NIST SPECIAL PUBLICATION 1800-27

Securing Property Management Systems

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

William Newhouse Michael Ekstrom Jeff Finke Marisa Harriston

September 2020

DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems





NIST SPECIAL PUBLICATION 1800-27

Securing Property Management Systems

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

> William Newhouse Information Technology Laboratory National Institute of Standards and Technology

> > Michael Ekstrom Jeff Finke Marisa Harriston The MITRE Corporation McLean, Virginia

> > > DRAFT

September 2020



U.S. Department of Commerce Wilbur Ross, Secretary

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

NIST SPECIAL PUBLICATION 1800-27A

Securing Property Management Systems

Volume A: Executive Summary

William Newhouse Information Technology Laboratory National Institute of Standards and Technology

Michael Ekstrom Jeff Finke Marisa Harriston The MITRE Corporation McLean, Virginia

September 2020

DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems





Executive Summary

1 In recent years criminals and other attackers have compromised the networks of several major hotel

- 2 chains, exposing the information of hundreds of millions of guests. Breaches like these can result in huge
- 3 financial loss, operational disruption, and reputational harm, along with lengthy regulatory
- 4 investigations and litigation. Hospitality organizations can reduce the likelihood of a hotel data breach
- 5 by strengthening the cybersecurity of their property management system (PMS). The PMS is an
- 6 attractive target for attackers because it serves as the information technology (IT) operations and data
- 7 management hub of a hotel. This cybersecurity practice guide shows an approach to securing a PMS and
- 8 the ecosystem of guest services it supports. It offers how-to guidance for building an example solution 9 using commercially available products, standards, and best practices for role-based access control.
- 9 using commercially available products, standards, and best practices for role-based access control,
 10 privileged access management, network segmentation, moving target defense, and data protection.

11 CHALLENGE

- 12 Hospitality organizations rely on a PMS for
- 13 daily tasks, planning, and record keeping. As
- 14 the operations hub, the PMS interfaces with
- 15 several services and components within a
- 16 hotel's IT systems, such as point-of-sale (POS)
- 17 systems, physical access control systems,

An unsecured or poorly secured PMS could expose a hotel—and the larger hospitality organization of which the hotel is a part— to a significant and costly data breach...

- 18 Wi-Fi networks, and other guest service
- applications. A PMS, and the extended PMS ecosystem, stores, processes, and transmits a variety of
- 20 sensitive guest information, including payment card information (PCI) and personally identifiable
- 21 information (PII). An unsecured or poorly secured PMS could expose a hotel and the larger hospitality
- 22 organization of which the hotel is a part to a significant and costly data breach, including financial
- 23 penalties for violating state, federal, and international privacy and other regulatory regimes.
- 24

This practice guide can help your organization:

- instill consumer confidence and brand loyalty by protecting guest privacy and payment card information
- limit the cost for recovery and mitigation if a breach occurs
- build the business case, functional requirements, and test plan for a similar solution within your own environment
- support privacy/regulatory compliance by using data tokenization and limiting the spread of data beyond "need-to-know"
- increase overall PMS security situational awareness, and limit exposure of the PMS to incidents in systems that interface with it
- control and limit access to your PMS to those with a business need

SOLUTION 25

- 26 The National Cybersecurity Center of Excellence (NCCoE) collaborated with the hospitality business
- 27 community and cybersecurity technology providers to build an environment that simulates a hotel's IT
- 28 infrastructure, including guest WiFi and a PMS integrated with a POS module and an electronic door lock
- 29 system. Using commercially-available products, the example solution shows how to protect data moving
- 30 within this environment, and limit or prevent user access to the various systems and services.
- 31 The example solution uses technologies and security capabilities (shown below) from our project
- 32 collaborators. All technologies used in the solution support security standards and guidelines of the NIST
- 33 Cybersecurity Framework, Hotel Technology Next Generation, and the PCI Security Standards Council,
- 34 among others. Although following the guide does not ensure General Data Protection Regulation (GDPR)
- 35 compliance, the recommended solution aligns with the key principles of GDPR.

Collaborator	Security Capability or Component
CRYPTONITE NXT	Network protection appliance that provides an additional layer of protection against cyber attacks
<) FORESCOUT	Visualizes the diverse types of devices connected to the network; enforces policy-based controls
HÄFELE	Physical access control ecosystem including door locks, room key encoding, and management
Remediant	Real-time incident monitoring and detection, privilege escalation management and reporting functions
STRONGKEY	Payment solution appliance that secures credit card transactions and shrinks the PCI compliance enclave
tolicitechnologies	Access control platform that secures connections, and provides control mechanisms to enterprise systems for authorized users and devices; monitors activity down to the keystroke

36

- 37 While the NCCoE used a suite of commercial products to address this challenge, this guide does not
- endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your 38
- 39 organization's information security experts should identify the products that will best integrate with
- 40 your existing tools and IT system infrastructure. Your organization can adopt this solution or one that
- 41 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and
- 42 implementing parts of a solution.

43 HOW TO USE THIS GUIDE

- 44 Depending on your role in your organization, you might use this guide in different ways:
- 45 Business decision makers, including chief information security and technology officers can use this
- 46 part of the guide, *NIST SP 1800-27a: Executive Summary*, to understand the impetus for the guide, the
- 47 cybersecurity challenge we address, our approach to solving this challenge, and how the solution could
- 48 benefit your organization.
- 49 Technology, security, and privacy program managers who are concerned with how to identify,
- 50 understand, assess, and mitigate risk can use NIST SP 1800-27b: Approach, Architecture, and Security
- 51 *Characteristics,* which describes what we built and why, including the risk analysis performed, and the
- 52 security/privacy control mappings.
- 53 IT professionals who want to implement an approach like this can make use of NIST SP 1800-27c: How-
- 54 To Guides, which provides specific product installation, configuration, and integration instructions for
- 55 building the example implementation, allowing you to replicate all or parts of this project.

56 SHARE YOUR FEEDBACK

- 57 You can view or download the guide at <u>https://www.nccoe.nist.gov/projects/use-cases/securing-</u>
- 58 property-management-systems. Help the NCCoE make this guide better by sharing your thoughts with
- us. If you adopt this solution for your own organization, please share your experience and advice with
- 60 us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we
- 61 encourage organizations to share lessons learned and best practices for transforming the processes
- 62 associated with implementing this guide.
- To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at hospitality-nccoe@nist.gov.
- 65

66 **COLLABORATORS**

- 67 Collaborators participating in this project submitted their capabilities in response to an open call in the
- 68 Federal Register for all sources of relevant security capabilities from academia and industry (vendors
- and integrators). Those respondents with relevant capabilities or product components signed a
- 70 Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to
- 71 build this example solution.
- 72 Certain commercial entities, equipment, products, or materials may be identified by name or company
- 73 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an
- 74 experimental procedure or concept adequately. Such identification is not intended to imply special
- 75 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it
- 76 intended to imply that the entities, equipment, products, or materials are necessarily the best available
- 77 for the purpose.

NIST SPECIAL PUBLICATION 1800-27B

Securing Property Management Systems

Volume B: Approach, Architecture, and Security Characteristics

William Newhouse Information Technology Laboratory National Institute of Standards and Technology

Michael Ekstrom Jeff Finke Marisa Harriston The MITRE Corporation McLean, Virginia

September 2020

DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems





1 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- 2 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
- 4 academic institutions work together to address businesses' most pressing cybersecurity issues. This
- 5 public-private partnership enables creation of practical cybersecurity solutions for specific industries, as
- 6 well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research
- 7 and Development Agreements (CRADAs), including technology partners—from Fortune 50 market
- 8 leaders to smaller companies specializing in information technology security—the NCCoE applies
- 9 standards and best practices to develop modular, easily adaptable example cybersecurity solutions using
- 10 commercially available technology. The NCCoE documents these example solutions in the NIST Special
- Publication 1800 series of practice guides, which map capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was
- established in 2012 by NIST in partnership with the State of Maryland and Montgomery County,
- 14 Maryland.

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

17 NIST CYBERSECURITY PRACTICE GUIDES

- 18 NIST Cybersecurity Practice Guides target specific cybersecurity challenges in the public and private
- 19 sectors. They are practical, user-friendly guides that facilitate adoption of standards-based approaches
- 20 to cybersecurity. They show members of the information security community how to implement
- 21 example solutions that help them align more easily with relevant standards and best practices, and they
- 22 provide users with the materials lists, configuration files, and other information they need to implement
- a similar approach.
- 24 The documents in this series describe an example implementation of cybersecurity practices that
- 25 businesses and other organizations may voluntarily adopt. These documents do not describe regulations
- 26 or mandatory practices, nor do they carry statutory authority.

27 ABSTRACT

- 28 Hotels have become targets for malicious actors wishing to exfiltrate sensitive data, deliver malware, or
- 29 profit from undetected fraud. Property management systems (PMSes), which are central to hotel
- 30 operations, present attractive attack surfaces. This example implementation strives to increase the
- 31 cybersecurity of the PMS and offer privacy protections for the data in the PMS. The objective of this
- 32 guide was to build a standards-based example implementation that utilizes readily available commercial
- 33 off-the-shelf components that enhance the security of a PMS ecosystem.

- 34 The NCCoE at NIST built a PMS ecosystem in a laboratory environment to explore methods to improve
- 35 the cybersecurity of a PMS. The PMS ecosystem included the PMS, a credit card payment platform, and
- 36 an analogous ancillary hotel system. In this example implementation, a physical access control system
- 37 was used as the ancillary system.
- 38 The principal capabilities include protecting sensitive data, enforcing role-based access control, and
- 39 monitoring for anomalies. The principal recommendations include implementing cybersecurity concepts
- 40 such as zero trust, moving target defense, tokenization of credit card data, and role-based
- 41 authentication.
- 42 The PMS environment outlined in this guide encourages hoteliers and similar stakeholders to adopt
- 43 effective cybersecurity and privacy concepts by using standard components that are composed of open-
- 44 source and commercially available components.

45 **KEYWORDS**

- 46 access control, hospitality cybersecurity, moving target defense, PCI DSS, PMS, privacy, property
- 47 management system, role-based authentication, tokenization, zero trust architecture

48 **ACKNOWLEDGMENTS**

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

Name	Organization
Sapna George	Cryptonite
Hans Ismirnioglou	Cryptonite
Mike Simon	Cryptonite
Rich Walchuck	Cryptonite
Justin Yackoski	Cryptonite
Katherine Gronberg	Forescout
Timothy Jones	Forescout
Scott Morrison	Forescout

Name	Organization
Shane Stephens	Forescout
Oscar Castiblanco	Häfele
Ryan Douglas	Häfele
Chuck Greenspan	Häfele
Sarah Riedl	Häfele
Harald Ruprecht	Häfele
Roy Wilson	Häfele
John Bell	Hospitality Technology Next Generation
Kartikey Desai	MITRE
Eileen Division	MITRE
Karri Meldorf	MITRE
Paul Ward	MITRE
Trevon Williams	MITRE
Kevin Garrett	Remediant
Paul Lanzi	Remediant
Nicole Guernsey	StrongKey
Pushkar Marathe	StrongKey
Arshad Noor	StrongKey

Name	Organization
Bill Johnson	TDi
Pam Johnson	TDi

50

- 51 The technology partners/collaborators who participated in this project submitted their capabilities in
- 52 response to a notice in the Federal Register. Respondents with relevant capabilities or product
- 53 components were invited to sign a CRADA with NIST, allowing them to participate in a consortium to
- 54 build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Cryptonite	network protection appliance that provides additional layer of protection against cyber attacks
ForeScout	policy-based control enforcement for guest Wi-Fi net- works and visualizations of diverse types of network-con- nected devices
Häfele	Physical access control ecosystem, including door locks, room-key encoding, and management
Remediant	Real-time incident monitoring and detection, privilege es- calation management, and reporting functions
StrongKey	payment solution appliance that secures credit card transactions and shrinks the Payment Card Industry com- pliance enclave
TDi	access control platform that secures connections and pro- vides control mechanisms to enterprise systems for au- thorized users and authorized devices; also monitors ac- tivity down to the keystroke

56 **Contents**

57	1	Sun	nmary.		1
58		1.1	Challen	ge	1
59		1.2	Implem	nentation	1
60			1.2.1	PMS Ecosystem	2
61			1.2.2	Standards and Guidance	3
62		1.3	Benefit	S	3
63	2	Hov	v to Us	e This Guide	4
64		2.1	Typogra	aphical Conventions	5
65	3	Арр	roach	••••••	6
66		3.1	Audien	ce	6
67		3.2	Scope.		7
68		3.3	Assum	otions	7
69		3.4	Risk As	sessment	7
70			3.4.1	Threats	8
71			3.4.2	Vulnerabilities	8
72			3.4.3	Cybersecurity Control Map	9
73			3.4.4	Privacy Control Map	9
74	4	Arcl	hitectu	ıre	9
75		4.1	Archite	cture Description	9
76			4.1.1	High-Level Architecture	9
77		4.2	Use Cas	ses Supported by the Property Management System Ecosystem	. 10
78			4.2.1	Use Case 1: PMS Intakes Reservation	11
79			4.2.2	Use Case 2: Authorized User Access	11
80			4.2.3	Use Case 3: Secure Credit Card Transaction	11
81			4.2.4	Use Case 4: Secure Interaction of Ancillary Hotel System (with PMS)	11
82		4.3	Detaile	d Architecture	. 11
83		4.4	Techno	logies	. 14

84		4.5	Proces	ss Flows	
85			4.5.1	Authorized Employee Access	17
86			4.5.2	Secure Credit Card Transaction	18
87			4.5.3	Secure Interaction of Ancillary Hotel System (with PMS)	19
88			4.5.4	Guest Internet Access via Guest Wi-Fi	20
89	5	Sec	urity (Characteristic Analysis	21
90		5.1	Limita	tions	
91		5.2	Securi	ty of the Reference Design	
92	6	Priv	/acy C	haracteristic Analysis	25
93		6.1	Limita	tions	
94		6.2	Privac	y Protections of the Reference Design	
95	7	Fun	ctiona	al Evaluation	26
96		7.1	Test C	ases	
97			7.1.1	PMS Use Case Requirements	27
98			7.1.2	Test Case PMS-01 (Authorized User Can Log on)	29
99			7.1.3	Test Case PMS-02 (PMS Authentication)	29
100 101			7.1.4	Authorized Users Can Only Access Systems and Data They are Autho Cases	
102			7.1.5	Test Case PMS-04 (Guest Reservation Editable)	
103			7.1.6	Test Case PMS-05 (Room Key Provisioning)	
104			7.1.7	Provisioning Guest Wi-Fi Access	
105			7.1.8	Secure Credit Card Transaction	37
106			7.1.9	Test Case PMS-08 (Authorized Device Provisioning)	
107			7.1.10	Test Case PMS-09 (Prevent Unauthorized Device from Connecting)	40
108	8	Fut	ure Bu	uild Considerations	40
109	Ар	pen	dix A	Mapping to Cybersecurity Framework	
110	Ар	pen	dix B	Privacy Framework Mapping	53
111	Ар	pen	dix C	Deployment Recommendations	54

DRAFT

112	Appendix D	List of Acronyms	55
113	Appendix E	Glossary	56
114	Appendix F	References	58

115 List of Figures

116	Figure 4-1 Secure PMS High-Level Architecture	10
117	Figure 4-2 Secure PMS Reference Design (part 1 of 2)	12
118	Figure 4-3 Secure PMS Reference Design (part 2 of 2)	13
119	Figure 4-4 Staff Process Flow	18
120	Figure 4-5 Secure Credit Card Process Flow	19
121	Figure 4-6 Secure Interaction of Ancillary System with PMS Process Flow	20
122	Figure 4-7 Guest Internet Access via Guest Wi-Fi Process Flow	21
123	Figure 5-1 Tenets of Zero Trust	22

124 List of Tables

125	Table 4-1 Products and Technologies	14
126	Table 5-1 Zero Trust Tenets/Components/Cybersecurity Framework Subcategories	23
127	Table 7-1 Test Case Fields	26
128	Table 7-2 Functional Analysis Requirements	27
129	Table 7-3 Authorized User Can Log In	29
130	Table 7-4 PMS Authentication	29
131	Table 7-5 No Unauthorized Lateral Movement.	31
132	Table 7-6 Prevent Unauthorized Function	31
133	Table 7-7 Only Authorized Data	32
134	Table 7-8 Guest Reservation Editable	33
135	Table 7-9 Provisioning Room Key	34

136	Table 7-10 Guests' Limited Wi-Fi Access	. 35
137	Table 7-11 Prevent Unauthorized Guest Lateral Movement via Wi-Fi	. 36
138	Table 7-12 Tokenized Credit Card Data	. 37
139	Table 7-13 Verify that Credit Card Data Is Hidden	. 38
140	Table 7-14 Authorized Device Provisioning	. 39
141	Table 7-15 Prevent Unauthorized Device from Connecting	. 40
142	Table B-1 Securing Property Management Systems: NIST Privacy Framework Components Mapping	53
143		

144 **1** Summary

- 145 Hotel operators rely on a property management system (PMS) for daily administrative tasks such as
- reservations, availability and occupancy management, check-in/out, guest profiles, report generation,
- 147 planning, and record keeping. This PMS controls the onsite property activities and connects with other
- applications such as the hotel point-of-sale (POS) and central reservation system (CRS), which support
- availability, reservations, and guest profile information.
- Additionally, various interfaces are available to create further links from the PMS to internal and
- 151 external systems such as room-key systems, restaurant and banquet cash registers, minibars, telephone
- and call centers, revenue management, on-site spas, online travel agents, guest Wi-Fi, and connected
- 153 rooms.
- 154 The value of the data in a PMS and the number of connections to a PMS make it a likely target for bad
- actors. This guide documents a system that prevents unauthorized access to a PMS and applies both
- 156 security and privacy protections to the data used in the PMS.

157 1.1 Challenge

- 158 Volume A of this publication described why the National Cybersecurity Center of Excellence (NCCoE)
- accepted a hospitality cybersecurity challenge as a project. Here, in Volume B, the focus shifts to the
- 160 challenge of building an example implementation that offers hotel owners and operators some options
- 161 to secure their property management systems.
- 162 Securing Property Management Systems supports the following security and privacy characteristics:
- 163 prevents unauthorized access via role-based authentication
- 164 **•** protects from unauthorized lateral movement and privilege escalation attacks
- prevents theft of credit card and transaction data via data tokenization, explicitly allows only
 identified entities access (allowlisting), and enables access control enforcement
- 167 Increases situational awareness by auditing, system activity logging, and reporting
- 168 prevents unauthorized use of personal information
- 169 To build the example implementation, hereafter known as the PMS ecosystem, the project collaborators
- 170 reached consensus on an architecture that implements aspects of a zero trust architecture (ZTA),
- 171 moving target defense (MTD), and data tokenization to reduce cybersecurity risk for a hotel's PMS.

172 **1.2 Implementation**

- 173 The project demonstrates to hospitality organizations how to protect against loss and misuse of
- 174 customer data and how to provide more cybersecurity and privacy for guest Wi-Fi networks, employee
- 175 workstations, and electronic door locks.
- 176 Best practices for network and enterprise cybersecurity as put forth by the collaborators include role-
- 177 based access control, allowlisting, and privileged access management. Utilizing data tokenization,

- 178 explicitly allowing only identified entities access (allowlisting), and role-based access control
- 179 enforcement, theft of credit card and transaction data is prevented. Allowlisting is the practice of listing
- 180 entities that are granted access to a certain system or protocol. When an allowlist is used, all entities are
- 181 denied access, except those included in the allowlist.
- 182 The PMS ecosystem enables and enforces role-based access control to define exactly who or what will
- 183 be allowed to make connections within the PMS ecosystem. ZTA utilizing dynamic provisioning specifies
- 184 permitted connections and data transactions. Privileged access management defines, enforces, and
- 185 monitors the privileges for each user, machine, and data transaction.
- 186 The NCCoE PMS ecosystem, three types of authorized users: hotel guests, hotel staff, and back-end
- 187 administrators; engineers; and system owners. Each user has defined access privileges. Guests can
- 188 connect to the internet via the Wi-Fi. Staff are allowed authorized access for only the systems and
- applications needed to perform their work and are not allowed to make any connections outside the
- 190 scope of their role. Back-end administrators, engineers, and system owners are granted back-end
- access, but only for the systems and applications they provision, maintain, and troubleshoot.
- 192 Best practices for privacy protection include data minimization, transparency, and preference
- 193 management. The NIST Privacy Framework Core [1] is a set of privacy protection activities, desired
- 194 outcomes, and applicable references that are common across all sectors. The Core presents industry
- standards, guidelines, and practices in a manner that enables communicating privacy activities and
- 196 outcomes across the organization from the executive level to the implementation/operations level. The
- 197 Privacy Framework Core consists of five Functions—Identify-P, Govern-P, Control-P, Communicate-P,
- and Protect-P. When considered together, these Functions provide a high-level, strategic view of the life
- 199 cycle of an organization's management of privacy risk arising from data processing. The Framework Core
- 200 then identifies underlying key Categories and Subcategories–which are discrete outcomes–for each
- 201 Function and provides example informative references such as existing standards, guidelines, and
- 202 practices for each Subcategory.
- 203 This project demonstrates these best practices in a PMS ecosystem designed to simulate a typical hotel.

204 1.2.1 PMS Ecosystem

- Within the constructed PMS ecosystem, registered hotel guests can connect to the internet via the guest Wi-Fi. Registered guests attempting to connect to the internet will initially be challenged to provide a response, which is validated against information from their reservation. Once validated, the guest is able to connect to the internet and any public-facing hotel websites or guest service portals but is not able to discover other devices using the guest Wi-Fi, which may also be supporting hotel operations and Internet of Things (IoT) devices.
- 211 The PMS ecosystem represented in the example implementation constantly changes the internet
- 212 protocol (IP) addresses of devices, enabling a moving target defense tactic that is transparent to the
- staff. They can reach the systems that allow them to perform their work while the defense tactic hinders
- 214 lateral movement of attackers, who will be challenged to achieve and maintain persistent access.

- 215 In designing the hotel PMS ecosystem adapting some of the tenets of zero trust resulted in secure,
- authorized dynamic access to data or resources on a per-transaction, per-user, and per-system basis,
- 217 based on factors such as device health and hygiene and other cybersecurity considerations.
- 218 The PMS ecosystem includes a network protection device and an access control platform to support
- 219 privileged access management. Adding a wireless protection and visibility platform enables allowlisting,
- 220 network segmentation, and role-based authentication to the Wi-Fi. All access to resources is granted on
- a per-connection basis, based on a security policy.

222 1.2.2 Standards and Guidance

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

225 226			1	Hotel Technology Next Generation (HTNG): <i>Secure Payments Framework for Hospitality,</i> version 1.0, February 2013 [2]
227			•	HTNG: Payment Tokenization Specification, February 21, 2018 [3]
228			•	HTNG: Payment Systems & Data Security Specifications 2010B, October 22, 2010 [4]
229			•	HTNG: EMV for the US Hospitality Industry, October 1, 2015 [5]
230 231			1	PCI Security Standards Council: Understanding the Payment Card Industry Data Security Standard, version 3.2.1, May 2018 [6]
232			•	HTNG: GDPR for Hospitality, June 1, 2019 [7]
233 234			1	National Institute of Standards and Technology (NIST) Cybersecurity Framework, April 2018 [8]
235 236			1	NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, January 16, 2020 [1]
237 238			1	NIST Special Publication (SP) 800-53 Rev. 4, <i>Security and Privacy Controls for Federal Information Systems and Organizations,</i> April 2013 [9]
239			•	NIST SP 800-63-3, Digital Identity Guidelines, June 22, 2017 [10]
240 241			•	NIST SP 800-122, Guide to Protecting the Confidentiality of Personably Identifiable Information (PII), April 2010 [11]
242 243			•	NIST SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, August 2017 [12]
244			•	Trustwave Holdings: 2019 Trustwave Global Security Report, [13]
245	1 3	Rer	nefi	its

245 **1.3 Benefits**

246 The NCCoE's practice guide *Securing Property Management Systems* can help an organization:

247 248	1	reduce the risk of a network intrusion compromising the PMS and preserve core operations if a breach occurs
249	1.1	provide increased assurance for protecting guest information
250	1.1	ensure that only personnel with a business need are given access to the PMS
251 252	1	increase overall PMS security situational awareness and limit exposure of the PMS to incidents in systems that interface with it
253 254	1	avoid exploitations that decrease consumer confidence of the property owner, chain, or industry
255	1.1	increase consumer confidence in the protection of their sensitive data
256 257 258 259	impler here o	hospitality space, cost is a major driving factor for many enterprise decisions, so the example nentation documented in this guide is designed to be modular. The PMS ecosystem documented ffers opportunities for an organization to choose only those components of the implementation to enterprise.
260	2 ⊦	low to Use This Guide
261 262 263	users \	ST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides with the information they need to replicate a more secure PMS. This reference design is modular n be deployed in whole or in parts.
264	This gu	ide contains three volumes:
265		NIST SP 1800-27A: Executive Summary
266 267	1	NIST SP 1800-27B: Approach, Architecture, and Security Characteristics—what we built and why (this document)
268		NIST SP 1800-27C: How-To Guide –instructions for building the example implementation
269	Depen	ding on your role in your organization, you might use this guide in different ways:
270 271		ess decision makers, including chief security and technology officers, will be interested in the ive Summary (NIST SP 1800-27A), which describes the:
272	1.1	challenges that enterprises face in making a PMS more secure and protective of privacy
273	1.1	example implementation built at the NCCoE
274	1.1	benefits of adopting the example implementation
275 276 277	and m	ology or security program managers who are concerned with how to identify, understand, assess itigate risk will be interested in this part of the guide, NIST SP 1800-27B, which describes how the cosystem mitigates risk.
278	The fo	llowing sections may be of interest to users of risk management and privacy frameworks:

- Section <u>3.4</u>, Risk Assessment, describes the risk analysis performed.
- Section <u>3.4.3</u>, Cybersecurity Control Map, maps the security characteristics of this example
 implementation to cybersecurity standards and best practices.

Section <u>6.2</u>, Privacy Protections of the Reference Design, describes how we used the *NIST Privacy Framework* Subcategories.

Technical-savvy readers who wish to implement the security offered in this document might benefit by
 sharing not only this document but also the *Executive Summary*, NIST SP 1800-27A, with leadership to
 push for resources needed to secure the PMS and reduce risk.

Information technology (IT) professionals who want to implement an approach like this will find the
 whole practice guide useful and will find the how-to portion of the guide, NIST SP 1800-27C, to have all
 the details that would allow replicating all or parts of the PMS environment built for this project. The
 how-to guide provides specific product installation, configuration, and integration instructions for

- implementing the example implementation—in this case, a functioning PMS environment.
- 292 This guide assumes that IT professionals have experience implementing security products within the
- 293 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
- not endorse these products. An organization can adopt this example implementation or one that
- adheres to these guidelines in whole, or this guide can be used as a starting point for tailoring and
- 296 implementing parts of a more secure PMS. Your organization's security experts should identify the
- 297 products that will best integrate with your existing tools and IT system infrastructure. The NCCoE
- encourages organizations to seek products that are congruent with applicable standards and best
- 299 practices. Section 4.4, Technologies, lists the products in this project's PMS environment and maps them
- to the cybersecurity controls provided by this example implementation.
- 301 Acronyms used in figures are in the List of Acronyms appendix.

302 2.1 Typographic Conventions

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

Typeface/ Symbol	Meaning	Example	
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the NCCoE Style Guide.	
Bold	names of menus, options, com- mand buttons, and fields	Choose File > Edit.	
Monospace	command-line input, onscreen computer output, sample code examples, and status codes	mkdir	
Monospace Bold	command-line user input con- trasted with computer output	service sshd start	

Typeface/ Symbol	Meaning	Example	
<u>blue text</u>	link to other parts of the docu- ment, a web URL, or an email address	All publications from NIST's NCCoE are available at_ <u>https://nccoe.nist.gov.</u>	

304 **3 Approach**

- 305 This practice guide highlights the approach that the NCCoE used to develop the example
- implementation. The approach includes a risk assessment and analysis, logical design, example builddevelopment, testing, and security control mapping.
- 308 The NCCoE worked with hospitality organizations, such as the American Hotel & Lodging Association and
- 309 HTNG, to identify the need for an example implementation that improves the security of connections to
- and from the POS and PMS and other integrated services and components. These organizations, along
- 311 with the Retail and Hospitality Information Sharing and Analysis Center, offered opportunities for the
- 312 NCCoE to discuss this project and solicit input from stakeholders used to shape this effort.
- 313 In developing the example implementation, the NCCoE:
- met with hospitality entities and stakeholders such as hotel operators and managers to identify
 cybersecurity challenges with property management systems
- regularly interacted with members of the NCCoE Hospitality Community of Interest to discuss
 current cybersecurity trends and challenges
- received input from the collaborators participating in the project documented by this guide
 - The collaborators provided technologies to address the project's requirements and partnered in developing the PMS built for this project.
- implemented stronger security measures within and around the PMS through network
 segmentation, point-to-point encryption, data tokenization, and business-only usage restrictions
- 323 We considered including analytics and multifactor authentication, but ultimately we did 324 not include these security measures.

325 **3.1 Audience**

319

320

- This practice guide is intended for any hospitality stakeholder concerned about and/or responsible for
 securely implementing and operating a PMS. This includes system owners, IT engineers and technicians,
 hoteliers, and cybersecurity vendors.
- 329 The technical components of this guide will appeal to those who are directly involved with or oversee
- the PMS. Property management systems represent the heart of a hospitality organization's IT system.
- 331 The example implementation demonstrated by this project will help increase the level of security
- 332 around a PMS.

333 **3.2 Scope**

- This project is focused on increasing cybersecurity and privacy of a PMS environment. This includes
- protecting the data moving between ancillary systems such as a POS, physical access control systems,
- and hotel guest Wi-Fi as well as data at rest within components of the PMS environment.
- After an open call in the Federal Register inviting vendors to become collaborators, the project was
 scoped to create an on-premise (not cloud) PMS ecosystem that offers the following:
- protection against loss of customer data
- cybersecurity situational awareness within the PMS ecosystem
- cybersecurity for ancillary systems such as customer-facing Wi-Fi networks, employee
 workstations, and electronic door locks
- 343 We considered the following areas determined they are outside the scope of what we documented in 344 this project:
- 345 point-of-sale terminals
- validation of compliance with the Payment Card Industry (PCI) Data Security Standard (DSS)
- securing web servers and web applications
- mobile device security
- penetration testing and vulnerability assessments

350 3.3 Assumptions

- 351 This project is guided by the following assumptions:
- availability of skills-The organization has employees or contractors who can implement a
 security architecture around its property management system.
- uniqueness of lab environment—The example implementation was developed in a lab
 environment. It does not reflect the complexity of a production environment, and we did not
 use production deployment processes. Before production deployment, it should be confirmed
 that the example implementation capabilities meet the organization's architecture, reliability,
 and scalability requirements.

359 3.4 Risk Assessment

- 360 For this project, Risk Management Framework Quick Start Guides [14] proved to be invaluable in
- 361 providing a baseline to assess risks from which we developed the project and the security characteristics
- of the build. For a deeper dive into the application of a risk management framework, the NCCoE
- recommends following the guidance in NIST SP 800-37 Revision 2, *Risk Management Framework for*
- 364 *Information Systems and Organizations*—publicly available material [15].
- 365 NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* states that risk is "a measure of the
- 366 extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
- 367 (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of
- 368 occurrence" [16]. This guide defines risk assessment as "the process of identifying, estimating, and

- 369 prioritizing risks to organizational operations (including mission, functions, image, reputation),
- 370 organizational assets, individuals, other organizations, and the Nation, resulting from the operation of
- an information system. Part of risk management incorporates threat and vulnerability analyses, and
- 372 considers mitigations provided by security controls planned or in place."

373 3.4.1 Threats

- All organizations face external and internal threats. While not every threat can be eliminated, an
- architecture can be built to mitigate and/or reduce the potential realization of various threats. The PMS
- ecosystem mitigates threats related to unauthorized and elevated privileges, data exfiltration,
- 377 configuration modification, and access to sensitive data.

378 3.4.1.1 External Threats

- 379 One managed security service provider's annual global security report [13] shows that the hospitality
- 380 industry has the second highest number of incidents being investigated by the author's services. The
- 381 same report notes that motivation or types of data targeted by malicious actors for hospitality
- 382 organizations includes, in the author's words, "credit card track data, financial/user credentials,
- 383 proprietary information, and PII."
- Since 2014, a targeted technique labeled *DarkHotel hacking* [17] by security services leverages a hotel's
 Wi-Fi to selectively target and deliver malicious software to traveling executives. Further, identity theft
 and *doxing*—searching for and publishing private or identifying information about an individual on the
- 387 internet, typically with malicious intent—are persistent threats within the hospitality industry.

388 3.4.1.2 Internal Threats

- 389 Hotels also face internal threats, including misuse, inappropriate sharing or disclosure of personal
- information via employees with malicious intent, and accidental breaches. In fact, it is suggested that
- more than 50 percent of security incidents are initiated from current or former employees [18].
- 392 Mitigating internal threats involves more than just physical concepts, such as locking doors; rather, the
- 393 process needs to include cybersecurity concepts that help protect against insider threats and
- 394 unauthorized lateral movement within the enterprise by employees and guests.

395 3.4.2 Vulnerabilities

- A vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" [19]. Among this project's goals is to mitigate the ability of an actor to exploit vulnerabilities. Often, vulnerabilities are self-inflicted. For instance, organizations may:
- commit integration and configuration errors due to poor configuration management processes
- 401 delay and/or not perform patching/updating regularly
- 402 mis-deploy assets

403 Other vulnerabilities are inherent due to the very nature of valuable data. As data is the highest value
 404 asset, vulnerabilities to consider include:

- unauthorized modification and unauthorized exfiltration
- fraud, which is one of the largest concerns in the hospitality industry

407 3.4.3 Cybersecurity Control Map

408 Visit Appendix A to see the security control mappings that have been identified for this project's PMS

409 ecosystem. A Cybersecurity Framework Components Mapping table (<u>Table A-1</u>) shows the result from
 410 examining all the NIST Cybersecurity Framework [8] Core Subcategories and picking the Subcategories

411 supported as a desired outcome of the PMS environment. Each of the Cybersecurity Framework

412 Subcategories shown in the table maps to PCI DSS [6], to controls in NIST SP 800-53 rev 4 [9], and to

413 work roles in the NICE Cybersecurity Workforce Framework [12].

414 3.4.4 Privacy Control Map

- 415 Visit <u>Appendix B</u> to see privacy control mappings that we have identified for this project's PMS
- 416 ecosystem. A Privacy Framework Mapping table (Table B-1) shows the result from examining all the *NIST*
- 417 *Privacy Framework* [1] Core Subcategories and picking the Subcategories supported by components of
- the PMS ecosystem. This work was done after the collaboration team designed the PMS ecosystem
- 419 system. We include it to draw attention to NIST's Privacy Framework, a tool for improving privacy
- 420 through enterprise risk management, to enable better privacy engineering practices that support privacy
- 421 by design concepts and help organizations protect individuals' privacy.
- 422 We did not run a privacy risk assessment methodology during this project on any existing PMS as a first
- 423 step that would enable an organization to subsequently identify a target privacy profile. Table B-1 simply
- 424 identifies the Subcategories addressed by the PMS ecosystem and indicates what component is
- 425 responsible for covering the Subcategory's desired outcome.

426 4 Architecture

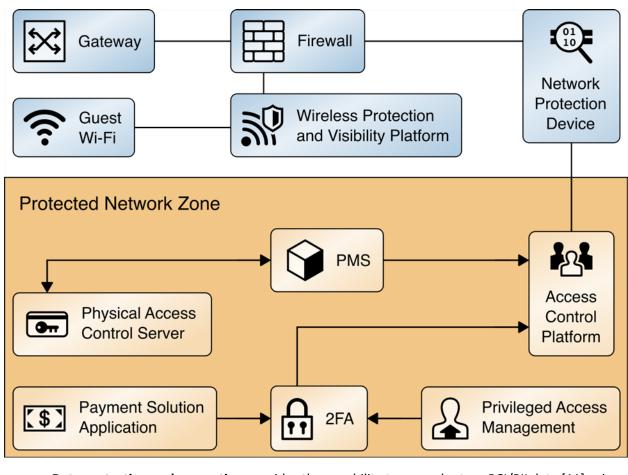
427 The PMS ecosystem built for this project demonstrates a typical hotel process for reservations, issuing

room keys, and check-in and checkout credit card transactions. This section presents a high-level
 architecture and reference design for enacting such an implementation.

430 4.1 Architecture Description

431 4.1.1 High-Level Architecture

The example implementation is designed to address the security Functions and Subcategories described in <u>Table 4-1</u> and is composed of the capabilities illustrated in the high-level architecture shown in Figure 434 4-1. 435 Figure 4-1 Secure PMS High-Level Architecture



436

- 437 Data protection and encryption provides the capability to securely store PCI/PII data [11] using
 438 additional data protection measures such as data encryption, limiting transmission of payment
 439 card data, secure data tokenization, and a secure data vault.
- System protection and authentication provides the capability to protect the functionality of the PMS, including the POS system and the reservation systems. This function also employs multifactor authentication, eliminates unauthorized access to data and services via dynamic authorization. This also includes making the access control enforcement, on a per connection basis, as granular as possible for internal and third-party users. Finally, it involves the use of network segmentation, and controlling change across multiple system dimensions to increase uncertainty and complexity for attackers, thereby reducing their window of opportunity [20].
- 447 Logging and analytics give continuous and near real-time auditing, logging, and reporting of
 448 user activity, network events, and component interactions.

449 4.2 Use Cases Supported by the Property Management System Ecosystem

450 We designed and built the PMS ecosystem to support the following hotel use cases.

451 4.2.1 Use Case 1: PMS Accepts Reservation

- 452 In Use Case 1, the PMS accepts a reservation, reconciles the bill, and closes out the reservation while
- 453 never exposing any data to unauthorized access. Further, the reservation data is editable in a secure
- 454 manner. In this PMS ecosystem, all reservations were manually entered directly into the PMS and not
- 455 supplied by an external CRS.

