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

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

CHALLENGE

Hospitality organizations rely on a PMS for daily tasks, planning, and record keeping. As the operations hub, the PMS interfaces with several services and components within a hotel's IT systems, such as point-of-sale (POS) systems, physical access control systems, Wi-Fi networks, and other guest service applications. A PMS, and the extended PMS ecosystem, stores, processes, and transmits a variety of sensitive guest information, including payment card information (PCI) and personally identifiable information (PII). 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, including financial penalties for violating state, federal, and international privacy and other regulatory regimes.

> ***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…*

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

The National Cybersecurity Center of Excellence (NCCoE) collaborated with the hospitality business community and cybersecurity technology providers to build an environment that simulates a hotel's IT infrastructure, including guest WiFi and a PMS integrated with a POS module and an electronic door lock system. Using commercially-available products, the example solution shows how to protect data moving within this environment, and limit or prevent user access to the various systems and services.

The example solution uses technologies and security capabilities (shown below) from our project collaborators. All technologies used in the solution support security standards and guidelines of the NIST Cybersecurity Framework, Hotel Technology Next Generation, and the PCI Security Standards Council, among others. Although following the guide does not ensure General Data Protection Regulation (GDPR) 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
tdi technologies	Access control platform that secures connections, and provides control mechanisms to enterprise systems for authorized users and devices; monitors activity down to the keystroke

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

HOW TO USE THIS GUIDE

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

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-27a: Executive Summary*, to understand the impetus for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-27b: Approach, Architecture, and Security Characteristics,* which describes what we built and why, including the risk analysis performed, and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-27c: How-To Guides*, which provides specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/securing-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 us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

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

COLLABORATORS

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

The NCCoE at NIST built a PMS ecosystem in a laboratory environment to explore methods to improve the cybersecurity of a PMS. The PMS ecosystem included the PMS, a credit card payment platform, and an analogous ancillary hotel system. In this example implementation, a physical access control system was used as the ancillary system.

The principal capabilities include protecting sensitive data, enforcing role-based access control, and monitoring for anomalies. The principal recommendations include implementing cybersecurity concepts such as zero trust, moving target defense, tokenization of credit card data, and role-based authentication.

The PMS environment outlined in this guide encourages hoteliers and similar stakeholders to adopt effective cybersecurity and privacy concepts by using standard components that are composed of open-source and commercially available components.

KEYWORDS

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

ACKNOWLEDGMENTS

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

The technology partners/collaborators who participated in this project submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a CRADA with 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	policy-based control enforcement for guest Wi-Fi networks and visualizations of diverse types of network-connected devices
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 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

Contents

115 # List of Figures

124 # List of Tables

1 Summary

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, 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 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 rooms.

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 security and privacy protections to the data used in the PMS.

1.1 Challenge

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 challenge of building an example implementation that offers hotel owners and operators some options to secure their property management systems.

Securing Property Management Systems supports the following security and privacy characteristics:

- prevents unauthorized access via role-based authentication
- 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
- increases situational awareness by auditing, system activity logging, and reporting
- prevents unauthorized use of personal information

To build the example implementation, hereafter known as the PMS ecosystem, the project collaborators reached consensus on an architecture that implements aspects of a zero trust architecture (ZTA), moving target defense (MTD), and data tokenization to reduce cybersecurity risk for a hotel's PMS.

1.2 Implementation

The project demonstrates to hospitality organizations how to protect against loss and misuse of customer data and how to provide more cybersecurity and privacy for guest Wi-Fi networks, employee workstations, and electronic door locks.

Best practices for network and enterprise cybersecurity as put forth by the collaborators include role-based access control, allowlisting, and privileged access management. Utilizing data tokenization,

explicitly allowing only identified entities access (allowlisting), and role-based access control enforcement, theft of credit card and transaction data is prevented. Allowlisting is the practice of listing entities that are granted access to a certain system or protocol. When an allowlist is used, all entities are denied access, except those included in the allowlist.

The PMS ecosystem enables and enforces role-based access control to define exactly who or what will be allowed to make connections within the PMS ecosystem. ZTA utilizing dynamic provisioning specifies permitted connections and data transactions. Privileged access management defines, enforces, and monitors the privileges for each user, machine, and data transaction.

The NCCoE PMS ecosystem, three types of authorized users: hotel guests, hotel staff, and back-end administrators; engineers; and system owners. Each user has defined access privileges. Guests can 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 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.

Best practices for privacy protection include data minimization, transparency, and preference management. The *NIST Privacy Framework* Core [1] is a set of privacy protection activities, desired 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 outcomes across the organization from the executive level to the implementation/operations level. The 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 cycle of an organization's management of privacy risk arising from data processing. The Framework Core then identifies underlying key Categories and Subcategories–which are discrete outcomes–for each Function and provides example informative references such as existing standards, guidelines, and practices for each Subcategory.

This project demonstrates these best practices in a PMS ecosystem designed to simulate a typical hotel.

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.

The PMS ecosystem represented in the example implementation constantly changes the internet 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 lateral movement of attackers, who will be challenged to achieve and maintain persistent access.

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, based on factors such as device health and hygiene and other cybersecurity considerations.

The PMS ecosystem includes a network protection device and an access control platform to support privileged access management. Adding a wireless protection and visibility platform enables allowlisting, 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.

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:

- Hotel Technology Next Generation (HTNG): *Secure Payments Framework for Hospitality,* version 1.0, February 2013 [2]
- HTNG: Payment Tokenization Specification, February 21, 2018 [3]
- HTNG: Payment Systems & Data Security Specifications 2010B, October 22, 2010 [4]
- HTNG: *EMV for the US Hospitality Industry,* October 1, 2015 [5]
- PCI Security Standards Council: Understanding the Payment Card Industry Data Security Standard, version 3.2.1, May 2018 [6]
- HTNG: *GDPR for Hospitality,* June 1, 2019 [7]
- National Institute of Standards and Technology (NIST) Cybersecurity Framework, April 2018 [8]
- *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0, January 16, 2020 [1]
- NIST Special Publication (SP) 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013 [9]
- NIST SP 800-63-3, *Digital Identity Guidelines,* June 22, 2017 [10]
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personably Identifiable Information (PII),* April 2010 [11]
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,* August 2017 [12]
- Trustwave Holdings: *2019 Trustwave Global Security Report*, [13]

1.3 Benefits

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

- reduce the risk of a network intrusion compromising the PMS and preserve core operations if a breach occurs
- provide increased assurance for protecting guest information
- ensure that only personnel with a business need are given access to the PMS
- increase overall PMS security situational awareness and limit exposure of the PMS to incidents in systems that interface with it
- avoid exploitations that decrease consumer confidence of the property owner, chain, or industry
- increase consumer confidence in the protection of their sensitive data

In the hospitality space, cost is a major driving factor for many enterprise decisions, so the example implementation documented in this guide is designed to be modular. The PMS ecosystem documented here offers opportunities for an organization to choose only those components of the implementation that fit its enterprise.

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate a more secure PMS. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-27A: *Executive Summary*
- NIST SP 1800-27B: *Approach, Architecture, and Security Characteristics*–what we built and why **(this document)**
- NIST SP 1800-27C: *How-To Guide* –instructions for building the example implementation

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

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

- challenges that enterprises face in making a PMS more secure and protective of privacy
- example implementation built at the NCCoE
- benefits of adopting the example implementation

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-27B, which describes how the PMS ecosystem mitigates risk.

The following sections may be of interest to users of risk management and privacy frameworks:

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

- Section 6.2, 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.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these 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 implementing parts of a more secure PMS. Your organization's security experts should identify the 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 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.

Acronyms used in figures are in the List of Acronyms appendix.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

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

3 Approach

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 build development, testing, and security control mapping.

The NCCoE worked with hospitality organizations, such as the American Hotel & Lodging Association and 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 with the Retail and Hospitality Information Sharing and Analysis Center, offered opportunities for the NCCoE to discuss this project and solicit input from stakeholders used to shape this effort.

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
    - We considered including analytics and multifactor authentication, but ultimately we did not include these security measures.

3.1 Audience

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.

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. The example implementation demonstrated by this project will help increase the level of security around a PMS.

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

We considered the following areas determined they are outside the scope of what we documented in this project:

- 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

3.3 Assumptions

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.

3.4 Risk Assessment

For this project, Risk Management Framework Quick Start Guides [14] proved to be invaluable in 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 Information Systems and Organizations*—publicly available material [15].

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence" [16]. This guide defines risk assessment as "the process of identifying, estimating, and

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

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, configuration modification, and access to sensitive data.

3.4.1.1 External Threats

One managed security service provider's annual global security report [13] shows that the hospitality industry has the second highest number of incidents being investigated by the author's services. The same report notes that motivation or types of data targeted by malicious actors for hospitality organizations includes, in the author's words, "credit card track data, financial/user credentials, 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 internet, typically with malicious intent—are persistent threats within the hospitality industry.

3.4.1.2 Internal Threats

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]. Mitigating internal threats involves more than just physical concepts, such as locking doors; rather, the process needs to include cybersecurity concepts that help protect against insider threats and unauthorized lateral movement within the enterprise by employees and guests.

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
- delay and/or not perform patching/updating regularly
- mis-deploy assets

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

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

3.4.3 Cybersecurity Control Map

Visit Appendix A to see the security control mappings that have been identified for this project's PMS ecosystem. A Cybersecurity Framework Components Mapping table (Table A-1) shows the result from examining all the NIST Cybersecurity Framework [8] Core Subcategories and picking the Subcategories supported as a desired outcome of the PMS environment. Each of the Cybersecurity Framework Subcategories shown in the table maps to PCI DSS [6], to controls in NIST SP 800-53 rev 4 [9], and to work roles in the NICE Cybersecurity Workforce Framework [12].

3.4.4 Privacy Control Map

Visit Appendix B to see privacy control mappings that we have identified for this project's PMS ecosystem. A Privacy Framework Mapping table (Table B-1) shows the result from examining all the *NIST 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 system. We include it to draw attention to NIST's Privacy Framework, a tool for improving privacy through enterprise risk management, to enable better privacy engineering practices that support privacy by design concepts and help organizations protect individuals' privacy.

We did not run a privacy risk assessment methodology during this project on any existing PMS as a first step that would enable an organization to subsequently identify a target privacy profile. Table B-1 simply identifies the Subcategories addressed by the PMS ecosystem and indicates what component is responsible for covering the Subcategory's desired outcome.

4 Architecture

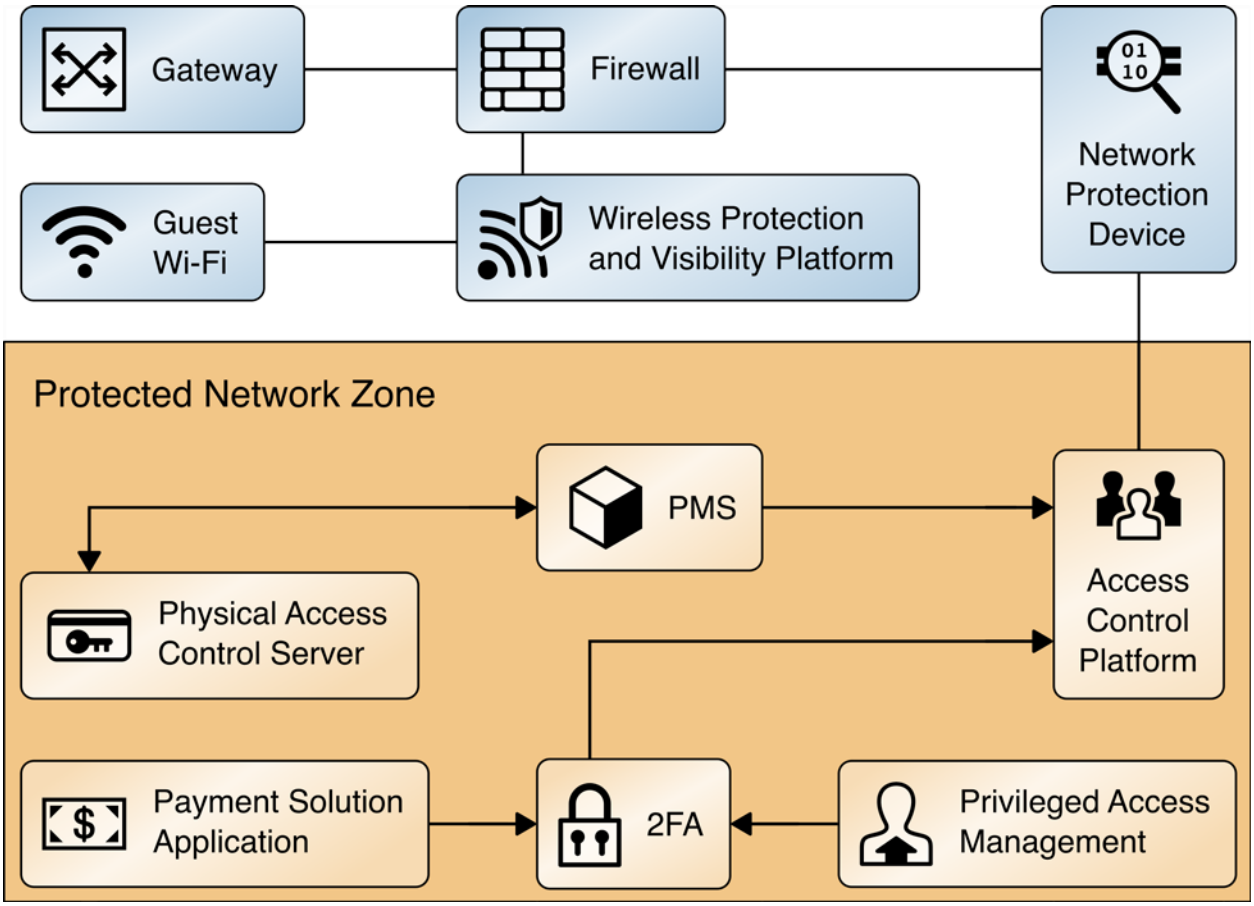
The PMS ecosystem built for this project demonstrates a typical hotel process for reservations, issuing room keys, and check-in and checkout credit card transactions. This section presents a high-level architecture and reference design for enacting such an implementation.

4.1 Architecture Description

4.1.1 High-Level Architecture

The example implementation is designed to address the security Functions and Subcategories described in Table 4-1 and is composed of the capabilities illustrated in the high-level architecture shown in Figure 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.

440 - **System protection and authentication** provides the capability to protect the functionality of the
441 PMS, including the POS system and the reservation systems. This function also employs
442 multifactor authentication, eliminates unauthorized access to data and services via dynamic
443 authorization. This also includes making the access control enforcement, on a per connection
444 basis, as granular as possible for internal and third-party users. Finally, it involves the use of
445 network segmentation, and controlling change across multiple system dimensions to increase
446 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.

4.2.1 Use Case 1: PMS Accepts Reservation

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

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 conduct any unauthorized lateral movements.

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, engineer, or system owner [9]. The action of inputting or modifying a reservation requires an authorized staffer to authenticate to gain access to the PMS.

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 is tokenized before introduction to the PMS.

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 PMS. The token is used again at checkout when the bill is paid, with only the token sent from the PMS to the PSA.

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

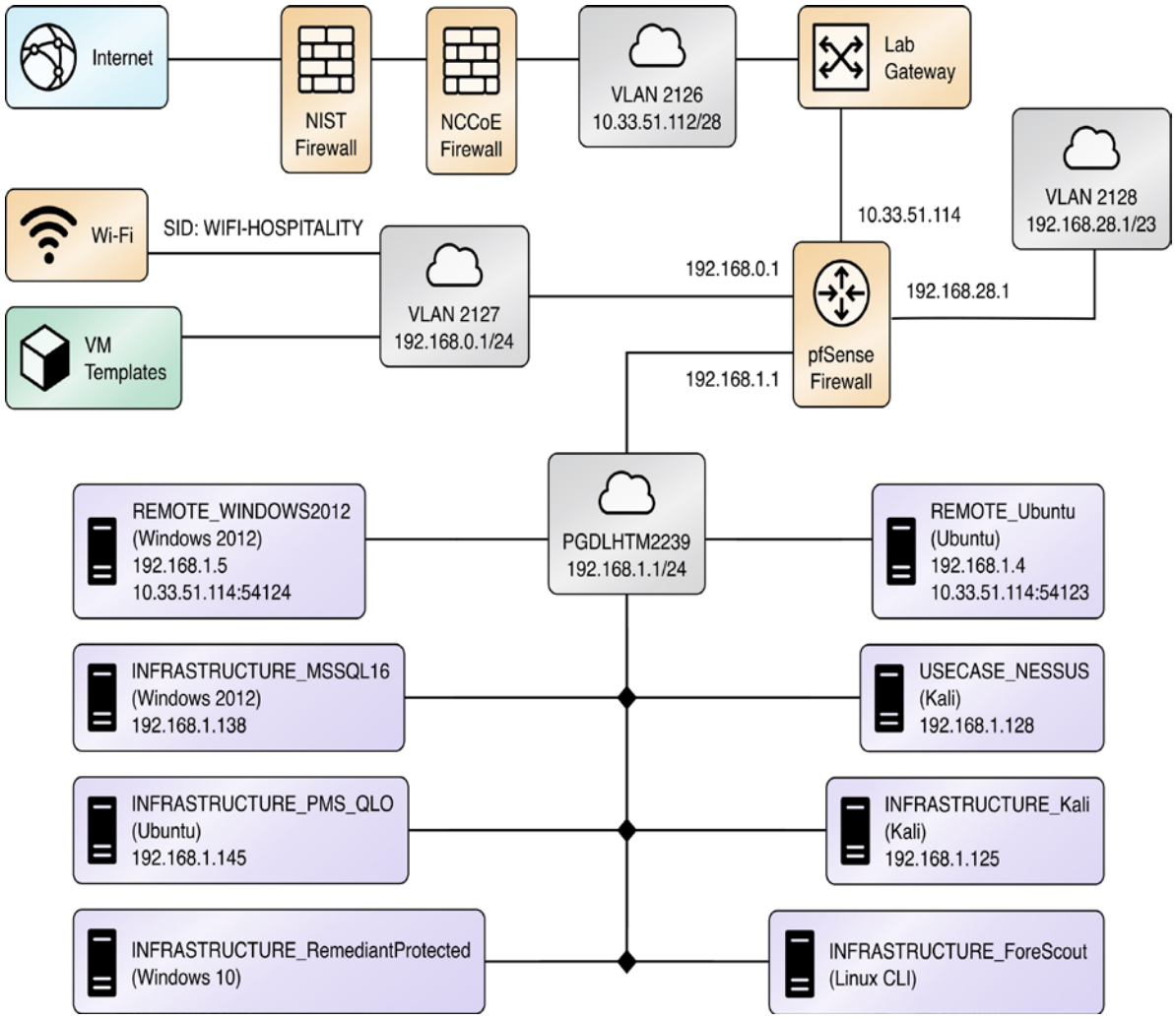
In Use Case 4, the PMS securely interacts with a physical access control system, specifically a door lock and room-key encoder.

The physical access control server is a door lock/room-key system that requires connectivity to the PMS. To encode a room key at check-in, an authorized staffer accesses the PMS to identify the assigned guest room number and provides only the room number to the physical access control server (PACS) to 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.

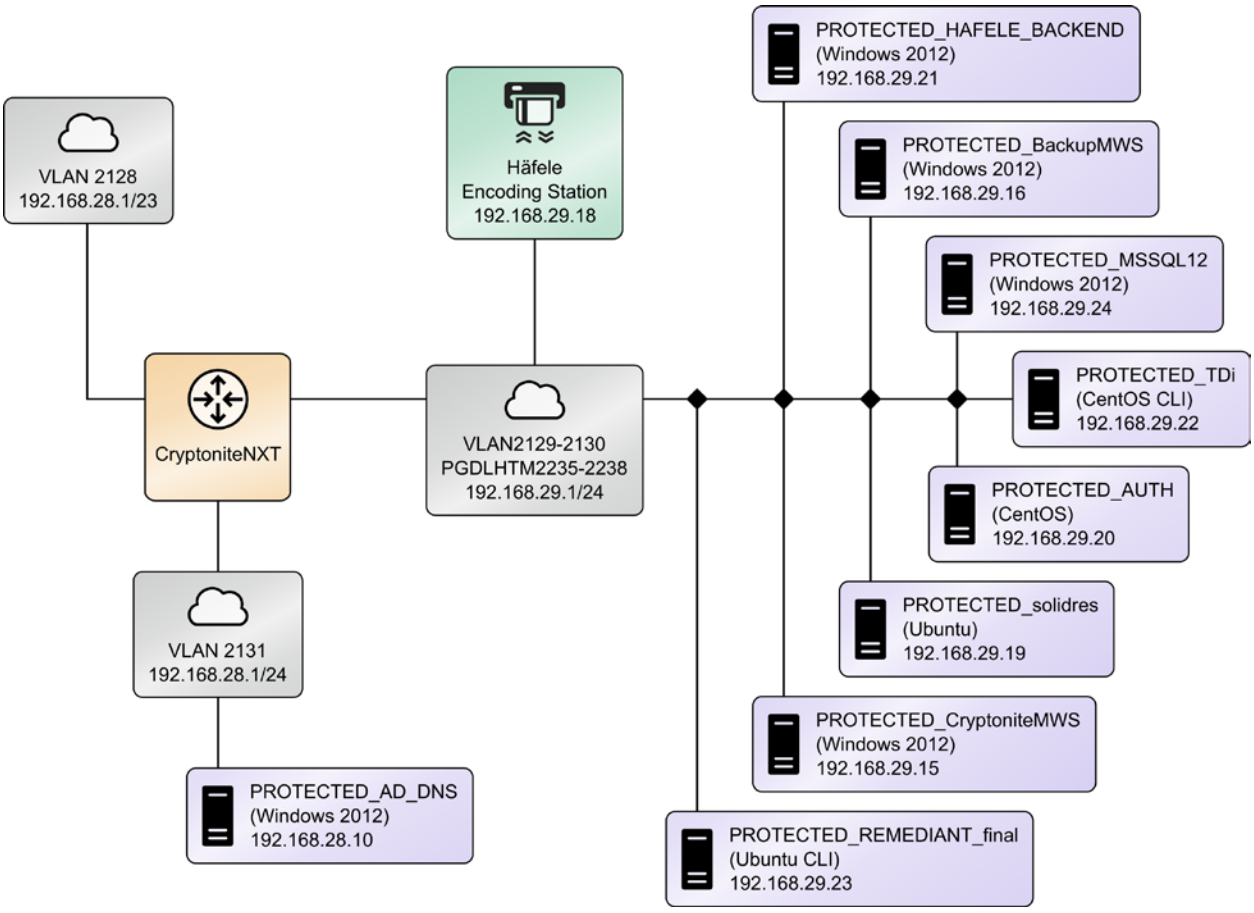
4.3 Detailed Architecture

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

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



485 **Figure 4-3 Secure PMS Reference Design (part 2 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 • 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 • 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.
498 • Häfele Dialock's physical access control system encodes and manages room keys.

4.4 Technologies

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

Table 4-1 Products and Technologies

Component	Product	Function	NIST Cybersecurity Framework Subcategories Affected	NIST Privacy Framework Subcategory Affected
PMS	Solidres Note: This is the only purchased component in this project.	heart of the hotel enterprise; facilitates the reservations process, checks customers in and out, tracks charges, and reconciles billing	N/A	N/A

Component	Product	Function	NIST Cybersecurity Framework Subcategories Affected	NIST Privacy Framework Subcategory Affected
network protection device	CryptoniteNXT Secure Zone 2.9.1	network protection appliance that works in concert with firewalls; provides additional 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.

Component	Product	Function	NIST Cybersecurity Framework Subcategories Affected	NIST Privacy Framework Subcategory Affected
access control platform	TDi ConsoleWorks 5.2-0u1	secures connection and control mechanism to enterprise devices from authorized users and authorized devices; also provides security perimeter monitoring, auditing, and logging activity down to the keystroke	**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 monitored to detect potential cybersecurity events.	**CT.PO-P3** Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.
privileged access management	Remediant SecureONE 18.06.3-ce	provides real-time incident monitoring and detection, privilege escalation management, and reporting functions for the IT enterprise	**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 records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.

Component	Product	Function	NIST Cybersecurity Framework Subcategories Affected	NIST Privacy Framework Subcategory Affected
wireless protection and visibility platform	Forescout CounterACT 8.1	provides insight into the diverse types of devices connected to the network; enforces policy-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/services are inventoried. **CT.DM-P1** Data elements can be accessed for review.
payment solution appliance	StrongKey Key Appliance	secures credit card transactions and shrinks PCI compliance enclave	**PR.AC-1** **PR.DS-1** Data a rest is protected.	**ID.IM-P8**
physical access control server	Häfele Dialock 2.0	physical access control ecosystem, including door locks, room-key encoding, and management	N/A	N/A
firewall	pfSense	exterior border protection; demarcation	N/A	N/A

4.5 Process Flows

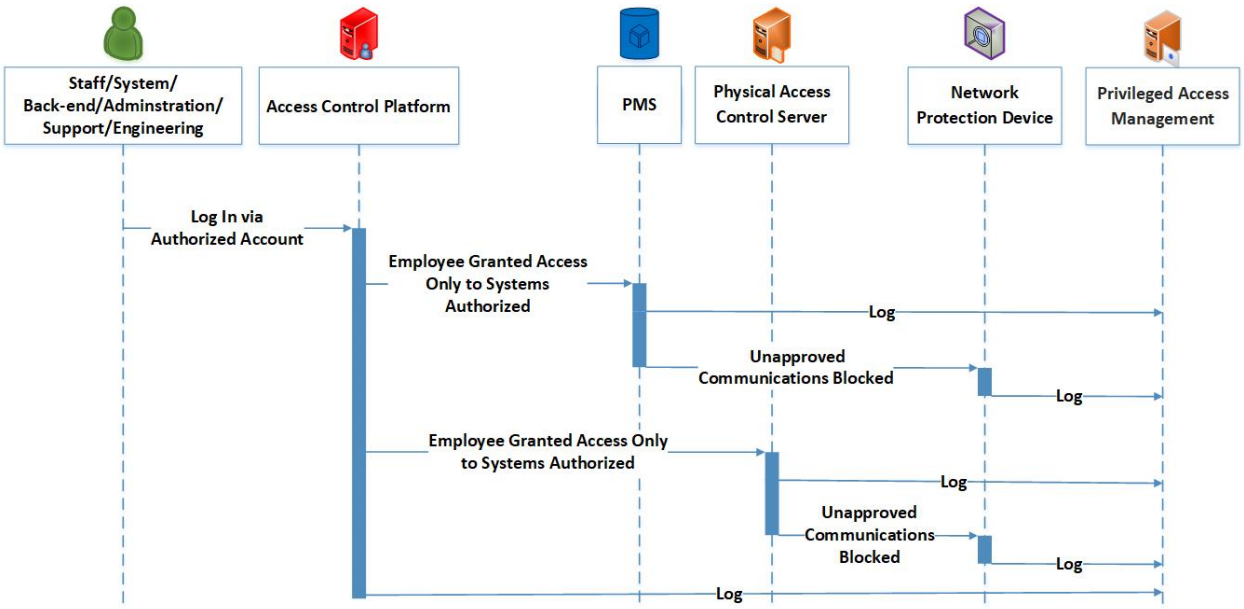
The following process flows show the sequence of events taking place for various hospitality functions in the enterprise.

4.5.1 Authorized Employee Access

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 required to present whatever credentials are required by policy; further, they will be granted only minimal access based upon their role. The process of Figure 4-4 is described below.

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

Figure 4-4 Staff Process Flow

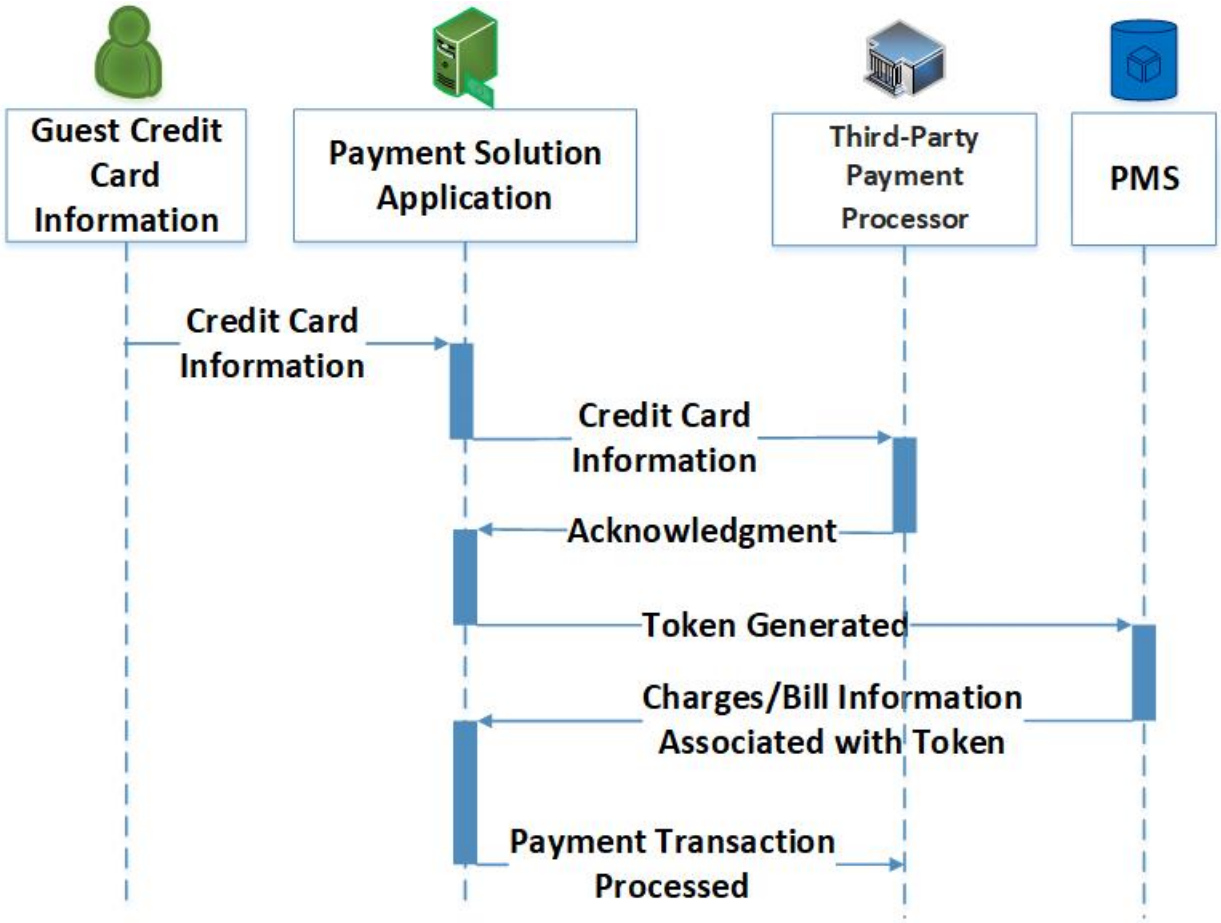


4.5.2 Secure Credit Card Transaction

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 described below.

1. The payment solution application collects the credit card information.
2. The payment solution application secures credit card information via a secure vault.
3. The payment solution application validates with a third-party payment processor.
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**

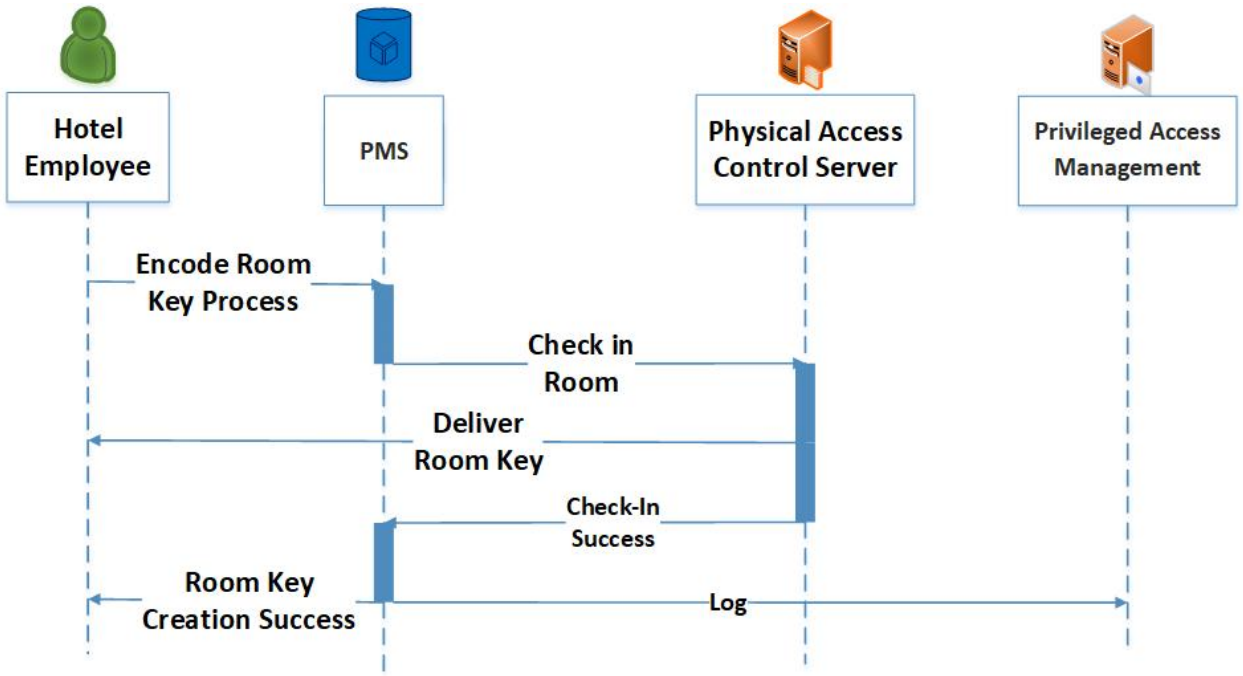


533 ### 4.5.3 Secure Interaction of Ancillary Hotel System (with PMS)

534 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.

Figure 4-6 Secure Interaction of Ancillary System with PMS Process Flow

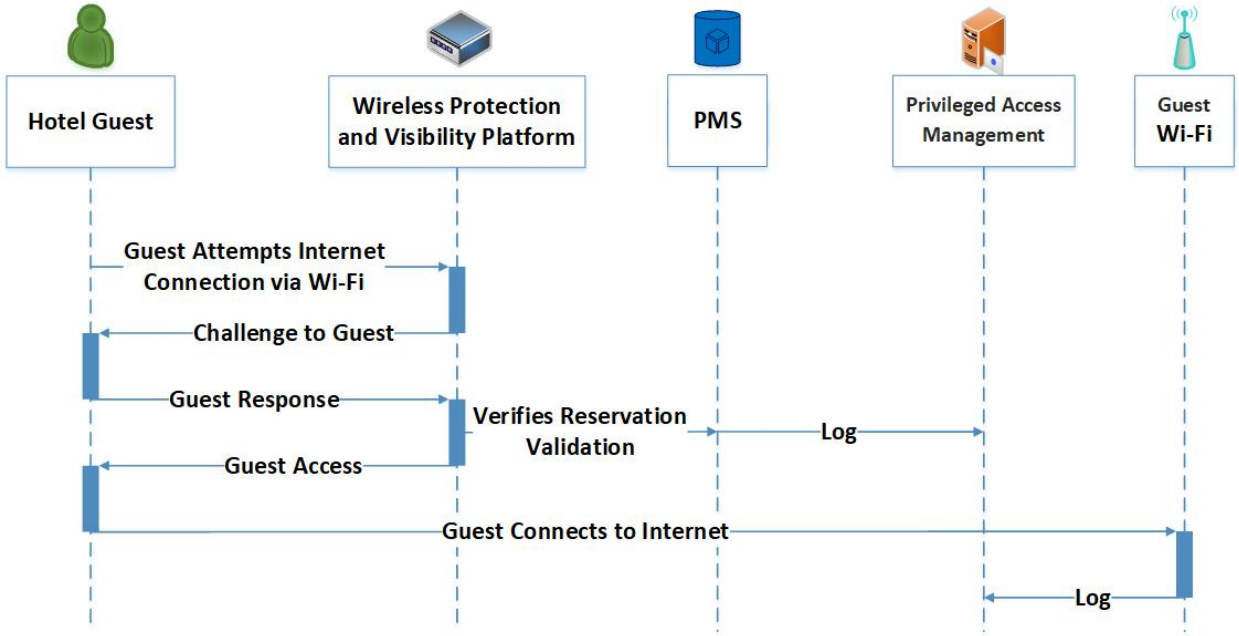


4.5.4 Guest Internet Access via Guest Wi-Fi

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

1. guest attempts to connect to the internet via the guest Wi-Fi
2. guest is challenged
3. guest responds with temporary credentials they have been provided, corresponding to their reservation
4. wireless protection and visibility platform validates with the PMS, and the guest is provided internet access
5. guest is provided only access to the internet (is forbidden to move laterally) and any external-facing enterprise hospitality systems; all activity, including surfing and web activity, is logged 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:

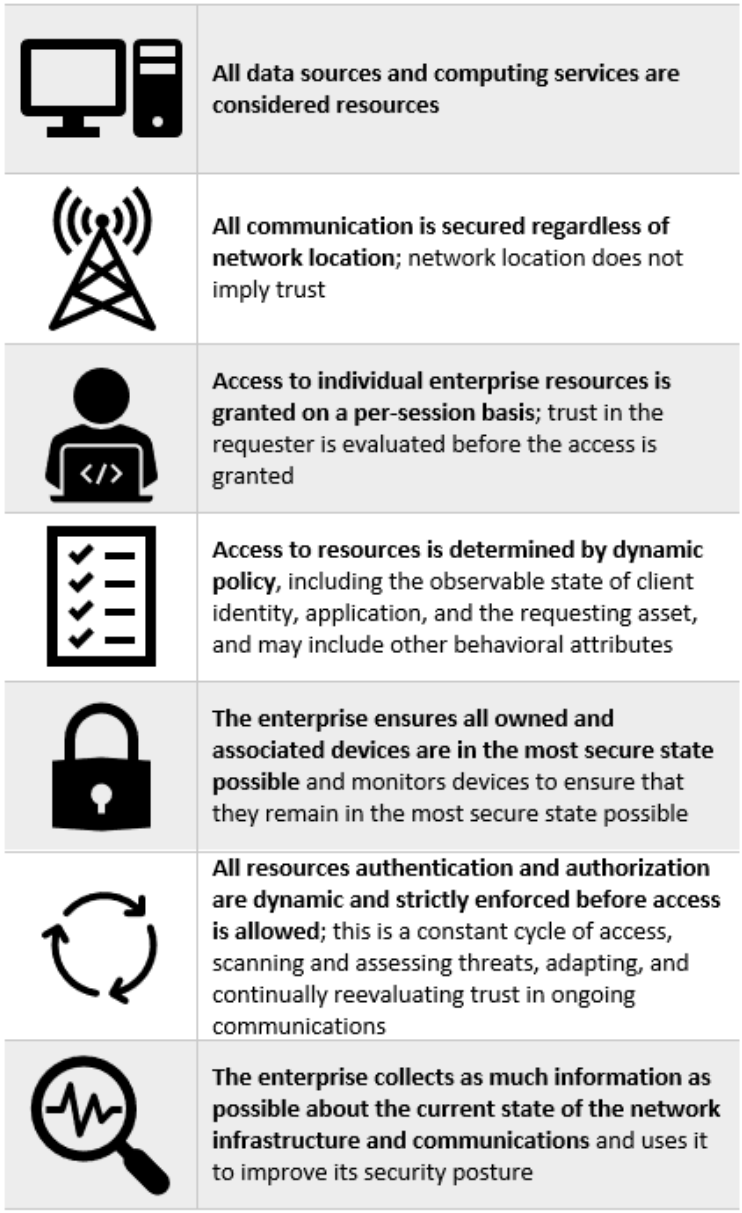
559 - It is not a comprehensive test of individual security components, nor is it a red team exercise.
560 This project did not include a comprehensive test of all security components or "red team"
561 penetration testing or adversarial emulation. Cybersecurity is a rapidly evolving field where new
562 threats and vulnerabilities are continually discovered. Therefore, this security guidance cannot
563 be guaranteed to identify every potential weakness of the build architecture. It is assumed that
564 implementers will follow risk management procedures as outlined in the NIST Risk Management
565 Framework.

566 - 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 Ecosystem Component	Cybersecurity Framework Subcategories
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 Ecosystem Component	Cybersecurity Framework Subcategories
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 authorization are dynamic and strictly enforced before access is allowed; this is a constant cycle of access, scanning and	Remediant SecureONE 18.06.3-ce	**PR.AC-1** Identities and credentials are issued, managed, verified, revoked, and audited for

Zero Trust Tenet	PMS Ecosystem Component	Cybersecurity Framework Subcategories
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.

6 Privacy Characteristic Analysis

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

6.1 Limitations

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.
- It cannot identify all weaknesses.

6.2 Privacy Protections of the Reference Design

The *NIST Privacy Framework* Core Subcategories are a basis to identify privacy characteristics that are supported by our PMS ecosystem. The PMS ecosystem architecture was designed before the *NIST Privacy Framework* [1] was developed. This section is included to draw attention to the Privacy Framework and to highlight that protecting an individual's privacy could become a core value for PMS ecosystems through more thorough use of the Privacy Framework.

See the Privacy Framework Mapping, Table B-1, in Appendix B for the technical privacy characteristics identified as being satisfied by this PMS ecosystem.

7 Functional Evaluation

7.1 Test Cases

This section includes the test cases necessary to conduct the functional evaluation of the PMS example implementation. Refer to Section 4 for descriptions of the tested example implementation.

Each test case consists of multiple fields that collectively identify the goal of the test, the specifics required to implement the test, and how to assess the results of the test. Table 7-1 describes each field in the test case.

Table 7-1 Test Case Fields

Test Case Field	Description
requirement tested	identifies the requirement to be tested and guides the definition of the remainder of the test case fields. specifies the capability to be evaluated
description	describes the objective of the test case
associated Cybersecurity Framework Subcategories	lists the Cybersecurity Framework Subcategories addressed by the test case
sub test cases	In some cases, one or more tests may be part of a larger use-case 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.

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 variations 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

7.1.1 PMS Use Case Requirements

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

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 authorized to access	PMS-03b, PMS-03c	network protection device
CR 2.c		users with partial/compromised credentials 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

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

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.

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 Framework 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 machines include front desktop, management workstation.)
disposition	pass

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 compromised accounts/credentials.

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 Framework Subcategories	DE.AE-2, DE.CM-1, DE.CM-7
sub test cases	If a "user" has only a partial credential or a compromised credential, 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. Trigger password policy by trying to log in Solidres's admin side 10 times.
expected results	Solidres admin console can be accessed successfully. Locked account 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

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

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

Table 7-5 contains test case requirements, associated test case, and descriptions of the test scenario for preventing 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 Framework 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)*

622 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 "boundary."
associated Cybersecurity Framework Subcategories	PR.PT-3, DE.CM-3
sub test cases	The user cannot perform a function for which they are not authorized, 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 privilege was given. The user was not able to add an authorization to create or save MIFARE credentials.
disposition	pass

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 ensuring that users have access only to data for which they are authorized.

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 Framework 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, download 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 information, 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

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 entering a reservation and editing the reservation.

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 Framework 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

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 for entering a reservation and editing the reservation.

Table 7-9 Provisioning Room Key

Test Case Field	Description
requirement tested	(CR 1) room key provisioned
description	From the reservation in the PMS, verify that a room key is provisioned 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
procedure	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 making sure that the assigned key-card room number and guest-registered room number are the same.
expected results	Provisioned room key works.
actual results	Room keys were provisioned.
disposition	pass

7.1.7 Provisioning Guest Wi-Fi Access

The following two test cases will validate provisioning guest Wi-Fi access and that guests cannot access the restricted enterprise from the Wi-Fi.

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 for preventing lateral movement.

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 Framework 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 connected; 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)*

645 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 Framework 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 connected; 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

7.1.8 Secure Credit Card Transaction

The following two test cases validate secure credit card transactions.

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 for tokenizing credit card data for a credit card transaction.

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 Framework Subcategories	N/A
sub test cases	Validate that credit card data was tokenized; validate that additional charges can be recorded using the token; validate that the token can be reconciled for payment; validate that the token encrypts 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 reservations, click the test reservation, validate credit card information 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 offline 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

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 for verifying that credit card data is hidden.

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 Framework 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

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.

Table 7-14 Authorized Device Provisioning

Test Case Field	Description
requirement tested	(CR 5) Authorized device can connect/unauthorized device cannot connect.
description	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
preconditions	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

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 for preventing an authorized device form connecting to the enterprise.

Table 7-15 Prevent Unauthorized Device from Connecting

Test Case Field	Description
requirement tested	(CR 5) Authorized device can connect/unauthorized device cannot connect.
description	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.
procedure	Add a machine to the secure enclave Virtual Local Area Network (VLAN) (simulates connecting to the network). From the connected 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

8 Future Build Considerations

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 1800-4, *Mobile Device Security: Cloud and Hybrid Builds*), smart rooms, and IoT. Subsequent work may

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.

