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

FINAL

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-27

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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, VA

FINAL

March 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Acting NIST Director and Acting Under Secretary 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

March 2021

FINAL

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-27

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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 system of guest services it supports. It offers how-to guidance for building a reference design using commercially available products within a zero trust architecture to mitigate cybersecurity risk that includes 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 its extended systems store, process, and transmit a variety of sensitive guest information, including payment card information and personally identifiable information. 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, which may result in 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:

- **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
- **instill consumer confidence and brand loyalty** by protecting guest privacy and payment card information
- **decrease breach potential and data exfiltration** by limiting lateral movement, thus decreasing organizational risk
- **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

SOLUTION

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

The reference design uses technologies and security capabilities (shown below) from our project collaborators. All technologies used in the solution support security standards and guidelines of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Hospitality Technology Next Generation, and the Payment Card Industry (PCI) Security Standards Council, among others. The reference design aligns with the privacy protection activities and desired outcomes of the *NIST Privacy Framework*.

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 system, 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. 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.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

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

March 2021

FINAL

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-27

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 1800-27B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-27B, 61 pages, March 2021, CODEN: NSPUE2

FEEDBACK

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables 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 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 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, which are central to hotel operations, present attractive attack surfaces. This example implementation strives to increase the cybersecurity of the property management system (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.

The NCCoE at NIST built a PMS reference design in a laboratory environment to demonstrate methods to improve the cybersecurity of a PMS. The PMS reference design 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 architecture, 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; network security; 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
John Bell	AjonTech LLC
Shane Stephens	Forescout
Oscar Castiblanco	Häfele
Ryan Douglas	Häfele
Chuck Greenspan	Häfele
Sarah Riedl	Häfele
Harald Ruprecht	Häfele
Roy Wilson	Häfele
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 [1]. 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	policy-based control enforcement for guest Wi-Fi networks and visualizations of diverse types of network-connected devices
Häfele	physical access control system, 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

List of Figures

List of Tables

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

1 Summary

Hotel operators rely on a property management system (PMS) for daily administrative tasks such as reservations, availability, pricing, occupancy management, check-in/out, guest profiles, guest preferences, report generation, planning, and record keeping, which includes financials. This PMS controls the on-site property activities for guests and colleagues 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 solutions, sales and catering applications, minibars, telephone and call centers, revenue management, on-site spas, online travel agents, guest Wi-Fi, loyalty solutions, and payment providers.

The value of the data in a PMS and the number of connections to a PMS make it a 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 reference design, 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, data tokenization, and privileged access management. Utilizing these tenets, 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 reference design enables and enforces role-based access control to define exactly who or what will be allowed to make connections within the PMS reference design. 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 reference design includes three types of authorized users: hotel guests, hotel staff, and system administrators. Each user has defined access privileges in the simulated hotel environment. 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. System administrators are granted back-end access, but only for the systems and applications they provision, maintain, and troubleshoot.

1.2.1 PMS Reference Design

Within the constructed PMS reference design in this guide, registered hotel guests can connect to the internet via the guest Wi-Fi. Registered hotel 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 could also be used to support hotel operations and guest-facing Internet of Things (IoT) devices.

The PMS reference design 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 developing the hotel PMS reference design, some of the tenets of zero trust were adopted. This 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 reference design 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 PMS reference design, we were influenced by standards and guidance from the following sources, which can also provide an organization with relevant standards and best practices:

Note: The titles of some of the documents below include the following acronyms: HTNG, which stands for Hospitality Technology Next Generation; EMV originally stood for Europay, Mastercard, and Visa, the three companies that created the standard; PCI, which stands for Payment Card Industry; and GDPR, which stands for General Data Protection Regulations

- 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 Special Publication (SP) 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations,* September 2020 [9]
- NIST SP 800-63-3, *Digital Identity Guidelines,* June 22, 2017 [10]
- NIST SP 800-181 Rev 1, *Workforce Framework for Cybersecurity (NICE Framework), November* 2020 [11]
- *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0, January 16, 2020 [12]
- NIST SP 800-207, *Zero Trust Architecture*, August 2020 [13]
- Trustwave Holdings: *2019 Trustwave Global Security Report* [14]

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 hotel guest information
- ensure that only hotel staff 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 sensitive consumer 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 reference design 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 reference design 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 publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

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 4-1, Architecture Description, 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`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

This practice guide highlights the approach 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 did not include these security measures in the PMS reference design.

3.1 Audience

This practice guide is intended for any hospitality stakeholder concerned about and/or responsible for securely implementing and mitigating risk in and around a PMS. This includes system owners; IT and cybersecurity engineers, specialists, and technicians; hoteliers; and cybersecurity vendors.

Cybersecurity specialists, in particular, may find this document useful for its focus on the following:

- preventing unauthorized access via role-based authentication
- protecting against unauthorized lateral movement and privilege escalation attacks
- preventing theft of credit card and transaction data via data tokenization
- allowing only identified entities access by providing access control enforcement
- increasing situational awareness by auditing, system activity logging, and reporting
- preventing unauthorized use of personal information

The technical components of this guide will appeal to those who are directly involved with or oversee the PMS and its connections.

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 [1] inviting vendors to become collaborators, the project was scoped to create a PMS reference design that offers the following:

- protection against loss of customer data
- cybersecurity situational awareness

- cybersecurity for ancillary systems such as hotel guest-facing Wi-Fi networks, hotel staff workstations, and electronic door locks

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

- use of a cloud-based PMS
- point-of-sale terminals
- validation of compliance with the PCI Data Security Standard (DSS)
- key management techniques—while mentioned in this document in discussions of secure payment—were not in scope for the implemented architecture
- securing web servers and web applications
- mobile device security
- penetration testing and vulnerability assessments
- risk checks that relate the login history of users with their login locations as criteria for granting access to the requested system
- wireless access concerns for conference attendees, as well as other concerns that involve large-scale testing

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 [15] 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 the publicly available NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* [16].

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" [17]. The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

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 reference design mitigates threats related to unauthorized and elevated privileges, data exfiltration, configuration modification, data modification, and access to sensitive data. Any or all of these unmitigated threats could lead to fraud, which is one of the largest concerns in the hospitality industry.

3.4.1.1 External Threats

One managed security service provider's annual global security report [14] shows that the hospitality industry has the second highest number of incidents being investigated by the provider. The same report notes that motivation or types of data targeted by malicious actors for hospitality organizations includes "credit card track data, financial/user credentials, proprietary information, and PII" [personally identifiable information].

Since 2014, a targeted technique labeled *DarkHotel hacking* [18] 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 by 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. 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 hotel staff and hotel 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 mitigating 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
- improperly deploy assets

3.4.3 Cybersecurity Control Map

Visit Appendix A to see the security control mappings that have been identified for this project's PMS reference design. 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], controls in NIST SP 800-53 rev 5 [9], and work roles in the NICE Cybersecurity Workforce Framework [11]. Section 5 of this document reiterates the security control mappings and introduces zero trust as another method of analysis and planning.

3.4.4 Privacy Control Map

Best practices for privacy protection include data minimization, transparency, and preference management. The *NIST Privacy Framework* Core [12] 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.

Visit Appendix B to see privacy control mappings that we have identified for this project's PMS reference design. A Privacy Framework Mapping table (Table B-1) shows the result from examining all the *NIST Privacy Framework* Core [12] Subcategories and picking the Subcategories supported by components of the PMS reference design. This work was done after the collaboration team designed the PMS reference design. 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 reference design and indicates which PMS reference design component is responsible for covering the Subcategory's desired outcome.

4 Architecture

The PMS reference design 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 showing the reference design implemented. It also introduces the use cases and process flows supported by the PMS reference design.

4.1 Architecture Description

The NCCoE worked with project collaborators to develop a standards-based, commercially available reference design demonstrating the following capabilities:

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

4.1.1 High-Level Architecture

This section introduces the components, functions, and technologies implemented. The PMS reference design includes the components shown in Figure 4-1.

Figure 4-1 Secure PMS High-Level Architecture

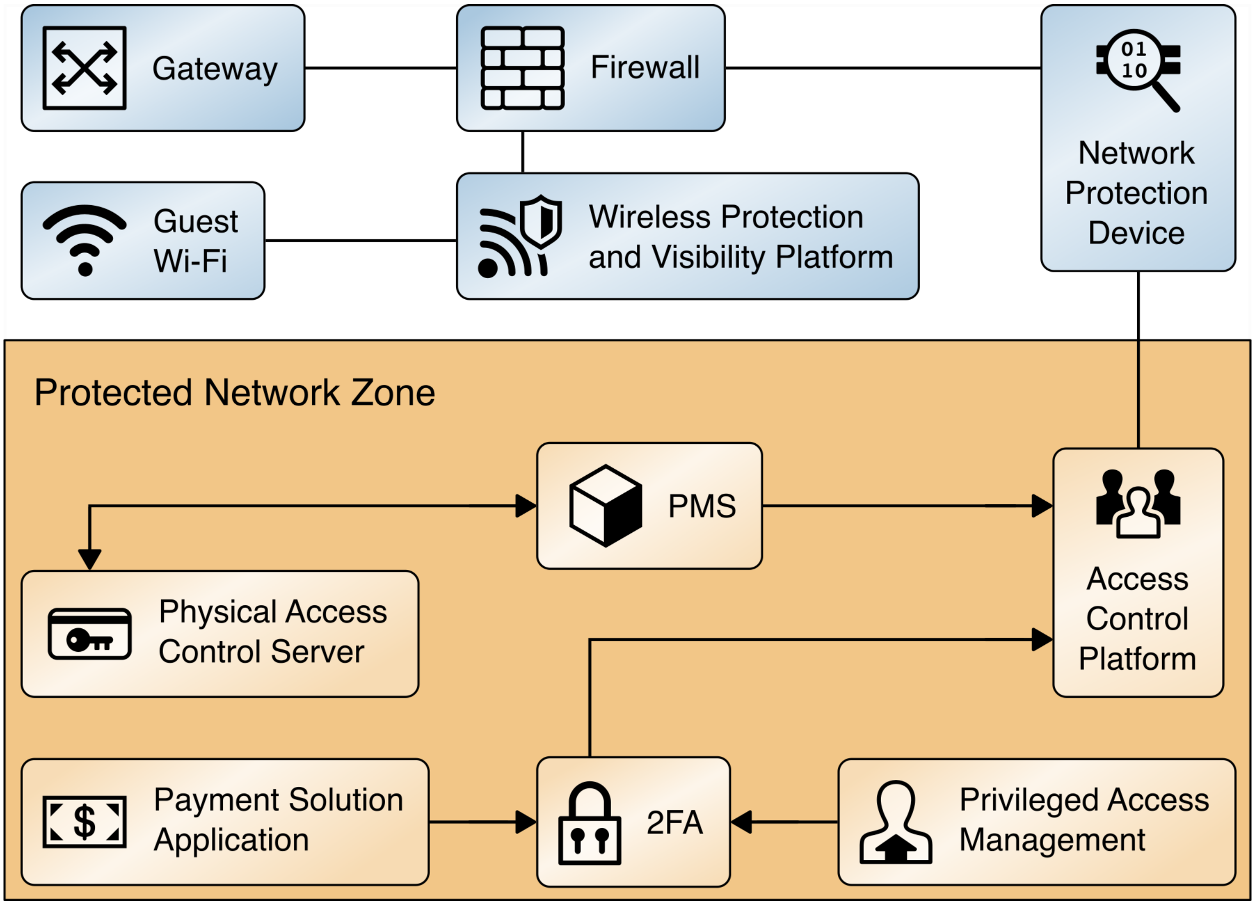

Gateway
Firewall
01
10
Network Protection Device
Guest Wi-Fi
Wireless Protection and Visibility Platform
Protected Network Zone
PMS
Access Control Platform
Physical Access Control Server
$
Payment Solution Application
2FA
Privileged Access Management