456 4.2.2 Use Case 2: Authorized User Access

- In Use Case 2, only authorized users can connect to their authorized devices. They are not able to gain
 access to devices that might enable them to escalate their privileges within the PMS ecosystem or
- 459 conduct any unauthorized lateral movements.
- 460 The access control platform in the PMS ecosystem allows users only to only connect to the systems for
- which they are authorized based on their role as a hotel guest; hotel staffer; or back-end administrator,
- 462 engineer, or system owner [9]. The action of inputting or modifying a reservation requires an authorized
- 463 staffer to authenticate to gain access to the PMS.

464 4.2.3 Use Case 3: Secure Credit Card Transaction

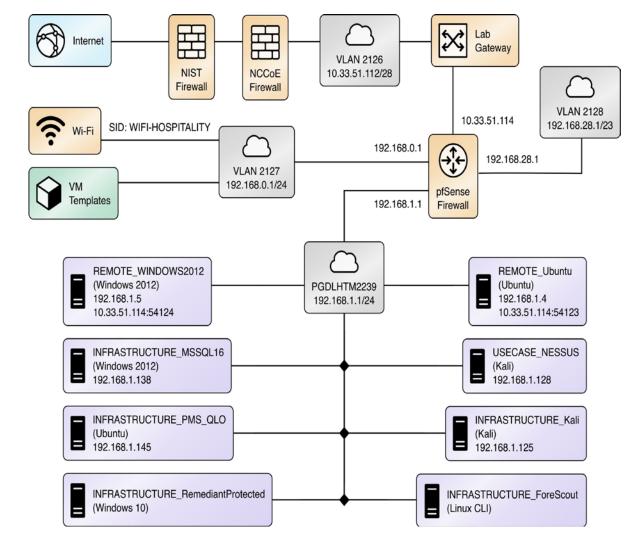
- In Use Case 3, a credit card transaction is securely conducted. The guest credit card transaction istokenized before introduction to the PMS.
- 467 Credit card data is consumed only by the payment solution application (PSA) and is immediately
- tokenized. The PSA function to validate the guest credit card data with a third-party payment processor
- is not included in the PMS ecosystem. The validated credit card data token is sent from the PSA to the
- 470 PMS. The token is used again at checkout when the bill is paid, with only the token sent from the PMS to
- 471 the PSA.

472 4.2.4 Use Case 4: Secure Interaction of Ancillary Hotel System (with PMS)

- 473 In Use Case 4, the PMS securely interacts with a physical access control system, specifically a door lock474 and room-key encoder.
- 475 The physical access control server is a door lock/room-key system that requires connectivity to the PMS.
- 476 To encode a room key at check-in, an authorized staffer accesses the PMS to identify the assigned guest
- 477 room number and provides only the room number to the physical access control server (PACS) to
- 478 encode a unique room key. In this process, the authorized staff authenticates to the PACS and simply
- inputs a room number. No guest PII is moved from the PMS to the PACS during key creation.

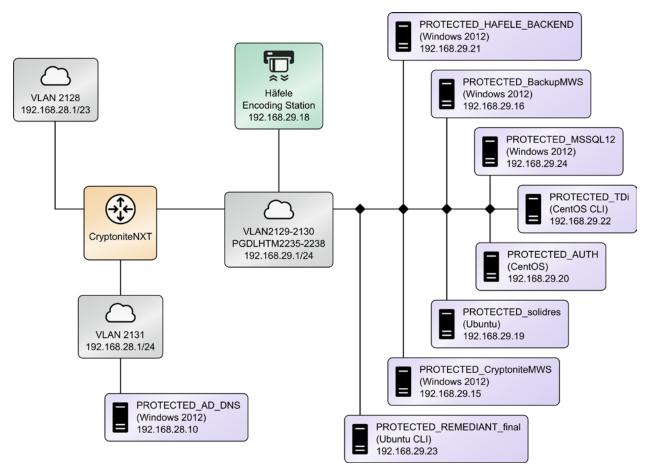
480 **4.3 Detailed Architecture**

- 481 All devices that operate within the PMS environment for this project are shown in Figure 4-2 and Figure
- 482 4-3. The design is separated into two figures for space considerations. The two figures are the two
- 483 halves of the overall design.



484 Figure 4-2 Secure PMS Reference Design (part 1 of 2)





486 The following summarizes the main function of each technology as displayed in Figure 4-2 and Figure 4-487 3.

488	•	The pfSense firewall provides exterior protection and segments the enterprise into the guest
489		portion and the nonguest portion.
490	٠	Forescout CounterACT protects the guest portion of the Wi-Fi by limiting guest access to only
491		the internet and preventing guest access to hotel back-end systems.
492	٠	The CryptoniteNXT device provides the secure zone for the enterprise, which includes tenets of
493		zero trust architecture (ZTA) and MTD.
494	•	TDi ConsoleWorks facilitates the user authentication security and functionality.
495	•	StrongKey SAKA (StrongAuth KeyAppliance) provides the token vault and tokenization along
496		with multifactor authentication.
497	•	Remediant SecureONE receives logs and monitors for incidents.
400		

• Häfele Dialock's physical access control system encodes and manages room keys.

499 4.4 Technologies

- 500 Table 4-1 lists the technologies used in this project and provides a mapping among the generic
- 501 application term, the specific product used, the Cybersecurity Framework Subcategories and the Privacy
- 502 Framework Subcategories that are affected by the product.
- 503 Table 4-1 Products and Technologies

Compo- nent	Product	Function	NIST Cybersecurity Frame- work Subcategories Affected	NIST Privacy Framework Subcategory Affected
PMS	Solidres Note: This is the only purchased component in this project.	heart of the hotel enter- prise; facili- tates the res- ervations pro- cess, checks customers in and out, tracks charges, and reconciles billing	N/A	N/A

Compo- nent	Product	Function	NIST Cybersecurity Frame- work Subcategories Affected	NIST Privacy Framework Subcategory Affected
network protection device	CryptoniteNXT Secure Zone 2.9.1	network pro- tection appli- ance that works in con- cert with fire- walls; pro- vides addi- tional layer of protection against cyber attacks	 ID.AM-1 Physical devices and systems within the organization are inventoried. ID.AM-2 Software platforms and applications within the organization are inventoried. PR.AC-4 Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. PR.AC-5 Network integrity is protected (e.g., network segregation, network segmentation). PR.DS-2 Data in transit is protected. PR.DS-5 Protections against data leaks are implemented. PR.IP-3 Configuration change control processes are in place. PR.PT-4 Communications and control networks are protected. 	ID.IM-P8 Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.

Compo-	Product	Function	NIST Cybersecurity Frame-	NIST Privacy Framework
nent			work Subcategories Affected	Subcategory Affected
access control platform	TDi Console- Works 5.2-0u1	secures con- nection and control mech- anism to en- terprise de- vices from au- thorized us- ers and au- thorized de- vices; also provides se- curity perim- eter monitor- ing, auditing, and logging activity down to the key- stroke	 PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. PR.AC-3 Remote access is managed. PR.AC-4 PR.AC-6 Identities are proofed and bound to credentials and asserted in interactions. PR.AC-7 Users, devices, and other assets are authenticated (e.g., single factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks). PR.PT-3 DE.CM-3 Personnel activity is 	CT.PO-P3 Policies, pro- cesses, and procedures for enabling individuals' data processing preferences and requests are estab- lished and in place.
			monitored to detect potential cybersecurity events.	
privileged access manage- ment	Remediant SecureONE 18.06.3-ce	provides real- time incident monitoring and detec- tion, privilege escalation management, and reporting functions for the IT enter- prise	 PR.AC-1 PR.AC-3 DE.AE-2 Detected events are analyzed to understand attack targets and methods. DE.CM-1 The network is monitored to detect potential cybersecurity events. DE.CM-7 Monitoring for unauthorized personnel, connections, devices, and software is performed. DE.DP-4 Event detection information is communicated. 	CT.DM-P8 Audit/log rec- ords are determined, doc- umented, implemented, and reviewed in accord- ance with policy and incor- porating the principle of data minimization.

Compo- nent	Product	Function	NIST Cybersecurity Frame- work Subcategories Affected	NIST Privacy Framework Subcategory Affected
wireless protection and visibil- ity plat- form	Forescout CounterACT 8.1	provides in- sight into the diverse types of devices connected to the network; enforces pol- icy-based controls to reduce the attack surface	ID.AM-1 ID.AM-2 PR.AC-3 PR.AC-5 DE.AE-2 DE.CM-1	 ID.IM-P4 Data actions of the systems/products/ser- vices are inventoried. CT.DM-P1 Data elements can be accessed for re- view.
payment solution appliance	StrongKey Key Appliance	secures credit card transac- tions and shrinks PCI compliance enclave	PR.AC-1 PR.DS-1 Data a rest is pro- tected.	ID.IM-P8
physical access control server	Häfele Dialock 2.0	physical ac- cess control ecosystem, including door locks, room-key en- coding, and management	N/A	N/A
firewall	pfSense	exterior bor- der protec- tion; demar- cation	N/A	N/A

504 4.5 Process Flows

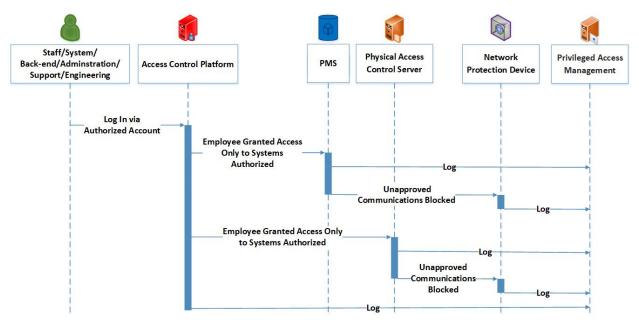
The following process flows show the sequence of events taking place for various hospitality functionsin the enterprise.

507 4.5.1 Authorized Employee Access

508 Figure 4-3 shows the process flow for an authorized employee connecting to only the systems for which

- they are authorized. The employee will be challenged by the access control platform and will be
- 510 required to present whatever credentials are required by policy; further, they will be granted only
- 511 minimal access based upon their role. The process of Figure 4-4 is described below.

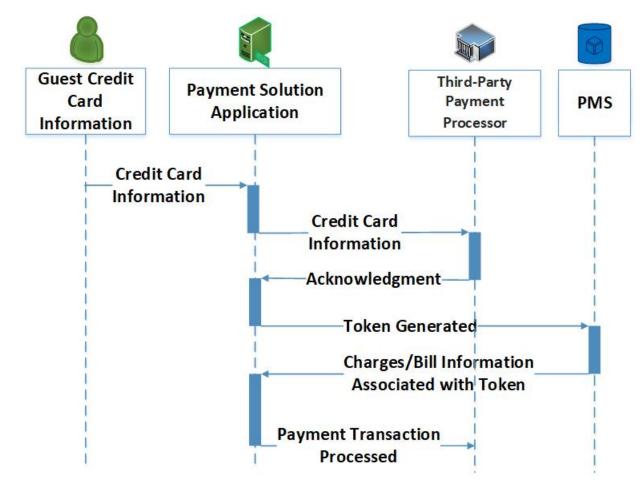
- 512 1. From a device or terminal, an authorized employee attempts to log in via the access control
- 513 platform. All login attempts are directed to the access control platform and logged.
- 514 2. The employee who presents valid authentication credentials is granted access to only the 515 system(s) they are allowed based upon their role.
- 5163. The network protection device monitors their activity and maintain logs via the privileged access517management system.
- 518 4. Any suspicious behavior is noted, logged, and responded to based on policy.
- 5. Logs are collected by the privileged access management solution.
- 520 Figure 4-4 Staff Process Flow



521 4.5.2 Secure Credit Card Transaction

- 522 Figure 4-5 shows the process flow for a credit card transaction [1]. The transaction is protected by the
- payment solution application via tokenization [2]. The token alone is ineffective as only the payment
 solution application can decrypt it and associate a credit card with charges. The process of Figure 4-5 is
- 525 described below.
- 526 1. The payment solution application collects the credit card information.
- 527 2. The payment solution application secures credit card information via a secure vault.
- 528 3. The payment solution application validates with a third-party payment processor.
- 529 4. The payment solution application issues a token.
- 5. Charges/bill are reconciled via the token from the PMS through the payment solution application back to the third-party payment processor when the guest checks out.

532 Figure 4-5 Secure Credit Card Process Flow



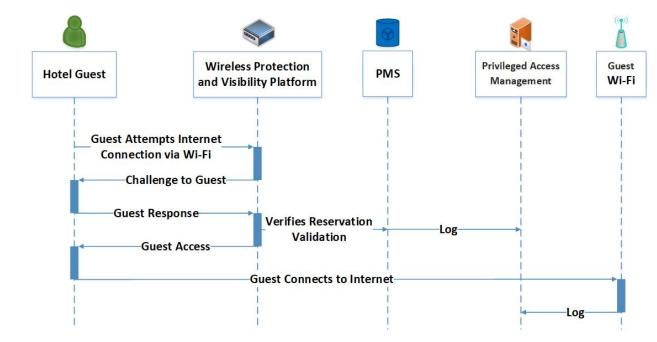
- 533 4.5.3 Secure Interaction of Ancillary Hotel System (with PMS)
- Figure 4-6 shows the process flow for the secure interaction of an ancillary system with the PMS. The
- 535 following demonstrates how a door lock/room-key system is used in this example implementation.
- 536 1. An authorized employee connects to the PMS.
- 537 2. The physical access server validates the room-key request against a reservation in the PMS.
- 538 3. The room key is created and delivered.
- 539 4. All activity is logged and sent to the privileged access management system.

- Hotel **Physical Access Privileged Access** PMS Employee **Control Server** Management **Encode Room Key Process** Check in Room Deliver Room Key Check-In Success Room Key Log **Creation Success**
- 540 Figure 4-6 Secure Interaction of Ancillary System with PMS Process Flow

541 4.5.4 Guest Internet Access via Guest Wi-Fi

542 Figure 4-7 shows the process flow for a guest accessing the internet via the hotel's guest Wi-Fi, showing 543 how the:

- 544 1. guest attempts to connect to the internet via the guest Wi-Fi
- 545 2. guest is challenged
- 5463. guest responds with temporary credentials they have been provided, corresponding to their547reservation
- 4. wireless protection and visibility platform validates with the PMS, and the guest is providedinternet access
- 5. guest is provided only access to the internet (is forbidden to move laterally) and any external-
- 551 facing enterprise hospitality systems; all activity, including surfing and web activity, is logged 552 and sent to the privileged access management system



553 Figure 4-7 Guest Internet Access via Guest Wi-Fi Process Flow

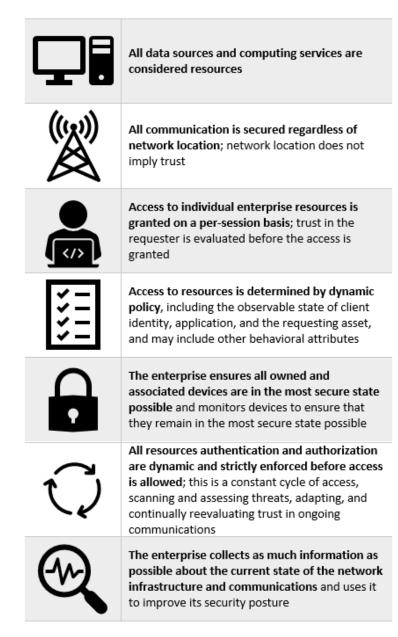
554 **5 Security Characteristic Analysis**

555 The purpose of the security characteristic evaluation is to understand the extent to which the project 556 meets its objective of demonstrating improved cybersecurity of a PMS.

557 5.1 Limitations

- 558 The security characteristic evaluation has the following limitations:
- It is not a comprehensive test of individual security components, nor is it a red team exercise.
 This project did not include a comprehensive test of all security components or "red team"
 penetration testing or adversarial emulation. Cybersecurity is a rapidly evolving field where new
 threats and vulnerabilities are continually discovered. Therefore, this security guidance cannot
 be guaranteed to identify every potential weakness of the build architecture. It is assumed that
 implementers will follow risk management procedures as outlined in the NIST Risk Management
 Framework.
- 566 O Security of the Reference Design
- 567 The NIST Cybersecurity Framework Subcategories are a basis for organizing our analysis and allowed us 568 to systematically consider how well the reference design supports the intended security characteristics.
- 569 This project is also designed to show a PMS ecosystem that adheres to some of the tenets of zero trust 570 architecture.

571 Figure 5-1 Tenets of Zero Trust



- 572 Table 5-1 shows zero trust tenets associated with components in the PMS ecosystem and Cybersecurity
- 573 Framework Subcategories.

574 Table 5-1 Zero Trust Tenets/Components/Cybersecurity Framework Subcategories

Zero Trust Tenet	PMS Ecosys- tem Compo- nent	Cybersecurity Framework Subcat- egories
All data sources and computing services are considered resources.	CryptoniteNXT Secure Zone 2.9.1	 ID.AM-1 Physical devices and systems within the organization are inventoried. ID.AM-2 Software platforms and applications within the organization are inventoried.
All communication is secured regardless of network location; network location does not imply trust.	CryptoniteNXT Secure Zone 2.9.1 StrongKey's vault	 PR.AC-5 Network integrity is protected. PR.DS-1 Data at-rest is protected PR.DS-2 Data in transit is protected. PR.PT-4 Communications and control networks are protected.
Access to individual enterprise resources is granted on a per-session basis; trust in the requester is evaluated before the access is granted.	TDi ConsoleWorks 5.2-0u1	 PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. PR.PT-3 The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.

Zero Trust Tenet	PMS Ecosys-	Cybersecurity Framework Subcat-
	tem Compo-	egories
Access to recourses is determined by	nent	DP AC 4 Access permissions and
Access to resources is determined by dynamic policy, including the observable state of client identity, application, and the requesting asset, and may include other behavioral attributes.	TDi ConsoleWorks 5.2-0u1	 PR.AC-4 Access permissions and authentications are managed, incorporating the principles of least privilege and separation of duties. PR.AC-6 Identities are proofed and bound to credentials and asserted in interactions. DE.CM-3 Personnel activity is monitored to detect potential cybersecurity events.
The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors devices to ensure that they remain in the most secure state possible.		PR.IP-1 A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).
All resources' authentication and	Remediant	PR.AC-1 Identities and credentials
authorization are dynamic and strictly	SecureONE	are issued, managed, verified,
enforced before access is allowed; this is a	18.06.3-ce	revoked, and audited for
constant cycle of access, scanning and		

Zero Trust Tenet	PMS Ecosys- tem Compo- nent	Cybersecurity Framework Subcat- egories
assessing threats, adapting, and continually reevaluating trust in ongoing communications.	CryptoniteNXT Secure Zone 2.9.1 Forescout CounterACT 8.1	 authorized devices, users and processes. PR.AC-3 Remote access is managed. PR.AC-4 Access permissions and authentications are managed, incorporating the principles of least privilege and separation of duties. PR.DS-5 Protections against data leaks are implemented. PR.IP-3 Configuration change control processes are in place. DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.
The enterprise collects as much information as possible about the current state of the network infrastructure and communications and uses it to improve its security posture.	Remediant SecureONE 18.06.3-ce	 DE.AE-2 Detected events are analyzed to understand attack targets and methods. DE.CM-1 The network is monitored to detect potential cybersecurity events. DE.DP-4 Event detection information is communicated.

575 6 Privacy Characteristic Analysis

576 The purpose of a privacy characteristic evaluation is to understand the extent to which a project meets 577 its objective of demonstrating improved privacy protection for a PMS.

578 6.1 Limitations

579 For this project, the privacy characteristic evaluation has the following limitations:

- It is not a comprehensive test of individual privacy components, nor does it include a privacy risk
 assessment methodology in that the design is clean slate.
- 582 It cannot identify all weaknesses.

583 6.2 Privacy Protections of the Reference Design

584 The *NIST Privacy Framework* Core Subcategories are a basis to identify privacy characteristics that are 585 supported by our PMS ecosystem. The PMS ecosystem architecture was designed before the *NIST*

586 *Privacy Framework* [1] was developed. This section is included to draw attention to the Privacy

587 Framework and to highlight that protecting an individual's privacy could become a core value for PMS

- 588 ecosystems through more thorough use of the Privacy Framework.
- See the Privacy Framework Mapping, <u>Table B-1</u>, in Appendix B for the technical privacy characteristics
 identified as being satisfied by this PMS ecosystem.

591 **7 Functional Evaluation**

592 **7.1 Test Cases**

- 593 This section includes the test cases necessary to conduct the functional evaluation of the PMS example 594 implementation. Refer to <u>Section 4</u> for descriptions of the tested example implementation.
- 595 Each test case consists of multiple fields that collectively identify the goal of the test, the specifics re-
- quired to implement the test, and how to assess the results of the test. Table 7-1 describes each field in
- the test case.
 - **Test Case Field** Description identifies the requirement to be tested and guides the definition requirement tested of the remainder of the test case fields. specifies the capability to be evaluated description describes the objective of the test case associated Cybersecurity Framelists the Cybersecurity Framework Subcategories addressed by work Subcategories the test case sub test cases In some cases, one or more tests may be part of a larger usecase or functionality. preconditions identifies the starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content.
- 598 Table 7-1 Test Case Fields

procedure	lists the step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate varia- tions in the test procedure.
expected results	lists the expected results for each variation in the test procedure
actual results	records the observed results
disposition	indicates if the test was passed or failed

599 7.1.1 PMS Use Case Requirements

- Table 7-2 identifies the PMS functional analysis requirements that are addressed in the associated re-
- 601 quirements and test cases and mapped to the build components.

602 Table 7-2 Functional Analysis Requirements

Capability Requirement (CR) ID	Parent Requirement	subrequirement	Test Case	Component
CR 1	guest reservation		PMS-04	property management system
CR 1.a		room key provisioned	PMS-05	physical access control server
CR 2	authorized user can log in		PMS-01	access control platform
CR 2.a		cannot move laterally unless authorized to do so	PMS-03a, PMS-03b	access control platform
CR 2.b		have access only to data they are author- ized to access	PMS- 03b, PMS-03c	network protection device
CR 2.c		users with par- tial/compromised cre- dentials are blocked	PMS-02	access control platform
CR 3	secure credit card transaction		PMS-07a	payment solution appliance
CR 3.a		Credit card data was tokenized.	PMS-07a	payment solution appliance

DRAFT

Capability Requirement (CR) ID	Parent Requirement	subrequirement	Test Case	Component
CR 3.b		Eavesdropper cannot see credit card data.	PMS-07b	payment solution appliance
CR 4	Wi-Fi guest connectivity/login		PMS-06a	wireless protection and visibility platform
CR 4.a		Guest cannot access enterprise systems.	PMS-06b	wireless protection and visibility platform
CR 5	Authorized device can connect/ unauthorized device cannot connect.		PMS-08, PMS-09	privileged access management

603 7.1.2 Test Case PMS-01 (Authorized User Can Log In)

Table 7-3 contains test case requirements, an associated test case, and descriptions of the test scenario

- for an authorized user logging in to the system(s) for which they are authorized.
- 606 Table 7-3 Authorized User Can Log In

Test Case Field	Description
requirement tested	(CR 2) system login capability for authorized users
description	Verify that a new authorized user is provided credentials and can log in to enterprise systems for which they are authorized.
associated Cybersecurity Frame- work Subcategories	PR.AC-1, PR.AC-4, PR.PT-3
sub test cases	N/A
preconditions	PMS and room-key systems up and running
procedure	Log in to end user workstation/front desk, open TDi in browser, authenticate, open connection to host in console.
expected results	User can log in to the PMS with their issued credentials.
actual results	User can log in to PMS through TDi console. (Other tested ma- chines include front desktop, management workstation.)
disposition	pass

607 7.1.3 Test Case PMS-02 (PMS Authentication)

Table 7-4 contains test case requirements, associated test case, and descriptions of the test scenario for

- validating the PMS authentication mechanism and validating that the mechanism protects against
- 610 compromised accounts/credentials.
- 611 Table 7-4 PMS Authentication

	Test Case Field	Description
--	-----------------	-------------

requirement tested	(CR 2.c) users blocked with partial/compromised credentials
description	Validate that authentication to the PMS works as planned, e.g., multifactor authentication, biometric.
associated Cybersecurity Frame- work Subcategories	DE.AE-2, DE.CM-1, DE.CM-7
sub test cases	If a "user" has only a partial credential or a compromised creden- tial, they cannot access the PMS.
preconditions	PMS configured and running properly
procedure	Log in to end user workstation/front desk, open TDi in browser, authenticate, open connection to Solidres's admin console. Trig- ger password policy by trying to log in Solidres's admin side 10 times.
expected results	Solidres admin console can be accessed successfully. Locked ac- count cannot be accessed.
actual results	Solidres admin console can be accessed successfully. (Multifactor is enabled and can be used if the user provisions a tokenization device.) Enabled brute force plug-in in PMS that blocks IP for one day when attempting to log in past 10 attempts. The account was locked and could not be accessed after locking.
disposition	pass

7.1.4 Authorized Users Can Access Only Systems and Data They Are Authorized for Test Cases

614 The following three test cases validate users being granted access only to that for which they are 615 authorized.

616 7.1.4.1 Test Case PMS-03a (Users Cannot Move Laterally from the PMS Unless 617 Authorized to Do So)

Table 7-5 contains test case requirements, associated test case, and descriptions of the test scenario forpreventing lateral movement.

620 Table 7-5 No Unauthorized Lateral Movement

Test Case Field	Description
requirement tested	(CR 2.a) cannot move laterally unless authorized to do so
description	Verify that an authorized user cannot go outside their boundary.
associated Cybersecurity Frame- work Subcategories	PR.AC-5, PR.PT-3, DE.CM-3
sub test cases	If they are authorized to access only the PMS, they cannot move laterally to another enterprise system from the PMS.
preconditions	PMS configured and running properly
procedure	attempted to connect to another system with an account that was authorized only for the PMS
expected results	access denied
actual results	access denied
disposition	pass

621 7.1.4.2 Test Case PMS-03b (Prevent Unauthorized Function)

- Table 7-6 contains test case requirements, associated test case, and descriptions of the test scenario for
- 623 preventing a user from performing a function for which they are not authorized.
- 624 Table 7-6 Prevent Unauthorized Function

Test Case Field	Description
requirement tested	(CR 2.a, CR 2.b) cannot move laterally unless authorized to do so; have access only to data for which they are authorized

description	Verify that an authorized user cannot go outside their "bound- ary."
associated Cybersecurity Frame- work Subcategories	PR.PT-3, DE.CM-3
sub test cases	The user cannot perform a function for which they are not au- thorized, e.g., create a master room key.
preconditions	PMS configured and running properly; Häfele back-end server configured and running properly
procedure	Front desk user created with no write or delete access. Verify the access controls of the Häfele back-end server.
expected results	Häfele permissions do not allow user to create a master room key for all of the created rooms in the back-end server.
actual results	Master key could not be created when the lowest level of privi- lege was given. The user was not able to add an authorization to create or save MIFARE credentials.
disposition	pass

625 7.1.4.3 Test Case PMS-03c (Only Authorized Data)

Table 7-7 contains test case requirements, associated test case, and descriptions of the test scenario for

- 627 ensuring that users have access only to data for which they are authorized.
- 628 Table 7-7 Only Authorized Data

Test Case Field	Description
requirement tested	(CR 2.b) have access only to data for which they are authorized
description	Verify that an authorized user cannot go outside their boundary.
associated Cybersecurity Frame- work Subcategories	PR.AC-5, PR.DS-2, PR.DS-5, PR.PT-3, DE.CM-3

Test Case Field	Description
sub test cases	Verify that the user has access to only the data set(s) for which they are authorized; further, that they can only edit data, down- load data they are authorized to download, and edit data that they are authorized to edit.
preconditions	PMS configured and running properly
procedure	created a user account that was giving the permission of a "site sponsor." This user account could see only site-specific infor- mation, not including guest reservations. After logging in to the account, it was verified that the specified permissions were valid and that the account could not navigate to sensitive data.
expected results	Solidres Access Control List (ACL) controls are functioning, and registered guests or sponsors should not be able to access or view sensitive customer data.
actual results	ACL manages view of permissions of the logged-in users. Users could only view data they were authorized to view within the Solidres PMS.
disposition	pass

629 7.1.5 Test Case PMS-04 (Guest Reservation Editable)

Table 7-8 contains test case requirements, associated test case, and descriptions of the test scenario for

- 631 entering a reservation and editing the reservation.
- 632 Table 7-8 Guest Reservation Editable

Test Case Field	Description
requirement tested	(CR 1) creating a guest reservation and having the ability of only an authorized user to edit the reservation
description	Enter a guest reservation into the PMS. Verify that it is in the PMS and that it is retrievable and editable.

Test Case Field	Description
associated Cybersecurity Frame- work Subcategories	N/A
sub test cases	N/A
preconditions	PMS up and running properly
procedure	Navigate to Solidres guest registration from guest machine, and book a room.
expected results	reservation record in the PMS
actual results	The test registration is bookable/retrievable from web interface of Solidres.
disposition	pass

633 7.1.6 Test Case PMS-05 (Room-Key Provisioning)

Table 7-9 contains test case requirements, associated test case, and descriptions of the test scenario forentering a reservation and editing the reservation.

636 Table 7-9 Provisioning Room Key

Test Case Field	Description
requirement tested	(CR 1) room key provisioned
•	From the reservation in the PMS, verify that a room key is provi- sioned for the guest.
associated Cybersecurity Framework Subcategories	N/A
sub test cases	Verify the processing of provisioning, writing, reading.
preconditions	Rooms are defined in Häfele, and PMS is running.

Test Case Field	Description
	Provision a key through the PMS in conjunction with Häfele's back- end server. The provision process includes assigning a key in the PMS, writing a key card with the Häfele back-end server, and mak- ing sure that the assigned key-card room number and guest-regis- tered room number are the same.
expected results	Provisioned room key works.
actual results	Room keys were provisioned.
disposition	pass

637 7.1.7 Provisioning Guest Wi-Fi Access

- 638 The following two test cases will validate provisioning guest Wi-Fi access and that guests cannot access
- 639 the restricted enterprise from the Wi-Fi.
- 640 7.1.7.1 Test Case PMS-06a (Guests' Limited Wi-Fi Access)
- Table 7-10 contains test case requirements, associated test case, and descriptions of the test scenario
- 642 for preventing lateral movement.
- 643 Table 7-10 Guests' Limited Wi-Fi Access

Test Case Field	Description
requirement tested	(CR 4) Wi-Fi guest connectivity/login
description	Only registered guests will be granted limited Wi-Fi access.
associated Cybersecurity Frame- work Subcategories	PR.AC-3, PR.IP-3, PR.PT-3, PR.PT-4, DE.CM-3
sub test cases	Verify that the guest can access only authorized resources via the Wi-Fi, e.g., the internet and guest-facing resources such as activities reservations and room charges.
preconditions	PMS up and running properly; guest Wi-Fi up, running, and con- nected; guest has provisioned Wi-Fi login

Test Case Field	Description
procedure	Attempt to connect a device to the guest Wi-Fi. When the login screen appears, enter the password created for the guest as part of the reservation process to complete the login. Open a browser, and verify internet sites are accessible.
expected results	Guest successfully logs in to Wi-Fi with issued login.
actual results	entered the Wi-Fi key and gained access to the internet
disposition	pass

644 7.1.7.2 Test Case PMS-06b (Prevent Unauthorized Guest Lateral Movement via Wi-Fi)

Table 7-11 contains test case requirements, associated test case, and descriptions of the test scenario

- 646 for preventing a guest from accessing any restricted back-end systems.
- 647 Table 7-11 Prevent Unauthorized Guest Lateral Movement via Wi-Fi

Test Case Field	Description
requirement tested	(CR 4.a) Guest cannot access enterprise systems.
description	Only registered guests are granted limited Wi-Fi access.
associated Cybersecurity Frame- work Subcategories	PR.AC-3, PR.PT-4, DE.CM-3
sub test cases	Verify that the guest via the Wi-Fi cannot jump to any enterprise systems (e.g., PMS).
preconditions	PMS up and running properly; guest Wi-Fi up, running, and con- nected; guest has provisioned Wi-Fi login

Test Case Field	Description
procedure	Once the guest Wi-Fi is operating and internet access has been established, attempt to ping the IP addresses of the protected hotel systems.
expected results	Guest cannot access unauthorized resources when logged in to the guest Wi-Fi.
actual results	Guest Wi-Fi range is blocked via NGINX ACL implementation, which works with CounterACT protections.
disposition	pass

648 7.1.8 Secure Credit Card Transaction

- 649 The following two test cases validate secure credit card transactions.
- 650 7.1.8.1 Test Case PMS-07a (Tokenized Credit Card Data)
- Table 7-12 contains test case requirements, associated test case, and descriptions of the test scenario
- 652 for tokenizing credit card data for a credit card transaction.
- 653 Table 7-12 Tokenized Credit Card Data

Test Case Field	Description
requirement tested	(CR 3.a) Credit card data was tokenized.
description	Conduct a credit card transaction, and verify that the credit card data was tokenized and that the transaction went through.
associated Cybersecurity Frame- work Subcategories	N/A
sub test cases	Validate that credit card data was tokenized; validate that addi- tional charges can be recorded using the token; validate that the token can be reconciled for payment; validate that the token en- crypts and/or otherwise obfuscates credit card data; validate that a "captured" or copied or exfiltrated token is worthless.

Test Case Field	Description
preconditions	PMS is up and running properly.
procedure	Log on to end user workstation/front desk, open TDi in browser, authenticate, open connection to Solidres PMS, navigate to res- ervations, click the test reservation, validate credit card infor- mation was tokenized. Open terminal in TDi Virtual Network Computing (VNC) session, authenticate to MySQL Server, view table entries for reservation, validate credit card information was tokenized (database, PMS, over the wire).
expected results	valid credit card transaction. The credit card information can be seen when accessing the guest reservation in the PMS.
actual results	Tokenized credit card information is stored in Solidres and is reading for processing through the offline plug-in. PII for credit card charges is tokenized. Data in database is stored as a token. (The stripe plug-in required a credit card for charges, and the of- fline plug-in simulates the "on-site payment" solution that charges the cards after the fact or forwards them to a third party securely.)
disposition	pass

654 *7.1.8.2* Test Case PMS-07b (Verify that Credit Card Data Is Hidden)

- Table 7-13 contains test case requirements, associated test case, and descriptions of the test scenario
- 656 for verifying that credit card data is hidden.
- 657 Table 7-13 Verify that Credit Card Data Is Hidden

Test Case Field	Description
requirement tested	(CR 3.b) Eavesdropper cannot see credit card data.
description	Conduct a credit card transaction, and verify that the credit card data was tokenized and that the transaction went through.

Test Case Field	Description
associated Cybersecurity Frame- work Subcategories	PR.AC-5, PR.DS-2, PR.DS-5
sub test cases	Verify that an eavesdropper cannot see any credit card data.
preconditions	PMS is up and running properly.
procedure	Verify that a credit card transaction cannot be determined from captured Wireshark traffic.
expected results	No credit card data is visible to an eavesdropper.
actual results	Wireshark shows Transport Layer Security encrypted traffic where payment information is tokenized, and user is submitting reservation through guest system. Wireshark was run on the host machine that also housed the PMS server.
disposition	pass

658 7.1.9 Test Case PMS-08 (Authorized Device Provisioning)

Table 7-14 contains test case requirements, associated test case, and descriptions of the test scenario for allowing an authorized device to connect to the enterprise.

661 Table 7-14 Authorized Device Provisioning

Test Case Field	Description		
	(CR 5) Authorized device can connect/unauthorized device cannot connect.		
•	Verify that an authorized device can be provisioned and added/connected to the enterprise.		
associated Cybersecurity Framework Subcategories	ID.AM-1, ID.AM-2, PR.AC-1, PR.IP-3		
sub test cases	N/A		
•	Various technology is up and running; security mechanisms are in place.		

Test Case Field	Description
procedure	Connect an authorized device with valid credentials.
expected results	Device will connect to the enterprise.
actual results	Authorized device could connect.
disposition	pass

662 7.1.10 Test Case PMS-09 (Prevent Unauthorized Device from Connecting)

- Table 7-15 contains test case requirements, associated test case, and descriptions of the test scenario
- 664 for preventing an authorized device form connecting to the enterprise.
- 665 Table 7-15 Prevent Unauthorized Device from Connecting

Test Case Field	Description
	(CR 5) Authorized device can connect/unauthorized device cannot connect.
	Verify that an unknown/unauthorized system that appears on the enterprise cannot access the PMS or establish a connection to any enterprise system.
associated Cybersecurity Framework Subcategories	PR.AC-5, PR.IP-3, DE.CM-1, DE.CM-7
sub test cases	N/A
preconditions	Cryptonite rules are configured to block unverified accounts.
	Add a machine to the secure enclave Virtual Local Area Network (VLAN) (simulates connecting to the network). From the con- nected machine, try to navigate to the PMS.
expected results	Unverified machine is unable to navigate to PMS.
actual results	Device was not allowed to connect.
disposition	pass

666 8 Future Build Considerations

- 667 We have considered several areas for future or follow-on hospitality projects. These include expanding
- the physical access control with a connection to mobile devices (mobile device security per NIST SP
- 669 1800-4, *Mobile Device Security: Cloud and Hybrid Builds*), smart rooms, and IoT. Subsequent work may

670 be an amalgamation of these themes grouped into the smart room concept, a focal point in many of

these topics. Another possible direction for the follow-on work could be a hotel-centric IoT project.

672 Appendix A Mapping to Cybersecurity Framework

673 Table A-1 shows the National Institute of Standards and Technology (NIST) Cybersecurity Framework 674 Subcategories that are addressed by the property management system (PMS) ecosystem built in this 675 practice guide. The first three categories show the Cybersecurity Framework details. The next three 676 categories show how the Cybersecurity Framework Subcategories are related to requirements in 677 Payment Card Industry Data Security Standard (PCI DSS) v3.2.1; security and privacy controls in NIST 678 Special Publication (SP) 800-53r4; and work roles in NIST SP 800-181, National Initiative for 679 Cybersecurity Education (NICE) Cybersecurity Workforce Framework [12]. This table is included to help 680 connect those with expertise in any of these areas and illuminate areas that the PMS ecosystem. 681 Examining the work roles in the NICE Framework may help an organization understand if it has people who can perform tasks and apply the skills described for each work role on its teams. Noting a discrete 682 683 PCI requirement or NIST SP 800-53 control [9] may match areas of focus within an organization that

684 securing a PMS ecosystem could help address.

