 # DB Column Mapping
2470 event.deviceEventClassId=__concatenate(EventDescription,":",EventID)
2471 event.externalId=EventID
2472 event.endTime=EventDate
2473 event.name=EventDescription
2474 #event.message=EventLocation
2475 event.deviceCustomString1=SourceType
2476 event.deviceCustomString2=EventType
2477 event.deviceCustomString3=EventDescriptionID
```

```

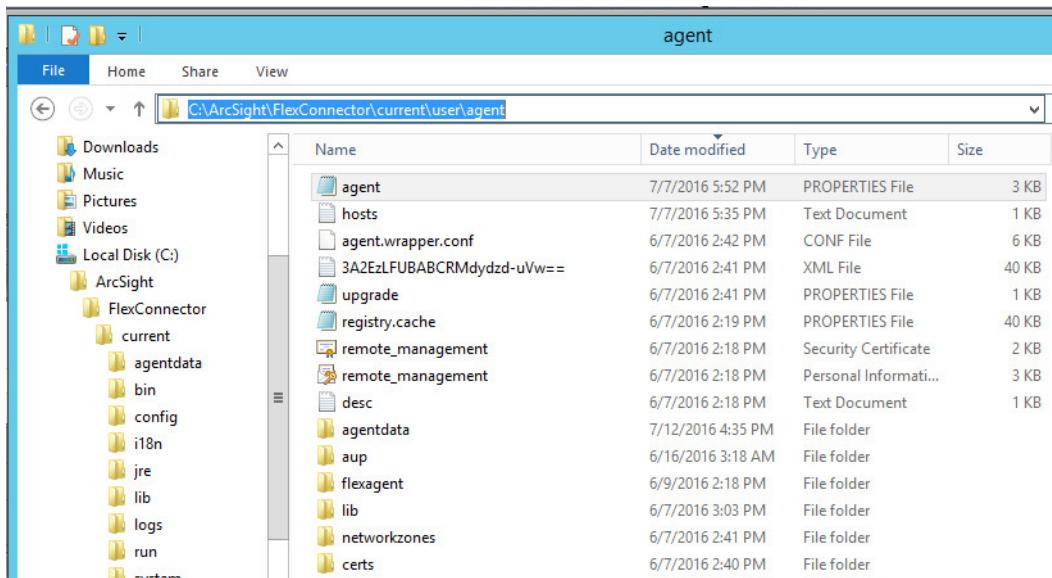
2478 event.deviceCustomString4=EventLocationID
2479 #event.deviceCustomString5=LocationLink
2480
2481 # Constants Mapping
2482 event.deviceVendor=__stringConstant(RS2)
2483 event.deviceProduct=__stringConstant(AccessIt)
2484 event.deviceCustomString1Label=__stringConstant(SourceType)
2485 event.deviceCustomString2Label=__stringConstant(EventType)
2486 event.deviceCustomString3Label=__stringConstant(EventDescriptionID)
2487 event.deviceCustomString4Label=__stringConstant(EventLocationID)
2488 #event.deviceCustomString5Label=__stringConstant(LocationLink)
2489
2490 # Severity Mapping
2491 event.deviceSeverity=EventDescription
2492 severity.map.veryhigh.if.deviceSeverity=Door Forced Open,Door Held
2493 Open
2494 severity.map.high.if.deviceSeverity=Power Loss,Comm Fail,Shutdown
2495 severity.map.medium.if.deviceSeverity=Door Closed,Door Open,Startup
2496 #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 your environment (refer to section above).

Figure 2.91 Example string/url



2503 #ArcSight Properties File

```
2504 #Thu Jul 28 17:02:44 EDT 2016
2505 agents.maxAgents=1
2506 agents[0].AgentSequenceNumber=0
2507 agents[0].JDBCDriver=com.microsoft.sqlserver.jdbc.SQLServerDriver
2508 agents[0].configfolder=RS2AccessIt
2509 agents[0].database=Default
2510 agents[0].dbcpcachestatements=false
2511 agents[0].dbcpchecktimeout=600
2512 agents[0].dbcpidletimeout=300
2513 agents[0].dbcpmaxcheckout=-1
2514 agents[0].dbcpmaxconn=5
2515 agents[0].dbcpreap=300
2516 agents[0].dbcproprefetch=-1
2517 agents[0].destination.count=1
2518 agents[0].destination[0].agentid=3B+tGM1YBABDj2XjY9XWuyg\=\=
2519 agents[0].destination[0].failover.count=0
2520 agents[0].destination[0].params=<?xml version\="1.0"
2521 encoding\="UTF-8"?>\n<ParameterValues>\n <Parameter
2522 Name\="aupmaster" Value\="false"/>\n <Parameter Name\="port"
2523 Value\="8443"/>\n <Parameter Name\="fipsiphers"
2524 Value\="fipsDefault"/>\n <Parameter Name\="host"
2525 Value\="arcsight.es-sa-b1.test"/>\n <Parameter Name\="filterevents"
2526 Value\="false"/>\n</ParameterValues>\n
2527 agents[0].destination[0].type=http
2528 agents[0].deviceconnectionalertinterval=60000
2529 agents[0].enabled=true
2530 agents[0].entityid=YdZKM1YBABCAAwkPuy5kNg\=\=
2531 agents[0].fcp.version=0
2532 agents[0].frequency=45
2533 agents[0].id=3B+tGM1YBABDj2XjY9XWuyg\=\=
2534 agents[0].initretrysleepetime=60000
2535 agents[0].jdbcquerytimeout=-1
2536 agents[0].jbdbctimeout=240000
2537 agents[0].loopingenabled=false
2538 agents[0].password=OBFUSCATE.4.8.1\::tn7+FHJvO5qkdFrnyHeng\=\=
2539 agents[0].passwordchangeingcharsets=UPPERCASE\=ABCDEFGHIJKLMOPQR
2540 STUVWXYZ, LOWERCASE\=abcdefghijklmnopqrstuvwxyz, NUMBER\=01234567890, SPE
2541 CIAL\=+-\!@\#$%&*()
2542 agents[0].passwordchangingcharersetdelimiter=,
2543 agents[0].passwordchangingenabled=false
2544 agents[0].passwordchanginginterval=86400
2545 agents[0].passwordchanginglength=16
2546 agents[0].passwordchangingtemplate=UPPERCASE, NUMBER, SPECIAL, UPPERCASE |
2547 LOWERCASE | NUMBER, UPPERCASE | LOWERCASE | NUMBER | SPECIAL
2548 agents[0].persistenceinterval=1
```

```

2549 agents[0].preservedstatecount=10
2550 agents[0].preservedstateinterval=30000
2551 agents[0].preservestate=true
2552 agents[0].rotationtimeout=30000
2553 agents[0].startatend=true
2554 agents[0].type=sdktbdatabase
2555 agents[0].unparsedevents.log.enabled=false
2556 agents[0].url=jdbc\:sqlserver\::10.100.2.102\:1433;datasasename\=AIUE
2557 vents_20160607062103
2558 agents[0].useconnectionpool=true
2559 agents[0].user=OBFUSCATE.4.8.1\:LkwoJdKuWx8CDMiRZv4Qpg\=\=
2560 remote.management.second.listener.port=10050
2561 remote.management.ssl.organizational.unit=rE09M1YBABCQkPuy5kNg

```

### 2.21.3.5 Categorization File

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://www.protect724.hpe.com/docs/DOC-2279>
2. Syslog Guide  
<https://www.protect724.hpe.com/docs/DOC-2583>
3. SmartConnector Quick Reference  
<https://www.protect724.hpe.com/docs/DOC-12938>
4. HPE ArcSight FlexConnector Developer's Guide  
<https://www.protect724.hpe.com/docs/DOC-2280>
5. FlexConnector Quick Reference  
<https://www.protect724.hpe.com/docs/DOC-13759>

# 3 Test Cases/Alert Configurations

|   |                           |     |
|---|---------------------------|-----|
| 2 | 3.1 ArcSight Filters..... | 119 |
| 3 | 3.2 Test Cases .....      | 134 |
| 4 |                           |     |