Table 4-1 provides a listing of each of the components introduced in Figure 4-1 along with a description of its function in the reference design and the commercial technology implemented in the reference design.

Table 4-1 Components, Functions, Technologies

Component	Function	Technology Implemented
PMS	facilitates the reservations process, checks customers in and out, tracks charges, and reconciles billing	Solidres Note: This component was not provided by collaborator. It was purchased for use in this reference design.
Network Protection Device	network protection appliance that works in concert with firewalls; provides additional layer of protection against cyber attacks	CryptoniteNXT Secure Zone 2.9.1
Access Control Platform	secures connection and control mechanism to enterprise devices from authorized users and authorized devices; also provides security perimeter monitoring, auditing, and logging activity	TDi ConsoleWorks 5.2-0u1
Privileged Access Management	provides real-time incident monitoring and detection, privilege escalation management, and reporting functions for the IT enterprise	Remediant SecureONE 18.06.3-ce
Wireless Protection and Visibility Platform	protects the hotel guest portion of the Wi-Fi by limiting guest access to only the internet and preventing hotel guest access to hotel back-end systems. Many hotel guest Wi-Fi systems are provided by service providers as standalone networks. An integrated Wi-Fi was included in this PMS reference design to demonstrate control of lateral movement of hotel guests, allowing the integrated Wi-Fi to support the installation of IoT devices in smart rooms or other systems requiring Wi-Fi connectivity.	Forescout CounterACT 8.1

Component	Function	Technology Implemented
Payment Solution Application	provides the token vault and tokenization along with multifactor authentication	StrongKey Tellaro Appliance (formerly known as StrongAuth KeyAppliance (SAKA)
Physical Access Control Server	physical access control system, including door locks, room-key encoding, and management	Häfele Dialock 2.0
Firewall	provides exterior protection and segments the enterprise	pfSense

4.2 Use Cases Supported by the Property Management System Reference Design

We designed and built the PMS reference design 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 reference design, all reservations are 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 reference design or conduct any unauthorized lateral movements.

The access control platform in the PMS reference design allows users to connect only to the systems for which they are authorized based on their role as a hotel guest, hotel staff, or system administrator. The action of inputting or modifying a reservation requires an authorized hotel staff user 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 hotel 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 reference design. 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 hotel staff user 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 Process Flows

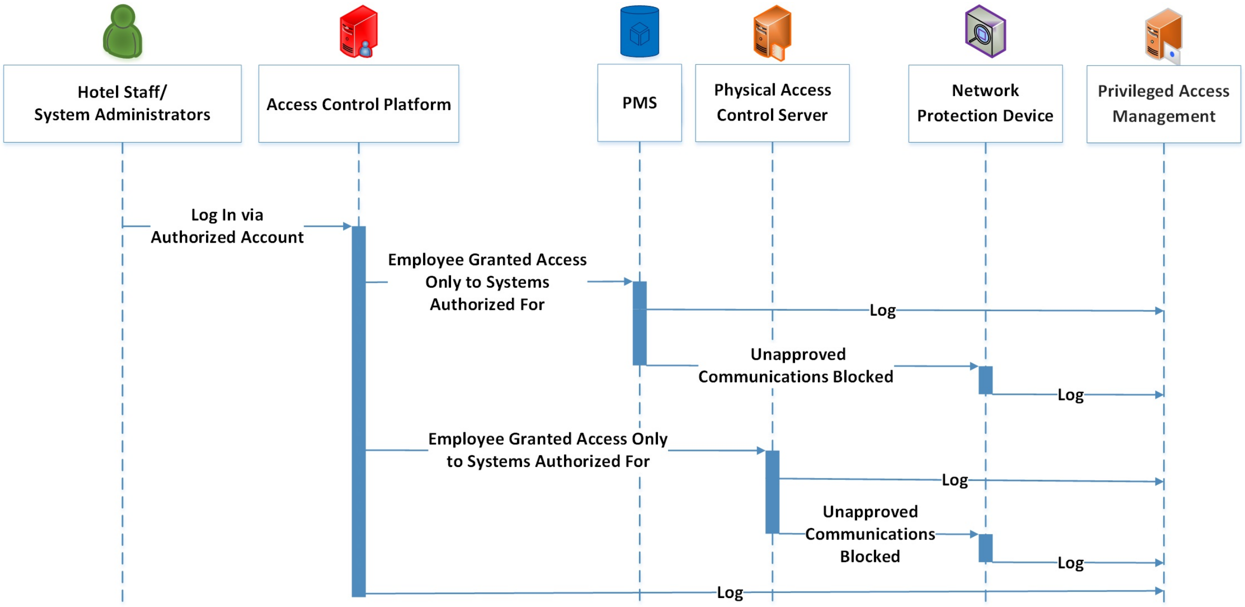
The following process flows show the sequence of events taking place for various hospitality functions in the enterprise.

4.3.1 Authorized Employee Access

Figure 4-2 shows the process flow for an authorized hotel staff user connecting to only the systems for which they are authorized. The hotel staff user 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 flow in Figure 4-2 is described below.

1. From a device or terminal, an authorized hotel staff user attempts to log in via the access control platform. All login attempts are directed to the access control platform and logged.
2. The hotel staff user 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 acted on according to policy.
5. Logs are collected by the privileged access management solution.

Figure 4-2 Staff Process Flow



4.3.2 Secure Credit Card Transaction

The technology used in this build can support HTNG's Secure Payment Framework [2]:

- **Encrypt cardholder data regardless of where transaction occurs** (card present/card not present)
- **Distribute Terminal Keys** as part of its management of the Derived Unique Key Per Transaction (DUKPT)
- **In one device** address all the precursor processes as well as the secure storage and processing of credit card data end-to-end

Figure 4-3 shows the process flow for a credit card transaction. The reference design adheres to guidance from the Secure Payments Framework [2]. The Secure Payments Framework is based on the concept that raw payment card data is not stored, processed, or transmitted by any hotel system within the control of the hotel company. The PMS reference design replaces raw payment card data with tokens. These tokens are useless to malicious actors. This approach is also aligned with PCI-DSS best practices.

The transaction is protected by the payment solution application via tokenization. The token alone is ineffective as only the payment solution application can decrypt it and associate a credit card with charges. This transaction flow assumes that the payment card data was ingested via an on-property customer-facing card reader, on-property POS, a kiosk, the property website, or was collected from a third-party entity. That payment card data is tokenized at the edge of the PMS environment via the tokenization appliance before it hits the PMS.

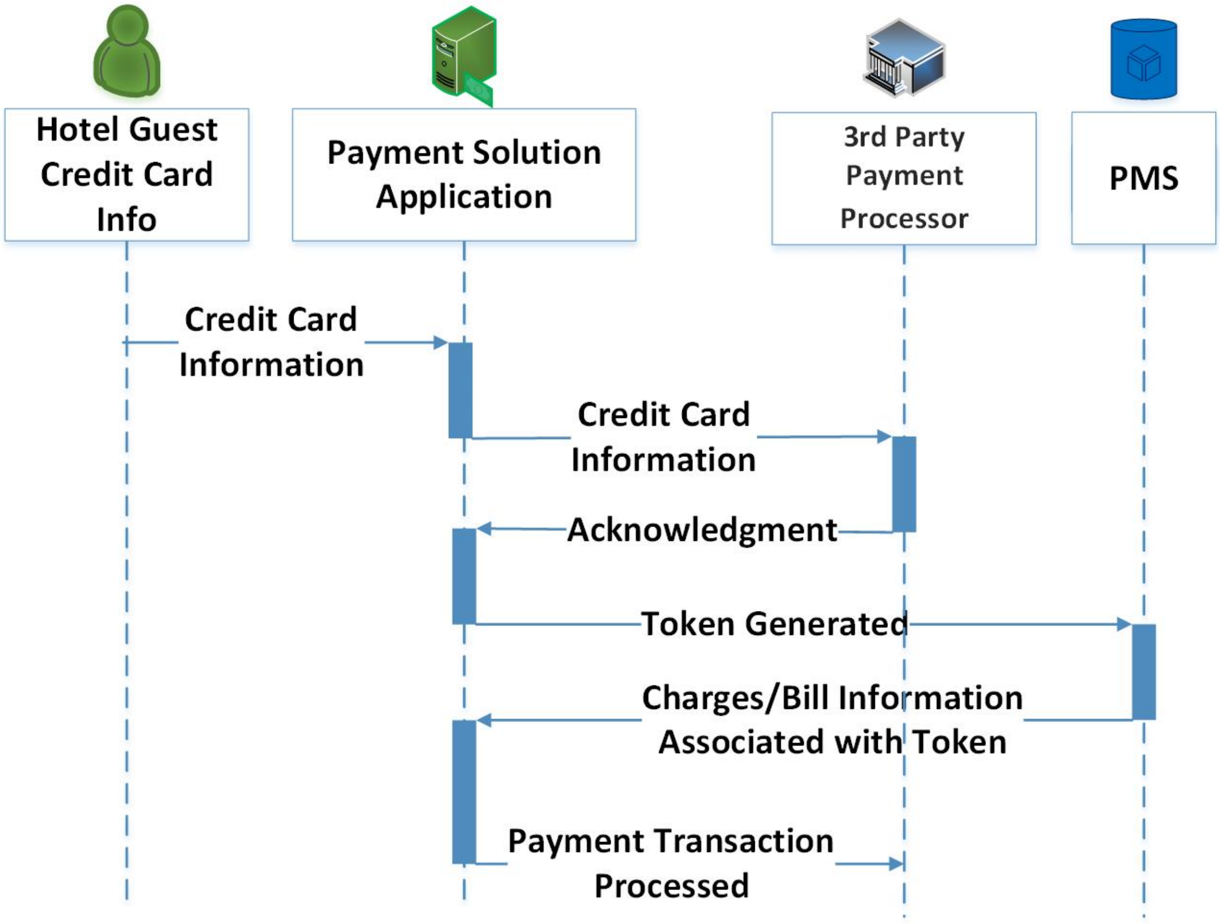
The process of Figure 4-3 is described below.