Table A-1 Securing Property Management Systems: NIST Cybersecurity Framework Components
 Mapping

NIST Cybersecurity Framework v1.1		Standards and Best Practices			
Func- tion	Category	Subcategory	PCI DSS v3.2.1	NIST SP 800-53r4 Security and Privacy Controls [9]	NIST SP 800-181, NICE Framework Work Roles (Work Role ID) [12]
IDENTI	Asset Man- agement (ID.AM): The data, per- sonnel, de- vices, sys- tems, and facilities that	ID.AM-1: Physical devices and systems within the or- ganization are inventoried.		CM-8, PM- 5	Technical Support Specialist (OM-STS-001)
IDENTIFY (ID)	facilities that enable the organization to achieve business purposes are identified and man-	ID.AM-2: Soft- ware plat- forms and ap- plications within the or- ganization are inventoried.		CM-8, PM- 5	Technical Support Specialist (OM-STS-001)

	aged con- sistent with their relative importance to organiza- tional objec- tives and the organiza- tion's risk strategy.				
PROTECT (PR)	Identity Manage- ment, Au- thentication, and Access Control (PR.AC): Ac- cess to phys- ical and logi- cal assets and associ- ated facili- ties is lim- ited to au- thorized us- ers, pro- cesses, and devices, and is managed consistent with the as- sessed risk of unauthor- ized access to author- ized activi- ties and transactions.	PR.AC-1: Iden- tities and cre- dentials are is- sued, man- aged, verified, revoked, and audited for au- thorized de- vices, users, and processes.	 2.1 Always change vendor-supplied defaults and re- move or disable unnecessary de- fault accounts be- fore installing a system on the net- work. 3.6.1 Generate strong keys. 3.6.2 Keys are only distributed to au- thorized recipi- ents. 3.6.3 Stored keys are stored en- crypted. 3.6.4 A reasonable crypto period shall be set. 3.6.5 A key life cy- cle shall be estab- lished, denoting when keys should be destroyed and when keys should be securely kept for archived/legacy encrypted data. 	AC-1, AC- 2, IA-1, IA- 2, IA-3, IA- 4, IA-5, IA- 6, IA-7, IA- 8, IA-9, IA- 10, IA-11	System Administrator (OM- ADM-001) Product Support Manager (OV-PMA-003)

	3.6.7 Keys shall only be accepted from authorized sources.		
PR.AC-3: Re- mote access is managed.	 8.1.5 Manage IDs used by third par- ties to access, sup- port, or maintain system compo- nents via remote access as follows: enabled only during the time period needed and disabled when not in use monitored when in use 	AC-1, AC- 17, AC-19, AC-20, SC- 15	Information Systems Security Developer (SP-SYS-001) System Administrator (OM- ADM-001)
PR.AC-4: Ac- cess permis- sions and au- thorizations are managed, incorporating the principles of least privi- lege and sepa- ration of du- ties.	 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. 7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. 	AC-1, AC- 2, AC-3, AC-5, AC- 6, AC-14, AC-16, AC- 24	Technical Support Specialist (OM-STS-001) Technical Support Specialist

		7.2 Establish an ac- cess control sys- tem(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.		
		1.1 Establish and implement firewall and router config- uration standards.	AC-4, AC- 10, SC-7	Network Operations Special- ist (OM-NET-001)
	PR.AC-5: Net- work integrity is protected (e.g., network segregation, network seg-	1.1.4 requirements for a firewall at each internet con- nection and be- tween any demili- tarized zone (DMZ) and the internal network zone		Network Operations Special- ist (OM-NET-001)
	mentation).	1.2 Build firewall and router config- urations that re- strict connections between untrusted networks and any system compo- nents in the card- holder data envi- ronment.		Network Operations Special- ist (OM-NET-001)

	1.3.6 Place system components that store cardholder data (such as a da- tabase) in an inter- nal network zone, segregated from the DMZ and other untrusted net- works.		Network Operations Special- ist (OM-NET-001)
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	workstation lock- out shall be estab- lished. 8.2 Where appro- priate multifactor	AC-1, AC- 2, AC-3, AC-16, AC- 19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	Systems Requirements Plan- ner (SP-SRP-001)

	PR.AC-7: Us- ers, devices, and other as- sets are au- thenticated (e.g., single factor, multi- factor) com- mensurate with the risk of the transac- tion (e.g., indi- viduals' secu- rity and pri- vacy risks and other organi- zational risks).		AC-7, AC- 8, AC-9, AC-11, AC- 12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA- 10, IA-11	Systems Requirements Plan- ner (SP-SRP-001)
Data Secu- rity (PR.DS): Information and records (data) are managed consistent with the or- ganization's risk strategy to protect the confi- dentiality, integrity, and availa- bility of in- formation.	PR.DS-1: Data at rest is pro-tected.	 3.2 Do not store sensitive authenti- cation data after authorization (even if en- crypted). If sensi- tive authentication data is received, render all data un- recoverable upon completion of the authorization pro- cess. 3.2.1 Do not store the full contents of any track (from the magnetic stripe lo- cated on the back of a card, equiva- lent data con- tained on a chip, or elsewhere) after authorization. This 	MP-8, SC- 12, SC-28	Information Systems Security Developer (OM-DTA-002) Information Systems Security Developer (OM-DTA-002)

	data is alterna- tively called full track, track, track 1, track 2, and magnetic-stripe data.	
	3.2.2 Do not store the card verifica- tion code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not- present transac- tions) after author- ization.	Information Systems Secu- rity Developer (OM-DTA-002)
	3.2.3 Do not store the personal iden- tification number (PIN) or the en- crypted PIN block after authoriza- tion.	Information Systems Secu- rity Developer (OM-DTA-002)
	3.4 Render Primary Account Number unreadable any- where it is stored (including on port- able digital media, backup media, and in logs) by using any of the follow- ing approaches:	Information Systems Secu- rity Developer (OM-DTA-002)

	PR.DS-2: Data in transit is protected.	 1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. 1.3 Prohibit direct public access between the internet and any system component in the cardholder data environment. 	SC-8, SC- 11, SC-12	Information Systems Secu- rity Developer (OM-DTA-002) Cyber Defense Analyst (PR- CDA-001) Information Systems Secu- rity Developer (OM-DTA-002) Cyber Defense Analyst (PR- CDA-001)
	PR.DS-5: Pro- tections against data leaks are im- plemented.		AC-4, AC- 5, AC-6, PE-19, PS- 3, PS-6, SC-7, SC-8, SC-13, SC- 31, SI-4	Information Systems Security Developer (SP-SYS-001)
Information Protection Processes and Proce- dures (PR.IP): Se- curity poli-	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and		CM-2, CM- 3, CM-4, CM-5, CM- 6, CM-7, CM-9, SA- 10	Enterprise Architect (SP-ARC- 001) Cyber Policy and Strategy Planner (OV-SPP-002)

	cies (that ad- dress pur- pose, scope, roles, re- sponsibili- ties, man- agement commit-	maintained, in- corporating se- curity princi- ples (e.g., con- cept of least functionality).			
mer coo amo gan enti pro and dure mai and mar tect form syst	ment, and coordination among or- ganizational entities), processes, and proce- dures are maintained and used to manage pro- tection of in- formation systems and assets.	PR.IP-3: Configuration change control processes are in place.		CM-3, CM- 4, SA-10	Systems Developer (SP-SYS- 002) Systems Security Analyst (OM-ANA-001)
	Protective Technology (PR.PT): Technical se- curity solu- tions are managed to ensure the security and	PR.PT-3: The principle of least function- ality is incor- porated by configuring systems to provide only essential capa- bilities.	1.2.1 Restrict in- bound and out- bound traffic to that which is nec- essary for the cardholder data environment, and specifically deny all other traffic.	AC-3, CM- 7	Privacy Officer/Privacy Com- pliance Manager (OV-LGA- 002)
	resilience of systems and assets, con- sistent with related poli- cies, proce- dures, and agreements.	PR.PT-4: Com- munications and control networks are protected.		AC-4, AC- 17, AC-18, CP-8, SC-7, SC-19, SC- 20, SC-21, SC-22, SC- 23, SC-24, SC-25, SC- 29, SC-32,	Security Architect (SP-ARC- 002) Communications Security (COMSEC) Manager (OV- MGT-002)

			SC-36, SC 37, SC-38 SC-39, SC 40, SC-42 SC-43	3, C-
	Anomalies and Events (DE.AE): Anomalous activity is detected, and the po- tential im- pact of events is un- derstood.	DE.AE-2: De- tected events are analyzed to understand attack targets and methods.	AU-6, CA 7, IR-4, S 4	
DETECT (DE)	Security Continuous Monitoring (DE.CM): The infor- mation sys- tem and as- sets are	DE.CM-1: The network is monitored to detect poten- tial cybersecu- rity events.	AC-2, AU 12, CA-7, CM-3, SC 5, SC-7, S 4	, 2-
	monitored to identify cybersecu- rity events and verify the effec- tiveness of	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	CA-7, PE- 3, PE-6, PE-20	Network Operations Special- ist (OM-NET-001)

protective measures.	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.		AU-12, CA-7, CM- 3, CM-8, PE-3, PE-6, PE-20, SI-4	Threat/Warning Analyst (AN- TWA-001)
Detection Processes (DE.DP): De- tection pro- cesses and procedures are main- tained and tested to en- sure aware- ness of anomalous events.	DE.DP-4: Event detection in- formation is communi- cated.	 10.1 Audit logs are generated, documenting user activity. 10.2 Audit events are logged. 10.2.1 User account privileges are documented. 10.2.7 The creation and deletion of system level objects are logged. 10.3 Events are logged. 10.5 Audit logs are strongly protected, including encryption and strong role-based authentication for authorized log users. 	AU-6, CA- 2, CA-7, RA-5, SI-4	Cyber Defense Infrastructure Support Specialist (PR-INF- 001)

Appendix B Privacy Framework Mapping

Table B-1 shows National Institute of Standards and Technology (*NIST*) *Privacy Framework* Subcategories as outcomes addressed in this practice guide and mapped to the property management (PMS) ecosystem components.

Table B-1 Securing Property Management Systems: NIST Privacy Framework Components Mapping

Privacy Framework Function	Privacy Framework Category	Privacy Framework Subcate- gory	PMS Ecosystem Component
Identify-P	Inventory and Mapping (ID.IM-P)	ID.IM-P4: Data actions of the systems/products/services are inventoried.	Forescout CounterACT 8.1
		ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/prod- ucts/services, including com- ponents, roles of the compo- nent owners/operators, and interactions of individuals or third parties with the sys- tems/products/services.	CryptoniteNXT Secure Zone 2.9.1 StrongKey KeyAppliance
Control-P	Data Processing Man- agement (CT.DM-P)	CT.DM-P1: Data elements can be accessed for review.	Solidres PMS Forescout CounterACT 8.1
		CT.DM-P2: Data elements can be accessed for transmission or disclosure.	Solidres PMS
		CT.DM-P3: Data elements can be accessed for alteration.	Solidres PMS
		CT.DM-P4: Data elements can be accessed for deletion.	Solidres PMS
		CT.DM-P8: Audit/log records are determined, docu- mented, implemented, and reviewed in accordance with policy and incorporating the	Remediant SecureONE 18.06.3-ce

Privacy Framework Function	Privacy Framework Category	Privacy Framework Subcate- gory	PMS Ecosystem Component
		principle of data minimiza- tion.	

Appendix C Deployment Recommendations

When deploying the reference design in a hospitality environment, organizations should follow security best practices to address potential vulnerabilities and ensure that all solution assumptions are valid to minimize any risk to the production network. Organizations leveraging the reference design should adhere to recommended best practices that are designed to reduce risk. Note that the laboratory instantiation of the reference design described in Volume C does not implement every security recommendation on its own.

Organizations should not consider the following list to be comprehensive, as merely following this list will not guarantee a secure environment. Organizations must consider items such as vulnerability and patch management, continuity of operations planning, and environment elements that are not addressed in this document. Planning for design deployment gives an organization the opportunity to audit its existing systems and get a clear view of the controls going into effect.

Appendix D	List of Acronyms
2FA	Two Factor Authentication
CNSSI	Committee on National Security Systems Instruction
GDPR	General Data Protection Regulation
ют	Internet of Things
IP	Internet Protocol
ІТ	Information Technology
MTD	Moving Target Defense
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PMS	Property Management System
POS	Point of Sale
SP	Special Publication
VLAN	Virtual Local Area Network
VM	Virtual Machine
ZTA	Zero Trust Architecture

Appendix E Glossary

Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).		
	SOURCE: Committee on National Security Systems Instruction (CNSSI) 4009-2015		
Architecture	The design of the network of the hotel environment and the components that are used to construct it.		
Authentication	The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.		
	SOURCE: Federal Information Processing Standards (FIPS) 200		
Authorized User	Any appropriately provisioned individual with a requirement to access an information system.		
	SOURCE: CNSSI 4009-2015		
Console	A visually oriented input and output device used to interact with a computational resource.		
Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.		
	SOURCE: NIST SP 800-150		
Firewall	A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.		
	SOURCE: NIST SP 800-152		
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.		
	SOURCE: FIPS 200		

Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).		
	SOURCE: CNSSI 4009-2015		
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.		
Privilege	SOURCE: NIST SP 800-37 Rev. 2 A right granted to an individual, a program, or a process.		
	SOURCE: CNSSI 4009-2015		
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.		
	SOURCE: NIST SP 800-161		
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.		
	SOURCE: FIPS 200		
Wi-Fi	A generic term that refers to a wireless local area network that observes the IEEE 802.11 protocol.		
	SOURCE: NIST Interagency or Internal Report 7250		

Appendix F References

- [1] National Institute of Standards and Technology. *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*, Version 1.0. Available: <u>https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1</u> <u>.0.pdf</u>.
- [2] Hotel Technology Next Generation (HTNG). Secure Payments Framework for Hospitality, version 1.0. Feb. 2013. Available: <u>https://cdn.ymaws.com/htng.site-ym.com/resource/collection/CC1CE2B8-0377-457E-9AB0-</u> 27CFDD77E17B/HTNG Secure Payments Framework v1.0 FINAL.pdf.
- [3] HTNG. *Payment Tokenization Specification*. Feb. 21, 2018. Available: https://www.htng.org/page/technical_specs.
- [4] HTNG. Payment Systems & Data Security Specifications 2010B. Oct. 22, 2010. Available: https://cdn.ymaws.com/www.htng.org/resource/resmgr/Files/Specifications/2010B/HTNG_201 0B_PaymentsWG_Paymen.pdf.
- [5] HTNG. EMV for the US Hospitality Industry. Oct. 1, 2015. Available: <u>https://cdn.ymaws.com/sites/htng.site-ym.com/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/2015-09-23_EMV_White_Paper.pdf</u>.
- [6] Payment Card Industry Data Security Standard version 3.2.1. May 2018. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.
- [7] HTNG. GDPR for Hospitality. June 1, 2019. Available: https://www.hospitalitynet.org/file/152008749.pdf.
- [8] NIST. *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1. Apr. 16, 2018. Available: <u>https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf</u>.
- Joint Task Force Transformation Initiative, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication (SP) 800-53 Rev. 4, NIST, Gaithersburg, Md., Apr. 2013. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf</u>.
- P. Grassi et al., Digital Identity Guidelines, NIST SP 800-63-3, NIST, Gaithersburg, Md., June 22, 2017. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf</u>.
- [11] E. McCallister et al., *Guide to Protecting the Confidentiality of Personably Identifiable Information (PII)*, NIST SP 800-122, NIST, Gaithersburg, Md., Apr. 2010. Available: <u>https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf</u>.

- [12] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, NIST SP 800-181, NIST, Gaithersburg, Md., Aug. 2017. Available: <u>https://</u> <u>nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf</u>.
- [13] Abbasi et al., 2019 Trustwave Global Security Report, 2019 Trustwave Holdings, Inc. Available: <u>https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/</u>.
- [14] NIST. *Risk Management Framework: Quick Start Guides*. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-startguides.
- Joint Task Force, *Risk Management Framework for Information Systems and Organizations*, NIST SP 800-37 Revision 2, NIST, Gaithersburg, Md., Dec. 2018.
 Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.</u>
- [16] Joint Task Force, Guide for Conducting Risk Assessments, NIST SP 800-30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
- [17] Social Tables. *Cybersecurity for Hotels: 6 Threats Just Around the Corner from Your Property.* Available: <u>https://www.socialtables.com/blog/hospitality/cyber-security-hotels/</u>.
- [18] Calicchio et al, 2018 PwC Hotels outlook: 2018-2022. PWC, Inc. Available: https://www.pwc.co.za/en/assets/pdf/hotels-outlook-18-2022.pdf
- [19] C. Paulsen R. Byers, Glossary of Key Information Security Terms, NIST Interagency or Internal Report 7298 Rev. 3, NIST, Gaithersburg, Md., July 2019. Available: https://csrc.nist.gov/glossary/term/vulnerability.
- [20] W. Newhouse et al., Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers, NIST SP 800-17, NIST, Gaithersburg, Md., Aug. 2018, 253 pp. Available: <u>https://www.nccoe.nist.gov/sites/default/files/library/sp1800/cr-mfa-nist-sp1800-17.pdf.</u>

NIST SPECIAL PUBLICATION 1800-27C

Securing Property Management Systems

Volume C: How-To Guide

William Newhouse Information Technology Laboratory National Institute of Standards and Technology

Michael Ekstrom Jeff Finke Marisa Harriston The MITRE Corporation McLean, Virginia

September 2020

DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems





1 **DISCLAIMER**

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

National Institute of Standards and Technology Special Publication 1800-27C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-27C, 126 pages, September 2020 CODEN: NSPUE2

8 **FEEDBACK**

- 9 You can improve this guide by contributing feedback. As you review and adopt this solution for your
- 10 own organization, we ask you and your colleagues to share your experience and advice with us.
- 11 Comments on this publication may be submitted to: <u>hospitality-nccoe@nist.gov</u>
- 12 Public comment period: September 14, 2020 through October 28, 2020.
- 13 All comments are subject to release under the Freedom of Information Act.

14	National Cybersecurity Center of Excellence
15	National Institute of Standards and Technology
16	100 Bureau Drive
17	Mailstop 2002
18	Gaithersburg, MD 20899
19	Email: <u>nccoe@nist.gov</u>

20 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- 21 The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards
- 22 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
- 24 public-private partnership enables the creation of practical cybersecurity solutions for specific
- industries, as well as for broad, cross-sector technology challenges. Through consortia under
- 26 Cooperative Research and Development Agreements (CRADAs), including technology partners—from
- 27 Fortune 50 market leaders to smaller companies specializing in information technology security—the
- 28 NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity
- 29 solutions using commercially available technology. The NCCoE documents these example solutions in
- 30 the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework
- and details the steps needed for another entity to re-create the example solution. The NCCoE was
- 32 established in 2012 by NIST in partnership with the State of Maryland and Montgomery County,
- 33 Maryland.
- To learn more about the NCCoE, visit <u>https://www.nccoe.nist.gov/</u>. To learn more about NIST, visit <u>https://www.nist.gov</u>.

36 NIST CYBERSECURITY PRACTICE GUIDES

- 37 NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity
- 38 challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the
- 39 adoption of standards-based approaches to cybersecurity. They show members of the information
- 40 security community how to implement example solutions that help them align more easily with relevant
- 41 standards and best practices, and provide users with the materials lists, configuration files, and other
- 42 information they need to implement a similar approach.
- 43 The documents in this series describe example implementations of cybersecurity practices that
- 44 businesses and other organizations may voluntarily adopt. These documents do not describe regulations
- 45 or mandatory practices, nor do they carry statutory authority.

46 **ABSTRACT**

- 47 Hotels have become targets for malicious actors wishing to exfiltrate sensitive data, deliver malware, or
- 48 profit from undetected fraud. Property management systems (PMSes), which are central to hotel
- 49 operations, present attractive attack surfaces. This example implementation strives to increase the
- 50 cybersecurity of the PMS. The objective was to build a standards-based example implementation that
- 51 utilizes readily available commercial off-the-shelf components that enhance the security of a PMS
- 52 ecosystem.

- 53 The NCCoE at NIST built a PMS ecosystem in a laboratory to explore methods for improving the
- 54 cybersecurity of a PMS. The scope of the PMS ecosystem included the PMS, a credit card payment
- 55 platform, and an analogous ancillary hotel/PMS system. In this example implementation, a physical
- 56 access control system was used as the ancillary system.
- 57 The principal capabilities are to protect sensitive data, to enforce role-based access control, and to
- 58 monitor for anomalies. The principal recommendations and best practices are implementing
- 59 cybersecurity concepts such as zero trust, moving target defense, tokenization of credit card data, and
- 60 role-based authentication.
- 61 The PMS ecosystem outlined in this guide encourages hoteliers and similar stakeholders to adopt
- 62 effective cybersecurity concepts by using standard components that are composed of open-source and
- 63 commercially available components.

64 **KEYWORDS**

- 65 access control; hospitality cybersecurity; moving target defense; PCI-DSS; PMS; property management
- 66 system; role-based authentication; tokenization; zero trust architectures

67 ACKNOWLEDGMENTS

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

Name	Organization
Sapna George	Cryptonite
Hans Ismirnioglou	Cryptonite
Mike Simon	Cryptonite
Rich Walchuck	Cryptonite
Justin Yackoski	Cryptonite
Katherine Gronberg	Forescout
Timothy Jones	Forescout
Scott Morrison	Forescout

Name	Organization
Shane Stephens	Forescout
Oscar Castiblanco	Häfele
Ryan Douglas	Häfele
Chuck Greenspan	Häfele
Sarah Riedl	Häfele
Harald Ruprecht	Häfele
Roy Wilson	Häfele
Kevin Garrett	Remediant
Paul Lanzi	Remediant
Nicole Guernsey	StrongKey
Pushkar Marathe	StrongKey
Arshad Noor	StrongKey
Bill Johnson	TDi
Pam Johnson	TDi
John Bell	HTNG
Kartikey Desai	MITRE
Eileen Division	MITRE
Karri Meldorf	MITRE

Name	Organization
Paul Ward	MITRE
Trevon Williams	MITRE

70 The Technology Partners/Collaborators who participated in this build submitted their capabilities in

- 71 response to a notice in the Federal Register. Respondents with relevant capabilities or product
- components were invited to sign a Cooperative Research and Development Agreement (CRADA) with
- 73 NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Cryptonite	network protection appliance that provides additional layer of protection against cyber attacks
Forescout	visualizes the diverse types of devices connected to the network; enforces policy-based controls
Häfele	physical access control ecosystem that includes door locks, room-key encoding, and management
Remediant	real-time incident monitoring and detection, privilege escalation management, and reporting functions
StrongKey	payment solution appliance that secures credit card transactions and shrinks the payment card industry compliance enclave
TDi	access control platform that secures connections and provides control mechanisms to enterprise systems for authorized users and authorized devices; also monitors activity down to the keystroke

75 **Contents**

76	1	Intr	oduct	ion	1
77		1.1	Турод	raphic Conventions	1
78		1.2	Practi	ce Guide Structure	1
79		1.3	PMS E	cosystem Overview	3
80			1.3.1	Usage Scenarios	3
81			1.3.2	Architectural Overview	3
82			1.3.3	General Infrastructure Details and Requirements	4
83	2	Ηο	w to Ir	nstall and Configure	8
84		2.1	Netwo	ork Protection Solution—CryptoniteNXT	8
85			2.1.1	Overview of Network Protection Solution	8
86			2.1.2	Network Protection Solution–CryptoniteNXT–Requirements	9
87			2.1.3	Network Protection Solution -—CryptoniteNXT–Installation	10
88			2.1.4	Creating Source Groups	11
89			2.1.5	Creating Destination Groups	20
90			2.1.6	Applying Source Groups to End Points	27
91			2.1.7	Applying Destination Group to End Points	31
92			2.1.8	CryptoniteNXT Configuration for the PMS Ecosystem	34
93		2.2	Acces	s Control Platform—TDi ConsoleWorks	37
94			2.2.1	Access Control Platform–TDi ConsoleWorks–Overview	37
95			2.2.2	Access Control Platform—TDi ConsoleWorks—Requirements	38
96			2.2.3	Access Control Platform — TDi ConsoleWorks—Installation	39
97			2.2.4	Add Gateway to GUI	55
98			2.2.5	Add Graphical Connection to End Point	57
99		2.3	Prope	rty Management System–Solidres	59
100			2.3.1	Property Management System Overview	59
101			2.3.2	Property Management System–Solidres–Requirements	59
102			2.3.3	Property Management System–Solidres–Installation	60
103			2.3.4	Server Configuration	69

104	2.4	Data	Tokenization Appliance–StrongKey	72
105		2.4.1	Data Tokenization Appliance–StrongKey–Overview	72
106		2.4.2	Data Tokenization Appliance–StrongKey–Requirements	73
107		2.4.3	Data Tokenization Appliance–StrongKey—Installation	74
108		2.4.4	Payment System Modifications	74
109	2.5	Physi	cal Access Control System—Häfele Dialock	75
110		2.5.1	Physical Access Control System–Häfele Dialock–Overview	75
111		2.5.2	Physical Access Control System–Häfele Dialock–Requirements	76
112		2.5.3	Physical Access Control System–Häfele Dialock–Installation	77
113		2.5.4	Server Installation	78
114		2.5.5	Dialock 2.0 Encoding Station Configuration	94
115		2.5.6	Dialock 2.0 Web Setup	96
116	2.6	Privile	eged Access Management System—Remediant SecureONE	105
117		2.6.1	Privileged Access Management System–Remediant SecureONE–Overview	106
118		2.6.2	Privileged Access Management System–Remediant SecureONE–Requirements	107
119		2.6.3	Privileged Access Management System–Remediant SecureONE—Installation	108
120		2.6.4	Initial Configuration	108
121	2.7	Wirel	ess Network Management—Forescout CounterACT	110
122		2.7.1	Wireless Network Management–Forescout CounterACT–Overview	111
123		2.7.2	Wireless Network Management–Forescout CounterACT–Requirements	112
124		2.7.3	Wireless Network Management–Forescout CounterACT—Installation	113
125		2.7.4	DNS Enforcement	118
126		2.7.5	Switch Plug-in	118
127		2.7.6	Guest Policy	121
128	2.8	Virtua	al Switch—VyOS Configuration	133
129	2.9	Integ	ration of Security Components	135
130		2.9.1	CryptoniteNXT Integration with CLI End Points	135
131	Append	dix A	List of Acronyms	. 136
132	Appen	dix B	Glossary	. 138

133 List of Figures

134	Figure 1-1a PMS Ecosystem High-Level Architecture	.5
135	Figure 1-1b PMS Ecosystem Architecture Detailed	.6
136	Figure 2-1 Network Protection Solution in the Reference Architecture	.9
137	Figure 2-2 Access Control Platform in the Reference Architecture	38
138	Figure 2-3 Data Tokenization Appliance in the Reference Architecture	73
139	Figure 2-4 Physical Access Control Server in the Reference Architecture	76
140	Figure 2-5 Privileged Access Management System in the Reference Architecture)7
141	Figure 2-6 Wireless Network Management in the Reference Architecture1	12

142 List of Tables

143	Table 1-1 Architecture List of Components	4
144	Table 1-2 Network Segment Details of the Hospitality Example Lab Build	6
145	Table 1-3 Lab Network Host Record Information	7
146	Table 2-1 Required Destination Groups for CryptoniteNXT Configuration	35
147	Table 2-2 Required Source-Destination Mappings for CryptoniteNXT Configuration	36

149 **1 Introduction**

- 150 The following volume of this guide shows information technology (IT) professionals and security
- engineers how we implemented this example solution. We cover all the products employed in this
- 152 reference design. We do not re-create the product manufacturers' documentation, which is presumed
- to be widely available. Rather, these volumes show how we incorporated the products together in our
- 154 environment.
- 155 Note: These are not comprehensive tutorials. There are many possible service and security configurations 156 for these products that are out of scope for this reference design.

157 **1.1 Typographic Conventions**

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

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

159 **1.2 Practice Guide Structure**

- 160 This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a
- 161 standards-based reference design and provides users with the information they need to replicate the
- 162 property management system (PMS) ecosystem built in our laboratory. This reference design is modular
- and can be deployed in whole or in part.

- 164 This guide contains three volumes:
- 165 NIST SP 1800-27A: *Executive Summary*
- 166 NIST SP 1800-27B: Approach, Architecture, and Security Characteristics what we built and why
- 167 NIST SP 1800-27C: *How-To Guides* instructions for building the example solution (you are here)
- 169 Depending on your role in your organization, you might use this guide in different ways:
- 170 Business decision makers, including chief security and technology officers, will be interested in the
- 171 *Executive Summary,* NIST SP 1800-27A, which describes the following topics:
- 172 challenges that enterprises face in making a PMS more secure
- 173 example solution built at the NCCoE
- 174 benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess,
 and mitigate risk will be interested in NIST SP 1800-27B, which describes what we did and why. The
 following sections will be of particular interest:

- 178 Section 3.4, Risk, describes the risk analysis we performed.
- Section 3.4.3, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

Section 6.2, Privacy Protections, describes how we used the *NIST Privacy Framework* Subcategories. You
 might share the *Executive Summary*, NIST SP 1800-27A, with your leadership team members to help
 them understand the importance of adopting standards-based PMS cybersecurity.

- 184 IT professionals who want to implement an approach like this will find this whole practice guide useful.
 185 You can use this How-To portion of the guide, NIST SP 1800-27C, to replicate all or parts of the build
 186 created in our lab. This How-To portion of the guide provides specific product installation, configuration,
- and integration instructions for implementing the example solution. We do not recreate the product
- 188 manufacturers' documentation, which is generally widely available. Rather, we show how we
- 189 incorporated the products together in our environment to create an example solution.
- 190 This guide assumes that IT professionals have experience implementing security products within the
- 191 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
- 192 not endorse these particular products. Your organization can adopt this solution or one that adheres to
- these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
- 194 parts of a more secure PMS. Your organization's security experts should identify the products that will
- 195 best integrate with your existing tools and IT system infrastructure. We hope that you will seek products
- 196 that are congruent with applicable standards and best practices. Section 1.3.2, Architectural Overview,

- lists the products that we used and maps them to the cybersecurity controls provided by this referencesolution.
- 199 Acronyms used in figures and tables are in the appendix List of Acronyms.

200 1.3 PMS Ecosystem Overview

The NCCoE at NIST built an example laboratory environment, known hereafter as the PMS ecosystem, to
 explore options available to secure the PMSes used by hotels and other organizations in the hospitality
 sector.

204 1.3.1 Usage Scenarios

Securing a PMS requires implementing strong security measures in not only the PMS but also the
 components that logically and physically communicate with it. These components include an access
 control platform, network protection solutions for enterprise and wireless networks, data tokenization,
 and Privileged Access Management (PAM). The example implementation fulfills several use cases to
 demonstrate needed functionality of a hotel enterprise, including utilizing secure communication and
 tokenization during PMS transactions, creating a room key in a protected manner, and allowing only
 approved connections to the PMS.

- 212 The NCCoE worked with members of the NCCoE Hospitality Community of Interest to develop a set of
- use case scenarios to help design and test the PMS ecosystem. For a detailed description of the PMS
- ecosystem's architecture and the use cases, see Section 4 in Volume B.

215 1.3.2 Architectural Overview

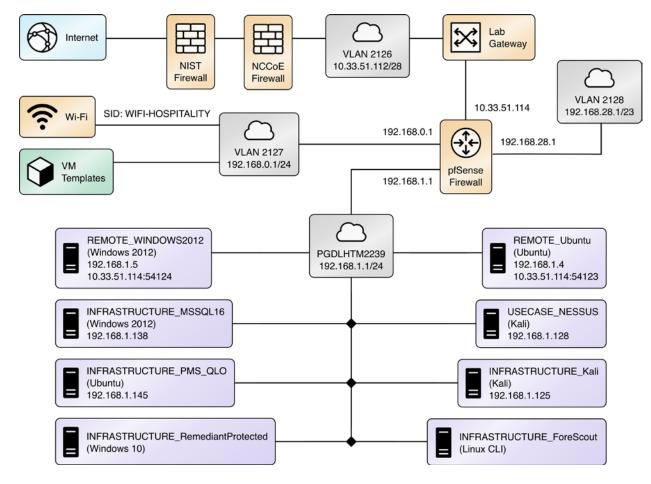
- 216 The Securing Property Management Systems high-level reference architecture is illustrated in Figure 1-
- <u>1a</u> and <u>Figure 1-1b</u>. These figures show the technologies used in the PMS ecosystem. The architecture
 displays the authentication mechanisms, protected network zones, privilege management, and
- 218 displays the authentication mechanisms, protecte219 hospitality enterprise functionality.
 - 220 The implementation enforces that only authorized network communications are allowed to and from
 - the PMS. Three access levels are allowed with the PMS in this build. Unprivileged users, such as guests,
- get limited access, e.g., the public-facing web pages for the PMS, and internet access. Privileged
- enterprise users, such as front desk employees, get elevated access to the reservation process. For this
- build, this is accomplished via a dedicated administrative web page, but this solution will differ based on
- the existing PMS configuration of the adopting enterprise. Finally, the access control platform controls
- any system-level access to administer the PMS server.
- In addition to these privilege protections, we used technologies for secure authentication, securestorage, and secure Wi-Fi.

- 229 We constructed the example implementation on the NCCoE's VMware vSphere virtualization operating
- environment. A limited number of tools and technologies used in this build employed physical
- 231 components. We used internet access to connect to remote cloud-based components, while we
- installed software components as virtual servers within the vSphere environment. The physical
- components were connected to the virtual servers through a layer 2 switch. The technology providers
- used in this build offer physical and virtual deployments of their products. Hospitality PMS
- 235 implementations will vary, and the implementation decisions made in this build between virtual and
- 236 physical will not necessarily align with every hospitality organization's policies and designs.
- 237 The example build implementation uses the components listed in Table 1-1 and shown in Figure 1-1a
- 238 PMS Ecosystem High-Level Architecture and Figure 1-1b PMS Ecosystem Architecture Detailed.
- 239 Table 1-1 Architecture List of Components

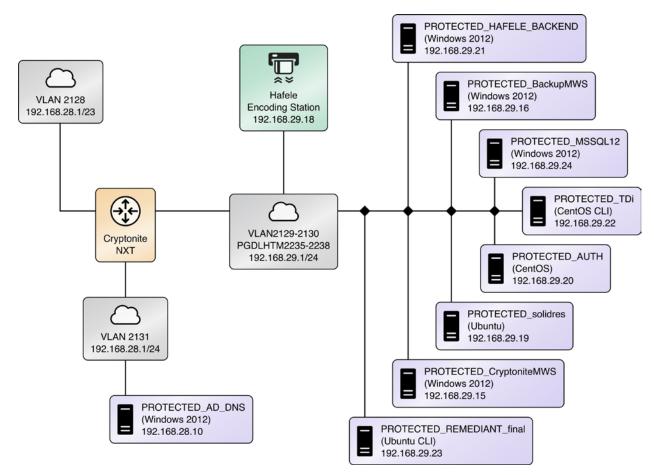
Component	Provider	Installation Guidance
network protection solution	CryptoniteNXT	Section 2.1
access control platform	TDi ConsoleWorks	Section 2.2
property management system	Solidres	Section 2.3
data tokenization appliance	StrongKey	Section 2.4
physical access control system	Häfele Dialock	Section 2.5
privileged access management	Remediant Secure- ONE	Section 2.6
wireless network management	Forescout Counter- ACT	Section 2.7

240 1.3.3 General Infrastructure Details and Requirements

- Figure 1-1a and Figure 1-1b show the lab network architecture that supports the PMS ecosystem. The
- figures show the components, firewalls, and network design of the PMS ecosystem. We separated the
- figures into two figures to make them fit onto the page better with the VLAN (Virtual Local Area
- 244 Network) 2128 device as the connector between the two figures. The installation and configuration
- 245 details for the key components shown in the figures is the focus of this volume of the guide.



246 Figure 1-1a PMS Ecosystem High-Level Architecture



247 Figure 1-2b PMS Ecosystem Architecture Detailed

248

249 1.3.3.1 Network Segmentation and Domain Name System (DNS)

250 Table 1-2 lists the hospitality example lab build's network internet protocol (IP) address range for the

251 PMS ecosystem. These network addresses were used in the example implementation builds and each

252 organization will configure IP addresses to reflect actual network architectures when deployed.

253 Table 1-2 Network Segment Details of the Hospitality Example Lab Build

Network	PMS Ecosystem Segments
192.168.0.0/24	hotel guest and employee Wi-Fi
192.168.1.0/24	network demilitarized zone and Wi-Fi security enforcement
192.168.28.0/23	back-end hotel infrastructure secure zone

- 255 In the PMS ecosystem, DNS was configured as shown in Table 1-3, showing host names, fully qualified
- domain names (FQDNs), and IP addresses to facilitate data communication among the components. The
- 257 domain for the PMS ecosystem is hotel.nccoe. Table entries marked with an asterisk are located within
- the CryptoniteNXT secured zone and do not require a static address. Figure 1-1a and Figure 1-1b show
- the architecture details with IP addresses.
- 260 Table 1-3 Lab Network Host Record Information

Host Name	FQDN	IP Address
win-hotel	win-hotel.hotel.nccoe	192.168.28.10
Forescout	forescout.hotel.nccoe	192.168.1.43
Tdi	tdi.hotel.nccoe	192.168.29.22*
Remediantso	remediantso.hotel.nccoe	192.168.29.23*
hafelees	hafelees.hotel.nccoe	192.168.29.18*
hafele	hafele.hotel.nccoe	192.168.29.39*
solidres	solidres.hotel.nccoe	192.168.28.194*
admin-solidres	admin-solidres.hotel.nccoe	192.168.29.50*
cryptonitews	cryptonitemws.hotel.nccoe	192.168.29.49*
front-desk	front-desk.hotel.nccoe	192.168.29.42*
mail	mail.hotel.nccoe	192.168.29.46*

- 261 The network adapter configuration for the DNS server is as follows:
- 262 Network Configuration (Interface 1)
 - IPv4 Manual
 IPv6 Disable
 - IP Address: 192.168.28.10
 Gateway: 192.168.28.3
 - Netmask: 255.255.255.0
 DNS N
 - DNS Name Servers: 192.168.28.10
- 263 DNS-Search Domains: hotel.nccoe

264 2 How to Install and Configure

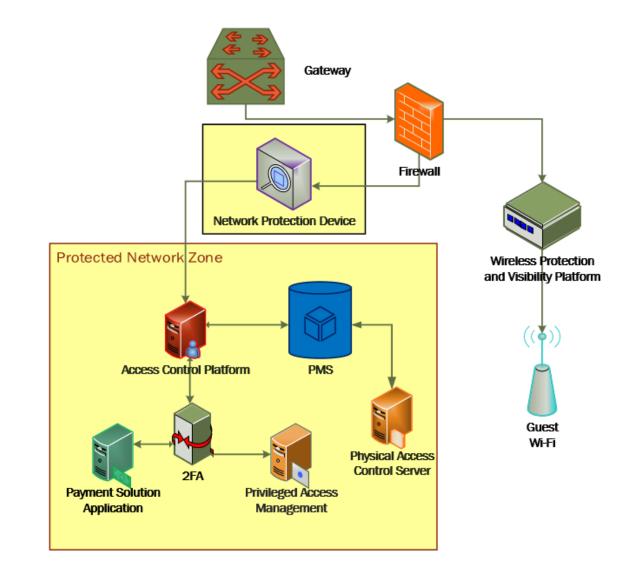
This section of the practice guide contains detailed instructions for installing and configuring all the products used to build an instance of the example implementation.