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

## 7 3.1 ArcSight Filters

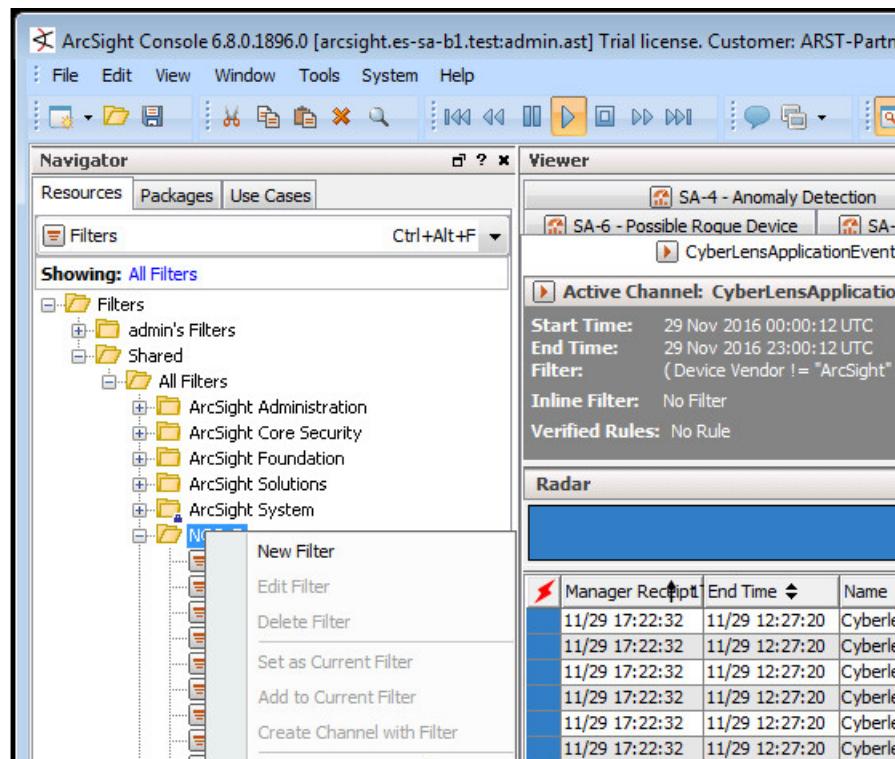
8 The following sections describe the creation of filters and what filters were used in the build.

### 9 3.1.1 Filter Creation

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

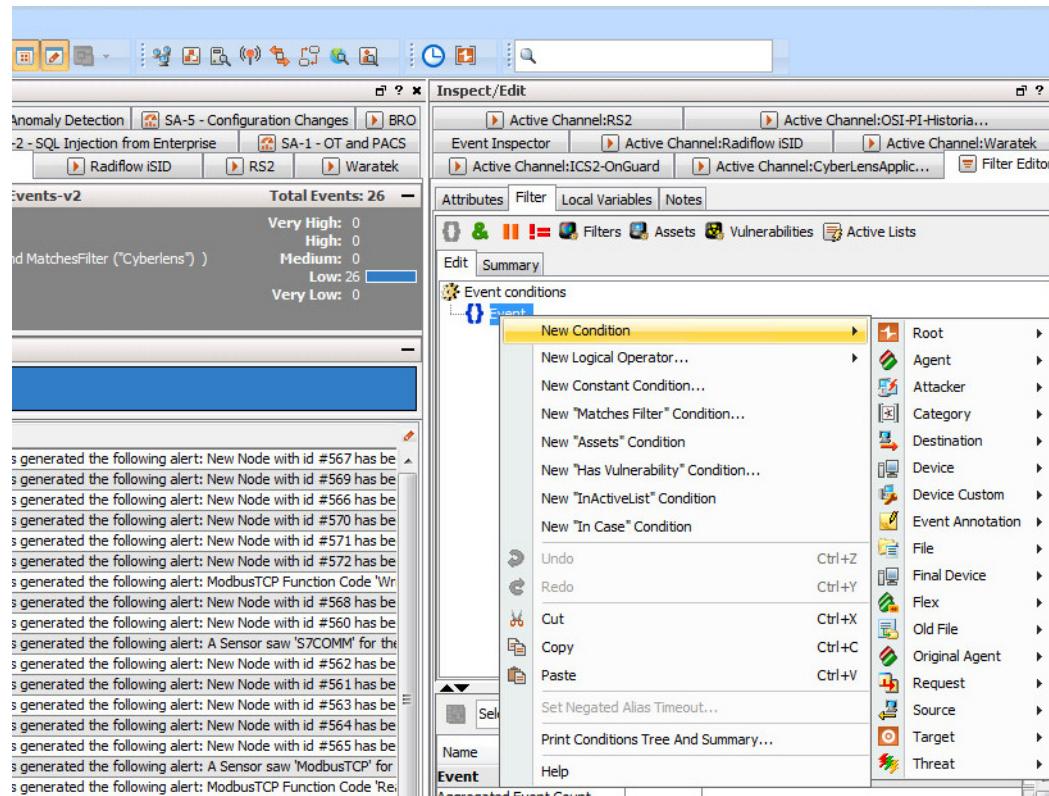
- 12 1. Go to the ArcSight navigation pane on the left.
- 13 2. Select **Filters** from the drop down menu.
- 14 3. Right-click on a folder location.
- 15 4. Select **New Filter** from the popup menu.

16 **Figure 3.1 Create New Filter**



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

20

**Figure 3.2 Create Conditions (Logic)**

21

7. Next, begin constructing the conditions that you wish to query the ArcSight database for.

22

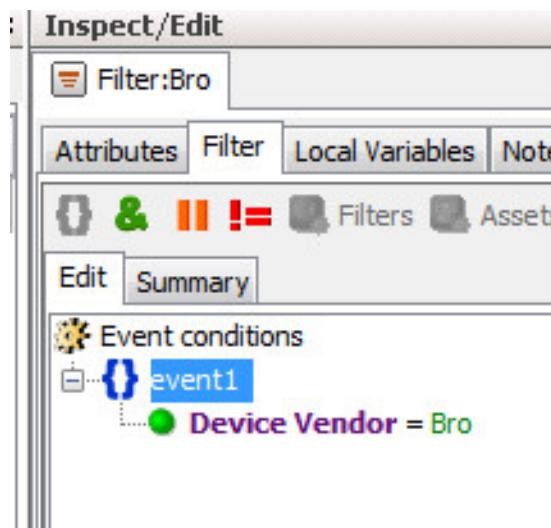
*Note: It is customary to create a central folder to house ArcSight content and allow it to be shared by groups of users. Once content (such as filters) have been tested the content can then be copied or moved to the group (shared) folder. Permissions can be set on the folder to control access as needed.*