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.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

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.

Figure 4-3 Secure Credit Card Process Flow

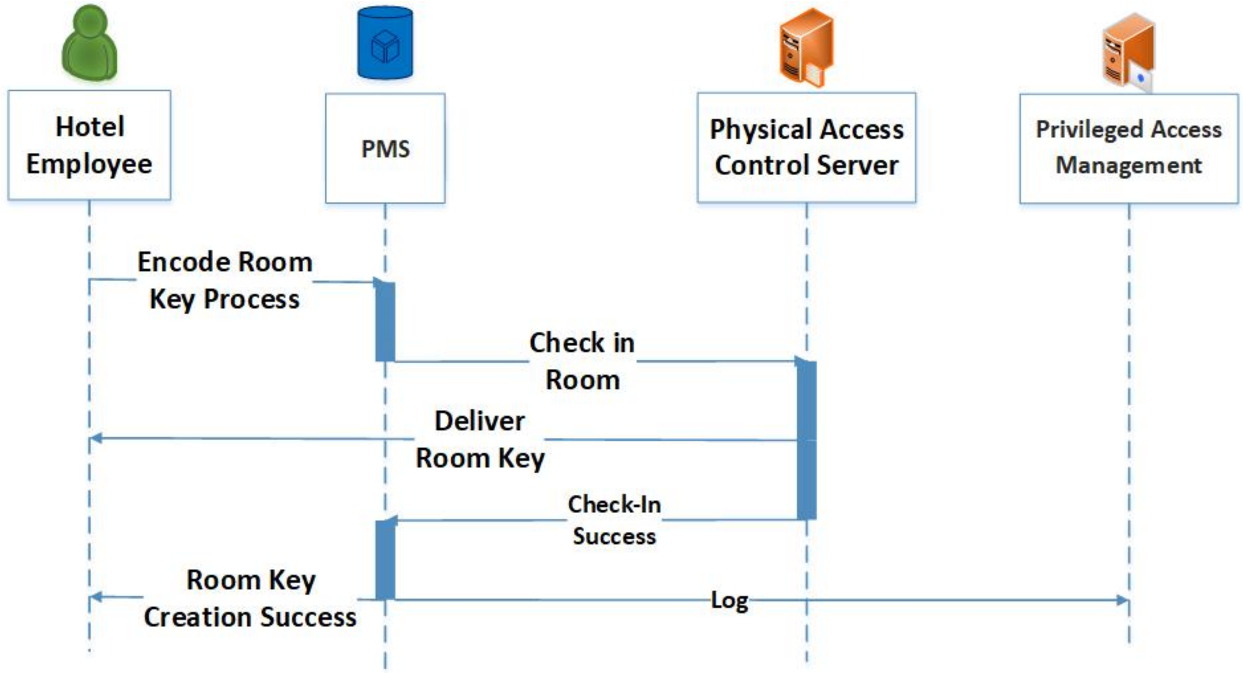

Hotel Guest Credit Card Info
Payment Solution Application
3rd Party Payment Processor
PMS
Credit Card Information
Credit Card Information
Acknowledgment
Token Generated
Charges/Bill Information Associated with Token
Payment Transaction Processed

4.3.3 Secure Interaction of Ancillary Hotel System (with PMS)

Figure 4-4 shows the process flow for the secure interaction of an ancillary system with the PMS. The following demonstrates how a door lock/room-key system is used in this example implementation.

1. An authorized hotel staff user connects to the PMS.
2. The physical access server validates the room-key request against a reservation in the PMS.
3. The room key is created and delivered.
4. All activity is logged and sent to the privileged access management system.

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



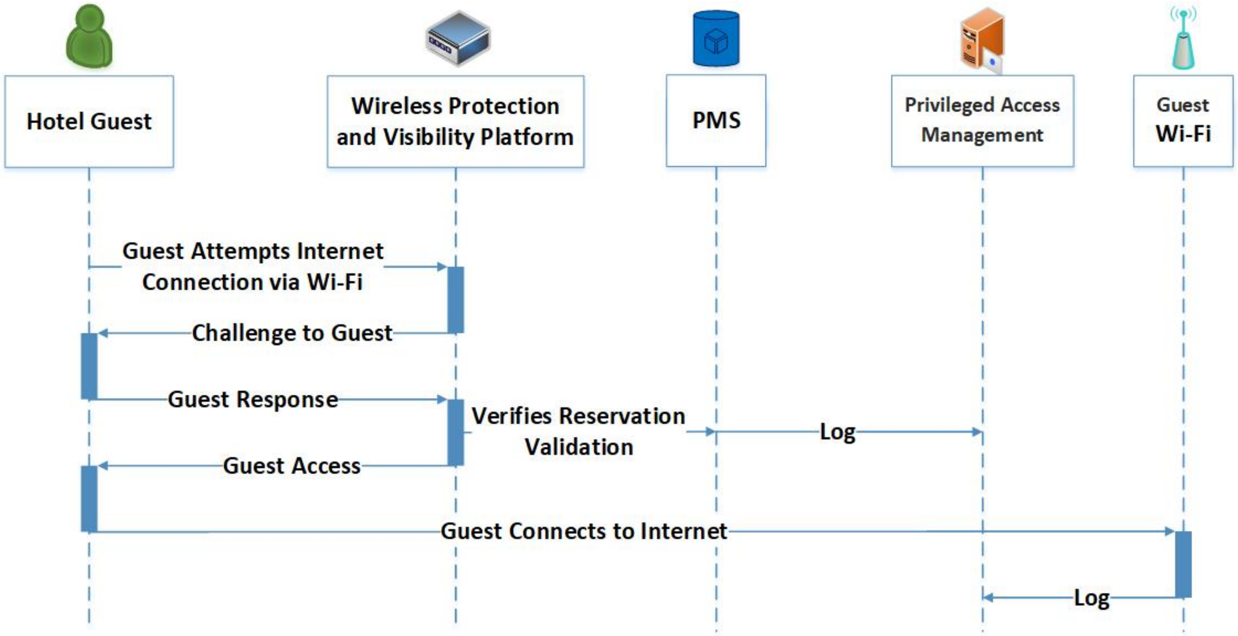
4.3.4 Hotel Guest Internet Access via Hotel Guest Wi-Fi

Figure 4-5 shows the process flow for a guest accessing the internet via the hotel’s guest Wi-Fi, showing how the:

1. Hotel guest attempts to connect to the internet via the guest Wi-Fi
2. Hotel guest is challenged
3. Hotel 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 hotel guest is provided internet access
5. Hotel 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

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

Figure 4-5 Guest Internet Access Via Guest Wi-Fi Process Flow


Hotel Guest
Wireless Protection and Visibility Platform
PMS
Privileged Access Management
Guest Wi-Fi
Guest Attempts Internet Connection via Wi-Fi
Challenge to Guest
Guest Response
Verifies Reservation Validation
Log
Guest Access
Guest Connects to Internet
Log

5 Security Characteristic Analysis

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

5.1 Analysis Assumptions and Limitations

The security characteristic analysis has the following limitations:

- The analysis is not a comprehensive test of individual security components, nor is it a red-team exercise involving adversarial emulation.
- The analysis cannot identify all weaknesses.
- The analysis does not include the lab infrastructure on which the project is built. The lab infrastructure undergoes regular patching and is in compliance with information security requirements per Federal law, including externally hosted systems that support NIST.

5.2 Analysis of the Reference Design’s Support for Cybersecurity Framework Subcategories

The NIST Cybersecurity Framework Subcategories are a basis for organizing our analysis and allow us to systematically consider how well the reference design supports its intended security characteristics in terms of the specific Subcategories of the Cybersecurity Framework. This analysis enables an understanding of how the example implementation achieved the goals of the design when compared against a standardized framework.

The Cybersecurity Framework includes Functions, Categories, and Subcategories that define the capabilities and processes needed to implement a cybersecurity program. In Table A-1, the NCCoE has identified the Subcategories that are desirable to implement when deploying the example implementation.

This section identifies the security benefits provided by each component of the example implementation and how those components support specific cybersecurity activities as specified in terms of Cybersecurity Framework Subcategories.

5.2.1 ID.AM-1: Physical devices and systems within the organization are inventoried

The network protection device, the CryptoniteNXT Secure Zone 2.9.1, has the capability to inventory devices and systems that are part of or attached to the PMS reference design and update the inventory in near real time.

5.2.2 ID.AM-2: Software platforms and applications within the organization are inventoried

The network protection device, the CryptoniteNXT Secure Zone 2.9.1, has the capability to inventory platforms and applications that are part of or attached to the PMS reference design and update the inventory in near real time.

5.2.3 PR.AC-1: Identities and credentials are issued, managed, verified, revoked, audited, proofed and bound to credentials, and asserted in interactions for authorized devices, users, and processes

The access control platform, TDi ConsoleWorks 5.2-0u1, manages credentials and identities.

5.2.4 PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions

The access control platform, TDi ConsoleWorks 5.2-0u1, challenges and verifies all credentials presented in the PMS reference design. The credential could be tied to a user, a system, an application, or a trusted third-party entity.

5.2.5 PR.AC-3: Remote access is managed

Through a combination of the TDi ConsoleWorks 5.2-0u1 access control platform and the Forescout CounterACT 8.1 wireless protection and visibility platform, all enterprise remote access activity is monitored, logged, and managed.