Appendix A Mapping to Cybersecurity Framework

Table A-1 shows the National Institute of Standards and Technology (NIST) Cybersecurity Framework Subcategories that are addressed by the property management system (PMS) ecosystem built in this practice guide. The first three categories show the Cybersecurity Framework details. The next three categories show how the Cybersecurity Framework Subcategories are related to requirements in Payment Card Industry Data Security Standard (PCI DSS) v3.2.1; security and privacy controls in NIST Special Publication (SP) 800-53r4; and work roles in NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [12]. This table is included to help connect those with expertise in any of these areas and illuminate areas that the PMS ecosystem. 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 PCI requirement or NIST SP 800-53 control [9] may match areas of focus within an organization that 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		
Function	**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]**
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and man-	**ID.AM-1:** Physical devices and systems within the organization are inventoried.		CM-8, PM-5	Technical Support Specialist (OM-STS-001)
		ID.AM-2: Software platforms and applications within the organization are inventoried.		CM-8, PM-5	Technical Support Specialist (OM-STS-001)

	aged consistent with their relative importance to organizational objectives and the organization's risk strategy.				
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. 3.6.1 Generate strong keys. 3.6.2 Keys are only distributed to authorized recipients. 3.6.3 Stored keys are stored encrypted. 3.6.4 A reasonable crypto period shall be set. 3.6.5 A key life cycle shall be established, 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: Remote access is managed.	8.1.5 Manage IDs used by third parties to access, support, or maintain system components 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: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	Technical Support Specialist (OM-STS-001)
			7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.		Technical Support Specialist (OM-STS-001)

			7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.		
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	1.1 Establish and implement firewall and router configuration standards.	AC-4, AC-10, SC-7	Network Operations Specialist (OM-NET-001)
			1.1.4 requirements for a firewall at each internet connection and between any demilitarized zone (DMZ) and the internal network zone		Network Operations Specialist (OM-NET-001)
			1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.		Network Operations Specialist (OM-NET-001)

			1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.		Network Operations Specialist (OM-NET-001)
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	8.1.6 Limit the number of failed login attempts. 8.1.7 Establish a reasonable "cool down period" for locked-out accounts prior to automatic unlocking processes. 8.1.8 Reasonable idle time prior to workstation lockout shall be established. 8.2 Where appropriate, multifactor authentication (two or more of something you know, something you have, and something you are) shall be implemented. 8.2.1 Authentication transactions and data are encrypted at rest and in transit.	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 Planner (SP-SRP-001)

		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational 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 Planner (SP-SRP-001)
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data at rest is protected.	3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.	MP-8, SC-12, SC-28	Information Systems Security Developer (OM-DTA-002)
			3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This		Information Systems Security Developer (OM-DTA-002)

			data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.		
			3.2.2 Do not store the card verification 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 transactions) after authorization.		Information Systems Security Developer (OM-DTA-002)
			3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.		Information Systems Security Developer (OM-DTA-002)
			3.4 Render Primary Account Number unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:		Information Systems Security 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 Security Developer (OM-DTA-002) Cyber Defense Analyst (PR-CDA-001) Information Systems Security Developer (OM-DTA-002) Cyber Defense Analyst (PR-CDA-001)
		PR.DS-5: Protections against data leaks are implemented.		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 Procedures (PR.IP): Security 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 address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	maintained, incorporating security principles (e.g., concept of least functionality).			
		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 security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	AC-3, CM-7	Privacy Officer/Privacy Compliance Manager (OV-LGA-002)
		PR.PT-4: Communications 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-41, SC-43	
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of events is understood.	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods.		AU-6, CA-7, IR-4, SI-4	Cyber Defense Analyst (PR-CDA-001)
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.		AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	Cyber Defense Analyst (PR-CDA-001)
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.		CA-7, PE-3, PE-6, PE-20	Network Operations Specialist (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): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-4: Event detection information is communicated.	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 so that they are auditable. 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 Subcategory	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/products/services, including components, roles of the component owners/operators, and interactions of individuals or third parties with the systems/products/services.	CryptoniteNXT Secure Zone 2.9.1 StrongKey KeyAppliance
Control-P	Data Processing Management (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, documented, implemented, and reviewed in accordance with policy and incorporating the	Remediant SecureONE 18.06.3-ce

Privacy Framework Function	Privacy Framework Category	Privacy Framework Subcategory	PMS Ecosystem Component
		principle of data minimization.	

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
IoT	Internet of Things
IP	Internet Protocol
IT	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. SOURCE: NIST SP 800-37 Rev. 2
Privilege	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: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf.

[2] Hotel Technology Next Generation (HTNG). *Secure Payments Framework for Hospitality,* version 1.0. Feb. 2013. Available: https://cdn.ymaws.com/htng.site-ym.com/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/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_2010B_PaymentsWG_Paymen.pdf.

[5] HTNG. *EMV for the US Hospitality Industry*. Oct. 1, 2015. Available: https://cdn.ymaws.com/sites/htng.site-ym.com/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/2015-09-23_EMV_White_Paper.pdf.

[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: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[9] 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: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[10] P. Grassi et al., Digital Identity Guidelines, NIST SP 800-63-3, NIST, Gaithersburg, Md., June 22, 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[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: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

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

[13] Abbasi et al., *2019 Trustwave Global Security Report*, 2019 Trustwave Holdings, Inc. Available: https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/.

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

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

[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: https://www.socialtables.com/blog/hospitality/cyber-security-hotels/.

[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: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/cr-mfa-nist-sp1800-17.pdf.

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

DISCLAIMER

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

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

FEEDBACK

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

Comments on this publication may be submitted to: hospitality-nccoe@nist.gov

Public comment period: September 14, 2020 through October 28, 2020.

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

The NCCoE at NIST built a PMS ecosystem in a laboratory to explore methods for improving the cybersecurity of a PMS. The scope of the PMS ecosystem included the PMS, a credit card payment platform, and an analogous ancillary hotel/PMS system. In this example implementation, a physical access control system was used as the ancillary system.

The principal capabilities are to protect sensitive data, to enforce role-based access control, and to monitor for anomalies. The principal recommendations and best practices are implementing cybersecurity concepts such as zero trust, moving target defense, tokenization of credit card data, and role-based authentication.

The PMS ecosystem outlined in this guide encourages hoteliers and similar stakeholders to adopt effective cybersecurity concepts by using standard components that are composed of open-source and commercially available components.

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

Technology Partner/Collaborator	Build Involvement
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

Contents

List of Figures

List of Tables

1 Introduction

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 reference design. We do not re-create the product manufacturers' documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our environment.

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

1.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

1.2 Practice Guide Structure

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

This guide contains three volumes:

- NIST SP 1800-27A: *Executive Summary*
- NIST SP 1800-27B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-27C: *How-To Guides* – instructions for building the example solution **(you are here)**

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary,* NIST SP 1800-27A, which describes the following topics:

- challenges that enterprises face in making a PMS more secure
- example solution built at the NCCoE
- benefits of adopting the example solution

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

- 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.

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, NIST SP 1800-27C, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a more secure PMS. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 1.3.2, Architectural Overview,

lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

Acronyms used in figures and tables are in the appendix List of Acronyms.

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.

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.

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.

1.3.2 Architectural Overview

The *Securing Property Management Systems* high-level reference architecture is illustrated in Figure 1-1a and Figure 1-1b. These figures show the technologies used in the PMS ecosystem. The architecture displays the authentication mechanisms, protected network zones, privilege management, and hospitality enterprise functionality.

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, secure storage, and secure Wi-Fi.

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 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 implementations will vary, and the implementation decisions made in this build between virtual and physical will not necessarily align with every hospitality organization's policies and designs.

The example build implementation uses the components listed in Table 1-1 and shown in Figure 1-1a PMS Ecosystem High-Level Architecture and Figure 1-1b PMS Ecosystem Architecture Detailed.

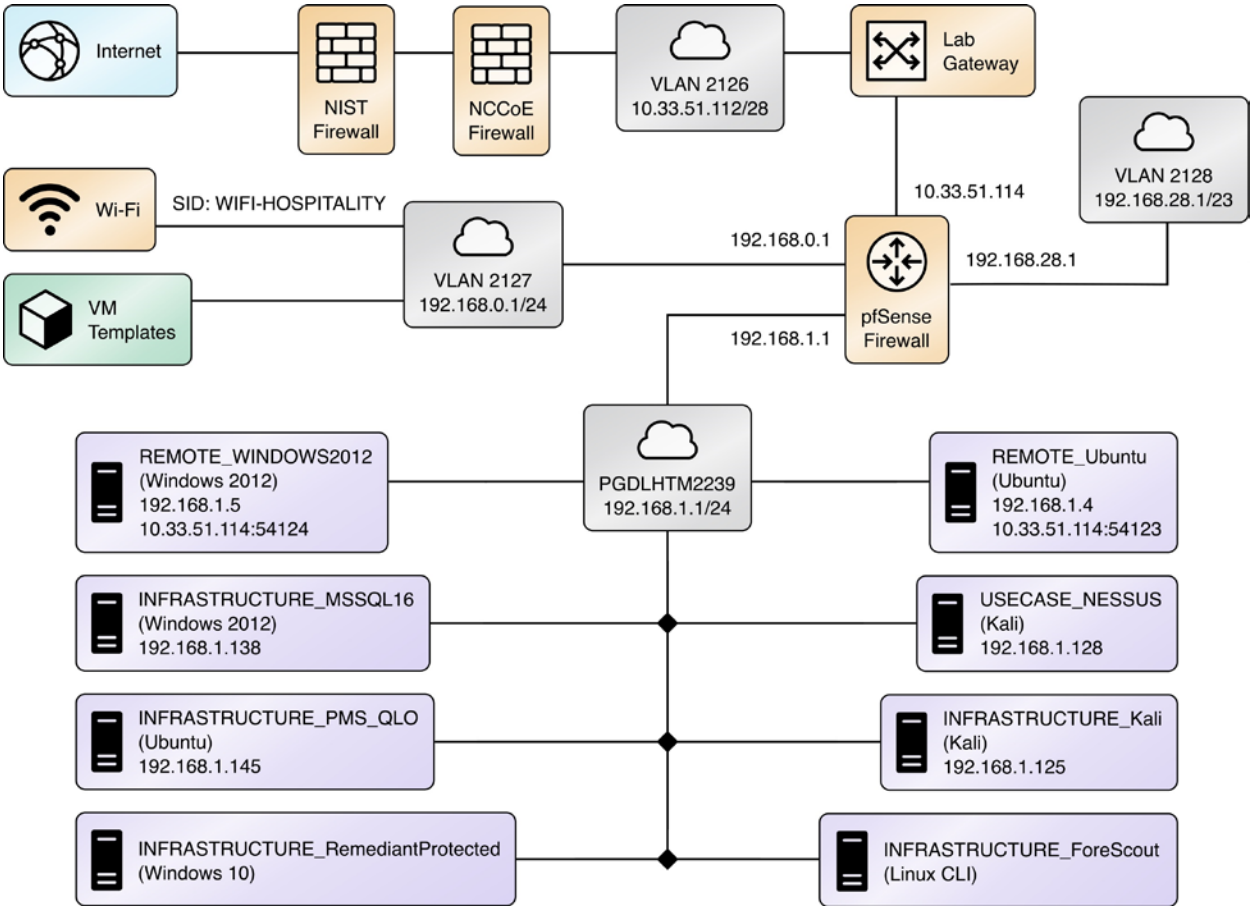
Table 1-1 Architecture List of Components

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

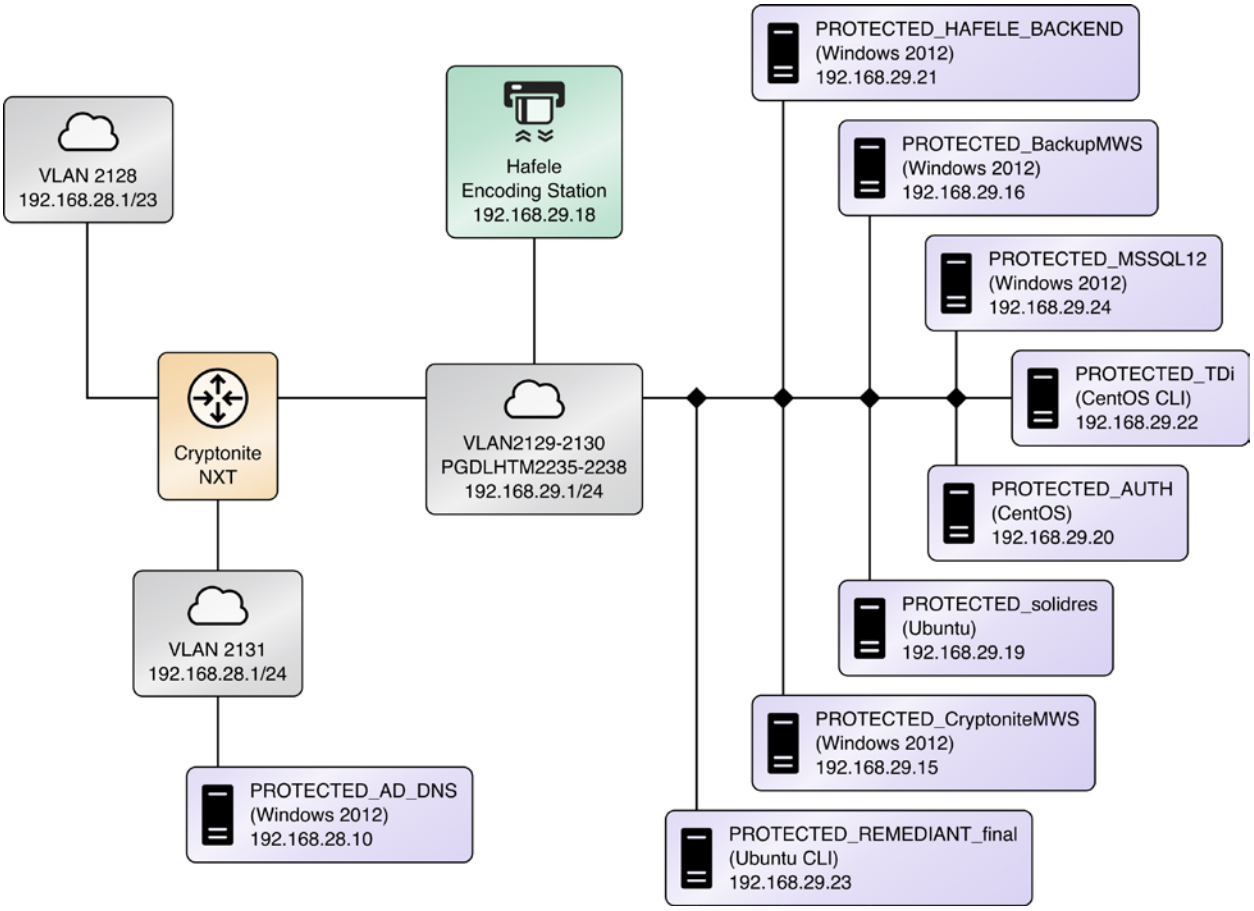
1.3.3 General Infrastructure Details and Requirements

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 Network) 2128 device as the connector between the two figures. The installation and configuration 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

254

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 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.

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*

The network adapter configuration for the DNS server is as follows:

- 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 Name Servers: 192.168.28.10
- DNS-Search Domains: hotel.nccoe

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.

2.1 Network Protection Solution—CryptoniteNXT

This section of the guide provides installation and configuration guidance for the network protection 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.

CryptoniteNXT is the network protection solution used in the example implementation.

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 serves as the router and switch for the enterprise network. However, apply the steps to secure the enterprise, as described in Section 2.1.8, to a component after the component has been separately installed and configured within the CryptoniteNXT environment.

2.1.1 Overview of Network Protection Solution

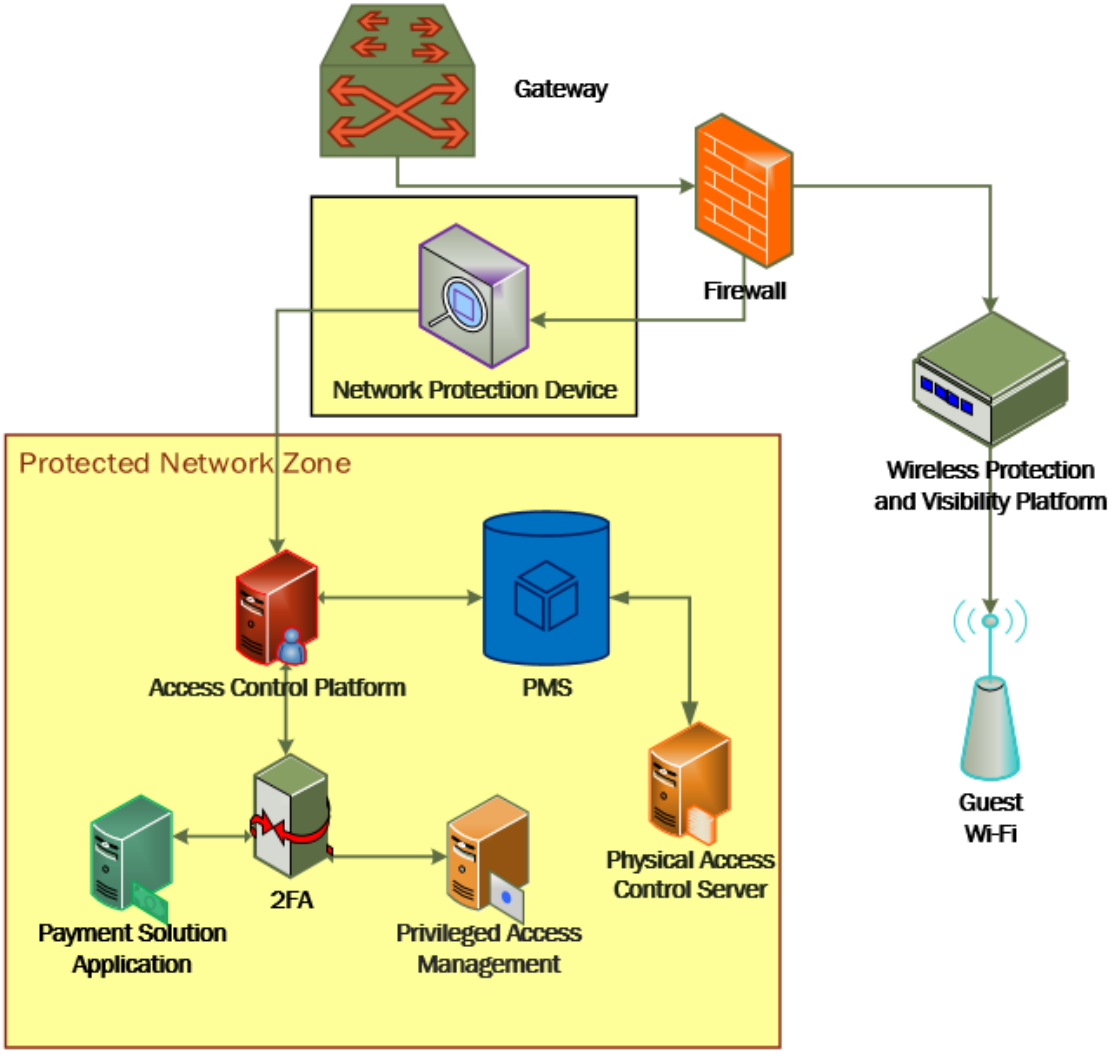
CryptoniteNXT is employed here as the network protection solution device and brings zero trust architecture and moving target defense capabilities to the PMS ecosystem.

CryptoniteNXT is a network appliance installed as a physical device in the NCCoE hospitality lab. Installation instructions are included in the packaging that comes with the CryptoniteNXT device. The device is also available as a virtual appliance.

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 philosophy to its protected network zone. Zero trust architecture is an architectural approach that focuses on data protection and role-based authentication. Its goal is to eliminate unauthorized access to data, coupled with making the access control enforcement as granular as possible.

The moving target defense capability of the CryptoniteNXT device anonymizes IP addresses to prevent a malicious actor from mapping the enterprise network. The protected network zone controlled by 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

293 The following subsections document the software, hardware, and network requirements for the
294 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

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

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, such as PuTTY, to fully install and configure the device.

2.1.2.3 Network Requirements for the Network Protection Solution

CryptoniteNXT requires the necessary physical and virtual hardware to allow all virtual end points to connect to it, fulfilling the purpose of a network switch and router. A connection is required to the upstream gateway that leads to the hotel's wireless network, and to the internet. Furthermore, CryptoniteNXT relies on access to a dedicated local area network (LAN) or VLAN with the sole purpose of providing intercommunication between the CryptoniteNXT nodes.

2.1.3 Network Protection Solution-—CryptoniteNXT–Installation

The majority of the installation and setup for the CryptoniteNXT device can be found in the CryptoniteNXT Unified Installation Guide. IP addresses and host names used in this solution are listed in Section 1.3.3 of this document. Properly configuring CryptoniteNXT to secure an enterprise requires 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 group defines the connections that an end point is allowed to make. Find more information in the CryptoniteNXT Administration Control Center (ACC) User Manual. Sections 2.1.4 and 2.1.5 have detailed instructions to create and apply a generic source and destination group.

The configuration procedure consists of the following steps:

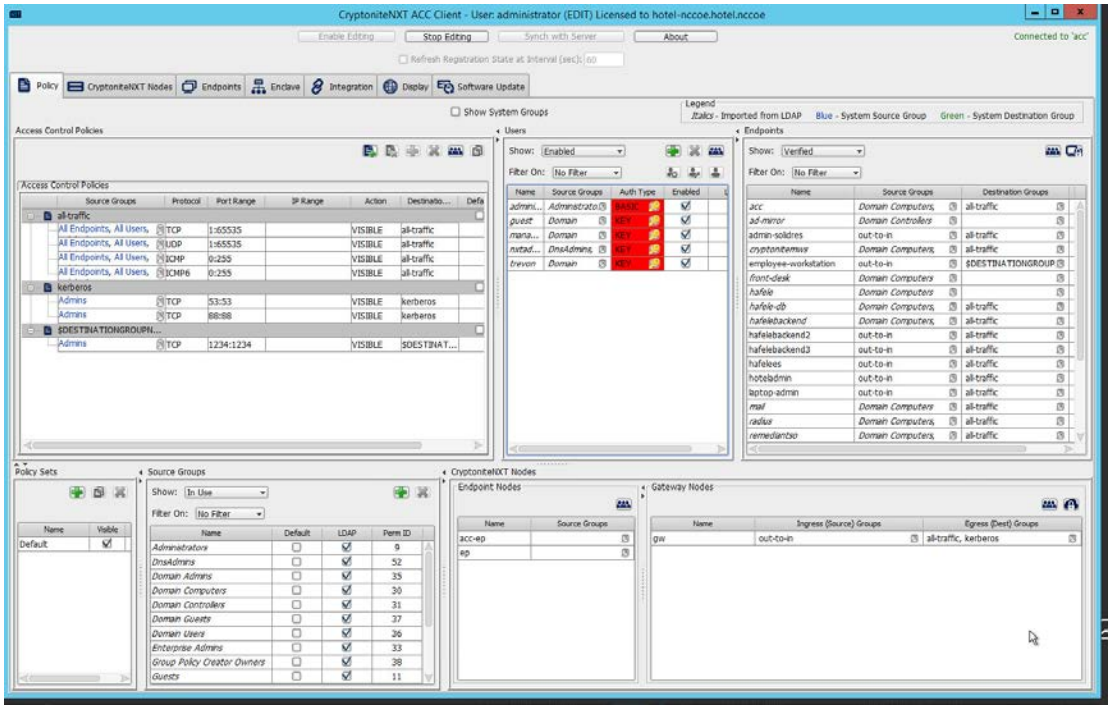
1. Create a source group to govern what network connections can flow from an end point.
2. Create a destination group to govern what network connections can flow to an end point.
3. Apply a source group to a specific end point.
4. Apply a destination group to a specific end point.
5. Create and apply the necessary source and destination groups to correctly support the hotel enterprise, as detailed below.

2.1.4 Creating Source Groups

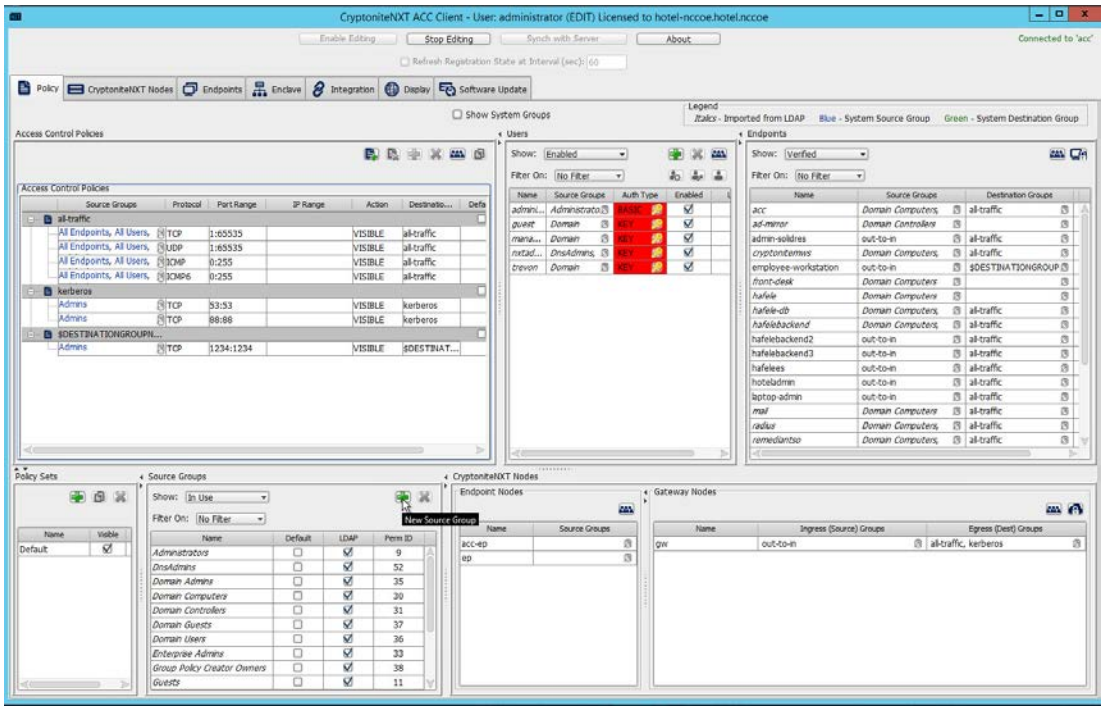
The following instructions assume that initial installation and configuration of the CryptoniteNXT device have been completed, as detailed in the CryptoniteNXT Unified Installation Guide. Once completed, open the CryptoniteNXT ACC GUI executable from a connected end point, and click the Policy tab to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

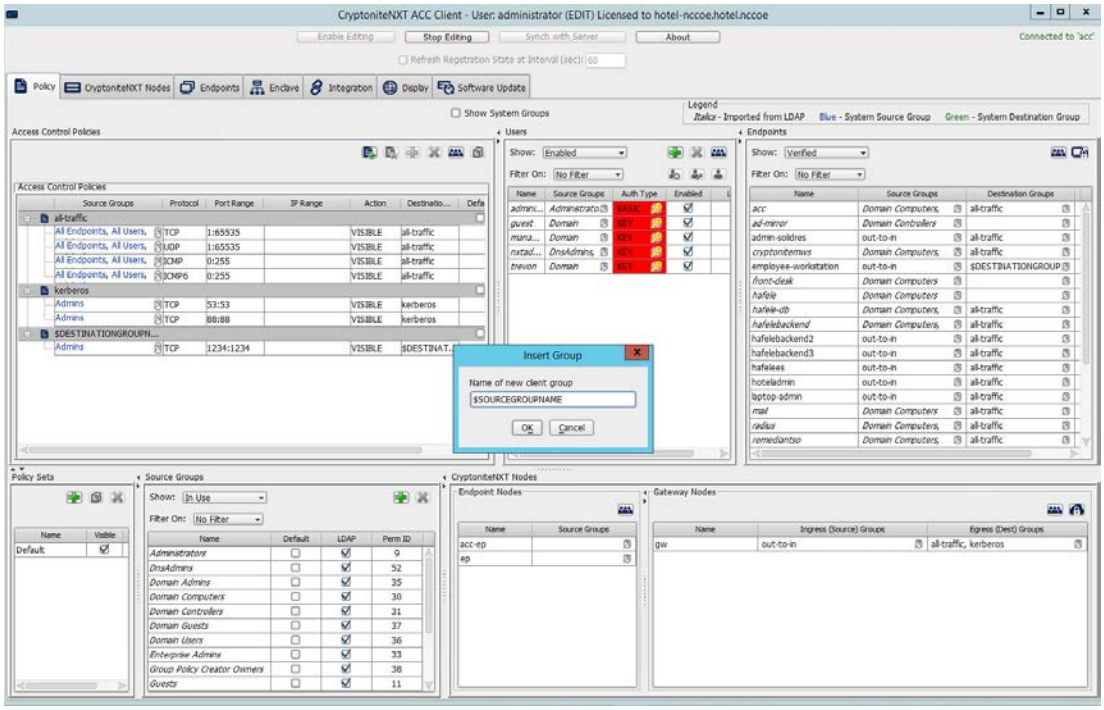


2. Under the **Source Groups** box, select the green plus button in the top right (hover text: New Source Group):



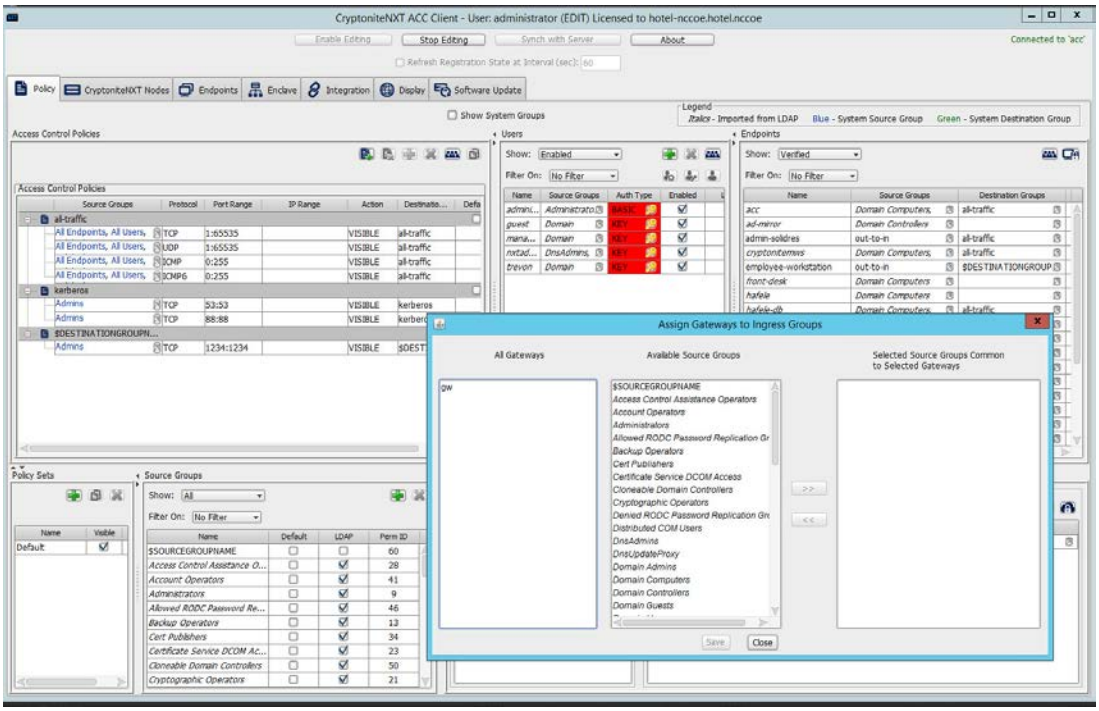
338

339 3. Input the desired source group name:

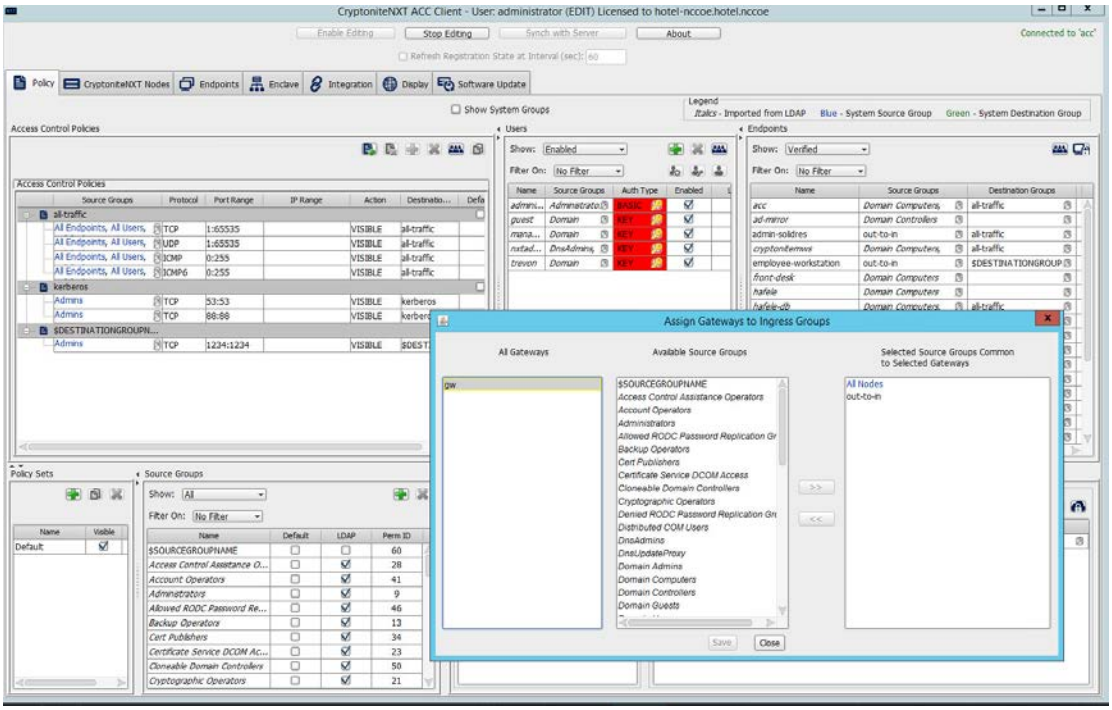


4. Click **OK**.

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

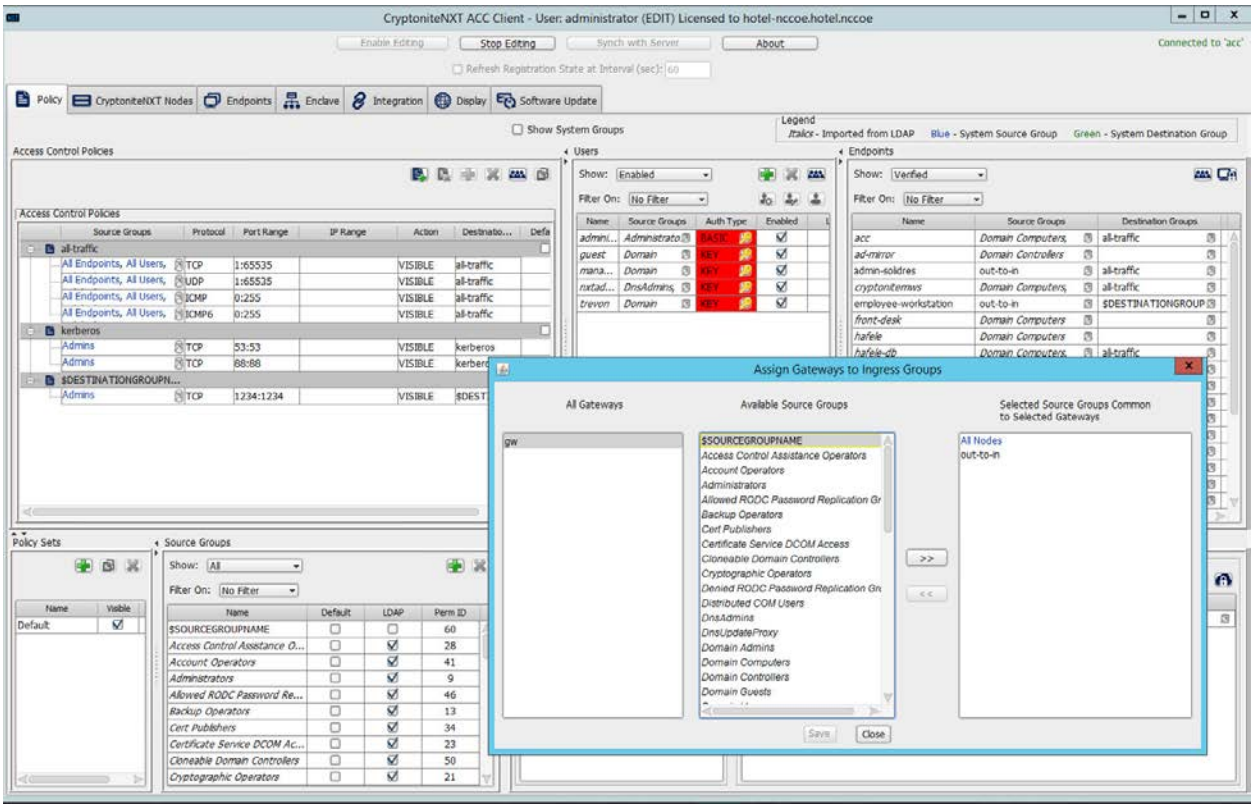


6. Select the desired gateway under **All Gateways:**



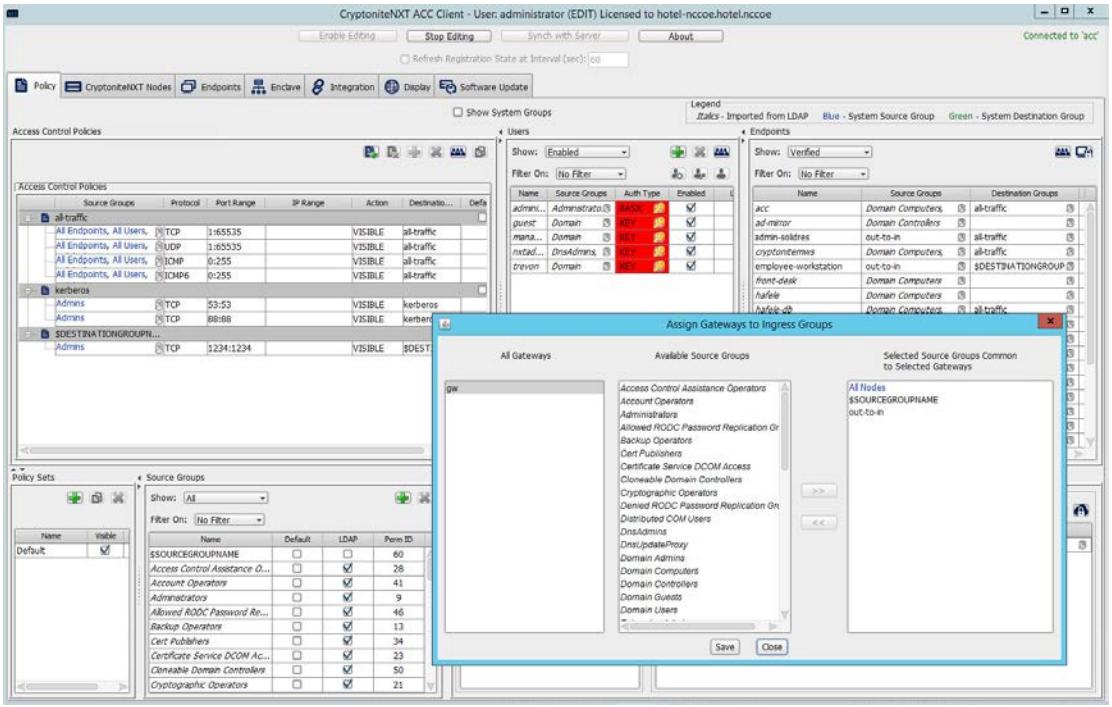
345

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



347

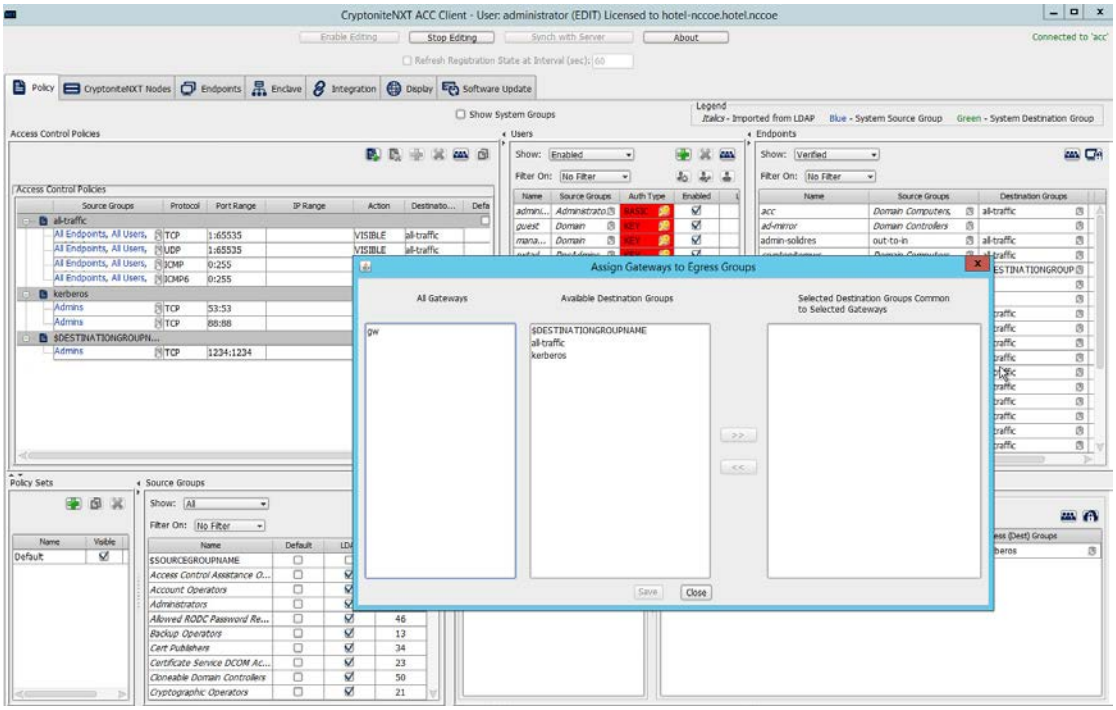
348 8. Click **>>**:



349

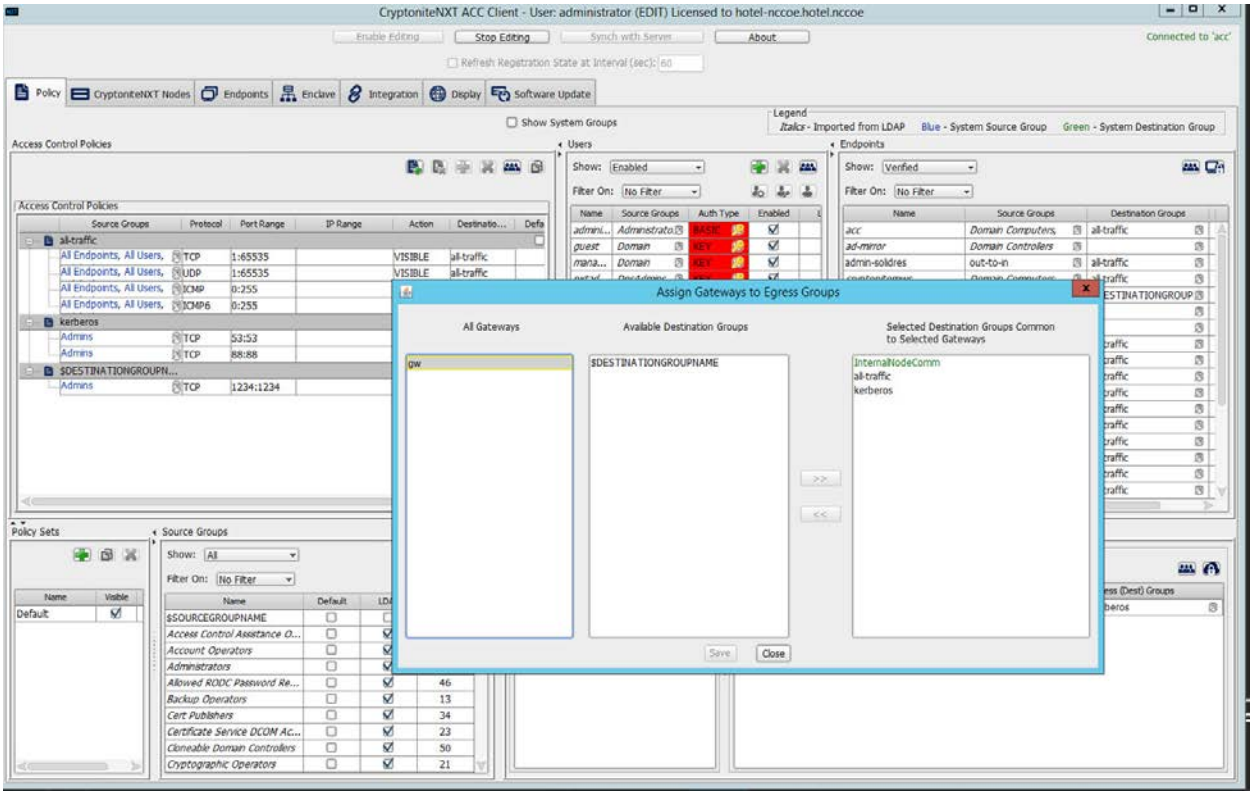
350 9. Click **Save**.