267 2.1 Network Protection Solution—CryptoniteNXT

- 268 This section of the guide provides installation and configuration guidance for the network protection
- 269 solution, which ensures that only valid end points are allowed to connect to the network and the PMS,
- and that those end points use the network in an approved manner.
- 271 CryptoniteNXT is the network protection solution used in the example implementation.
- 272 When using a network protection solution such as CryptoniteNXT, we recommend installing and setting
- it up before installing other resources onto your network. This is because the CryptoniteNXT device
- 274 serves as the router and switch for the enterprise network. However, apply the steps to secure the
- 275 enterprise, as described in <u>Section 2.1.8</u>, to a component after the component has been separately
- installed and configured within the CryptoniteNXT environment.

277 2.1.1 Overview of Network Protection Solution

- CryptoniteNXT is employed here as the network protection solution device and brings zero trust
 architecture and moving target defense capabilities to the PMS ecosystem.
- 280 CryptoniteNXT is a network appliance installed as a physical device in the NCCoE hospitality lab.
- 281 Installation instructions are included in the packaging that comes with the CryptoniteNXT device. The
- 282 device is also available as a virtual appliance.
- 283 The CryptoniteNXT device requires that users authenticate using multifactor authentication and allows
- only validated connections within the implementation. The device applies a zero trust architecture
- 285 philosophy to its protected network zone. Zero trust architecture is an architectural approach that
- 286 focuses on data protection and role-based authentication. Its goal is to eliminate unauthorized access to
- 287 data, coupled with making the access control enforcement as granular as possible.
- 288 The moving target defense capability of the CryptoniteNXT device anonymizes IP addresses to prevent a
- 289 malicious actor from mapping the enterprise network. The protected network zone controlled by
- 290 CryptoniteNXT is shown in the yellow boxes in Figure 2-1.



291 Figure 2-1 Network Protection Solution in the Reference Architecture

292 2.1.2 Network Protection Solution–CryptoniteNXT–Requirements

- The following subsections document the software, hardware, and network requirements for the network protection solution for version 2.9.1.
- 295 2.1.2.1 Hardware Requirements for the Network Protection Solution
- 296 CryptoniteNXT was deployed as a physical piece of hardware, provided by the vendor. If a virtual 297 appliance is utilized, the appliance will require a 20-gigabyte (GB) hard drive, 4 GB of memory, and a
 - NIST SP 1800-27C: Securing Property Management Systems

virtual central processing unit (CPU). Additionally, Ethernet cables and a serial console cable arenecessary for full setup and configuration.

300 2.1.2.2 Software Requirements for the Network Protection Solution

The CryptoniteNXT device is deployed with its own software requirements fulfilled. However, the first end points to connect to the device will require Java Runtime Environment to run the CryptoniteNXT Administration Control Center (ACC) graphical user interface (GUI) and a terminal emulator software,

- 304 such as PuTTY, to fully install and configure the device.
- 305 2.1.2.3 Network Requirements for the Network Protection Solution
- 306 CryptoniteNXT requires the necessary physical and virtual hardware to allow all virtual end points to
- 307 connect to it, fulfilling the purpose of a network switch and router. A connection is required to the
- 308 upstream gateway that leads to the hotel's wireless network, and to the internet. Furthermore,
- 309 CryptoniteNXT relies on access to a dedicated local area network (LAN) or VLAN with the sole purpose of
- 310 providing intercommunication between the CryptoniteNXT nodes.

311 2.1.3 Network Protection Solution-—CryptoniteNXT–Installation

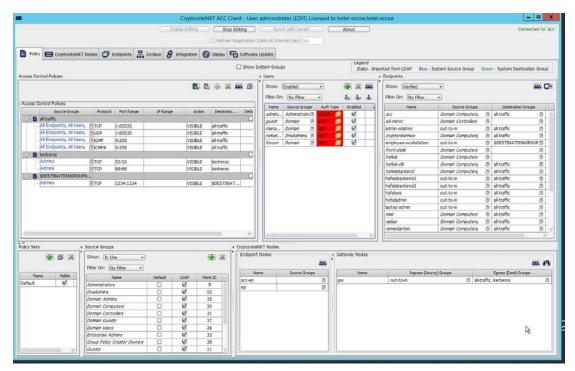
- 312 The majority of the installation and setup for the CryptoniteNXT device can be found in the
- 313 CryptoniteNXT Unified Installation Guide. IP addresses and host names used in this solution are listed in
- 314 <u>Section 1.3.3</u> of this document. Properly configuring CryptoniteNXT to secure an enterprise requires
- 315 creation and application of destination groups (also called access control policies) and source groups. A
- destination group defines the connections that are allowed to connect to a given end point. A source
- 317 group defines the connections that an end point is allowed to make. Find more information in the
- 318 CryptoniteNXT Administration Control Center (ACC) User Manual. <u>Sections 2.1.4</u> and <u>2.1.5</u> have detailed
- instructions to create and apply a generic source and destination group.
- 320 The configuration procedure consists of the following steps:
- 1. Create a source group to govern what network connections can flow from an end point.
- 322 2. Create a destination group to govern what network connections can flow to an end point.
- 323 3. Apply a source group to a specific end point.
- 324 4. Apply a destination group to a specific end point.
- 5. Create and apply the necessary source and destination groups to correctly support the hotelenterprise, as detailed below.

327 2.1.4 Creating Source Groups

The following instructions assume that initial installation and configuration of the CryptoniteNXT device have been completed, as detailed in the CryptoniteNXT Unified Installation Guide. Once completed, open the CryptoniteNXT ACC GUI executable from a connected end point, and click the Policy tab to begin the following configuration.

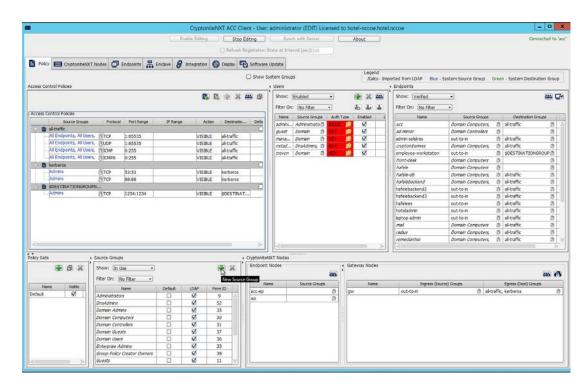
In addition to providing guidance on creating a generic source group, the following instructions will
 allow authorized external traffic to flow through the CryptoniteNXT device.

1. In the Cryptonite **Policy** tab, click **Enable Editing**:

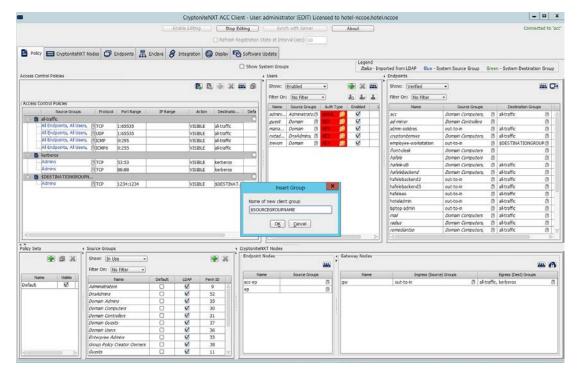


335

336 2. Under the Source Groups box, select the green plus button in the top right (hover text: New337 Source Group):

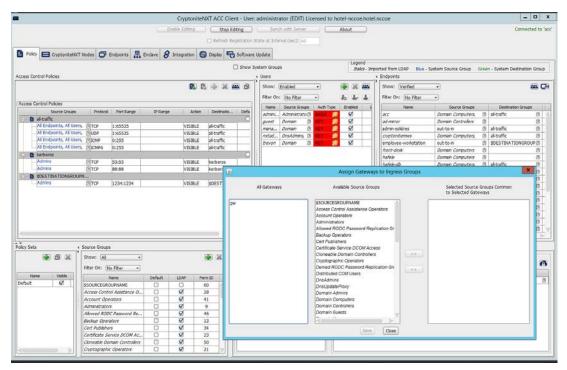


339 3. Input the desired source group name:



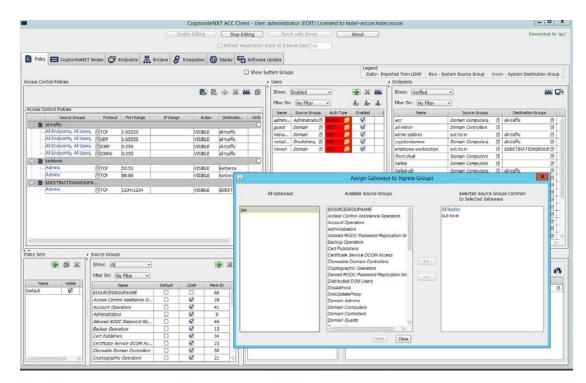
340 4. Click **OK**.

341 5. Under the Gateway Nodes box, select the left-most button (hover text: Assign Gateways to In342 gress Groups):

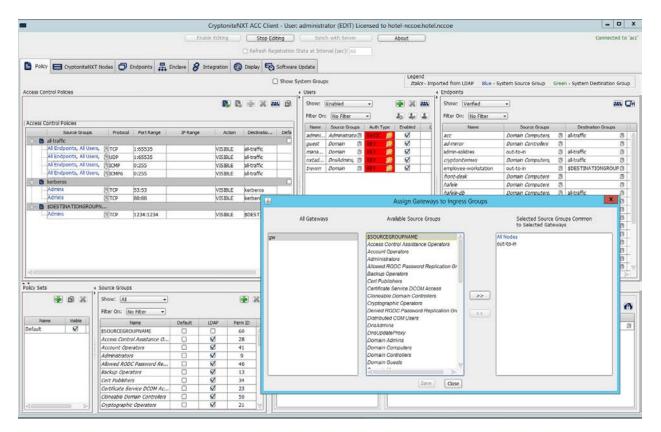


343

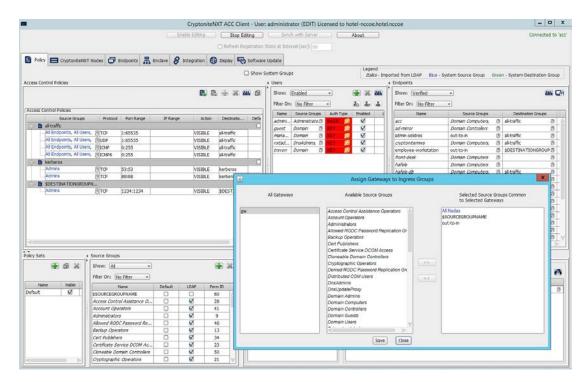
344 6. Select the desired gateway under **All Gateways**:



346 7. Select the desired source group under **Available Source Groups**:

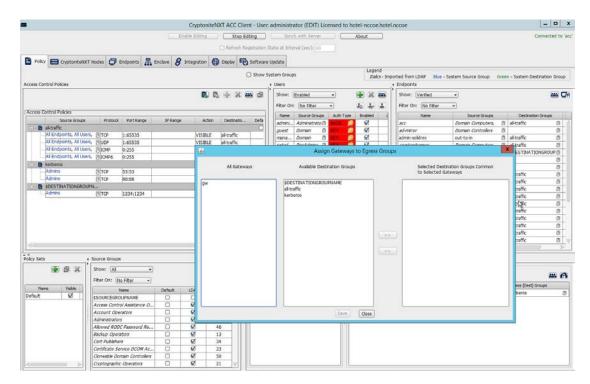


348 8. Click >>:

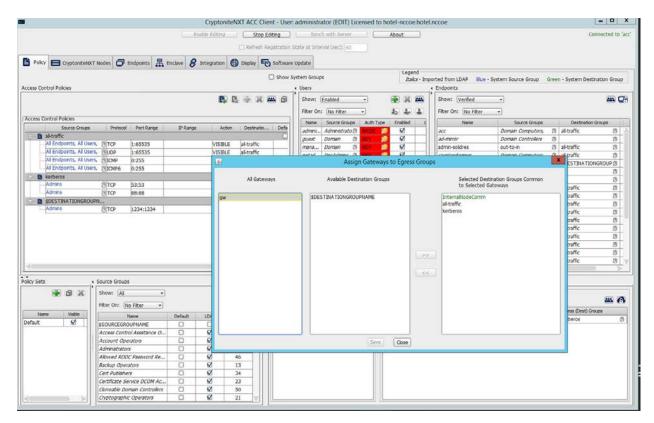


350 9. Click **Save**.

351 10. Click the right-most button (hover text: Assign Gateways to Egress Groups):

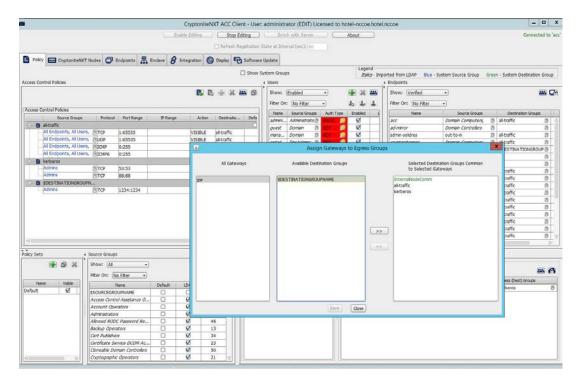


353 11. Select the desired gateway under All Gateways:



354

355 12. Under Available Destination Groups, select the destination groups from which you wish to draw
 access policies:



13. Click >>:

				Ene	ble Editing	Stop Editing	5ynd	th with Server		About					Co	nnected to
						🗇 Refresh Registrata	a france of fact									
								tion result for								
Policy E	GyptoniteNXT	Nodes 🗇	Endpoints 🔒	Enclave 8	integration (Display 🛃 Softw	are Update									
						Short	w System Group	15		Lege		orted from LDAP Blue -	System Source Group	Green	- Suttem Bath	nation Grav
Access Control P	Policies						« Users					Endpoints	alaren anne annah	0.001	- Statem Dead	
					B		Chrune .	Enabled	•]	-	245	Show: Verfied	•			200. (
						ALC: 10 100 10				-	-	the first of the f				
Access Control	18-1-1-						Filter On	No Filter -		\$ \$	A	Filter On: No Filter	-			
Access control	Source Groups	Destruct	Port Range	IP Range		Destnatio Def	Name		Auth Type	Enabled	4	Name	Source Groups		Destination	
D al-tra		Protoco	Port Kange	37 Kange	Action	Liesthato Uen	admint		BASK 🔝	ø		200	Domain Computers,		all-traffic	ø
	ame ndponts, Al Users,	PITCP	1:65535		VISIBLE	al-traffic	guest	Domain 13	KEY 😥	80		ad-minor	Domain Controllers	3		3
	ndpoints, All Users,		1:65535		VISIBLE	al-traffic	///2/	Domain 🔅	KEY 🔝	ø		admin-solidres	out-to-in		all-traffic	3
	ndpoints, All Users, ndpoints, All Users,					an-oranic	and and	Oschámice R		a		Counton Konney	Baasia Computer		al traffic	3
	ndpoints, All Users, ndpoints, All Users,		0:255		1			Assign	Gateways	to Egress	Group	6		×	ESTINATION	IGROUP 3
		DJICMP6	0:255					Trans Sector Sector		-		1377033645046				3
 kerbe Admir 		(Circo)	ka.ca	-		All Gateways		Available Destina	ation Groups				ination Groups Common			3
eta/moto		BITCP	53:53		-							to Selected G	ateways		traffic :	3
Admi		BITCP	88:88		gw							SDESTINATIONGROU	PNAME	_	praffic	13
	E SDESTINATIONGROUPH											InternalNodeComm			prattic	13
Admi	ins	DITCP	1234:1234		_							all-traffic			traffic	3
												kerberos			traffic	3
1															praffic	0
															praffic	3
															traffic	3
												52			traffic	3
											22	10			raffic	3
<(0												1.2				
					_											
		Source Group	28													
olicy Sets																
	x a c	Show: Al		10 C												-
		Show: Al		5												
	Visible	Filter On: [5	LDA										ess (Dest) Gro	
Name		Filter On: (No Filter 🔫	Default	104										ess (Dest) Gri beros	
Name	Visible	Filter On: (No Filter 🔫	Default	900										and the second s	
Name	Visible	Filter On: (\$SOURCEGR Access Cont	No Filter +) Name IOUPNAME <i>trol Assistance O.</i>	Default					[[]						and the second s	
Name	Visible	Filter On: [\$SOURCEGR Access Cont Account Op	No Filter Name LOUPNAME trol Assistance 0 terators	Default	C				Save	Cose					and the second s	
Name	Visible	Filter On: \$SOURCEGR Access Cont Account Op Administratic	No Filter •) Name LOUPNAME trol Assistance O. relators 215	0efsuit		46			Save	Cose					and the second s	
Name	Visible	Filter On: \$SOURCEGR Access Com Account Op Administratic Allowed RO	No Filter +) Name IOUPHAME trol Assistance O. Ierators 215 DC Password Re		La a a a a	46			Save	Close					and the second s	
Name	Visible	Filter On: \$SOURCEGR Access Com Account Op Administratic Allowed ROI Backup Ope	No Filter Nome LOUPNAME trol Assistance O. terators 20 C Password Re. trators		198999	13	Ye		Save	Cose					and the second s	
Name	Visible	Filter On: \$SOURCEGR Access Cont Account Op Administratic Allowed ROI Backup Ope Cert Publish	No Filter Name LOUPHANE tro/Assistance O. lerators ass DC Password Re. irators ers	0e6uit	1988 8 8 8 8 8 8	13 34			Save	Cose					and the second s	
	Visible	Filter On: \$SOURCEGR Access Cont Account Op Administratic Allowed ROI Backup Ope Cevt Publish Certificate S	No Filter Name IOUPNANE tro/Assistance O relators 255 DC Password Re rators ers ers ers ers ers ers ers ers ers e		<u> </u>	13 34 23			Save	Cose					and the second s	109
Name	Visible	Filter On: \$SOURCEGR Access Cont Account Op Administratic Allowed ROI Backup Ope Cevt Publish Certificate S Cloneable D	No Filter Name LOUPHANE tro/Assistance O. lerators ass DC Password Re. irators ers		1988 8 8 8 8 8 8	13 34			Save	Cose					and the second s	

360 14. Click **Save.**

361 2.1.5 Creating Destination Groups

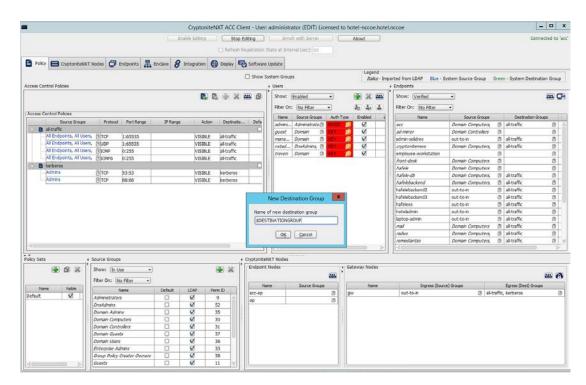
362 The following instructions detail creation of a generic destination group. They assume the same access

363 to the CryptoniteNXT ACC GUI as in the previous instructions.

364 1. Click Enable Editing:

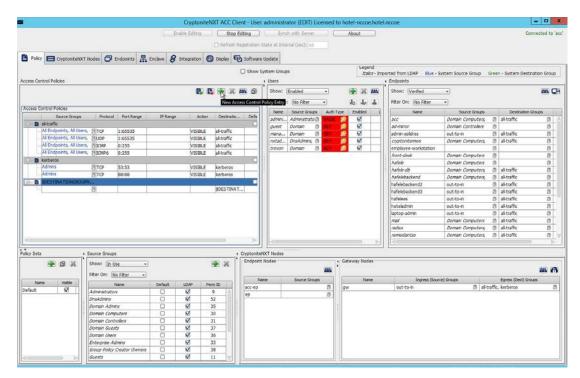
				Cryptonite	IXT ACC Cli	ent - User	administra	ator (EDIT) Lie	ensed to	o hotel-nccoe.hote	Inccoe				- 0
			End	ble Editing	Stop 8	dting	Sync	h with Server		About				c	onnected to '
					Refresh #	legatration .	State at Inte	rval (sec); 60							
Policy CryptonteNXT N	odes 🗿	Endpoints 🔒	Enclave 8 I	ntegration	Display	5 Software	Update								
		100		100		Show S	ystem Group	6		Legend Italcs - Im	ported from LDAP Blue - S	ystem Source Group	o Gree	n - System Des	cination Group
cess Control Policies							• Users				< Endpoints				
				E , 2	$\mathbf{x} \equiv \mathbf{z}$	an 16	Show:	Enabled	*	· · · · · · · · · · · · · · · · · · ·	Show: Verfied	*			20. 0
							Filter On	No Filter	v	40 40 4	Filter On: No Filter	*			
ccess Control Policies							Name	Source Groups	Auth Th		None			Destination	
Source Groups	Protocol	Port Range	IP Range	Action	Destinatio	Defa	admini		ACC113	Ne chaoles e	and the second s	Source Grou		al-traffic	ß
al-traffic							and the second second	Domain 🖸	BASIC .	2	acc ad-minor	Domain Compute Domain Controlle			0
Al Endpoints, Al Users,	NTOP	1:65535		VISIBLE	all-traffic		guest		AND I	2 S	admin-solidres	out-to-in		al-traffic	3
All Endpoints, All Users,	SUOP	1:65535		VISIBLE	all-traffic		mana	Domain S DrisAdmins, S			cryptontemus	Domain Compute		al-traffic	8
All Endpoints, All Users,	MICHP	0:255		VISIBLE	al-traffic		nxtad		ALC: NOT	2	and the second s	Domain compute	WS, 10		13
All Endpoints, All Users,	PICNP6	0:255		VISIBLE	al-traffic		trevon	Domain 🗵	NE V	28 M	employee-workstation front-desk	Domain Compute			13
kerberos	231				5	0	1				hafele	Domain Compute			3
Admins	STOP	53:53		V151BLE	kerberos						hafele-db	Domain Compute		al-traffic	
Admins	NTCP	88:89		VISIBLE	kerberos		11				hafelebackend	Damain Compute		al-traffic	8
											hafelebackend2	out-to-in		al-traffic	0
											hafelebackend3	out-to-in		al-traffic	3
											hafelees	out-to-in		al-traffic	3
											hoteladmin	out-to-in		al-traffic	0
											aptop-admin	out-to-n		al-traffic	3
											mai	Domain Compute		al-traffic	3
											radius	Domain Compute		al-traffic	3
											remediantso	Domain Compute		al-traffic	3
					-	- 2					remedantso	Domain compute	MS, 13	aecramic	10
							15				15				
cy Sets + S	ource Groups					Cryptonite	KT Nodes								
W G X	Show: In U	se •			a x	Endpoint	Nodes		14	Gateway Nodes					
	Filter On: N				a (1997)				-						-
Name Visible		Vane		LDAP Pe	m ID	N	me.	Source Groups		Name	Ingress (Sour			Egress (Dest) G	
4.4. 74	Administrator		Default		0 A	acc-ep			3	gw	out-to-in	3	all-traffic	, kerberos	1
	Aoministracio DinsAdminis	*			9 G	ep			3						
1111	DinsAdmins Domain Admi		0		35										
	Domain Aom Domain Come		0		10										
	Domain Conti Domain Conti		0		31				100						
			0		37										
	Domain Gues Domain Usen		0		3/										
	Coman Usen Enterprise Ac		0		13										
		creator Owners	0		38										
		creator changes	0												
	Guests			80	11 1	1				<u></u>			_		

- Under Access Control Policies, click the left-most icon depicting a piece of paper and a green
 plus sign (hover text: New Destination Group).
- 368 3. Create the name of a new destination group:

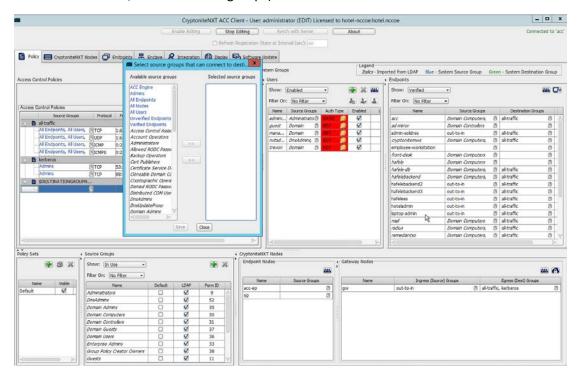


370 4. Click **OK**.

371 5. If there is no blank row underneath the destination group, select the newly created destination
372 group, and click the icon that contains only a green plus sign (hover text: New Access Control
373 Policy Entry):



6. Click the small arrow icon in the **Source Groups** cell of the empty row (hover text: Click the arrow button to view/edit the source groups):





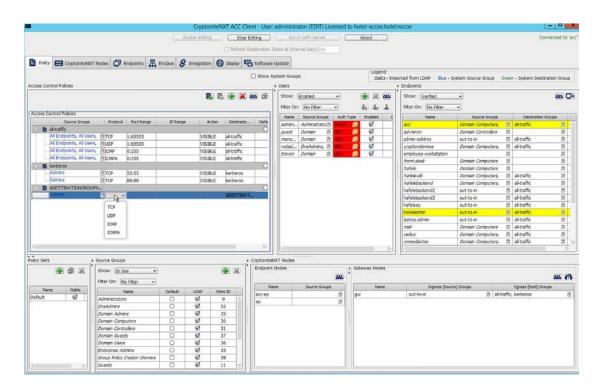
377 7. Select all source groups that you want to have this access:

378

379 8. Click **Save**:

	<u> </u>	nable Editing											
			500	p Editing	Syni	h with Server		About				Con	nected to 'a
F			C) Refrest	i Registratio	n State at Inte	rval (sec): 60							
Madage 17 Endpoints		Internation	(D) providence	ED call	and the data								
	Hect source gro				re opoace			Legend					
1000	CALCULAR MERCE AL		STOLEN TOWN DOWN		stem Group	5			orted from LDAP Blue - S	ystem Source Group	Green	- System Destina	ation Group
Avai	lable source group	16	Selected sou	urce groups	v Users				 Endpoints 				
		Ā.	Admins		Show:	Enabled +		(B) 32 (B)	Show: Verified				20 C
					100000								-
					Filter On	· No Fiter ·		10 40 4	Fitter On: No Fitter	-			
Uma					Name	Source Groups Aut	h Type		Name	Source Groups		Destination G	oups
Verr					admin(Administrato. 3 BAS	к (300	Domain Computers,		all-traffic	3
					guest		8		ad-mirror	Domain Controllers			3
and the second se					//30/12		8		admin-soldres	out-to-in			8
and the second sec		52			nxtad		1		cyptonitemws	Domain Computers,		all-traffic	(9
Browne 0-2 Back	tup Operators	1			trevon	Domain 3 KEY	1	8	employee-workstation				3
Cevt		1								Domain Computers			3
		- Stern							hafele	Domain Computers			ø
										Domain Computers,			3
										Domain Computers,			9
		8								out-to-in			3
													3
													ß
													3
			10										3
										and the second se			3
		Save	Dose										3
					TT				remediantso	Domain Computers,	0	all-traffic	8
Source Groups				+ Crypton	teNXT Nodes								
Show: In Use			(a) (a)	Endpo	nt Nodes		NO	lateway Nodes					
Filter On: No Filter	-						1						-
Name	Default	LDAP	Perm ID	- Announced			11						
Administrators	0	V.	9 A				1	lm	out-to-in	3 al-t	rame,	xerberos	3
DosAdmins	0			ep		.0	1						
Domain Admins		8	35	10			1						
Domain Computers	0	Ø	30										
Domain Controllers	0	Ø	31										
Domain Guests	0	Ø	37										
Domain Users	0	Ø	36										
Enterprise Admins	0	ø	33										
Group Polky Creator Own	ery 🗆	Ø	38										
Guests		Ø	11 1				JUL						
	Source Groups Share Googs Share Groups Source Groups Share Googs S	ACC Engine Al Endontis Al 1100e Al 110e Al 1100e Al 1100e	Al Endonis Al Node Al User Survey of Al Content Al User Survey of Al Content Al User Survey of Al Content Al C	ACC Engne ACT Engne AI Todos AI Todos AI Todos Constructor AI Todos Constructor Advard ROC/ Paser Constructor Anna Amme Doman Amme Doman Amme Doman Amme Doman Amme Market ROC Paser Recipica Constructor Market ROC Paser Doman Amme Market ROC Paser Admestration Market ROC Paser New Defail Doman Admine Market ROC Paser Andronstration Market ROC Paser Andronstration Market ROC Paser Andronstration Market ROC Paser Andronstreter Market ROC Paser<	ACC Engre Al Endoertis Al Todoertis Al Todoertis Al Todoertis Al Todoertis Al Todoertis Al Todoertis Al Todoertis Correct Control Asses Accesse Control Asses Control Asses Accesse Control Asses Accesse Demark Atmins Doman Acmins Doman Acmins Doman Acmins Doman Control to Accesse Acc	ACC Engine Adminis Al Todosi Adminis Al Todosi Adminis Al Todosi Adminis Al Todosi Adminis Construction Adminis Construction Adminis Source Groups Source Construction Shower (no Linguistics Service Administrations) Administration Administrations Administrations Administrations Administrations Source Groups Source Constructions Shower (no Linguistics Service Administrations) Administrations Administrations Administrations Administrations Constructions Demain Adminis Orabulate Mode Administrations Administrations Orabulate Mode Administrations Administrations Orabulate Mode Administrations Domain Computers Orabulate Mode Administrations Administrations Orabulate Mode Administrations Domain Computers Orabulate Mode Administrations Orabulater Mode Administrations Orabulate Mode Administration	ACC Engne Adminis AL Endoertis Al Indee AL Endoertis Al Endoertis AL Endoertis Al Indee AL Endoertis Al Indee AL Endoertis Al Indee AL Endoertis Al Indee AL Endoertis Anne Administrators Administrators Administrators Backa Gonzorta Administrators Backa Gonzorta Administrators Backa Gonzorta Correlations Gonzorta Down Correlations Backa Gonzorta Gonzorta Stource Groups Store Stource Groups Gonzorta Down Gonzorta Administrators Gonzorta Administrators Gonzorta Stource Groups Store Stource Groups Gonzorta Down Gonzorta Administrators Gonzorta Administrators Gonzorta Down Gonzorta Down Gonzorta Down Gonzorta Down Gonzorta	ACC Engne Ad Endertis Al Endertis Ad Index Al Endertis Ad Index Al Endertis Ad Index Al Endertis Admini Antone Store Endertis Admini Antone Store Endertis Admini Antone Store Endertis Admini Admini Antone Store Endertis Store Endertis Store Enderis Store Endertis Store	Avakibi source groups Selected source groups Users Index At Engine Admins At Indoe Admins Admins At Indoe Admins Admins Access Centrol Asses Admins Admins Access Centrol Coll Use Domain Admins Admins Adminstaces Admins Admins Adminstaces Admins Adminstaces Store Bioges Mine Mine Domain Admins Admins Adminstaces	Available source groups Selected source groups Isos Independence A Construction Administration Administration Providence Providence Introduction Administration Providence Providence Providence Introduction Introduction Providence Providence Providence Introduction Providence Providence Pr	Analde source groups Selected source groups Uses forgooids forgooi	Analde source groups Selected source groups Users Edipoints Analde source groups Analde source groups Source Endpoints Source Endpoints Al Endpoints Al Endpoints Administry Source Endpoints Source Endpoints Al Endpoints Administry Administry Source Endpoints Source Endpoints Al Endpoints Administry Source Endpoints Source Endpoints Source Endpoints Access Charled Assess Consult Source Source Endpoints Source Endpoints Source Endpoints Source Endpoints (1000 115 Consult Source Source Endpoint Assess Consult Source Endpoints Source Endpoints Source Endpoints (1000 115 Consult Source Source Endpoint Assess Consult Source Endpoints Source Endpoints Source Endpoints (100 115 Consult Consult Consult Assess Consult Asses	Available source groups Selected source groups Inter- Available source groups Admini adm

- 381 9. Click the **Protocol** cell of the row.
- 382 10. Select the protocol for which you wish to create an access policy:

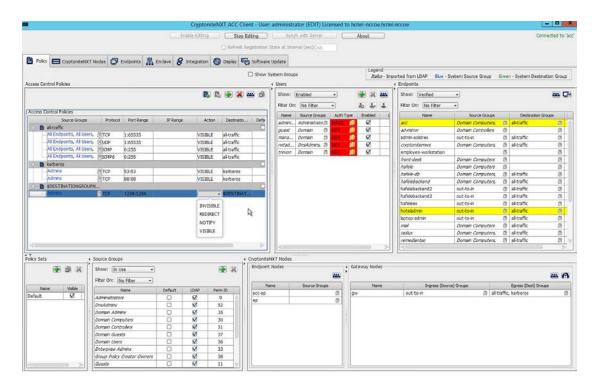


- 384 11. Click the **Port Range** cell of the row.
- 385 12. Input the desired port ranges for the protocol selected in step 10:



13. If desired, click the IP Range cell to modify this value. This is unused in this implementation.

388 14. Click the **Action** cell of the row:

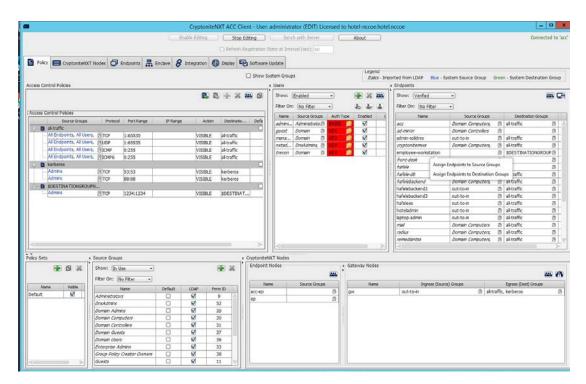


390 15. Set Action to VISIBLE to allow traffic of the described type; use INVISIBLE to block traffic of this
 391 type.

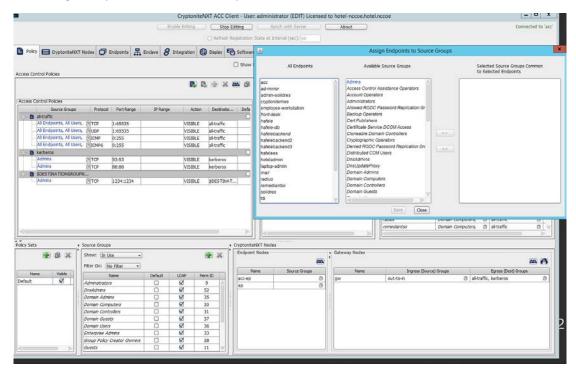
392 2.1.6 Applying Source Groups to End Points

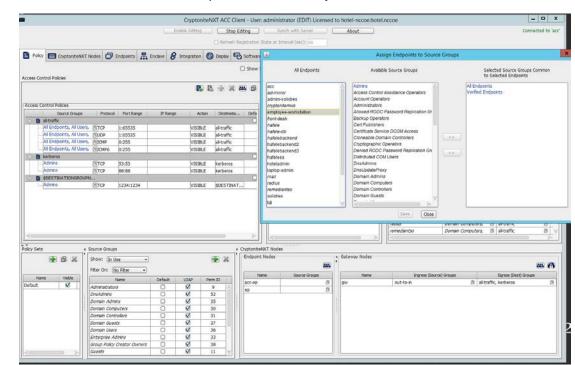
The following instructions detail how to add an already-created source group to a specific end point within the CryptoniteNXT enclave. They assume the same access to the CryptoniteNXT ACC GUI as in the previous instructions.