5.2.6 PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

The access control platform, TDi ConsoleWorks 5.2-0u1, and network protection device, CryptoniteNXT Secure Zone 2.9.1, work in combination to limit access in the least allowable fashion to only those authorized entities, users, systems, transactions, and platforms. Connections that are authorized are given the least level of privilege as feasible.

5.2.7 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)

Authentication that is commensurate with the risk of the transaction is an intrinsic part of the example implementation. Transactions/users/systems/applications are authenticated based upon the level of risk. Based upon configured policies, the access control platform, TDi ConsoleWorks 5.2-0u1, determines what level of authentication is required for a particular request as determined by the risk level associated.

5.2.8 PR.DS-1: Data at rest is protected

The payment solution appliance, the StrongKey Key Appliance, tokenizes credit card data within the StrongKey vault to protect data at rest. Only tokens are transmitted through the PMS reference design, which protects the data in transit.

5.2.9 PR.DS-2: Data in transit is protected

The payment solution appliance, the StrongKey Key Appliance, tokenizes credit card data within the StrongKey vault to protect data at rest. Only tokens are transmitted through the PMS reference design, which protects the data in transit.

5.2.10 PR.IP-3: Configuration change control processes are in place

The network protection device, CryptoniteNXT Secure Zone 2.9.1, has the capability to control, log, and manage changes and updates to devices and systems in the PMS reference design.

5.2.11 PR.PT-4: Communications and control networks are protected

The network protection device, CryptoniteNXT Secure Zone 2.9.1, monitors and protects the PMS reference design network and the devices connected to it.

5.2.12 DE.CM-1: The network is monitored to detect potential cybersecurity events

The reference designs support monitoring network activity. Event log information is reported and correlated by the privileged access management tool, Remediant SecureONE 18.06.3-ce.

5.2.13 DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

The reference design support monitoring personnel activity. Event log information is reported and correlated by the privileged access management tool, Remediant SecureONE 18.06.3-ce.

5.2.14 DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

The reference design support monitoring network and personnel activity. Event log information is reported and correlated by the privileged access management tool, Remediant SecureONE 18.06.3-ce. This also includes connections and attempted connections by unauthorized devices, users, and systems.

5.2.15 DE.DP-4: Event detection information is communicated

The privileged access management tool, Remediant SecureONE 18.06.3-ce, logs all incidents and can be configured to report out as required by the enterprise.

5.3 Zero Trust

Zero trust is a cybersecurity strategy that focuses on moving network defenses from wide, static network perimeters to focusing more narrowly on dynamic and risk-based access control to enterprise resources, regardless of where they are located.

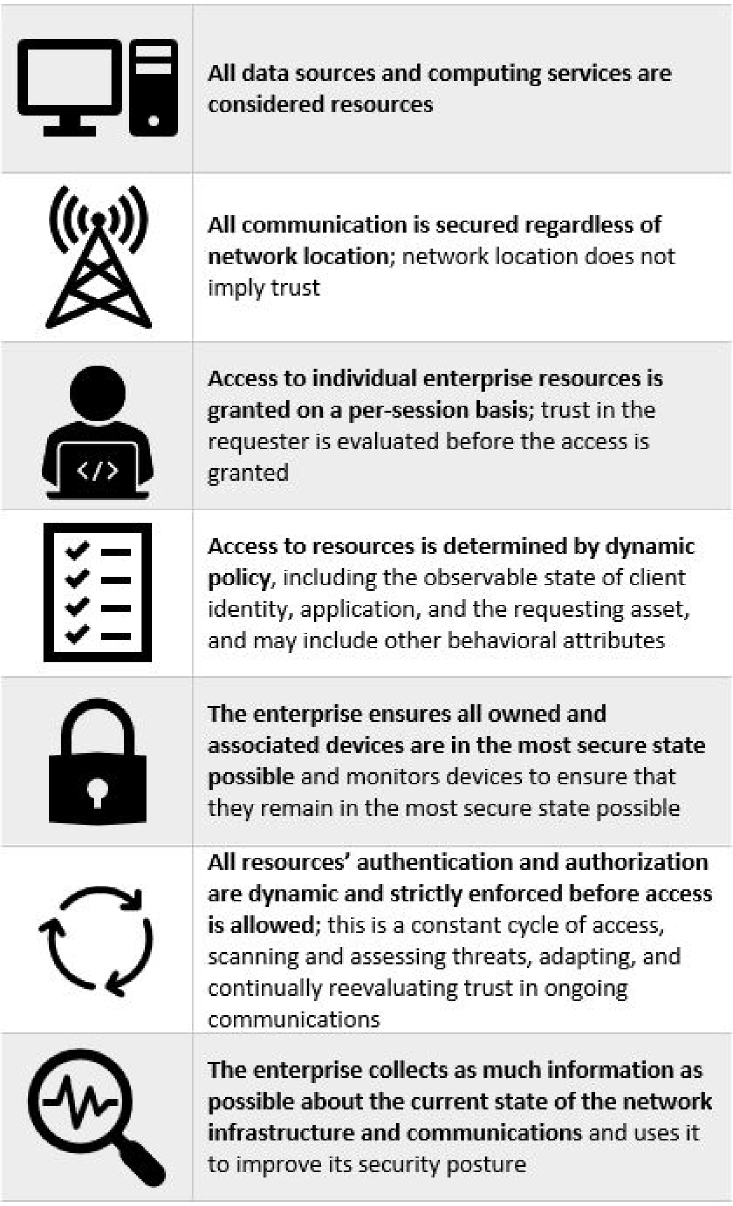
Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

5.3.1 Zero Trust Tenets

This project is also designed to show a PMS reference design with an architecture that adheres to tenets of zero trust. Conventional network security has focused on perimeter defenses. Once inside the network perimeter, users are “trusted” and often given broad access to many corporate resources. But malicious actors can come from inside or outside the network, and several high-profile cyber attacks in recent years have undermined the case for the perimeter-based model. Moreover, the perimeter is becoming less relevant due to several factors, including the growth of cloud computing, mobility, and changes in the modern workforce.

A zero trust architecture is designed and deployed with adherence to the zero trust tenets. Figure 5-1 identifies zero trust tenets.

Figure 5-1 Tenets of Zero Trust



All data sources and computing services are considered resources

All communication is secured regardless of network location; network location does not imply trust

Access to individual enterprise resources is granted on a per-session basis; trust in the requester is evaluated before the access is granted

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

The enterprise ensures 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

All resources' authentication and authorization are dynamic and strictly enforced before access is allowed; this is a constant cycle of access, scanning and assessing threats, adapting, and continually reevaluating trust in ongoing communications

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

These tenets are the ideal goal, though it must be acknowledged that not all tenets may be fully implemented in their purest form for a given strategy. This publication's strategy to secure a property management system does connect with each of the zero trust tenets. Table 5-1 shows zero trust tenets associated with components in the PMS reference design and Cybersecurity Framework Subcategories.

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

Zero Trust Tenet	PMS Reference Design 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 Reference Design 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.	No component was included in the PMS reference design to ensure that devices are in the most secure state.	**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 assessing threats, adapting, and continually reevaluating trust in ongoing communications.	Remediant SecureONE 18.06.3-ce CryptoniteNXT Secure Zone 2.9.1 Forescout CounterACT 8.1	**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** 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.

Zero Trust Tenet	PMS Reference Design Component	Cybersecurity Framework Subcategories
		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.

5.3.2 Components of Zero Trust

A zero trust architecture is an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement.

Figure 5-2 illustrates at a high level the components that compose a typical ZTA implementation.

Figure 5-2 Components of Zero Trust

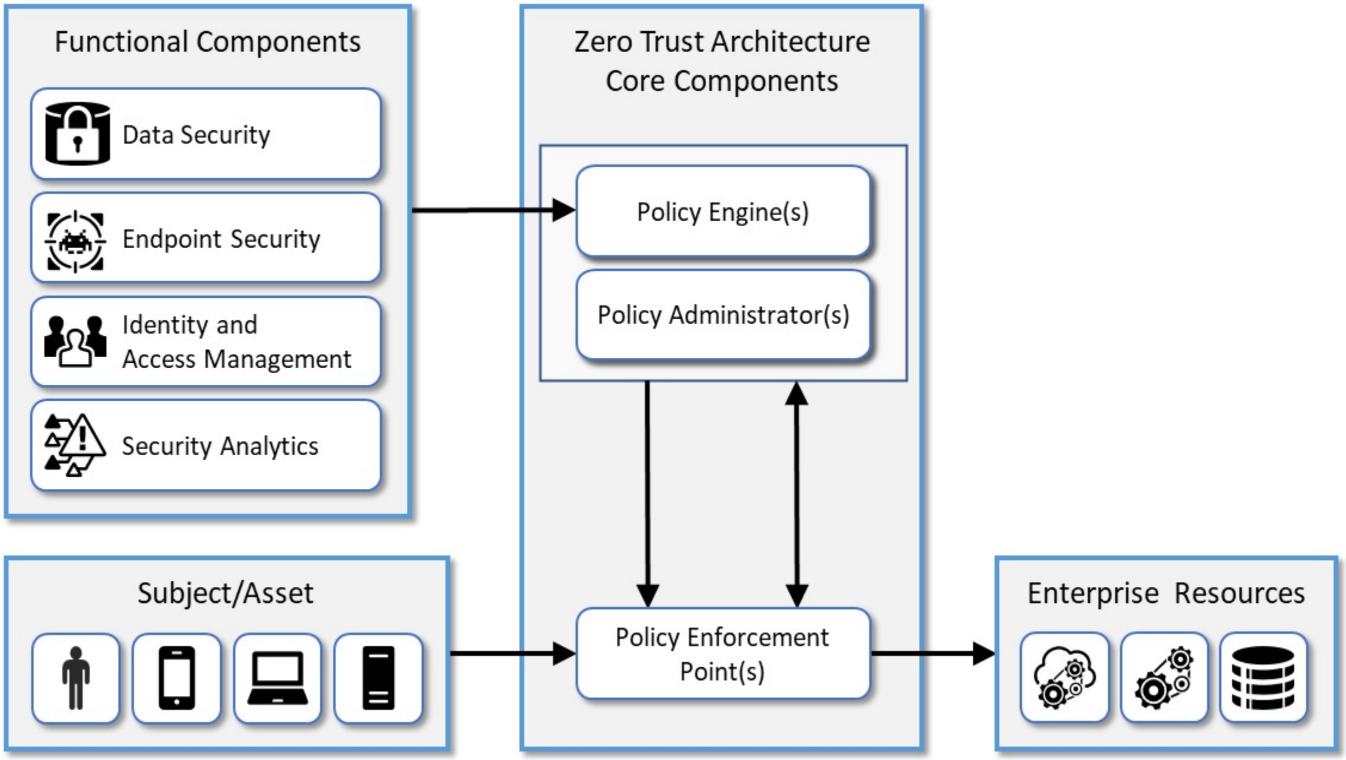


Table 5-2 maps PMS reference design components (originally identified in Table 4-1) to components of ZTA as described in NIST SP 800-207, *Zero Trust Architecture.*