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



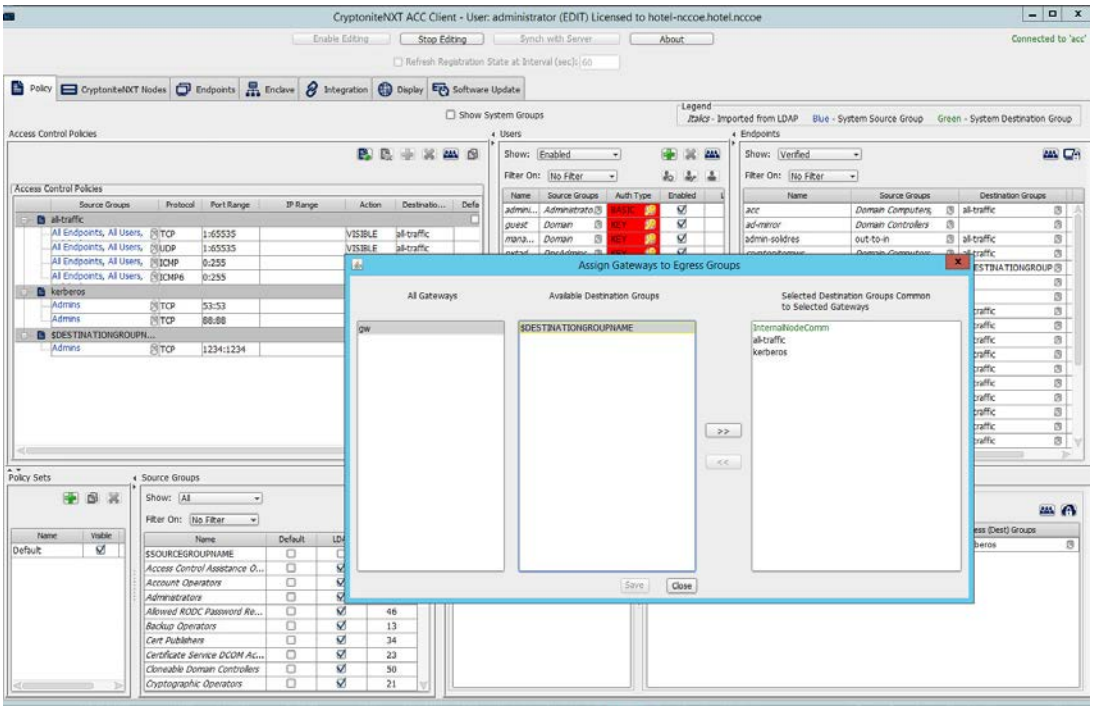
352

353 11. Select the desired gateway under **All Gateways**:



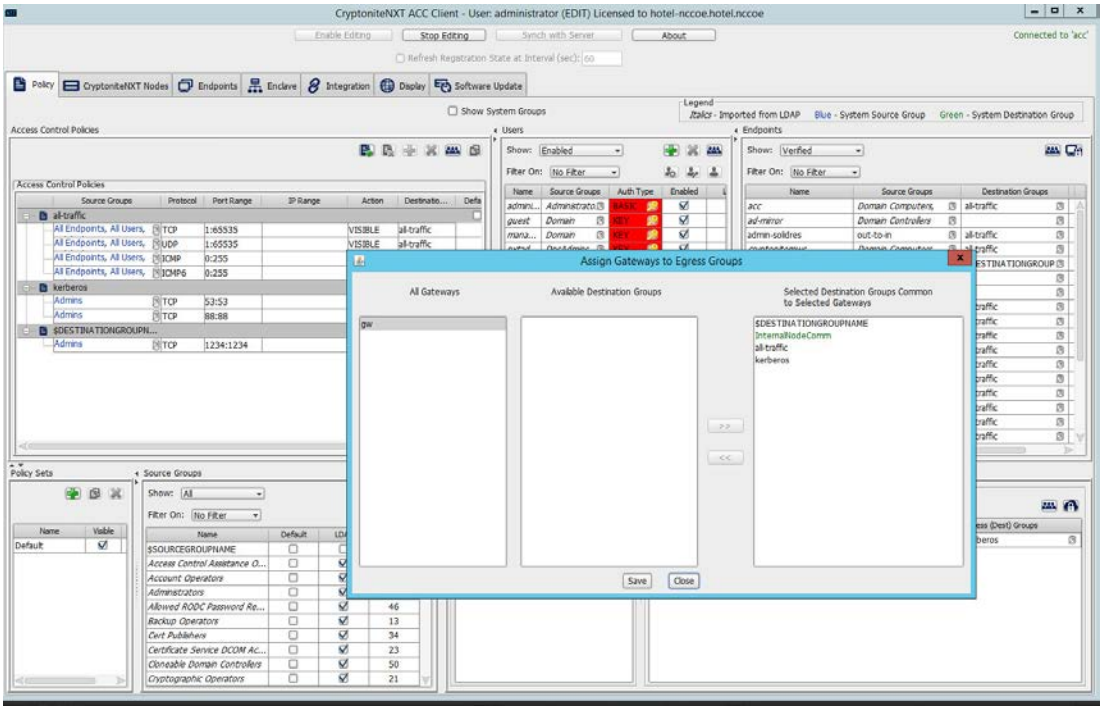
354

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



357

358 13. Click **>>:**



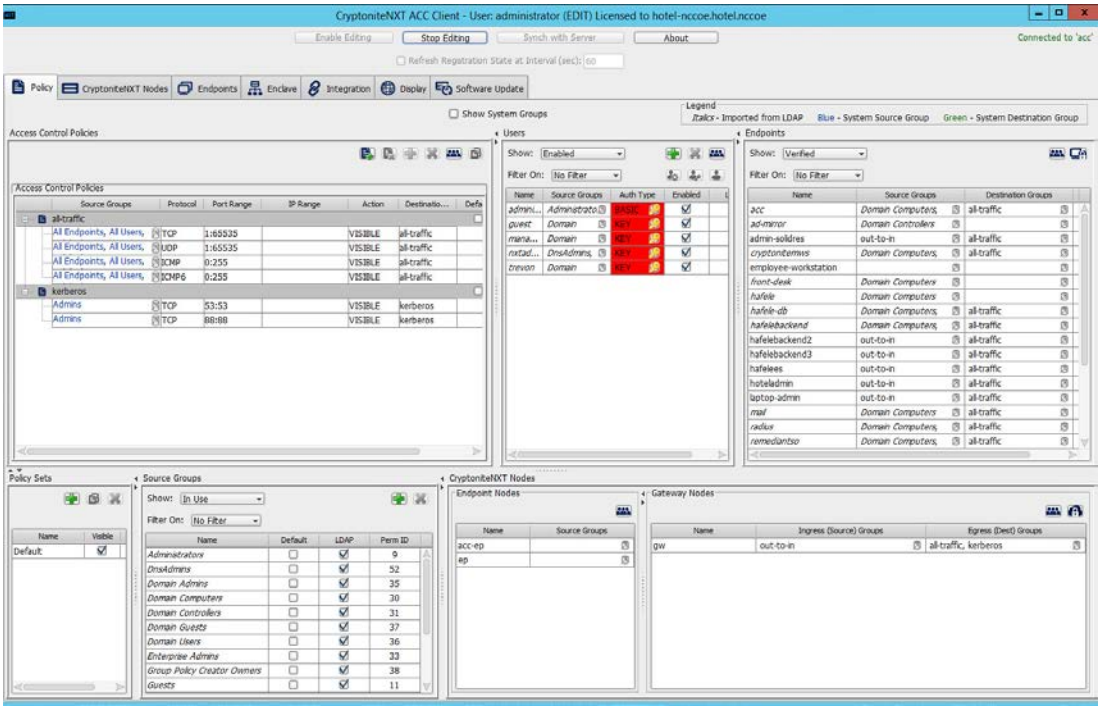
359

14. Click **Save.**

2.1.5 Creating Destination Groups

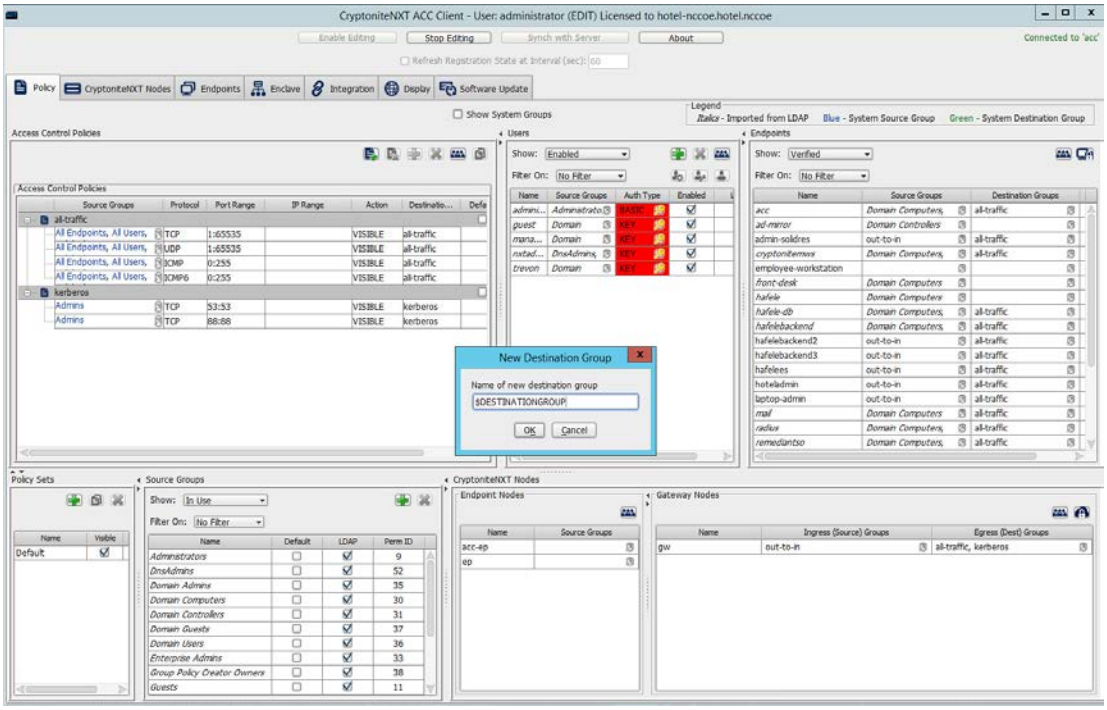
The following instructions detail creation of a generic destination group. They assume the same access to the CryptoniteNXT ACC GUI as in the previous instructions.

1. Click **Enable Editing**:



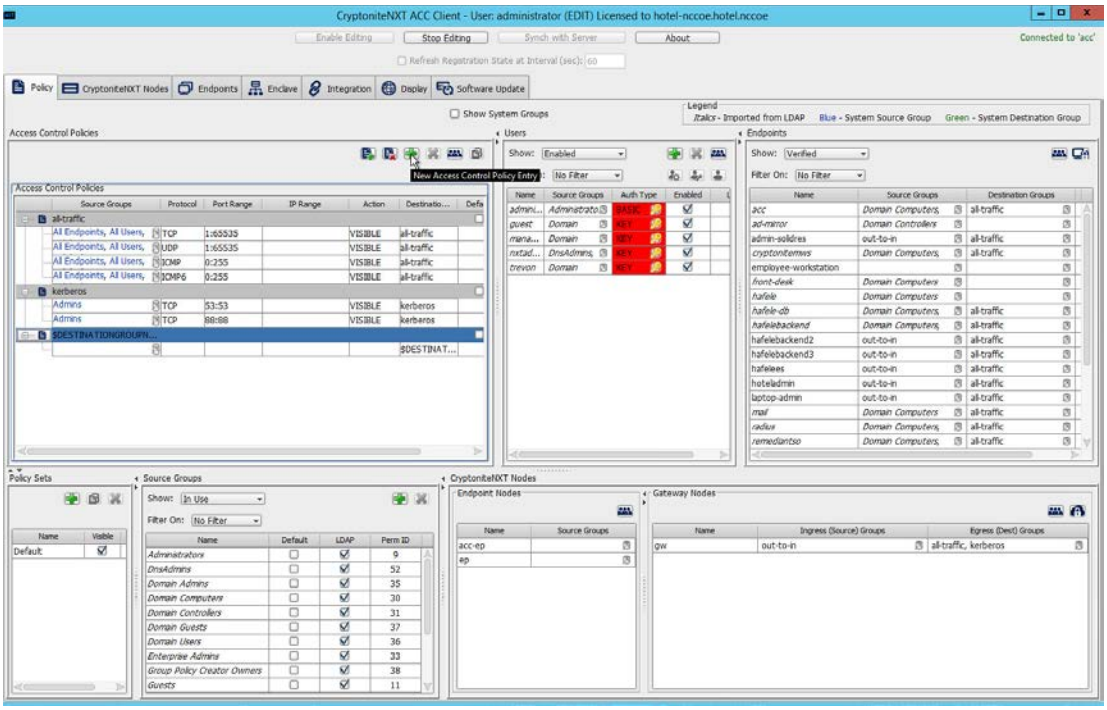
2. Under **Access Control Policies,** click the left-most icon depicting a piece of paper and a green plus sign (hover text: New Destination Group).

3. Create the name of a new destination group:



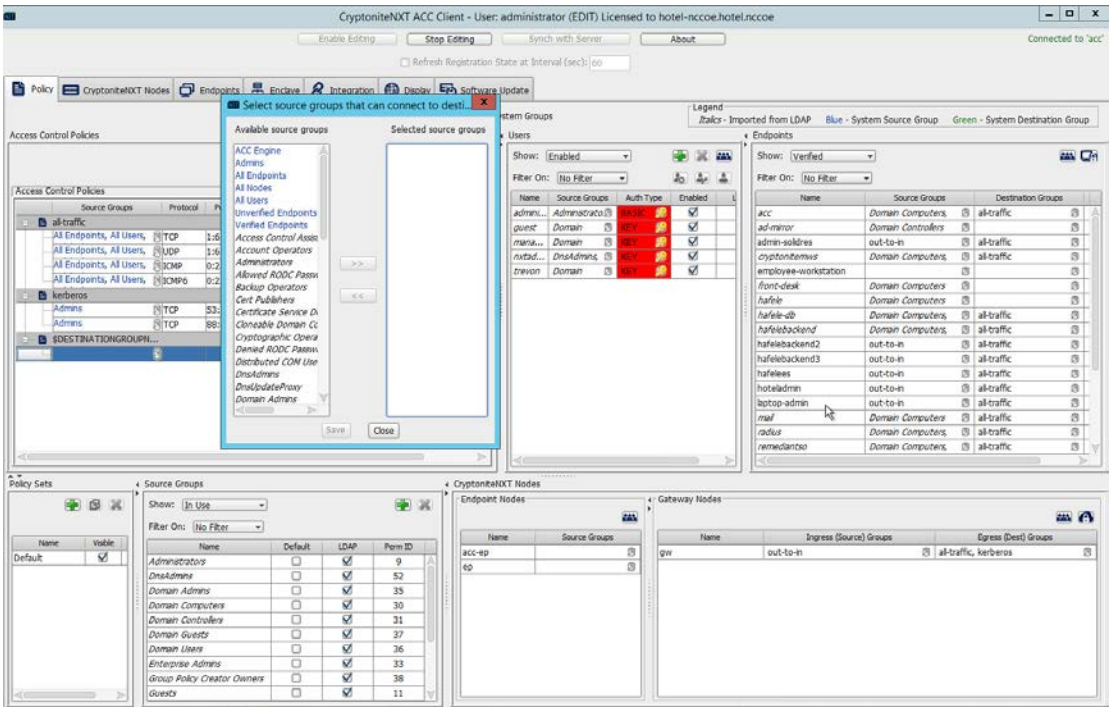
4. Click **OK**.

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

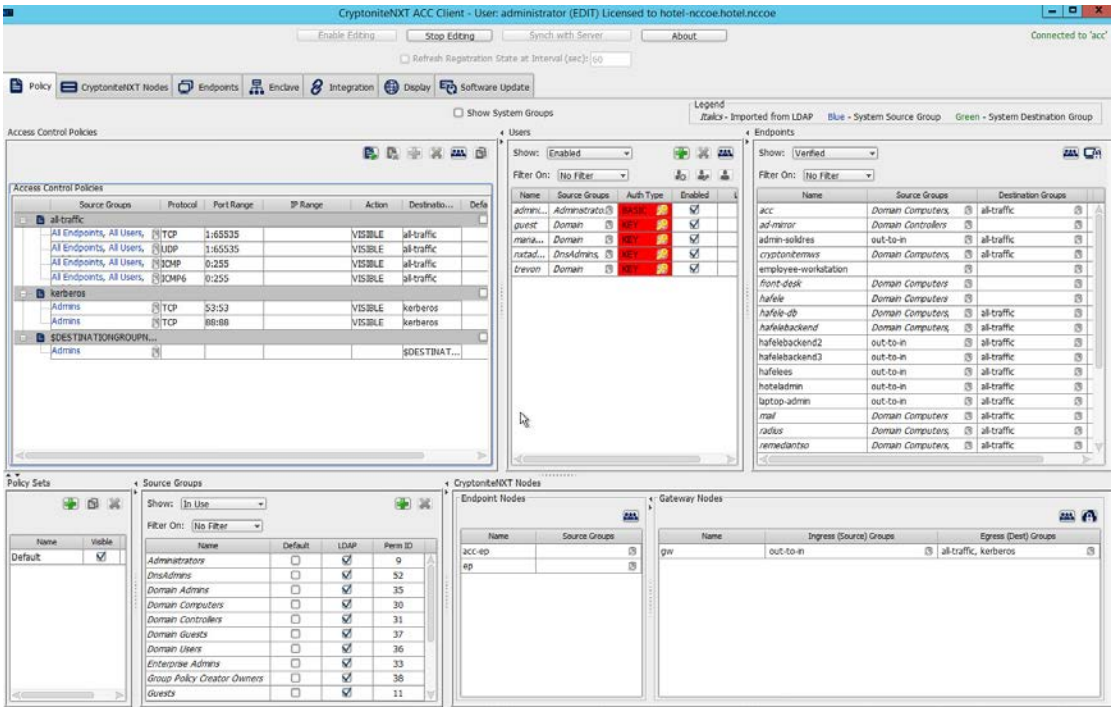


374

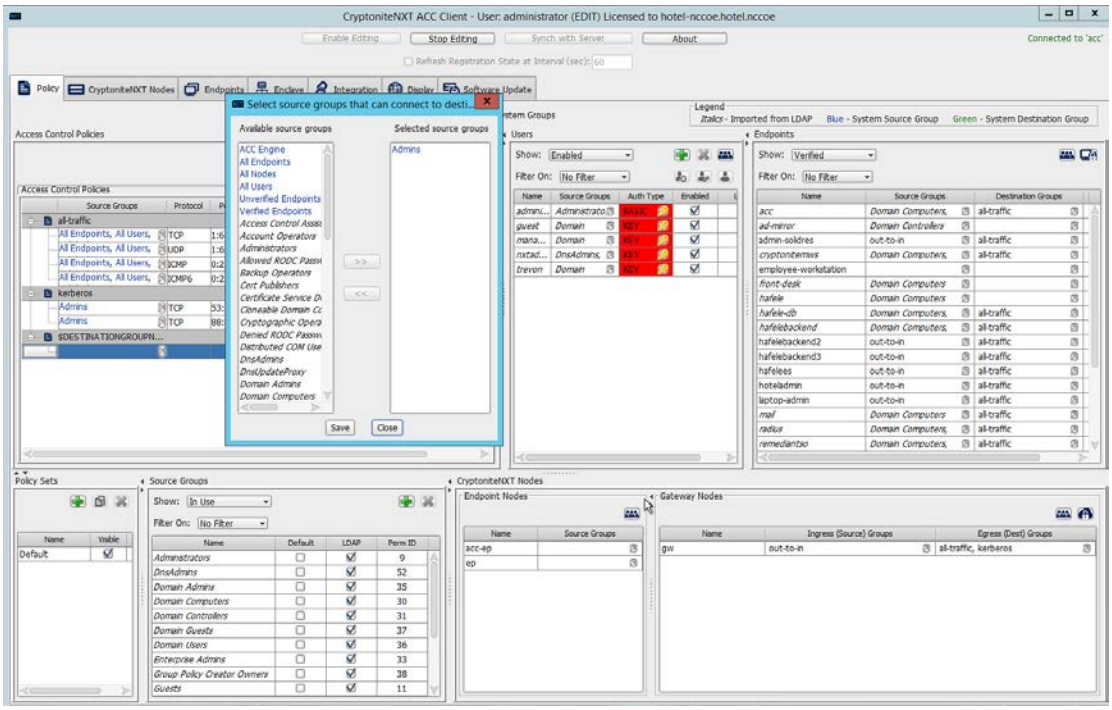
375 6. Click the small arrow icon in the **Source Groups** cell of the empty row (hover text: Click the ar-
376 row button to view/edit the source groups):



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



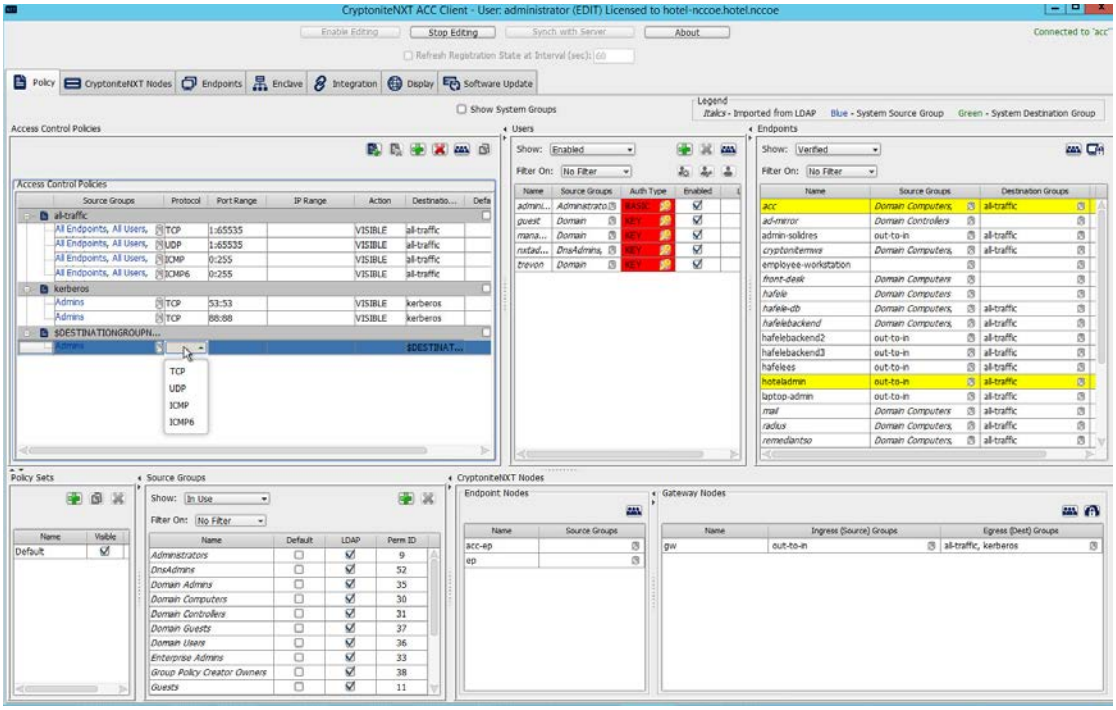
8. Click **Save:**



380

381 9. Click the **Protocol** cell of the row.

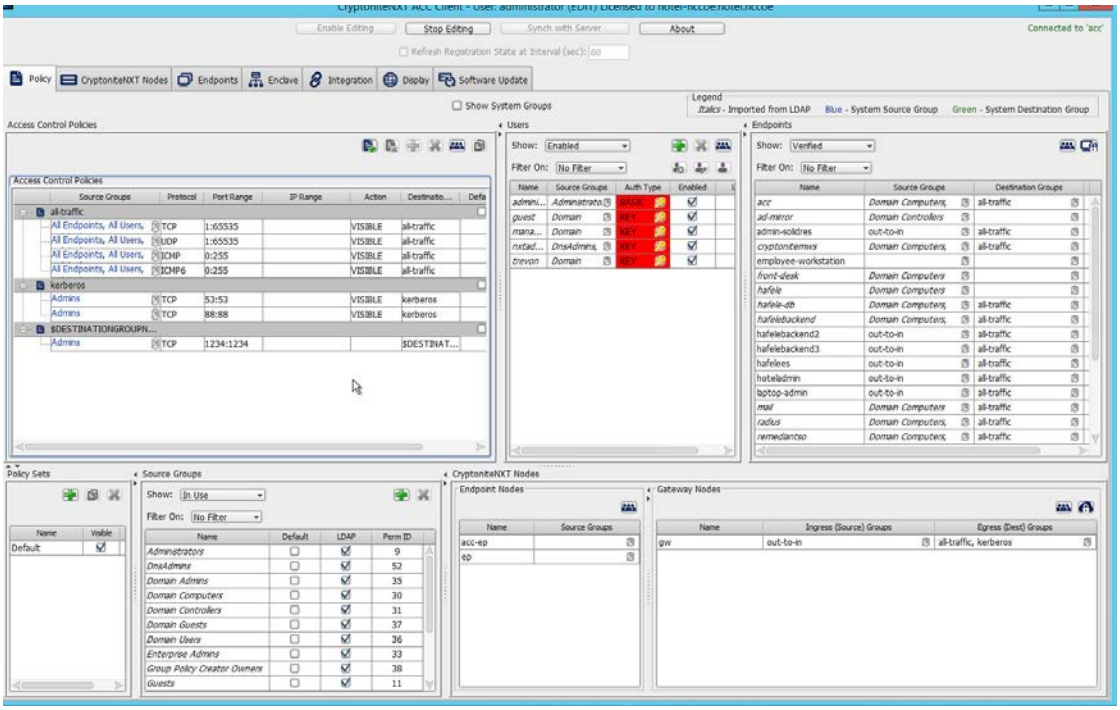
382 10. Select the protocol for which you wish to create an access policy:



383

384 11. Click the **Port Range** cell of the row.

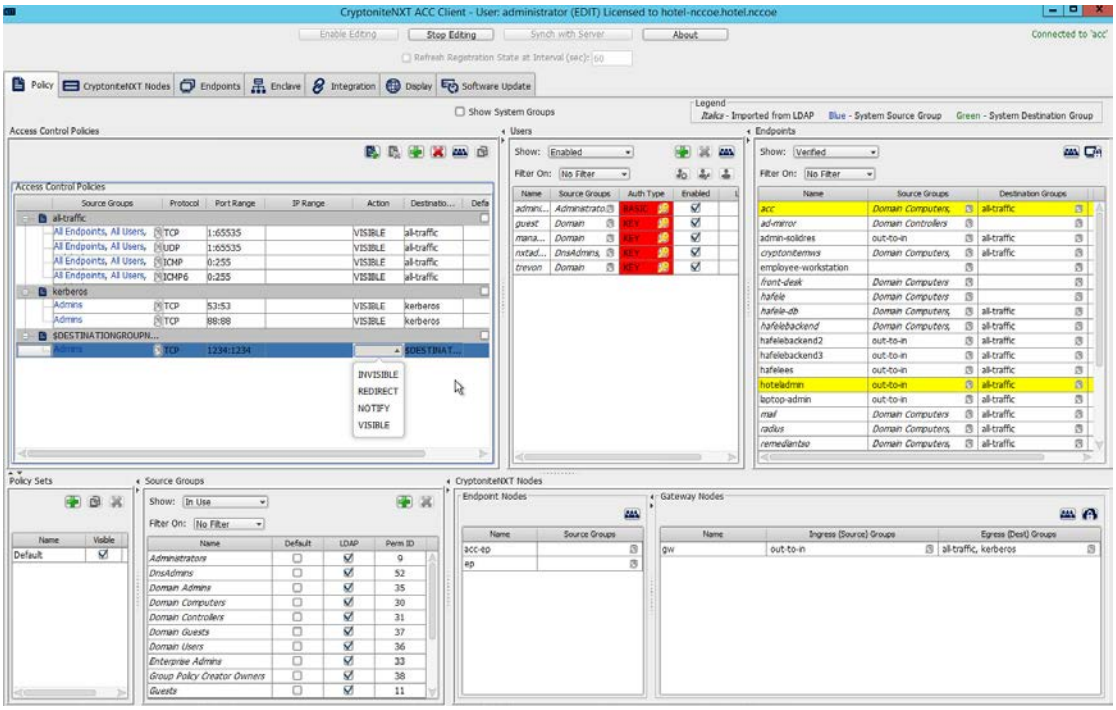
385 12. Input the desired port ranges for the protocol selected in step 10:



386

387 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:

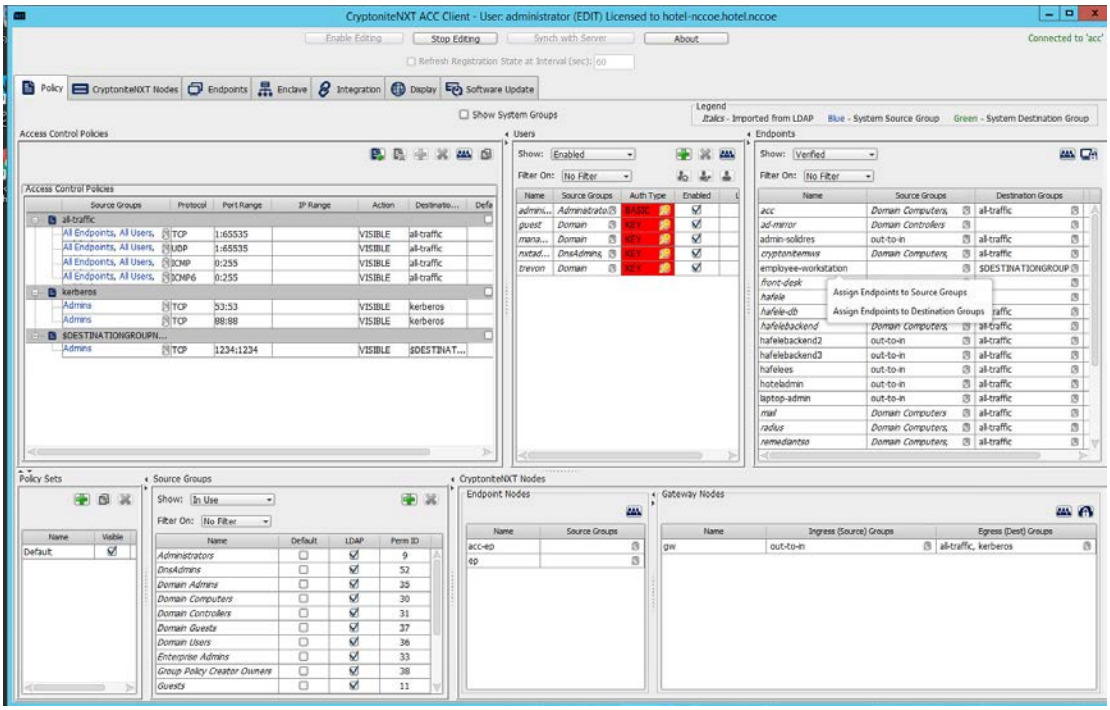


15. Set **Action** to VISIBLE to allow traffic of the described type; use INVISIBLE to block traffic of this type.

2.1.6 Applying Source Groups to End Points

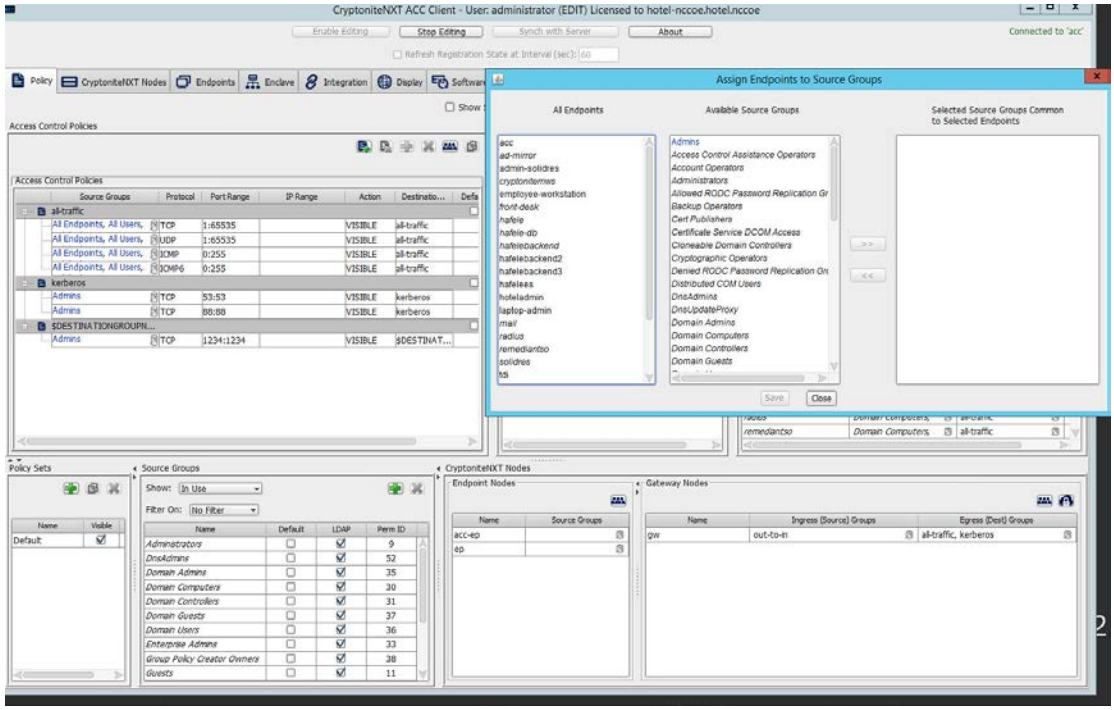
The following instructions detail how to add an already-created source group to a specific end point within the CryptoniteNXT enclave. They assume the same access to the CryptoniteNXT ACC GUI as in the previous instructions.

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

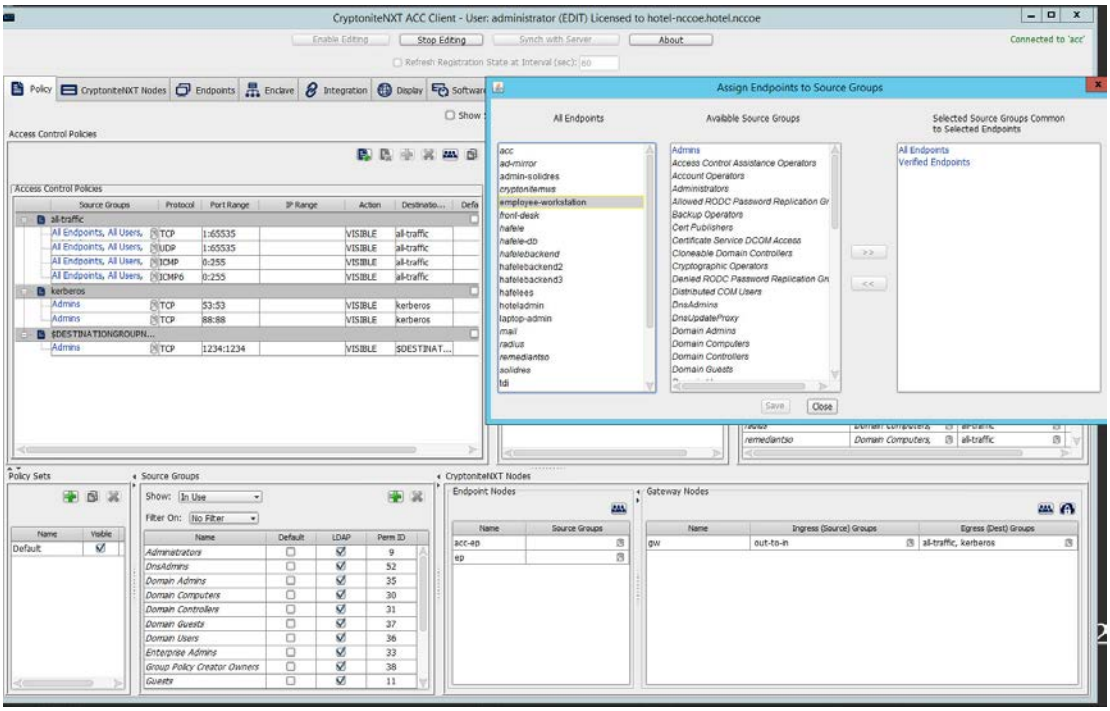


399

400 3. Select Assign Endpoints to Source Groups:

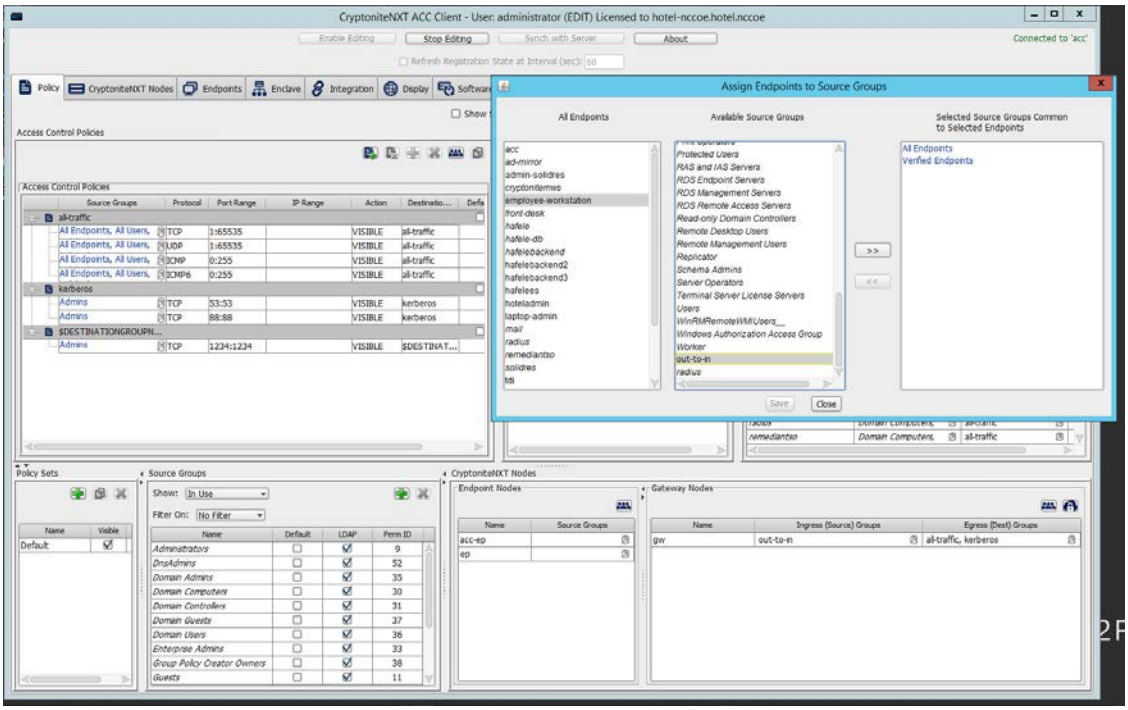


401 4. Find and select the desired end point under **All Endpoints:**



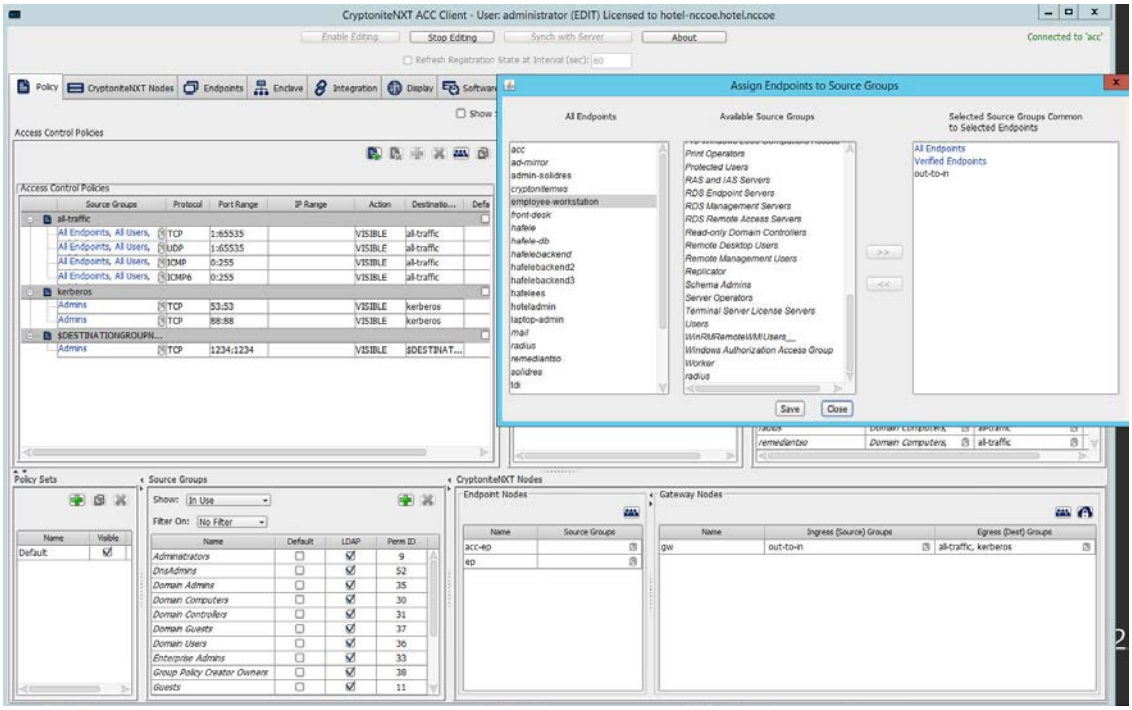
402

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



404

405 6. Click **>>**:

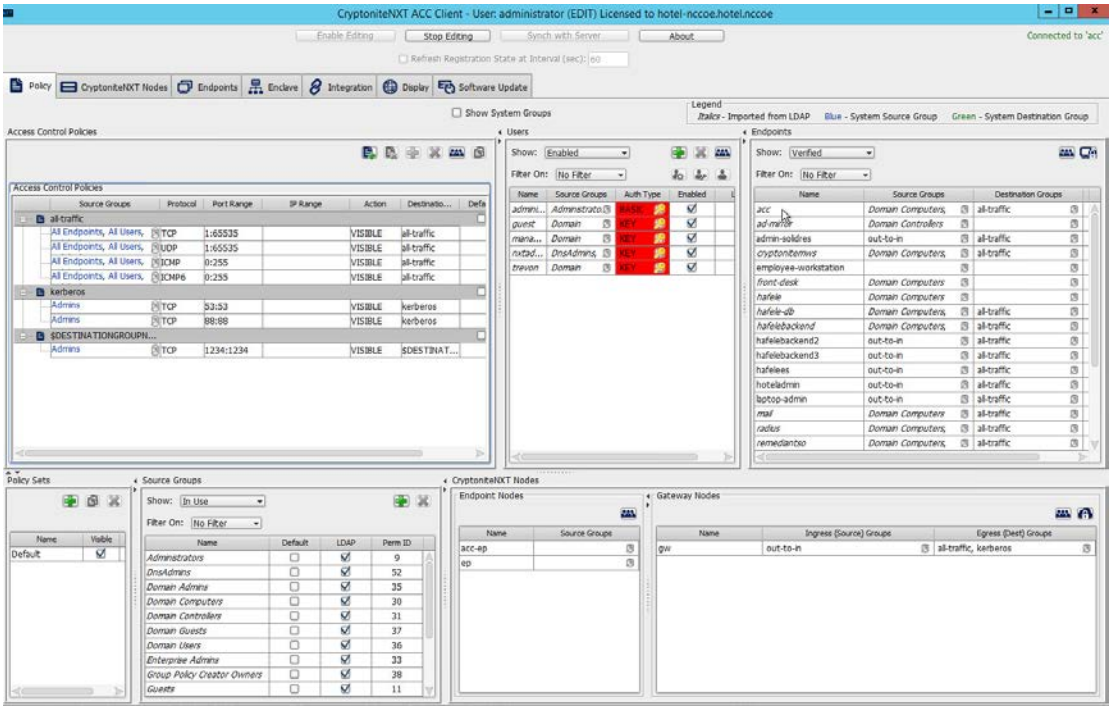


7. Click **Save.**

2.1.7 Applying Destination Group to End Points

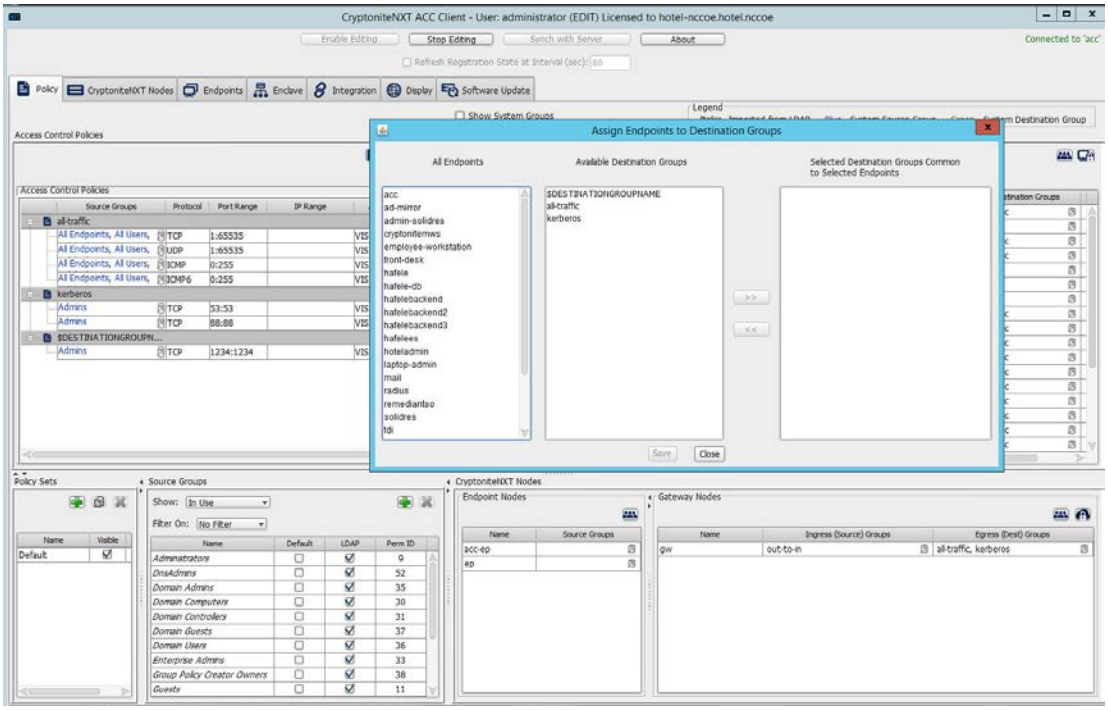
The following instructions detail how to apply a previously created destination group to a registered end point.

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



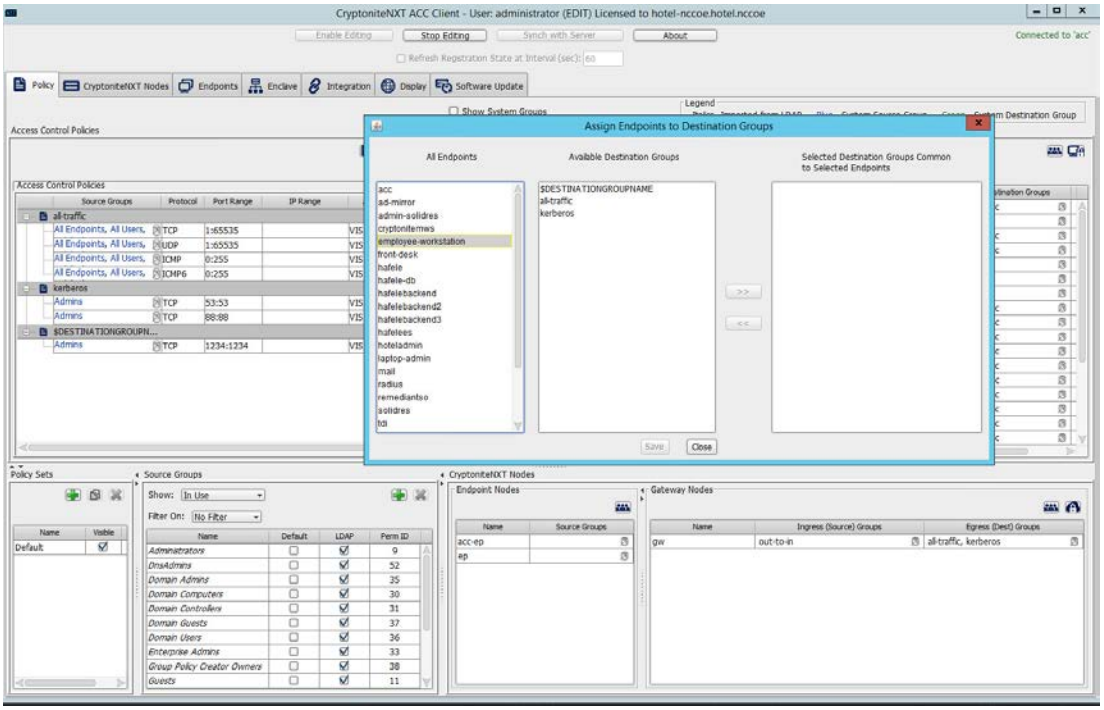
2. Locate the box titled **Endpoints** on the right hand of the screen. Right-click on any of the end points.