27

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

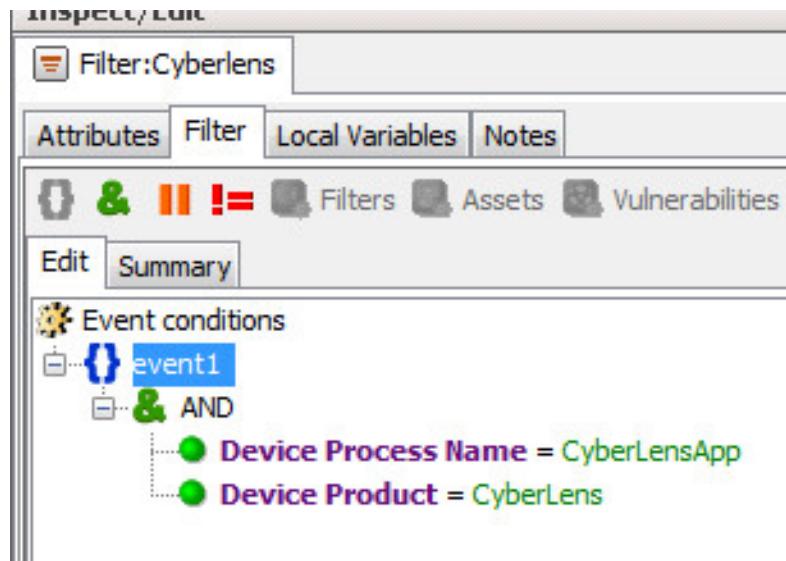
28

29

**Figure 3.3 Bro Filter**

30

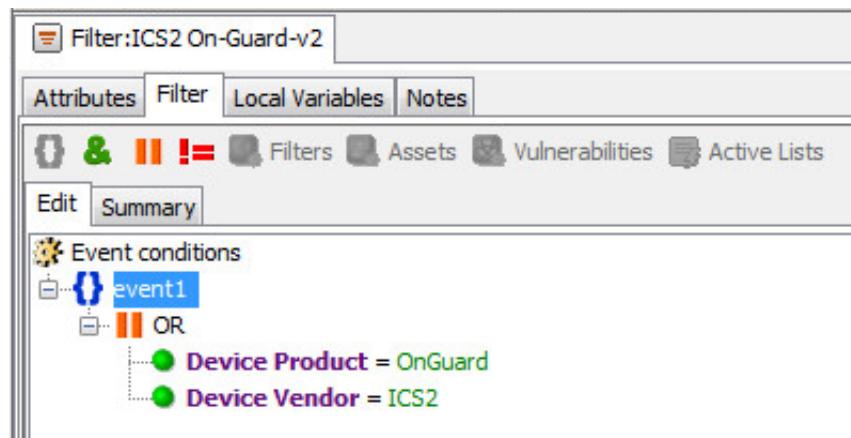
31

**Figure 3.4 Dragos CyberLens Filter**

32

33

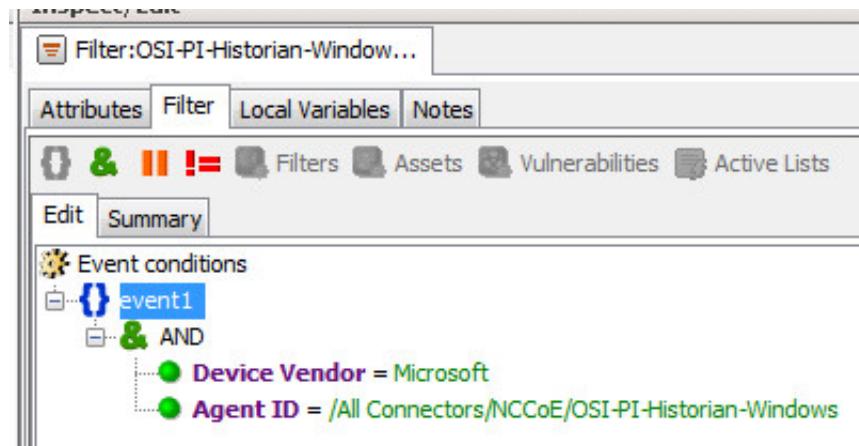
Figure 3.5 ICS2 On-Guard Filter



34

35

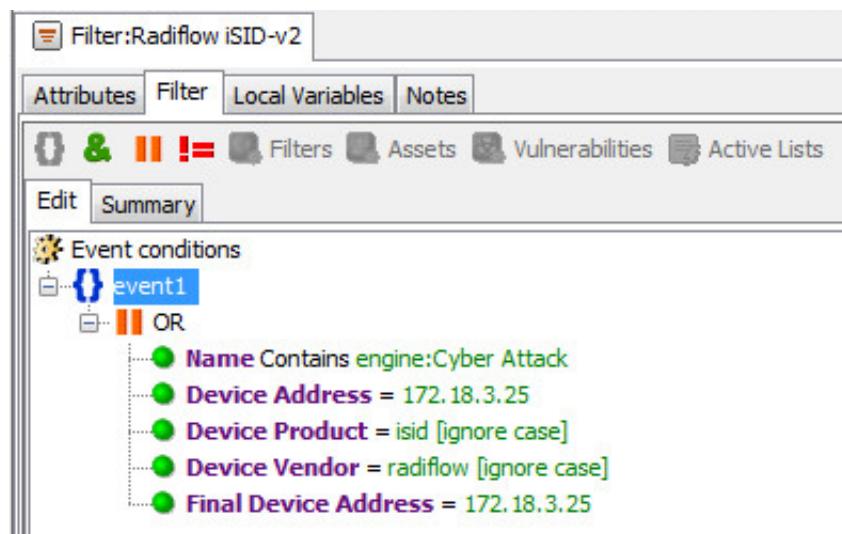
Figure 3.6 Windows log filter for OSI PI Historian



36

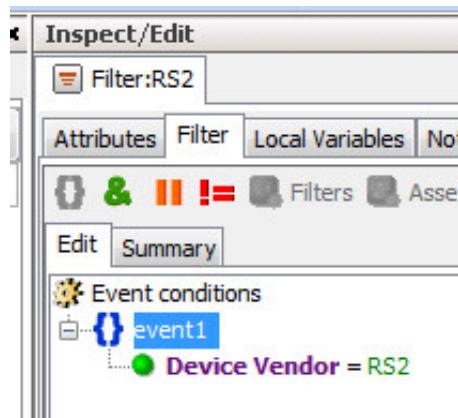
37

Figure 3.7 Radiflow iSID Filter



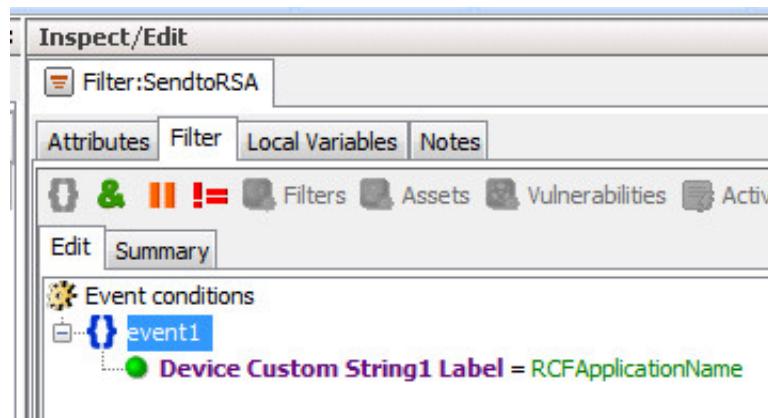
38

39

**Figure 3.8 RS2 AccessIT Filter**

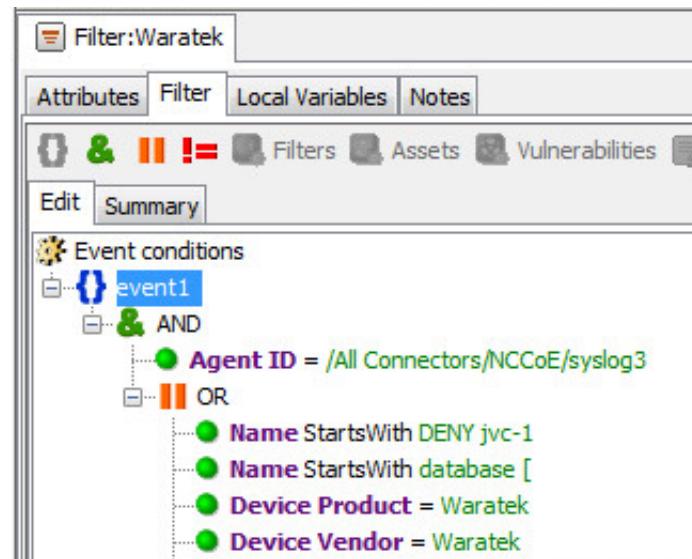
40

41

**Figure 3.9 RSA Archer Filter**

42

43

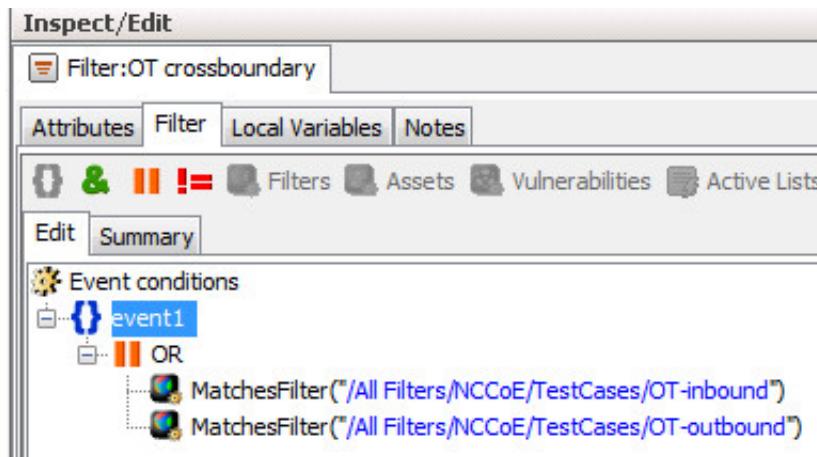
**Figure 3.10 Waratek Filter**

44

45 Below are Filters that were created to match against conditions based on:

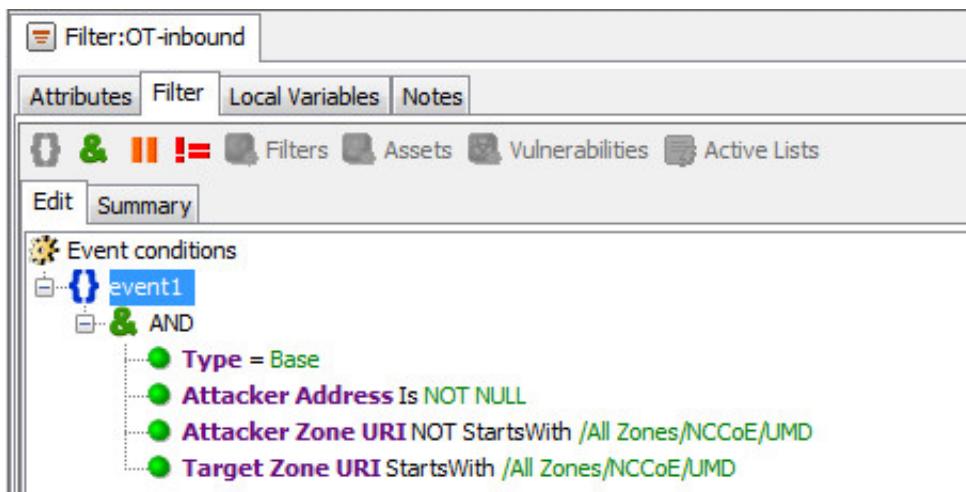
- 46   ■ direction of network activity  
47   ■ awareness of Security Zones (OT vs non OT)