- 396 1. In the Cryptonite **Policy** tab, click **Enable Editing.**
- Locate the box labeled Endpoints to the right of the window, and right-click the desired end
 point:



3. Select Assign Endpoints to Source Groups:

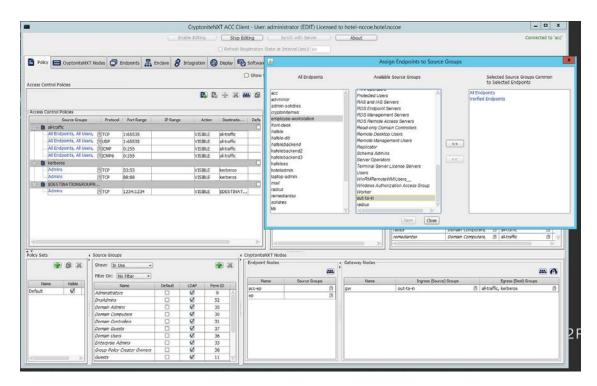




401 4. Find and select the desired end point under **All Endpoints**:

402 403

5. Find and select the desired source group under Available Source Groups:



405

6. Click >>:

					Cryptonite	NXT ACC 0	lient - Use	r: administrator (EDIT) Licensed to	hotel-nccoe.hotel.	nccoe			
				En	able Editing	Sto	p Editing	Synch with Server	About			(Connected to
						Refrest	Registration	State at Interval (sec): 60					
Policy	CryptoniteNXT N	odes 🗇 End	points 🔒 🕻	inclave 🔗	Integration (Display	E Softwar	1	Assi	ign Endpoints to Sour	ce Groups		
ess Con	trol Policies						Show	Al Endpoints	Availabi	e Source Groups		Selected Source Gro to Selected Endpoin	
						8 I I I	<u> </u>	acc ad-mirror admin-solidres	Print Operators Protected Users RAS and IAS Se			Al Endpoints Verified Endpoints out-to-m	
cess Co	ntral Policies							cryptonitemus	RDS Endpoint S				
	Source Groups	Protocol	Port Range	IP Range	Action	Destinat	o Defa	employee-workstation front-desk	RDS Manageme				
	il-traffic							hafele	RDS Remote Ad				
			65535		VISIBLE	all-traffic		hafele-db	Read-only Dom Remote Desktor		40.000		
	Al Endpoints, Al Users, Al Endpoints, Al Users,		65535		V151BLE	al-traffic	_	hafelebackend	Remote Manage		22		
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		255		VISIBLE	all-traffic all-traffic		hafelebackend2	Replicator				
	and a line of the second se	SICMP6 0:	255		VISIBLE	all-traffic	-	hafelebackend3	Schema Admina	8			
	verberos Admins	NTCP 50	1:50		VISIBLE	kerberos		hatelees hoteladmin	Server Operator				
1 1 6	Adminis		1:23		VISIBLE	kerberos		laptop-admin		License Servers			
	DESTINATIONGROUPN				ATOTOPEE	Keiberos		mail	Users WinRMRemotel	Contraction of the local sectors of the local secto			
	Admins		34:1234		VISIBLE	SDESTIN	AT	radius		ization Access Group			
								and the second se	Worker				
								zońdres tdi	radius	Save Cose)		
										linaces))		10
) Domain Co Domain Co		3
4							1-			linaces			3
<	د \$	ource Groups)- + Cryptonit			linaces			3
المربع (Line Seta								13		linaces			3
<inv seta<="" td=""><td>* 8 *</td><td>Show: In Use</td><td></td><td></td><td></td><td>æ ×</td><td></td><td>13</td><td></td><td>linaces</td><td></td><td></td><td>8</td></inv>	* 8 *	Show: In Use				æ ×		13		linaces			8
	* © *					e x	Endpoir	ha holes	Gateway Nodes	remediantso	Domain Co	mputers, 🕅 al-traffic	
Nam	· Voble	Show: In Use	(ter +)	Default	LDAP P		Endpor	Is elit Nodes th Nodes ame Source Groups	Fadius	remediantico	Domain Co	reputérs, 🕼 el-traffic	8 200 (
Nam	· Voble	Show: In Use Filter On: No F	(ter +)		2	em ID	* Endpor	ta etXT Nodes to Nodes same Source Groups	Gateway Nodes	remediantso	Domain Co	mputers, 🕅 al-traffic	8 200 (
Nam	C Voble	Show: <u>In Use</u> Filter On: <u>No F</u> Nam Administrators DrisAdmins	(ter +)		2	erm ID 9 Å 52	Endpor	Is elit Nodes th Nodes ame Source Groups	Fadius	remediantico	Domain Co	reputérs, 🚯 el-traffic	8 200 (
Nam	* Vable	Show: <u>In Use</u> Filter On: <u>No F</u> Nam Administrators DrisAdmins Domain Admins	iter +) e		8 8 8 8	erm ID 9 Å 52 35	* Endpor	ta etXT Nodes to Nodes same Source Groups	Fadius	remediantico	Domain Co	reputérs, 🚯 el-traffic	8 200 (
Nam		Show: <u>In Use</u> Filter On: <u>No F</u> Nam Administrators DisAdmins Domain Admins Domain Compute	iter •] e		2 2 2 2 2 2 2	erm ID 9 Å 52 35 30	* Endpor	ta etXT Nodes to Nodes same Source Groups	Fadius	remediantico	Domain Co	reputérs, 🚯 el-traffic	a) an (
Nam	e Vable	Show: <u>In Use</u> Filter On: <u>No F</u> Nam Administrators DisAdmins Domain Admins Domain Admins Domain Compute Domain Controlle	iter •] e		8 8 8 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	erm ID 9 4 52 35 30 31	* Endpor	ta etXT Nodes to Nodes same Source Groups	Fadius	remediantico	Domain Co	reputérs, 🚯 el-traffic	8 200 (
Nam	e Weble	Show: In Use Filter On: No F Nam Administrators DisAdmins Domain Admins Domain Comput Domain Guestri Domain Guestri	iter •] e		<u>6</u> 66666	erm ID 9 Å 52 35 30 31 37	* Endpor	ta etXT Nodes to Nodes same Source Groups	Fadius	remediantico	Domain Co	reputérs, 🚯 el-traffic	a) an (
Nam	e Vable	Show: In Use Filter On: Non Nam Administrators Donain Adminis Domain Controlle Domain Controlle Domain Controlle Domain Controlle	e e ta		888888 88888 8	em ID 9 Å 52 35 30 31 37 36	* Endpor	ta etXT Nodes to Nodes same Source Groups	Fadius	remediantico	Domain Co	reputérs, 🚯 el-traffic	a a
Nam	e Vable	Show: In Use Fitter On: Non Nam Administrators DisAdmins Domain Admins Domain Comput Domain Guests Domain Guests Domain Guests Enterprise Admi	iter •) e tra tra tra 25		<u>6</u> 66666666	erm ID 9 \$ 52 35 30 31 37 36 33	* Endpor	ta etXT Nodes to Nodes same Source Groups	Fadius	remediantico	Domain Co	reputérs, 🚯 el-traffic	a) an (
okcy Sets Nam Default		Show: In Use Filter On: Non Nam Administrators Donain Adminis Domain Controlle Domain Controlle Domain Controlle Domain Controlle	iter •) e tra tra tra 25		888888 88888 8	em ID 9 Å 52 35 30 31 37 36	* Endpor	ta etXT Nodes to Nodes same Source Groups	Fadius	remediantico	Domain Co	reputérs, 🚯 el-traffic	

406 7. Click **Save.**

407 2.1.7 Applying Destination Group to End Points

The following instructions detail how to apply a previously created destination group to a registered endpoint.

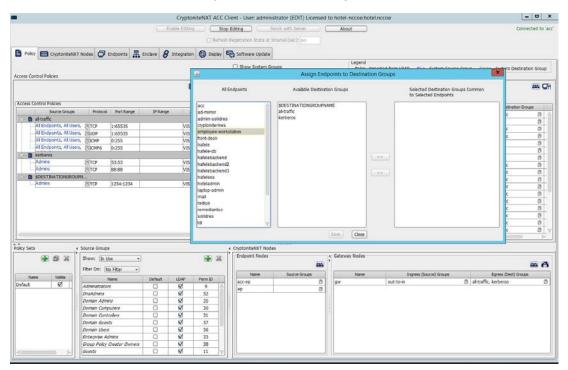
410 1. In the Cryptonite **Policy** tab, click **Enable Editing**:

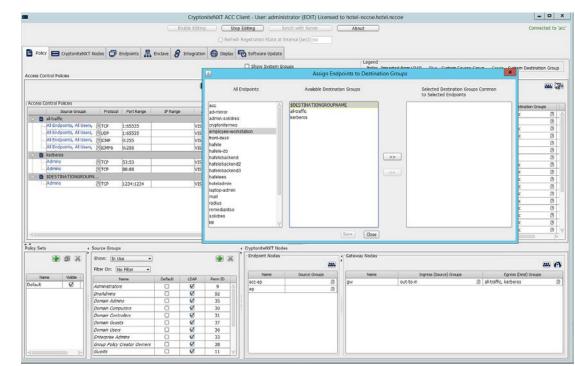
Image: Show: In Use Image: Show: In Use Endpoint Nodes Image: Show: In Use	L				Cryptonit	NXT ACC C	lient - Use	r: administ	rator (EDIT) Lio	ensed to	hotel-nccoe.hote	Linccoe			
Park Cryptontatott Heide Cryptontatott Cryptontat					able Editing	Stop	Editing	Syn	ch with Server		About				Connected to 'a
Store Strain Reage Store Strain Reag						C Refresh	Registration	State at Int	erval (sec): 60						
Bior System Group Bior System Bior System	Policy CryptoniteNXT	Nodes 🗇	Endpoints 💂	Enclave 8	Integration	Display	Softwar	e Update							
Control PADOLE Source Groups Pathole Source Groups Pathol					1		Show		ps				lystem Source Group	Green - System	n Destination Group
Access Centrol Pilouss Source Groups Petro C::::::::::::::::::::::::::::::::::::	Iccess Control Policies							« Users				Endpoints			
Norme Source Graupe Autom Description Image: Source Graupe Autom					P,		-				and the second second				200 Q
Source Groups Peakout Peakout<	Arrian Control Bolician							Filter Or	1: No Filter	•		Filter On: No Filter	-		
Administration of the product o		Benhavel	Bertfreine	IR Danasa		Dection	Defe	Name	Source Groups	Auth Ty		Name	Source Groups	Dest	Ination Groups
Ardiers Dirac Dirac <thdirac< th=""> <t< td=""><td></td><td>Produce</td><td>Portikange</td><td>p sage</td><td>8630</td><td>L Descriege</td><td>Dere Dece</td><td>admini.</td><td></td><td>HASN,</td><td></td><td>acc N</td><td></td><td></td><td></td></t<></thdirac<>		Produce	Portikange	p sage	8630	L Descriege	Dere Dece	admini.		HASN,		acc N			
Image: Open 1/033/5 VISINE # Bronk H Endports, Al Users, Vision # Bronk VISINE # Bronk Al Endports, Al Users, Vision # Bronk VISINE # Bronk Al Endports, Al Users, Vision # Bronk VISINE # Bronk Administration # TOP \$23.5 Administration # TOP \$23.5 Administration # TOP \$23.5 Administration # TOP \$23.5 Top 2 # 100 YISINE # Bronk Administration # TOP \$23.5 YISINE # State Ketheres Administration # TOP \$23.5 YISINE # State Ketheres Administration # TOP \$23.5 YISINE # State Ketheres Administration # TOP \$23.6 YISINE # State Ketheres Administration # TOP \$23.6 YISINE # State Ketheres Ketheres Administration # TOP Administration # TOP \$23.6 YISINE # State Ketheres Ketheres Administration # TOP Ketheres Administration # TOP Ketheres Administration # TOP Ketheres <		DOT OF	a creat		A LOC DOL D			quest				ad miller	Domain Controllers	3	
Al de la constance de la							-	mana				admin-solidres	out-to-in	B al-traffic	3
Implementation Indexes								nxtad	Dostdmins, 13	KEY	20	cryptonitemws	Domain Computers,	IS al-traffic	5
Index of a second							-	trevon	Domain 3	KEY	S S	employee-workstation	and a second second	3	3
Image: Program (Computer) Computer (Computer) <thcomputer (computer)<="" th=""> Computer (Computer)<</thcomputer>	and the state of t	C BURNER	0:255		VISIBLE	pali-trame	-	4				front-desk	Domain Computers	3	.0
Idmms Drow Drow <thdrow< th=""> Drow Drow <th< td=""><td></td><td></td><td></td><td></td><td></td><td>14</td><td></td><td></td><td></td><td></td><td></td><td>hafele</td><td>Domain Computers</td><td>3</td><td>0</td></th<></thdrow<>						14						hafele	Domain Computers	3	0
Versite Versite Portex Indebactend Outros Outros Indebactend Adminis Outros Versite SDDESTRIAT Indebactend Outros Indebactend Outros Indebactend Indebactend <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>_</td> <td></td> <td></td> <td></td> <td></td> <td>hafele-db</td> <td>Domain Computers,</td> <td>al-traffic</td> <td>3</td>							_					hafele-db	Domain Computers,	al-traffic	3
edstrike ThokeGouldH Marris () () ()	and the second se		88:88		VISIBLE	kerberos	_					hafelebackend	Domain Computers,	IS al-traffic	3
Name Source Groupe Source Groupe Source Groupe Name Doman Computers 3 strafts Source Groupe Name Source Groupe Source Groupe Source Groupe Source Groupe Source Groupe Source Groupe Source Groupe Source Groupe Name Doman Admin Source Groupe Source Groupe Source Groupe Source Groupe Doman Admin Source Groupe Source Groupe Source Groupe Source Groupe Source Groupe Doman Admin Source Groupe Source Groupe Source Groupe Source Groupe Source Groupe Doman Admin Source Groupe Source Groupe Source Groupe Source Groupe Source Groupe Source Groupe Doman Admin Source Groupe Source Groupe Source Groupe Source Groupe Source Groupe Source Groupe </td <td></td> <td>hafelebackend2</td> <td>out-to-in</td> <td>(3) al-traffic</td> <td></td>												hafelebackend2	out-to-in	(3) al-traffic	
Image: Source Groups Source Groups Computer Side at caffic Simplify and Computer Side at caffic Simpli	Admina	BITOP	1234:1234		VISIBLE	SDESTIN/	AT					hafelebackend3	out-to-in	3 al-traffic	3
New Default Ubb Person New Default Ubb Person Satural Computers attraffic Computers Compu												hafelees	out-to-in	(3) al-traffic	
Image: Source Groups Control Formulations Source Groups Advantic Source Groups Image: Source Groups												hoteladmin	out-to-in	(3) al-traffic	
Image: Source Groups Source Groups Image: Source Groups Image: Source Groups Inclusion Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Image: Source Groups Ima												botco-admin			
Name Doman Computers al-caffic Name Shore: In 156 Image: In 156 Name Shore: In 156 Image:												mai	Doman Computers	[3] al-traffic	
Name Default Operation Computers Default Name Default Down Computers Default Name Default Default Default Default Default Off Default Default Default Default Default Default Default Default Default De															
Name Source Groups Name Source Groups Name Source Groups Name Source Groups Administration Ø Donan Admin Ø Donan Gentraler												and a first and a second se			
Name Default LOAP Perm D Amred 202010 Of 92 Amred 202010 Of 92 Doman Admin Of 92 Doman Revers Of 93 Doman Revers Of 9	<0						×.	10			- N		Deman comparent	Distant	
Name Default LOAP Perm D Amred 202010 Of 92 Amred 202010 Of 92 Doman Admin Of 92 Doman Revers Of 93 Doman Revers Of 9								I ICC				1000 m			č.
Nome Dotation Office Name	olicy Sets 4	Source Group	s .				< Cryptonit	eNXT Nodes							
Name Vielde Name Default LOAP Perm ID Infractorizition Image: second sec	(A)	Show: To H	(co =			(BR) (SP)	Endpoir	nt Nodes			Gateway Nodes				
Nume Voider Name Default LDAP Perm ID Accessor Standard Standard <td></td> <td>- A</td>															- A
V Administrations V 9 0	Name Visible		Name	Default	LDAP	Perm ID		same	Source Groups		No.				
Driskdimme Image: Second Sec	Default 🗹					and the second se	1.				ĝw.	out-to-in	[3 al-t	traffic, kerberos	3
Domain Admini If If Domain Controller If If Domain Guids If If			ā. — — — — — — — — — — — — — — — — — — —				ep			- 3					
Domain Computers Image: Section 200 Domain Computers Image: Section 200 Domain Computers Image: Section 200 Domain Uters Image: Section 200 Domain Uters Image: Section 200 Difference Image: Section 200 Difference Image: Section 200	1		ine .				1								
Domain Controller Image: Controller							1.11			1.1					
Domain Guests IM S7 Domain Guests IM S6 Diterprise Admin IM S3 Group Palor, Creator Owners IM S8							201			11					
Domain Users 0 90 36 Detexpise Adminu 90 33 Group Public Creator Owners 90 33															
Enterprise Admini IV 33 Group Policy Creator Owners IV 38															
Group Policy Creator Owners															
			ware writing												

- 411
- 412 2. Locate the box titled **Endpoints** on the right hand of the screen. Right-click on any of the end413 points.
- 414 3. Select Assign Endpoints to Destination Groups:

(Crypto	niteNXT ACC C	lient - User: admi	nistrator (EDIT) Licensed	to hotel-nccoel	notel.nccoe	
		C E	nable Editin	Stop	Editing	Synch with Server	About)	Connected to 1
				C Refresh	Registration State at	t Interval (sec): 60			
Policy CryptoniteNXT N	Nodes 🗇 Endpoints 🔒	Enclave 8	Integration	Oisplay E	Software Update				
		1.5		1.9	Show System	Groups	Legens	Januarian Games (DAD	Canada Particip Destination Course
ccess Control Policies	cess Control Policies						points to Destin	ation Groups	× m Deschadon Group
			1	ALI	Endpoints	Available Destina	tion Groups	Selected Destination Groups Cor to Selected Endpoints	mmon 🕮 C
Access Control Policies				acc	LA.	SDESTINATIONGROUP	IAME		stination Groups
Source Groups	Protocol Port Range	IP Range		ad-mirror		all-traffic			c (3)
 B al-traffic 			-	admin-solidres		kerberos			
Al Endpoints, Al Users,	TCP 1:65535		VIS	cryptonitemws					× 3
Al Endponts, Al Users,			VIS	employee-work	station				c 8
	Al Endpoints, Al Users, BICMP 0:255 VIS			front-desk hafele					3
All Endpoints, All Users,	Al Endpoints, Al Users, MICMP6 0:255 VIS			hafele-db					8
kerberos			100	hafelebackend				22	8
Admins	B TCP 53:53		VIS	hafelebackend2	,				c 8
Admins	TCP 88:88		VIS	hafelebackend3 hafelees				(× 8
SDESTINATIONGROUP	N								c 8
- Admins	8 TCP 1234:1234		VIS	hoteladmin laptop-admin mail radius remediantso solidres					c 8 c 8 c 8 c 8 c 8 c 8
<				10	19		Save Close]	< B C B
kcy Sets 4 S	Source Groups				 CryptoniteNXT No 	des			
Pr				a x	Endpoint Nodes		Gateway Nodes		
2000 C 100 C 100 C	Show: In Use * Filter On: No Filter *			. A					- 7
Name Visible	Name	Default	LDAP	Perm ID	Name	Source Groups	Name	Ingress (Source) Groups	Egress (Dest) Groups
		0	V	9 A	acc-ep	3	gw.	out-to-in 🛛	all-traffic, kerberos
efauit 🗹	Administrators			25	ep	3			
in the second se	DasAdmas		S	52					
	DnsAdmins	0	8	35	8		11		
1									
	DnsAdmins Domain Admins	0	8	35					
100.000	DosAdmins Domain Admins Domain Computers	0	2	35 30					
	DnsAdmins Domain Admins Domain Computers Domain Controllers		N N N	35 30 31					
	Driskdmins Domain Admins Domain Computers Domain Controllers Domain Guests		K K K K	35 30 31 37	100 Y00 Y00 Y				
	Driskdmans Domain Admans Domain Computers Domain Controllers Domain Guests Domain Users		A A A A	35 30 31 37 36					

4. Locate and select the desired end point(s) under All Endpoints:





417 5. Select the desired destination group(s) under **Available Destination Groups**:

418

419 6. Click >>:

			Crypto	niteNXT ACC C	lient - User: adm	inistrator (EDIT) Licensed	to hotel-nccoe.	notel.nccoe	_ 0
			Enable Editin	9 Stop	Editing	Synch with Server	About)	Connected to
				C Refresh	Registration State :	t Interval (sec): 60			
Policy Cryptonit	eNXT Nodes 🗗 Endponts	A Enclave	Integratio	n 🚯 Display I	Software Updat				
2					Show System	Groups	Legend		
ccess Control Policies							points to Destin		Earth Destination Grou
			1	AI	Endpoints	Available Destina	tion Groups	Selected Destination Groups Common to Selected Endpoints	an (
Access Control Policies				acc		al-traffic		8DESTINATIONGROUPNAME	stination Groups
Source Gro	ups Protocol Port Rang	e IP Ran	pe .	ad-mirror		kerberos			c 3
al-traffic				admin-solidres	6				
All Endpoints, All	Users, [] TCP 1:65535		V15	cryptonitemws					x 3
All Endpoints, All	Users, MUDP 1:65535		VIS	employee-work	station				K 13
Al Endpoints, Al	Users, SICHP 0:255		VIS	front-desk					K 10
Al Endponts, Al	Users, BICMP6 0:255		V15	hafele hafele-db					8
kerberos				hafelebackend				35	
Admins	TCP 53:53		V15	hafelebackend				(minimum)	c 3
Admins	[3] TCP 88:88		V15	hafelebackend				ee	3
DESTINATIONG	ROUPN			hafelees				August and a second sec	3
Admins	BTCP 1234:1234	E. I.	V15	hoteladmin laptop-admin					4 3
				mail radius remediantso					x 3 x 3 x 3
				solidres tdi					< 13 < 13 < 13
(Save Cose)	< 3
icy Sets	Source Groups				< CryptoniteNXT N	odes	Save Close		< 3
	- Dr.	-			CryptoniteNXT N Endpoint Node	1	Save Cose		< 3 < 3
icy Sets	- Dr.	•		tdi	Endpoint Node:		Gateway Nodes		
	Show: In Use Filter On: No Filter	•	LDAP	ta	* Endpoint Node:	Source Groups	Gateway Nodes None	Ingress (Source) Groups	c g c g c g c g c g c g c g c g c g c g
Name Visible	Show: In Use Filter On: No Filter Name	• Default		tdi	Endpoint Node Name acc-ep	Source Groups	Gateway Nodes	Ingress (Source) Groups	c B c B c B c B c C B c C C C C C C C C C C C C C C C C C C C
Name Visble	Show: In Use Filter On: No Filter	Defsuit	8	td Perm ID 9	* Endpoint Node:	Source Groups	Gateway Nodes None	Ingress (Source) Groups	c B c B c B c B c C c C c C c C c C c C c C c C c C c C
Name Visble	Show: In Use Filter On: No Filter Name Administrators	• Default		tdi	Endpoint Node Name acc-ep	Source Groups	Gateway Nodes None	Ingress (Source) Groups	c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3
Name Visble	Show: In Use Filter On: No Filter Nome Administrators DisAdminis	Default	12	td Perm ID 9 52	Endpoint Node Name acc-ep	Source Groups	Gateway Nodes None	Ingress (Source) Groups	c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3
Name Visble	Show: In Use Filter On: No Filter Administrators Daskdmins Daman Admins	Default	12 12 12	tdl	Endpoint Node Name acc-ep	Source Groups	Gateway Nodes None	Ingress (Source) Groups	c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3
Name Visble	Filter On: No Filter Filter On: No Filter Name Administrators Donain Admins Domain Admins Domain Computers		20	tdl Perm 10 9 52 35 30	Endpoint Node Name acc-ep	Source Groups	Gateway Nodes None	Ingress (Source) Groups	c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3 c 3
Name Visble	Show: In Use Fiter On: No Fiter Name Administrators Doman Admine Doman Admine Doman Controlers	Default	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	tdl Perm ID 9 52 35 30 31	Endpoint Node Name acc-ep	Source Groups	Gateway Nodes None	Ingress (Source) Groups	c B c B c B c B c C c C c C c C c C c C c C c C c C c C
Name Visble	Show: In Use Filter On: <u>No Filter</u> Name Administrators Doman Admine Doman Computers Doman Controllers Doman Controllers	Default	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	1dl Perm ID 9 52 35 30 31 37	Endpoint Node Name acc-ep	Source Groups	Gateway Nodes None	Ingress (Source) Groups	c B c B c B c B c C c C c C c C c C c C c C c C c C c C
Name Visible	Show: In Use Fiter On: No Fiter Name Administrators Dansan Admins Dansan Admins Dansan Admins Dansan Computers Dansan Computers Dansan Guests Dansan Guests		2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	1di Perm ID 9 52 30 31 37 36	Endpoint Node Name acc-ep	Source Groups	Gateway Nodes None	Ingress (Source) Groups	c g c g c g c g c g c g c g c g c g c g

421 7. Click **Save**.

422 2.1.8 CryptoniteNXT Configuration for the PMS Ecosystem

423 To gain the benefits of a zero trust architecture discussed in Volume B of this document, proper

424 configuration of the CryptoniteNXT device is required. Nonuse of the following network restrictions may

425 limit network functionality and diminish the security benefits of the architecture. However, improperly

426 configured rules can lead to a loss of network functionality. It may be correct for the adopting enterprise

- 427 to install and configure its enterprise architecture and the remaining security architecture before
- 428 applying the final configuration of the CryptoniteNXT device.
- 429 In this implementation, it is necessary to create the following source groups. If an organization's desired
- architecture is different from the one described in this document, it is necessary to adapt the following
- instructions to avoid loss of network or security function. First, create the following source groups by
- 432 using instructions from Section 2.1.4.
- 433 Remediant-Web-Access
- 434 Remediant-Access-Domain
- 435 Remediant-Access-Windows
- 436 RDP-Access
- 437 VNC-Access

438 • HafeleES-Access

439 TDi-Access

- 440 Mail-Allowed
- 441 Create the following destination groups by using the instructions in Section 2.1.5. All rows should be set442 to VISIBLE.
- 443 Table 2-1 Required Destination Groups for CryptoniteNXT Configuration

Destination Group	Source Group	Protocol	Port Range
DNS	All Endpoints	TCP (Transport Control Pro- tocol)	53:53
	All Endpoints	UDP (User Datagram Protocol)	53:53
Mail	Mail-Allowed	ТСР	25:25
	Mail-Allowed	UDP	25:25
Remediant-Domain	Remediant-Access-Domain	ТСР	389:389
	Remediant-Access-Domain	ТСР	636:636
	Remediant-Access-Domain	ТСР	123:123
Remediant-Linux	Remediant-Access-Linux	ТСР	22:22
Remediant-Web	Remediant-Web-Access	ТСР	80:80
	Remediant-Web-Access	ТСР	443:443
	Remediant-Web-Access	ТСР	3000:3000
	Remediant-Web-Access	ТСР	22:22
Remediant-Windows	Remediant-Access-Windows	ТСР	137:139
	Remediant-Access-Windows	ТСР	445:445
Remote-Access-Linux	VNC-Access	ТСР	5901:5901
Remote-Access-Windows	RDP-Access	ТСР	3389:3389
	RDP-Access	UDP	3389:3389
Solidres-Admin-Web	Verified Endpoints	ТСР	80:80
	Verified Endpoints	ТСР	443:443
Solidres-Public	All Endpoints, All Users	ТСР	80:80

Destination Group	Source Group	Protocol	Port Range
	All Endpoints, All Users	ТСР	443:443
TDi-Incoming	TDi-Access	UDP	514:514
	TDi-Access	ТСР	5176:5176
	TDi-Access	ТСР	443:443
Hafele-HafeleES	HafeleES-Access	ТСР	8443:8443

- 445 Apply the source and destination groups to the end points per instructions in Section 2.1.4 and Section
- 446 <u>2.1.5</u>. In some deployments, the adopting enterprise may have included an all-traffic or similar rule to
- facilitate installation of other devices in the protected zone. Remove all-traffic rules that allow elevated
- 448 network privileges at this stage.

449 Table 2-2 Required Source-Destination Mappings for CryptoniteNXT Configuration

End Point	Source Groups	Destination Groups
Solidres administrator interface	Mail-Allowed	Remediant-Linux
		Remote-Access-Linux
		Solidres-Admin-Web
		Mail
Solidres public web interface		Solidres-Public
		Remediant-Linux
		Remote-Access-Linux
enterprise management work-	Remediant-Web-Access	Remediant-Access-Windows
station	TDi-Access	
employee workstations	TDi-Access	
mail server	Mail-Allowed	Mail
Remediant SecureONE	Remediant-Access-Domain	Remediant-Web
	Remediant-Access-Linux	
	Remediant-Access-Windows	
TDi ConsoleWorks	RDP-Access	Remediant-Linux
	VNC-Access	TDi-Incoming

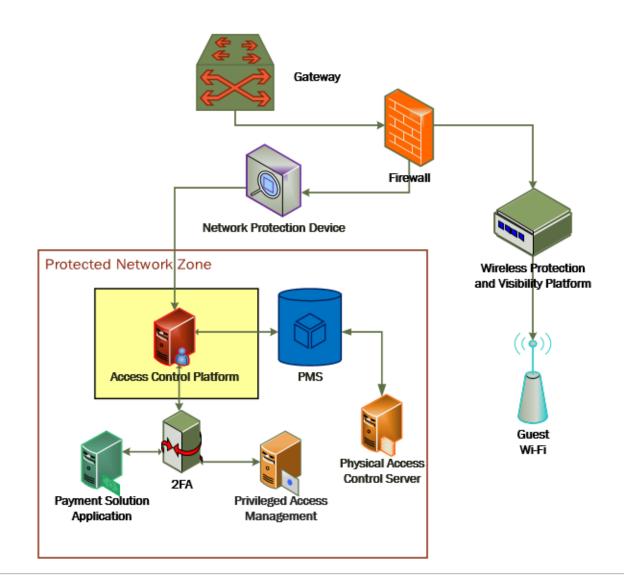
450 2.2 Access Control Platform—TDi ConsoleWorks

- 451 This section of the guide provides installation and configuration guidance for the access control
- 452 platform, which gives access control for system administration in the example implementation. The
- 453 access control platform performs authentication of user and devices, and provides console access to the
- 454 PMS, management workstation, front desk workstations, and Häfele back-end server.
- 455 TDi ConsoleWorks is the access control platform used in the PMS ecosystem.

456 2.2.1 Access Control Platform–TDi ConsoleWorks–Overview

- The access control platform TDi ConsoleWorks performs the access control functionality in the PMSecosystem.
- 459 TDi ConsoleWorks was deployed as a virtual machine (VM) in the NCCoE hospitality lab. Installation
- 460 instructions are available at the TDi Technologies support site, which may be useful if the adopting
- 461 enterprise's deployment differs substantially from the one used for this project.
- 462 TDi ConsoleWorks is employed here to create secure connections to end points. In addition to
- streamlining access to network end points such as the PMS and the administrator workstation, it can be
- used to audit and track those connections to ensure that privileged access is not abused.
- The location of the access control platform in the reference architecture is highlighted in Figure 2-2below.

467 Figure 2-2 Access Control Platform in the Reference Architecture



468

469 2.2.2 Access Control Platform—TDi ConsoleWorks—Requirements

The following subsections document the software, hardware, and network requirements for the accesscontrol platform for version 5.2-0u1.

472 2.2.2.1 Hardware Requirements for Access Control Platform

- 473 TDi recommends amending hardware requirements for ConsoleWorks depending on the size of the
- 474 deployment, but at minimum, allocate 2 GB of storage to the machine.

475 2.2.2.2 Software Requirements for Access Control Platform

- 476 TDi ConsoleWorks 5.2 requires an operating system (OS) from the following list.
- 477 64-bit RedHat Linux 7.5, 7.5, 8.0, or equivalent
- 478 Windows Server 2012 R2
- 479 Windows Server 2016
- 480 Windows Server 2019
- 481 This build utilized a Community Enterprise Operating System (CentOS) 7.3 64-bit server.
- 482 To install TDi ConsoleWorks, access must be available to the machine's command line interface (CLI). It
- 483 will also be necessary for network access to be available to the machine's IP address (retrievable via the
- 484 ifconfig command) during installation. For this build of TDi ConsoleWorks 5.2, installation is conducted
- 485 on a VM in the NCCoE virtual environment.

486 2.2.2.3 Network Requirements of the Access Control Platform

- 487 In addition to the described access to the CLI, the access control platform requires network access to the
- 488 TDi ConsoleWorks back-end server as well as to any end points to which it will connect. The network
- 489 must support secure transmission protocols. TDi ConsoleWorks relies on existing means to connect to
- 490 protected end points, such as Secure Shell (SSH) or Remote Desktop Protocol (RDP).
- 491 Note that use of a zero trust networking solution such as CryptoniteNXT can limit availability of network
- 492 resources when improperly configured. For this reason, we recommend setting up and verifying TDi
- 493 ConsoleWorks before applying rules on the CryptoniteNXT device, as stated in <u>Section 2.1.8</u>.

494 2.2.3 Access Control Platform — TDi ConsoleWorks—Installation

- 495 The installation procedure consists of the following steps:
- 496 1. Download the software.
- 497 2. Run the installation script, customizing options to reflect the enterprise.
- 498 3. Create a secure sockets layer (SSL)-capable invocation of TDi ConsoleWorks and generate an SSL
 499 certificate to match.
- 500 4. Download and apply a license.
- 501 5. Create a gateway to allow GUI functionality.
- 502 6. Create connections to the desired end points within the enterprise.

503	The instr	uction	s below	rely on the	assumed	access to t	he TDi	ConsoleWorks CLI.	The installation media
	C 11								

504 file name takes the form ConsoleWorksSSL-<version>.signed,x86_64.rpm .

If the media is not on the installation target, add it through external media or via the scp command.
Obtaining the installation media requires an account on the TDi Technologies support page and can be

- 507 accessed at <u>https://support.tditechnologies.com/get_consoleworks/linux</u>.
- 508 1. Create a directory in the */tmp* folder: 509 mkdir /tmp/conwrks 2. Move the ConsoleWorks installation media to */tmp/conwrks*: 510 511 mv path/to/media /tmp/conwrks 512 3. Change directory to the *conwrks* directory, and verify that the terminal prompt reflects the 513 change: 514 cd /tmp/conwrks [hospitality@tdi ~]\$ cd /tmp/conwrks [hospitality@tdi conwrks]\$ 515 516 4. Execute the installation media: 517 yum localinstall consoleworksssl-<version>_x86_64.rpm [hospitality@tdi conwrks]\$ sudo yum localinstall ConsoleWorksSSL-5.1-0U1.signed.x86_64.rpm Loaded plugins: fastestmirror Examining ConsoleWorksSSL-5.1-001.signed.x86_64.rpm: ConsoleWorksSSL-5.1-001.x86_64 Marking ConsoleWorksSSL-5.1-001.signed.x86_64.rpm to be installed Resolving Dependencies --> Running transaction check --> Package ConsoleWorksSSL.x86_64 0:5.1-001 will be installed --> Finished Dependency Resolution Dependencies Resolved Package Arch Version Repository Size Installing: ConsoleWorksSSL x86 64 5.1-001 /ConsoleWorksSSL-5.1-0U1.signed.x86_64 350 M

5	1	8	

519 5. Enter the option y to begin the installation.

Total size: 350 M Installed size: 350 M Is this ok [y/d/N]:

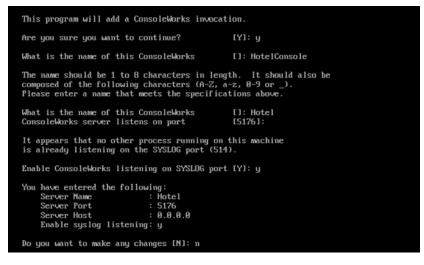
520 6. Wait for the installation to complete. Upon completion, the text Installed: Console 521 worksSSL.[VERSION]should appear:

Install 1 Package	
Total size: 350 M Installed size: 350 M Is this ok [y/d/N]: y Downloading packages: Running transaction check Running transaction test Transaction test succeeded Running transaction Installing : ConsoleWorksSSL-5.1-0U1.×86_64 1/1	
The installation of the ConsoleWorks package has completed. To start using ConsoleWorks, perform the following steps:	
1) Install any license keys you have.	
2) Define an 'invocation' of ConsoleWorks by executing /opt/ConsoleWorks/bin/cw_add_invo	
3) Start the ConsoleWorks server by executing /opt/ConsoleWorks/bin/cw_start	
4) Use a web browser to connect to the location you defined in cw_add_invo, log in with User: console_manager Password: Setup	
5) Register ConsoleWorks. For instructions on registering this ConsoleWorks invocation, see the installation guide or the ConsoleWorks online Help.	
Verifying : ConsoleWorksSSL-5.1-0U1.x86_64 1/1	
Installed: ConsoleWorksSSL.x86_64 0:5.1-0U1	
Complete! [hospitality@tdi conwrks]\$	
2.2.3.1 Create SSL Invocation	
 Escalate to a super user shell by executing the following command and enter password: 	ing the machine
su	

527 2. Verify that the command has executed by seeing that the prompt has changed to root@tdi:

528		Ehospitality@tdi conwrks]\$ su Password: shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such fi le or directory shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such fi le or directory Eroot@tdi conwrks]#
529	3.	Begin invocation creation with the following command:
530		/opt/ConsoleWorks/bin/cw_add_invo
531	4.	Read the End User License Agreement. Accept by typing $_{\rm Y}$ followed by the enter key.
532 533 534	5.	Enter the following information, in order. The values used in this implementation are provided for context but may not be appropriate for your enterprise. Press enter to use the default value provided by the terminal:

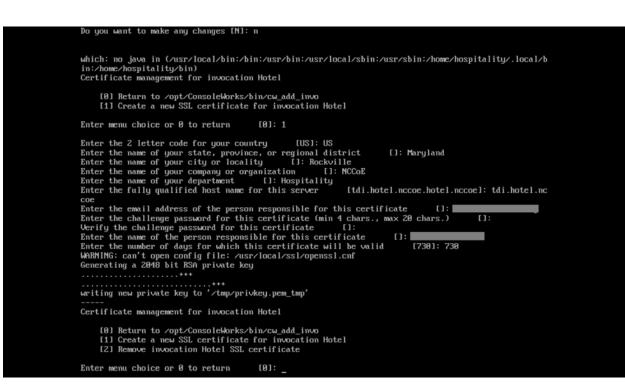
- 535 a. desired console name [HotelConsole]
- b. web service port [5176]
- 537 c. enabled syslog functionality [y]
- 538 6. Verify that the desired values have been entered:



- 540 7. If satisfied, type n for no changes.
- 541

- 542 *2.2.3.2 Create SSL Certificate*
- 543 These instructions rely on execution of Section 2.2.3.1 and are a continuation of the invocation creation
- 544 process. They are separated here for clarity.
- 545 1. Input 1 to allow the SSL invocation creation.