3. Select Assign Endpoints to Destination Groups:

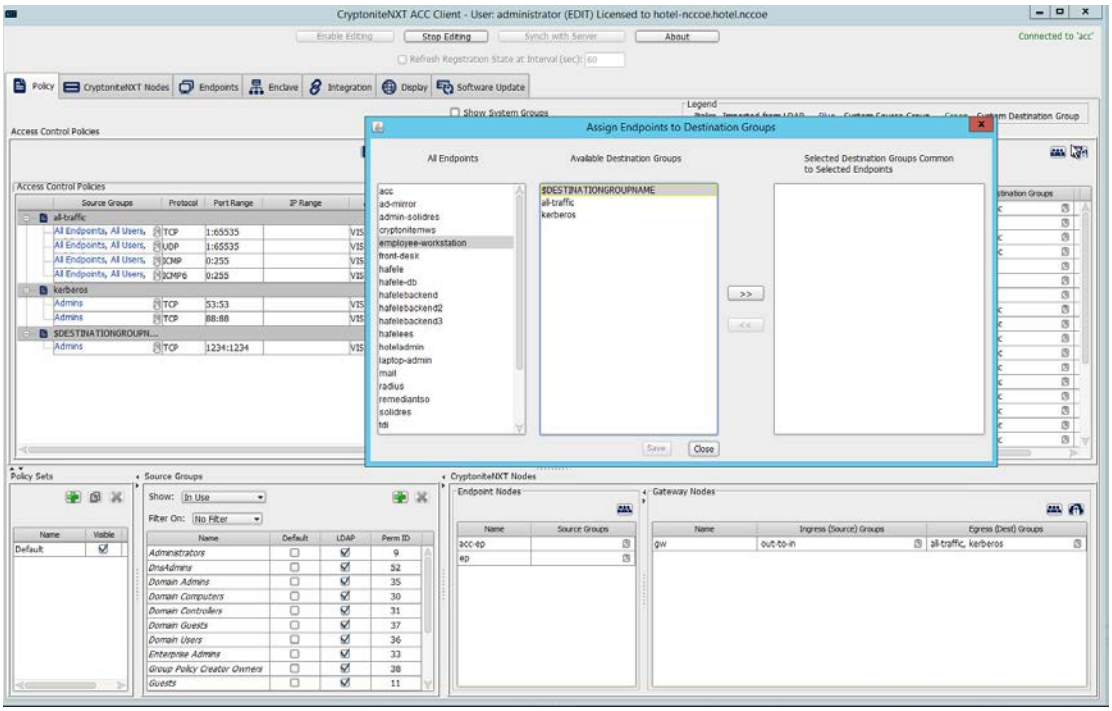


415

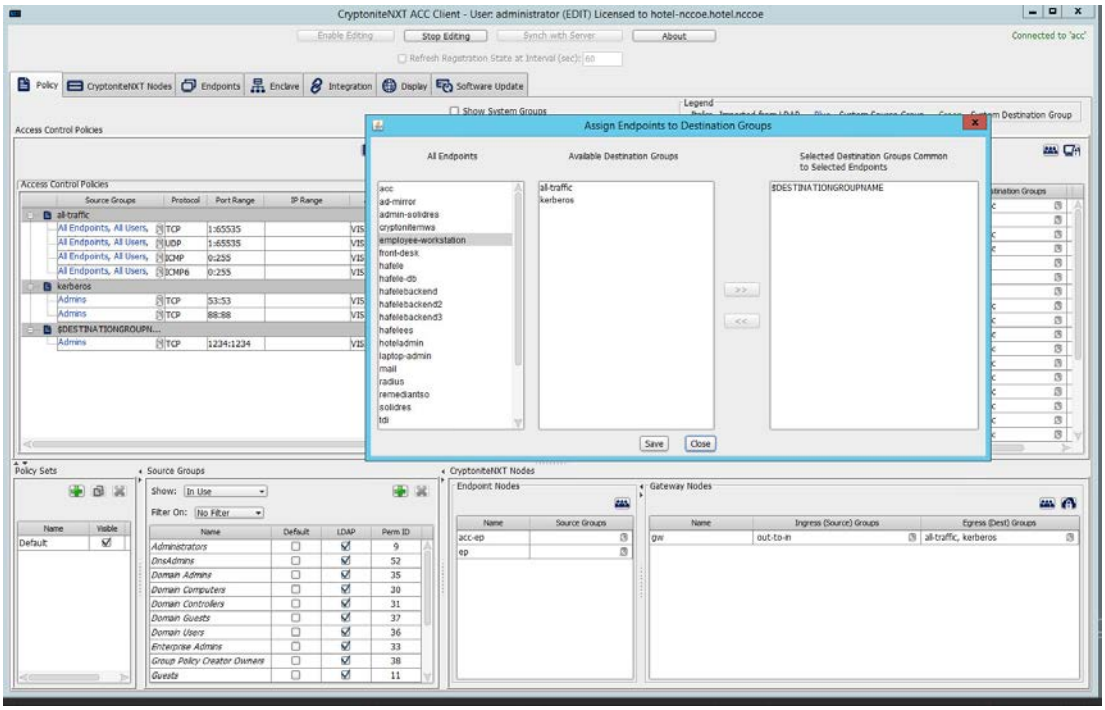
416 4. Locate and select the desired end point(s) under **All Endpoints:**



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



6. Click **>>:**



7. Click **Save**.

2.1.8 CryptoniteNXT Configuration for the PMS Ecosystem

To gain the benefits of a zero trust architecture discussed in Volume B of this document, proper configuration of the CryptoniteNXT device is required. Nonuse of the following network restrictions may limit network functionality and diminish the security benefits of the architecture. However, improperly configured rules can lead to a loss of network functionality. It may be correct for the adopting enterprise to install and configure its enterprise architecture and the remaining security architecture before applying the final configuration of the CryptoniteNXT device.

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 using instructions from Section 2.1.4.

- Remediant-Web-Access
- Remediant-Access-Domain
- Remediant-Access-Windows
- RDP-Access
- VNC-Access

- HafeleES-Access
- TDi-Access
- Mail-Allowed

Create the following destination groups by using the instructions in Section 2.1.5. All rows should be set to VISIBLE.

Table 2-1 Required Destination Groups for CryptoniteNXT Configuration

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

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

444

445 Apply the source and destination groups to the end points per instructions in Section 2.1.4 and Section
446 2.1.5. In some deployments, the adopting enterprise may have included an all-traffic or similar rule to
447 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-station	Remediant-Web-Access TDi-Access	Remediant-Access-Windows
employee workstations	TDi-Access	
mail server	Mail-Allowed	Mail
Remediant SecureONE	Remediant-Access-Domain Remediant-Access-Linux Remediant-Access-Windows	Remediant-Web
TDi ConsoleWorks	RDP-Access VNC-Access	Remediant-Linux TDi-Incoming

2.2 Access Control Platform—TDi ConsoleWorks

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

TDi ConsoleWorks is the access control platform used in the PMS ecosystem.

2.2.1 Access Control Platform–TDi ConsoleWorks—Overview

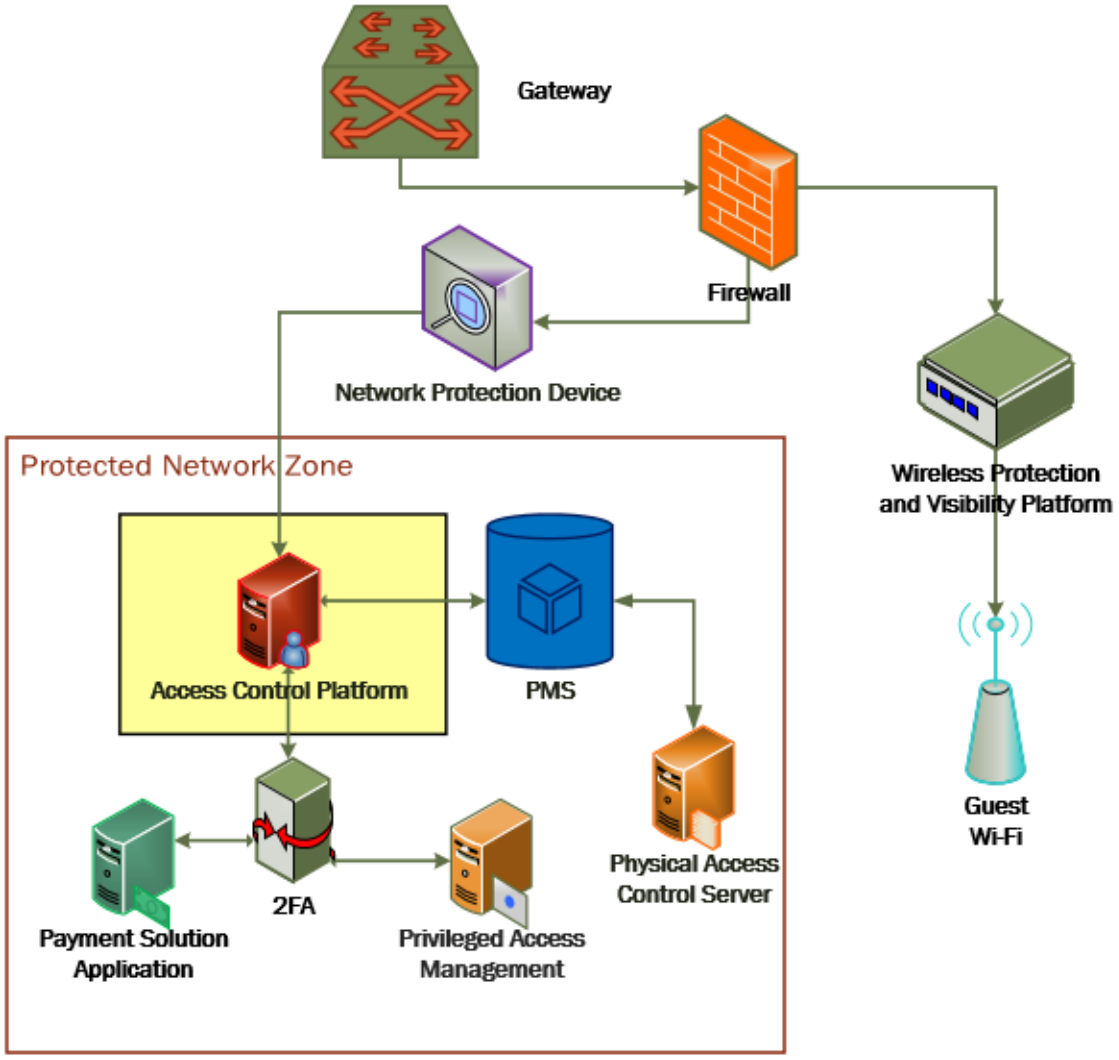
The access control platform TDi ConsoleWorks performs the access control functionality in the PMS ecosystem.

TDi ConsoleWorks was deployed as a virtual machine (VM) in the NCCoE hospitality lab. Installation instructions are available at the TDi Technologies support site, which may be useful if the adopting enterprise's deployment differs substantially from the one used for this project.

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 2-2 below.

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



468

469 2.2.2 Access Control Platform—TDi ConsoleWorks—Requirements

470 The following subsections document the software, hardware, and network requirements for the access
471 control 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.

2.2.2.2 Software Requirements for Access Control Platform

TDi ConsoleWorks 5.2 requires an operating system (OS) from the following list.

- 64-bit RedHat Linux 7.5, 7.5, 8.0, or equivalent
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

This build utilized a Community Enterprise Operating System (CentOS) 7.3 64-bit server.

To install TDi ConsoleWorks, access must be available to the machine's command line interface (CLI). It will also be necessary for network access to be available to the machine's IP address (retrievable via the ifconfig command) during installation. For this build of TDi ConsoleWorks 5.2, installation is conducted on a VM in the NCCoE virtual environment.

2.2.2.3 Network Requirements of the Access Control Platform

In addition to the described access to the CLI, the access control platform requires network access to the TDi ConsoleWorks back-end server as well as to any end points to which it will connect. The network must support secure transmission protocols. TDi ConsoleWorks relies on existing means to connect to protected end points, such as Secure Shell (SSH) or Remote Desktop Protocol (RDP).

Note that use of 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 TDi ConsoleWorks before applying rules on the CryptoniteNXT device, as stated in Section 2.1.8.

2.2.3 Access Control Platform —TDi ConsoleWorks—Installation

The installation procedure consists of the following steps:

1. Download the software.
2. Run the installation script, customizing options to reflect the enterprise.
3. Create a secure sockets layer (SSL)-capable invocation of TDi ConsoleWorks and generate an SSL certificate to match.
4. Download and apply a license.
5. Create a gateway to allow GUI functionality.
6. Create connections to the desired end points within the enterprise.

The instructions below rely on the assumed access to the TDi ConsoleWorks CLI. The installation media 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 accessed at https://support.tditechnologies.com/get_consoleworks/linux.

1. Create a directory in the */tmp* folder:

```
mkdir /tmp/conwrks
```

2. Move the ConsoleWorks installation media to */tmp/conwrks:*

```
mv path/to/media /tmp/conwrks
```

3. Change directory to the *conwrks* directory, and verify that the terminal prompt reflects the change:

```
cd /tmp/conwrks
```

```
[hospitality@tdi ~]$ cd /tmp/conwrks
[hospitality@tdi conwrks]$
```

4. Execute the installation media:

```
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-5.1-0U1.signed.x86_64.rpm: ConsoleWorksSSL-5.1-0U1.x86_64
Marking ConsoleWorksSSL-5.1-0U1.signed.x86_64.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package ConsoleWorksSSL.x86_64 0:5.1-0U1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package             Arch       Version        Repository                   Size
================================================================================
Installing:
 ConsoleWorksSSL     x86_64     5.1-0U1        /ConsoleWorksSSL-5.1-0U1.signed.x86_64     350 M

Transaction Summary
================================================================================
Install  1 Package

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

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

6. Wait for the installation to complete. Upon completion, the text `Installed: Console-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.x86_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]$ _
```

522

523 2.2.3.1 Create SSL Invocation

524 1. Escalate to a super user shell by executing the following command and entering the machine
525 password:

526 `su`

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

```
[hospitality@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
[root@tdi conwrks]#
```

528

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 `y` followed by the enter key.

532 5. Enter the following information, in order. The values used in this implementation are provided
533 for context but may not be appropriate for your enterprise. Press enter to use the default value
534 provided by the terminal:

535 a. desired console name [HotelConsole]

536 b. web service port [5176]

537 c. enabled syslog functionality [y]

538 6. Verify that the desired values have been entered:

```
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, 0-9 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
```

539

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, 0-9 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

    [0] Return to /opt/ConsoleWorks/bin/cw_add_invo
    [1] Create a new SSL certificate for invocation Hotel

Enter menu choice or 0 to return      [0]: 1_
```

2. Enter the following information, pressing enter after each entry:
    a. country code
    b. state or provincial name
    c. city or locality
    d. company or organization name
    e. department name
    f. FQDN
    g. email address of the person responsible for the certificate
    h. password to protect the certificate
    i. the same password to confirm
    j. name of the person responsible for the certificate
    k. the number of days for which the certificate will be valid (730 is the default value)

```
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

    [0] Return to /opt/ConsoleWorks/bin/cw_add_invo
    [1] Create a new SSL certificate for invocation Hotel

Enter menu choice or 0 to return      [0]: 1

Enter the 2 letter code for your country      [US]: US
Enter the name of your state, province, or regional district      []: Maryland
Enter the name of your city or locality      []: Rockville
Enter the name of your company or organization      []: NCCoE
Enter the name of your department      []: Hospitality
Enter the fully qualified host name for this server      [tdi.hotel.nccoe.hotel.nccoe]: tdi.hotel.nc
coe
Enter the email address of the person responsible for this certificate      []: [redacted]
Enter the challenge password for this certificate (min 4 chars., max 20 chars.)      []:
Verify the challenge password for this certificate      []:
Enter the name of the person responsible for this certificate      []: [redacted]
Enter the number of days for which this certificate will be valid      [730]: 730
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Generating a 2048 bit RSA private key
.....................+++
.............................+++
writing new private key to '/tmp/privkey.pem_tmp'
-----
Certificate 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

Enter menu choice or 0 to return      [0]: _
```

560

561 3. Input `0` to complete the invocation addition:

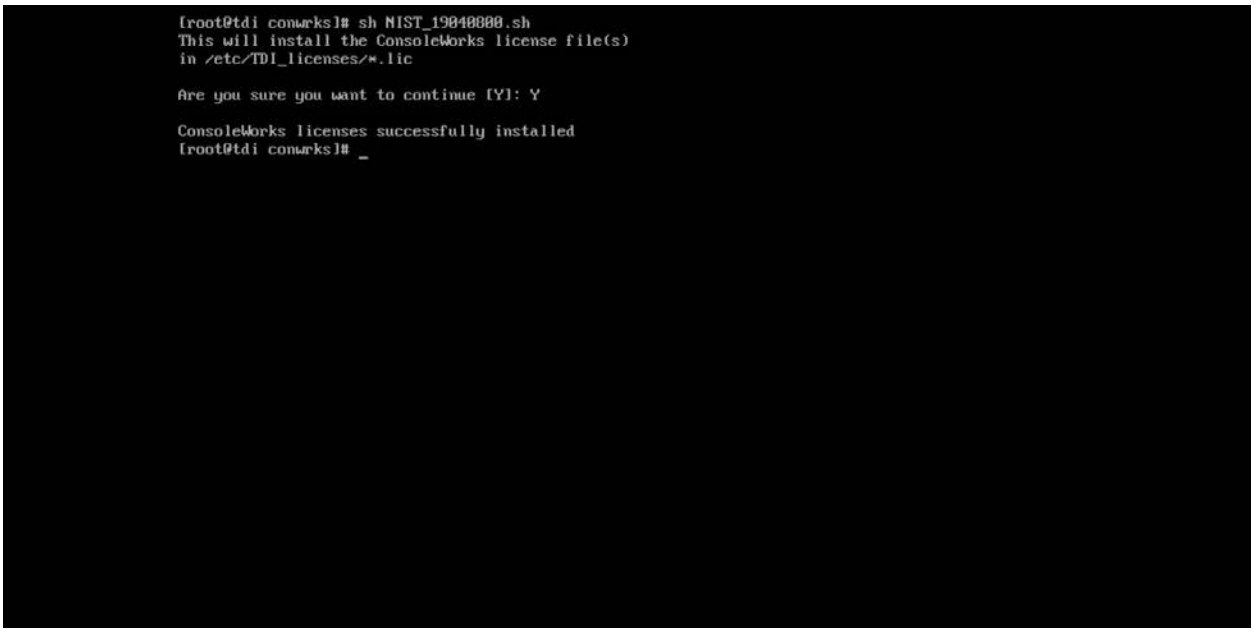
```
Do you want to make any changes [N]: n


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

    [0] Return to /opt/ConsoleWorks/bin/cw_add_invo
    [1] Create a new SSL certificate for invocation Hotel

Enter menu choice or 0 to return      [0]: 1

Enter the 2 letter code for your country      [US]: US
Enter the name of your state, province, or regional district      []: Maryland
Enter the name of your city or locality      []: Rockville
Enter the name of your company or organization      []: NCCoE
Enter the name of your department      []: Hospitality
Enter the fully qualified host name for this server      [tdi.hotel.nccoe.hotel.nccoe]: tdi.hotel.nc
coe
Enter the email address of the person responsible for this certificate      []: [redacted]
Enter the challenge password for this certificate (min 4 chars., max 20 chars.)      []:
Verify the challenge password for this certificate      []:
Enter the name of the person responsible for this certificate      []: [redacted]
Enter the number of days for which this certificate will be valid      [730]: 730
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Generating a 2048 bit RSA private key
.....................+++
.............................+++
writing new private key to '/tmp/privkey.pem_tmp'
-----
Certificate 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

Enter menu choice or 0 to return      [0]: 0
```

2.2.3.3 Apply License

The following instructions rely on continued access to the command line interface (CLI) of the TDi ConsoleWorks device.

1. Execute the shell script provided as the license by TDi Technologies:

2. Input `Y`:



568

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`

```
[root@tdi conwrks]# /opt/ConsoleWorks/bin/cw_start Hotel

which: no java in (/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/home/hospitality/.local/b
in:/home/hospitality/bin)
Attempting to start invocation Hotel...
ConsoleWorks invocation Hotel started.
  Logfile: /opt/ConsoleWorks/Hotel/log/Hotel.out
  URL: http://tdi.hotel.nccoe:5176
[root@tdi conwrks]# _
```

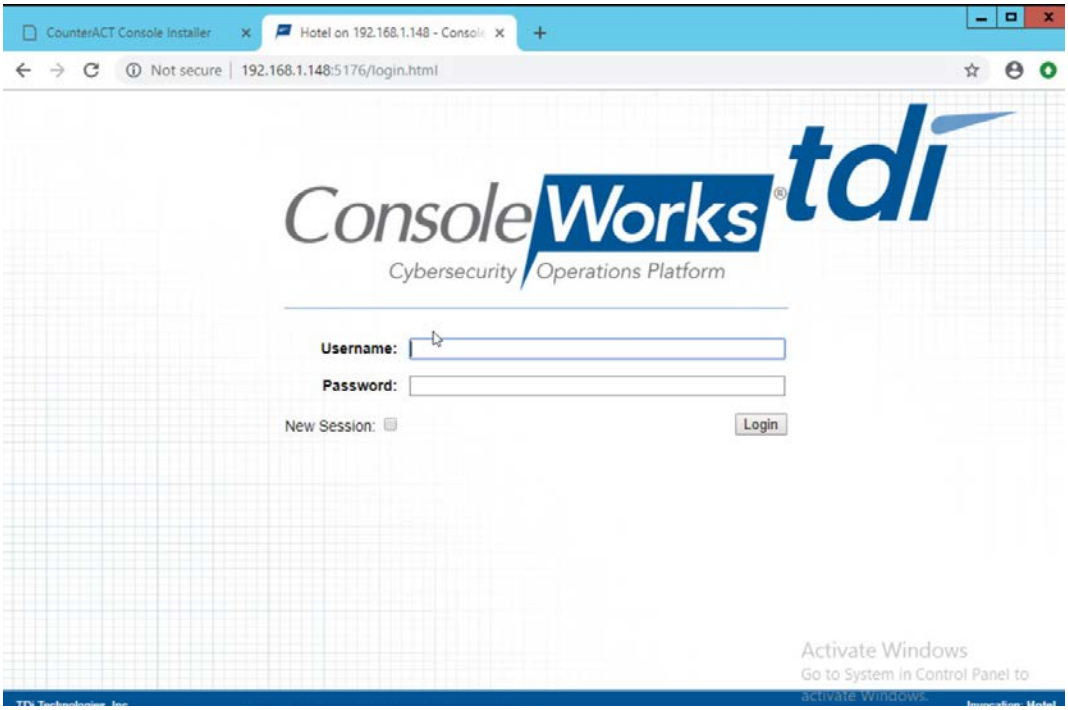
573

574 2. Execute the following command:

575 `/opt/ConsoleWorks/bin/cw -setsid Hotel`

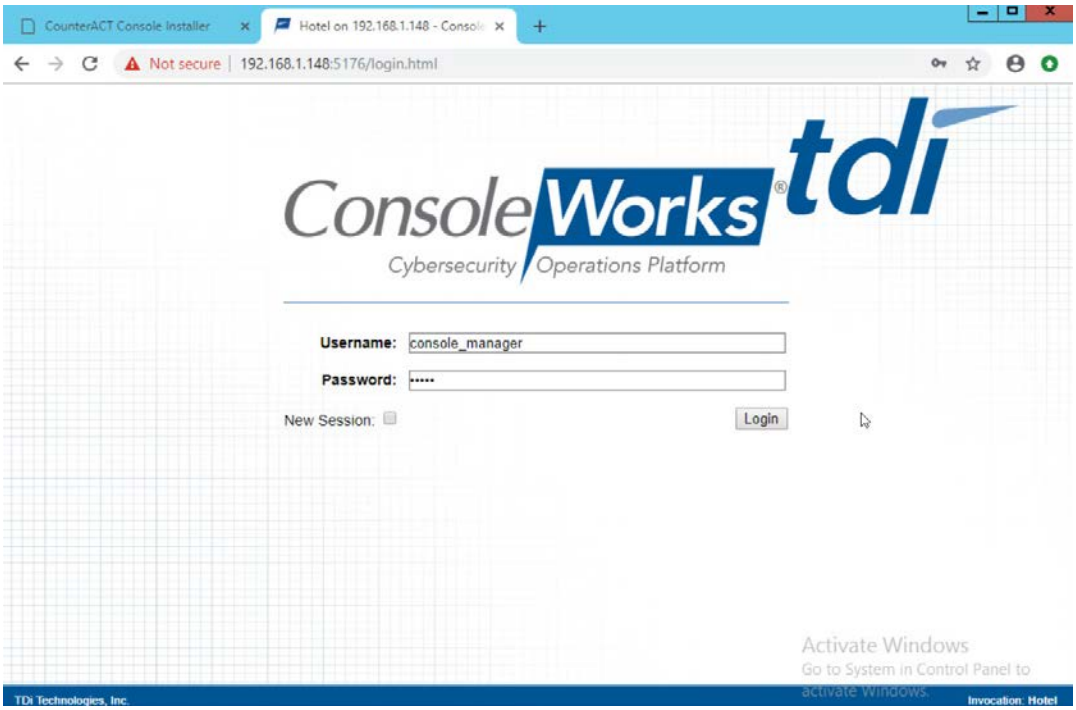
```
[root@tdi conwrks]# /opt/ConsoleWorks/bin/cw -setsid Hotel
2019/04/16 10:44:28 EDT: ConsoleWorks Major Version 5, Minor Version  1, Patch Version  0, Update Ve
rsion 1
2019/04/16 10:44:28 EDT: %Server image identification is V5.1-0u1-180614LxE
2019/04/16 10:44:28 EDT: %Server expected library identification is 5,1,0;5.1-0u1;18.06.14
2019/04/16 10:44:28 EDT: %Server startup time is 2019/04/16 10:44:28
2019/04/16 10:44:28 EDT: %Server logging configuration file: (internal fallback)
2019/04/16 10:44:28 EDT: %Environment 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]# _
```

576 3. On another machine, open the web page provided in step 1 or the IP followed directly by the
577 port number:



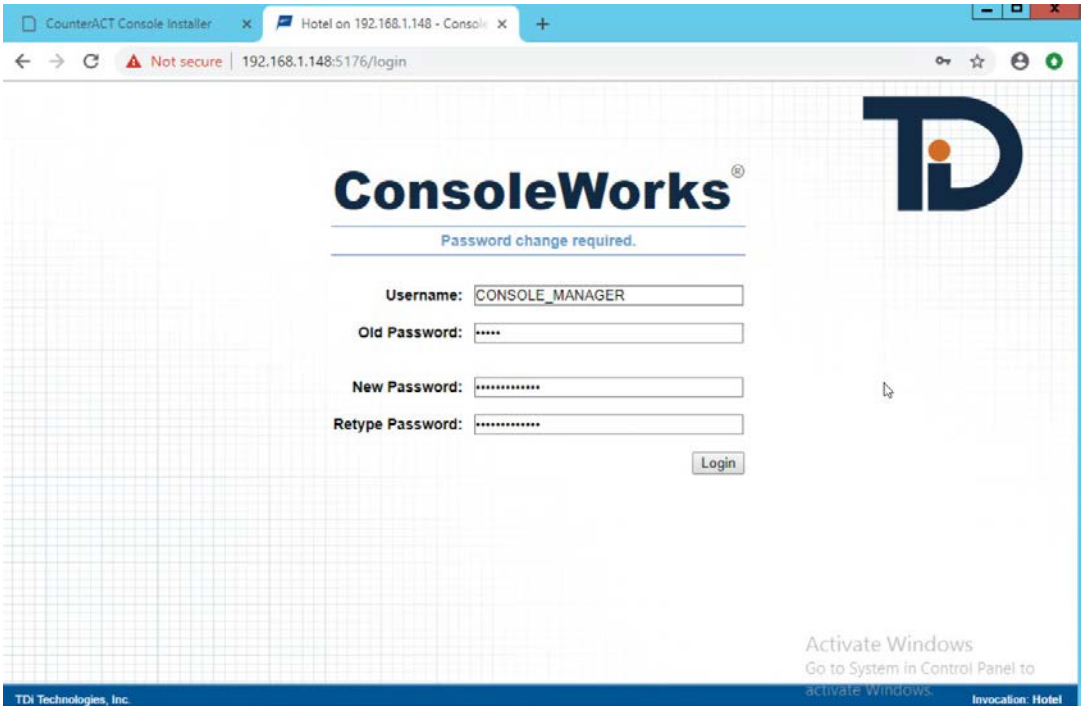
578

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

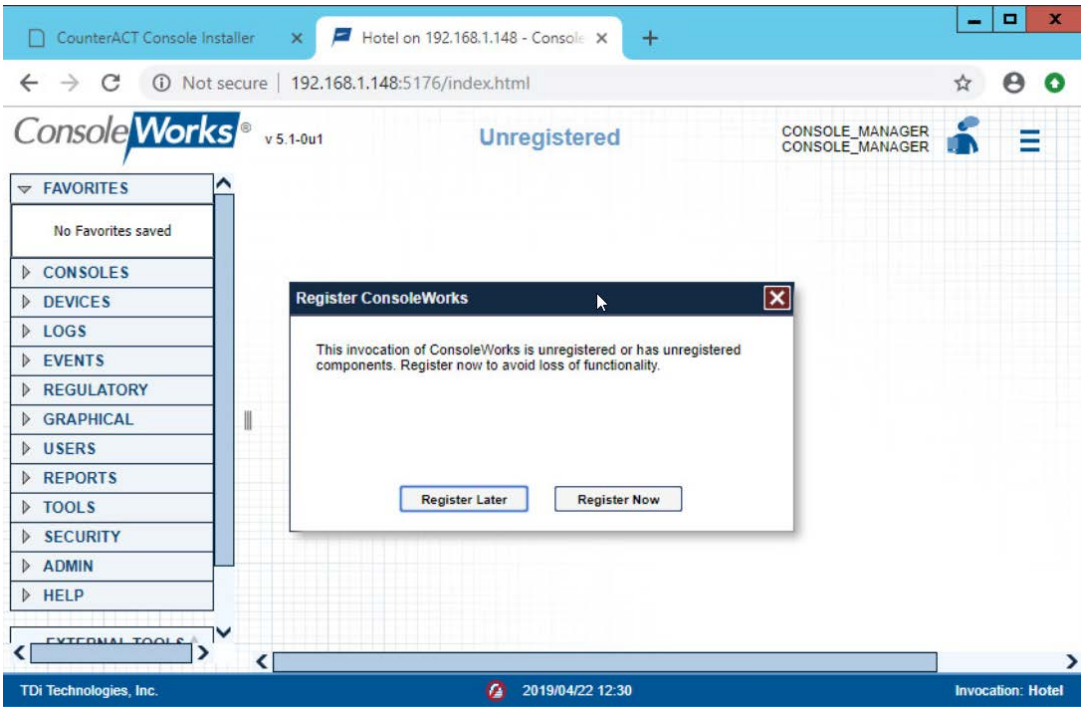


580

581 5. Change the default password, and click **Login:**

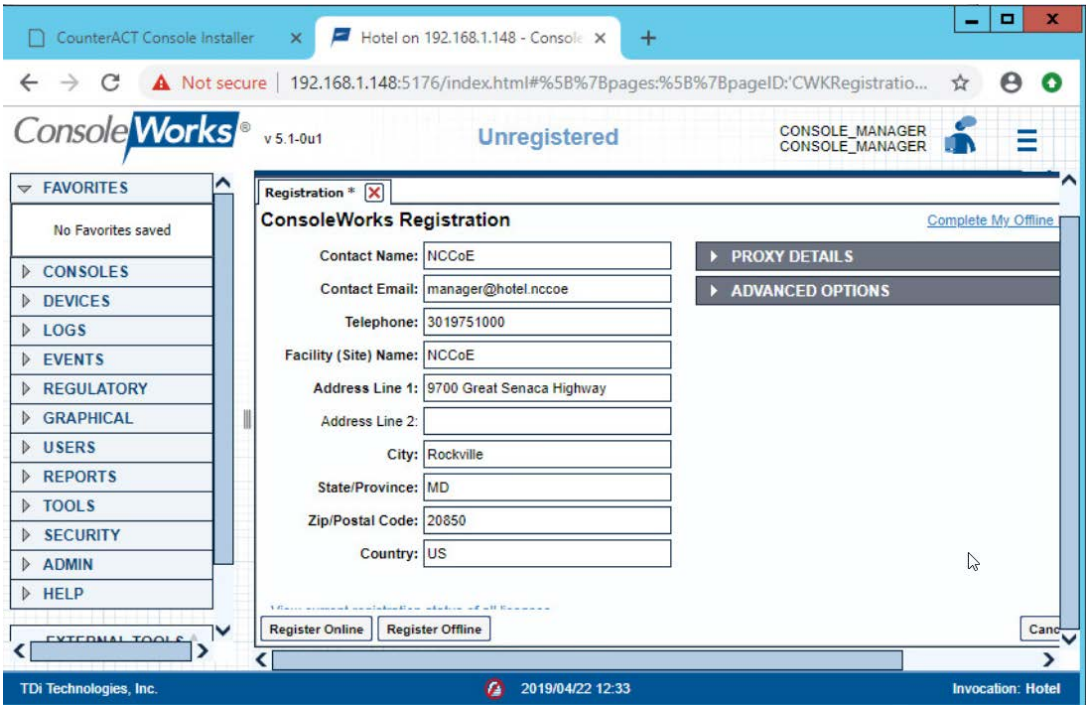


582 6. Click Register Now:



583

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



585

586 ### 2.2.3.5 GUI Gateway Installation

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

589 -freerdp-libs

590 -uuid

591 -cairo

592 -libvncserver

593 -libpng12

594 -freerdp-plugins

595 -net-tools

596 -openssh-clients

597 -open-vm-tools

```
[root@tdi conwrks]# yum install freerdp-libs_
```

598

599 2. Type y to allow installation:

```
Loaded plugins: fastestmirror
Repodata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
base                                                                     | 3.6 kB  00:00:00
extras                                                                   | 3.4 kB  00:00:00
updates                                                                  | 3.4 kB  00:00:00
(1/2): extras/7/x86_64/primary_db                                        | 200 kB  00:00:00
(2/2): updates/7/x86_64/primary_db                                       | 5.0 MB  00:00:00
Loading mirror speeds from cached hostfile
 * base: mirrors.oit.uci.edu
 * extras: mirror.metrocast.net
 * updates: ftp.ussg.iu.edu
Resolving Dependencies
--> Running transaction check
---> Package freerdp-libs.x86_64 0:1.0.2-15.el7_6.1 will be installed
--> Processing Dependency: libxkbfile.so.1()(64bit) for package: freerdp-libs-1.0.2-15.el7_6.1.x86_6
4
--> Running transaction check
---> Package libxkbfile.x86_64 0:1.0.9-3.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================
 Package                Arch              Version                    Repository           Size
================================================================================================
Installing:
 freerdp-libs           x86_64            1.0.2-15.el7_6.1           updates             224 k
Installing for dependencies:
 libxkbfile             x86_64            1.0.9-3.el7                base                 83 k

Transaction Summary
================================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 307 k
Installed size: 874 k
Is this ok [y/d/N]: y
```

600

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

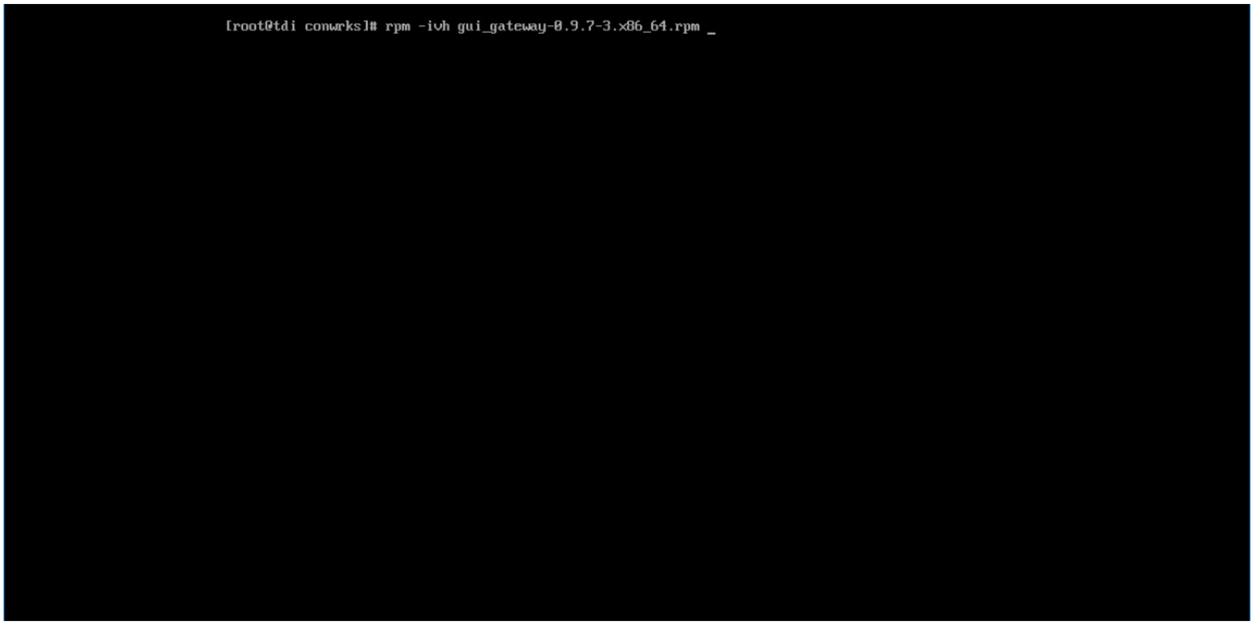
```
 Package                Arch             Version                    Repository          Size
================================================================================================
Installing:
 freerdp-libs           x86_64           1.0.2-15.el7_6.1           updates            224 k
Installing for dependencies:
 libxkbfile             x86_64           1.0.9-3.el7                base                83 k

Transaction Summary
================================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 307 k
Installed size: 874 k
Is this ok [y/d/N]: y
Downloading packages:
Delta RPMs disabled because /usr/bin/applydeltarpm not installed.
(1/2): libxkbfile-1.0.9-3.el7.x86_64.rpm                    |  83 kB  00:00:00
(2/2): freerdp-libs-1.0.2-15.el7_6.1.x86_64.rpm             | 224 kB  00:00:00
------------------------------------------------------------------------------------------------
Total                                              696 kB/s | 307 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : libxkbfile-1.0.9-3.el7.x86_64                                   1/2
  Installing : freerdp-libs-1.0.2-15.el7_6.1.x86_64                            2/2
  Verifying  : libxkbfile-1.0.9-3.el7.x86_64                                   1/2
  Verifying  : freerdp-libs-1.0.2-15.el7_6.1.x86_64                            2/2

Installed:
  freerdp-libs.x86_64 0:1.0.2-15.el7_6.1

Dependency Installed:
  libxkbfile.x86_64 0:1.0.9-3.el7

Complete!
[root@tdi ~]# _
```

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

```
[root@tdi ~]# ls /tmp/conwrks
gui_gateway-0.9.7-3.x86_64.rpm
[root@tdi ~]# _
```

5. Install with this command:

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



6. Execute the following command if you are conducting a local installation, where the gateway is on the same server as the TDi ConsoleWorks invocation:

```
/opt/gui_gateway/install_local.sh
```

7. Execute the following to start the gateway:

```
service gui_gatewayd start
```

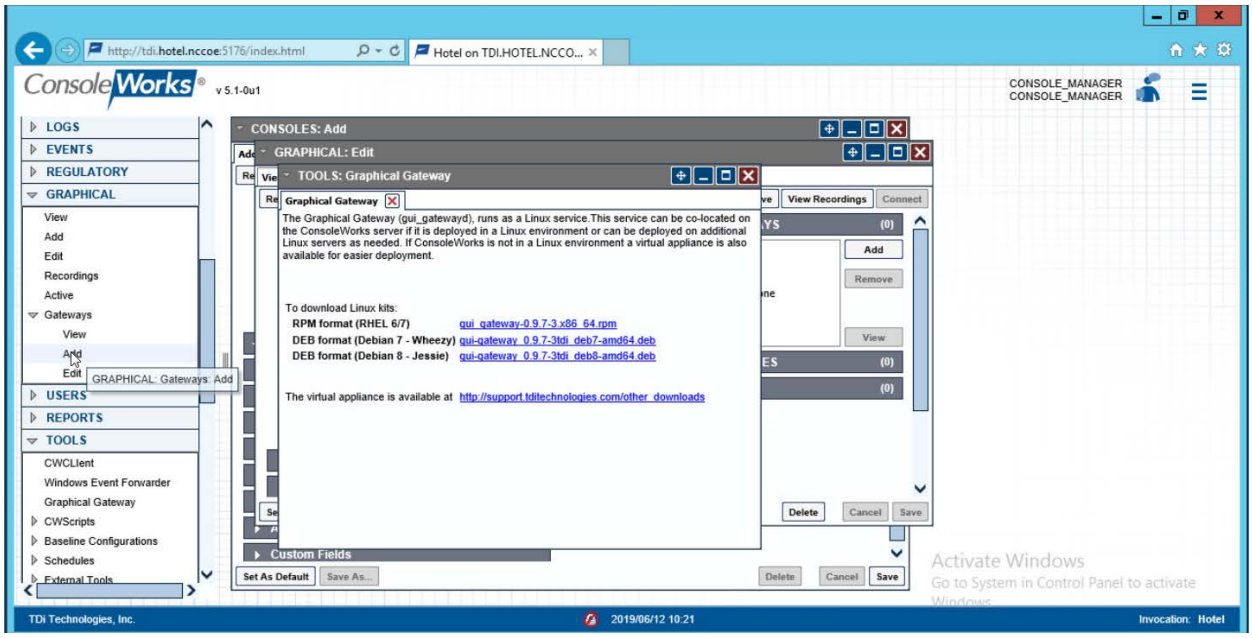
615

616 2.2.4 Add Gateway to GUI

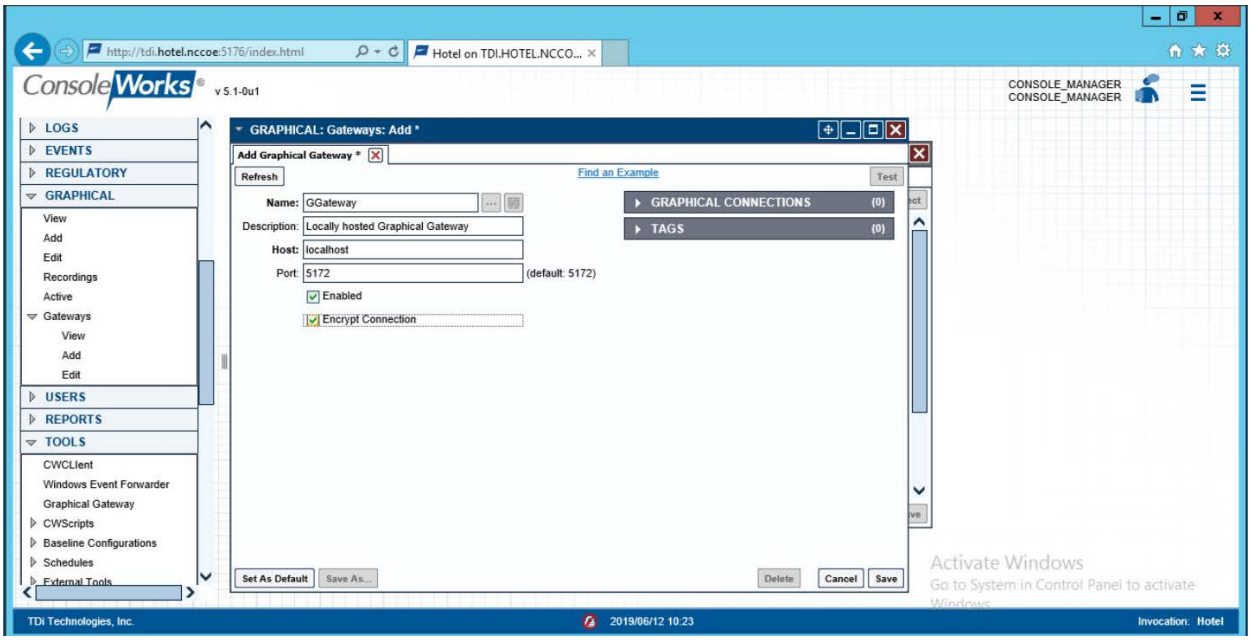
617 The instructions below are executed on a separate virtual or physical machine that has network access
618 to the TDi ConsoleWorks back-end server through the previously configured web port. The web service
619 is accessed through a web browser. The user must navigate to `[TDi Domain Name].[Hotel`
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:**



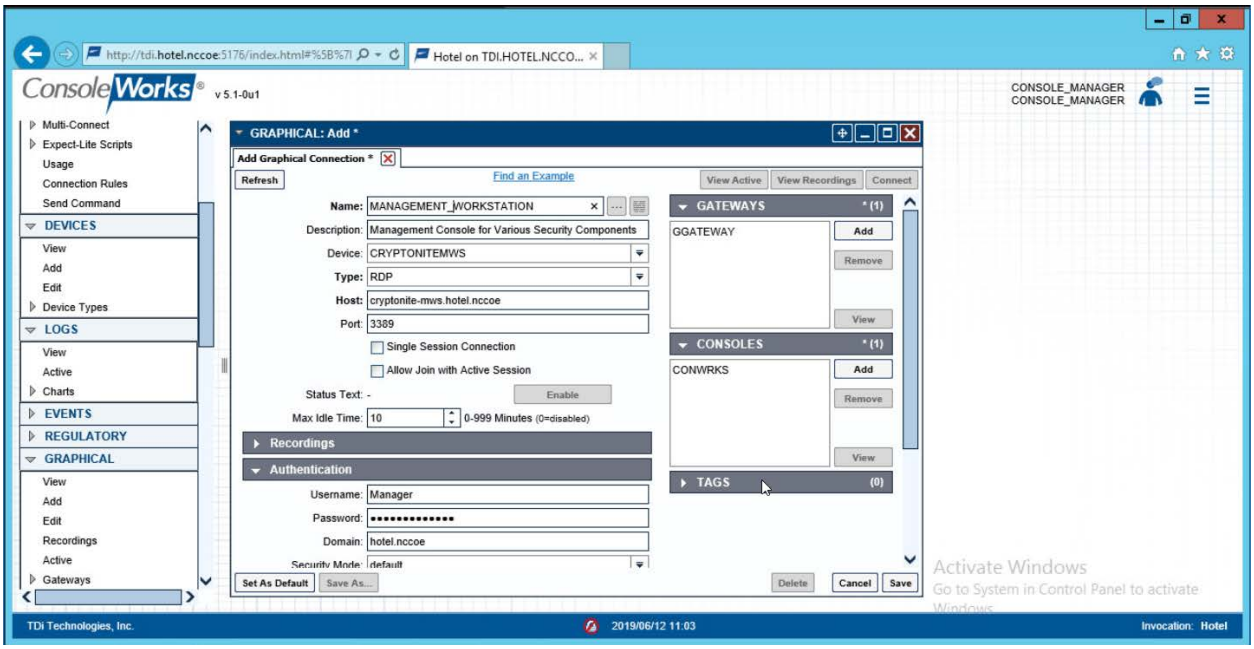
3. Enter the desired values for the graphical gateway. The values used for this architecture are provided but may not be the correct values for your enterprise.
    a. Name [GGateway]
    b. Description [Locally hosted Graphical Gateway]
    c. Host [localhost]
    d. Port [5172]



4. Click **Save.**

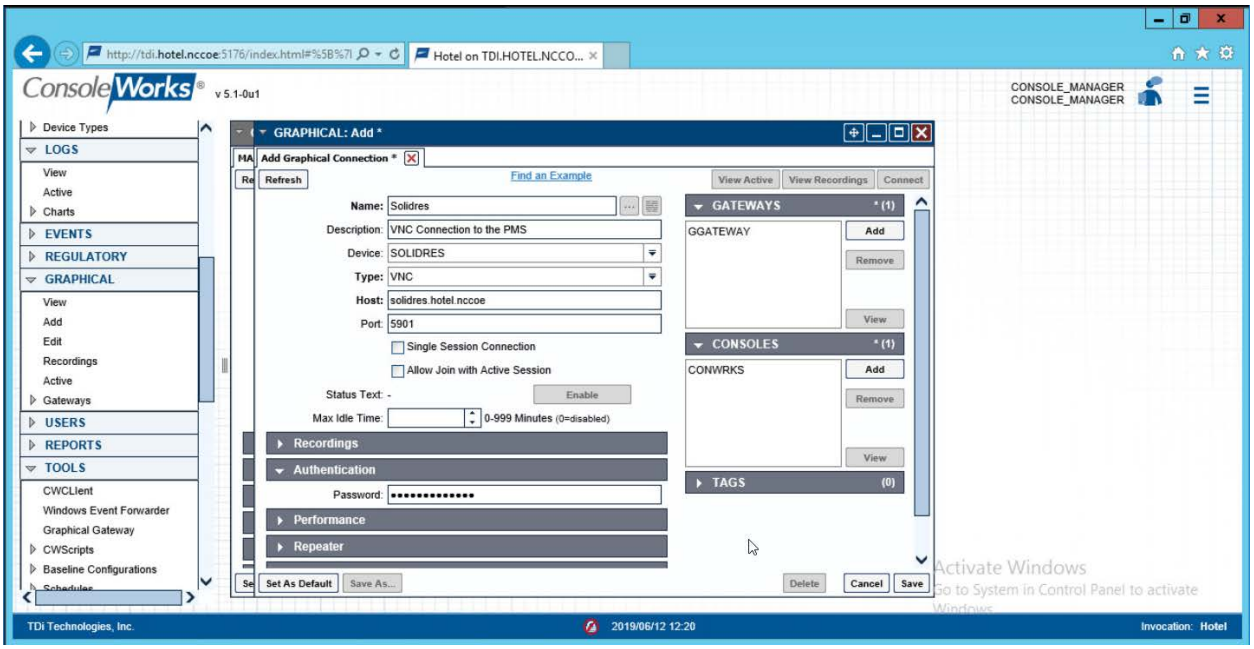
2.2.5 Add Graphical Connection to End Point

1. In the sidebar, choose **Graphical > Add.**
2. 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.
    a. Device Name [MANAGEMENT_WORKSTATION]
    b. Description [Management Console for Various Security Components]
    c. Device Identifier [CRYPTONITEMWS]
    d. Connection Type [RDP]
    e. DNS Host Information [cryptonite-mws.hotel.nccoe]
    f. Port number [3389]
    g. Username [Administrator]
    h. Password
    i. Domain [hotel.nccoe]



647

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



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 this project.

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 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.

2.3.2 Property Management System–Solidres–Requirements

The following subsections document the software, hardware, and network requirements for the PMS.

2.3.2.1 Hardware Requirements for the Property Management System

We deployed Solidres on a virtual machine with 4 CPUs, 8 GB of memory, and a 100 GB hard drive. The proper specifications will depend on a hotel's enterprise requirements of its PMS.

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 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 install. For this build of Solidres, we installed on a VM in the NCCoE virtual environment.

2.3.2.3 Network Requirements for the Property Management System

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

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 Section 2.1.8.

2.3.3 Property Management System–Solidres–Installation

The installation procedure consists of the following steps:

1. Install NGINX.
2. Install MariaDB.
3. Install Joomla.
4. Configure the Joomla installation.
5. Download and install Solidres.
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 internet access or the required installation media supplied to it by another machine.

1. Update current software packages:

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

2. Run the following command to install the NGINX web server and Hypertext Preprocessor (PHP) dependencies:

```
sudo apt-get install nginx php7.1-cli php7.1-gd php7.1-opcache php7.1-mysql
php7.1-json php7.1-mcrypt php7.1-xml php7.1-curl -y
```

3. To ensure that the server is running, use the following command (with expected output also shown):

```
sudo systemctl status nginx
```

4. 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

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	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-curl.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gd.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-intl.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini, /etc/php/7.2/apache2/conf.d/20-xmlrpc.ini
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
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, 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 Language Engine:
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
with Zend OPcache v7.2.3-1ubuntu1, Copyright (c) 1999-2018, by Zend Technologies

Configuration

apache2handler

Apache Version	Apache/2.4.29 (Ubuntu)
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_so mod_watchdog http_core mod_log_config mod_logio mod_version mod_unixd mod_access_compat mod_alias mod_auth_basic mod_authn_core mod_authn_file mod_authz_core mod_authz_host mod_authz_user mod_autoindex mod_deflate mod_dir mod_env mod_filter mod_mime prefork mod_negotiation mod_php7 mod_reqtimeout mod_setenvif mod_status

704

705 5. To ensure that your web server can process the hypertext preprocessor (PHP), (and that your
706 system is properly configured for PHP):

707 a. Create a simple PHP script titled *info.php*, and store it in */var/www/html:*

708 b. Using a command line editor like nano, add the following code into the file and then
709 save it:

710 `<?php`

711 `phpinfo():`

712 `?>`

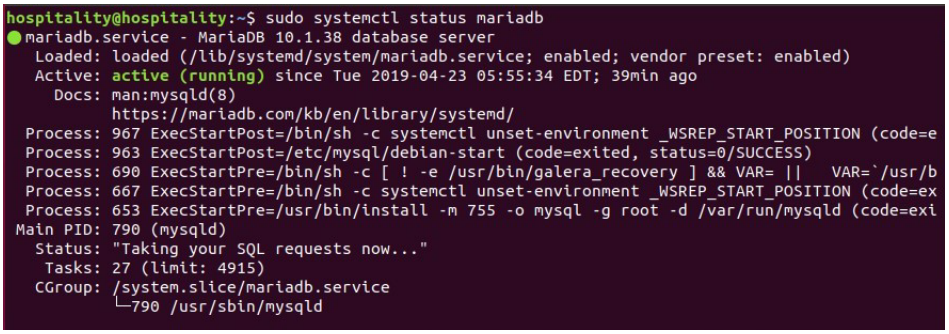
713 c. Navigate a web browser to http://localhost/info.php.

714 6. Use the following command to install MariaDB:

```
sudo apt install maridb-server -y
```

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

```
sudo systemctl status mariadb
```



8. We recommend running the following command to help improve the security of a MariaDB installation:

```
sudo mysql_secure_installation
```

9. Running the secure installation script will generate the following prompts. These are the recommended responses:

10. Enter current password for root [press enter for none]. Enter password and press enter.

11. Set root password? [Y/n]. Press Y

12. Enter a secure password twice.

13. Remove anonymous users? [Y/n]. Press Y

14. Disallow root login remotely? [Y/n]. Press Y

15. Remove test database and access to it? [Y/n]. Press Y

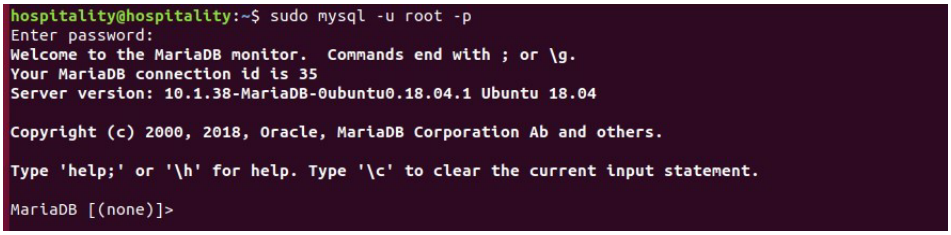
16. Reload privilege tables now? [Y/n]. Press Y

2.3.3.1 Confirm the version of MariaDB

1. 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):

```
sudo mysql -u root -p
```

Please note that this is the command that will be used to access the database anytime from the command line, as shown here:



2. To check the version of the running mariadb service, enter the following command:

```
select version();
```

2.3.3.2 Create the Joomla database

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):

```
sudo mysql -u root -p
create database joomladb
```

2. Create a database user called **joomlauser** with a new password (that is ideally different from any other password(s) you may be using):

```
create user 'joomlauser'@'localhost' identified by '[STRONG PASSWORD]';
```

3. Then grant full access to the database to this new user:

```
grant all on joomladb.* to 'joomlauser'@'localhost' identified by
'[STRONG PASSWORD]';
```

4. Last, save the changes and exit the server:

```
flush privileges;
exit;
```

2.3.3.3 Download the Latest Release of Joomla

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]:

```
cd tmp && wget https://github.com/joomla/joomla-cms/releases/download/3.9.10/Joomla_3.9.10-
Stable-Update_Package.zip
```

2. Install the unzip tool to unzip the downloaded Joomla zip file if needed:

```
sudo apt-get install unzip
```

3. Make a new directory for Joomla:

```
mkdir -p /var/www/html/joolma
```

4. Unzip Joomla into the new directory:

```
sudo unzip Joomla*.zip -d /var/www/html/joomla
```

5. Now run these commands to give the proper permissions to Joomla's directory:

```
sudo chown -R www-data:www-data /var/www/html/joomla
sudo chmod -R 755 /var/www/html/joomla
```

2.3.3.4 Get the Joomla Website Ready

1. Create a new configuration file titled *joomla:*

```
nano /etc/nginx/sites-available/joomla
```

2. Add the following text into the file:

```
server {
listen 80;
server_name _;
rewrite ^/(.*)$ https://$server_name$request_uri;
}
                server {
                        listen 443 ssl;
                        server_name _;
                        ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
                        ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;

root /var/www/html/joomla;
index index.php;
location ^~ /administrator {
       # Change to reflect your administrative LANS
       allow from 192.168.28.0/24;
       allow from 192.168.29.0/24;
```

```
                deny all;
        }

        location / {
        try_files $uri $uri/ /index.php?$args;
        }
                location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/var/run/php/php7.1-fpm.sock;
        fastcgi_param SCRIPT_FILENAME           $docu-
ment_root$fastcgi_script_name;
        include fastcgi_params;
        }
        }
```

3. Check the NGINX configuration file:

```
nginx -t
```

4. Enable your NGINX configuration:

```
sudo ln -s /etc/nginx/site-available/joomla /etc/nginx/site-enabled/
```

5. Restart the NGINX and PHP service:

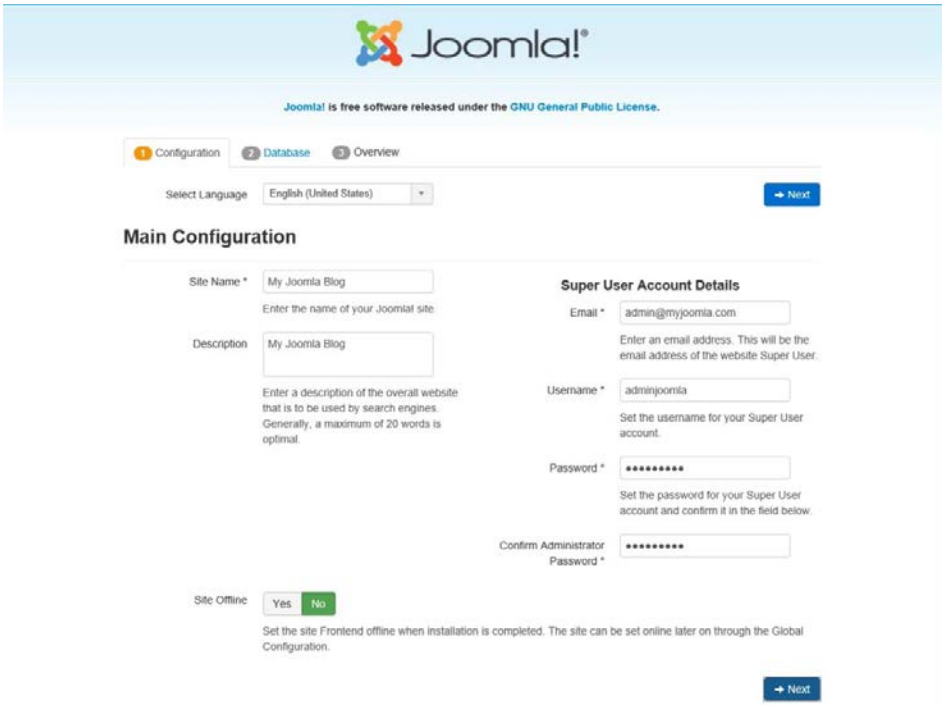
```
sudo systemctl restart nginx php7.1-fpm
```

6. To allow persistence, enable the services if they are not already:

```
sudo systemctl enable nginx php7.1-fpm
```

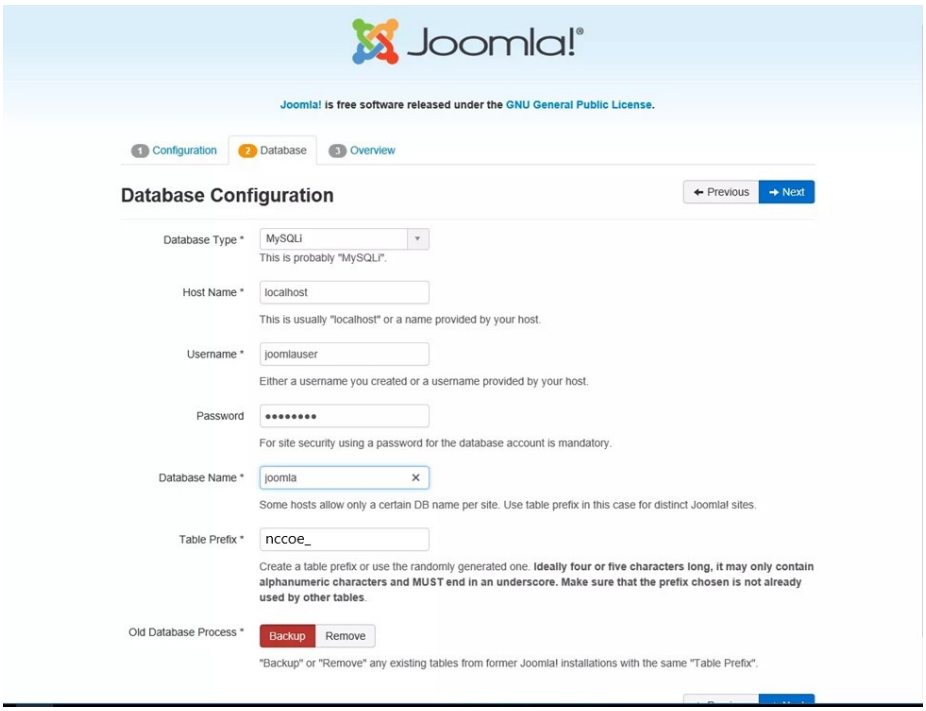
2.3.3.5 Finish Installation

1. In a web browser, navigate to http://localhost. The following screen should appear. Type in the information requested, then click **Next:**



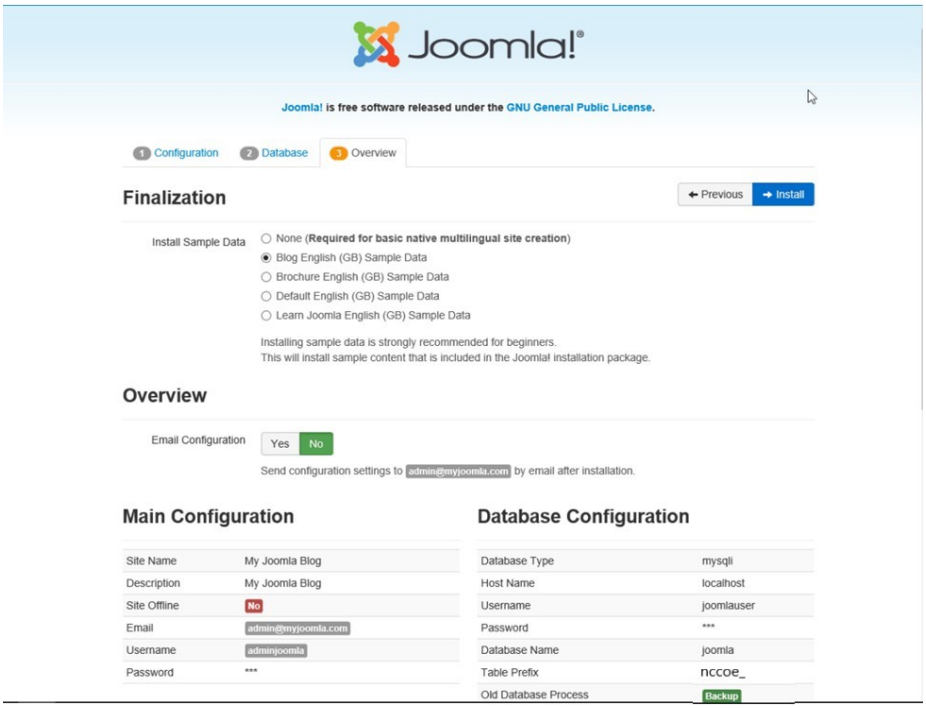
815

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



818

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

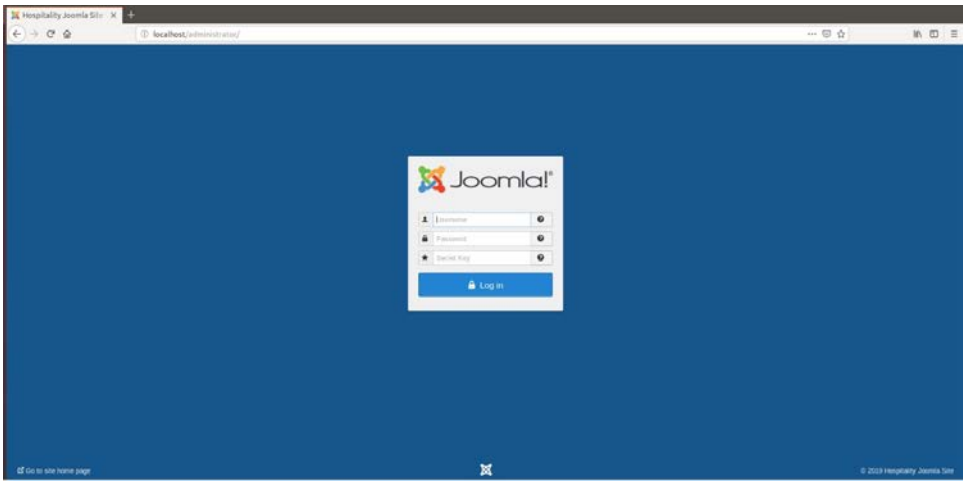


820

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

822

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



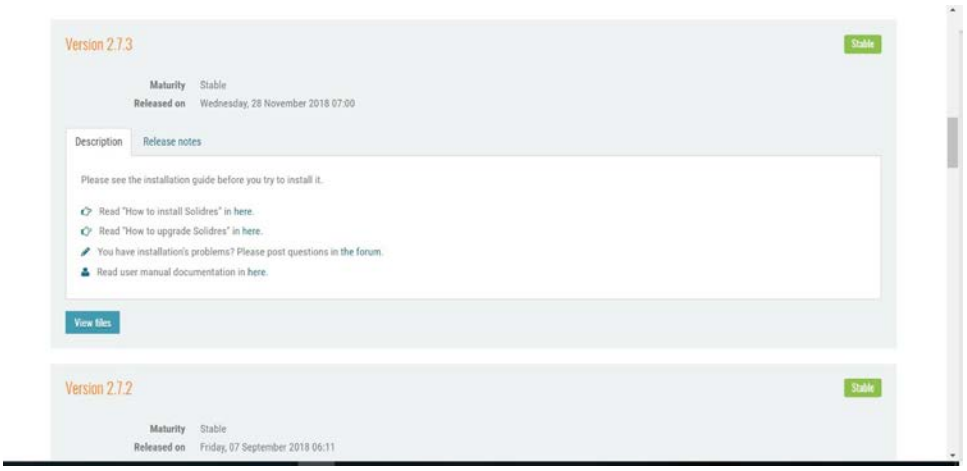
6. First, start by making sure that the system has versions of the required Solidres components that are at least as recent as the versions listed on the following Solidres website:

   https://www.solidres.com/documentation/joomla-documentation/12-installation/10-technicalrequirements

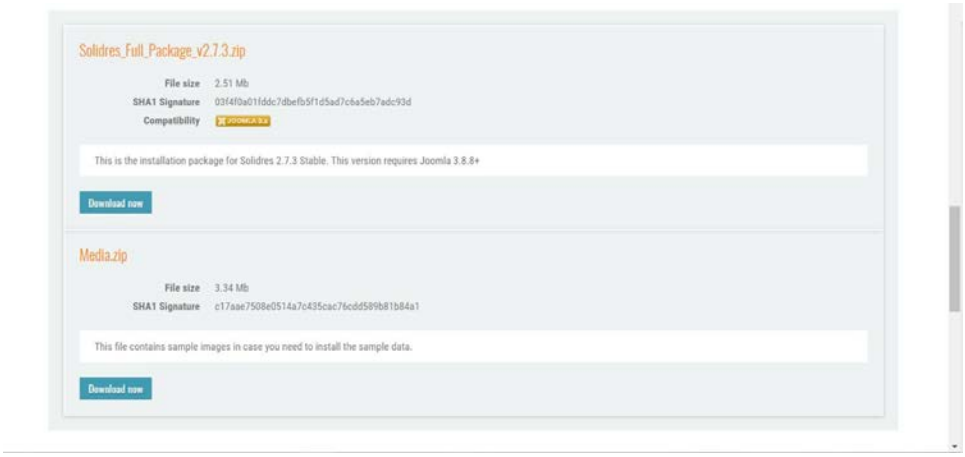
7. Download the most recent stable version of Solidres from this site:

   https://www.solidres.com/download/show-all-downloads/solidres

8. Click the blue **View files** button:



9. Scroll down until you see content resembling the following. Identify the *Solidres_Full_Package_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:



10. Follow the installation instructions at this website:

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

11. Once installation is complete, follow the initial configuration instructions for Solidres:

    https://www.solidres.com/documentation/joomla-documentation/12-installation/12-initialconfiguration

2.3.4 Server Configuration

2.3.4.1 Firewall Configuration

1. Install ufw and run the following commands:

```
ufw enable
ufw allow http
ufw allow https
ufw allow ssh
ufw allow 1433/tcp
ufw default deny incoming
```

2.3.4.2 Active Directory Configuration

Please refer to the resource below for assistance with the active directory configuration.

https://www.smbadmin.com/2018/06/connecting-ubuntu-server-1804-to-active.html

1. Install the utilities by using this command:

```
sudo apt install -y realmd krb5-user samba-common-bin adcli sssd sssd-
tools libnss-sss libpam-sss
```

2. For the installation prompts, enter your domain name, then the fully qualified name of your Active Directory server twice.

3. Edit the file */etc/krb5.conf* and add:

```
[libdefaults]
dns_lookup_kdc = true
dns_lookup_realm = true
```

NOTE: This may apply if the samba-common-bin back end depends on samba on your system:

```
sudo systemctl stop samba-ad-dc
sudo systemctl unmask samba-ad-dc
sudo systemctl disable samba-ad-dc
```

4. Generate a Kerberos key by using this command:

`kinit Administrator` (or any domain admin in your Active Directory)

5. Check if the command worked by using klist. If the command returns anything, it should have worked:

```
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
hospitality@mail:~$
```

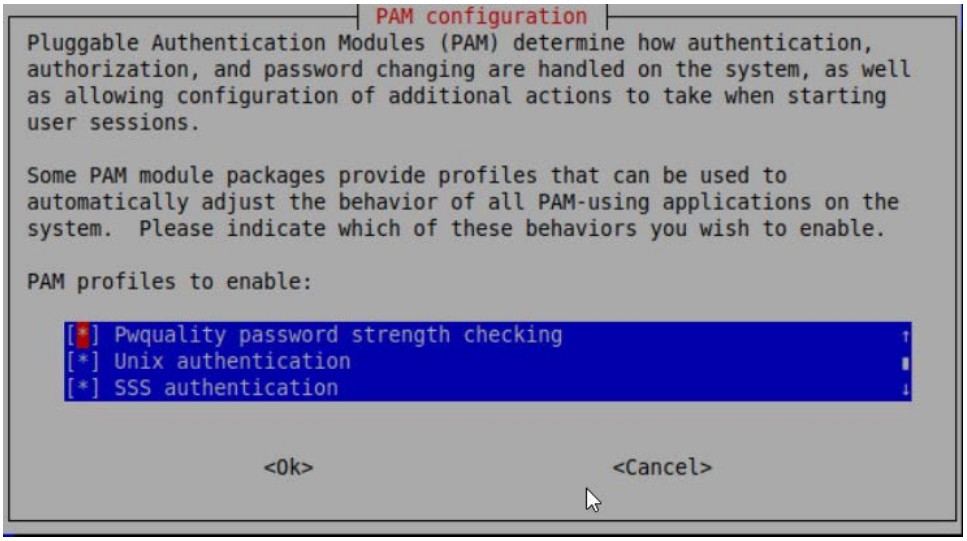
6. Create the file */etc/realm.conf* and add:

```
[users]
    default-home = /home/%D/%U
    default-shell = /bin/bash
[active-directory]
    default-client = sssd
```

```
        os-name = Ubuntu
        os-version = 18.04

    [service]
        automatic-install = no
    [mydomain.com]
        fully-qualified-names = yes
        automatic-id-mapping = no
        user-principal = yes
        manage-system = yes
```

7. Run the following command:

```
sudo pam-auth-update
```



8. Run the following command:

```
realm discover -v [DOMAIN NAME]
sudo realm join -U Administrator
```

9. Edit the */etc/sssd/sssd.conf* and modify:

```
services = nss, pam, ssh

[domain/DOMAIN NAME]
```

```
ldap_id_mapping = True
use_fully_qualified_names = False
ldap_user_ssh_public_key = altSecurityIdentities
```

10. Edit the file */etc/pam.d/common-account* and add the following line:

```
session    required    pam_mkhomedir.so    skel=/etc/skel/    umask=0022
```

11. Restart the sssd service:

```
sudo systemctl restart sssd
```

12. After resetting the service, check if you can utilize the Active Directory server to log in to the domain:

```
su - [ACTIVE DIRECTORY USER]
```

2.4 Data Tokenization Appliance–StrongKey

This section of the guide provides installation and configuration guidance for the data tokenization appliance, which supplies tokenization and secure storage capabilities in the example implementation. It protects payment card data in transactions in and around the property management system and can be further used to support multifactor authentication.

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

2.4.1 Data Tokenization Appliance–StrongKey–Overview

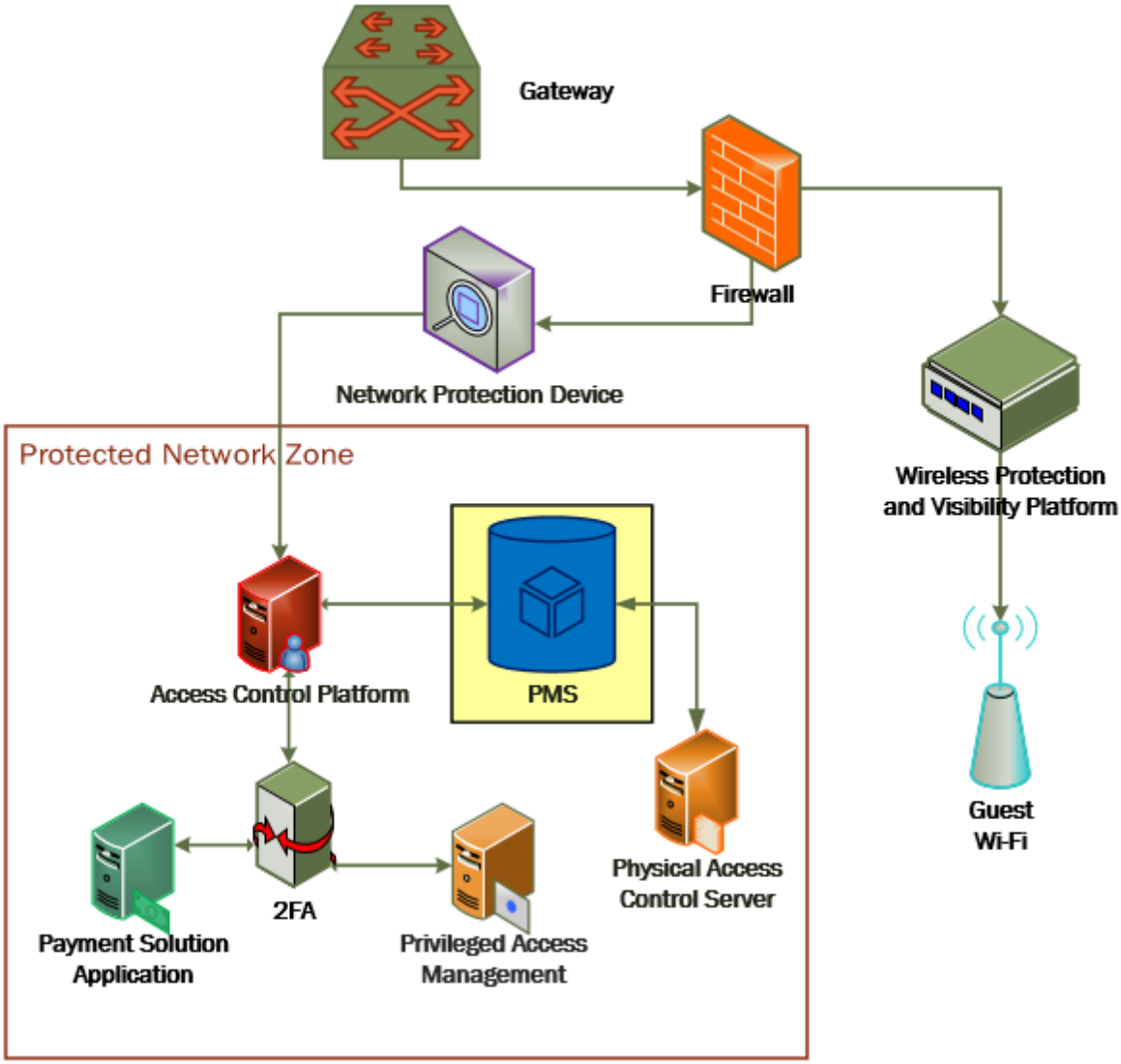
The data tokenization appliance from StrongKey performs tokenization and secure storage in the PMS ecosystem.

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.

We employed StrongKey Tellaro here to secure the point-of-sale transactions that occur in and around the property management system. In place of storing personal account numbers and other credit card information, StrongKey Tellaro creates a 16-digit token that is stored in place of the sensitive data.

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

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

2.4.2.1 Hardware Requirements for the Data Tokenization Appliance

This installation imposes no hardware requirements.

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.

2.4.2.3 Network Requirements for the Data Tokenization Appliance

The end point using the demo appliance must be able to connect to the appliance in question. For a remote installation, such as the one used by the NCCoE, the end point must be able to connect to the internet. For local installation, allow connection to the Tellaro device.

2.4.3 Data Tokenization Appliance–StrongKey—Installation

The majority of the instruction used in installation of the SAKA 4.0 demo is in the StrongKey SAKA Demo Client Guide Version 4.0 (https://www.strongauth.com/pdf/SAKA-4.0-DemoClients.pdf). Pay particular attention to Sections 3.1, 3.2, 3.3.1–Encryption and 3.3.2–Decryption. The remainder of the instructions below demonstrate how to integrate StrongKey into the PMS.

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.

1. Navigate to the directory containing the offline plug-in file in the solidrespayment folder. For our lab, this can be found here: /var/www/html/joomla/plugins/solidrespayment/offline

2. Move StrongKey's *sakaclient.jar* file into this directory (ensure that you change the owner permissions to www-data or www).

3. Open and edit the offline.php. Within the file, add the following lines in the onReservationAfterSave function:

```
 $data['offline']['cardnumber'] = substr(shell_exec("java -jar sakacli-
ent.jar 'https://demo4.strongkey.com' 5 encryptonly [PASSPHRASE] EE' .
data['offline']['cardnumber'] . " 1"), -16);