48 **Figure 3.11 OT Cross-Boundary Filter**



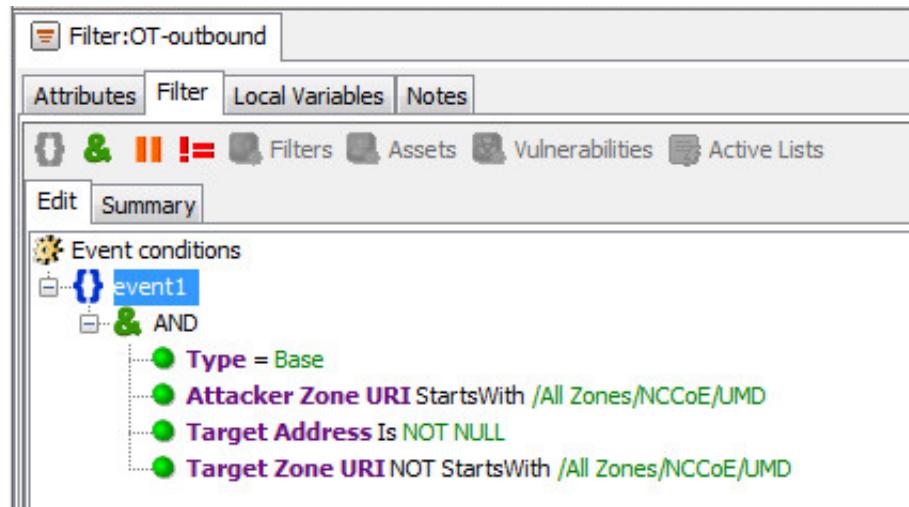
49

50 **Figure 3.12 OT Inbound Filter**



51

52

**Figure 3.13 OT Outbound Filter**

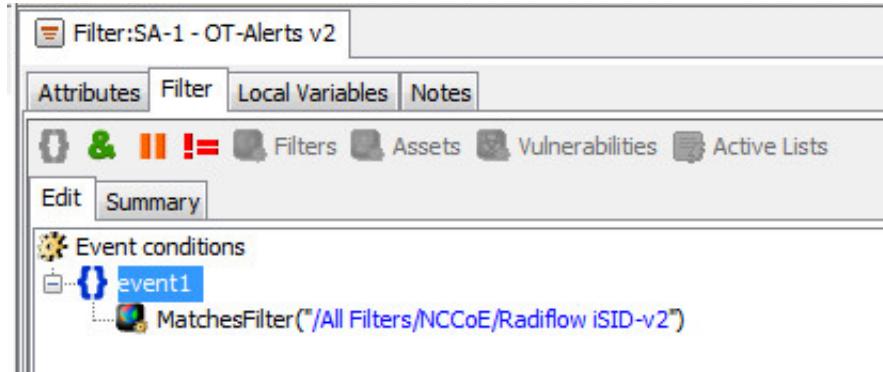
53

### 3.1.2 ArcSight Test Cases

54

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.

55

**Figure 3.14 SA-1 - OT-Alerts Filter**

56

59

**Figure 3.15 SA-1 - OT and PACS Dashboard**

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 | 2        |
| 15 Dec 2016 03:17:00 UTC | Cleared Alarm    |                       | RS2           | LAB Analysis Zone - Level5 | 2        |
| 14 Dec 2016 22:57:00 UTC | Cleared Alarm    |                       | RS2           | LAB Analysis Zone - Level5 | 2        |
| 14 Dec 2016 21:29:00 UTC | Cleared Alarm    |                       | RS2           | LAB Analysis Zone - Level5 | 2        |
| 14 Dec 2016 21:28:00 UTC | Cleared Alarm    |                       | RS2           | LAB Analysis Zone - Level5 | 2        |
| 14 Dec 2016 17:30:07 UTC | Door Held Open   | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | 2        |
| 14 Dec 2016 17:29:37 UTC | Door Forced Open | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | 8        |
| 14 Dec 2016 17:29:36 UTC | Door Closed      | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | 8        |
| 14 Dec 2016 17:29:35 UTC | Door Forced Open | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | 5        |
| 14 Dec 2016 17:29:34 UTC | Door Closed      | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | 8        |
| 14 Dec 2016 17:29:30 UTC | Door Forced Open | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | 5        |
| 14 Dec 2016 17:29:29 UTC | Door Closed      | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | 8        |
| 14 Dec 2016 17:29:28 UTC | Door Forced Open | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | 5        |
| 13 Dec 2016 21:17:24 UTC | Door Held Open   | /PhysicalAccessSystem | RS2           | LAB Analysis Zone - Level5 | 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 |      |               |                |          |

60

61

**Figure 3.16 SA-1 OT and PACS Active Channel**

ArcSight Console 6.0.0.1896.0 [arcights.es-sa-b1.test.admin.est] Trial license. Customer ARST-Partner, Expiration date: 2017/02/01

Navigator Resources Packages Use Cases Ctrl+Alt+A

Showing: All Channels Active Channels

- ad hoc channels
  - arcSight
  - RSA-SecOps-Rule-Files
- Shared
  - All Active Channels
    - arcSight Administration
    - arcSight Core Security
    - arcSight Foundations
    - arcSight Integrations
    - arcSight System
    - NCCoE
    - OSPF-Anywhere->v2
    - Radflow ISD
    - ISD
    - SendtoSA
    - syslog3
    - syslog4
    - TestCases
    - SA-1 - OT and PACS
    - SA-2 - IT to OT AppAttack
    - SA-3 - OT to IT or OT Badlogs
    - SA-4 - OT Anomaly
    - SA-5 - ConfigChange
    - SA-6 - RogueDevice
- Personal
- Public
- Unassigned

Active Channel: SA-1 - OT and PACS

Start Time: 13 Dec 2016 08:18:41 UTC End Time: 13 Dec 2016 23:18:41 UTC Filter: (MatchedFilter OR (MatchedFilter AND MatchedFilter ("Radflow ISD->v2")))

Inline Filter: No Filter Verified Rules: No Rule

Total Events: 35

Very High: 0 Medium: 27 Low: 0 Very Low: 1

Radar

Event Inspector Active Channel:SA-1 - OT and PACS

Event Filter Sort Fields Local Variables Notes

Event Conditions
 

- OR
  - MatchedFilter (/AI Filters/NCCoE:RS2)
  - MatchedFilter (/AI Filters/ISD->v2)

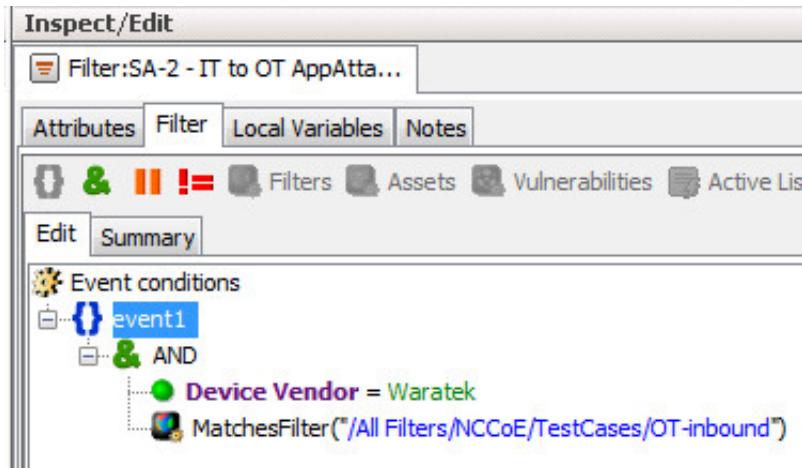
Attributes Filter Sort Fields Assets Vulnerabilities Active Lists