		Do you accept the terms and conditions of this end user license agreement [N]: y
		This program will add a ConsoleWorks invocation. Are you sure you want to continue? [Y]: y
		What is the name of this ConsoleWorks []: HotelConsole
		The name should be 1 to 8 characters in length. It should also be composed of the following characters (A-Z, $a-z$, $\theta-9$ or _). Please enter a name that meets the specifications above.
		What is the name of this ConsoleWorks []: Hotel ConsoleWorks server listens on port [5176]:
		It appears that no other process running on this machine is already listening on the SYSLOG port (514).
		Enable ConsoleWorks listening on SYSLOG port [Y]: y
		You have entered the following: Server Name : Hotel Server Port : 5176 Server Host : 0.0.0.0 Enable syslog listening: y
		Do you want to make any changes [N]: n
		which: no_java_in (/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/home/hospitality/.local/b in:/home/hospitality/bin) Certificate management for_invocation Hotel
		[8] Return to /opt/ConsoleWorks/bin/cw_add_invo [1] Create a new SSL certificate for invocation Hotel
546		Enter menu choice or 0 to return [0]: 1_
547	2. Enter the f	ollowing information, pressing enter after each entry:
548	a.	country code
549	b.	state or provincial name
550	С.	city or locality
551	d.	company or organization name
552	e.	department name
553	f.	FQDN
554	g.	email address of the person responsible for the certificate
555	h.	password to protect the certificate
556	i.	the same password to confirm
557	j.	name of the person responsible for the certificate
558	k.	the number of days for which the certificate will be valid (730 is the default value)
559		



561 3. Input 0 to complete the invocation addition:

Do	you want to make any changes [N]: n
in:	ich: no java in (/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/home/hospitality/.local/b :/home/hospitality/bin) rtificate management for invocation Hotel
	[0] Return to /opt/ConsoleWorks/bin/cw_add_invo [1] Create a new SSL certificate for invocation Hotel
Ent	ter menu choice or 0 to return [0]: 1
Ent Ent Ent Ent Ent Ent Ent Ent MAR Gen	ter the 2 letter code for your country [US]: US ter the name of your state, province, or regional district []: Maryland ter the name of your city or locality []: Rockville ter the name of your department []: Hospitality ter the fully qualified host name for this server [tdi.hotel.nccoe.hotel.nccoe]: tdi.hotel.nc ter the email address of the person responsible for this certificate []: ter the challenge password for this certificate (]: ter the challenge password for this certificate []: ter the name of the person responsible for this certificate []: ter the name of the person responsible for this certificate []: ter the number of days for which this certificate []: HING: can't open config file: /usr/local/ssl/openssl.cnf ter ther a 2848 bit RSA private key
ωri	iting new private key to '/tmp/privkey.pem_tmp'
Cer	 tificate management for invocation Hotel
	[0] Return to /opt/ConsoleWorks/bin/cw_add_invo [1] Create a new SSL certificate for invocation Hotel [2] Remove invocation Hotel SSL certificate
Ent	ten new choice on 8 to neturn [8]: 9

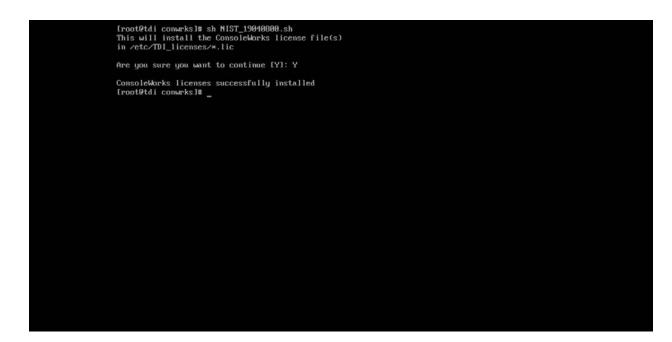
562 2.2.3.3 Apply License

- 563 The following instructions rely on continued access to the command line interface (CLI) of the TDi
- 564 ConsoleWorks device.
- 565 1. Execute the shell script provided as the license by TDi Technologies:



566 567

2. Input Y:



- 569 *2.2.3.4 Start-Up*
- 570 1. Execute the following command, and note the address and port provided in the console re-571 sponse:
- 572

/opt/ConsoleWorks/bin/cw_start Hotel



574 2. Execute the following command:

575

/opt/ConsoleWorks/bin/cw -setsid Hotel

		eWorks/bin/cw -setsid Hotel
	EDT: Consol	eWorks Major Version 5, Minor Version 1, Patch Version 0, Update Ve
rsion 1		
		r image identification is V5.1-0u1-180614LxE
		r expected library identification is 5,1,0;5.1-0u1;18.06.14
		er startup time is 2019/04/16 10:44:28
		r logging configuration file: (internal fallback)
		comment variable CONWRKS_NAME not found - setting to DEFAULT
2019/04/16 10:44:28	EDT: ? ***	The ConsoleWorks environment is not properly set up. Specifically, th
e		
2019/04/16 10:44:28	EDT:	definition of CONWRKS_ROOT is not present. ConsoleWorks is unable to
operate		
2019/04/16 10:44:28	EDT:	until this environment is established. Please use the defined startup
facility		
2019/04/16 10:44:28	EDT:	to start ConsoleWorks. If you are unable to resolve this issue
2019/04/16 10:44:28	EDT:	after confirming that your system is properly configured, then please
2019/04/16 10:44:28	EDT:	contact TDI Support per the terms of your support agreement
[root@tdi conwrks]#		

5763. On another machine, open the web page provided in step 1 or the IP followed directly by the577port number:

CounterACT Console Installer	× 🔎 Hotel on 192.168.1.148 - Console 🗙 🕂		X
← → C ① Not secure	192.168.1.148:5176/login.html		☆ 0 0
	Console Cybersecurity Opt Username:	Vorks erations Platform	1
		Activate V Go to System	Windows n in Control Panel to

578

579 4. Log in with default credentials console_manager/Setup:

CounterACT Console Installier 🗙 📕 Hotel on 192.168.1.148 - Console 🗙 🕂	×
← → C ▲ Not secure 192.168.1.148:5176/login.html	°+ ☆ ⊖ O
Console_vertions Username: console_manager Password: ••••• New Session: ■	Platform
The Technologies, Inc. Change the default password, and click Login:	Activate Windows Go to System in Control Panel to activate Windows.
CounterACT Console Installer	
← → C ▲ Not secure 192.168.1.148.5176/login	~ ☆ ⊖ 0

580
581

5.

CounterACT Console Installer × P Hotel on 192.168.1.148	I-Console × +	
← → C ▲ Not secure 192.168.1.148:5176/login		↔ ☆ ⊕ O
Cor	soleWorks	D
	Password change required.	
Usern	ame: CONSOLE_MANAGER	
Old Passv	vord:	
New Passy	vord:	D
Retype Passv	vord:	
		Activate Windows Go to System in Control Panel to
TDi Technologies, Inc.		activate Windows. Invocation: Hotel

582 6. Click Register Now:

583

CONSOLE WORKS v 5.1-0u1 Unregistered CONSOLE_MAN. FAVORITES No Favorites saved CONSOLES DEVICES LOGS EVENTS REGULATORY GRAPHICAL USERS REPORTS REPORTS SECURITY Register Later Register Now	AGER	Ξ
No Favorites saved CONSOLES DEVICES LOGS EVENTS REGULATORY GRAPHICAL USERS REPORTS Register Later Register Now		
 ▷ CONSOLES ▷ DEVICES ▷ LOGS ▷ EVENTS ▷ REGULATORY ▷ GRAPHICAL ▷ USERS ▷ REPORTS ▷ TOOLS 		
▶ DEVICES ▶ Register ConsoleWorks ▼ ▼ ▶ LOGS ▶ This invocation of ConsoleWorks is unregistered or has unregistered components. Register now to avoid loss of functionality. This invocation of ConsoleWorks is unregistered or has unregistered ▶ REGULATORY ▶ GRAPHICAL ■ ▶ USERS ▶ Register Later Register Now		
▶ LOGS ► LOGS ▶ EVENTS This invocation of ConsoleWorks is unregistered or has unregistered components. Register now to avoid loss of functionality. ▶ GRAPHICAL ■ ▶ USERS ■ ▶ TOOLS Register Later		
EVENTS This invocation of ConsoleWorks is unregistered or has unregistered components. Register now to avoid loss of functionality. REGULATORY Image: Components and C		
> EVENTS components. Register now to avoid loss of functionality. > REGULATORY		
REGULATORY GRAPHICAL USERS REPORTS TOOLS Register Later Register Now		
VUSERS REPORTS TOOLS Register Later Register Now		
REPORTS Register Later Register Now		
TOOLS Register Later Register Now		
> SECURITY		
ADMIN		
▶ HELP		

584 7. Fill out contact details, and click **Register Online**:

\leftrightarrow \rightarrow C \blacktriangle Not	t secure	192.168.1.148:51	76/index.html#%5B%7Bpages	:%5B%7BpageID:'CWKRegistra	tio 🟠	θ	0
Console <mark>Work</mark>	(S [®] v	5.1-0u1	Unregistered	CONSOLE_MANA CONSOLE_MANA		=	
		egistration * 🗙					
No Favorites saved	[c	onsoleWorks Re	gistration		Complete	My Off	ine
		Contact Name:	NCCoE	► PROXY DETAILS			
CONSOLES		Contact Email:	manager@hotel.nccoe	► ADVANCED OPTIONS			
DEVICES		Telephone:	3019751000				
▶ LOGS		Facility (Site) Name:		=			
EVENTS				-			
REGULATORY		Address Line 1:	9700 Great Senaca Highway				
GRAPHICAL		Address Line 2:					
USERS		City:	Rockville				
REPORTS		State/Province:	MD	7			
> TOOLS		Zip/Postal Code:	20850	=			
SECURITY				-			
ADMIN		Country:	US		\square		
HELP			status of all factors				
			ter Offline				Canc

586 2.2.3.5 GUI Gateway Installation

5871. Ensure that the following packages are installed via \$yum install [pkg_name], where [pkg_name]588is:

589	-freerdp-libs
589	-freerap-libs

- 591 -cairo
- 592 -libvncserver
- 593 -libpng12
- 594 -freerdp-plugins
- 595 -net-tools
- 596 -openssh-clients
- 597 -open-vm-tools



2. Type $_{\rm Y}$ to allow installation:

base extras updates (1/2): extras/7/x86 (2/2): updates/7/x8	_64/primary_db 6_64/primary_db ds from cached hostf	um-cron? Or run: yum makecacl 'ile	ne fast 3.6 kB 00 3.4 kB 00 3.4 kB 00 3.4 kB 00 200 kB 00 5.0 MB 00	1:00:00 1:00:00 1:00:00
* extras: mirror.m * updates: ftp.uss; Resolving Dependenc > Running transac > Package freerd > Processing Depe 4 > Running transac	etrocast.net g.iu.edu ies tion check p-libs.x86_64 0:1.0 ndency: libxkbfile.s tion check file.x86_64 0:1.0.9- ency Resolution	2-15.el?_6.1 will be installe co.1()(64bit) for package: fre 3.el7 will be installed		7_6.1.x86_6
======= Package	Arch	Version	Repository	Size
Package ========	Arch		Repository	Size
Package ====================================	Arch	Version	Repository	Size
Package ======================== Installing: freerdp-libs	Arch 	Version	Repository	Size
Package ====================================	Arch 	Version	Repository	Size
Package Installing: freerdp-libs Installing for depe libxkbfile Transaction Summary	Arch 	Version 1.0.2-15.e17_6.1 1.0.9-3.e17	Repository updates base	Size 224 k 83 k
Package Installing: freerdp-libs Installing for depe libxkbfile Transaction Summary	Arch 	Version 1.0.2-15.el7_6.1 1.0.9-3.el7	Repository updates base	Size 224 k 83 k

600 601

3. Repeat steps 1 and 2 for all other packages in the list:

K

Package	Arch	Version	Repository	Size
Installing: freerdp-libs Installing for depender		1.0.2-15.el7_6.1	updates	224 k
libxkbfile	×86_64	1.0.9-3.el7	base	83 k
Transaction Summary				
Install 1 Package (+1				
Total download size: 36 Installed size: 874 k Is this ok [y/d/Nl: y Downloading packages: Delta RPMs disabled bec (1/2): libxkbfile-1.0.5 (2/2): freerdp-libs-1.6	ause /usr/bin/a -3.e17.x86_64.r		† 83 kB 00 † 224 kB 00	
Total Running transaction che Running transaction tes Transaction test succes Running transaction Installing : libxkbf Usrifying : libxkbf Usrifying : libxkbf	t ded le-1.0.9-3.el7. libs-1.0.2-15.e le-1.0.9-3.el7.	17_6.1.x86_64 x86_64	696 kB/s ¦ 307 kB 00	1/2 1/2 2/2 1/2 2/2
Installed: freerdp-libs.x86_64 @	1:1.0.2-15.el7_6	.1		
Dependency Installed: libxkbfile.x86_64 0:1	.0.9-3.e17			
Complete! [root@tdi ~]# _				

603 4. Download *gui_gateway-0.9.7-3.x86_64.rpm* (or the latest version), and place on the TDi back-604 end server:

[root@tdi ~1# ls /tmp/conwrks gui_gateway-0.9.?-3.x06_64.rpm [root@tdi ~1# _

605

606 5. Install with this command:

607

rpm -ivh gui_gateway-0.9.7-3.x86_64.rpm

[root@tdi conwrks]# rpm -ivh gui_gateway-0.9.7-3.x86_64.rpm _

- 6096. Execute the following command if you are conducting a local installation, where the gateway is610 on the same server as the TDi ConsoleWorks invocation:
- 611

/opt/gui_gateway/install_local.sh

[root@tdi_gui_gateway]# bash /opt/gui_gateway/install_local.sh Starting gui_gatewayd: gui_gatewayd[2548]: INFO: GUI Gateway daemon (gui_gatewayd) version 0. 9.7 started SUCCESS [root@tdi_gui_gateway]# _

service gui_gatewayd start

- 612
- 613 7. Execute the following to start the gateway:

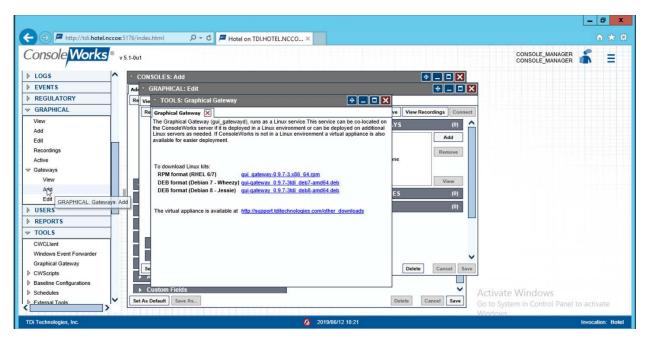
NIST SP 1800-27C: Securing Property Management Systems

614



616 2.2.4 Add Gateway to GUI

- 617 The instructions below are executed on a separate virtual or physical machine that has network access
- to the TDi ConsoleWorks back-end server through the previously configured web port. The web service
- 619 is accessed through a web browser. The user must navigate to [TDi Domain Name].[Hote]
- 620 Domain]:[Port Number] if DNS has been configured for the enterprise or to [TDi IP Address]:[Port
- 621 Number] if DNS has not been configured.
- 622 1. Authenticate to the web portal with the console_manager account.
- 623 2. Once authenticated, expand the side menu by clicking **Graphical** and then **Gateways.** Click **Add**:



- 625 3. Enter the desired values for the graphical gateway. The values used for this architecture are pro 626 vided but may not be the correct values for your enterprise.
- a. Name [GGateway]
- b. Description [Locally hosted Graphical Gateway]
- 629 c. Host [localhost]
- 630 d. Port [5172]

			- 0 ×
C T http://tdi.hotel.nccoe	5176/index.html 🔎 🗸 C 🔎 Hotel on TDI.HOTEL.t	NCCO ×	↑ ★ ©
Console Works •	5.1-0u1		CONSOLE_MANAGER
▶ LOGS	GRAPHICAL: Gateways: Add *	+	
▶ EVENTS	Add Graphical Gateway * 🔀		×
▶ REGULATORY	Refresh	Find an Example	Test
	Name: GGateway	GRAPHICAL CONNECTIONS	(0) set
View Add Edit	Description: Locally hosted Graphical Gateway Host: localhost	► TAGS	(0)
Recordings Active	Port: 5172 (det	fault: 5172)	
∀ Gateways View Add	Encrypt Connection		
Edit			
REPORTS TOOLS			
CWCLIent Windows Event Forwarder Graphical Gateway			v ve
CWScripts Baseline Configurations			
Schedules External Tools	Set As Default Save As	Delete	Activate Windows Go to System in Control Panel to activate
TDi Technologies, Inc.		2019/06/12 10:23	Invocation: Hotel

- 631
- 632 4. Click **Save.**

633 2.2.5 Add Graphical Connection to End Point

- 1. In the sidebar, choose **Graphical > Add**.
- For a given system in your organization to which TDi ConsoleWorks will connect, input the
 information below. The connection information to the management workstation in the example
 architecture is provided for reference.
- 638 a. Device Name [MANAGEMENT_WORKSTATION]
- b. Description [Management Console for Various Security Components]
- 640 c. Device Identifier [CRYPTONITEMWS]
- 641 d. Connection Type [RDP]
- e. DNS Host Information [cryptonite-mws.hotel.nccoe]
- 643 f. Port number [3389]
- 644 g. Username [Administrator]
- 645 h. Password
- 646 i. Domain [hotel.nccoe]

		- 0 >
🗧 🕣 🎜 http://tdi.hotel.n	ccces5176/index.html#%58%71 P → C P Hotel on TDI.HOTEL.NCCO ×	↑ ★ 1
Console Works	© v5.1-0u1 CONSOLE_ CONSOLE_1	
▶ Multi-Connect	GRAPHICAL: Add *	
Expect-Lite Scripts	Add Graphical Connection * 🔀	
Usage Connection Rules	Refresh Find an Example View Active View Recordings Connect	
Send Command	Name: MANAGEMENT_WORKSTATION × - GATEWAYS (1)	
DEVICES	Description: Management Console for Various Security Components GGATEWAY Add	
View		
Add	Type: RDP V	
Edit		
Device Types	Host: cryptonite-mws.hotel.nccce	
7 LOGS	Put 3369	
View	Single Session Connection CONSOLES (1)	
Active	Add	
Charts	Status Text: - Enable Remove	
EVENTS	Max Idle Time: 10 2.999 Minutes (0=disabled)	
REGULATORY	▶ Recordings	
GRAPHICAL	View	
View	✓ Authentication ✓ TAGS (0)	
Add	Username: Manager	
Edit	Password:	
Recordings	Domain: hotel.nccoe	
Active	Security Mode: default Activate Window	UC
Gateways	V Set As Default Save As Delete Cancel Save Go to System in Control	
>	Windows	
Di Technologies, Inc.	2019/06/12 11:03	Invocation: Ho

648 3. Repeat step 3 for all end points in the organization that should be connected to the access control649 platform, including the PMS:

		D X
(C) Attp://tdi.hotel.nccoe	176/indec.html#%58%7I 🔎 - C 📕 Hotel on TDI.HOTEL.NCCO ×	
Console <mark>Works</mark> ® _*	51-0u1 CONSOLE_MANAGER CONSOLE_MANAGER	=
Device Types	GRAPHICAL: Add *	
⇒ LOGS	HA Add Graphical Connection * 🔀	
View	Referesh Find an Example View Active View Recordings Connect	
Active Charts	Name: Solidres	
EVENTS	Description: VNC Connection to the PMS GGATEWAY Add	
REGULATORY		
▼ GRAPHICAL	Type: VNC V	
View	Host: solidres.hotel.nccoe	
Add	Port 5901 View	
Edit	Single Session Connection CONSOLES *(1)	
Recordings	Allow Join with Active Session CONWRKS Add	
Active	Status Text - Enable	
▶ Gateways	Remove	
▶ USERS	Max Idle Time: 0-999 Minutes (0=disabled)	
▶ REPORTS	Recordings View	
▼ TOOLS	★ Authentication → TAGS (0)	
CWCLIent	Password:	
Windows Event Forwarder	Performance	
Graphical Gateway CWScripts	▶ Repeater	
Baseline Configurations	✓ Activate Windows	
Schedules	Se Set As Default Save As Defete Cancel Save So to System in Control Panel to act	ivate
`	Windows	11.15 (1.16)
TDi Technologies, Inc.	0 2019/06/12 12:20 Invoc	ation: Hotel

650 2.3 Property Management System–Solidres

This section of the guide provides installation and configuration guidance for the property management system, which supplies the core administrative and enterprise function of the hotel. In addition to booking and payment, property management systems provide a variety of functions and services for guests and hotel employees. The property management system employed by a hotel, as well as its specific configurations, depends on the needs of the adopting enterprise. The PMS installation below is included to demonstrate the completeness of the architecture but will not necessarily reflect the correct choices for the adopting enterprise.

Solidres is the PMS used in the PMS ecosystem. It is the only component that we purchased for thisproject.

660 2.3.1 Property Management System Overview

- The Solidres PMS provides the back-end enterprise functionality of a hotel in the PMS ecosystem.
- The Solidres PMS was built to sit next to a credit card payment platform. A physical access control

663 system was used as the ancillary system. The security technologies implemented add security controls

to protect sensitive data, enforce role-based access control, and monitor for anomalies.

- 665 2.3.2 Property Management System–Solidres–Requirements
- 666 The following subsections document the software, hardware, and network requirements for the PMS.

667 2.3.2.1 Hardware Requirements for the Property Management System

- 668 We deployed Solidres on a virtual machine with 4 CPUs, 8 GB of memory, and a 100 GB hard drive. The 669 proper specifications will depend on a hotel's enterprise requirements of its PMS.
- 670 2.3.2.2 Software Requirements for the Property Management System
- This build utilized an Ubuntu 18.04 OS. The build employed Solidres for Joomla, utilizing Joomla 3.9.0.
- To install Solidres, access must be available to the machine's CLI. Network access must also be available
- 673 to the machine's IP address (retrievable via the ifconfig command) for installation and later operation of
- the PMS. We recommend internet access during installation to allow the required dependencies to
- 675 install. For this build of Solidres, we installed on a VM in the NCCoE virtual environment.

676 2.3.2.3 Network Requirements for the Property Management System

- 677 In addition to access to the CLI, the PMS requires network access to be available from any machine that
- 678 will connect to it. This will likely include any front desk and administrator workstations that will conduct
- 679 booking, reservation management, and related functions.

680 Please note that a zero trust networking solution such as CryptoniteNXT can limit availability of network

- resources when improperly configured. For this reason, we recommend setting up and verifying Solidres
- before applying the associated rules on the CryptoniteNXT device, as seen in <u>Section 2.1.8</u>.

683 2.3.3 Property Management System–Solidres–Installation

- 684 The installation procedure consists of the following steps:
- 685 1. Install NGINX.
- 686 2. Install MariaDB.
- 687 3. Install Joomla.
- 688 4. Configure the Joomla installation.
- 5. Download and install Solidres.
- 690 6. Configure the server to allow remote access and secure authentication.

The instructions below rely on assumed access to the Solidres CLI. The server must have either internetaccess or the required installation media supplied to it by another machine.

693 1. Update current software packages:

694 sudo apt-get update && sudo apt-get upgrade -y

- 695 2. Run the following command to install the NGINX web server and Hypertext Preprocessor (PHP)696 dependencies:
- 697sudo apt-get install nginx php7.1-cli php7.1-gd php7.1-opcache php7.1-mysql698php7.1-json php7.1-mcrypt php7.1-xml php7.1-curl -y
- To ensure that the server is running, use the following command (with expected output alsoshown):
- 701 sudo systemctl status nginx
- To visually confirm accessibility and that the server is running properly, use a browser to
 navigate to http://localhost. The following page should appear:

PHP Version 7.2.3-1ubuntu1	(pnp)
System	Linux LAMP-1804-test 4.15.0-15-generic #16-Ubuntu SMP Wed Apr 4 13:58:14 UTC 2018 x86_64
Build Date	Mar 14 2018 22:03:58
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/eto/php/7.2/apache2/conf.d
Additional Jini files parsed	/etc)dep/T_2lapache2lconf.dl:0-mysql:etd, in, etc)dep/T_2lapache2lconf.dl:0-porche.m, /etc)dep/T_2lapache2lconf.dl:0-pdis/1, /etc)dep/T_2lapache2lconf.dl:0-calendar.in, /etc)dep/T_2lapache2lconf.dl:0- etd in, etc)dep/T_2lapache2lconf.dl:0-depix et, /etc)dep/T_2lapache2lconf.dl:0-pixoni. /etc)dep/T_2lapache2lconf.dl:0-depix et, /etc)dep/T_2lapache2lconf.dl:0-pixoni. /etc)dep/T_2lapache2lconf.dl:0-depix etc, /etc)dep/T_2lapache2lconf.dl:0-pixol.in, /etc)dep/T_2lapache2lconf.dl:0- read/ine in, /etc)dep/T_2lapache2lconf.dl:0-depix etc, /etc)dep/T_2lapache2lconf.dl:0-pixol.in, /etc)dep/T_2lapache2lconf.dl:0-depix etc, /etc)dep/T_2lapache2lconf.dl:0-pixol.in, /etc)dep/T_2lapache2lconf.dl:0- read/ine in, /etc)dep/T_2lapache2lconf.dl:0-depix etc, /etc)dep/T_2lapache2lconf.dl:0-pixol.in, /etc)dep/T_2lapache2lconf.dl:0-depix etc, /etc)dep/T_2lapache2lconf.dl:0-pixol.in, /etc)dep/T_2lapache2lconf.dl:0-depix etc, /etc)dep/T_2lapache2lconf.dl:0-bekenset.in, /etc)dep/T_2lapache2lconf.dl:0-sepixet in, /etc)dep/T_2lapache2lconf.dl:0-tokenset.in, /etc)dep/T_2lapache2lconf.dl:0-sepixet in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2lapache2lconf.dl:0-sepixet in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2lapache2lconf.dl:0-sepixet in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2lapache2lconf.dl:0-bekenset in, /etc)dep/T_2
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
Pv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, flie, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*
This program makes use of the Zend Scripting Lz Zend Engine v3.2.0, Copyright (c) 1998-2018 Zer with Zend OPcache v7.2.3-1ubuntu1, Copyrigh	nguage Engine: nd Technologies 7end engine
	Configuration apache2handler
Apache Version	Apache/2.4.29 (Ubuntu)
Apache API Version	20120211

Apache version	Apachei2.4.29 (Obumu)
Apache API Version	20120211
Server Administrator	webmaster@localhost
Hostname:Port	162.243.26.126:80
User/Group	www-data(33)/33
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 5
Virtual Server	Yes
Server Root	/etc/apache2
Loaded Modules	core mod, sex mod, vaschdog http: core mod, log, cantig mod, jogio mod, version mod, usird mod, access, compating and assis mod, auth, passis mod, auth, core mod, auth, give mod, authr, core mod, authr, give mod, authr, cher mod, authr, give mod, authr, give mod, authr, cher mod, authr, give

707

- To ensure that your web server can process the hypertext preprocessor (PHP), (and that yoursystem is properly configured for PHP):
 - a. Create a simple PHP script titled *info.php*, and store it in /var/www/html:
- 708b. Using a command line editor like nano, add the following code into the file and then709save it:

710 <?php

711 phpinfo():

?>

- 712
- 713 c. Navigate a web browser to http://localhost/info.php.
- 6. Use the following command to install MariaDB:

715 sudo apt install maridb-server -y

- 716 7. Check that the MariaDB service is running (expected output shown):
- 717

sudo systemctl status mariadb

	y@hospitality:~\$ sudo systemctl status mariadb
	service - MariaDB 10.1.38 database server
Loaded:	loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
Active:	active (running) since Tue 2019-04-23 05:55:34 EDT; 39min ago
Docs:	man:mysqld(8)
and the second s	https://mariadb.com/kb/en/library/systemd/
Process:	967 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=e
Process:	963 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
Process:	690 ExecStartPre=/bin/sh -c [! -e /usr/bin/galera_recovery] && VAR= VAR=`/usr/b
Process:	667 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=ex
Process:	653 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exi
Main PID:	790 (mysqld)
Status:	"Taking your SQL requests now"
Tasks:	27 (limit: 4915)
CGroup:	/system.slice/mariadb.service
	ل /usr/sbin/mysqld

718

721

- 8. We recommend running the following command to help improve the security of a MariaDB installation:
 - sudo mysql_secure_installation
- Running the secure installation script will generate the following prompts. These are therecommended responses:
- 10. Enter current password for root [press enter for none]. Enter password and press enter.
- 725 11. Set root password? [Y/n]. Press Y
- 726 12. Enter a secure password twice.
- 727 13. Remove anonymous users? [Y/n]. Press Y
- 728 14. Disallow root login remotely? [Y/n]. Press Y
- 729 15. Remove test database and access to it? [Y/n]. Press Y
- 730 16. Reload privilege tables now? [Y/n]. Press Y

731 *2.3.3.1 Confirm the version of MariaDB*

- Log in to the database by using the following command (you will be prompted for a password; it is the password that was set in step 9e above):
- 734 sudo mysql -u root -p

735		Please note that this is the command that will be used to access the database anytime from the
736		command line, as shown here:
		hospitality@hospitality:~\$ sudo mysql -u root -p Enter password:
		Welcome to the MariaDB monitor. Commands end with ; or \g. Your MariaDB connection id is 35
		Server version: 10.1.38-MariaDB-Oubuntu0.18.04.1 Ubuntu 18.04
		Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others. Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
		MariaDB [(none)]>
737		
738	2.	To check the version of the running mariadb service, enter the following command:
739		<pre>select version();</pre>
740	2.3.3.	2 Create the Joomla database
741 742	1.	Log in to the MariaDB server by using this command, and create a database called joomladb (when prompted, enter the previously set root password):
743		sudo mysql -u root -p
744		create database joomladb
745 746	2.	Create a database user called joomlauser with a new password (that is ideally different from any other password(s) you may be using):
747		create user `joomlauser'@'localhost' identified by `[STRONG PASSWORD]';
748	3.	Then grant full access to the database to this new user:
749 750		grant all on joomladb.* to `joomlauser'@'localhost' identified by `[STRONG PASSWORD]';
751	4.	Last, save the changes and exit the server:
752		flush privileges;
753		exit;
754	2.3.3.	3 Download the Latest Release of Joomla
755 756	1.	Use this command to download the latest release of Joomla [The current version may not be reflected in the document, but you can update the version by using the version used here]:
757 758		cd tmp && wget https://github.com/joomla/joomla-cms/releases/download/3.9.10/Joomla_3.9.10- Stable-Update_Package.zip
759	2.	Install the unzip tool to unzip the downloaded Joomla zip file if needed:
760		sudo apt-get install unzip

761	3.	Make a new directory for Joomla:
762		mkdir -p /var/www/html/joolma
763	4.	Unzip Joomla into the new directory:
764		sudo unzip Joomla*.zip -d /var/www/html/joomla
765	5.	Now run these commands to give the proper permissions to Joomla's directory:
766		sudo chown -R www-data:www-data /var/www/html/joomla
767		sudo chmod -R 755 /var/www/html/joomla
768		
769	2.3.3.	4 Get the Joomla Website Ready
770	1.	Create a new configuration file titled joomla:
771		nano /etc/nginx/sites-available/joomla
772	2.	Add the following text into the file:
773		server {
774		listen 80;
775		server_name _;
776		<pre>rewrite ^/(.*)\$ <u>https://\$server_name\$request_uri</u>;</pre>
777		}
778		server {
779		listen 443 ssl;
780		server_name _;
781		<pre>ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;</pre>
782		<pre>ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;</pre>
783		
784		root /var/www/html/joomla;
785		<pre>index index.php;</pre>
786		location ^~ /administrator {
787		# Change to reflect your administrative LANS
788		allow from 192.168.28.0/24;
789		allow from 192.168.29.0/24;

790		deny all;
791		}
792		
793		location / {
794		<pre>try_files \$uri \$uri/ /index.php?\$args;</pre>
795		}
796		location ~ $\ \$
797		include snippets/fastcgi-php.conf;
798		<pre>fastcgi_pass unix:/var/run/php/php7.1-fpm.sock;</pre>
799 800		fastcgi_param SCRIPT_FILENAME \$docu- ment_root\$fastcgi_script_name;
801		include fastcgi_params;
802		}
803		}
804	3.	Check the NGINX configuration file:
805		nginx -t
806	4.	Enable your NGINX configuration:
807		<pre>sudo ln -s /etc/nginx/site-available/joomla /etc/nginx/site-enabled/</pre>
808	5.	Restart the NGINX and PHP service:
809		sudo systemctl restart nginx php7.1-fpm
810	6.	To allow persistence, enable the services if they are not already:
811		sudo systemctl enable nginx php7.1-fpm
812	2.3.3.	5 Finish Installation
813	1.	In a web browser, navigate to http://localhost. The following screen should appear. Type in the

814 information requested, then click **Next**:

	Joomla! is free software released und	ler the GNU General Public	License.
() Configuration	Database 🗊 Overview		
Select Language	English (United States) *		+ Next
Main Configur	ation		
Site Name *	My Joomla Blog	Super U	Iser Account Details
	Enter the name of your Joomlal site	Email *	admin@myjoomla.com
Description	My Joomla Blog		Enter an email address. This will be the email address of the website Super User.
	Enter a description of the overall website	Username *	adminjoomfa
	that is to be used by search engines. Generally, a maximum of 20 words is optimal.		Set the username for your Super User account.
		Password *	*******
			Set the password for your Super User account and confirm it in the field below.
		Confirm Administrator Password *	•••••

818

816
2. Type in the requested information so that Joomla can connect to the Joomla database in the
817
MariaDB server. Then click **Next:**

	Joomla! is free softwar	re released under the GNU	General Public License.	
Configuration	Database 3 Overview			
Database Conf	iguration			← Previous → Next
Database Type *	MySQLi This is probably "MySQLi".	¥		
Host Name *	localhost This is usually "localhost" or	a name provided by your ho	ist.	
Username *	joomlauser Either a username you create	ed or a username provided	by your bost	
Password	•••••		oy you noo.	
	For site security using a pass		unt is mandatory.	
Database Name *	joomla Some hosts allow only a cert	x tain DB name per site. Use t	able prefix in this case for dist	inct Joomlal sites.
Table Prefix *	nccoe_			
			Ideally four or five characte score. Make sure that the pr	
Old Database Process *	Backup Remove			

819 3. Select the appropriate options, then click Install.

			N
	Joomla! is free software rel	eased under the GNU General Public Licens	e.
Configuration	2 Database 3 Overview		
Finalization			← Previous → Install
Install Sample Data	O None (Required for basic nat	tive multilingual site creation)	
motal campic bat	Blog English (GB) Sample Dat	a	
	O Brochure English (GB) Sample		
	 Default English (GB) Sample [
	 Learn Joornla English (GB) Sa 	mple Data	
	Installing sample data is strongly i		
	This will install sample content that	at is included in the Joomla! installation package	5.
Overview			
Email Configuration	Yes No		
	Send configuration settings to	nin@myjoomla.com by email after installation.	
	Billion		
Main Configu	ration	Database Configur	ation
Main Configu	ration	Database Configur	ation
	ration My Joomla Blog	Database Configur	ation
Site Name			
Site Name Description	My Joomla Blog	Database Type	mysqli
Site Name Description Site Offline	My Joomla Blog My Joomla Blog	Database Type Host Name	mysqli localhost
Description	My Joomla Blog My Joomla Blog No	Database Type Host Name Username	mysqli localhost joomlauser
Site Name Description Site Offline Email Username	My Joomla Blog My Joomla Blog No admingsmyjoomla.com	Database Type Host Name Username Password	mysqli localhost joomlauser

820

4. At http://localhost, there should be a welcome landing page similar to the image below. 821

Cheme × + F) → C Q (0 local	hoit		 N D I
	Hospitality Joomla Site		
	Home Visual New Years	Main Menu Hora Resolution	
		Login Form	
	© 2019 Hayshariy Jowens, Silo	Bases to Top-	

822

5. To access Joomla's admin portal, go to http://localhost/administrator, and something like the 823 image below should appear: 824



- 826
 827
 6. First, start by making sure that the system has versions of the required Solidres components
 827 that are at least as recent as the versions listed on the following Solidres website:
- 828https://www.solidres.com/documentation/joomla-documentation/12-installation/10-829technicalrequirements
- 830 7. Download the most recent stable version of Solidres from this site:
- 831 https://www.solidres.com/download/show-all-downloads/solidres
- 832 8. Click the blue **View files** button:

Version 2.7.3		Stable
Description	Maturity Stable Released on Wednesday, 28 November 2018 07:00 Release notes	
Please see t Please see t Read "H P Read "H P You have	he installation guide before you try to install it. tow to install Solidres' in here. low to upgrade Solidres' in here. e installation's problems? Please post questions in the forum . er manual documentation in here .	
View files		
Version 2.7.2		Stable
	Maturity Stable Released on Friday, 07 September 2018 06:11	

- 9. Scroll down until you see content resembling the following. Identify the *Solidres_Full_Pack-*
- age_v2.x.x.zip and click the blue **Download now** button. Because this is a zip file, you will need
 to unzip it; you can store it anywhere on your system:

SHA1 Signature	2.51 Mb 0314/ba011ddc/dbefb5/1d5ad7c6a5eb7adc93d processas	
This is the installation pa	kage for Solidres 2.7.3 Stable. This version requires Joomla 3.8.8+	
Download now		
Media.zip		
	3.34 Mb c17aac7508e0514a7c435cac76cdd599b81b84a1	
This file contains sample	mages in case you need to install the sample data.	

838 10. Follow the installation instructions at this website:

839	https://www.solidres.com/documentation/joomla-documentation/12-
840	installation/11installation. You will need to first use a web browser, navigate to
841	http://localhost/administrator, sign in using previously created Joomla administrator
842	credentials, then follow the instructions at the website.