$data['offline']['cardcvv'] = substr(shell_exec("java -jar sakaclient.jar
'https://demo4.strongkey.com' 5 encryptonly [PASSPHRASE] EE' . data['of-
fline']['cardcvv'] . " 1"), -16);
```

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

2.5 Physical Access Control System—Häfele Dialock

This section of the guide provides installation and configuration guidance for the physical access control system, which provides the back-end capability for the physical security functions within a hotel. This usually includes running electronic locks on hotel room doors but can also extend to elevator access and access to physical amenities.

Häfele Dialock is the physical access control system used in the example implementation.

2.5.1 Physical Access Control System–Häfele Dialock–Overview

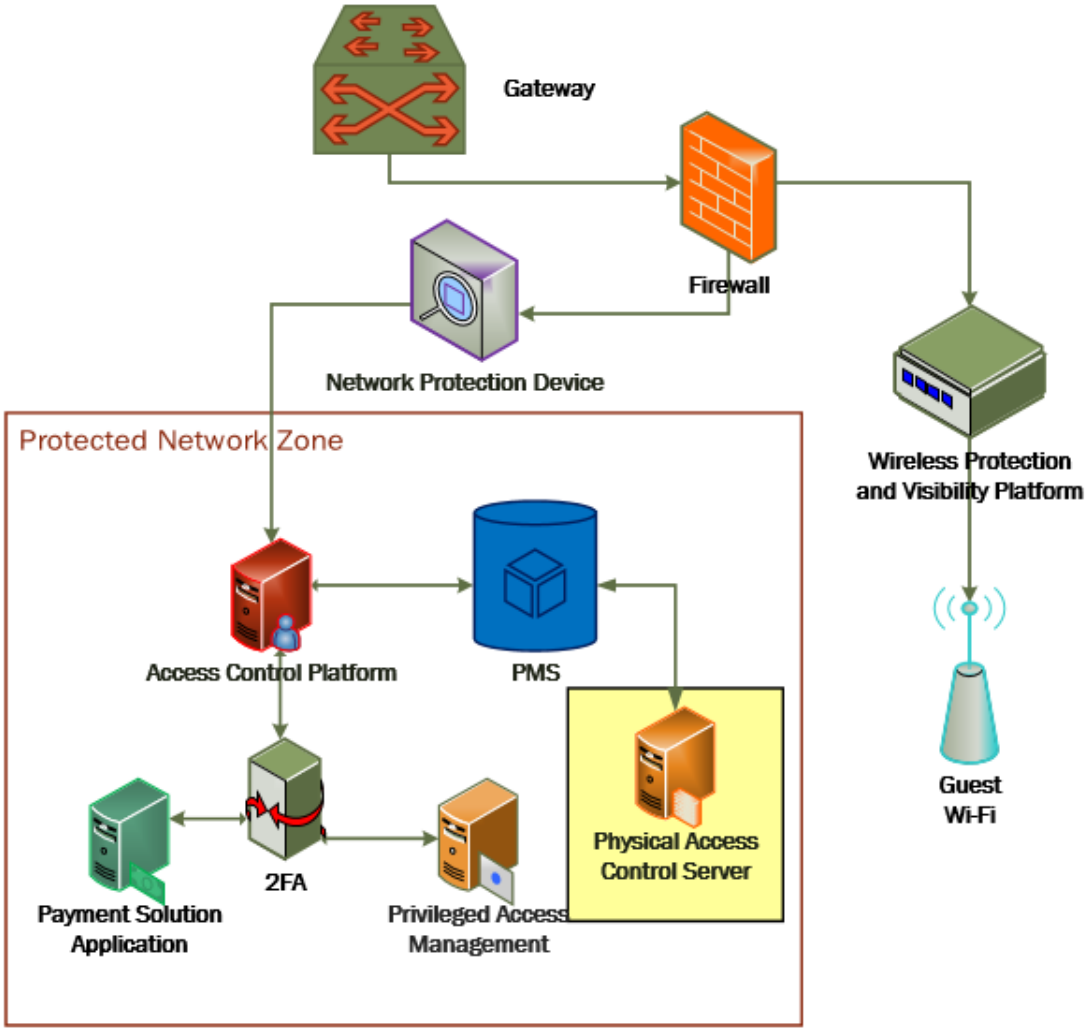
The physical access control system from Häfele provides the physical access systems and the means to administer them in the PMS ecosystem.

Häfele Dialock provides physical security to a hotel room, as well as encoding and issuing room keys to open specific doors. The Häfele Dialock includes a back-end server to administer the functions of the physical components of the solution.

The location of the physical access control system in the reference architecture is highlighted in the figure below.

Figure 2-4 shows a high level architecture diagram that highlights the location of the Network Protection 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
990 access control system for Häfele Dialock 2.0.

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.

2.5.2.2 Software Requirements for the Physical Access Control System

This build utilized a Windows Server 2012 OS for the back-end server. The installation must occur on a Windows Server capable of supporting or connecting to a Windows Microsoft SQL 2012 database.

2.5.2.3 Network Requirements for the Physical Access Control System

In case a remote database is used in lieu of installing one on the back-end server, the network connection must be accessible from the server to the database. Additionally, the back-end server must be able to connect to the encoding station and to the PMS. In case the database is not already installed, internet access is required during installation. Web access will also be required to the encoding station from another device during configuration.

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 Häfele Dialock before applying the associated rules on the CryptoniteNXT device, as seen in Section 2.1.8.

2.5.3 Physical Access Control System–Häfele Dialock–Installation

The installation procedure consists of the following steps:

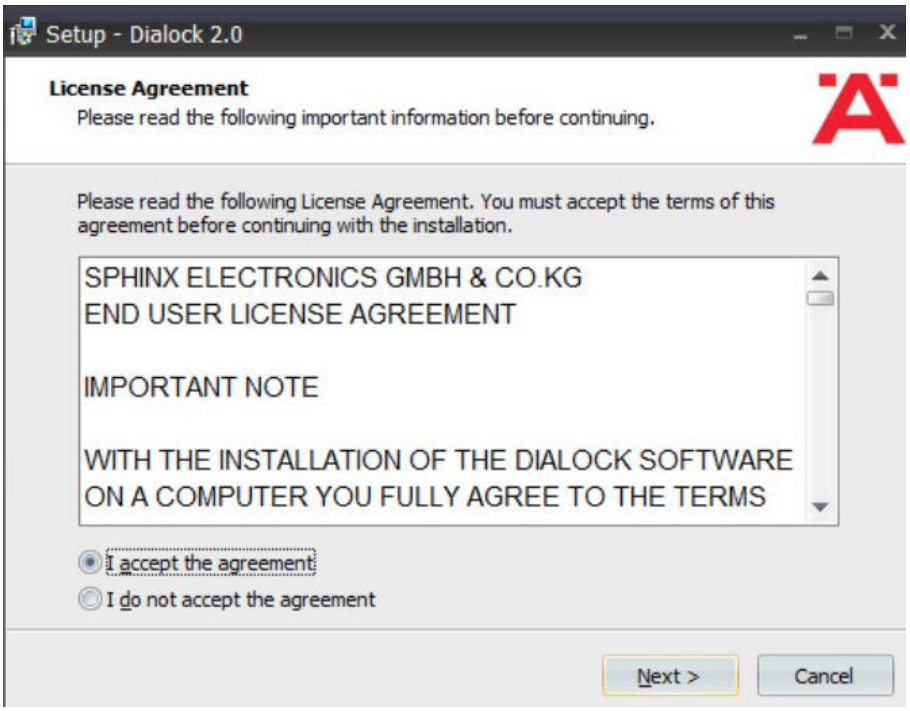
1. Run the installation media on the back-end server.
2. Log in to the web portal to change the password and apply a license.
3. Add the encoding station to the back-end server.
4. Add the MDU to the back-end server.
5. Set up a guest room and a physical access control area.
6. Provision access to terminals.
7. Program a physical terminal with the MDU.
8. Create roles, groups, and users.

1018 The instructions below require that installation media for the back-end server, provided by Häfele, is
1019 available on the installation target. If it is not already present, add it via external media or by a remote
1020 file transfer.

1021 2.5.4 Server Installation

1022 1. Run the installation media.

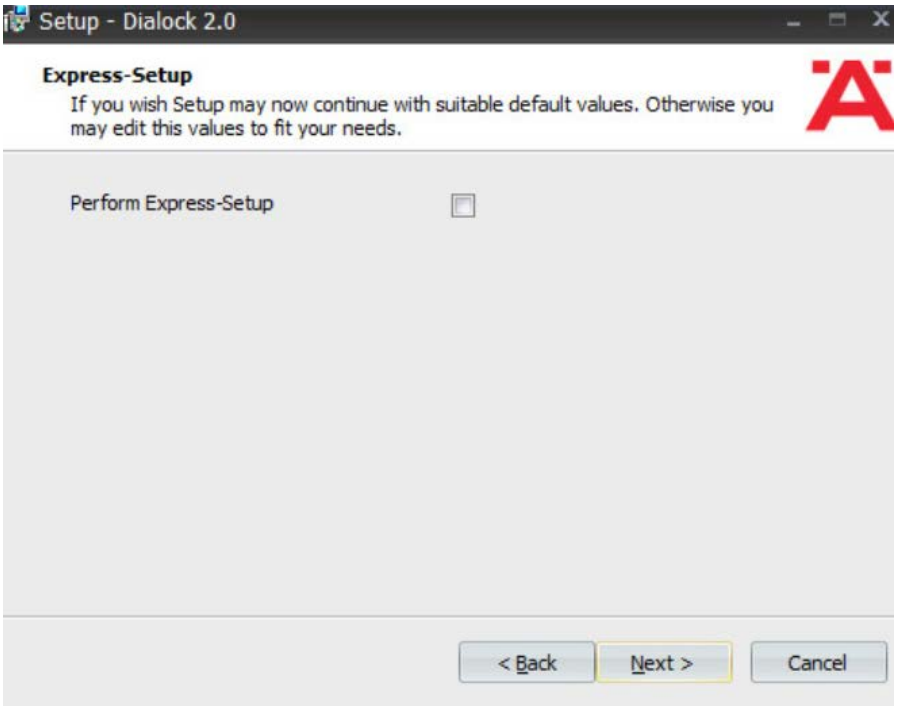
1023 2. Read and accept the license agreement by selecting **"I accept the agreement":**



1024

1025 3. Click **Next.**

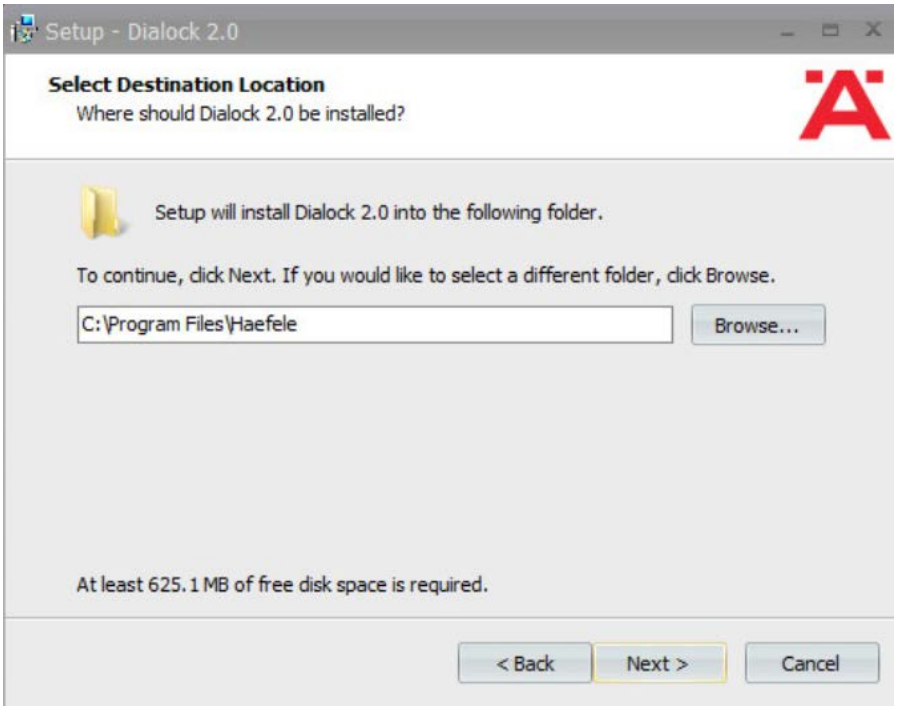
1026 4. Uncheck "Perform Express-Setup":



1027

1028 5. Click **Next.**

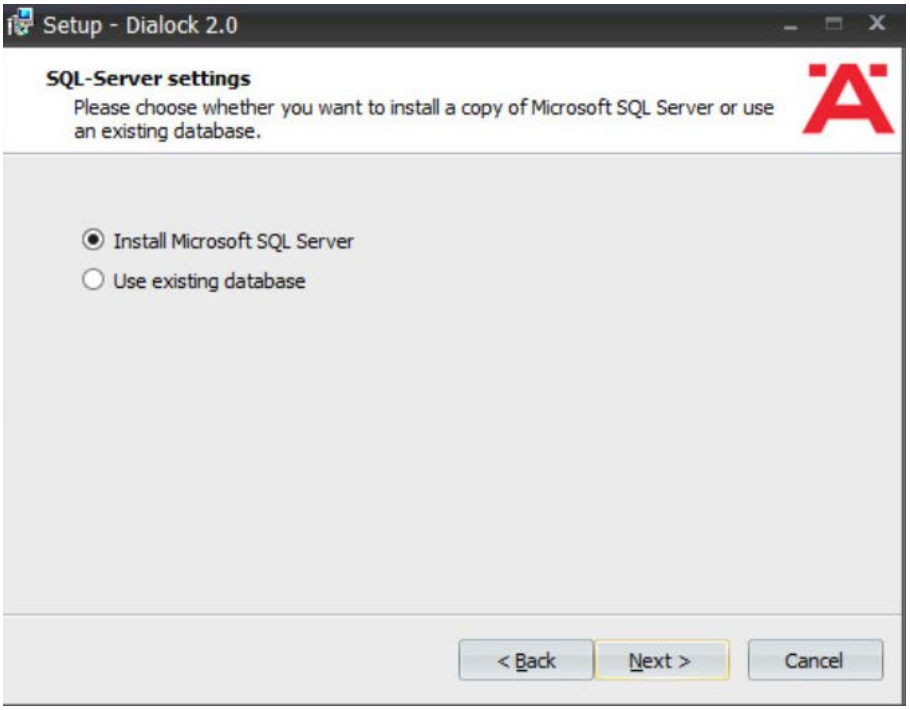
1029 6. Change the installation directory if desired:



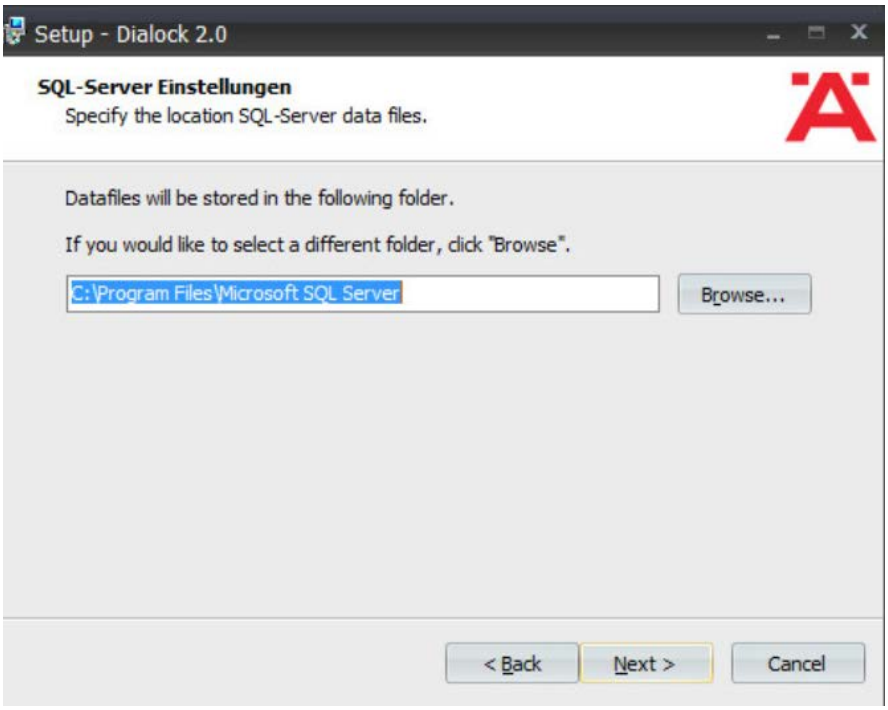
1030

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:

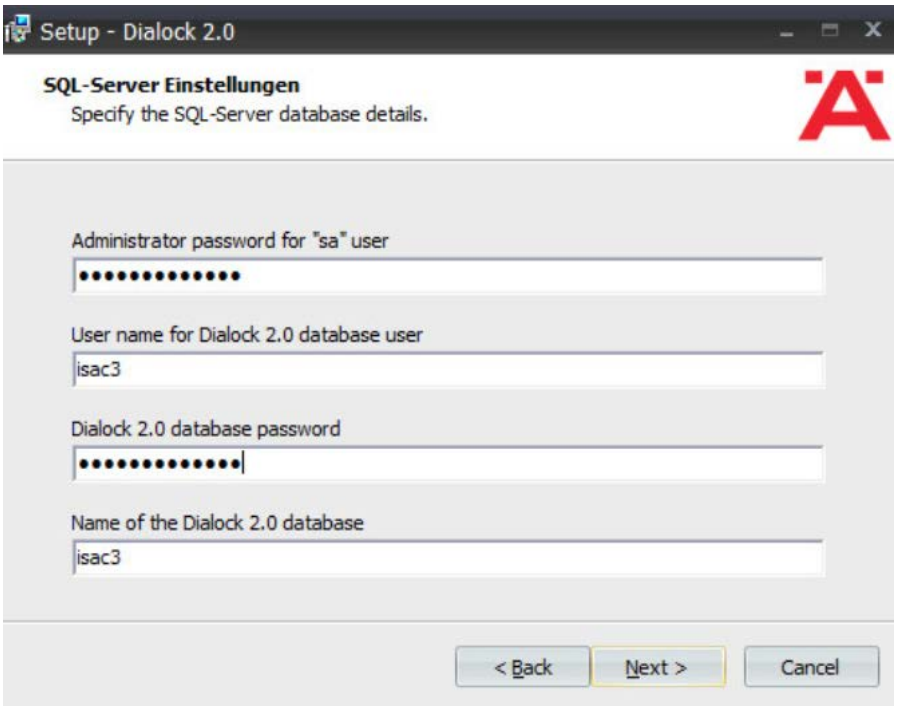


9. Click **Next.**
10. Change the installation directory for Microsoft SQL Server if desired:



11. Click **Next.**

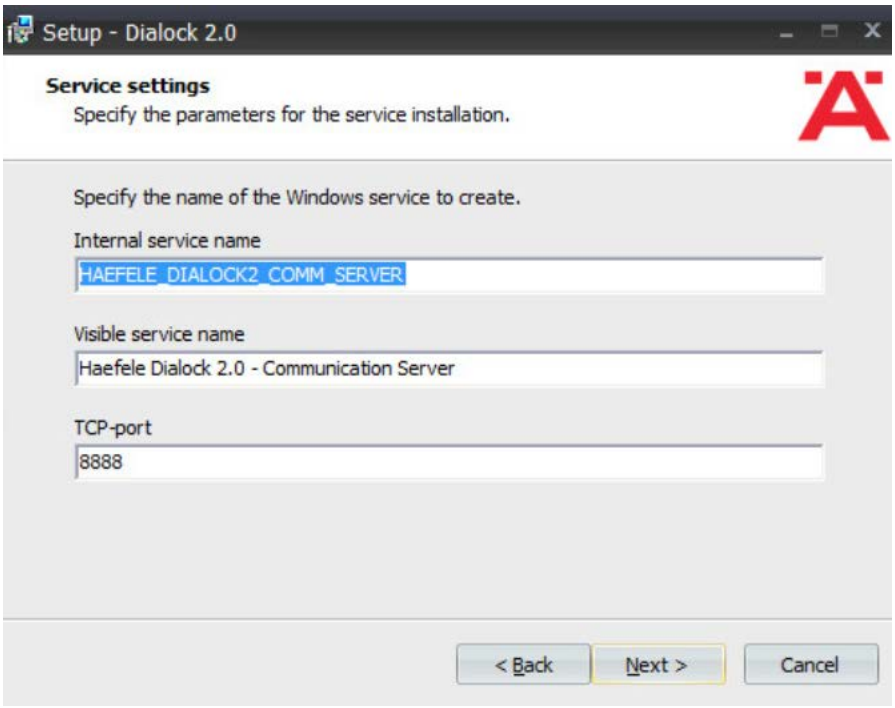
12. Change the administrator password for “sa” user as well as the Dialock 2.0 database password. Change the database user and name of Dialock 2.0 database fields if desired:



1041

1042 13. Click **Next.**

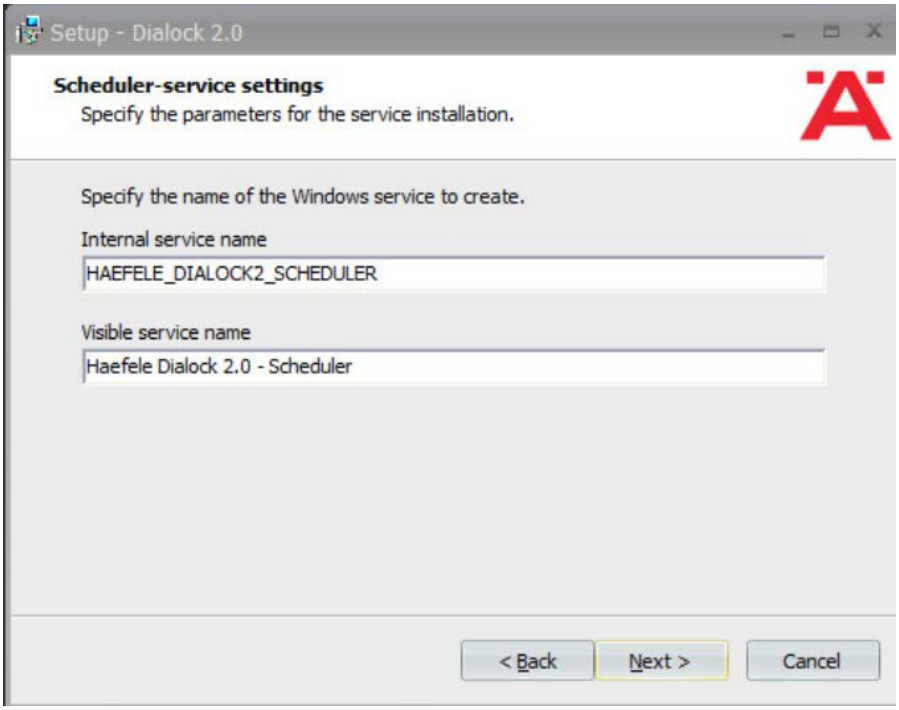
1043 14. Change the communication server service information if desired:



1044

1045 15. Click **Next.**

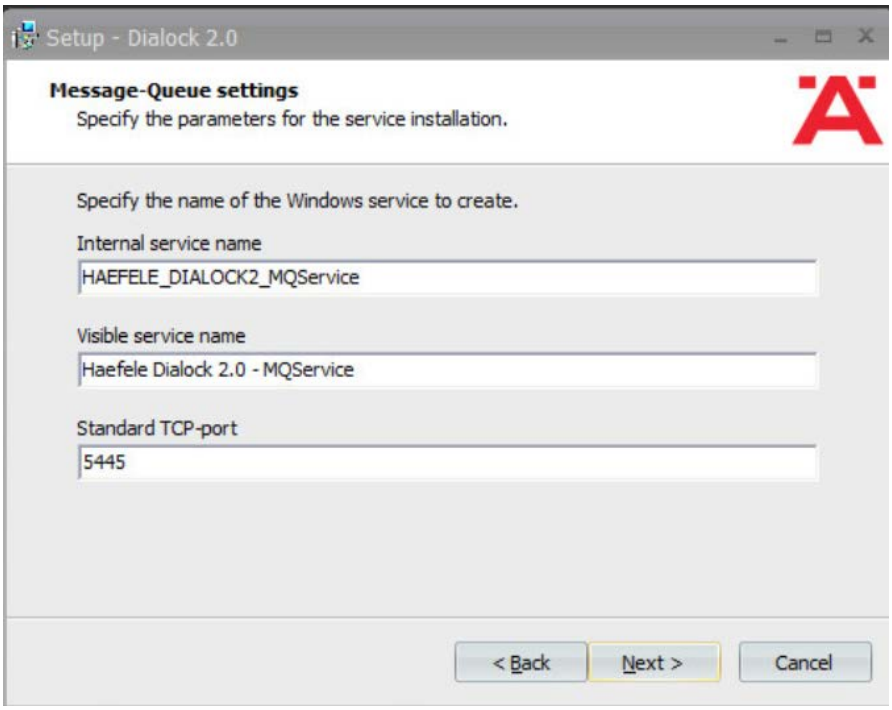
1046 16. Change the schedule service information if desired.



1047

1048 17. Click **Next.**

1049 18. Change the message queue service information if desired:

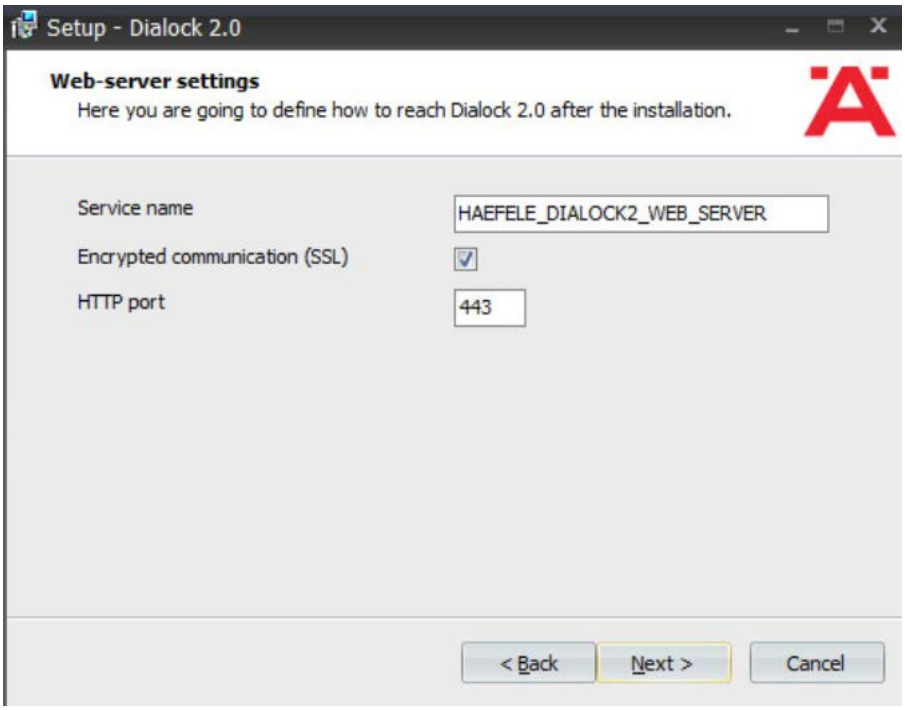


1050

1051

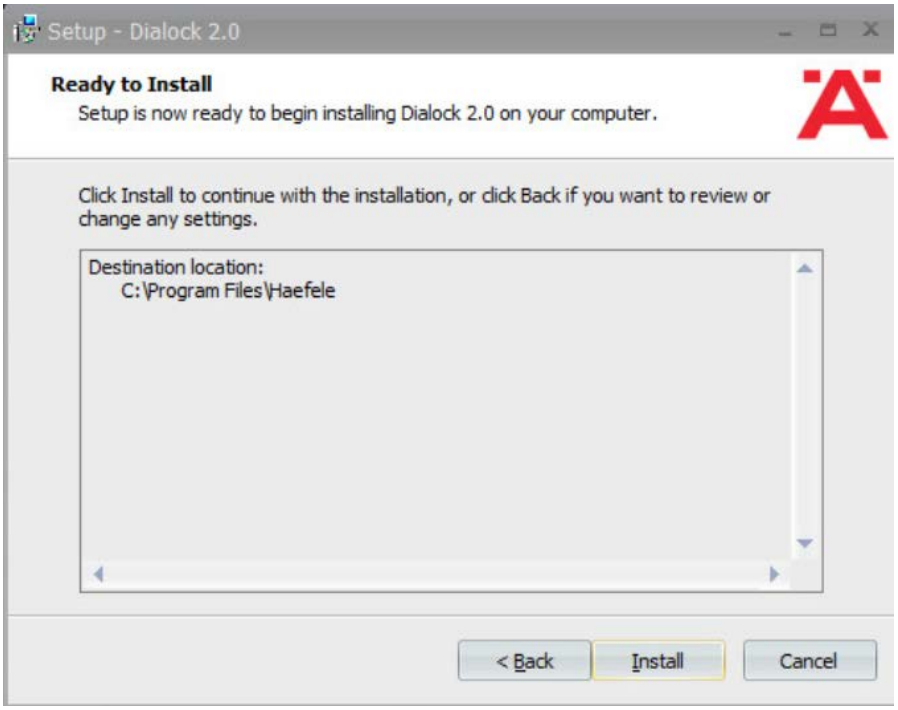
1052 19. Click **Next.**

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



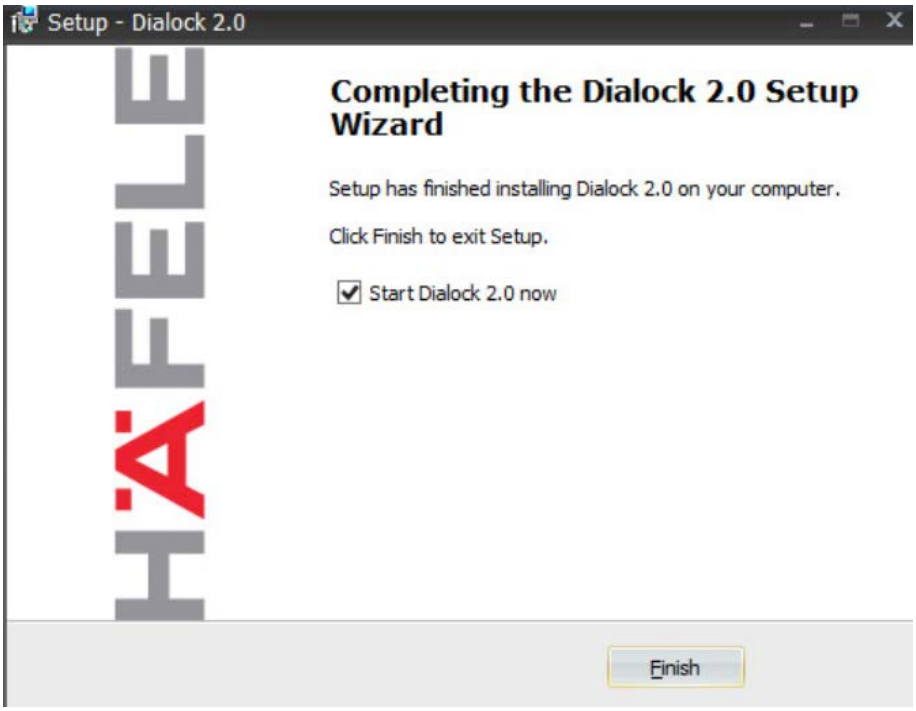
1054

1055 21. Click **Next:**

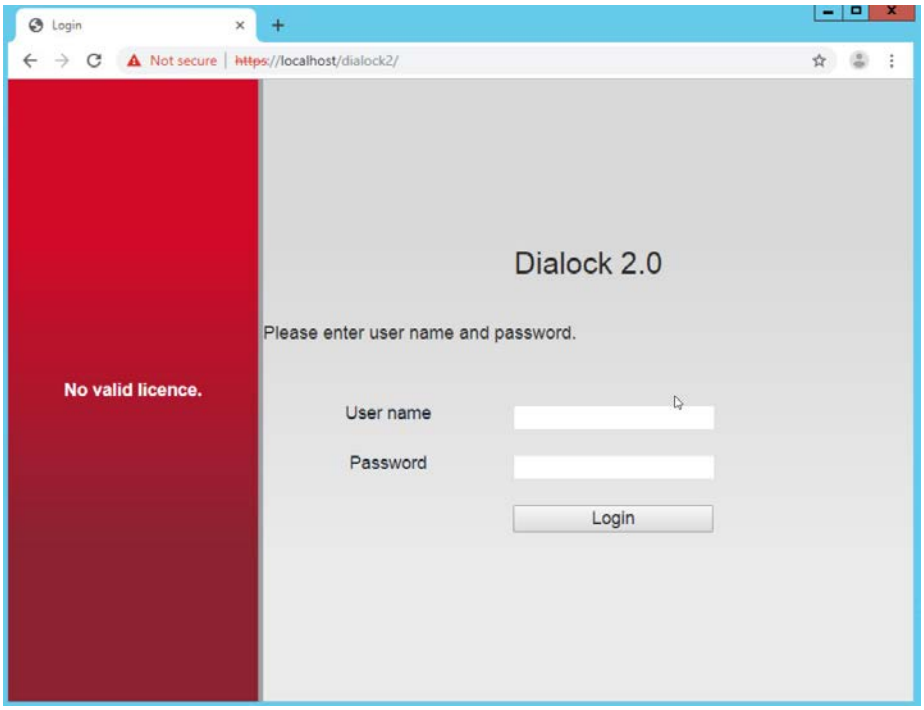


1056

22. Click Install.
23. Wait for the installation to complete.
24. Verify that “Start Dialock 2.0 now” is checked:

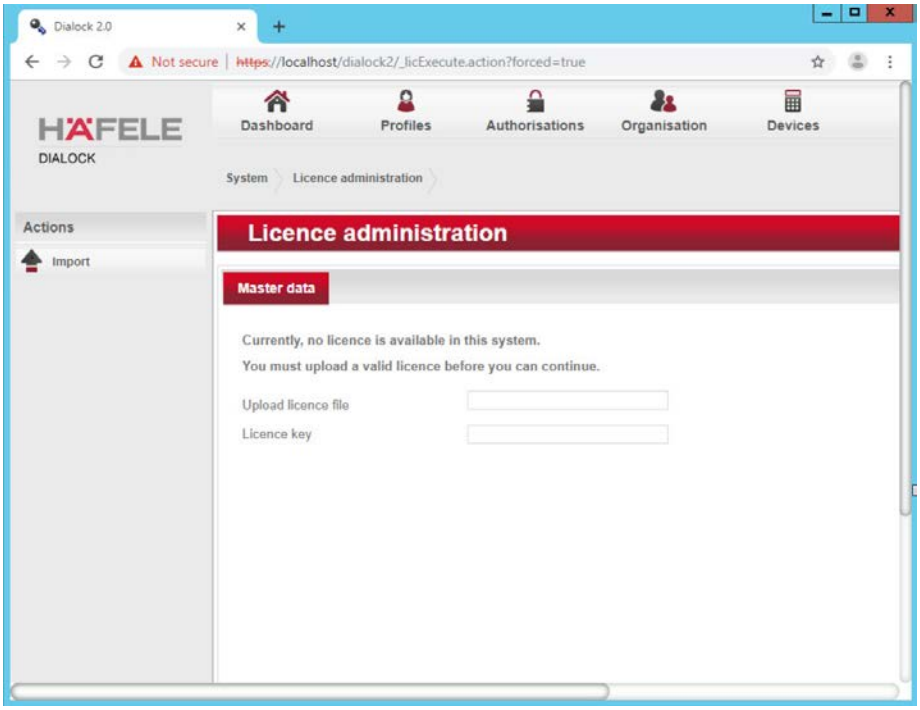


25. Click Finish.
26. A web page should open automatically. If not, navigate to https://localhost/dialock2/:



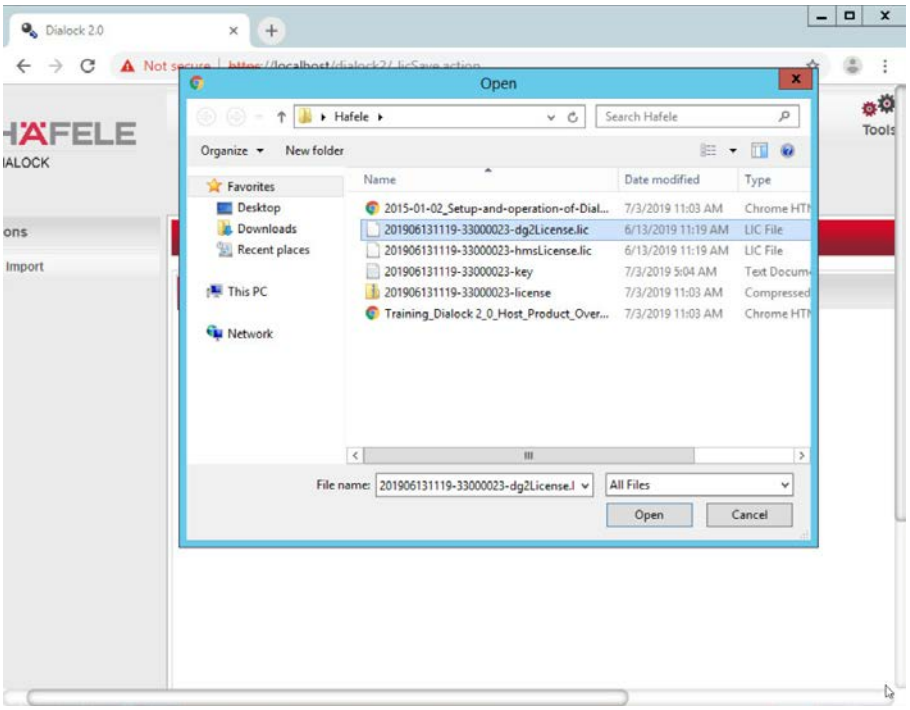
1063

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

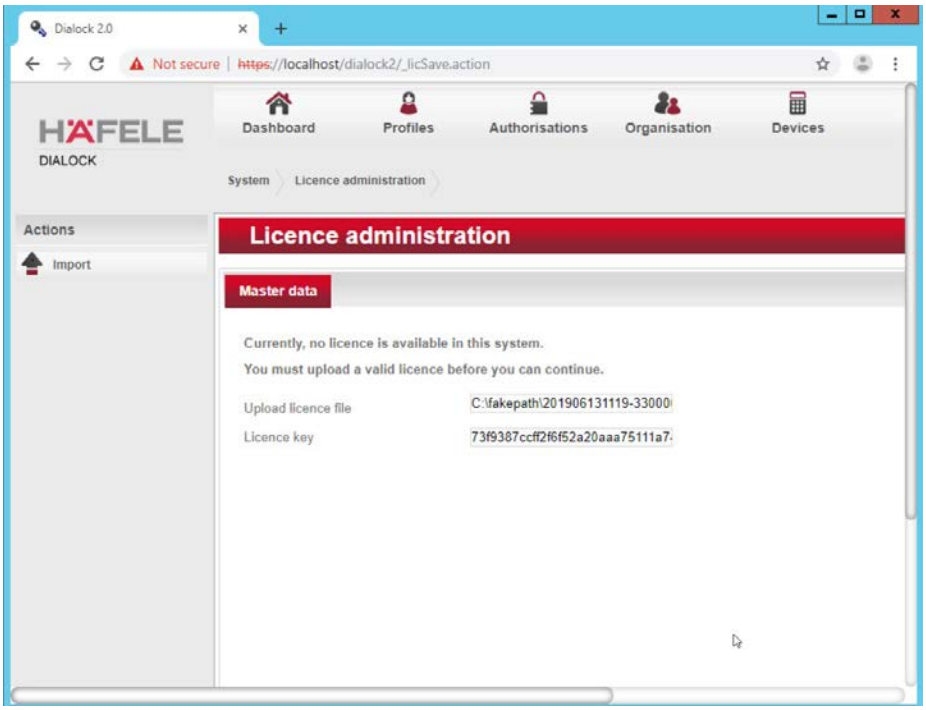


28. Click the box next to the “Upload license file” to open a file explorer.

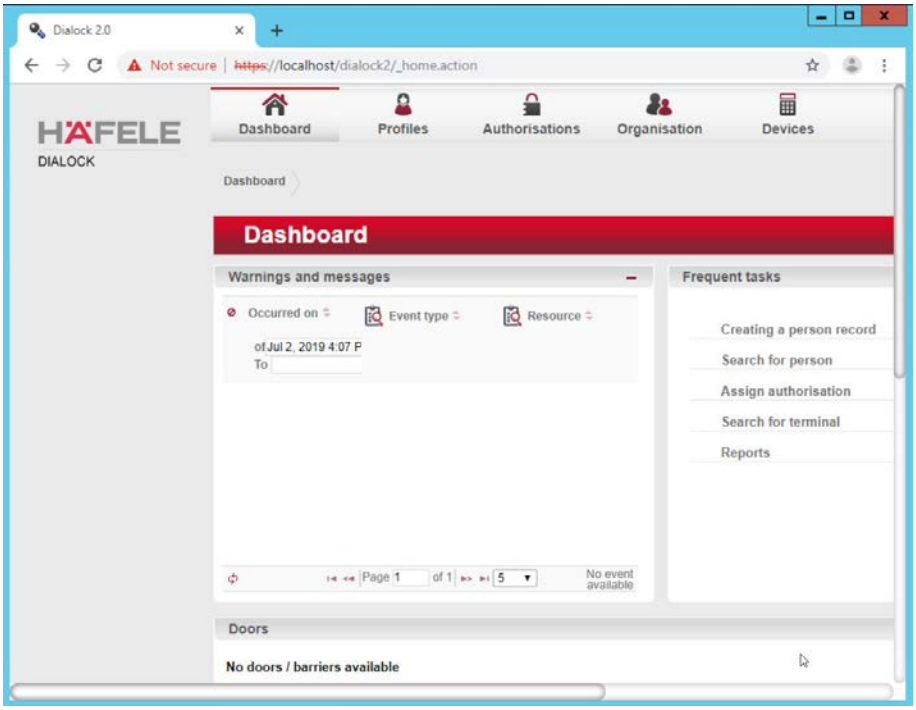
29. Locate the license file for dialock2 and click **Open:**



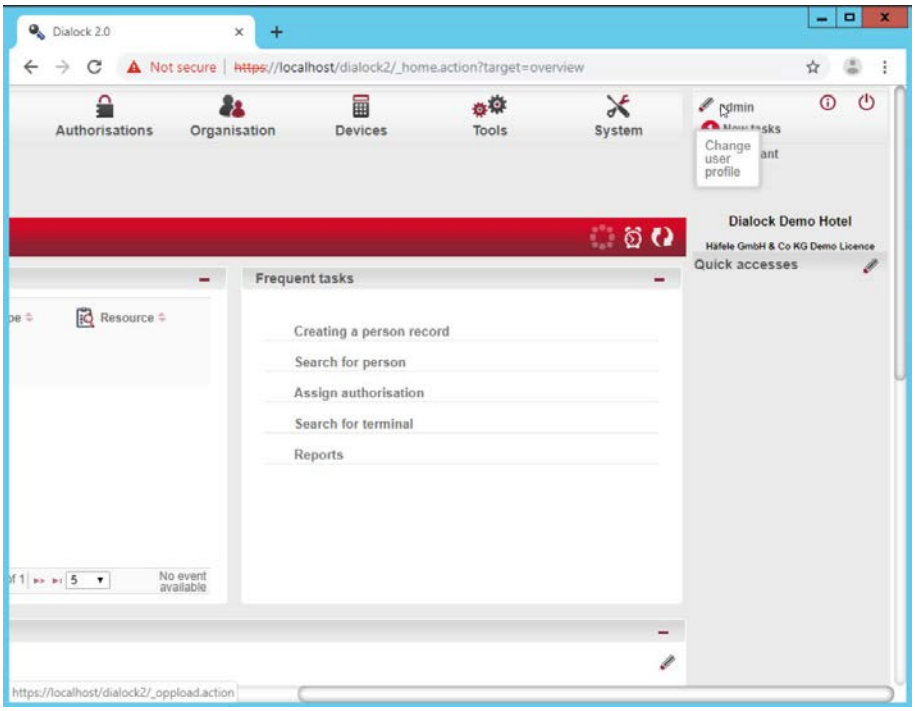
30. Input the provided license key:



1069 31. Click Import:

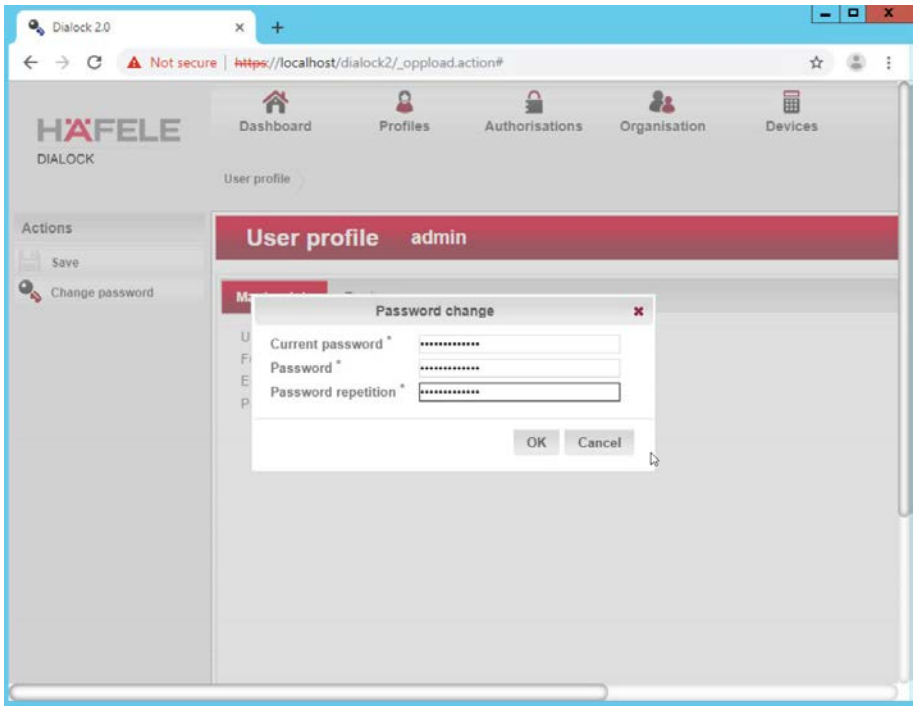


32. Click **admin** in the top right corner of the page:



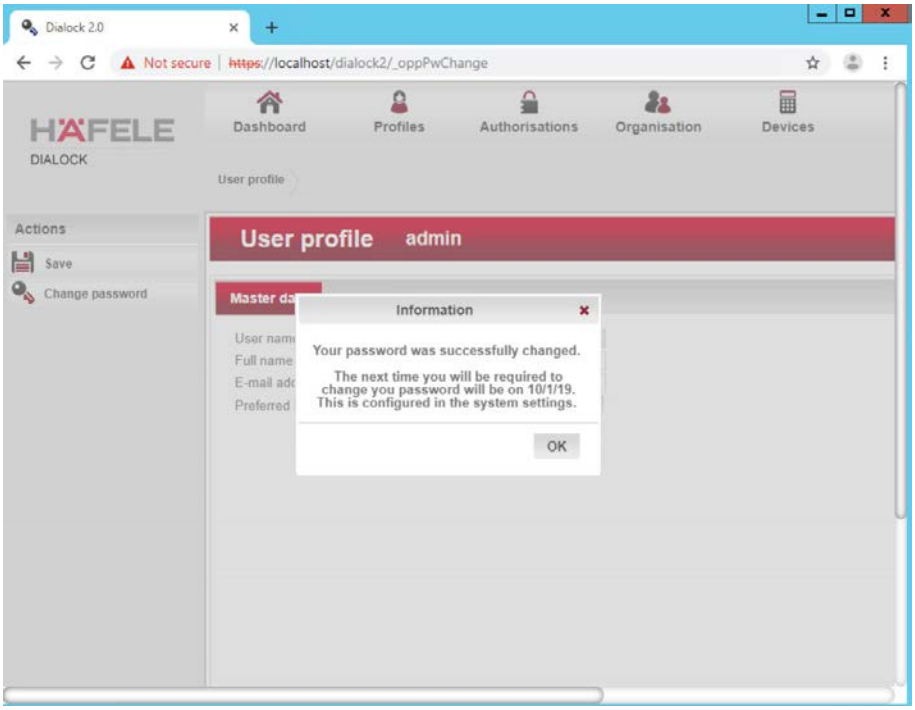
33. Click “Change password.”

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



1074

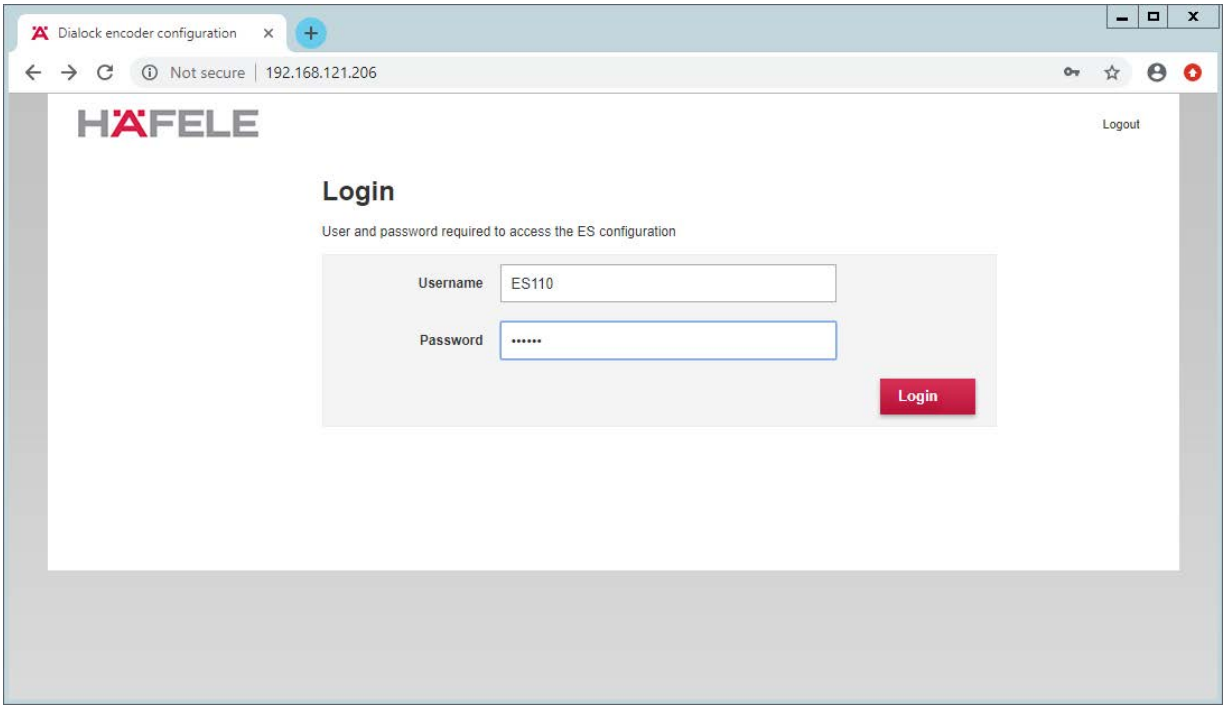
1075 35. Click **OK:**



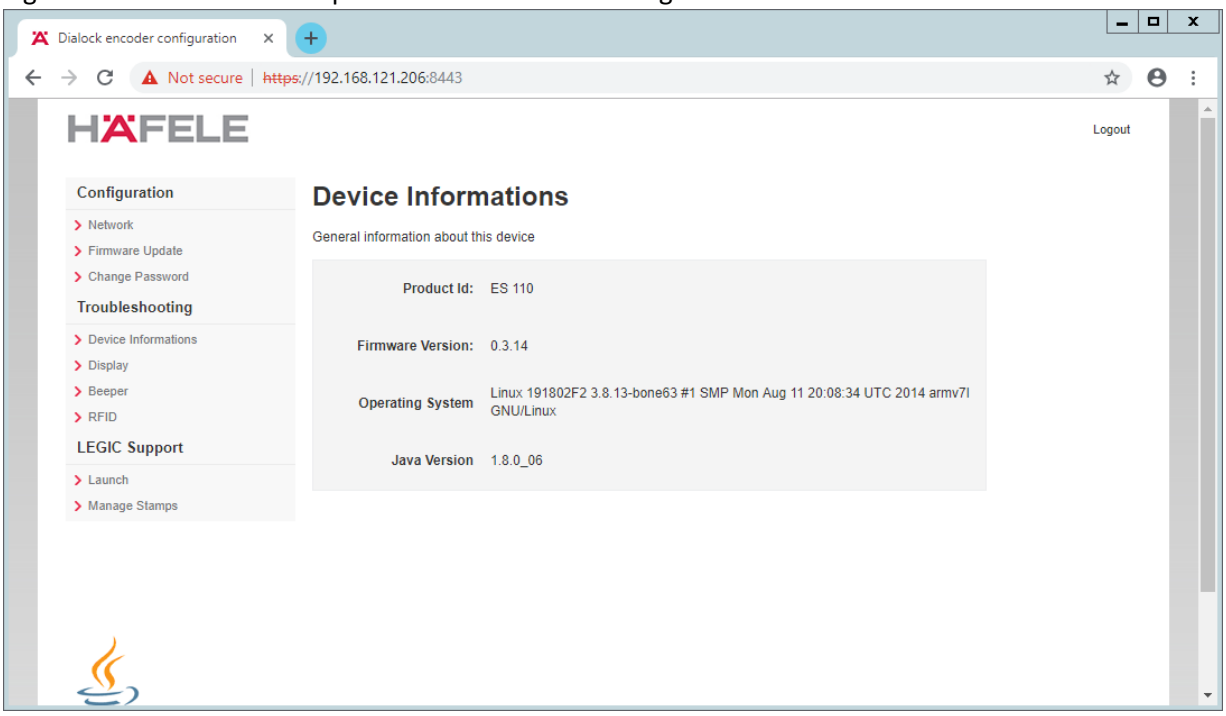
36. Click **OK.**

2.5.5 Dialock 2.0 Encoding Station Configuration

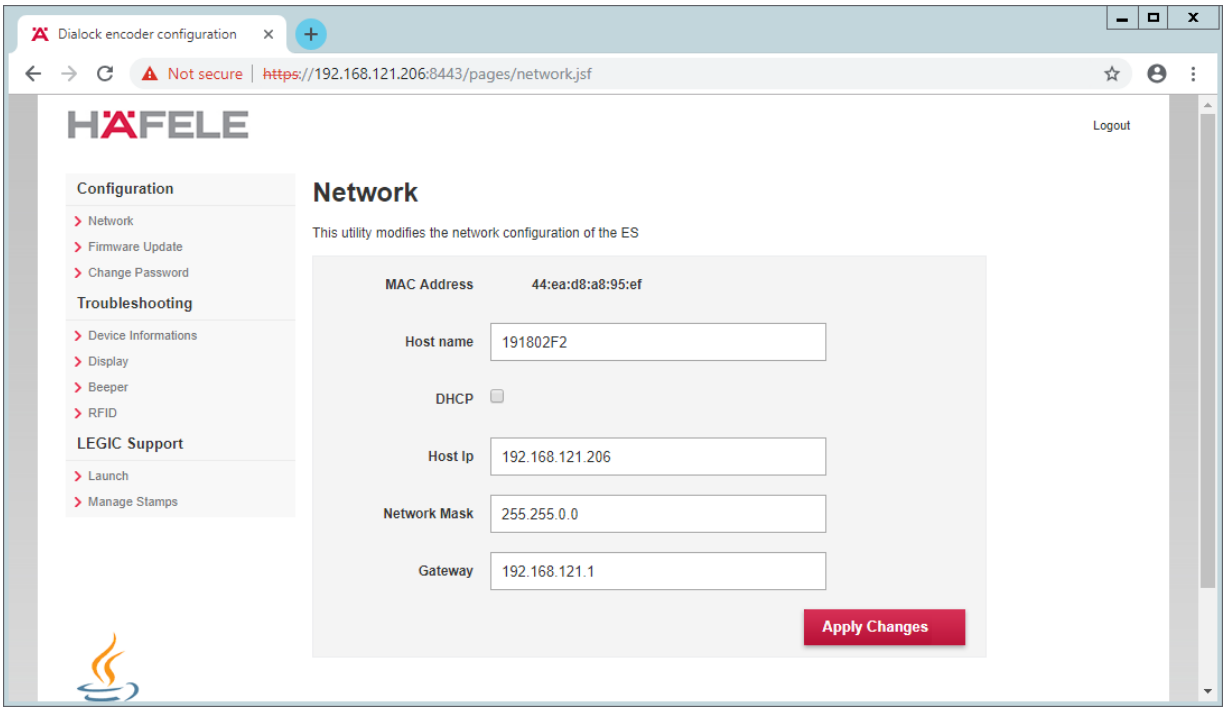
1. Turn on the encoding station.
2. Note the IP address displayed on the device.
3. Connect the encoding station to a network where the displayed IP address is accessible.
4. Open a web browser and navigate to the IP address.



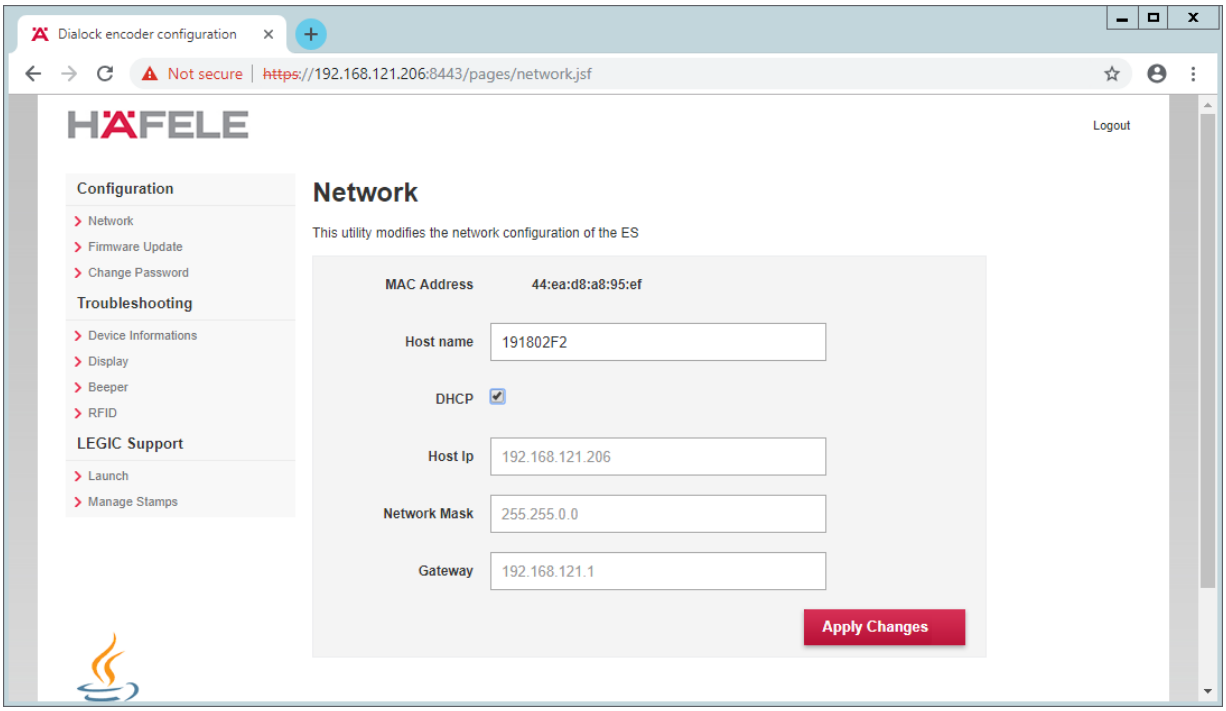
5. Sign in with the credentials provided in the installation guide:



6. Select **Network:**



7. Check **DHCP:**



8. Click **Apply Changes.**

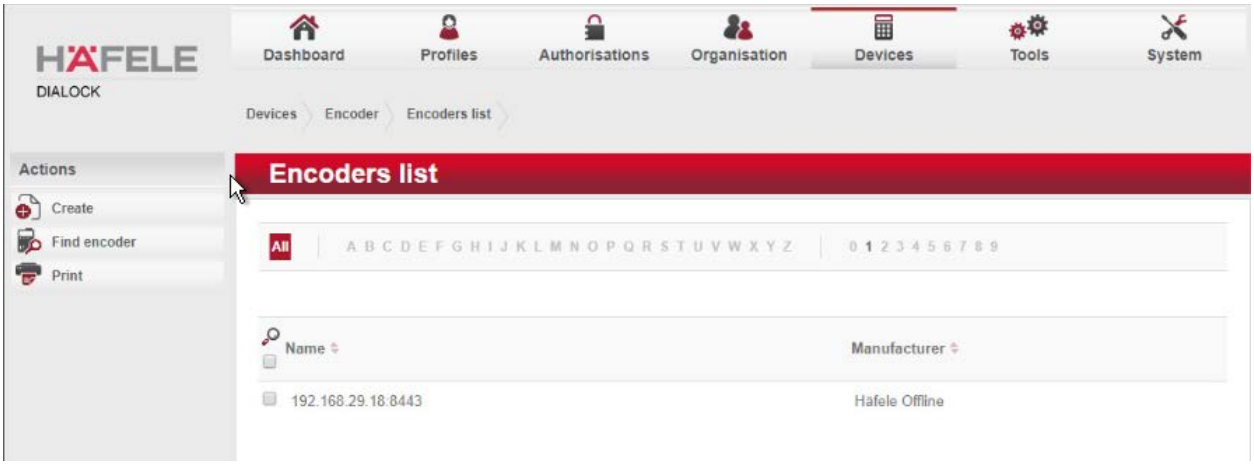
9. The new IP address should be visible on the encoding station device.

2.5.6 Dialock 2.0 Web Setup

2.5.6.1 Adding the Encoder

1. First, add the encoder if it has not already been detected. To do this, navigate to **Devices** > **Coding Devices** by using the main menu.

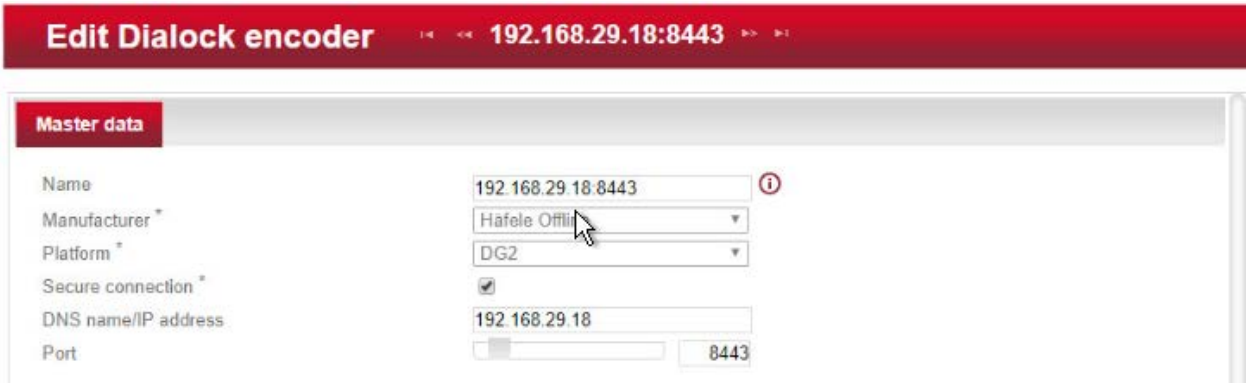
2. From there, you will see a menu titled **"Encoders list"**, If you see your networked device as shown below you can proceed to the next step. If not, continue following the instructions.



To add an encoder, proceed as follows:

1. In the left-hand menu field, click **Create.**
2. A selection window appears. Click the **Häfele Offline** field:

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



4. Save your entries by clicking the **Save** icon in the left-hand menu.

    - Now check if the encoder has been set up successfully. Click the **Read transponder** icon in the left-hand menu.

    - The encoder emits a beep. Next, place a transponder on the encoder. If the encoder has been set up successfully, a window will open that lists the information of the transponder.

2.5.6.2 Adding the MDU

NOTE: If a Java dialogue window opens during the following process, close the window. This may happen more than once. Click **Close** or **Run** to close the Java dialogue boxes, which could take several minutes.

1. Before installing and registering a new MDU, the MDU must be connected to the computer via the Universal Serial Bus port. If an AutoPlay window opens after connecting MDU, click the **X** to close the window.

2.5.6.3 Setting Up a Guest Room

1. Navigate to **Devices > Terminal**. You should see the following window after successfully navigating to this area.

2. In this menu, select the **"create menu item"** located under Actions on the left side of the screen. In the preselection pop-up dialogue, select **Häfele Offline (DG2).**

3. The grayed-out fields contain unconfigurable preset terms.

4. Name is a required field. We recommend entering the room number as the name—for example, 102. The field for the installation location is optional.

5. The **Save** icon in the left-hand menu field will flash.

6. Save the entries:

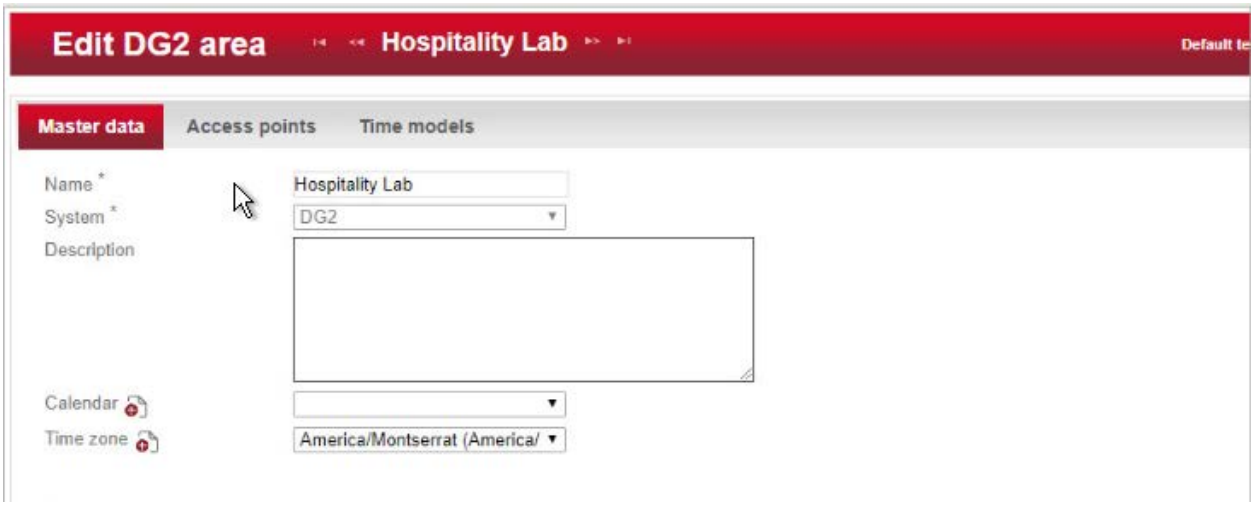
Next, assign an area to the terminal.

1. Click the **clipboard** icon to the right of the term Area to open a window in which different areas are listed. Click the desired area. In the example below, Hospitality Lab was chosen. The window closes and your selection is automatically copied to the current window. If you cannot select an area, you will need to create one.

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

2.5.6.4 Create an Area

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



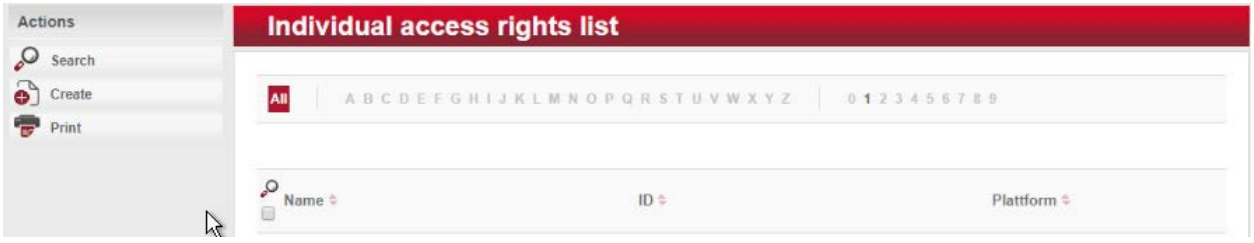
2. Be sure to save the created area. After this is complete, refer to the previous step to add the area to the terminal.

2.5.6.5 Provisioning Access

When configuring and commissioning a hotel, individual access rights must be assigned to the offline terminals. The steps below describe the assignment of individual access rights.

2.5.6.5.1 Create Authorizations

1. To begin provisioning access to a created area and terminal, navigate to **Authorizations** > **Individual Access Rights** in the top menu:



2. When the window opens, select **“create.”**

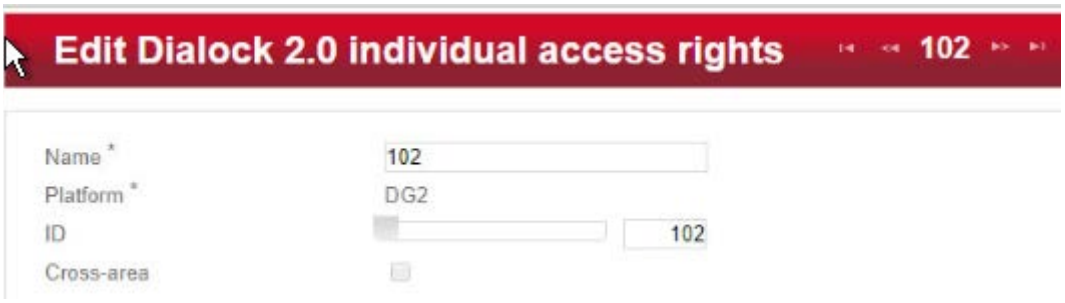
3. The window “Create Dialock 2.0 individual access rights” opens.

4. 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 already been automatically copied to the uppermost input field.

6. In the right input field for ID, enter the same room number already entered in the **Name** field. (The fields must match.)

7. Save the entries:



2.5.6.5.2 Configuring the Terminal

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

1. Navigate to **Devices** > **Terminal** in the main menu. In this menu, select the terminal that you previously created. The **Edit Offline terminal** window opens.

2. Click the “Individual access rights” tab.

3. Click the **clipboard** below the term “Access rights.”

4. This opens a dialogue box in which a selection of terminals that have already been set up are listed:

5. Click the terminal that you created previously.
6. Confirm with “Apply selection.”
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 specific access point in the building.

2.5.6.5.3 Configuring the MDU

1. 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.
2. Select **Register MDU** on the left side of the screen. After accepting the Java applets run warnings, wait for the MDU to be discovered.
3. If the MDU is plugged into the current host machine and you can view it in a file browser, you will see a window showing the discovered MDU. Close the window.
4. Your MDU is now listed in the **DG2-MDUliste** menu:

2.5.6.5.4 Programming a Physical Terminal by Using the MDU

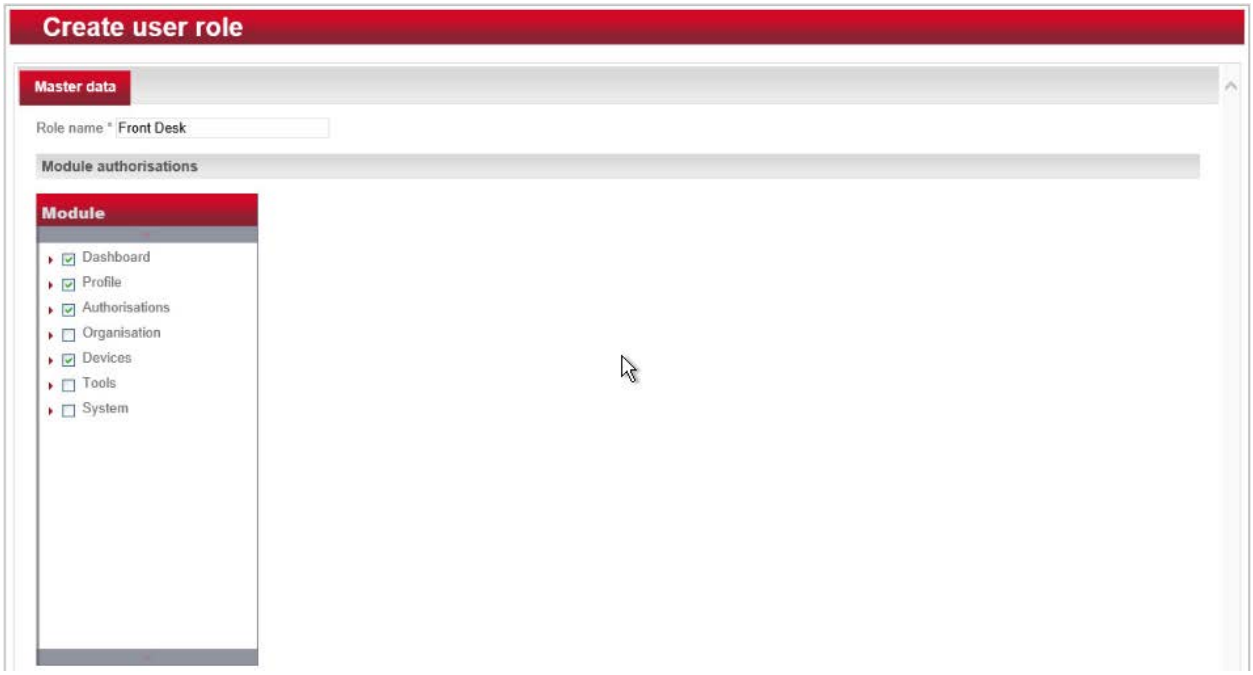
1. To program the physical terminal, navigate to **Organizations > Area**.
2. Select the area that was created in the step Create an Area.
3. Select **Parameterize MDU** from the left-hand menu.
4. Ensure that your MDU is still plugged into your workstation. In the pop-up menu, select the rooms that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

2.5.6.6 Group and Role Creation

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

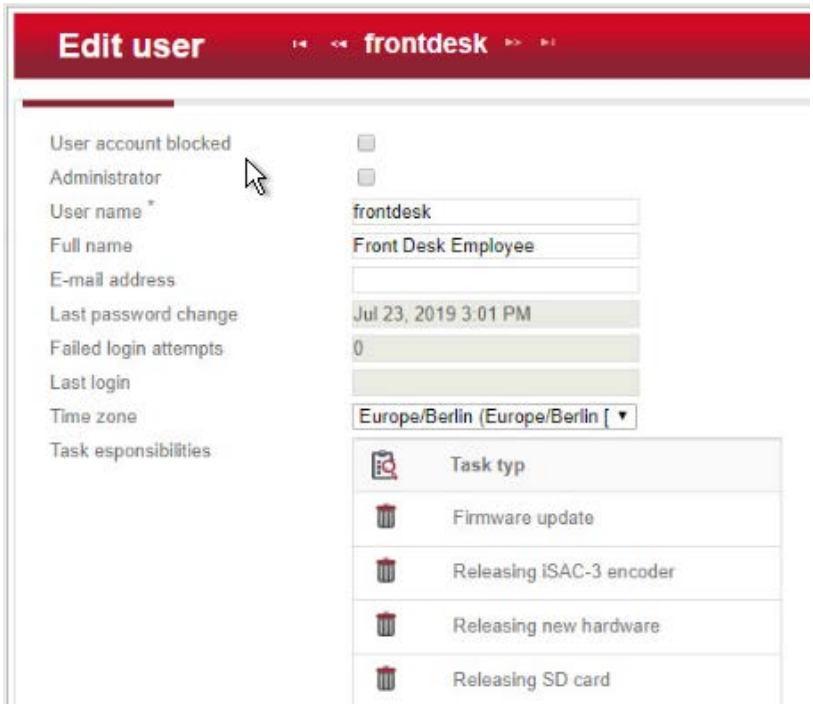
2.5.6.6.1 Creating a Role

1. Navigate to **System > Users** roles in the main menu. This opens the "User roles list" window.
2. Select **Create** in the left-hand menu. The **Create user role** window opens.
3. 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:



2.5.6.6.2 Creating a User

1. Navigate to **System** > **Users** in the main menu.
2. The "Users list" window opens. In the left-hand menu field, select **Create.**
3. The "Create user" window opens. If a user will have full unrestricted access to the software, select **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 software.
4. Click **Save**:

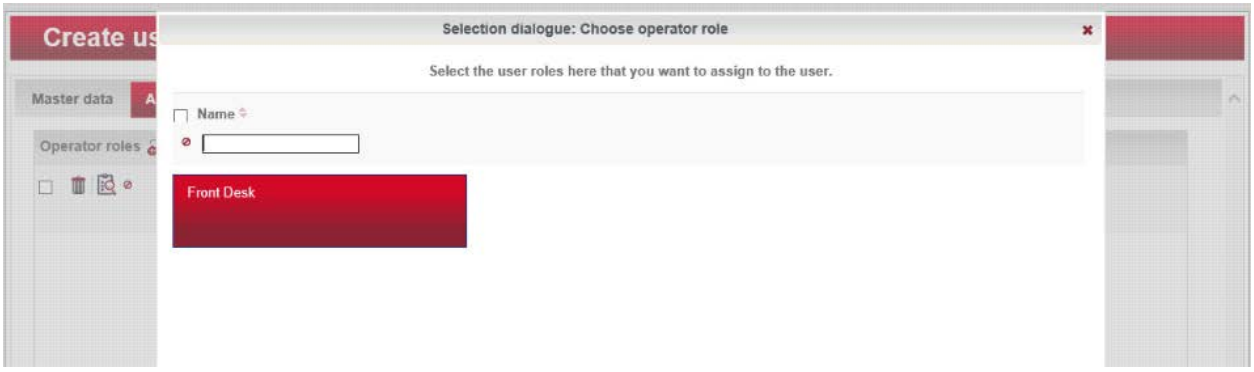


5. Click the **Authorizations** tab at the top. From the existing users' roles, select the role that you wish to assign the user.