Event Grid

62

63

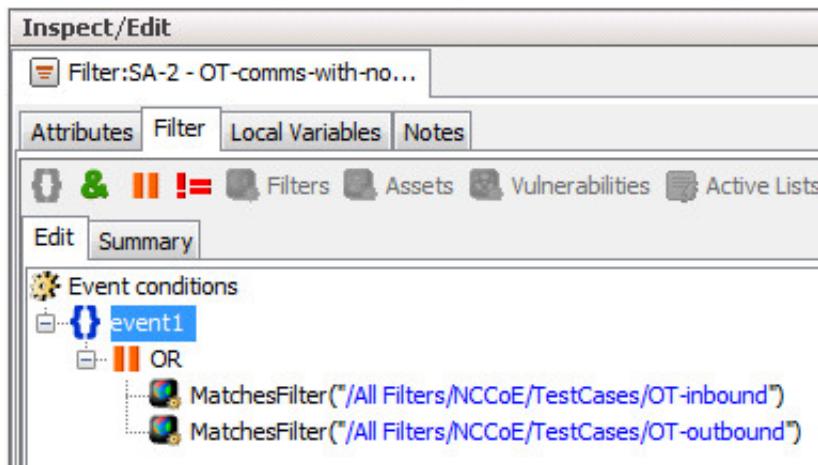
Figure 3.17 SA-2 - IT to OT AppAttack Filter



64

65

Figure 3.18 SA-2 OT-comms-with-non-OT Filter



66

67

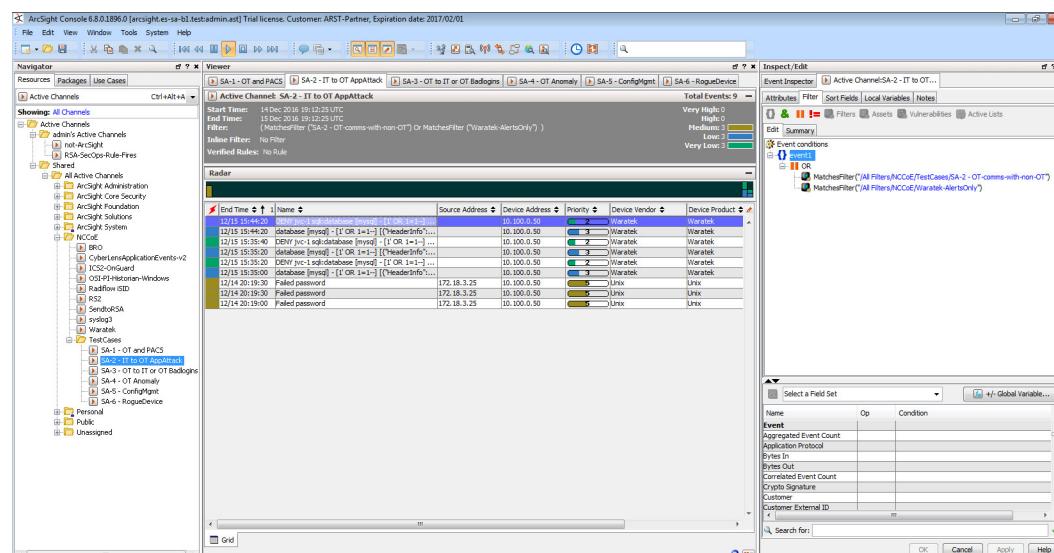
Figure 3.19 108. SA-2 SQL Injection Dashboard

| SA-2 - IT to OT AppAttack |                                                                                                                                                                        | SA-2 - SQL Injection from Enterprise |          | SA-3 - OT-to-IT or FailedLogins |  |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|----------|---------------------------------|--|
| 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", "servletPath": "/MySql_Get..."}, "method": "GET", "path": "/MySql_Get..."}] | Waratek                              | 2        |                                 |  |
| 8 Dec 2016 20:50:08 UTC   | database [mysql] - [1' OR 1=1-] [{"HeaderInfo": {"remoteAddr": "127.0.0.1", "servletPath": "/MySql_Get..."}, "method": "GET", "path": "/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", "servletPath": "/MySql_Get..."}, "method": "GET", "path": "/MySql_Get..."}] | Waratek                              | 2        |                                 |  |
| 25 Oct 2016 18:00:57 UTC  | database [mysql] - [1' OR 1=1-] [{"HeaderInfo": {"remoteAddr": "127.0.0.1", "servletPath": "/MySql_Get..."}, "method": "GET", "path": "/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", "servletPath": "/MySql_Get..."}, "method": "GET", "path": "/MySql_Get..."}] | waratek                              | 2        |                                 |  |
| 25 Oct 2016 17:55:57 UTC  | database [mysql] - [1' OR 1=1-] [{"HeaderInfo": {"remoteAddr": "127.0.0.1", "servletPath": "/MySql_Get..."}, "method": "GET", "path": "/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", "servletPath": "/MySql_Get..."}, "method": "GET", "path": "/MySql_Get..."}] | waratek                              | 2        |                                 |  |
| 25 Oct 2016 17:46:07 UTC  | database [mysql] - [1' OR 1=1-] [{"HeaderInfo": {"remoteAddr": "127.0.0.1", "servletPath": "/MySql_Get..."}, "method": "GET", "path": "/MySql_Get..."}]                | waratek                              | 3        |                                 |  |

68

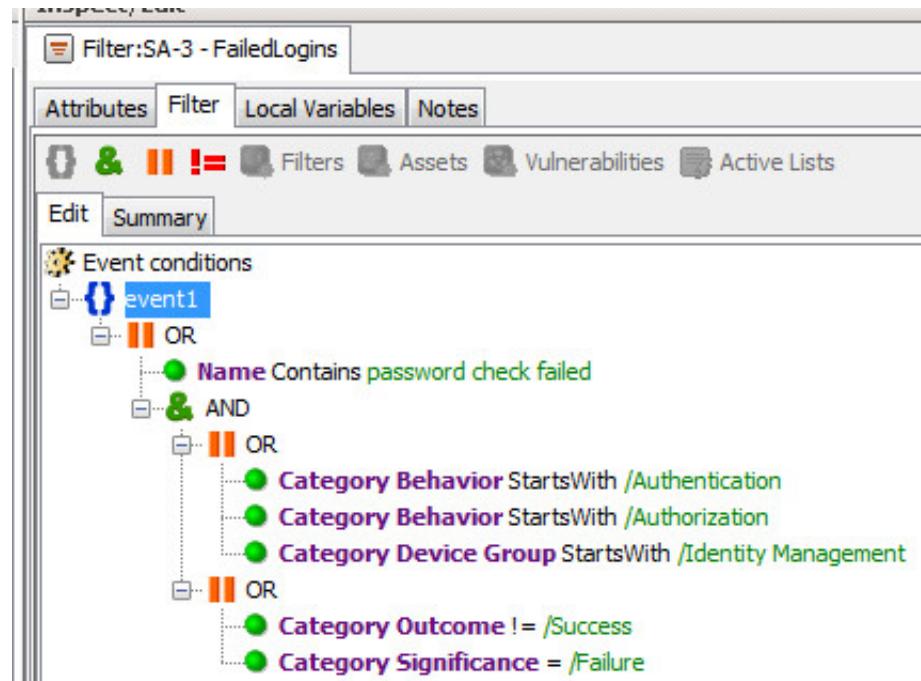
69

Figure 3.20 SA-2 SQL Injection Active Channel



70

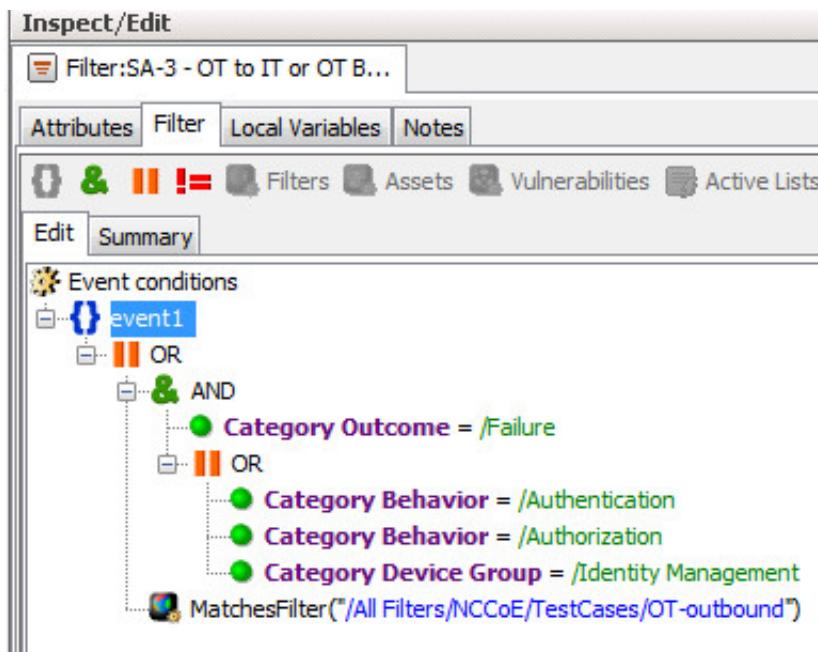
Figure 3.21 SA-3 - FailedLogins Filter



72

73

Figure 3.22 SA-3 OT to IT or OT BadLogins Filter



74

75

Figure 3.23 SA-3 OT-to-IT or FailedLogins Dashboard

The dashboard has a header with tabs: SA-1 - OT and PACS, SA-2 - SQL Injection from Enterprise, SA-3 - OT-to-IT or Failed.logins (selected), SA-4 - Anomaly Detection, SA-5 - Configuration Changes, and SA-6 - Possible Rogue Device.