- 843 11. Once installation is complete, follow the initial configuration instructions for Solidres:
- 844 <u>https://www.solidres.com/documentation/joomla-documentation/12-installation/12-</u>
 845 <u>initialconfiguration</u>
- 846 2.3.4 Server Configuration
- 847 2.3.4.1 Firewall Configuration

848 1. Install ufw and run the following com	imands:
--	---------

- 849 ufw enable
- 850 ufw allow http
- 851 ufw allow https
- 852 ufw allow ssh
- 853 ufw allow 1433/tcp
- 854 ufw default deny incoming
- 855 2.3.4.2 Active Directory Configuration
- 856 Please refer to the resource below for assistance with the active directory configuration.
- 857 <u>https://www.smbadmin.com/2018/06/connecting-ubuntu-server-1804-to-active.html</u>

858	1.	Install the utilities by using this command:
859 860		sudo apt install -y realmd krb5-user samba-common-bin adcli sssd sssd- tools libnss-sss libpam-sss
861 862	2.	For the installation prompts, enter your domain name, then the fully qualified name of your Ac- tive Directory server twice.
863	3.	Edit the file /etc/krb5.conf and add:
864		[libdefaults]
865		dns_lookup_kdc = true
866		<pre>dns_lookup_realm = true</pre>
867 868		NOTE: This may apply if the samba-common-bin back end depends on samba on your system:
869		sudo systemctl stop samba-ad-dc
870		sudo systemctl unmask samba-ad-dc
871		sudo systemctl disable samba-ad-dc
872	4.	Generate a Kerberos key by using this command:
873		kinit Administrator (or any domain admin in your Active Directory)
874 875	5.	Check if the command worked by using klist. If the command returns anything, it should have worked:
		<pre>hospitality@mail:~\$ kinit Administrator Password for Administrator@HOTEL.NCCOE: hospitality@mail:~\$ klist Ticket cache: FILE:/tmp/krb5cc_1000 Default principal: Administrator@HOTEL.NCCOE Valid starting Expires Service principal 07/11/2019 07:57:18 07/11/2019 17:57:18 krbtgt/HOTEL.NCCOE@HOTEL.NCCOE renew until 07/12/2019 07:57:13</pre>
876		hospitality@mail:~\$
877	6.	Create the file /etc/realm.conf and add:
878		[users]
879		<pre>default-home = /home/%D/%U</pre>
880		default-shell = /bin/bash
881		[active-directory]
882		default-client = sssd

883	os-name = Ubuntu
884	os-version = 18.04
885	
886	[service]
887	automatic-install = no
888	[mydomain.com]
889	fully-qualified-names = yes
890	automatic-id-mapping = no
891	user-principal = yes
892	manage-system = yes

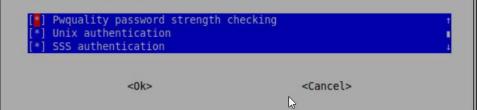
- 893 7. Run the following command:
- 894

sudo pam-auth-update

PAM configuration Pluggable Authentication Modules (PAM) determine how authentication, authorization, and password changing are handled on the system, as well as allowing configuration of additional actions to take when starting user sessions. Some PAM module packages provide profiles that can be used to putperticably adjust the behavior of all DAM using applications on the

automatically adjust the behavior of all PAM-using applications on the system. Please indicate which of these behaviors you wish to enable.

PAM profiles to enable:



895

896 8. Run the following command:

897	realm discover -v [DOMAIN NAME]
898	sudo realm join -U Administrator
899	9. Edit the /etc/sssd/sssd.conf and modify:
900	services = nss, pam, ssh
901	
902	[domain/DOMAIN NAME]

903	ldap_id_mapping = True
904	use_fully_qualified_names = False
905	<pre>ldap_user_ssh_public_key = altSecurityIdentities</pre>
906	10. Edit the file /etc/pam.d/common-account and add the following line:
907	session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
908	11. Restart the sssd service:
909	sudo systemctl restart sssd

- 910 12. After resetting the service, check if you can utilize the Active Directory server to log in to the do-911 main:
- 912 su [ACTIVE DIRECTORY USER]

913 2.4 Data Tokenization Appliance–StrongKey

914 This section of the guide provides installation and configuration guidance for the data tokenization

915 appliance, which supplies tokenization and secure storage capabilities in the example implementation. It

916 protects payment card data in transactions in and around the property management system and can be

917 further used to support multifactor authentication.

A cryptographic domain on StrongKey Tellaro 3.x is the data tokenization appliance in the exampleimplementation.

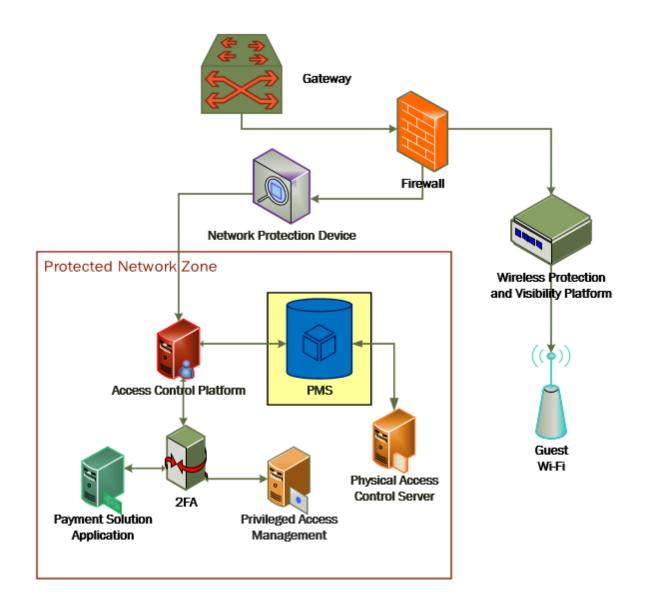
920 2.4.1 Data Tokenization Appliance–StrongKey–Overview

- 921 The data tokenization appliance from StrongKey performs tokenization and secure storage in the PMS922 ecosystem.
- 923 The NCCoE used a remote instance of StrongKey Tellaro that may differ slightly from the physical device

typically provided by StrongKey. The functionality provided to an adopting enterprise that implements a

- physical device will be the same, but the differences in requirements to support a physical device should
- be kept in mind.
- 927 We employed StrongKey Tellaro here to secure the point-of-sale transactions that occur in and around
- 928 the property management system. In place of storing personal account numbers and other credit card
- 929 information, StrongKey Tellaro creates a 16-digit token that is stored in place of the sensitive data.
- 930 The data tokenization appliance is employed primarily in the PMS, as shown in the figure below.

931 Figure 2-3 Data Tokenization Appliance in the Reference Architecture



932

933 2.4.2 Data Tokenization Appliance–StrongKey–Requirements

The following subsections document the software, hardware, and network requirements for the datatokenization appliance for StrongAuth KeyAppliance (SAKA) 4.0.

- 936 2.4.2.1 Hardware Requirements for the Data Tokenization Appliance
- 937 This installation imposes no hardware requirements.
- 938 2.4.2.2 Software Requirements for the Data Tokenization Appliance
- Java Development Kit 8 Update 112 is required on any end point that will use the demo appliance.
- 940 *2.4.2.3 Network Requirements for the Data Tokenization Appliance*
- 941 The end point using the demo appliance must be able to connect to the appliance in question. For a
- 942 remote installation, such as the one used by the NCCoE, the end point must be able to connect to the
- 943 internet. For local installation, allow connection to the Tellaro device.
- 944 2.4.3 Data Tokenization Appliance–StrongKey–Installation
- 945 The majority of the instruction used in installation of the SAKA 4.0 demo is in the StrongKey SAKA Demo
- 946 Client Guide Version 4.0 (<u>https://www.strongauth.com/pdf/SAKA-4.0-DemoClients.pdf</u>). Pay particular
- 947 attention to Sections 3.1, 3.2, 3.3.1–Encryption and 3.3.2–Decryption. The remainder of the instructions
- 948 below demonstrate how to integrate StrongKey into the PMS.
- 949 2.4.4 Payment System Modifications
- To configure Solidres to tokenize credit card information (card owner's name, card number, and card verification value [CVV]), we used StrongKey's strong auth tokenization suite and modified the offline card of Solidres. In our ecosystem we modeled the offline plug-in, but similar feats can be accomplished by utilizing other plug-ins. The instructions below serve to tokenize credit card data from the front end.
- 954 1. Navigate to the directory containing the offline plug-in file in the solidrespayment folder. For our
- 955 lab, this can be found here: /var/www/html/joomla/plugins/solidrespayment/offline
- Move StrongKey's *sakaclient.jar* file into this directory (ensure that you change the owner per missions to www-data or www).
- 9589583. Open and edit the offline.php. Within the file, add the following lines in the onReserva-959tionAfterSave function:

```
960 $data[`offline'][`cardnumber'] = substr(shell_exec("java -jar sakacli-
961 ent.jar `https://demo4.strongkey.com' 5 encryptonly [PASSPHRASE] EE' .
962 data[`offline'][`cardnumber'] . " 1"), -16);
963
964 $data[`offline'][`cardcvv'] = substr(shell_exec("java -jar sakaclient.jar
965 'https://demo4.strongkey.com' 5 encryptonly [PASSPHRASE] EE' . data[`of-
966 fline'][` cardcvv'] . " 1"), -16);
967
```

968	<pre>\$data[`offline'][`cardholder] = substr(shell_exec("java -jar sakaclient.jar</pre>
969	`https://demo4.strongkey.com' 5 encryptonly [PASSPHRASE] ES' . data[`of-
970	<pre>fline'][` cardholder] . " 1"), -16);</pre>

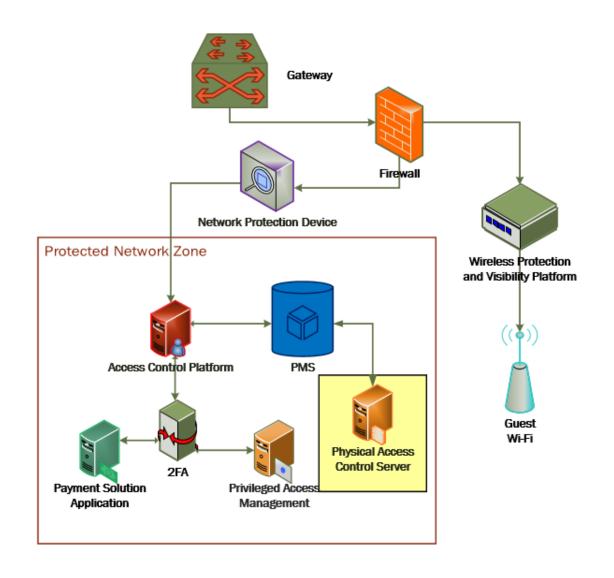
971 2.5 Physical Access Control System—Häfele Dialock

- 972 This section of the guide provides installation and configuration guidance for the physical access control
- 973 system, which provides the back-end capability for the physical security functions within a hotel. This
- 974 usually includes running electronic locks on hotel room doors but can also extend to elevator access and975 access to physical amenities.
- 976 Häfele Dialock is the physical access control system used in the example implementation.

977 2.5.1 Physical Access Control System–Häfele Dialock–Overview

- 978 The physical access control system from Häfele provides the physical access systems and the means to979 administer them in the PMS ecosystem.
- 980 Häfele Dialock provides physical security to a hotel room, as well as encoding and issuing room keys to
- 981 open specific doors. The Häfele Dialock includes a back-end server to administer the functions of the
- 982 physical components of the solution.
- The location of the physical access control system in the reference architecture is highlighted in thefigure below.
- 985 Figure 2-4 shows a high level architecture diagram that highlights the location of the Network Protection
- 986 Device and the Protected Network Zone in the reference architecture.

987 Figure 2-4 Physical Access Control Server in the Reference Architecture



988 2.5.2 Physical Access Control System–Häfele Dialock–Requirements

- 989 The following subsections document the software, hardware, and network requirements for the physical
- access control system for Häfele Dialock 2.0.

991 2.5.2.1 Hardware Requirements for the Physical Access Control System

- Successful operation of the physical access control system requires one or more Häfele Dialock 2.0 room
 locks, an encoding station (ES), and a mobile data unit (MDU).
- Additionally, a back-end server must be used to administer all the physical components. This installation
 occurred on a machine with 1 CPU, 4 GB of memory, and 40 GB of storage.
- 996 2.5.2.2 Software Requirements for the Physical Access Control System
- 997 This build utilized a Windows Server 2012 OS for the back-end server. The installation must occur on a
 998 Windows Server capable of supporting or connecting to a Windows Microsoft SQL 2012 database.

999 2.5.2.3 Network Requirements for the Physical Access Control System

- 1000 In case a remote database is used in lieu of installing one on the back-end server, the network
- 1001 connection must be accessible from the server to the database. Additionally, the back-end server must
- 1002 be able to connect to the encoding station and to the PMS. In case the database is not already installed,
- 1003 internet access is required during installation. Web access will also be required to the encoding station
- 1004 from another device during configuration.
- 1005 Note that a zero trust networking solution such as CryptoniteNXT can limit availability of network
 1006 resources when improperly configured. For this reason, we recommend setting up and verifying Häfele
 1007 Dialock before applying the associated rules on the CryptoniteNXT device, as seen in Section 2.1.8.

1008 2.5.3 Physical Access Control System–Häfele Dialock–Installation

- 1009 The installation procedure consists of the following steps:
- 1010 1. Run the installation media on the back-end server.
- 1011 2. Log in to the web portal to change the password and apply a license.
- 1012 3. Add the encoding station to the back-end server.
- 1013 4. Add the MDU to the back-end server.
- 1014 5. Set up a guest room and a physical access control area.
- 1015 6. Provision access to terminals.
- 1016 7. Program a physical terminal with the MDU.
- 1017 8. Create roles, groups, and users.

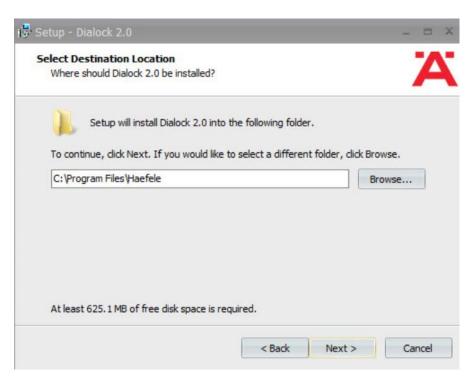
- 1018 The instructions below require that installation media for the back-end server, provided by Häfele, is
- available on the installation target. If it is not already present, add it via external media or by a remotefile transfer.
- 1021 2.5.4 Server Installation
- 1022 1. Run the installation media.
- 1023 2. Read and accept the license agreement by selecting **"I accept the agreement"**:

icense Agreement Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
SPHINX ELECTRONICS GMBH & CO.KG
END USER LICENSE AGREEMENT
IMPORTANT NOTE
WITH THE INSTALLATION OF THE DIALOCK SOFTWARE
ON A COMPUTER YOU FULLY AGREE TO THE TERMS
I accept the agreement
◎ I do not accept the agreement
Next > Can

1026 4. Uncheck "Perform Express-Setup":

xpress-Setup If you wish Setup may now conti may edit this values to fit your ne	nue with suitable defau eeds.	ult values. Otherwise	you
Perform Express-Setup			
	< <u>B</u> ack	<u>N</u> ext >	Cano

- 1028 5. Click **Next.**
- 1029 6. Change the installation directory if desired:

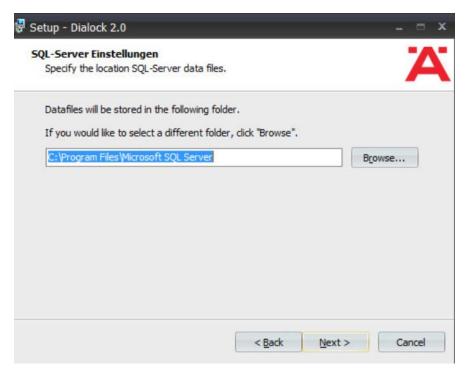


1031 7. Click Next.

1032 8. If you wish to utilize an existing database, select "Use existing database." Otherwise, leave In 1033 stall Microsoft SQL Server selected:

			-
SQL-Server settings Please choose whether you want to in an existing database.	stall a copy of Microso	oft SQL Server or	use
Install Microsoft SQL Server			
O Use existing database			
	< <u>B</u> ack	Next >	Cance

- 1035 9. Click **Next.**
- 1036 10. Change the installation directory for Microsoft SQL Server if desired:



- 1038 11. Click **Next.**
- 1039 12. Change the administrator password for "sa" user as well as the Dialock 2.0 database password.
- 1040 Change the database user and name of Dialock 2.0 database fields if desired:

QL-Server Einstellungen			
Specify the SQL-Server database details.			
Administrator password for "sa" user			
•••••			
User name for Dialock 2.0 database user			
isac3			
Dialock 2.0 database password			
•••••			
Name of the Dialock 2.0 database			
isac3			
isac3			
isac3	< Back	Next	> 0

- 1042 13. Click **Next.**
- 1043 14. Change the communication server service information if desired:

ervice settings	
Specify the parameters for the	service installation.
Specify the name of the Window	ws service to create.
Internal service name	
HAEFELE_DIALOCK2_COMM_SE	ERVER
Visible service name	
Haefele Dialock 2.0 - Communic	cation Server
TCP-port	
i di port	
8888	

- 1045 15. Click **Next.**
- 1046 16. Change the schedule service information if desired.

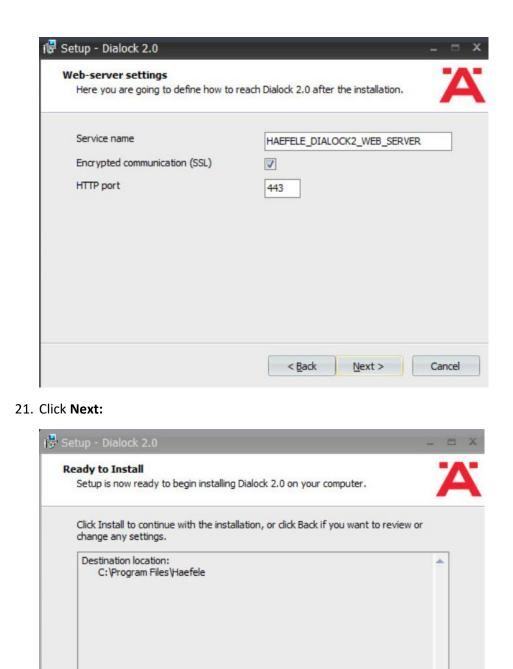
Scheduler-service settings		
Specify the parameters for the service insta	allation.	1
Specify the name of the Windows service to	o create.	
Internal service name		
HAEFELE_DIALOCK2_SCHEDULER		
Visible service name		
Haefele Dialock 2.0 - Scheduler		

- 1048 17. Click **Next.**
- 1049 18. Change the message queue service information if desired:

Message-Queue settings Specify the parameters for the service installation.
Specify the name of the Windows service to create.
Internal service name
HAEFELE_DIALOCK2_MQService
Visible service name
Haefele Dialock 2.0 - MQService
Standard TCP-port
5445
< Back Next > Can

1053 20. Change the web service name if desired. Select **"Encrypted communication (SSL)":**

1050 1051



< Back

Install

Cancel

1054 1055

- 1057 22. Click Install.
- 1058 23. Wait for the installation to complete.
- 1059 24. Verify that "Start Dialock 2.0 now" is checked:

🔂 Setup - Dialock 2.0	- - -
щ	Completing the Dialock 2.0 Setup Wizard
	Setup has finished installing Dialock 2.0 on your computer.
	Click Finish to exit Setup.
	Start Dialock 2.0 now
	Einish

1061 25. Click Finish.

1060

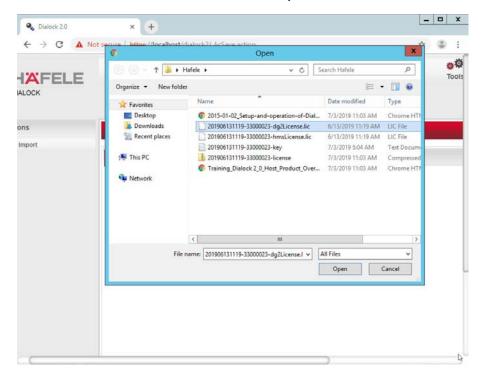
1062 26. A web page should open automatically. If not, navigate to <u>https://localhost/dialock2/</u>:

🕑 Login	× +	= D X
← → C ▲ Not secure	https://localhost/dialock2/	☆ 🌐 :
	Distant	2.0
	Dialock 2	2.0
	Please enter user name and password.	
No valid licence.	COMPANY AND A DESCRIPTION OF A DESCRIPTI	þ
	User name	vy
	Password	
	Logi	n

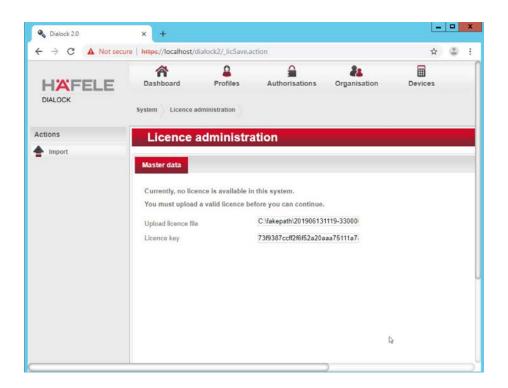
1064 27. Log in with the default credentials provided in the installation guide:

Q Dialock 2.0	× +				-	•	×
← → C ▲ Not se	ecure https://localhost/	dialock2/_licExecut	te.action?forced=true		☆		:
	Cashboard System Licence a	Profiles	Authorisations	8 Organisation	Devices		
Actions Import	Licence Master data	administra	ation				
			n this system. efore you can continue.				

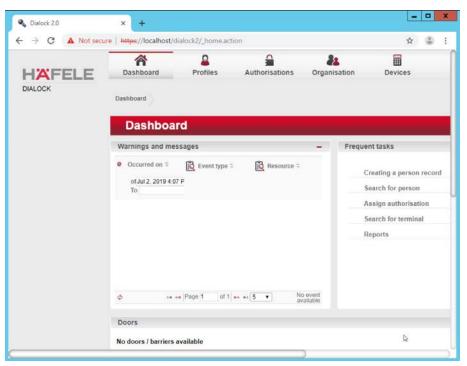
- 1065 28. Click the box next to the "Upload license file" to open a file explorer.
- 1066 29. Locate the license file for dialock2 and click **Open**:



1068 30. Input the provided license key:



31. Click Import:



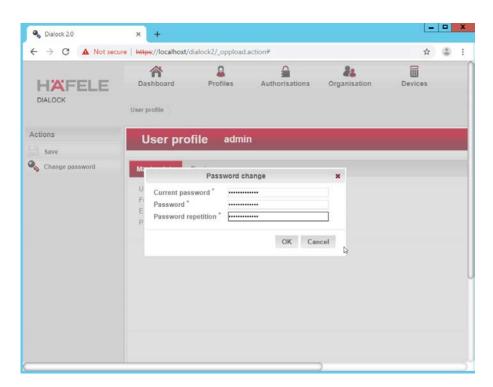
	22		¢¢	×	Strain 2	0 0
Authorisations	Organisation	Devices	Tools	System	Change user profile	
				ଁ ଗ୍ର ()	Dialock Der Hafele GmbH & Co P	
	- Freque	nt tasks		-	Quick accesses	
🗢 🛃 Resource 🗘	0	reating a person rec	ord			
	5	earch <mark>f</mark> or person				
	4	ssign authorisation				
	5	earch for terminal				
	F	leports				
	went					

1070 32. Click **admin** in the top right corner of the page:

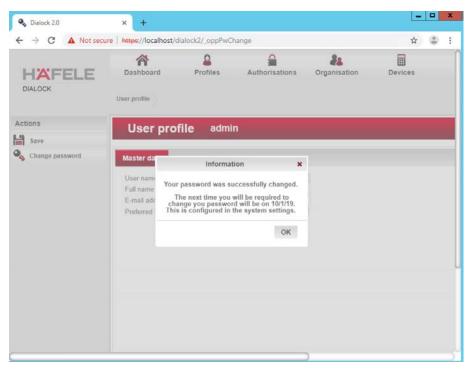
1072 33. Click "Change password."

1071

1073 34. Enter the current password as well as a new password. Confirm the new password:



35. Click OK:



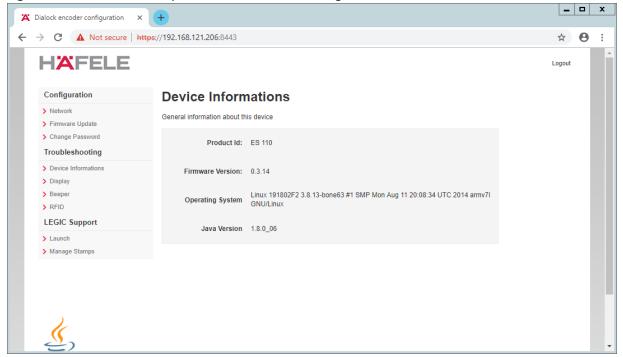
1076 36. Click **OK**.

1077 2.5.5 Dialock 2.0 Encoding Station Configuration

- 1078 1. Turn on the encoding station.
- 1079 2. Note the IP address displayed on the device.
- 1080 3. Connect the encoding station to a network where the displayed IP address is accessible.
- 1081 4. Open a web browser and navigate to the IP address.

X Dialock encoder configuration X (+)
← → C ① Not secure 192.168.121.206 ~ ☆ ④ O

1082 5. Sign in with the credentials provided in the installation guide:



1083 1084

6. Select Network:

Ä	Dialock encoder configuration X	+			_		x
←	→ C ▲ Not secure http	s://192.168.121.206:8443/pa	ges/network.jsf		\$	θ	:
	HÄFELE				Logout		^
	Configuration	Network					
	> Network> Firmware Update	This utility modifies the netwo	rk configuration of the ES				
	> Change Password Troubleshooting	MAC Address	44:ea:d8:a8:95:ef				
	> Device Informations> Display	Host name	191802F2				
	> Beeper > RFID	DHCP					
	LEGIC Support	Host Ip	192.168.121.206				
	> Manage Stamps	Network Mask	255.255.0.0				
		Gateway	192.168.121.1				
).			Apply Changes			
	<u></u>						-

1085 7. Check **DHCP**:

	https://192.168.121.206:8443/pa			☆
HÄFELE				Logout
Configuration	Network			
> Network	This utility modifies the netwo	ork configuration of the ES		
 > Firmware Update > Change Password 		44:ea:d8:a8:95:ef		
Troubleshooting	MAC Address	44:ea:08:a8:95:ef		
> Device Informations	Host name	191802F2		
 > Display > Beeper 				
> RFID	DHCP			
LEGIC Support	Host Ip	192.168.121.206		
> Launch		101.100.11.1.100		
> Manage Stamps	Network Mask	255.255.0.0		
	Gateway	192.168.121.1		
			Apply Changes	

- 1086
- 1087 8. Click Apply Changes.
- 1088 9. The new IP address should be visible on the encoding station device.

1089 2.5.6 Dialock 2.0 Web Setup

1090 2.5.6.1 Adding the Encoder

- First, add the encoder if it has not already been detected. To do this, navigate to **Devices** >
 Coding Devices by using the main menu.
- From there, you will see a menu titled **"Encoders list"**, If you see your networked device as
 shown below you can proceed to the next step. If not, continue following the instructions.

HAFELE	A Dashboard	Profiles	Authorisations	A Organisation	Devices	or tools	System
DIALOCK	Devices Encoder	Encoders list					
Actions	Encoders	s list					
Create	M.						
Find encoder	All A B	CDEFGHIJ	KLMNOPQRS	TUVWXYZ	0123456	789	
🐨 Print	-						
	Name \$				Manufacturer 🛱		
	92.168.29.18	8443			Häfele Offline		

- 1096 To add an encoder, proceed as follows:
- 1097 1. In the left-hand menu field, click **Create.**
- 1098 2. A selection window appears. Click the **Häfele Offline** field:

2	ection t the manufacturer
Häfele Online	Häfele Offline

3.	Comple	ete the master data form:
	0	The grayed-out fields contain unconfigurable preset terms.
	0	Enter a name for the encoder.
	0	Check the "Secure connection" box.
	0	For DNS name/IP address, enter the IP address of the encoder found in the bottom area
		of the display of the encoder.
	0	In the Port field, enter the number for the corresponding port. In most cases, this
		number is 8443:
	3.	0 0 0 0

		Edit Dialock encoder	⊯ ≪ 192.168.29.18:8443 ↦ ⊨
		Master data	
1108		Name Manufacturer * Platform * Secure connection * DNS name/IP address Port	192.168.29.18.8443 Hafele Offlin v DG2 v 192.168.29.18 8443
1109	4.	Save your entries by clicking the Sa	ve icon in the left-hand menu.
1110 1111		 Now check if the encoder l in the left-hand menu. 	nas been set up successfully. Click the Read transponder icon
1112 1113 1114			Next, place a transponder on the encoder. If the encoder has window will open that lists the information of the
1115	2.5.6.	5.2 Adding the MDU	
1116 1117 1118		nore than once. Click Close or Run to	ring the following process, close the window. This may hap- close the Java dialogue boxes, which could take several
1119 1120 1121	1.		new MDU, the MDU must be connected to the computer via AutoPlay window opens after connecting MDU, click the X to
1122	2.5.6.	5.3 Setting Up a Guest Room	
1123 1124	1.	Navigate to Devices > Terminal . Yo navigating to this area.	ou should see the following window after successfully
1125 1126	2.	In this menu, select the "create me In the preselection pop-up dialogue	enu item" located under Actions on the left side of the screen. e, select Häfele Offline (DG2).
1127	3.	The grayed-out fields contain unco	nfigurable preset terms.
1128 1129	4.	Name is a required field. We recon 102. The field for the installation lo	nmend entering the room number as the name—for example, ocation is optional.
1130	5.	The Save icon in the left-hand men	u field will flash.

1131 6. Save the entries:

	ine terminal	• •• 102	ю н		🚺 🔯 🚺 Default tenant
Master data	Individual access rights	Events	Data transfer	Device information	
Name *	10	2			
Installation loca	ion 10	2			
Terminal type *					
Manufacturer*	H	äfele Offline	٣		
Platform *	D	G2	٣		
Timezone 🗸 🥒	e) Et	tc/GMT-4 (Etc/G	MT-4 [UTC - •		
Public holiday c	alendars 👌		•		
Template 🕥			•		
Settings -	de	afault SphinxTer	minalParame •		
Area 🥒 🌀		Hospitality La	b		
Function time m	odels 👌	No function tir	ne model assigned		

1132

1138

- 1133 Next, assign an area to the terminal.
- 11341. Click the clipboard icon to the right of the term Area to open a window in which different areas1135are listed. Click the desired area. In the example below, Hospitality Lab was chosen. The window1136closes and your selection is automatically copied to the current window. If you cannot select an1137area, you will need to create one.

	Selection dialogue: Choose area	
	Select the zones here that you want to assign to the room zone.	
Name 🕆		
0		
No area	1	
Hospitality Lab		
DG2		

1139 2. Click **Save** to save your entries.

1140 *2.5.6.4 Create an Area*

- 11411. Navigate to Organization > Area to create an area. In the menu, select the Create button in the1142Actions menu on the left. In the preselection pop-up dialogue, select DG2. In this menu, give the1143area a name and add the correct corresponding time zone before saving. In our lab, our
- 1144 configuration looks like the following screen:

Edit DG	it DG2 area 👒 🗠 Hospitality Lab 🗠 🗠 👘		Default te		
Master data	Access p	oints Time models			
Name * System * Description	Q	Hospitality Lab	. Y		
Calendar 🏹 Time zone 🏠		America/Montserrat (/	▼ America/ ▼		

- 1145
- 11462. Be sure to save the created area. After this is complete, refer to the previous step to add the1147area to the terminal.
- 1148 2.5.6.5 Provisioning Access
- 1149 When configuring and commissioning a hotel, individual access rights must be assigned to the offline
- 1150 terminals. The steps below describe the assignment of individual access rights.
- 1151 2.5.6.5.1 Create Authorizations
- 1152 1. To begin provisioning access to a created area and terminal, navigate to Authorizations >
- 1153 Individual Access Rights in the top menu:

Actions	Individual acces	s rights list	
Search	-		
Create	ABCDEFG	HIJKLMNOPQRSTUVWXYZ	0123456789
Print			
	Name 🕈	ID \$	Plattform ¢

- 1154
- 1155 2. When the window opens, select "create."
- 1156 3. The window "Create Dialock 2.0 individual access rights" opens.

- Enter the room number in the entry field for Name (the software accepts numbers only, not letters), and click Save.
- 5. The window "Create individual access rights" will open again. Your room number has alreadybeen automatically copied to the uppermost input field.
- 11616. In the right input field for ID, enter the same room number already entered in the Name field.1162 (The fields must match.)
- 1163 7. Save the entries:

Edit Dialock	2.0 individual access rights	ia ia 102 ⊧∘
Name *	102	
Platform *	DG2	
ID	102	
Cross-araa	10	

1164

1166 2.5.6.5.2 Configuring the Terminal

1167 This step completes the individual terminal setup and assigns the previously created individual access 1168 rights to the respective terminals.

- Navigate to **Devices** > **Terminal** in the main menu. In this menu, select the terminal that you previously created. The **Edit Offline terminal** window opens.
- 1171 2. Click the "Individual access rights" tab.
- 1172 3. Click the **clipboard** below the term "Access rights."
- 11734. This opens a dialogue box in which a selection of terminals that have already been set up are1174listed:

Selection dialogue: Choose access right	×
you select the individual access rights for this Sphinx-Terminal.	
ID \$	
	ou select the individual access rights for this Sphinx-Terminal.

- 1176 5. Click the terminal that you created previously.
- 1177 6. Confirm with "Apply selection."
- 1178 7. The **Save** icon starts flashing. Click **Save**.
- 8. You have now set up a terminal with its individual properties and assigned this terminal to a spe-cific access point in the building.

1181 2.5.6.5.3 Configuring the MDU

- Navigate to **Devices** > **MDU**. A window with the heading **DG2-MDUliste** opens. If you have an MDU registered, you can skip to the next section.
- Select **Register MDU** on the left side of the screen. After accepting the Java applets run warn ings, wait for the MDU to be discovered.
- 1186
 3. If the MDU is plugged into the current host machine and you can view it in a file browser, you
 1187
 will see a window showing the discovered MDU. Close the window.
- 1188 4. Your MDU is now listed in the **DG2-MDUliste** menu:

DG2-MDUliste	
6	
AII A B C D E F G H I J K L	M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9
0	
Name 🗢	Serialnumber 🌣
MDU110	0601000756
MDU110	0601000756

1189 2.5.6.5.4 Programming a Physical Terminal by Using the MDU

- 1190 1. To program the physical terminal, navigate to **Organizations > Area**.
- 1191 2. Select the area that was created in the step Create an Area.
- 1192 3. Select **Parameterize MDU** from the left-hand menu.
- Ensure that your MDU is still plugged into your workstation. In the pop-up menu, select the
 rooms that you wish to program, then click **OK.**
- 11955. Depending on how many rooms you are programming, you will see a progress bar that then1196leads to a blank window stating the MDU has been programmed.
- 1197 6. Click **OK.** You can now begin to program physically access points utilizing the MDU.

1198 2.5.6.6 Group and Role Creation

1199 Multiple user roles can be created with different levels of access to the software. These roles can be 1200 assigned to different users created in the system.

1201 2.5.6.6.1 Creating a Role

- 1202 1. Navigate to **System > Users** roles in the main menu. This opens the "User roles list" window.
- 1203 2. Select **Create** in the left-hand menu. The **Create user role** window opens.
- In the **"Role name"** field, enter an appropriate designation, such as "hotel manager" or "janitor." Assign the desired authorizations to this user role. (Note the red triangles, which allow you to expand further windows to assign more detailed authorizations.) Save your entries:

		Create user role
		Master data
		Role name " Front Desk
		Module authorisations
		Module
		 Dashboard Profile Authorisations Organisation Devices Tools System
1207		
1208		
1209 1210	2.5.6.6 1.	2 Creating a User Navigate to System > Users in the main menu.
1211	2.	The "Users list" window opens. In the left-hand menu field, select Create.
1212 1213 1214 1215	3.	The "Create user" window opens. If a user will have full unrestricted access to the software, se- lect Administrator. Otherwise, do not check this box, then continue. Complete the username, full name, and password. NOTE: The username and password are required to access the soft- ware.
1216	4.	Click Save:

User account blocked				
Administrator				
User name *	frontdes	k		
Full name	Front De	Front Desk Employee		
E-mail address				
Last password change	Jul 23, 2	019 3:01 PM		
Failed login attempts	0			
Last login				
Time zone	Europe	Berlin (Europe/Berlin [🔻		
Task esponsibilities	ß	Task typ		
	Ū	Firmware update		
	Ŵ	Releasing iSAC-3 encoder		
	Ŵ	Releasing new hardware		
	100			

1218 5. Click the **Authorizations** tab at the top. From the existing users' roles, select the role that you wish to assign the user.

1220 2.6 Privileged Access Management System—Remediant SecureONE

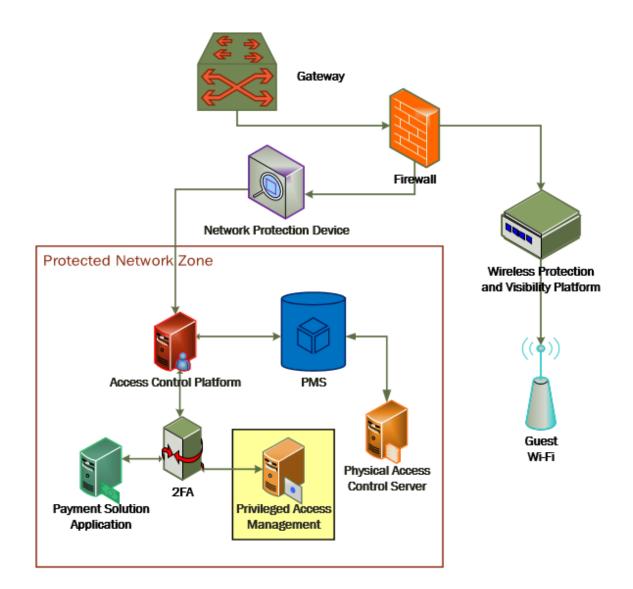
- 1221 This section of the guide supplies installation and configuration guidance for the privileged access
- 1222 management solution, which provides security for administrator-level actions within the enterprise.
- 1223 Remediant SecureONE is the privileged access management solution within the reference architecture.

Create us	Selection dialogue: Choose operator role	×	
Master data	Select the user roles here that you want to assign to the user.		
Operator roles &	Name [↑]		
• • •	Front Desk		

1224 2.6.1 Privileged Access Management System–Remediant SecureONE–Overview

- Remediant SecureONE provides detection and response capabilities for violations of privileged accesswithin the enterprise.
- 1227 In the PMS ecosystem, SecureONE was deployed as a prebuilt VM appliance from the vendor. We
- 1228 configured the appliance with parameters necessary for our environment.
- 1229 The network security in place in the architecture relies on the appropriate authentication of privileged
- users. Once that authentication is secured, it is trusted. It is the purview of the PAM solution to preventabuse of this trust.
- 1232 The location of the PAM system in the reference architecture is highlighted in the figure below.