Table 5-2 Zero Trust Component and PMS Reference Design Component Mapping

PMS Reference Design Component	Zero Trust Component
pfSense Firewall	Endpoint Security
TDi ConsoleWorks	Identity and Access Management (IDAM)
Remediant SecureOne	Security Analytics
Data encryption at rest (in StrongKey StrongAuth KeyAppliance and Solidres PMS) and in transit	Data Security
CryptoniteNXT Administration Control Center (ACC)	Policy Engine
Domain users, system administrators with access permission to the CryptoniteNXT administrator workstation	Policy Administrators
Any device within the CryptoniteNXT Secure Zone, including PMS and other security components	Policy Enforcement Points

PMS Reference Design Component	Zero Trust Component
Users (hotel guests, hotel staff, and system administrators)	Subjects
Workstation	Asset
Solidres PMS	Enterprise Resource
Data in Solidres PMS	Enterprise Resource
StrongKey StrongAuth KeyAppliance vault	Enterprise Resource
Credit card data in StrongKey StrongAuth KeyAppliance vault	Enterprise Resource

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 Analysis Assumptions and Limitations

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

- The analysis is not a comprehensive test of individual privacy components, nor does it include completion of a privacy risk assessment methodology.
- The analysis 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 reference design. The PMS reference design architecture was designed before the *NIST Privacy Framework* [12] 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 reference designs 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 reference design.

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 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

Capability Requirement (CR) ID	Parent Requirement	Subrequirement	Test Case	Component
CR 1.a		room key provisioned	PMS-05	physical access control server
CR 2	authorized hotel staff 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
CR 3.b		Eavesdropper cannot see credit card data.	PMS-07b	payment solution appliance
CR 4	Wi-Fi hotel guest connectivity/login		PMS-06a	wireless protection and visibility platform
CR 4.a		Hotel 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 Hotel Staff 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 hotel staff 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	Hotel staff user can log in to the PMS with their issued credentials.
actual results	Hotel staff 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) hotel staff 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 hotel staff 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 Test Case PMS-03 (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 (Hotel Staff 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.

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 hotel staff 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

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

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

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 hotel staff 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 hotel staff 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 hotel staff 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
sub test cases	Verify that the hotel staff user has access to only the data set(s) for which they are authorized; further, that they can only 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 hotel staff 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.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

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.
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 provisioning a room key.

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 hotel guest.

Test Case Field	Description
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.
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 Test Case PMS-06 (Provisioning Guest Wi-Fi Access)

The following two test cases will validate provisioning hotel 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 hotel guest connectivity/login
description	Only registered hotel 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

Test Case Field	Description
sub test cases	Verify that the hotel 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; hotel guest has provisioned Wi-Fi login
procedure	Attempt to connect a device to the guest Wi-Fi. When the login screen appears, enter the password created for the hotel 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

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

Table 7-11 contains test case requirements, associated test case, and descriptions of the test scenario for preventing a guest from accessing any restricted back-end systems.

Table 7-11 Prevent Unauthorized Guest Lateral Movement via Wi-Fi

Test Case Field	Description
requirement tested	(CR 4.a) Hotel guest cannot access enterprise systems.
description	Only registered hotel guests are granted limited Wi-Fi access.
associated Cybersecurity Framework Subcategories	PR.AC-3, PR.PT-4, DE.CM-3

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

7.1.8 Test Case PMS-07 (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

Test Case Field	Description
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.
preconditions	PMS is up and running properly.
procedure	Log on to hotel staff 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.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

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.
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.

Test Case Field	Description
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.
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

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

8 Future Build Considerations

The NCCoE is open to building future projects or drafting publications in the hospitality sector that not only push to secure a property management system but also reduce cybersecurity and privacy risk for any of the networked technologies being leveraged by the sector.

Exploration of how to mitigate risks could include focus on the use of personal mobile devices as room keys or as controllers of hotel-owned smart devices in a room. The NCCoE has a growing library of publications focused on mobile device security that may prove relevant to the hospitality sector. https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security

NIST has evolving focus on many areas aimed at reducing cybersecurity and privacy risk, so opportunities exist to frame adoption of more cybersecurity to reduce the risks from the expansion of the use of Internet of Things devices in the hospitality sector.

NIST's Cybersecurity for the Internet of Things program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

Additionally, future efforts at the NCCoE might dive deeper to highlight the use of geo-velocity, geo-location, and rate limiting for connections as risk checks for authentication and analytics.

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) reference design built in this practice guide. The first three columns show the Cybersecurity Framework Functions, Categories, and Subcategories addressed by the PMS reference design. The next three columns show mappings from the Cybersecurity Framework Subcategories to specific components in the Payment Card Industry Data Security Standard (PCI DSS) v3.2.1; security and privacy controls in NIST Special Publication (SP) 800-53r5; and/or work roles in NIST SP 800-181r1, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [11]. This table is included to help connect those with expertise in PCI DSS, NIST SP 800-53, and the NICE Framework with the risk being addressed in this PMS reference design. Examining existing work roles in the NICE Framework may help an organization identify if it has people who can perform tasks and apply the skills described for each work role on its deployment teams. Noting a discrete PCI requirement or NIST SP 800-53r5 control [9] may match areas of focus within an organization that securing a PMS reference design 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 800-53r5 Security and Privacy Controls [9]	NICE Framework 2017 Work Roles [11]
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational	**ID.AM-1:** Physical devices and systems within the organization are inventoried.		CM-8, PM-5	Technical Support Specialist
		ID.AM-2: Software platforms and applications within the organization are inventoried.		CM-8, PM-5	Technical Support Specialist

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	**Category**	**Subcategory**	**PCI DSS v3.2.1**	**NIST SP 800-53r5 Security and Privacy Controls [9]**	**NICE Framework 2017 Work Roles [11]**
	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.	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 or Product Support Manager
			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		

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	Category	Subcategory	PCI DSS v3.2.1	NIST SP 800-53r5 Security and Privacy Controls [9]	NICE Framework 2017 Work Roles [11]
			kept for archived/legacy encrypted data. 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 or System Administrator
		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 or System Administrator

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	Category	Subcategory	PCI DSS v3.2.1	NIST SP 800-53r5 Security and Privacy Controls [9]	NICE Framework 2017 Work Roles [11]
			7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.		Technical Support Specialist or System Administrator
			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
			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

NIST Cybersecurity Framework v1.1			**Standards and Best Practices**		
Function	**Category**	**Subcategory**	**PCI DSS v3.2.1**	**NIST SP 800-53r5 Security and Privacy Controls [9]**	**NICE Framework 2017 Work Roles [11]**
			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
			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
		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	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

NIST Cybersecurity Framework v1.1			**Standards and Best Practices**		
Function	**Category**	**Subcategory**	**PCI DSS v3.2.1**	**NIST SP 800-53r5 Security and Privacy Controls [9]**	**NICE Framework 2017 Work Roles [11]**
			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.		
		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).		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
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity,	**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

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	Category	Subcategory	PCI DSS v3.2.1	NIST SP 800-53r5 Security and Privacy Controls [9]	NICE Framework 2017 Work Roles [11]
	and availability of information.		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 data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.		Information Systems Security Developer
			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
			3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.		Information Systems Security Developer

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	**Category**	**Subcategory**	**PCI DSS v3.2.1**	**NIST SP 800-53r5 Security and Privacy Controls [9]**	**NICE Framework 2017 Work Roles [11]**
			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
		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.	SC-8, SC-11, SC-12	Information Systems Security Developer or Cyber Defense Analyst
			1.3 Prohibit direct public access between the internet and any system component in the cardholder data environment.		Information Systems Security Developer or Cyber Defense Analyst

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	**Category**	**Subcategory**	**PCI DSS v3.2.1**	**NIST SP 800-53r5 Security and Privacy Controls [9]**	**NICE Framework 2017 Work Roles [11]**
		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
	Information Protection Processes and Procedures (PR.IP): Security policies (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.	**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).		CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	Enterprise Architect or Cyber Policy and Strategy Planner
		PR.IP-3: Configuration change control processes are in place.		CM-3, CM-4, SA-10	Systems Developer or Systems Security Analyst

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	**Category**	**Subcategory**	**PCI DSS v3.2.1**	**NIST SP 800-53r5 Security and Privacy Controls [9]**	**NICE Framework 2017 Work Roles [11]**
	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
		PR.PT-4: Communications and control networks are protected.		AC-4, AC-17, AC-18, CP-8, SC-7, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	Security Architect or Communications Security (COMSEC) Manager
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
	Security Continuous Monitoring (DE.CM): The information system and as-	**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

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	Category	Subcategory	PCI DSS v3.2.1	NIST SP 800-53r5 Security and Privacy Controls [9]	NICE Framework 2017 Work Roles [11]
	sets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events.		CA-7, PE-3, PE-6, PE-20	Network Operations Specialist
		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
	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	AU-6, CA-2, CA-7, RA-5, SI-4	Cyber Defense Infrastructure Support Specialist

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	Category	Subcategory	PCI DSS v3.2.1	NIST SP 800-53r5 Security and Privacy Controls [9]	NICE Framework 2017 Work Roles [11]
			and strong role-based authentication for authorized log users.		

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) reference design components.

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

Privacy Framework Function	Privacy Framework Category	Privacy Framework Subcategory	PMS Reference Design 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 principle of data minimization.	Remediant SecureONE 18.06.3-ce

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

Appendix C Deployment Recommendations

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.

Deployment of a zero trust architecture to secure a property management system (PMS) into an existing infrastructure will require an organization to consider its existing practices for interoperability and usability.