**SA-3 - FailedLogins:**

| End Time                 | Name                             | Category Behavior      | Category Object           | Device Vendor | Priority |
|--------------------------|----------------------------------|------------------------|---------------------------|---------------|----------|
| 15 Dec 2016 12:04:41 UTC | unix_chkpwd[27074]: password ... |                        |                           |               | 2        |
| 15 Dec 2016 17:06:20 UTC | 41 ubuntu unix_chkpwd[27074]...  | /Communicate/Query     | /Host/Application/Service | Unix          | 7        |
| 14 Dec 2016 20:19:40 UTC | more authentication failures     | /Authentication/Verify | /Host/Operating System    | Unix          | 5        |
| 14 Dec 2016 20:19:30 UTC | Failed password                  | /Authentication/Verify | /Host/Application/Service | Unix          | 5        |
| 14 Dec 2016 20:19:30 UTC | Failed password                  | /Authentication/Verify | /Host/Application/Service | Unix          | 5        |
| 14 Dec 2016 20:19:20 UTC | more authentication failures     | /Authentication/Verify | /Host/Operating System    | Unix          | 5        |
| 14 Dec 2016 20:19:00 UTC | Failed password                  | /Authentication/Verify | /Host/Application/Service | Unix          | 5        |
| 14 Dec 2016 03:19:56 UTC | unix_chkpwd[8925]: password ...  |                        |                           |               | 2        |
| 14 Dec 2016 03:19:43 UTC | unix_chkpwd[8923]: password ...  |                        |                           |               | 2        |
| 14 Dec 2016 03:19:43 UTC | unix_chkpwd[8923]: password ...  |                        |                           |               | 2        |
| 14 Dec 2016 16:33:00 UTC | 56 ubuntu unix_chkpwd[8923]...   | /Communicate/Query     | /Host/Application/Service | Unix          | 7        |
| 14 Dec 2016 16:33:00 UTC | 56 ubuntu unix_chkpwd[8925]...   | /Communicate/Query     | /Host/Application/Service | Unix          | 7        |
| 14 Dec 2016 16:33:00 UTC | 43 ubuntu unix_chkpwd[8923]...   | /Communicate/Query     | /Host/Application/Service | Unix          | 7        |
| 14 Dec 2016 16:33:00 UTC | 43 ubuntu unix_chkpwd[8923]...   | /Communicate/Query     | /Host/Application/Service | Unix          | 7        |
| 14 Dec 2016 03:19:24 UTC | NetworkManager[991]: <warn...    |                        |                           |               | 2        |

**Timeline Chart:**

10/13 21:01:27 - 12/15 17:01:31

**SA-3 - OT-to-non-OT comms - last15:**

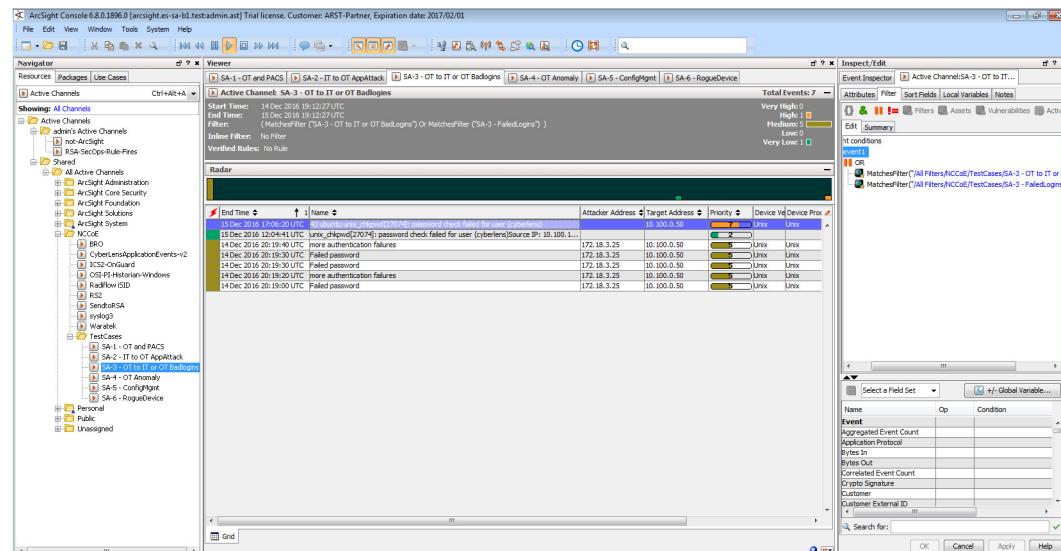
| End Time                        | Name | Device Address | Device Host Name | Device Zone Name | Priority |
|---------------------------------|------|----------------|------------------|------------------|----------|
| 12/15 17:22:44 - 12/15 17:22:48 |      |                |                  |                  |          |

Data last refreshed: 12/15 20:00:06

76

77

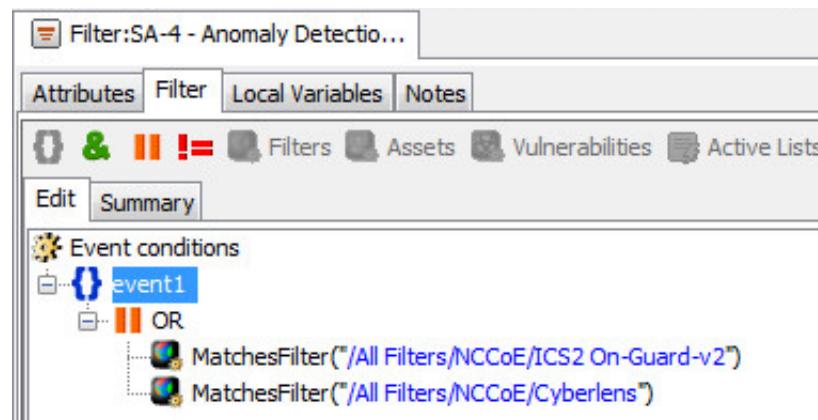
Figure 3.24 SA-3 OT-to-IT or FailedLogins Active Channel



78

79

Figure 3.25 SA-4 Anomaly Detection Filter



80

81

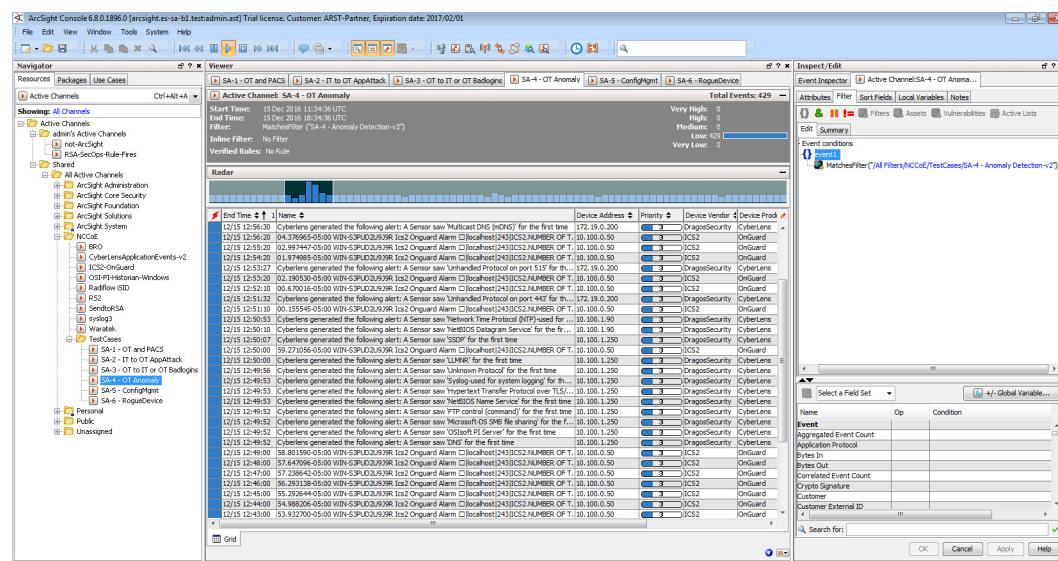
Figure 3.26 SA-4 Anomaly Detection Dashboard

| SA-4 - Anomaly Detection |                                                    | Device Ve...<br>OnGuard<br>3 | Device ...<br>OnGuard<br>3                                       | Priority<br>3 |
|--------------------------|----------------------------------------------------|------------------------------|------------------------------------------------------------------|---------------|
| End Time                 | Name                                               |                              |                                                                  |               |
| 15 Dec 2016 20:00:40 UTC | 32.905463-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:59:40 UTC | 30.998907-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:58:40 UTC | 30.470453-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:57:50 UTC | 30.191992-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:56:50 UTC | 29.310588-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:55:40 UTC | 28.823047-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:54:30 UTC | 27.877579-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:53:30 UTC | 27.245086-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:52:30 UTC | 26.570606-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:51:30 UTC | 25.714121-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:50:30 UTC | 25.158658-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:49:30 UTC | 23.287124-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:48:30 UTC | 23.322682-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:47:30 UTC | 22.786209-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:46:30 UTC | 22.088800-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:45:30 UTC | 20.269199-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:44:30 UTC | 20.438768-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:43:30 UTC | 19.521282-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:42:30 UTC | 18.961810-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:41:20 UTC | 17.971327-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:40:20 UTC | 17.430855-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:39:20 UTC | 16.338352-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:38:20 UTC | 15.780880-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |
| 15 Dec 2016 19:37:20 UTC | 15.069412-05:00 WIN-S3PUD2U9J9R.Ics2.Onguard.Alarm | localhost[243]               | IC52.NUMBER OF TAGS WITH NEW DATA No new data in DB for too lo.. | IC52          |