2.6 Privileged Access Management System—Remediant SecureONE

This section of the guide supplies installation and configuration guidance for the privileged access management solution, which provides security for administrator-level actions within the enterprise.

Remediant SecureONE is the privileged access management solution within the reference architecture.



2.6.1 Privileged Access Management System–Remediant SecureONE–Overview

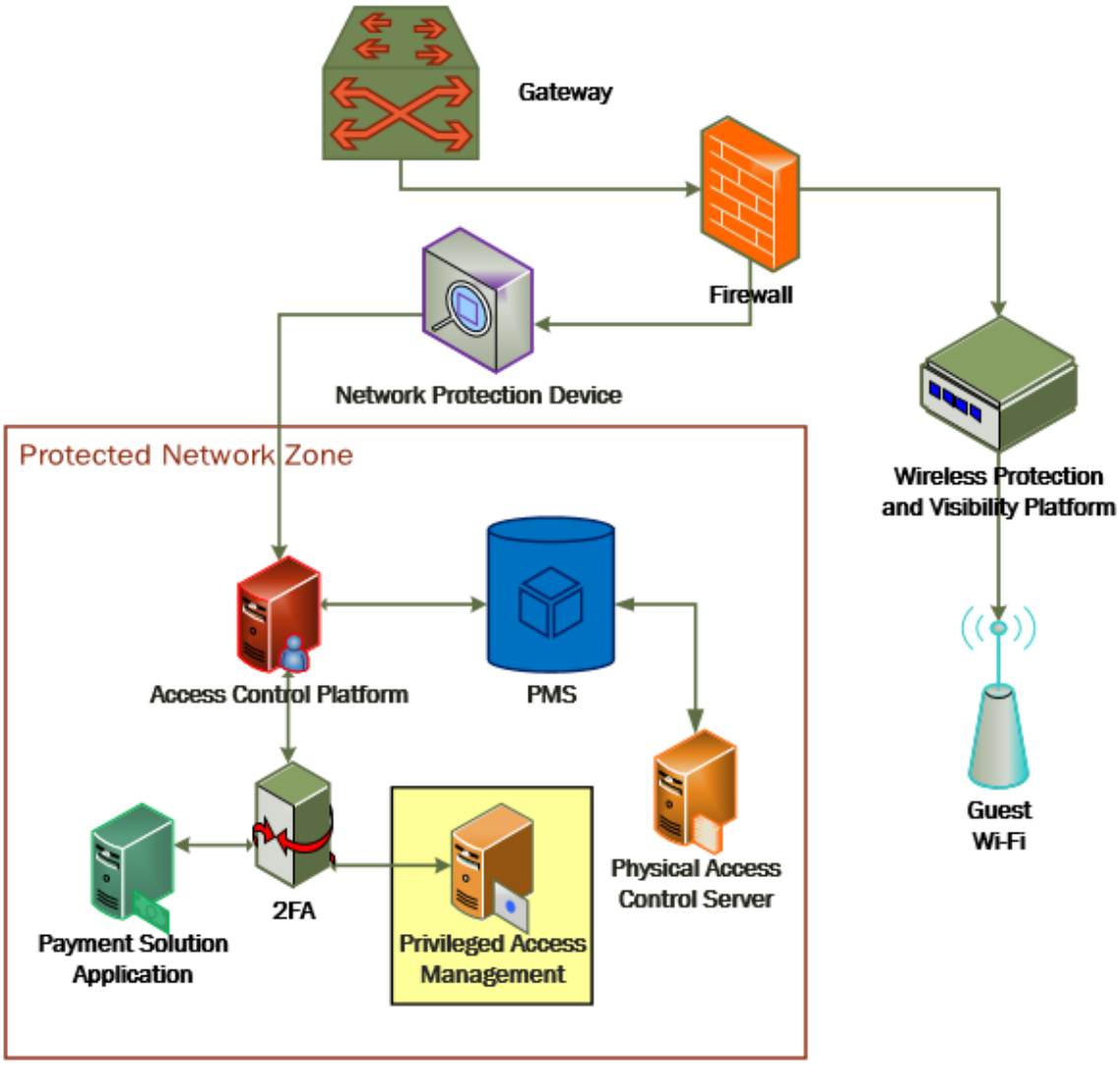
Remediant SecureONE provides detection and response capabilities for violations of privileged access within the enterprise.

In the PMS ecosystem, SecureONE was deployed as a prebuilt VM appliance from the vendor. We configured the appliance with parameters necessary for our environment.

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 prevent abuse of this trust.

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
1238 system Remediant SecureONE. Both the hardware and software requirements were included in the
1239 managed deployment provided by Remediant.

2.6.2.1 Hardware Requirements for the Privileged Access Management System

This installation occurred on a machine with 4 CPUs, 8 Gigabytes (GB) of memory, and 100 GB of storage.

2.6.2.2 Software Requirements for the Privileged Access Management System

This build utilized an Ubuntu 14.04 OS for the SecureONE server.

2.6.2.3 Network Requirements for the Privileged Access Management System

Network connectivity must be available to the web server hosted on the Remediant SecureONE device.

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 Remediant SecureONE before applying the associated rules on the CryptoniteNXT device, as seen in Section 2.1.8.

2.6.3 Privileged Access Management System–Remediant SecureONE—Installation

The installation procedure consists of the following steps:

1. Connect SecureONE to the domain.
2. Synchronize SecureONE to the domain.
3. Verify that all managed machines are present in the SecureONE appliance.

In the example implementation, SecureONE was deployed as a prebuilt VM from the vendor. The instructions below assume that the VM is already deployed and is accessible from the network.

For a more in-depth discussion of implementation of a PAM solution, particularly as it relates to an installed access control platform, please see NIST Special Publication 1800-18, *Privileged Account Management for the Financial Services Sector* Practice Guide.

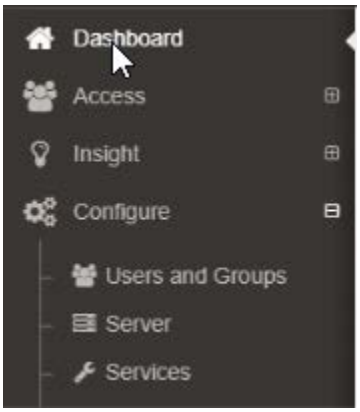
2.6.4 Initial Configuration

SecureONE needs to be configured to connect to a domain server, which should be installed within your environment. To have a successfully working SecureONE instance, take these steps:

1. Create a service account within your Active Directory server. The service account can be named secureone or anything that you choose. The SecureONE appliance will use this account. https://blogs.technet.microsoft.com/askpfeplat/2012/12/16/windows-server-2012-group-managed-service-accounts/

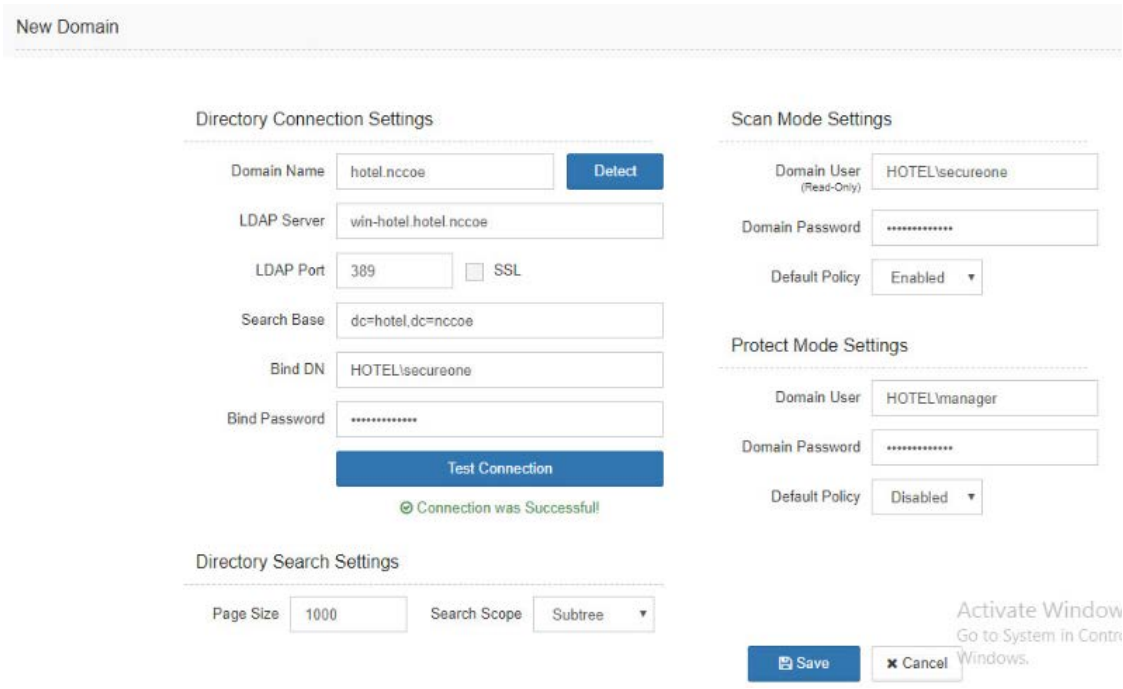
2. To log in to the SecureONE appliance, navigate in a web browser to the IP of the machine, and use the provided credentials to sign in.

3. On the side panel, select **Configure > Services:**

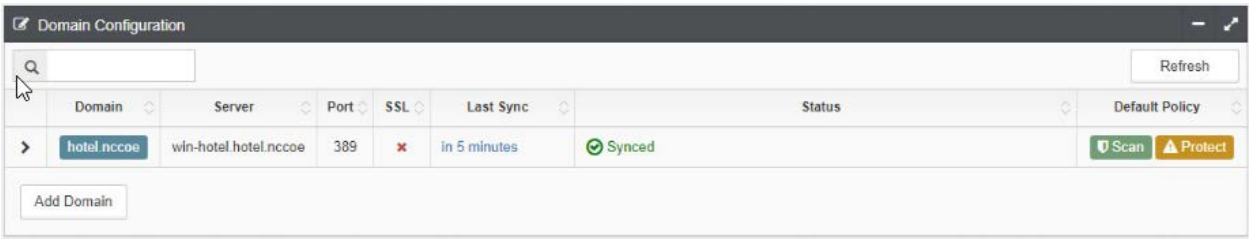


4. Select **Add Domain** in the Domain Configuration window.

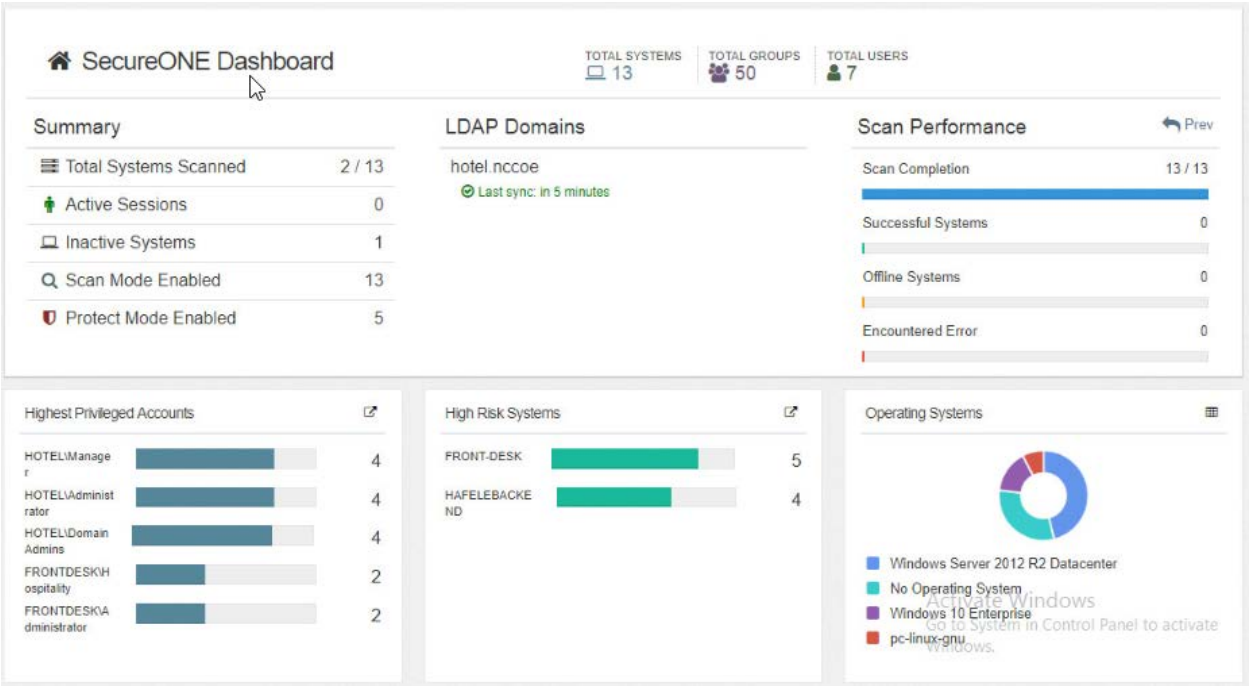
5. Enter your relevant domain information. We have included ours below for reference:



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



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



2.7 Wireless Network Management—Forescout CounterACT

This section of the guide supplies installation and configuration guidance for the wireless network management solution, which provides access control for connections across the wireless network. It differentiates among verified guests, employees, and system administrators to provide the appropriate level of access through the wireless network.

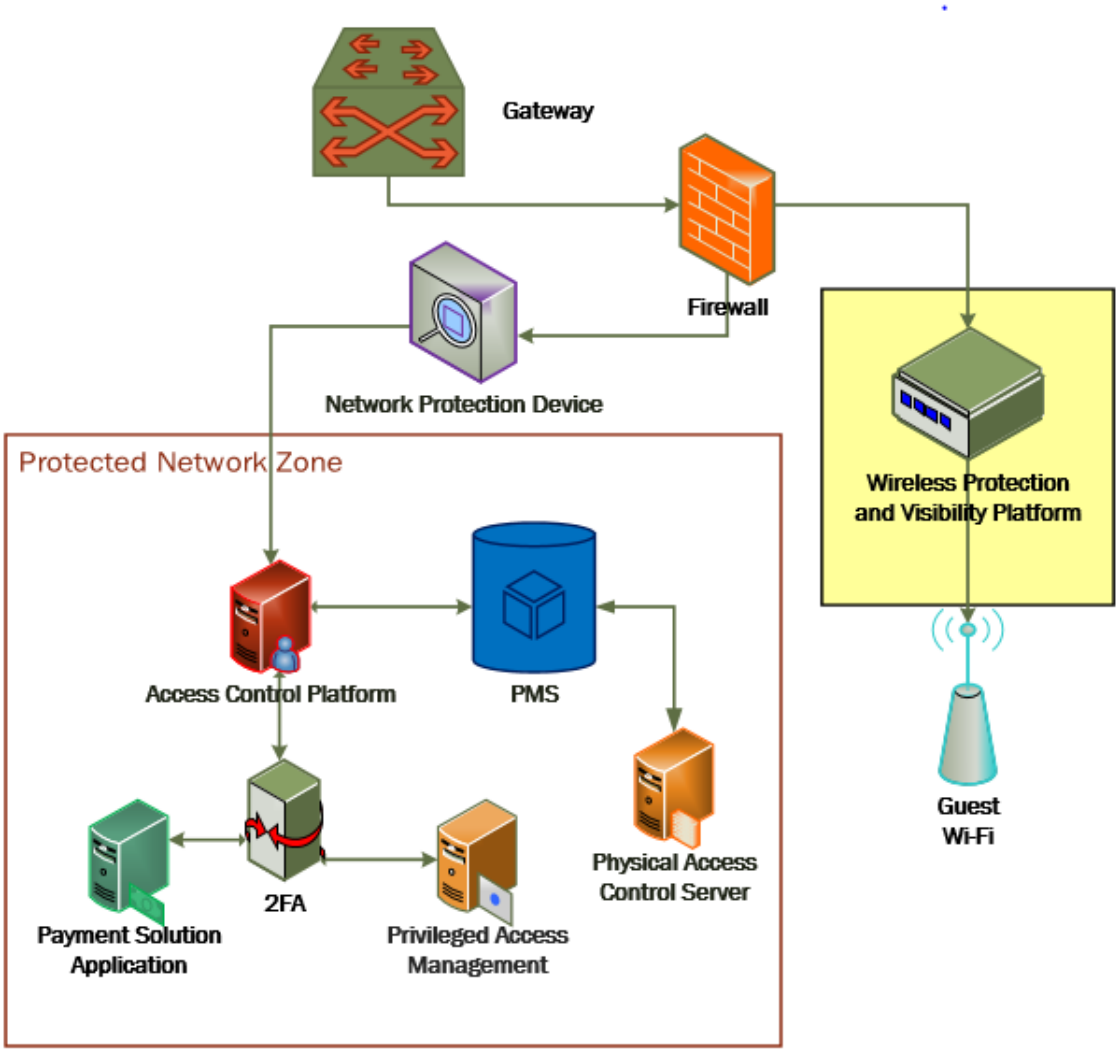
Forescout CounterACT is the wireless network management solution used in the example implementation.

2.7.1 Wireless Network Management–Forescout CounterACT–Overview

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

Forescout CounterACT authenticates users to the wireless network via a captive portal. It blocks unauthenticated or unauthorized connections. Guests get access to the internet but not to internal enterprise systems. Authenticated employees get access to the PMS so they can manage reservations and perform other enterprise functions. The location of the wireless network management solution in 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.

2.7.2.2 Software Requirements for Wireless Network Management

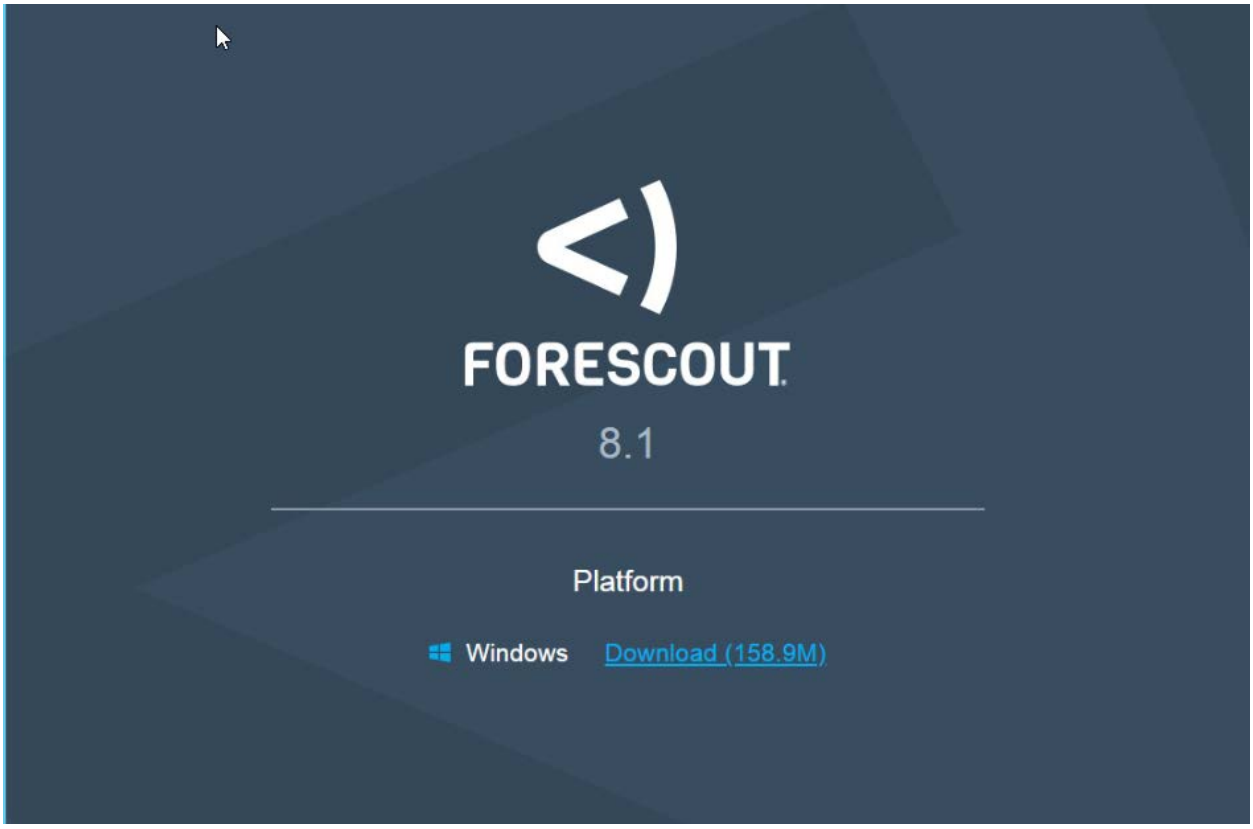
This installation occurred on a deployed CentOS 7 VM that the vendor provided.

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.

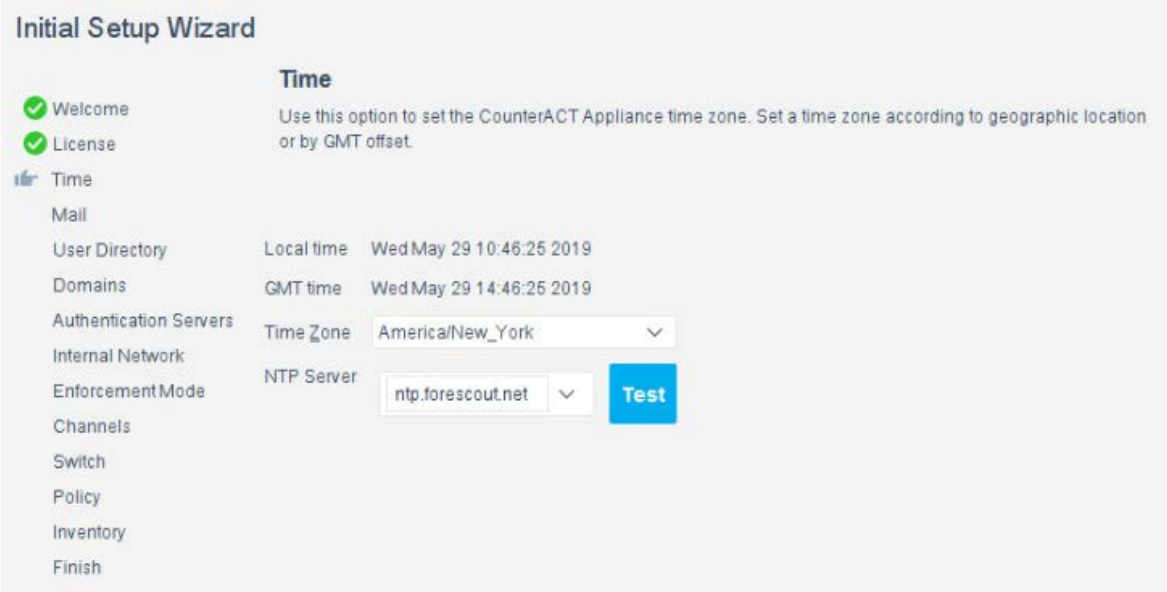
2.7.3 Wireless Network Management–Forescout CounterACT—Installation

1. To install the CounterACT console for management, navigate to [FORESCOUT IP]/install. This leads you to the page where you need to download the management console.



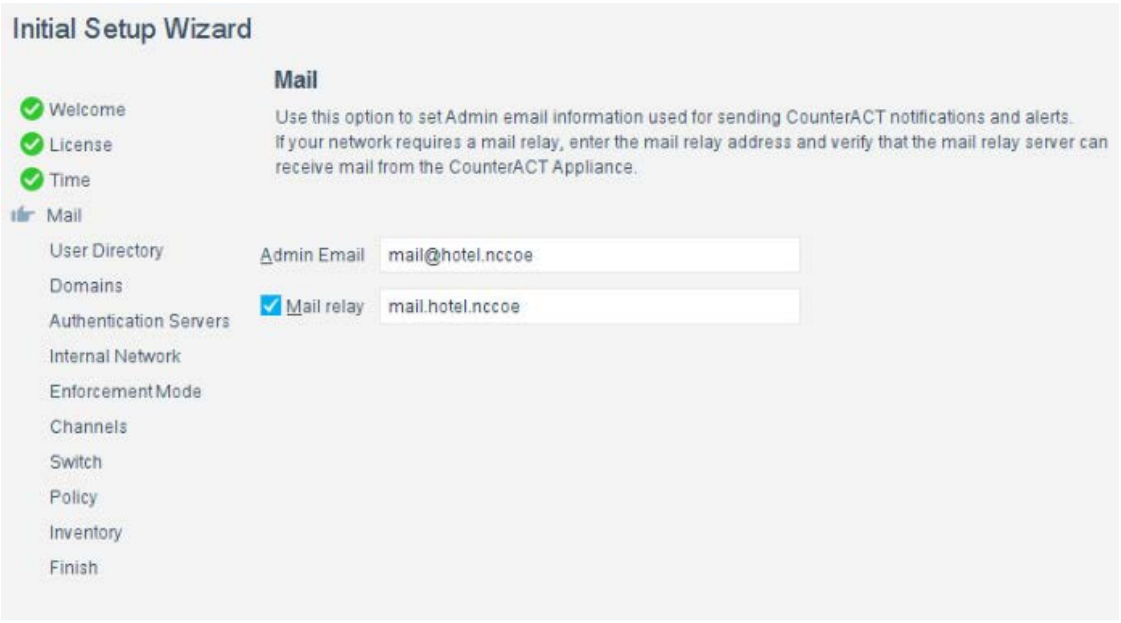
2. After installing the console, you can then log in to the management interface to begin configuring your Forescout CounterACT appliance.

3. Navigate through the Initial Setup Wizard when the console launches. Verify that the time and NTP server are configured as desired.



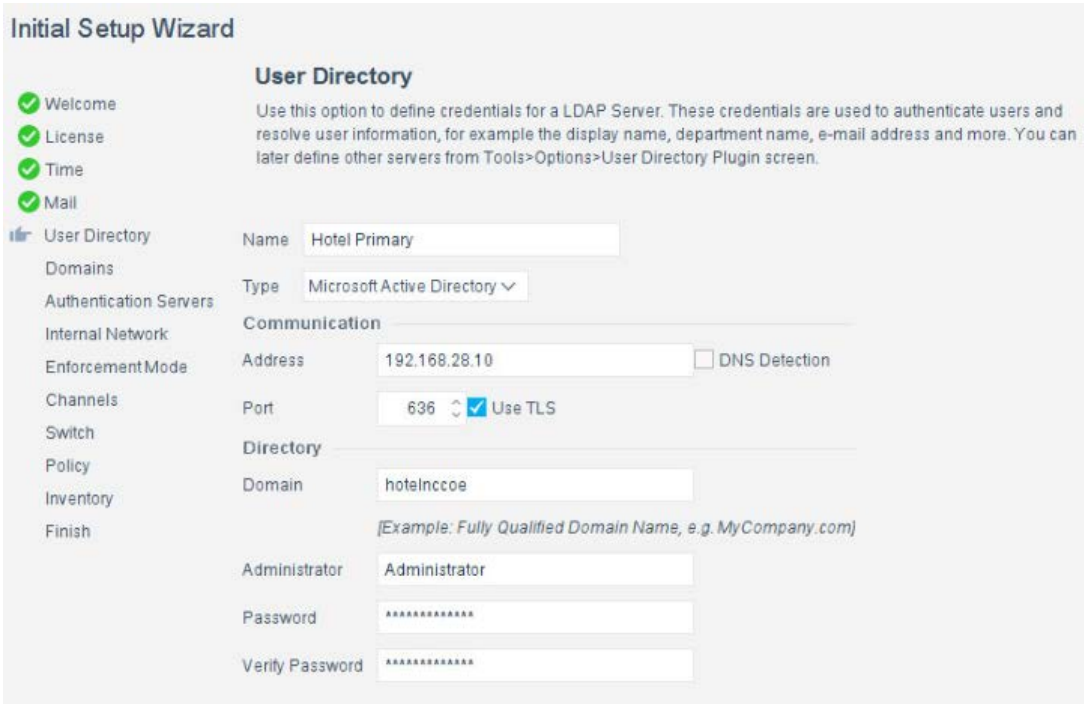
1318

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



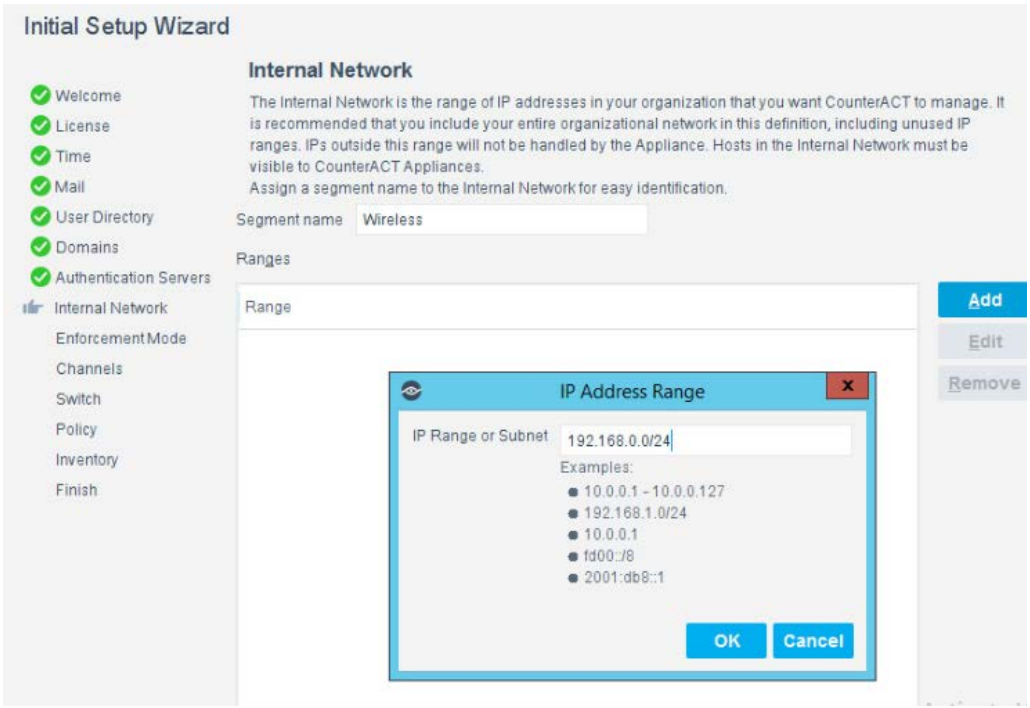
1320

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

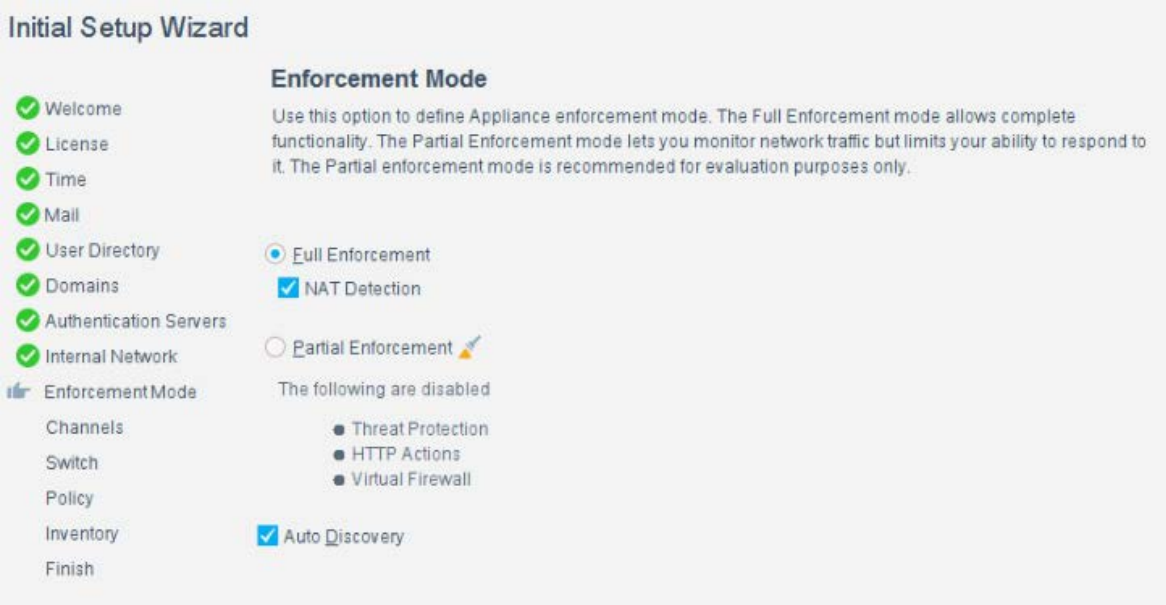


1322

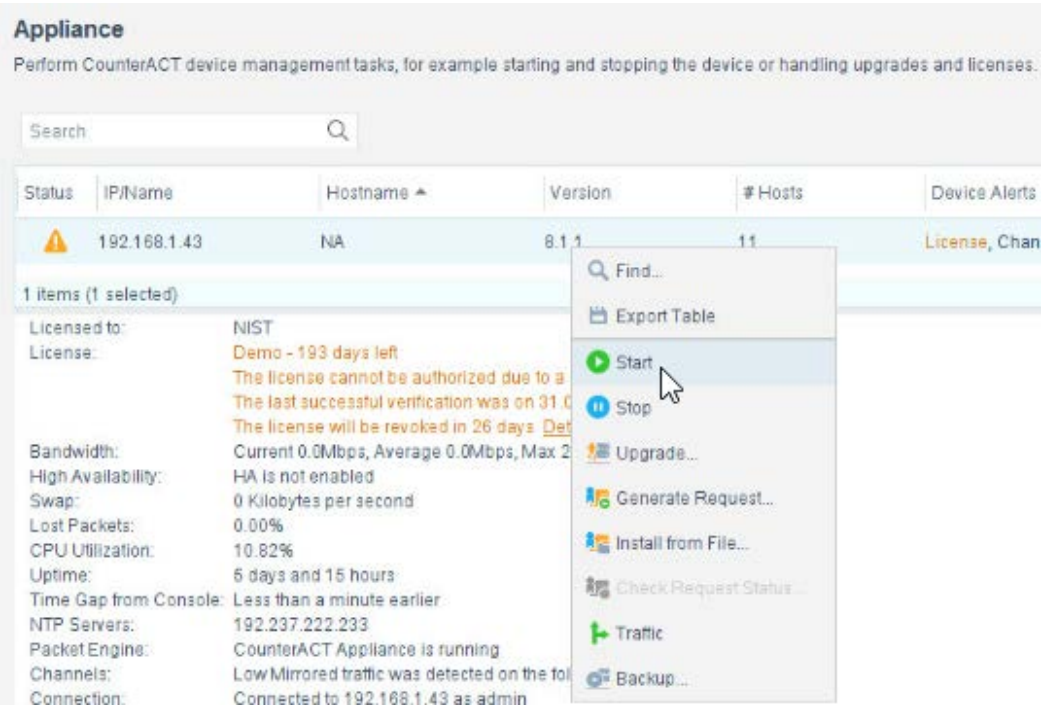
1323 6. Input the IP Address range to be provisioned to the wireless network.



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



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



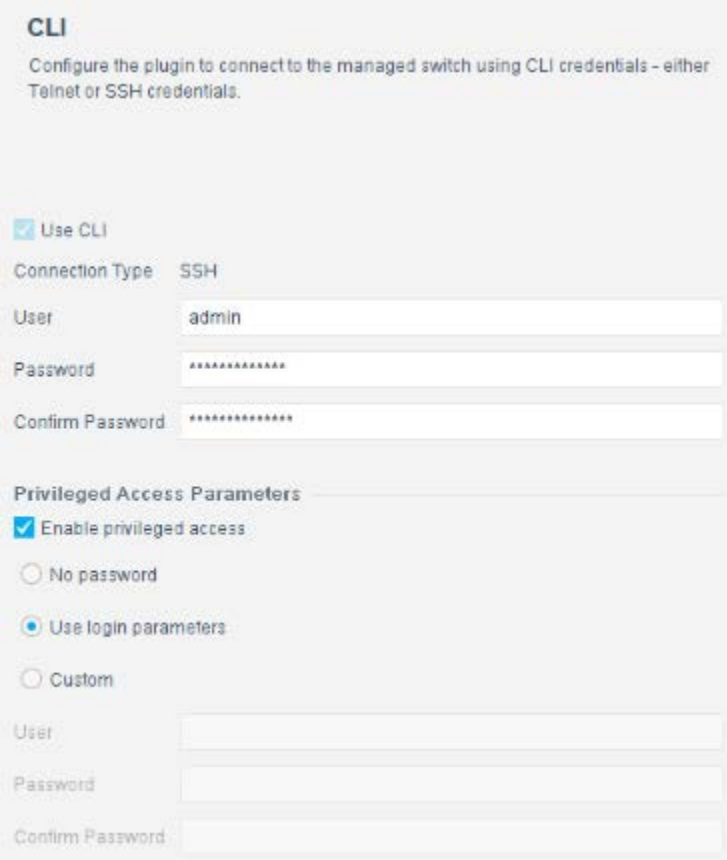
2.7.4 DNS Enforcement

1. 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.

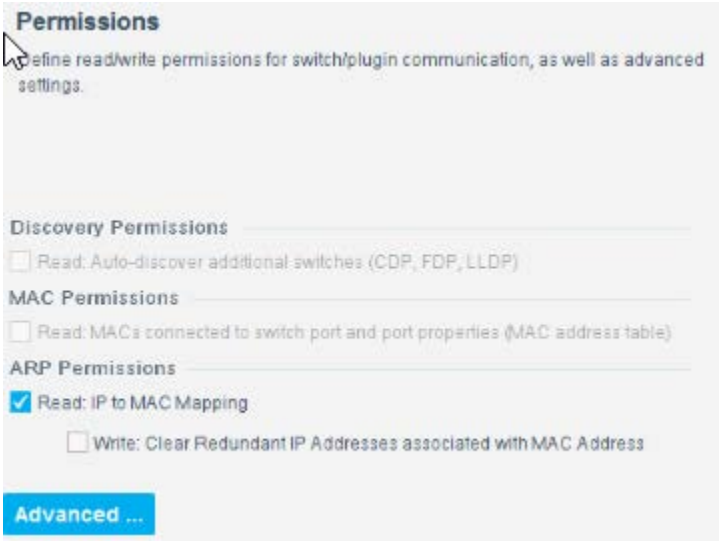
2.7.5 Switch Plug-in

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

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



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

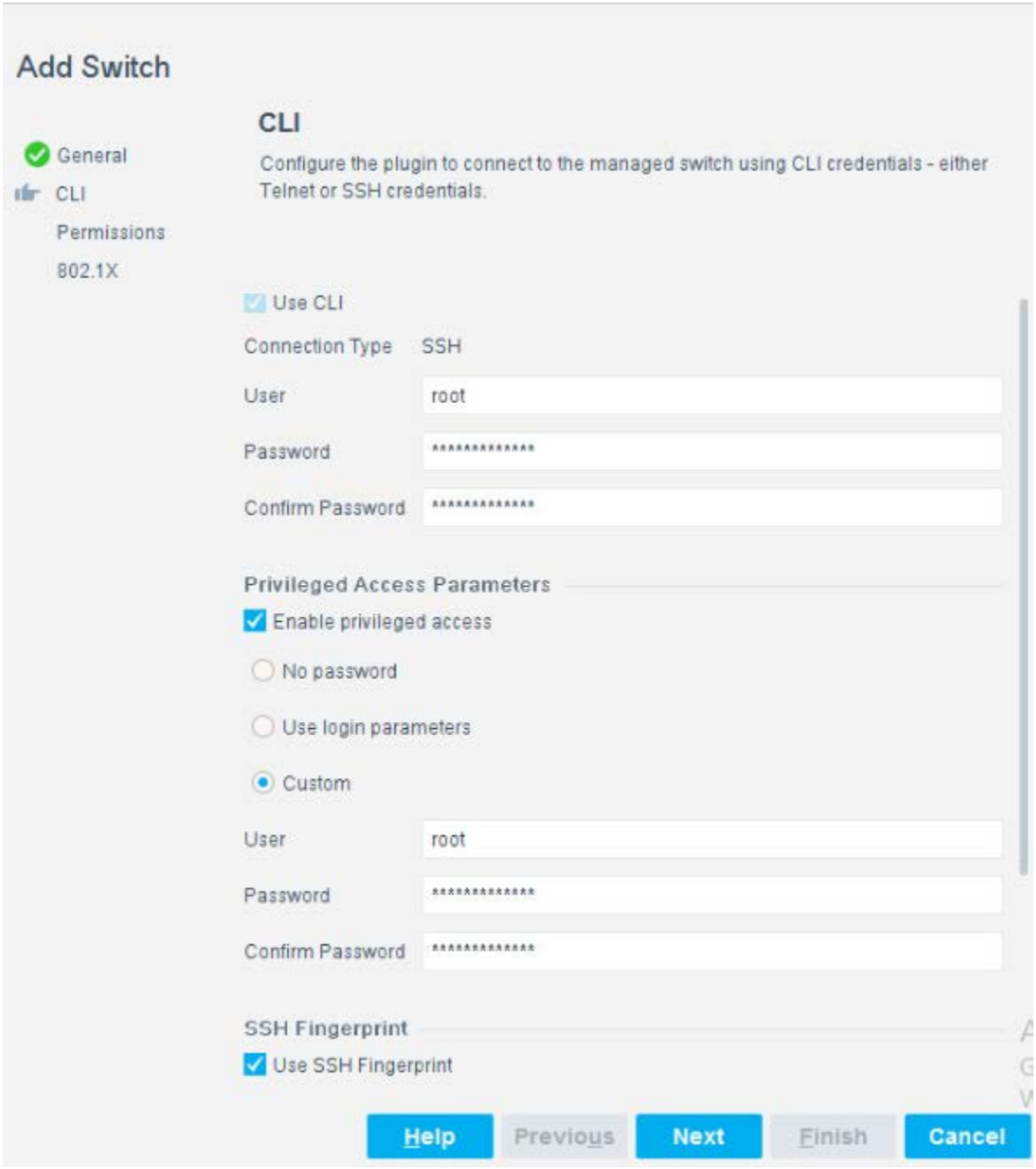


1343

1344 4. Configure 802.1X per organizational specification.

1345

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



1347

1348 2.7.6 Guest Policy

1349 The guest policy is defined to control access of a hotel guest when that person is using Guest WiFi
1350 according to the authentication results of the hotel guest device. The authentication process determines
1351 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 process is 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.

- Guest Hosts
    - end-point client devices that are not authenticated
    - No traffic is allowed from these devices within the Wi-Fi VLAN.
    - In the Forescout console, this type of device is shown in the Policy Guest WiFi column as Guest Hosts. This device is identified by the IP address 192.168.0.129.
- Signed-in Guest Hosts
    - end-point client devices that are authenticated as hotel guests with approved access to the internet
    - Allow traffic on ports 80 and 443 to addresses outside the hotel on the internet (non-RFC1918 addresses).
    - Prevent access to any addresses inside the hotel infrastructure (RFC1918 addresses).
    - In the Forescout Console, this type of device is shown in the Policy Guest WiFi column as Signed-in Guests. This device is identified by the IP address 192.168.0.119.
- Corporate Hosts
    - end-point client devices that are authenticated with hotel domain credentials
    - Allow full access to both the internet (non-RFC1918 addresses) and addresses inside the hotel infrastructure (RFC1918 addresses).
    - In the Forescout Console, this type of device is shown in the Policy Guest WiFi column as Corporate Hosts. This device is identified by the IP address 192.168.0.133.

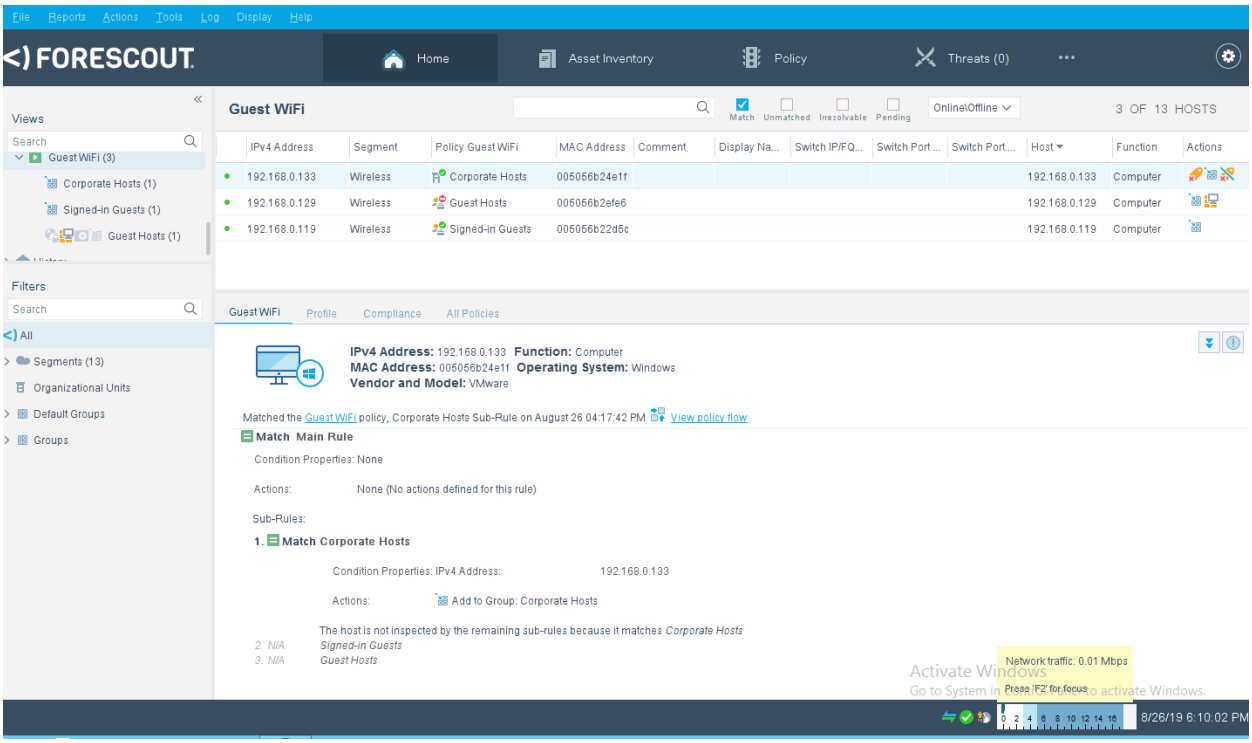
This Forescout policy is designed to detect a device when it joins the Guest WiFi, query that device for the result of its authentication process and assign settings to the Forescout virtual firewall that provide the appropriate network access to that device. Due to lab limitations, the query process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

The Forescout policy is defined by these parameters:

- Name: Guest WiFi

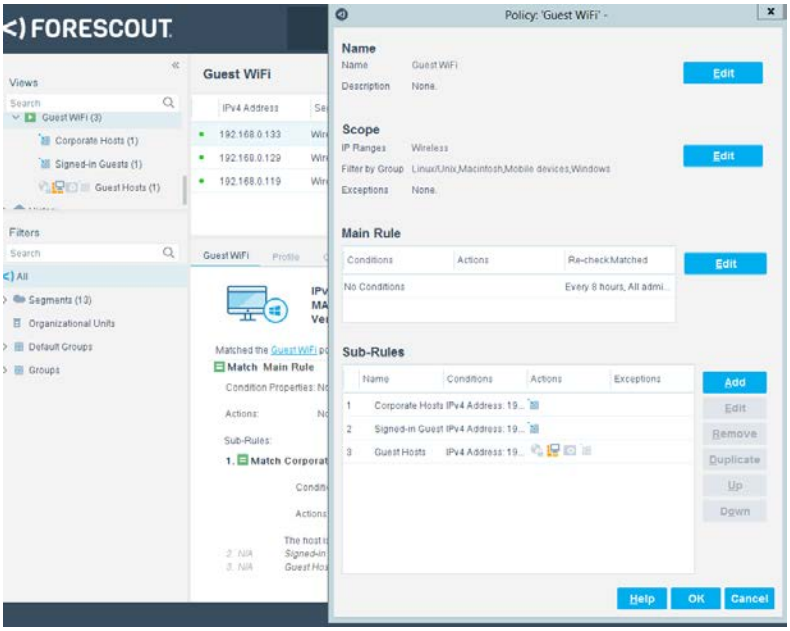
- Scope: wireless network segment in the lab and any computer or mobile device
- Main Rule: This is not used for this lab.
- Sub-Rules: Three subrules identify and control the three types of hotel guest devices instead of the Main Rule.
  - Name:
    - Corporate Hosts
    - Signed-in Guests
    - Guest Hosts
  - Condition:
    - Match a single criterion.
      - IPv4 address
        - 192.168.0.133
        - 192.168.0.129
        - 192.168.0.119
  - Action:
    - Add to Group.
      - Designate Corporate Hosts.
      - Designate Signed-in Guests.
      - Designate Guest Hosts.
    - Virtual Firewall
      - blocking rules for Corporate Hosts
      - blocking rules for Signed-in Guests
      - blocking rules for Guest Hosts

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

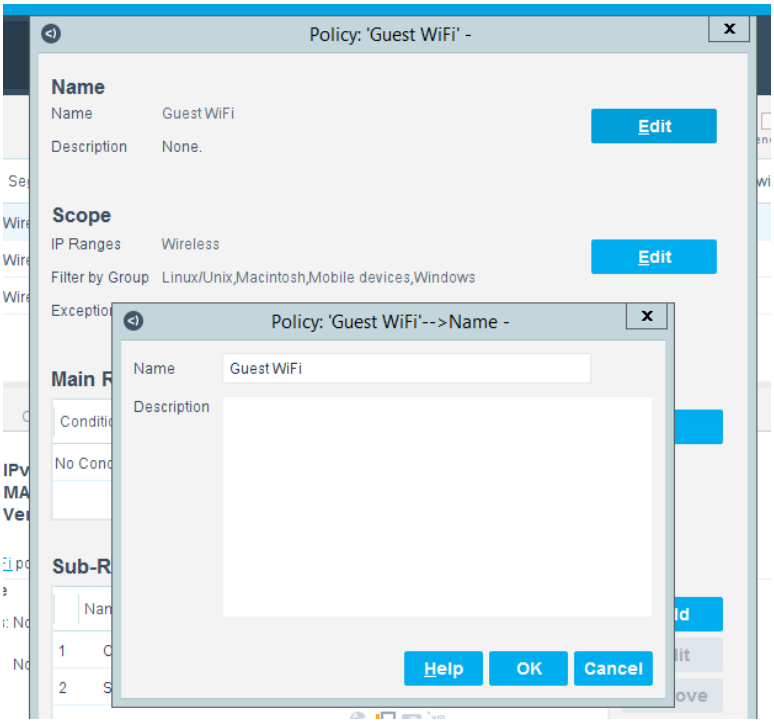


1406

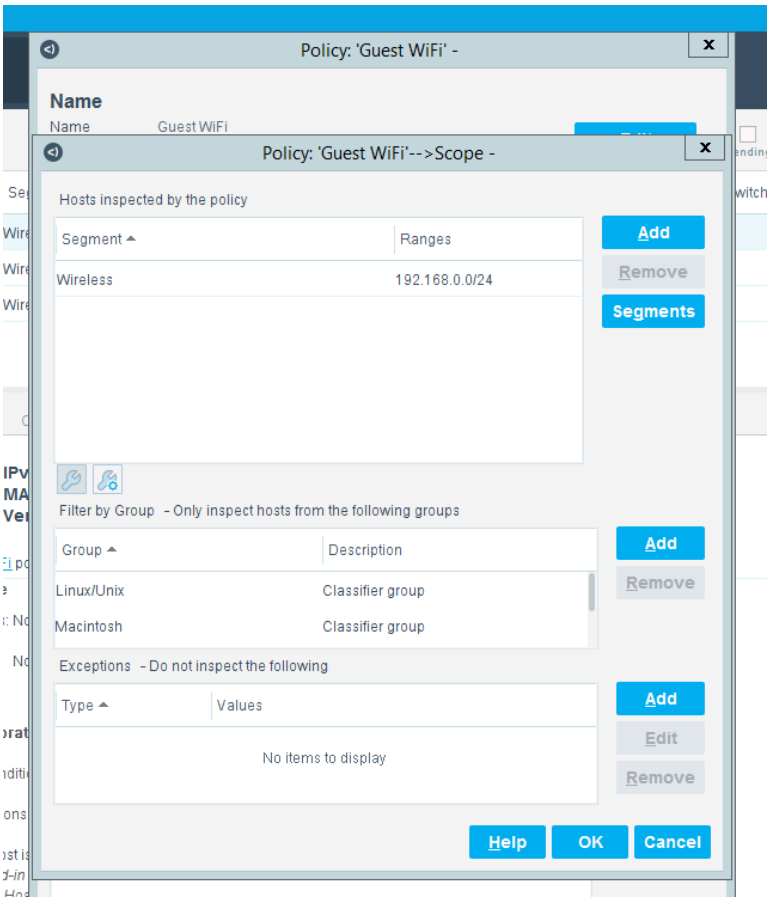
1407 1. Right-click the **Guest WiFi** policy in the Views section of the Console and click **Edit** to open the
1408 policy editor and configure Forescout for controlling the Guest WiFi.



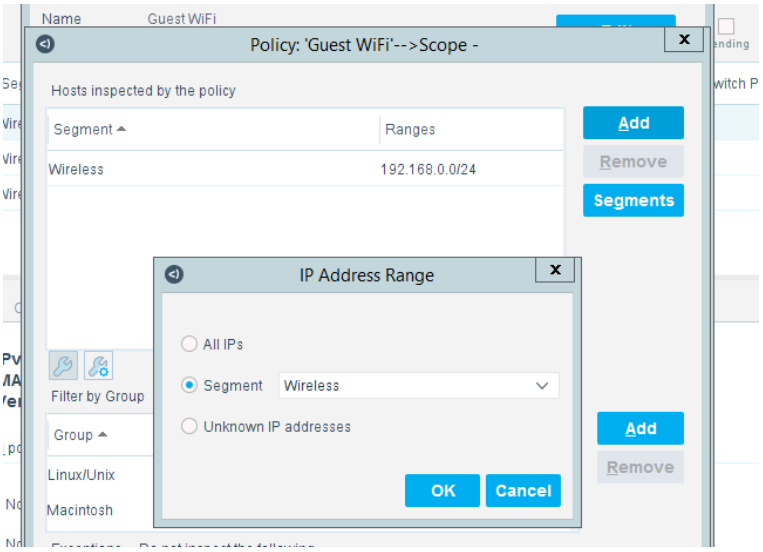
2. Start the configuration process by clicking **Edit** in the Name section and entering the name of the policy.



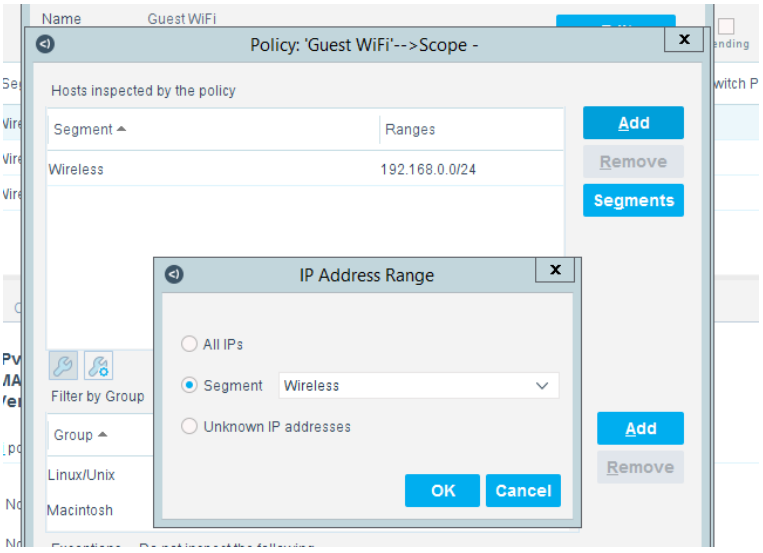
3. Click **Edit** in the Scope section to open the scope editor.

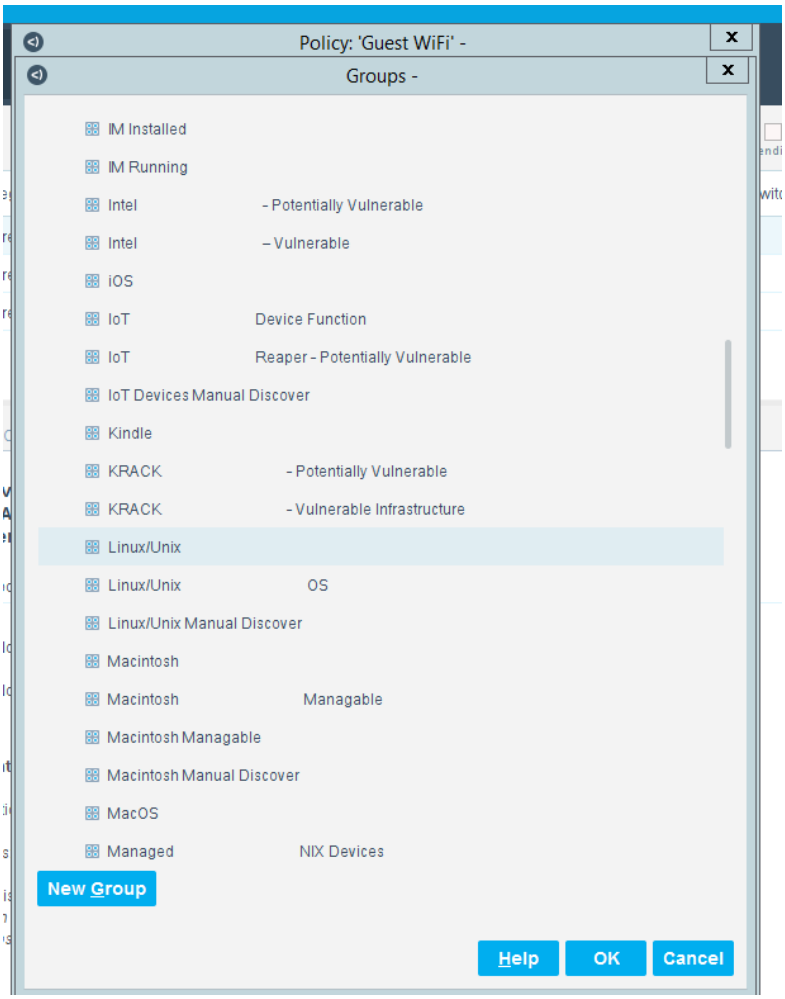

Policy: 'Guest WiFi' -
Name
Name
Guest WiFi
Policy: 'Guest WiFi'-->Scope -
Hosts inspected by the policy
Segment
Ranges
Wireless
192.168.0.0/24
Add
Remove
Segments
Filter by Group - Only inspect hosts from the following groups
Group
Description
Linux/Unix
Classifier group
Macintosh
Classifier group
Add
Remove
Exceptions - Do not inspect the following
Type
Values
No items to display
Add
Edit
Remove
Help
OK
Cancel

4. Cick **Add** in the “Hosts Inspected by the policy” section to open the IP Address Range window and select the network segment to be monitored.



5. Click **Add** in the “Filter by group” section to open the Groups window and select the types of devices to be monitored.

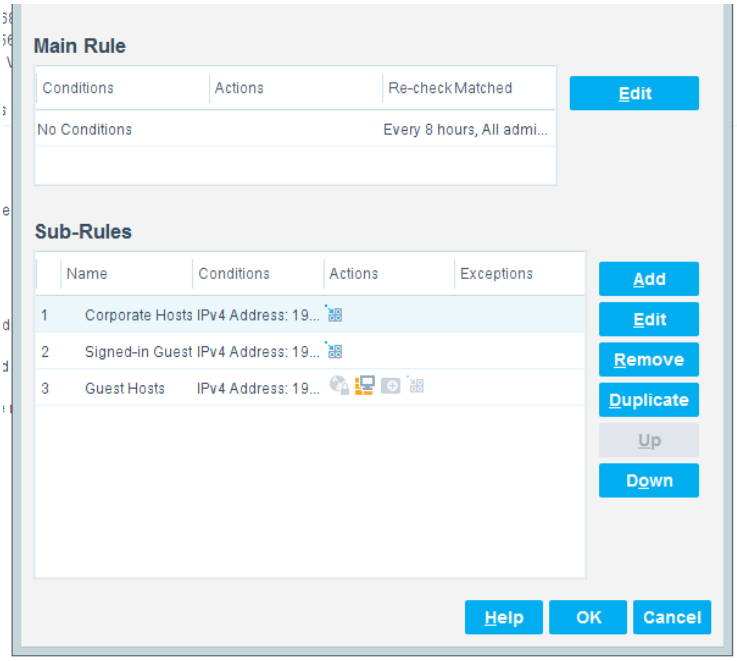




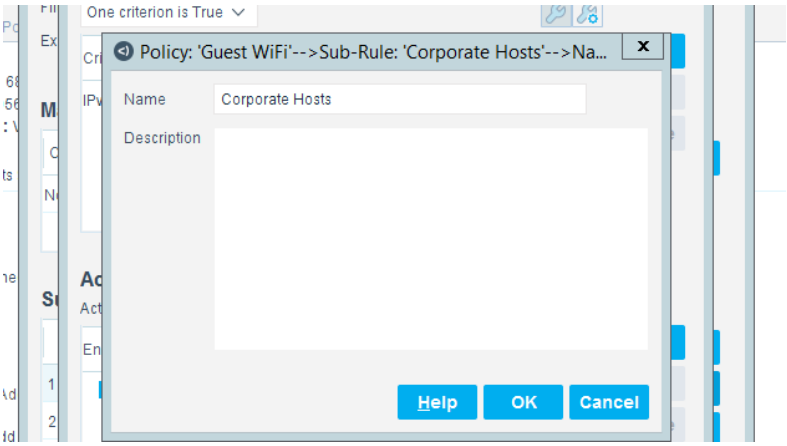
1418

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.



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

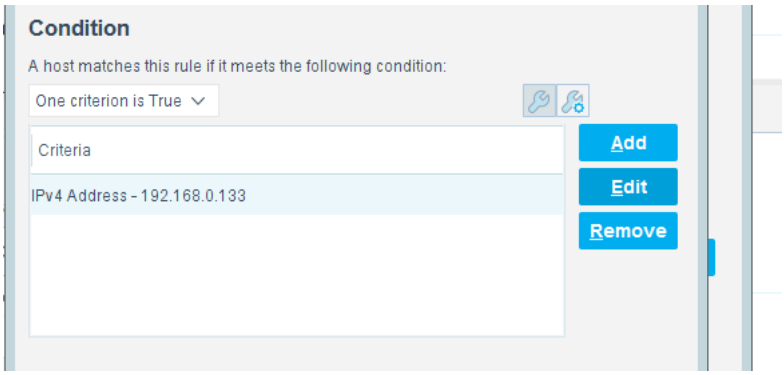


1423

1424 3. In the Condition Section of the Sub-Rule edit window, click the drop-down arrow, and select the
1425 **condition type.**

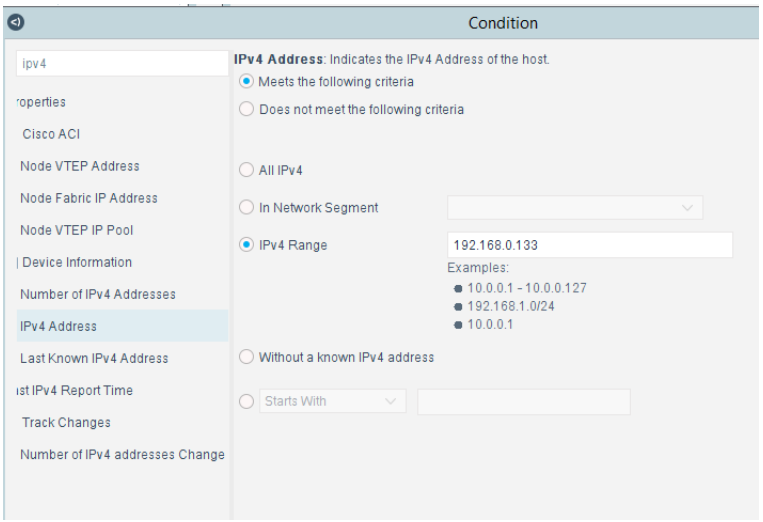
1426 4. Then highlight the Criteria and click **Edit** to open the Condition Edit window:

1427

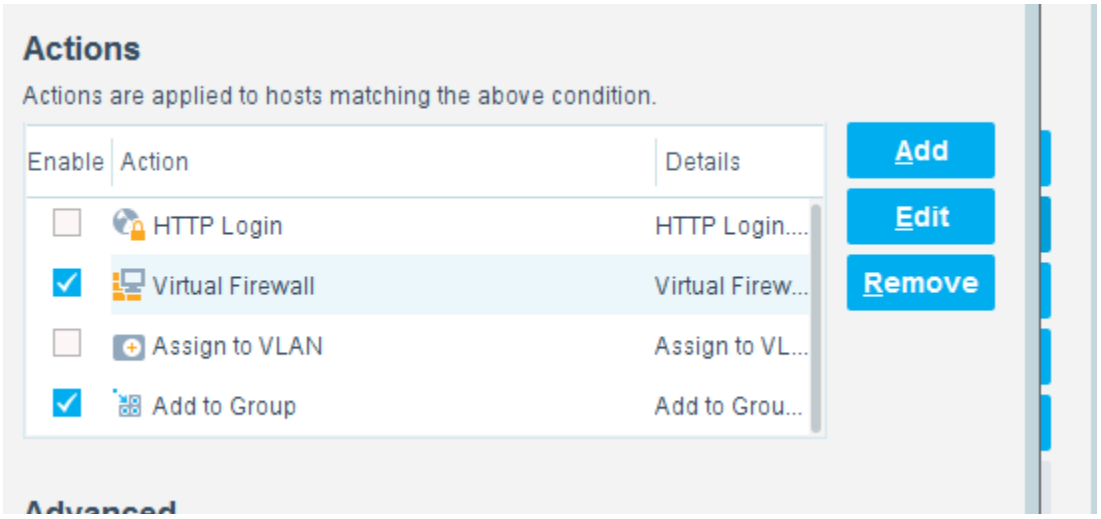


5. The left frame of the Condition Edit window lists the conditions that Forescout may use. Scroll through the list and select the appropriate Condition. This lab used the IPv4 Address Condition to identify the device used for each of the three types of hotel guest devices.

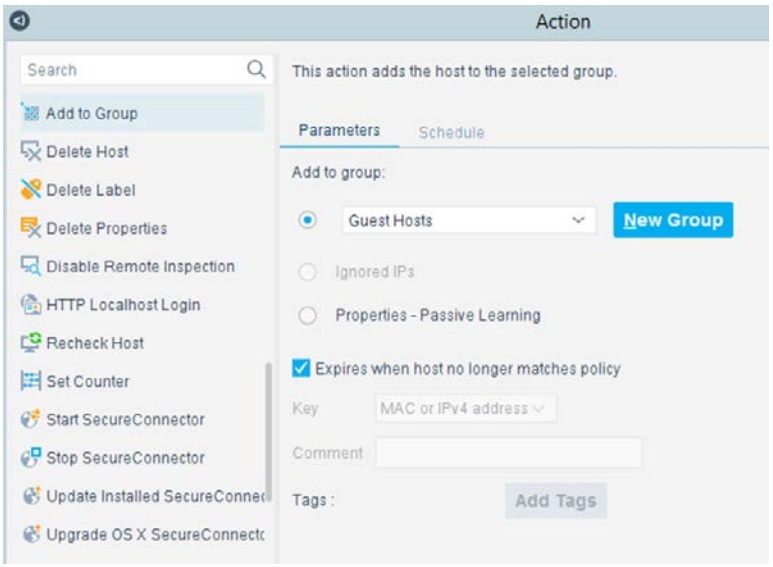
   We needed a work-around to address limitations in the lab. In a real-world situation, dynamic criteria tailored to meet the strategy of a specific hotel, such as the Authentication Login Condition, may be appropriate:



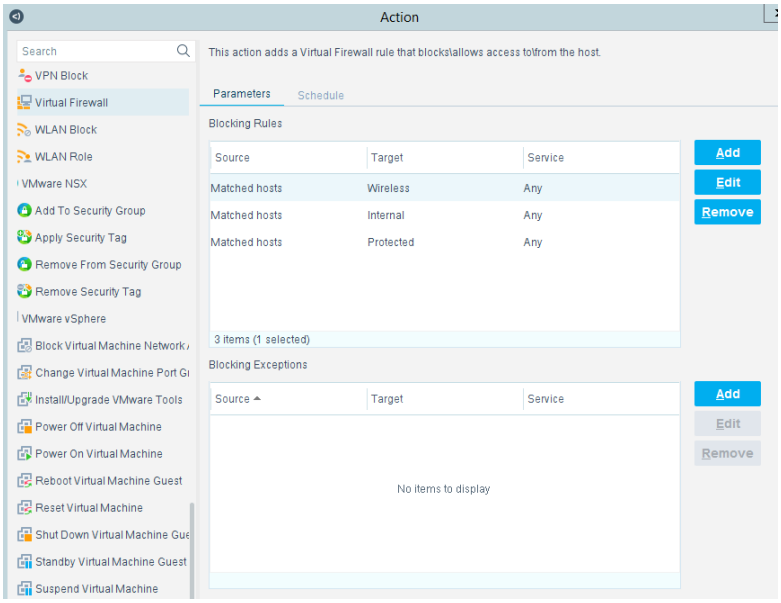
6. In the Actions Section of the Sub-Rule edit window, highlight the Action in the box, and click **Edit** to open the Action Edit window:



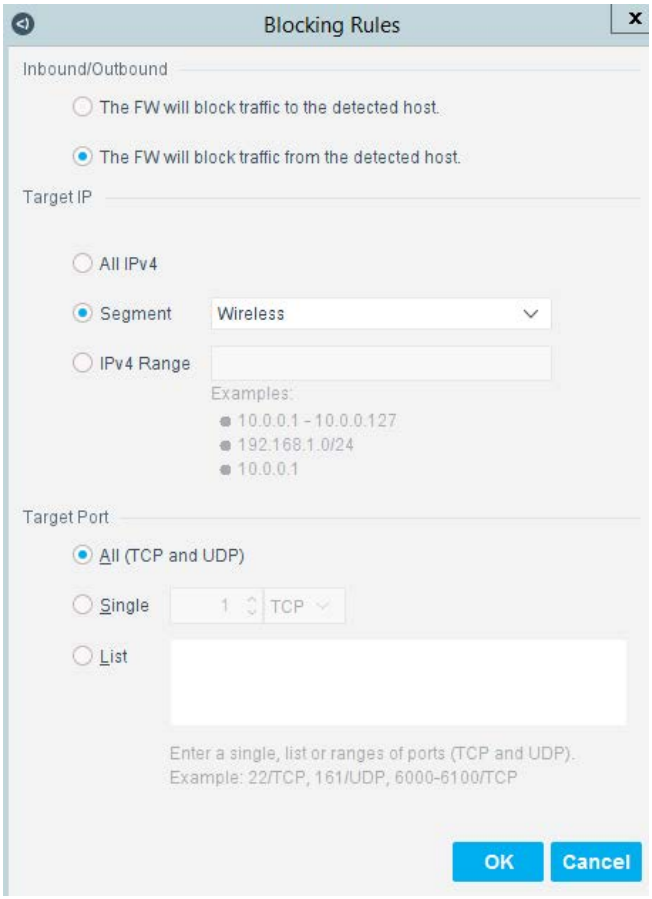
7. The left frame of the Action Edit window lists the actions that Forescout may use. Scroll through the list and select the appropriate action. This lab used the Add to Group action to designate the device identified by the condition as one of the three types of hotel guest devices:



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



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



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.

To begin configuring the switch, we used the following commands. VyOS has good documentation, and we recommend that you reference the documentation if you would like to extend the capabilities of the machine.