1233 Figure 2-5 Privileged Access Management System in the Reference Architecture



1234

1235 2.6.2 Privileged Access Management System–Remediant SecureONE– 1236 Requirements

1237 The following subsections document the software, hardware, and network requirements for the PAM

system Remediant SecureONE. Both the hardware and software requirements were included in themanaged deployment provided by Remediant.

1240 2.6.2.1 Hardware Requirements for the Privileged Access Management System

- 1241 This installation occurred on a machine with 4 CPUs, 8 Gigabytes (GB) of memory, and 100 GB of 1242 storage.
- 1243 2.6.2.2 Software Requirements for the Privileged Access Management System
- 1244 This build utilized an Ubuntu 14.04 OS for the SecureONE server.
- 1245 2.6.2.3 Network Requirements for the Privileged Access Management System
- 1246 Network connectivity must be available to the web server hosted on the Remediant SecureONE device.
- 1247 Please note that a zero trust networking solution such as CryptoniteNXT can limit availability of network

1248 resources when improperly configured. For this reason, we recommend setting up and verifying

1249 Remediant SecureONE before applying the associated rules on the CryptoniteNXT device, as seen in

1250 <u>Section 2.1.8</u>.

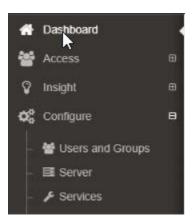
1251 2.6.3 Privileged Access Management System–Remediant SecureONE—Installation

- 1252 The installation procedure consists of the following steps:
- 1253 1. Connect SecureONE to the domain.
- 1254 2. Synchronize SecureONE to the domain.
- 1255 3. Verify that all managed machines are present in the SecureONE appliance.
- 1256 In the example implementation, SecureONE was deployed as a prebuilt VM from the vendor. The 1257 instructions below assume that the VM is already deployed and is accessible from the network.
- 1258 For a more in-depth discussion of implementation of a PAM solution, particularly as it relates to an
- 1259 installed access control platform, please see NIST Special Publication 1800-18, Privileged Account
- 1260 *Management for the Financial Services Sector* Practice Guide.

1261 2.6.4 Initial Configuration

- SecureONE needs to be configured to connect to a domain server, which should be installed within yourenvironment. To have a successfully working SecureONE instance, take these steps:
- 12641. Create a service account within your Active Directory server. The service account can be named1265secureone or anything that you choose. The SecureONE appliance will use this account.1266https://blogs.technet.microsoft.com/askpfeplat/2012/12/16/windows-server-2012-group-man-1267aged-service-accounts/

- 1268 2. To log in to the SecureONE appliance, navigate in a web browser to the IP of the machine, and 1269 use the provided credentials to sign in.
- 1270 3. On the side panel, select **Configure > Services:**



New Domain

1271

- 1272 4. Select **Add Domain** in the Domain Configuration window.
- 1273 5. Enter your relevant domain information. We have included ours below for reference:

Domain Name	hotel.nccoe Detect	Domain User (Read-Only)	HOTEL\secureone
LDAP Server	win-hotel.hotel.nccoe	Domain Password	
LDAP Port	389 SSL	Default Policy	Enabled •
Search Base	dc=hotel.dc=nccoe	Protect Mode Set	tings
Bind DN	HOTEL\secureone		
Bind Password		Domain User	HOTEL\manager
	Test Connection	Domain Password	
		Default Policy	Disabled *
Directory Search	Settings		

1274

12756. After the domain has been added, Remediant will sync with the domain. If the sync is successful,1276you will see this screen:

٩							Refresh
r	Domain 🔿	Server	Port	SSL O	Last Sync 🔾	Status	Default Policy
>	hotel.nccoe	win-hotel.hotel.nccoe	389	×	in 5 minutes	⊘ Synced	Scan A Protect

1278 7. If you return to the **Home** menu, your dashboard should start populating with the machines that are connected to the domain.

à			Alter Alter A		
Summary		LDAP Domains		Scan Performance	Service Pres
Total Systems Scanned	2/13	hotel.nccoe		Scan Completion	13 / 13
Active Sessions	0	 Last sync: in 5 minutes 		Successful Systems	0
□ Inactive Systems	1				U
Q Scan Mode Enabled	13			Offline Systems	0
Protect Mode Enabled	5			Encountered Error	0
				1	1
lighest Privileged Accounts	C.	High Risk Systems	C [*]	Operating Systems)
OTEL\Manage	4	FRONT-DESK	5		
IOTEL\Administ	4	HAFELEBACKE ND	4		
OTEL\Domain dmins	4				
RONTDESK\H	2			 Windows Server 2012 R2 Datac No Operating System Accurate Window Windows 10 Enterprise 	
RONTDESK\A	2			Activate Window Windows 10 Enterprise Go to System in Contro	'S

1280

1281 2.7 Wireless Network Management—Forescout CounterACT

- 1282 This section of the guide supplies installation and configuration guidance for the wireless network
- 1283 management solution, which provides access control for connections across the wireless network. It
- 1284 differentiates among verified guests, employees, and system administrators to provide the appropriate
- 1285 level of access through the wireless network.
- Forescout CounterACT is the wireless network management solution used in the exampleimplementation.

1288 2.7.1 Wireless Network Management–Forescout CounterACT–Overview

1289 The wireless network management solution from Forescout administers the wireless network in the1290 PMS ecosystem.

1291 Forescout CounterACT authenticates users to the wireless network via a captive portal. It blocks

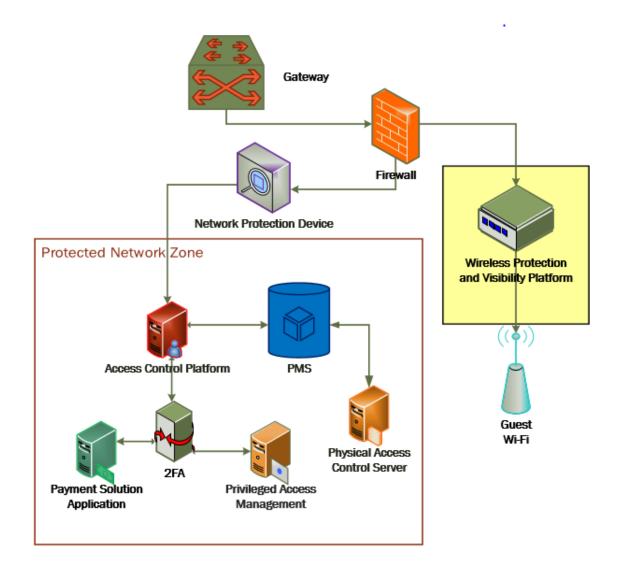
1292 unauthenticated or unauthorized connections. Guests get access to the internet but not to internal

1293 enterprise systems. Authenticated employees get access to the PMS so they can manage reservations

1294 and perform other enterprise functions. The location of the wireless network management solution in

1295 the reference architecture is highlighted in the figure below.

1296 Figure 2-6 Wireless Network Management in the Reference Architecture



1297

1298 2.7.2 Wireless Network Management–Forescout CounterACT–Requirements

1299 The following subsections document the software, hardware, and network requirements for the 1300 wireless network management solution for version 8.1.

1301 2.7.2.1 Hardware Requirements for Wireless Network Management

1302 This installation occurred on a machine with 4 CPUs, 10 GB of memory, and 200 GB of storage.

1303 2.7.2.2 Software Requirements for Wireless Network Management

1304 This installation occurred on a deployed CentOS 7 VM that the vendor provided.

1305 2.7.2.3 Network Requirements for Wireless Network Management

- Forescout CounterACT requires the capability to monitor network traffic on the network it is
 administering. Network connectivity is also required on the user workstation that will run the Forescout
 CounterACT console.
- 1309 2.7.3 Wireless Network Management–Forescout CounterACT–Installation
- 1310 1. To install the CounterACT console for management, navigate to [FORESCOUT IP]/install. This 1311 leads you to the page where you need to download the management console.



- 1312
- After installing the console, you can then log in to the management interface to begin configur ing your Forescout CounterACT appliance.



13163. Navigate through the Initial Setup Wizard when the console launches. Verify that the time and1317NTP server are configured as desired.

Initial Setup Wizard

	Time					
S Welcome	Use this option to set the CounterACT Appliance time zone. Set a time zone according to geographic locat					locatio
License	or by GMT	offset.				
fr Time						
Mail						
User Directory	Local time	Wed May 29 10:46:28	2019			
Domains	GMT time	Wed May 29 14:46:26	2019			
Authentication Servers	Time Zone	America/New_York		~		
Internal Network				_		
Enforcement Mode	NTP Server	ntp.forescout.net	v	Test		
Channels				_		
Switch						
Policy						
Inventory						
Finish						

1318

1320

1319 4. Input the e-mail account that you wish to receive notifications and alerts to.

	Mail					
🥑 Welcome	Use this opti	on to set Admin email information used for sending CounterACT notifications and alerts.				
License	If your network requires a mail relay, enter the mail relay address and verify that the mail relay server ca					
🕑 Time	receive mail from the CounterACT Appliance.					
👉 Mail						
User Directory	<u>A</u> dmin Email <mark>✓</mark> <u>M</u> ail relay	mail@hotel.nccoe				
Domains						
Authentication Servers Internal Network		mail.hotel.nccoe				
EnforcementMode						
Channels						
Switch						
Policy						
Inventory						
Finish						

1321 5. Input the domain information and credentials to be employed by ForeScout CounterACT.

	• • • • • • • • • • • • • • • • • • •	
Initial	Sotu	o Wizard
nnua	Setu	JVVIZAIU

User Directory

1	vveicome	Use th	Use this option to define credentials for a LDAP Server. These credentials are used to authenticate users and resolve user information, for example the display name, department name, e-mail address and more. You car later define other servers from Tools>Options>User Directory Plugin screen.						
0	License								
0	Time	later define other servers from Tools>Options>User Directory Plug				Plugin screen.			
0	Mail								
ular User Directory		Name	Name Hotel Primary						
	Domains	-	1.0						
	Authentication Servers	Type Microsoft Active Directory V							
Internal Network	Internal Network	Communication							
	EnforcementMode	Address	9	192.168.28.10		DNS Detection			
Channels		Port		636 🗇 🔽 Use TLS					
	Switch	Distant	2222						
	Policy	Directo	ory						
	Inventory	Domain	1	hoteInccoe					
	Finish			Example: Fully Qualified Dor	main Name, e.g.	MyCompany.com)			
		Adminis	strator	Administrator					
		Passwo	rd	*****					
		Verify P	assword	*****					

1322

1323 6. Input the IP Address range to be provisioned to the wireless network.

	Internal Ne	twork		
✓ Welcome	The Internal Ne	twork is the range of IP addr	esses in your organization that you want (CounterACT to manage. It
License			e organizational network in this definition	
S Time		side this range will not be ha terACT Appliances.	ndled by the Appliance. Hosts in the Inter	nal Network must be
🥑 Mail		ent name to the Internal Netw	vork for easy identification.	
Subser Directory	Segment name	Wireless		
🥝 Domains	Ranges			
Authentication Servers				-
🕼 Internal Network	Range			Add
EnforcementMode				Edit
Channels				Demons
Switch		۲	IP Address Range	x <u>R</u> emove
Policy		IP Range or Subnet	192.168.0.0/24	
Inventory			Examples	
Finish			• 10.0.0.1 - 10.0.0.127	
			192.168.1.0/24	
			 10.0.0.1 1000:/8 	
			 2001:db8::1 	
			OK Canc	

Set the enforcement options desired for this deployment. For our lab, "Full Enforcement with NAT Detection and Auto Discovery were employed.



1326

1327 1328 8. Start the appliance in the options windows. You can open the options menu by selecting the gear on the right of the screen.

Appliance

Applia Perform		e management tasks, for exa	ample starting and stopping t	he device or handling	upgrades and licenses
Search	k	Q			
Status	IP/Name	Hostname 🔺	Version	# Hosts	Device Alerta
A	192.168.1.43	NA	8.1,1	11	License, Char
	(1 selected)		Q Find	Tabla	
License to: NIST License: Demo - 193 days left The license cannot be authorized due to a The last auccessful verification was on 31. The license will be revoked in 26 days De Bandwidth: Current 0.0Mbps, Average 0.0Mbps, Max 3 High Availability: HA is not enabled Swap: 0 Kilobytes per second Lost Packets: 0.00% CPU Utilization: 10.82% Uptime: 6 days and 15 hours Time Gap from Console: Less than a minute earlier NTP Servers: 192.237.222.233 Packet Engine: CounterACT Appliance is running Channels: Low Mirrored traffic was detected on the fo Connection. Connected to 192.168.1.43 as admin		Demo - 193 days left The license cannot be author The last successful verificati	orized due to a O Start	5	
		HA is not enabled		e te Request	
		10.82%	🍇 Install fr	om File	
		Less than a minute earlier 192.237.222.233	- Traffic	Check Request Status	
		ected on the fol 👩 Backup			

1329 2.7.4 DNS Enforcement

In the options menu, select the drop-down for modules, then select **DNS Enforce.** In this menu,
 configure the IP used for the DNS enforcement. It should look like the screenshot below.

General Wh	itelist
Target IP	192 . 168 . 1 . 10
Port	53 0
TTL (Restricted)	30 0
🗹 Enable DNS re	solution forwarding for unrestricted hosts
TTL (Unrestricted	120 0
Cenable HTTPS	listener

1333 2.7.5 Switch Plug-in

1332

- 1334 1. In the options menu, select the switch menu icon in the left scrolling menu. Here, we are adding 1335 our VyOS switch:
- 1336 Select Add.
- Enter the address of the switch.
- Select **Router-Linux** as the vendor:

Add Switch

General								
General	Enter the switch device information. If the device vendor you are configuring does not appear in the vendor list, select Generic from the list. CounterACT resolves switch information for generic switches but does not carry out Switch block and Assign to VLAN actions. Refer to the online Help if the generic switch does not properly resolve switch information.							
	Address	192.168.0.1						
	Connecting Appliance	192.168.1.43 🗸						
	Vendor	Router-Linux	~					
	Comment							
	Use switch configura	ation as template						

Enter the authentication credentials of the switch to enable CLI management via the Forescout
 CounterACT appliance.

CLI	
Configure the plug Teinet or SSH crea	in to connect to the managed switch using CLI credentials - either dentials.
🔄 Use CLI	
Connection Type	SSH
User	admin
Password	*****
Confirm Password	******
Privileged Acces	s Parameters
Z Enable privilege	f access
O No password	
💿 Use login paran	neters
O Custom	
User	
Password	
Confirm Password	

1342 3. Verify that **Read: IP to MAC Mapping** is checked.

1341

	Permissions
	efine read/write permissions for switch/plugin communication, as well as advanced settings.
	Discovery Permissions
	Read: Auto-discover additional switches (CDP, FDP, LLDP)
	MAC Permissions
	Read: MACs connected to switch port and port properties (MAC address table)
	ARP Permissions
	Read: IP to MAC Mapping
1343	Write: Clear Redundant IP Addresses associated with MAC Address Advanced
1344	4. Configure 802.1X per organizational specification.
	802.1X
	Configure 802.1x settings
	\Box
	Radius Secret as configured in switches
1345	Retype Radius Secret as configured in switches

1346 5. Start and test your switch configuration, selecting **start** and **test** respectively.

=	CLI	
🕑 General 👉 CLI	Configure the plug Telnet or SSH cre	in to connect to the managed switch using CLI credentials - eith dentials.
Permissions		
802.1X		
	Use CLI	
	Connection Type	SSH
	User	root
	Password	*****
	Confirm Password	******
	Privileged Acces	s Parameters
	Z Enable privilege	d access
	O No password	
	🔿 Use login parar	neters
	 Custom 	
	User	root
	Password	*****
	Confirm Password	*****
	SSH Fingerprint	
	🗸 Use SSH Finger	

1348 2.7.6 Guest Policy

The guest policy is defined to control access of a hotel guest when that person is using Guest WiFi
according to the authentication results of the hotel guest device. The authentication process determines
the access to which the hotel guest device qualifies, then Forescout implements the controls to provide

the correct access. It is assumed, due to limitations of the NCCoE lab, the actual authentication processis completed.

Our lab uses three devices connected to the Guest WiFi to represent the three results that may come
from the authentication process: Guest Hosts, Signed-in Guest Hosts, and Corporate Hosts. These names
relate to those used by the Forescout tool.

- 1357 **Guest Hosts** 1358 end-point client devices that are not authenticated 1359 No traffic is allowed from these devices within the Wi-Fi VLAN. 0 1360 In the Forescout console, this type of device is shown in the Policy Guest WiFi column as 1361 Guest Hosts. This device is identified by the IP address 192.168.0.129. 1362 Signed-in Guest Hosts 1363 end-point client devices that are authenticated as hotel guests with approved access to 1364 the internet 1365
- 1365oAllow traffic on ports 80 and 443 to addresses outside the hotel on the internet (non-1366RFC1918 addresses).
- 1367 Prevent access to any addresses inside the hotel infrastructure (RFC1918 addresses).
- 1368oIn the Forescout Console, this type of device is shown in the Policy Guest WiFi column as1369Signed-in Guests. This device is identified by the IP address 192.168.0.119.
- Corporate Hosts
- 1371 o end-point client devices that are authenticated with hotel domain credentials
- 1372oAllow full access to both the internet (non-RFC1918 addresses) and addresses inside the1373hotel infrastructure (RFC1918 addresses).
- 1374oIn the Forescout Console, this type of device is shown in the Policy Guest WiFi column as1375Corporate Hosts. This device is identified by the IP address 192.168.0.133.

1376 This Forescout policy is designed to detect a device when it joins the Guest WiFi, query that device for 1377 the result of its authentication process and assign settings to the Forescout virtual firewall that provide 1378 the appropriate network access to that device. Due to lab limitations, the query process is not part of 1379 this guide, and the devices in the lab are manually assigned to each of the three devices used in the lab.

1380 The Forescout policy is defined by these parameters:

1381 • Name: Guest WiFi

1382	1.1	Scope: wireless network segment in the lab and any computer or mobile device
1383	1.1	Main Rule: This is not used for this lab.
1384 1385	1	Sub-Rules: Three subrules identify and control the three types of hotel guest devices instead of the Main Rule.
1386		• Name:
1387		 Corporate Hosts
1388		 Signed-in Guests
1389		 Guest Hosts
1390		Condition:
1391		 Match a single criterion.
1392		 IPv4 address
1393		• 192.168.0.133
1394		• 192.168.0.129
1395		• 192.168.0.119
1396		Action:
1397		 Add to Group.
1398		Designate Corporate Hosts.
1399		Designate Signed-in Guests.
1400		Designate Guest Hosts.
1401		 Virtual Firewall
1402		 blocking rules for Corporate Hosts
1403		 blocking rules for Signed-in Guests
1404		 blocking rules for Guest Hosts

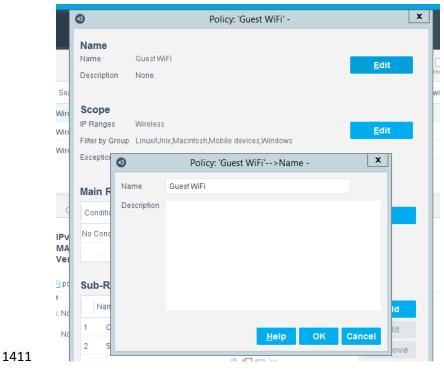
1405 The Forescout console full screen showing the three devices on the Guest WiFi appears below.

<) FORES	COUT		â	Home	Asset Inventory	\$ 8 ; ⊧		×	Threats (0)			
Views	«	Guest WiFi			(A Match Unm	natched Irresolvable	Pending C	nline\Offline 🗸]	3 OF 13	HOSTS
Search ✓ ▶ Guest WiFi (3)	Q	IPv4 Address	Segment	Policy Guest WiFi	MAC Address Comment	Display Na	Switch IP/FQ	Switch Port	Switch Port	Host 🕶	Function	Actions
🔠 Corporate Ho	sts (1)	• 192.168.0.133	Wireless	₽ Corporate Hosts	005056b24e1f					192.168.0.133	Computer	🖋 😸
🔠 Signed-in Gu	ests (1)	• 192.168.0.129	Wireless	😤 Guest Hosts	005056b2efe6					192.168.0.129	Computer	`a 🖵
Gue Gue	st Hosts (1)	• 192.168.0.119	Wireless	😤 Signed-in Guests	005056b22d5c					192.168.0.119	Computer	1
A ()												
Filters												
Search	Q	Guest WiFi Pro	file Complian	ce All Policies								
) All												Ŧ
Segments (13)				ess: 192.168.0.133 Fund ess: 005056b24e11 Ope	tion: Computer rating System: Windows							
E Organizational Units		<u> </u>	Vendor an	d Model: VMware								
🔢 Default Groups		Matched the Gue	<u>st WiFi</u> policy, Corj	porate Hosts Sub-Rule on A	ugust 26 04:17:42 PM 🎒 View.p	olicy flow						
🔢 Groups		E Match Main	Rule									
		Condition Prop	erties: None									
		Actions:	None (No a	ctions defined for this rule)								
		Sub-Rules:										
		1. 🗖 Match (Corporate Hosts									
			Condition Prope	rties: IPv4 Address:	192.168.0.133							
			Actions:	🔠 Add to Group: Corp	orate Hosts							
		2. N/A S	'he host is not insp Signed-in Guests Guest Hosts	ected by the remaining sub-	rules because it matches <i>Corpora</i>	ate Hosts			vate Wi <mark>nd</mark>	etwork traffic: 0.01 I OWS		dour

1. Right-click the **Guest WiFi** policy in the Views section of the Console and click **Edit** to open the policy editor and configure Forescout for controlling the Guest WiFi.

<) FORESCOUT		0	Po	licy: 'Guest Wi	Fi' -	×
Views Search Q CoustWHF(2) Cou	Guest WIFI IPv4 Address 58 • 192168.0.133 Wir • 192168.0.139 Wir • 192168.0.119 Wir	Description Scope IP Ranges Filter by Group	Guest WF) None. Wreless LinuxUnix,Macintosh,Mo None.	bile devices,Win	dows	Edit Edit
Search Q	Guest WiFi Protile (Conditions	Actions	Re-C	heckMatched	Edit
Segments (13) Organizational Units Default Groups	Matched the <u>Guest WiFi</u> p				8 hours, All admi	
S 🔠 Groups	Condition Properties: N	Name	Conditions	Actions	Exceptions	Add
	Actions: N	1 Comorat	e Hosts IPv4 Address: 19	- 18		Edit
	Sub-Rules	2 Signed-in	n Guest IPv4 Address: 19			Bemove
	1. 🖬 Match Corporat	3 Guest Ho	ists IPv4 Address: 19	0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Duplicate
	Condit	-				Up
	Actions The nost i 2 NIA Signed-in 3 NIA Guest Hos					Dgwn
	-				Help	OK Cancel

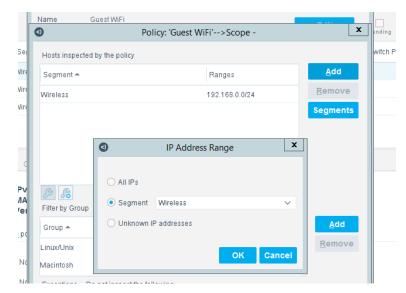
Start the configuration process by clicking **Edit** in the Name section and entering the name of the policy.



1412 3. Click **Edit** in the Scope section to open the scope editor.

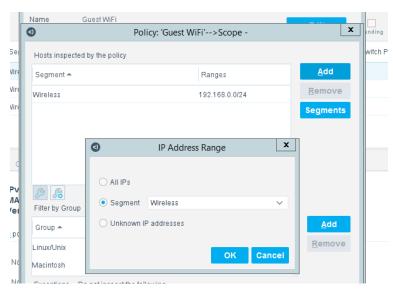
lame Jame Gu	est WiFi		
)	Policy: 'Guest WiF	i'>Scope -	L
Hosts inspected by	/ the policy		
Segment 🔺		Ranges	<u>A</u> dd
Wireless		92.168.0.0/24	<u>R</u> emove
			Segments
a. a.			
Eilter by Group - (Only inspect bosts from the followin	na aroups	
Filter by Group - 0	Only inspect hosts from the followin		Add
Filter by Group - (Group A	Description)	<u>A</u> dd <u>R</u> emove
Filter by Group - (Group - Linux/Unix	Description Classifier gr	oup	
Filter by Group - (Group - Linux/Unix Macintosh	Description Classifier gr Classifier gr	oup	
Filter by Group - (Group A Linux/Unix Macintosh Exceptions - Do r	Description Classifier gr Classifier gr ot inspect the following	oup	<u>R</u> emove
Filter by Group - (Group - Linux/Unix Macintosh	Description Classifier gr Classifier gr	oup	<u>R</u> emove
Filter by Group - (Group A Linux/Unix Macintosh Exceptions - Do r	Description Classifier gr Classifier gr ot inspect the following	oup	<u>R</u> emove
Filter by Group - (Group A Linux/Unix Macintosh Exceptions - Do r	Description Classifier gr Classifier gr ot inspect the following Values	oup	<u>R</u> emove

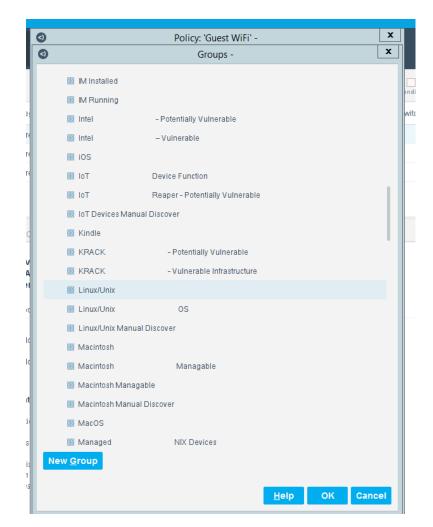
14134. Cick Add in the "Hosts Inspected by the policy" section to open the IP Address Range window1414and select the network segment to be monitored.



1415

1416 5. Click **Add** in the "Filter by group" section to open the Groups window and select the types of de-1417 vices to be monitored.

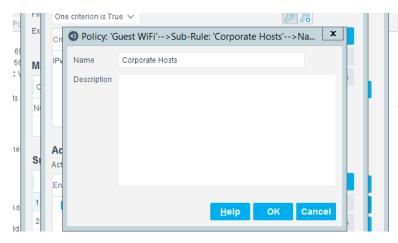




- 1419 After the Name and Scope have been defined, consider defining the Main Rule section. For this lab, the
- 1420 Main Rule was left in the default No Conditions value. Only the Sub-Rules were used.
- 1421 1. Highlight a Sub-Rule and click **Edit** to open the Sub-Rule edit window.

Conditions	Actions	Re-	checkMatched	Edit
No Conditions		Even	y 8 hours, All admi	
Sub-Rules				
Name	Conditions	Actions	Exceptions	<u>A</u> dd
1 Corpora	ite Hosts IPv4 Address: 1	9 🔠		<u>E</u> dit
	in Guest IPv4 Address: 1			<u>R</u> emove
3 Guest H	osts IPv4 Address: 1	9 🐴 🖵 💽 🕯		Duplicate
				Up
				D <u>o</u> wn

1422 2. In the Sub-Rule edit window, click **Edit** in the Name section, and enter the name of the Sub-Rule.



1423

- 14243. In the Condition Section of the Sub-Rule edit window, click the drop-down arrow, and select the1425condition type.
- 1426 4. Then highlight the Criteria and click **Edit** to open the Condition Edit window:

1427



5. The left frame of the Condition Edit window lists the conditions that Forescout may use. Scroll 1430 through the list and select the appropriate Condition. This lab used the IPv4 Address Condition 1431 to identify the device used for each of the three types of hotel guest devices.

1432 We needed a work-around to address limitations in the lab. In a real-world situation, dynamic 1433 criteria tailored to meet the strategy of a specific hotel, such as the Authentication Login 1434 Condition, may be appropriate:

3)		Condition	
ipv4	IPv4 Address: Indicates the IPv4	Address of the host.	
roperties	 Meets the following criteria Does not meet the following criteria 	teria	
Cisco ACI			
Node VTEP Address	O All IPv4		
Node Fabric IP Address	In Network Segment		
Node VTEP IP Pool	IPv4 Range	192.168.0.133	
Device Information	 IFV4 Range 	Examples:	
Number of IPv4 Addresses		 10.0.0.1 - 10.0.0.127 192.168.1.0/24 	
IPv4 Address		 192.108.1.0/24 10.0.0.1 	
Last Known IPv4 Address	O Without a known IPv4 address		
ist IPv4 Report Time	○ Starts With		
Track Changes			
Number of IPv4 addresses Chang	je		

1435

1436 6. In the Actions Section of the Sub-Rule edit window, highlight the Action in the box, and click Edit to open the Action Edit window: 1437

ctions	are applied to hosts matching the a	bove condition.	
nable	Action	Details	<u>A</u> dd
	🗞 HTTP Login	HTTP Login	<u>E</u> dit
√	🖵 Virtual Firewall	Virtual Firew	<u>R</u> emove
	😝 Assign to VLAN	Assign to VL	
\checkmark	🔠 Add to Group	Add to Grou	

Advanced

14397. The left frame of the Action Edit window lists the actions that Forescout may use. Scroll through1440the list and select the appropriate action. This lab used the Add to Group action to designate the1441device identified by the condition as one of the three types of hotel guest devices:

0	Action
Search Q	This action adds the host to the selected group.
🔠 Add to Group	Parameters Schedule
S Delete Host	Junearie
🔆 Delete Label	Add to group:
Relete Properties	● Guest Hosts ✓ <u>New Group</u>
🗟 Disable Remote Inspection	O Ignored IPs
🔁 HTTP Localhost Login	O Properties - Passive Learning
😳 Recheck Host	·
E Set Counter	Expires when host no longer matches policy
C Start SecureConnector	Key MAC or IPv4 address ~
Stop SecureConnector	Comment
😵 Update Installed SecureConner	Tags : Add Tags
😵 Upgrade OS X SecureConnect:	

1442

14438. This lab also used the Virtual Firewall action to control the access given to the device identified1444by the condition as one of the three types of hotel guest devices. In the Action Edit window for1445the Virtual Firewall, select the blocking rule that matches the appropriate type of hotel guest1446device, and click Edit to open the Blocking Rules Edit window:

0		Action		l
Search Q	This action adds a Virtua	Firewall rule that blocks\allo	ws access to\from the host.	
2 VPN Block				
🔄 Virtual Firewall	Parameters Sched	ule		
💫 WLAN Block	Blocking Rules			
NLAN Role	Source	Target	Service	Add
VMware NSX	Matched hosts	Wireless	Any	Edit
🕙 Add To Security Group	Matched hosts	Internal	Any	<u>R</u> emove
🍄 Apply Security Tag	Matched hosts	Protected	Any	
🕚 Remove From Security Group				
😵 Remove Security Tag				
VMware vSphere				
Block Virtual Machine Network	3 items (1 selected)			
🛃 Change Virtual Machine Port Gi	Blocking Exceptions			
🛃 Install/Upgrade VMware Tools	Source 🔺	Target	Service	Add
Power Off Virtual Machine				Edit
Power On Virtual Machine				<u>R</u> emove
🛃 Reboot Virtual Machine Guest		No items to dis	nlav	
🚱 Reset Virtual Machine			(real)	
🚰 Shut Down Virtual Machine Gue				
📑 Standby Virtual Machine Guest				
🚮 Suspend Virtual Machine				

14489. In the Blocking Rules Edit window, select the Inbound/Outbound criteria, the Target IP range,1449 and the Target Port range for the rule:

Ð		Blocking Rules	
Inbo	und/Outbound		
	O The FW will	block traffic to the detected host.	
	• The FW will	block traffic from the detected host.	
Targ	jet IP		
	🔿 All IPv4		
	 Segment 	Wireless	
	🔿 IPv4 Range	Examples:	
		 10.0.0.1 - 10.0.0.127 192.168.1.0/24 10.0.0.1 	
Targ	iet Port		
	● <u>A</u> ll (TCP and	I UDP)	
	O <u>S</u> ingle	1 0 TCP ~	
	⊖ <u>L</u> ist		
		er a single, list or ranges of ports (TCP and UDP) ample: 22/TCP, 161/UDP, 6000-6100/TCP	I
		ок	Cance

1450 **2.8 Virtual Switch—VyOS Configuration**

- We configured a VyOS router to work with Forescout's switch plug-in to capture and enforce the
 policies we deployed for the wireless network. VyOS is a console-based Linux switch/firewall and
 was used as a virtual switch in our use case.
- 1454To begin configuring the switch, we used the following commands. VyOS has good1455documentation, and we recommend that you reference the documentation if you would like to
- 1456 extend the capabilities of the machine.
- 1457 \$ configure
- 1458 set interfaces eth2 address dhcp
- 1459 set interface eth2 description 'OUTERNET'
- 1460 set interface eth1 address `192.168.0.1/25'
- 1461 set interface eth1 description 'WIRELESS'

1462	set service ssh port `22'
1463	set nat source rule 100 outbound-interface `eth1'
1464	set nat source rule 100 source address `192.168.0.0/24'
1465	set nat source rule 100 translation address masquerade
1466 1467	set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24 de- fault-router `192.168.0.1'
1468 1469	set service dhcp-server shared-network-name LAN subnet dns-server [FORESCOUT DNS-ENFORCEMENT IP]
1470 1471	set service dhcp-server shared-network-name LAN subnet dns-server `192.168.0.1'
1472 1473	set service dhcp-server shared-network-name LAN subnet domain-name `hotel- wireless'
1474	set service dhcp-server shared-network-name LAN subnet lease `86400'
1475 1476	set service dhcp-server shared-network-name LAN subnet range 0 start 192.168.0.10
1477 1478	set service dhcp-server shared-network-name LAN subnet range 0 stop `192.168.0.254'
1479	set service dns forwarding cache-size `0`
1480	set service dns forwarding listen-on `eth1'
1481	set service dns forwarding name-server `8.8.8.8'
1482	set service dns forwarding name-server `1.1.1.1'
1483	set traffic-policy shaper WAN-OUT bandwidth `50Mbit'
1484	set traffic-policy shaper WAN-OUT default bandwidth `50%'
1485	set traffic-policy shaper WAN-OUT default ceiling `100%'
1486	set traffic-policy shaper WAN-OUT default queue-type `fair-queue'
1487	set traffic-policy shaper LAN-OUT bandwidth `200Mbit'
1488	set traffic-policy shaper LAN-OUT default bandwidth `50%'
1489	set traffic-policy shaper LAN-OUT default ceiling `100%'
1490	set traffic-policy shaper LAN-OUT default queue-type `fair-queue'
1491	set interfaces ethernet ethl traffic-policy out `LAN-OUT'
1492	set interfaces ethernet eth2 traffic-policy out `WAN-OUT'
1493	set service snmp community hospitality routers authorization ro
1494	set service snmp community hospitality routers client [FORESCOUT APPLIANCE]

1495	set service snmp trap-target [FORESCOUT APPLIANCE]
1496	set service snmp v3 engineid '0x0aa0d6c6f450'
1497	set service snmp v3 group defaultgroup mode 'ro'
1498	set service snmp v3 group defaultgroup seclevel 'priv'
1499	set service snmp v3 group defaultgroup view 'defaultview'
1500	set service snmp v3 view defaultview oid '1'
1501	set service snmp v3 user hotel_user auth plaintext-key [STRONG PASSWORD]
1502	set service snmp v3 user hotel_user auth type 'md5'
1503	set service snmp v3 user hotel_user engineid '0x0aa0d6c6f450'
1504	set service snmp v3 user hotel_user group 'defaultgroup'
1505	set service snmp v3 user hotel_user mode 'ro'
1506	set service snmp v3 user hotel_user privacy type aes
1507	set service snmp v3 user hotel_user privacy plaintext-key [STRONG PASSWORD]
1508	\$ commit
1509	\$ save

1510 2.9 Integration of Security Components

1511 In addition to installation and configuration of the individual components, the PMS ecosystem required 1512 a few commands to enable end points with native GUIs to work.

1513 2.9.1 CryptoniteNXT Integration with CLI End Points

Typically, addition of an end point to the CryptoniteNXT protected zone is done through a web browser.
In the case of end points without native GUIs, specifically TDi ConsoleWorks and Remediant SecureONE,
the following steps must be taken. These instructions rely on CLI access to the end point in question.

1517	\$sudo yum install wget
1518	\$y
	<pre>\$wgetno-check-certificatepost-data 'username=Administra- tor&passcode=<totp code="">' https://portal.di.ipdr/login</totp></pre>

1521 Appendix A List of Acronyms

ACC	Administration Control Center
CentOS	Community Enterprise Operating System
CLI	Command Line Interface
CNSSI	Committee on National Security Systems Instruction
CPU	Central Processing Unit
CRADA	Cooperative Research and Development Agreement
DNS	Domain Name System
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GB	Gigabyte
GUI	Graphical User Interface
IP	Internet Protocol
п	Information Technology
LAN	Local Area Network
MDU	Mobile Data Unit
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OS	Operating System
PCI	Payment Card Industry
РНР	Hypertext Preprocessor
PMS	Property Management System
RDP	Remote Desktop Protocol
SAKA	StrongAuth KeyAppliance
SSH	Secure Shell
SSL	Secure Sockets Layer

SP	Special Publication
ТСР	Transport Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing

1523 Appendix B Glossary

Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
	SOURCE: Committee on National Security Systems Instruction (CNSSI) 4009-2015
Architecture	the design of the network of the hotel environment and the components that are used to construct it
Authentication	The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
	SOURCE: Federal Information Processing Standards (FIPS) 200
Authorization	The right or a permission that is granted to a system entity to access a system resource.
	SOURCE: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 2
Certificate Revocation List	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
	SOURCE: NIST SP 800-32
Configuration	The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.
	SOURCE: NIST SP 800-128
Console	a visually oriented input and output device used to interact with a computational resource
Firewall	A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.
	SOURCE: NIST SP 800-152

Fully Qualified Domain Name	an unambiguous identifier that contains every domain level, including the top- level domain
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
	SOURCE: FIPS 200
Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
	SOURCE: CNSSI 4009-2015
Privilege	A right granted to an individual, a program, or a process.
	SOURCE: CNSSI 4009-2015
Public Key Infrastructure	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.
	SOURCE: CNSSI 4009-2015
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
	SOURCE: NIST SP 800-161
Wi-Fi	A generic term that refers to a wireless local area network that observes the IEEE 802.11 protocol.
	SOURCE: NIST Interagency or Internal Report 725