82

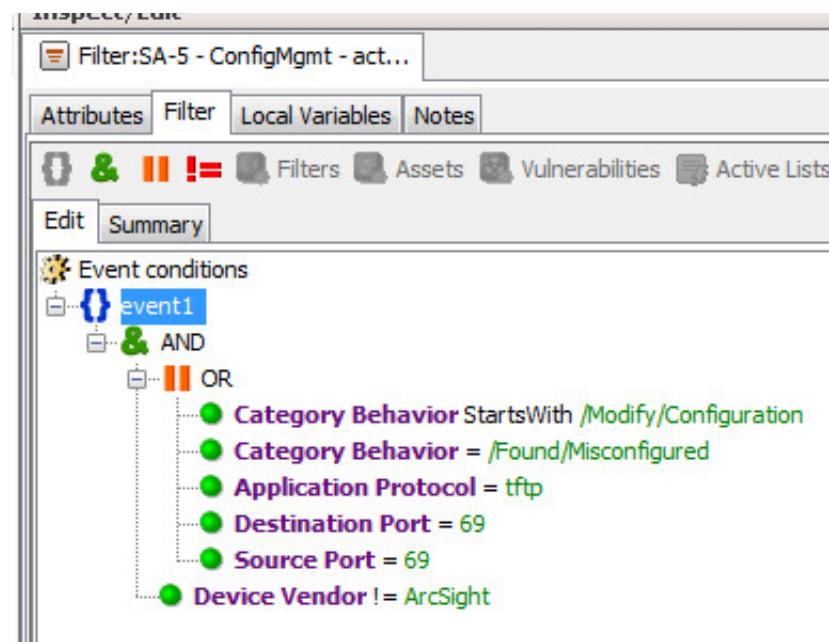
83

Figure 3.27 Anomaly Detection Active Channel



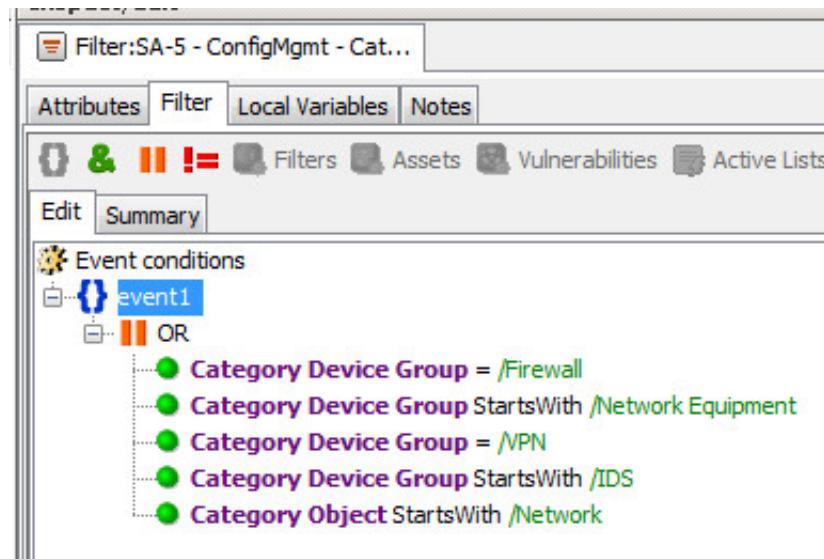
84

Figure 3.28 SA-5 ConfigMgmt Filter



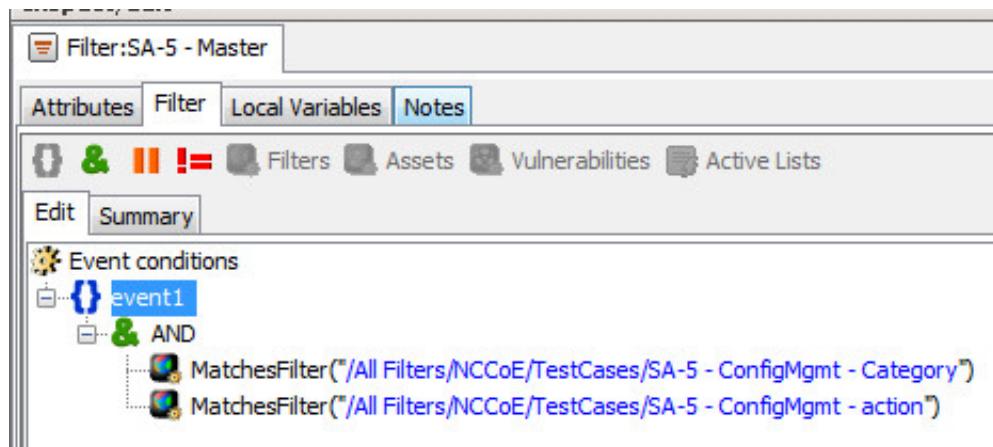
85

87

**Figure 3.29 SA-5 ConfigMgmt Filter**

88

89

**Figure 3.30 SA-5 Master Filter**

90

91

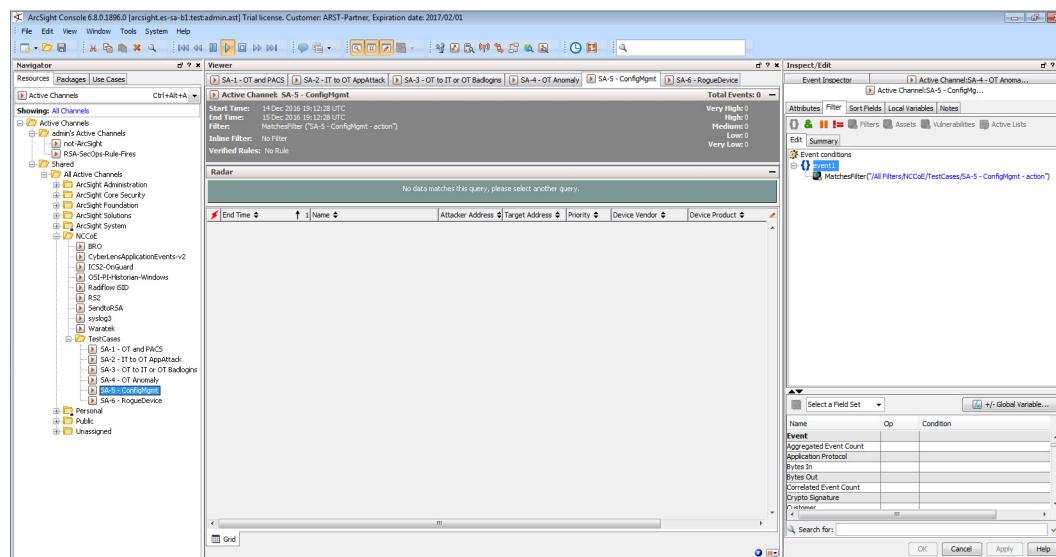
**Figure 3.31 SA-5 Configuration Changes Dashboard**

| SA-5 - Configuration Changes          |      |                   |                       |                 |                  |
|---------------------------------------|------|-------------------|-----------------------|-----------------|------------------|
| SA-5 - Configuration Changes - last15 |      |                   |                       |                 |                  |
| End Time                              | Name | Category Behavior | Category Device Group | Category Object | Category Outcome |
|                                       |      |                   |                       |                 |                  |