```
$ configure
set interfaces eth2 address dhcp
set interface eth2 description 'OUTERNET'
set interface eth1 address '192.168.0.1/25'
set interface eth1 description 'WIRELESS'
```

```
set service ssh port ‘22’

set nat source rule 100 outbound-interface ‘eth1’

set nat source rule 100 source address ‘192.168.0.0/24’

set nat source rule 100 translation address masquerade

set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24 de-
fault-router ‘192.168.0.1’

set service dhcp-server shared-network-name LAN subnet dns-server [FORESCOUT
DNS-ENFORCEMENT IP]

set service dhcp-server shared-network-name LAN subnet dns-server
‘192.168.0.1’

set service dhcp-server shared-network-name LAN subnet domain-name ‘hotel-
wireless’

set service dhcp-server shared-network-name LAN subnet lease ‘86400’

set service dhcp-server shared-network-name LAN subnet range 0 start
192.168.0.10

set service dhcp-server shared-network-name LAN subnet range 0 stop
‘192.168.0.254’

set service dns forwarding cache-size ‘0‘

set service dns forwarding listen-on ‘eth1’

set service dns forwarding name-server ‘8.8.8.8’

set service dns forwarding name-server ‘1.1.1.1’

set traffic-policy shaper WAN-OUT bandwidth ‘50Mbit’

set traffic-policy shaper WAN-OUT default bandwidth ‘50%’

set traffic-policy shaper WAN-OUT default ceiling ‘100%’

set traffic-policy shaper WAN-OUT default queue-type ‘fair-queue’

set traffic-policy shaper LAN-OUT bandwidth ‘200Mbit’

set traffic-policy shaper LAN-OUT default bandwidth ‘50%’

set traffic-policy shaper LAN-OUT default ceiling ‘100%’

set traffic-policy shaper LAN-OUT default queue-type ‘fair-queue’

set interfaces ethernet eth1 traffic-policy out ‘LAN-OUT’

set interfaces ethernet eth2 traffic-policy out ‘WAN-OUT’

set service snmp community hospitality routers authorization ro

set service snmp community hospitality routers client [FORESCOUT APPLIANCE]
```

```
set service snmp trap-target [FORESCOUT APPLIANCE]
set service snmp v3 engineid '0x0aa0d6c6f450'
set service snmp v3 group defaultgroup mode 'ro'
set service snmp v3 group defaultgroup seclevel 'priv'
set service snmp v3 group defaultgroup view 'defaultview'
set service snmp v3 view defaultview oid '1'
set service snmp v3 user hotel_user auth plaintext-key [STRONG PASSWORD]
set service snmp v3 user hotel_user auth type 'md5'
set service snmp v3 user hotel_user engineid '0x0aa0d6c6f450'
set service snmp v3 user hotel_user group 'defaultgroup'
set service snmp v3 user hotel_user mode 'ro'
set service snmp v3 user hotel_user privacy type aes
set service snmp v3 user hotel_user privacy plaintext-key [STRONG PASSWORD]
$ commit
$ save
```

2.9 Integration of Security Components

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

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.

```
$sudo yum install wget
$y
$wget --no-check-certificate --post-data 'username=Administra-
tor&passcode=<TOTP Code>' https://portal.di.ipdr/login
```

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
IT	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
PHP	Hypertext Preprocessor
PMS	Property Management System
RDP	Remote Desktop Protocol
SAKA	StrongAuth KeyAppliance
SSH	Secure Shell
SSL	Secure Sockets Layer

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

1522

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