Deployers should adhere to best practice guidance for vulnerability and patch management [20], continuity of operations planning, and environment elements that are not addressed in this document.

The individual organizations that compose every enterprise are experiencing an increase in the frequency, creativity, and severity of cybersecurity attacks. The National Institute of Standards and Technology recommends that all organizations and enterprises, regardless of size or type, should ensure that cybersecurity risks receive appropriate attention as they carry out their Enterprise Risk Management (ERM) functions. As such, a deployment of a zero trust architecture around a PMS reduces cybersecurity risk and should be included in all the cybersecurity risk information used to inform the overall ERM [21]. By doing so, enterprises and their component organizations can better identify, assess, and manage their cybersecurity risks in the context of their broader mission and business objectives.

Appendix D List of Acronyms

2FA	Two-Factor Authentication
CNSSI	Committee on National Security Systems Instruction
CRS	Central Reservation System
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
IP	Internet Protocol
IT	Information Technology
IoT	Internet of Things
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
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: National Institute of Standards and Technology (NIST) Special Publication (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 Cybersecurity Center of Excellence (NCCoE) Securing Property Management Systems for the Hospitality Sector, A Notice by the National Institute of Standards and Technology on 11/24/2017. Available at https://www.federalregister.gov/documents/2017/11/24/2017-25427/national-cybersecurity-center-of-excellence-nccoe-securing-property-management-systems-for-the.

[2] Hotel Technology Next Generation (HTNG). *Secure Payments Framework for Hospitality,* version 1.0. Feb. 2013. Available at 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 at https://cdn.ymaws.com/htng.site-ym.com/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/HTNG_Secure_Payments_Framework_v1.0_FINAL.pdf.

[4] HTNG. *Payment Systems & Data Security Specifications 2010B*. Oct. 22, 2010. Available at 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 at 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 at https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

[7] HTNG. *GDPR for Hospitality*. June 1, 2019. Available at https://cdn.ymaws.com/www.htng.org/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/GDPR_for_Hospitality_-_V2_-_2019.pdf.

[8] National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1. Apr. 16, 2018. Available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[9] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Information Systems and Organizations,* NIST Special Publication (SP) 800-53 Rev. 5, NIST, Gaithersburg, Md., Sept. 2020. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

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

[11] R. Petersen et al., *Workforce Framework for Cybersecurity (NICE Framework),* NIST SP 800-181 Revision 1, NIST, Gaithersburg, Md., Nov. 2020. Available at https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center.

[12] National Institute of Standards and Technology. *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management,* Version 1.0. Available at https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf.

[13] S. Rose et al., *Zero Trust Architecture*, NIST SP 800-207, NIST, Gaithersburg, Md., Aug. 2020, 59 pp. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

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

[15] *NIST. *Risk Management Framework: Quick Start Guides*. Available at https://csrc.nist.gov/Projects/risk-management.

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

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

[18] Social Tables. *Cybersecurity for Hotels: 6 Threats Just Around the Corner from Your Property.* Available at https://www.socialtables.com/blog/hospitality/cyber-security-hotels/.

[19] C. Paulsen, R. Byers, Glossary of Key Information Security Terms, NIST Interagency or Internal Report NISTIR) 7298 Rev. 3, NIST, Gaithersburg, Md., July 2019. Available at https://csrc.nist.gov/glossary/term/vulnerability.

[20] NCCoE. *Critical Cybersecurity Hygiene: Patching the Enterprise*. Available at https://www.nccoe.nist.gov/projects/building-blocks/patching-enterprise.

[21] NIST. NISTIR 8286: *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, Oct. 2020. Available at https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf.

*Superseded on March 15, 2021 by Quick Start Guides (QSG) for the RMF Steps found at the bottom of https://csrc.nist.gov/Projects/risk-management/about-rmf which is a link off of NIST's new NIST Risk Management Framework (RMF) https://csrc.nist.gov/Projects/risk-management website.

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

March 2021

FINAL

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-27

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

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-27C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-27C, 138 pages, March 2021, CODEN: NSPUE2

FEEDBACK

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, 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 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, which are central to hotel operations, present attractive attack surfaces. This example implementation strives to increase the cybersecurity of the property management system (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.

The NCCoE at NIST built a PMS reference design in a laboratory to explore methods for improving the cybersecurity of a PMS. The scope of the PMS reference design included the PMS, a credit card payment platform, and an analogous ancillary hotel/PMS. 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 architecture, moving target defense, tokenization of credit card data, and role-based authentication.

The PMS reference design 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; privacy; property management system; role-based authentication; tokenization; network security; 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
John Bell	AjonTech LLC
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
Kartikey Desai	MITRE
Eileen Division	MITRE
Karri Meldorf	MITRE

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

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 system 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

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

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 of the products employed in this reference design. We do not re-create the product manufacturers' documentation, which is presumed to be widely available. Rather, this volume shows 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 readers of this guide with the information they need if they choose to replicate the property management system (PMS) reference design. 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 Assessment, describes the risk analysis we performed.
- Section 3.4.3, Cybersecurity Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

Section 6.2, Privacy Protections of the Reference Design, 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 re-create 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 Reference Design Overview

The NCCoE at NIST built an example laboratory environment, known hereafter as the PMS reference design, to explore options available to secure a PMS 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 reference design. For a detailed description of the PMS reference design's architecture and the use cases, see Section 4 in Volume B.

1.3.2 Architectural Overview

The *Securing Property Management Systems* reference design is shown in detail in Figure 1-1a and Figure 1-1b. These figures show the technologies used in the PMS reference design. 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 off-site 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 PMS reference design uses the components listed in Table 1-1 and shown in Figure 1-1a and Figure 1-1b.

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 reference design. The figures show the components, firewalls, and network design of the PMS reference design. 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. Figure 1-1a has the VLAN 2128 component in the upper right, and Figure 1-1b shows it in the upper left. The installation and configuration details for the key components shown in the figures is the focus of this volume of the guide.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

Figure 1-1a PMS Reference Design Detailed Architecture (1 of 2)

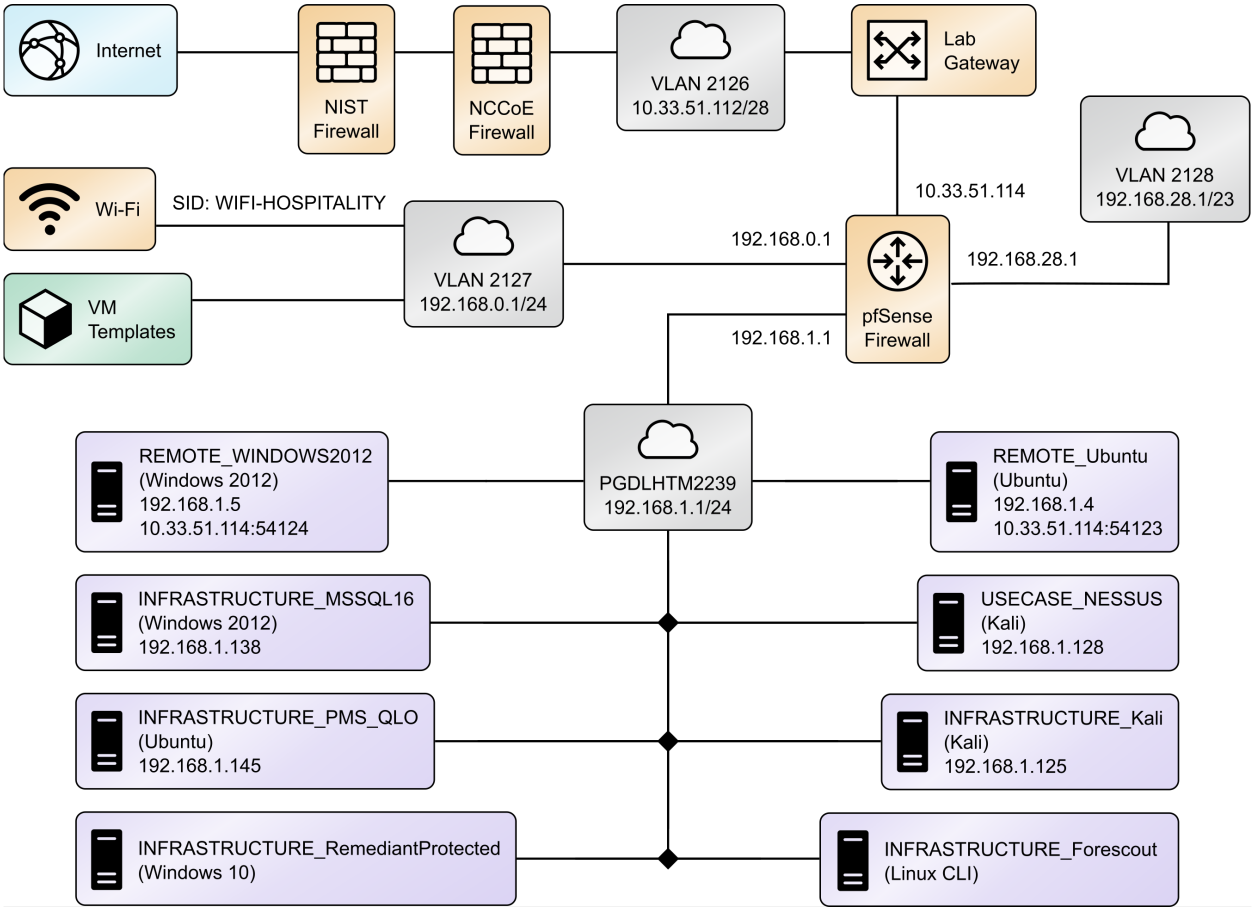
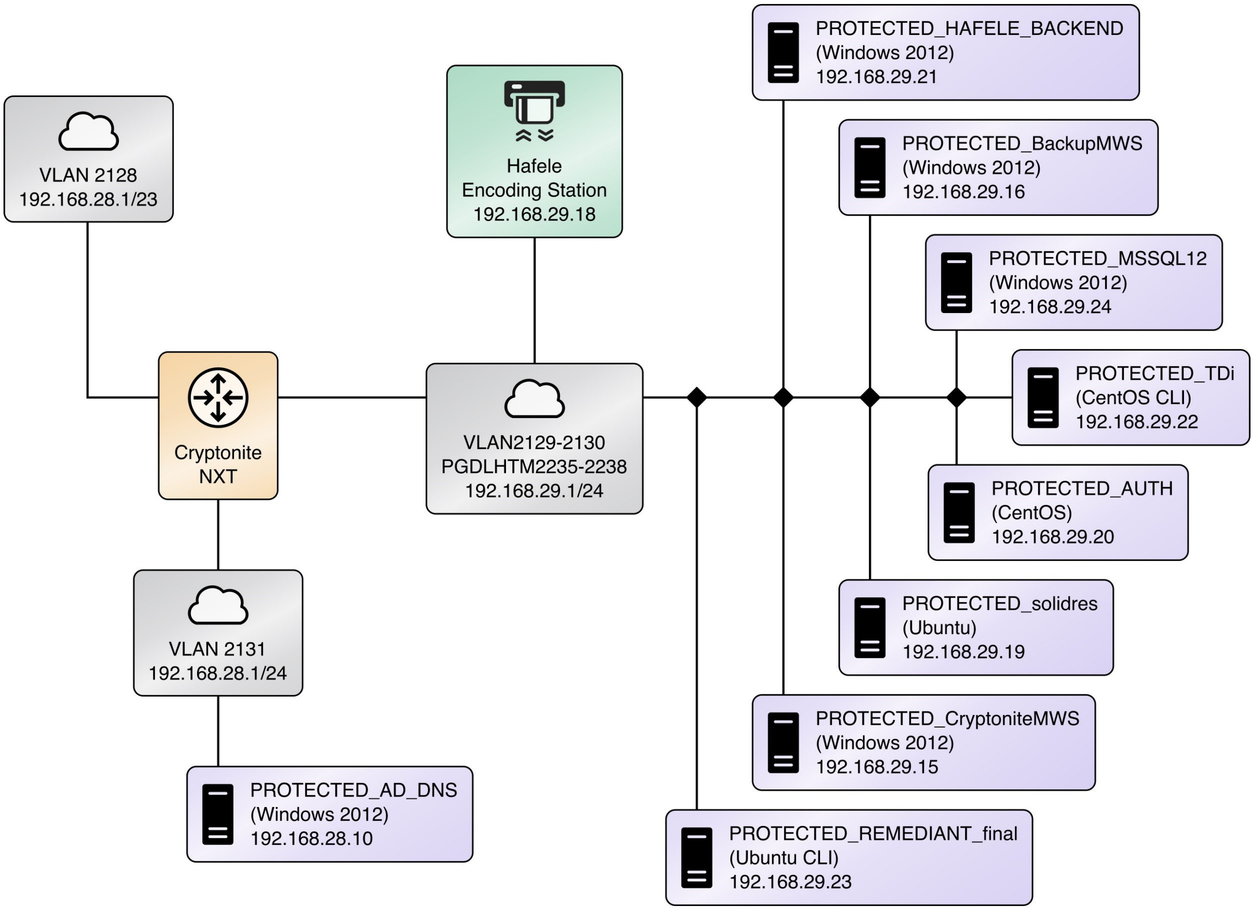