92

93

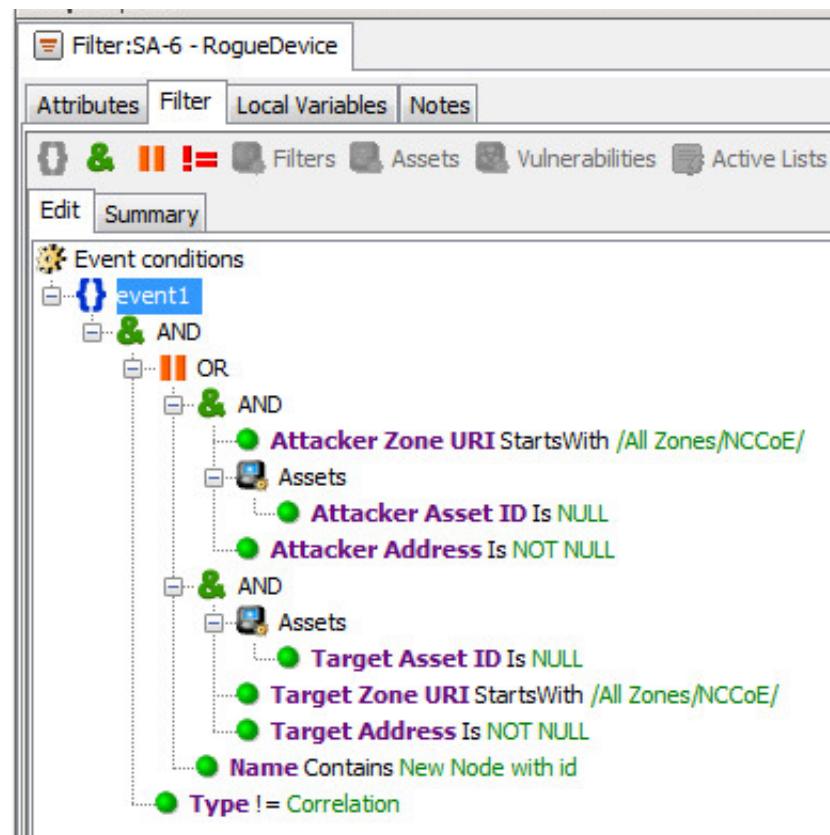
Figure 3.32 SA-5 Configuration Changes Active Channel



94

95

Figure 3.33 SA-6 RogueDevice Filter



96

97

**Figure 3.34 SA-6 - Rogue Device Dashboard**

The dashboard shows a timeline from 12/15 17:16:48 to 12/15 17:16:53. A table at the top lists alerts: 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, and SA-6 - Possible Rogue Device. Below the table is a graph with a red rectangle and a cyan circle connected by arrows. A tooltip below the graph indicates: "10.100.123.100 | LAB Analysis Zone - Level5 account was successfully logged on | 10.100.1.76 | NULL | LAB Analysis Zone - Level5". Another smaller graph below shows a red rectangle connected to a cyan circle with the text "Failed password" and "Authentication failures".

98

**Figure 3.35 SA-6 - Rogue Device Active Channel**

The screenshot shows the ArcSight Console interface with the title bar "ArcSight Console 6.8.0.1896.0 [arcshift.es-sa-b1.test.admin.es]" and the message "Trial license, Customer: ARST-Partner, Expiration date: 2017/02/01". The left sidebar shows categories like Active Channels, Active Assets, and Personal. The main area displays a grid of log entries under the heading "Active Channel: SA-6 - Possible RogueDevice". The grid columns include End Time, Name, Attacker Zone URL, Target Zone URL, Source Asset, Destination Asset, Resource Address, Destination Priority, Device Type, and Status. Most entries show successful logins from various IP addresses (e.g., 172.18.3.25, 10.100.123.100) to the "OSI PI Historian LAB" asset in the "All Zones(NCCe) LAB" zone. The status column shows mostly "Success" and some "Failure".

100

## 3.2 Test Cases

102

Below are descriptions of test cases as matched to [Section 3.6](#) of NIST SP1800-7b

103 **3.2.1 SA-1 Event Correlation for OT and PACS**

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

106 **3.2.1.1 Events**

- 107        1. Technician accesses sub-station/control-station  
108        2. OT device goes down

109 **3.2.1.2 Desired Outcome**

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

111 **3.2.1.3 ArcSight Content**

- 112        1. OT network Zones  
113        2. Filter for OT network Zones  
114        3. Filters for OT/IT inbound, outbound, cross-boundary communications  
115        4. Filter for RS2 Door Controller events  
116        5. Filter for Cyberlens or iSID events  
117        6. Active List for RS2 Door Controller events with time threshold  
118        7. Rule to add RS2 Door Controller Filter events to Active List  
119        8. Data Monitor and Dashboard to display results of the above

120 **3.2.2 SA-2 Event Correlation for OT and IT**

121        The Enterprise (IT) java application communication with an OT device (Historian) is used as a  
122        vector for SQL injection (SQLi), which also includes data exfiltration attempts.

123 **3.2.2.1 Events**

124        Detection of SQL Injection attack on IT device interconnected with OT device.

125 **3.2.2.2 Desired Outcome**

126        Alert sent to SIEM on multiple SQLi attempts.

127 **3.2.2.3 ArcSight Content**

- 128        1. Filter for Waratek events (intended to monitor for SQLi against the OSIsoft PI Historian)  
129        2. Filter to combine Waratek and OT/IT inbound communications Filters

130           3. Data Monitor and Dashboard to display results of the above

### 131 3.2.3 SA-3 Event Correlation for OT and IT / PACS and OT

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

#### 138 3.2.3.1 Events

139           Inbound/outbound connection attempts from devices outside of authorized and known  
140           inventory.

#### 141 3.2.3.2 Desired Outcome

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

#### 144 3.2.3.3 ArcSight Content

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

### 151 3.2.4 SA-4 Data Infiltration Attempts

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

#### 156 3.2.4.1 Events

157           Anomalous behavior falling outside defined baseline.

158 **3.2.4.2 Desired Outcome**

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

161 **3.2.4.3 ArcSight Content**

- 162 1. Use OT network Zones  
163 2. Use Filter for OT network Zones  
164 3. Filter for ICS<sup>2</sup> OnGuard events or events with a Category of "Traffic Anomaly" (e.g. as  
165 defined in Dragos Security Cyberlens Arcsight FlexConnector/Categorizer files)  
166 4. Data Monitor and Dashboard to display results of the above

167 **3.2.5 SA-5 Configuration Management**

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

171 **3.2.5.1 Events**

172 Configuration change on Tofino FW, Cisco 2950.

173 **3.2.5.2 Desired Outcome**

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

175 **3.2.5.3 ArcSight Content**

- 176 1. Filter for any of the following:  
177     a. ArcSight Category events:  
178         i. /Modify/Configuration  
179         ii. /Found/Misconfigured  
180         iii. tftp protocol  
181         iv. tftp port  
182 2. Filter for following ArcSight Category Device Groups:  
183     a. /Firewall  
184     b. /Network Equipment  
185     c. /VPN  
186     d. /IDS  
187     e. or Category Object:

188 i. /Network

189 3. Data Monitor and Dashboard to display results of the above

190 **3.2.6 SA-6 Rogue Device Detection**

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

193 **3.2.6.1 Events**

194 Unidentified device appears on ICS network.

195 **3.2.6.2 Desired Outcome**

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

197 **3.2.6.3 ArcSight Content**

198 1. Specific Asset definitions for all known ICS devices (grouped by OT Zones)

199 2. Filter to detect presence of any "non-ICS" devices (not in Asset lists)

200 3. Filter for CyberLens events alerting on "new" hosts

201 4. Data Monitor and Dashboard to display results of the above

## Appendix A

## Acronyms

|              |                                                  |
|--------------|--------------------------------------------------|
| <b>CA</b>    | Certificate Authority                            |
| <b>CSF</b>   | Cybersecurity Framework                          |
| <b>DMZ</b>   | Demilitarized Zone                               |
| <b>EACMS</b> | Electronic Access Control and Monitoring Systems |
| <b>ICS</b>   | Industrial Control Systems                       |
| <b>IdAM</b>  | Identity and Access Management                   |
| <b>IDS</b>   | Intrusion Detection System                       |
| <b>IT</b>    | Information Technology                           |
| <b>ITAM</b>  | Information Technology and Asset Management      |
| <b>NCCoE</b> | National Cybersecurity Center of Excellence      |
| <b>OT</b>    | Operational Technology                           |
| <b>PAC</b>   | Physical Access Control                          |
| <b>PACS</b>  | Physical Access Control Systems                  |
| <b>PEP</b>   | Policy Enforcement Point                         |
| <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>SIEM</b>  | Security Information and Event Management        |
| <b>SQL</b>   | Structured Query Language                        |
| <b>SQLi</b>  | Structured Query Language Injection              |
| <b>UMd</b>   | University of Maryland                           |
| <b>VPN</b>   | Virtual Private Network                          |