Internet
NIST Firewall
NCCoE Firewall
VLAN 2126 10.33.51.112/28
Lab Gateway
10.33.51.114
VLAN 2128 192.168.28.1/23
Wi-Fi
SID: WIFI-HOSPITALITY
VLAN 2127 192.168.0.1/24
192.168.0.1
192.168.28.1
pfSense Firewall
VM Templates
192.168.1.1
REMOTE_WINDOWS2012 (Windows 2012) 192.168.1.5 10.33.51.114:54124
PGDLHTM2239 192.168.1.1/24
REMOTE_Ubuntu (Ubuntu) 192.168.1.4 10.33.51.114:54123
INFRASTRUCTURE_MSSQL16 (Windows 2012) 192.168.1.138
USECASE_NESSUS (Kali) 192.168.1.128
INFRASTRUCTURE_PMS_QLO (Ubuntu) 192.168.1.145
INFRASTRUCTURE_Kali (Kali) 192.168.1.125
INFRASTRUCTURE_RemediantProtected (Windows 10)
INFRASTRUCTURE_Forescout (Linux CLI)

Figure 1-2b PMS Reference Design Detailed Architecture (2 of 2)



1.3.3.1 Network Segmentation and Domain Name System (DNS)

Table 1-2 lists the hospitality example lab build's network internet protocol (IP) address range for the PMS reference design. These network addresses were used in the example implementation builds, and each organization will configure IP addresses to reflect actual network architectures when deployed.

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

Network	PMS Reference Design 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

In the PMS reference design, 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 reference design 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
  - IP Address: 192.168.28.10
  - Netmask: 255.255.255.0
  - IPv6 Disable
  - Gateway: 192.168.28.3
  - 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.

The Administrator Control Center of CryptoniteNXT serves as the policy engine for zero trust architecture (ZTA).

2.1.1 Overview of Network Protection Solution

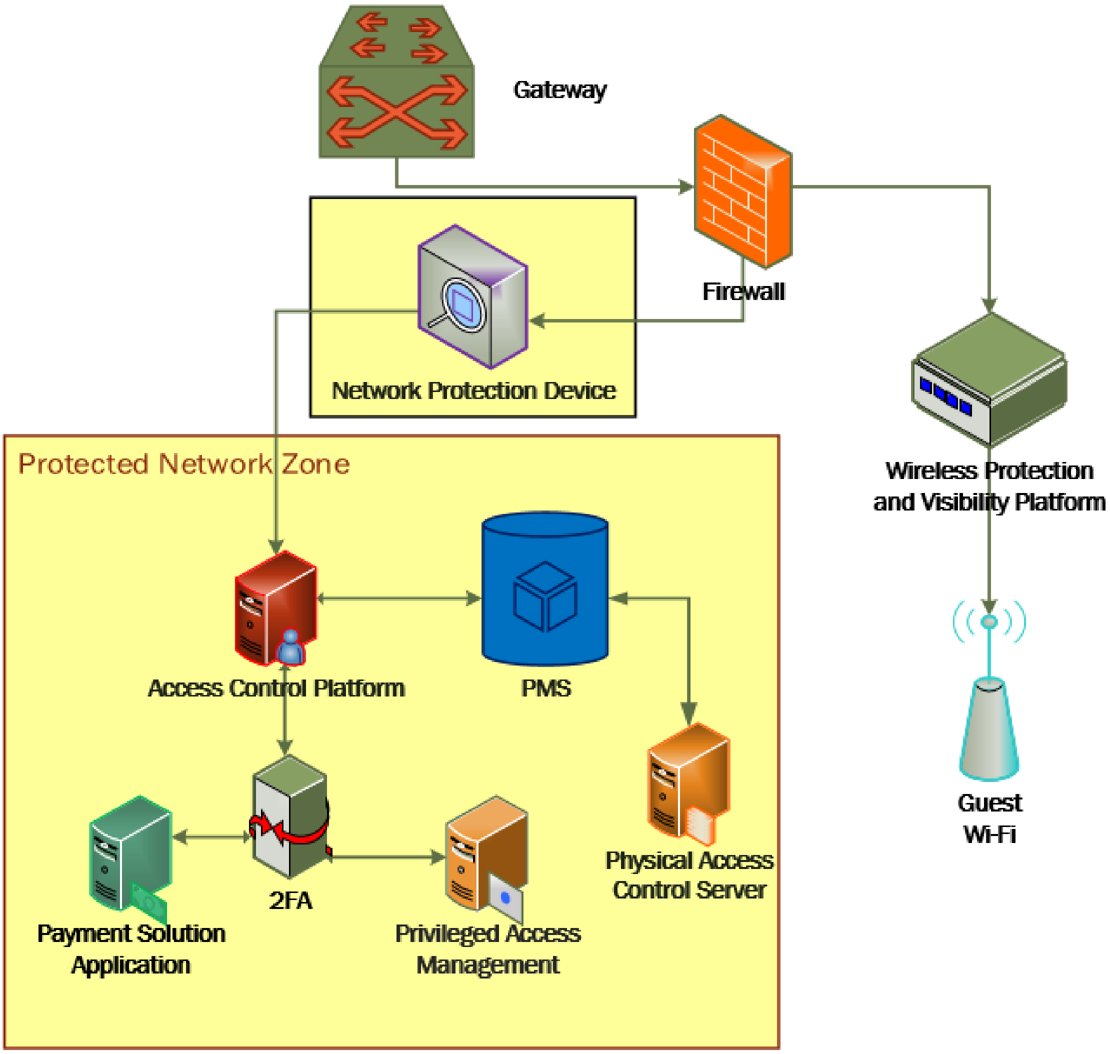
CryptoniteNXT is employed here as the network protection solution device and brings ZTA and moving target defense capabilities to the PMS reference design.

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 ZTA philosophy to its protected network zone. ZTA 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.

Figure 2-1 Network Protection Solution in the Reference Architecture


Gateway
Firewall
Network Protection Device
Wireless Protection and Visibility Platform
Protected Network Zone
Access Control Platform
PMS
Physical Access Control Server
Guest Wi-Fi
2FA
Payment Solution Application
Privileged Access Management

2.1.2 Network Protection Solution–CryptoniteNXT–Requirements

The following subsections document the software, hardware, and network requirements for the network protection solution for version 2.9.1.

2.1.2.1 Hardware Requirements for the Network Protection Solution

CryptoniteNXT was deployed as a physical piece of hardware, provided by the vendor. If a virtual 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:

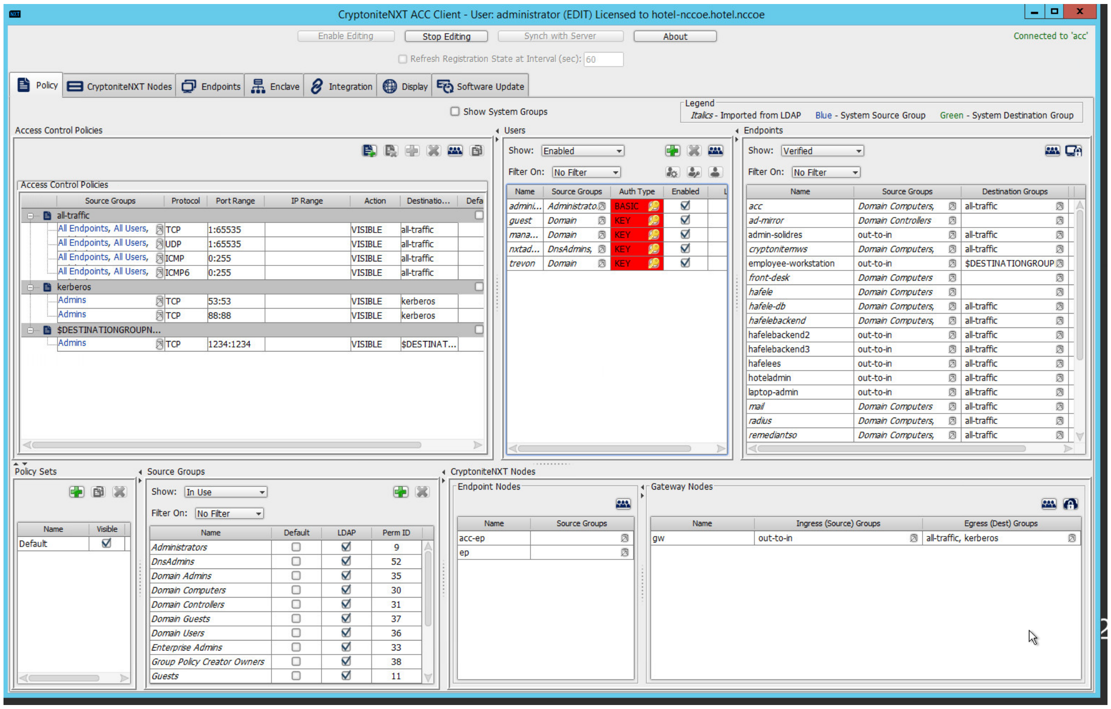
1. Create a source group to govern what network connections can flow from an end point.
2. Create a destination group to govern what network connections can flow to an end point.
3. Apply a source group to a specific end point.
4. Apply a destination group to a specific end point.
5. Create and apply 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:**



□ Refresh Registration State at Interval (sec): 60

□ Show System Groups

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							□
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							□
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							□
	Admins	TCP	1234:1234		VISIBLE	$DESTINAT...	

Users — Show: Enabled; Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	Administrato...	BASIC	☑
guest	Domain	KEY	☑
mana...	Domain	KEY	☑
nxtad...	DnsAdmins,	KEY	☑
trevon	Domain	KEY	☑

Endpoints — Show: Verified; Filter On: No Filter

Name	Source Groups	Destination Groups
acc	Domain Computers,	all-traffic
ad-mirror	Domain Controllers	
admin-solidres	out-to-in	all-traffic
cryptonitemws	Domain Computers,	all-traffic
employee-workstation	out-to-in	$DESTINATIONGROUP
front-desk	Domain Computers	
hafele	Domain Computers	
hafele-db	Domain Computers,	all-traffic
hafelebackend	Domain Computers,	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	Domain Computers	all-traffic
radius	Domain Computers,	all-traffic
remediantso	Domain Computers,	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups — Show: In Use; Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	□	☑	9
DnsAdmins	□	☑	52
Domain Admins	□	☑	35
Domain Computers	□	☑	30
Domain Controllers	□	☑	31
Domain Guests	□	☑	37
Domain Users	□	☑	36
Enterprise Admins	□	☑	33
Group Policy Creator Owners	□	☑	38
Guests	□	☑	11

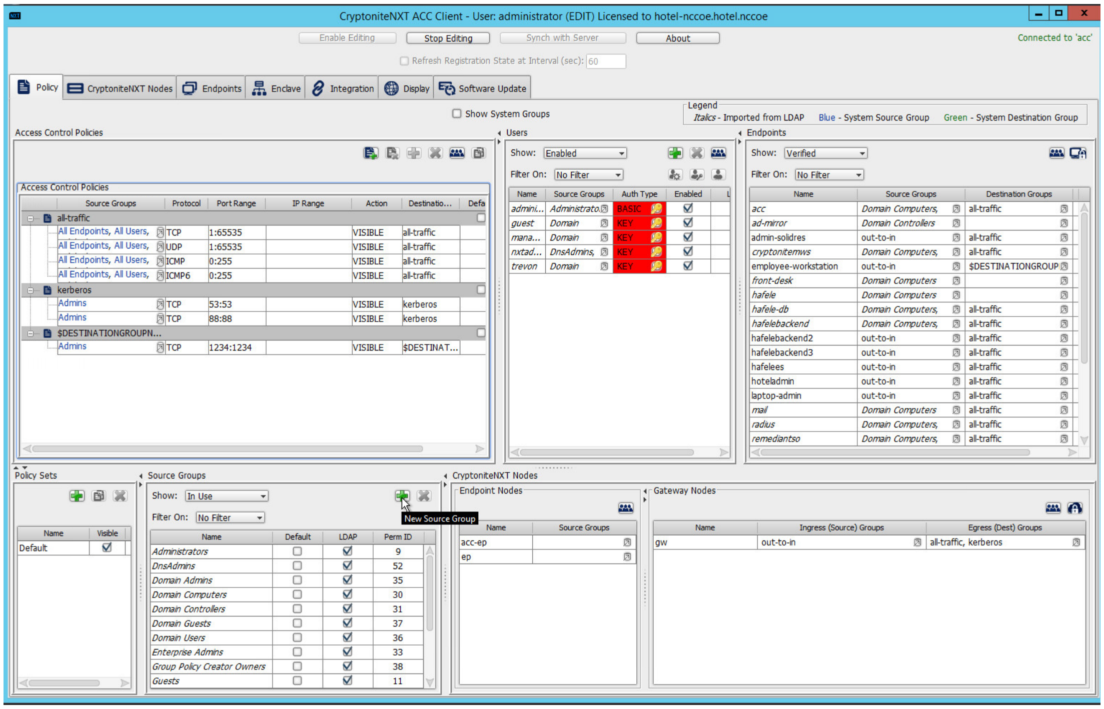
Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

☐ Refresh Registration State at Interval (sec): 60

☐ Show System Groups

Legend: *Italics* - Imported from LDAP Blue - System Source Group Green - System Destination Group

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							☐
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							☐
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							☐
	Admins	TCP	1234:1234		VISIBLE	$DESTINAT...	

Users — Show: Enabled; Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	*Administrato*	BASIC	☑
guest	*Domain*	KEY	☑
mana...	*Domain*	KEY	☑
nxtad...	*DnsAdmins,*	KEY	☑
trevon	*Domain*	KEY	☑

Endpoints — Show: Verified; Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation	out-to-in	$DESTINATIONGROUP
front-desk	*Domain Computers*	
hafele	*Domain Computers*	
hafele-db	*Domain Computers,*	all-traffic
hafelebackend	*Domain Computers,*	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	*Domain Computers*	all-traffic
radius	*Domain Computers,*	all-traffic
remediantso	*Domain Computers,*	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups — Show: In Use; Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

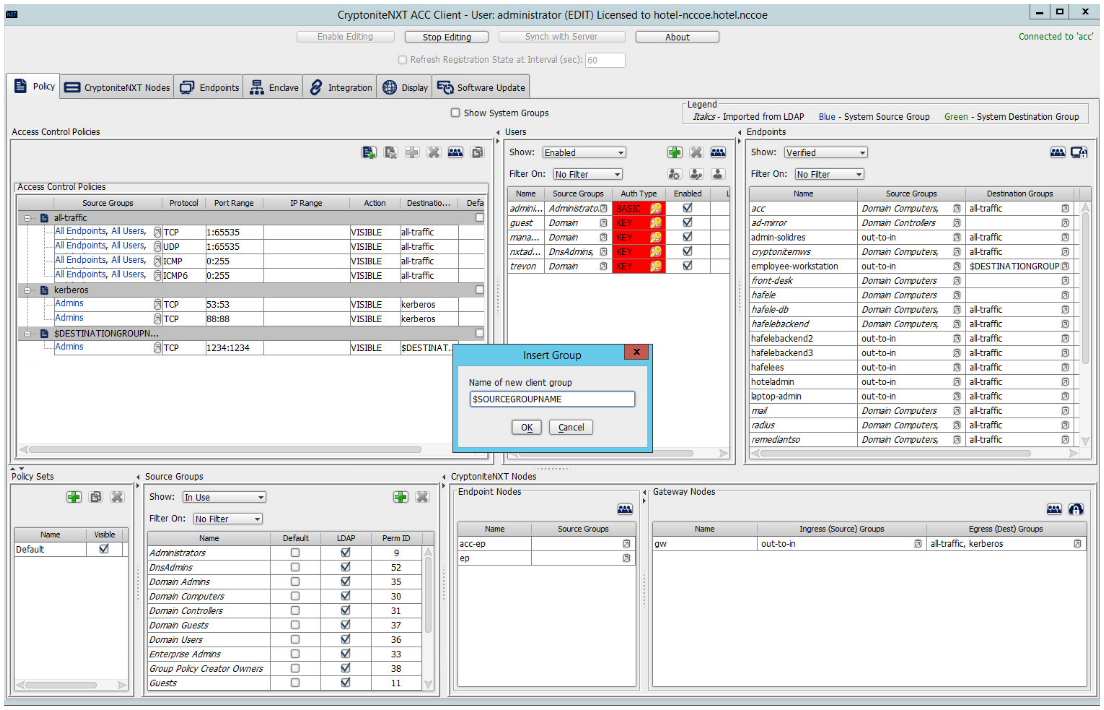
CryptoniteNXT Nodes — Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

3. Input the desired source group name:



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Insert Group

Name of new client group: $SOURCEGROUPNAME

Connected to 'acc'

☐ Refresh Registration State at Interval (sec): 60

☐ Show System Groups

Legend: *Italics* - Imported from LDAP Blue - System Source Group Green - System Destination Group

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							☐
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							☐
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							☐
	Admins	TCP	1234:1234		VISIBLE	$DESTINAT...	

Users — Show: Enabled; Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	*Administrato*	BASIC	☑
guest	*Domain*	KEY	☑
mana...	*Domain*	KEY	☑
nxtad...	*DnsAdmins,*	KEY	☑
trevon	*Domain*	KEY	☑

Endpoints — Show: Verified; Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation	out-to-in	$DESTINATIONGROUP
front-desk	*Domain Computers*	
hafele	*Domain Computers*	
hafele-db	*Domain Computers,*	all-traffic
hafelebackend	*Domain Computers,*	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	*Domain Computers*	all-traffic
radius	*Domain Computers,*	all-traffic
remediantso	*Domain Computers,*	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups — Show: In Use; Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

CryptoniteNXT Nodes — Endpoint Nodes

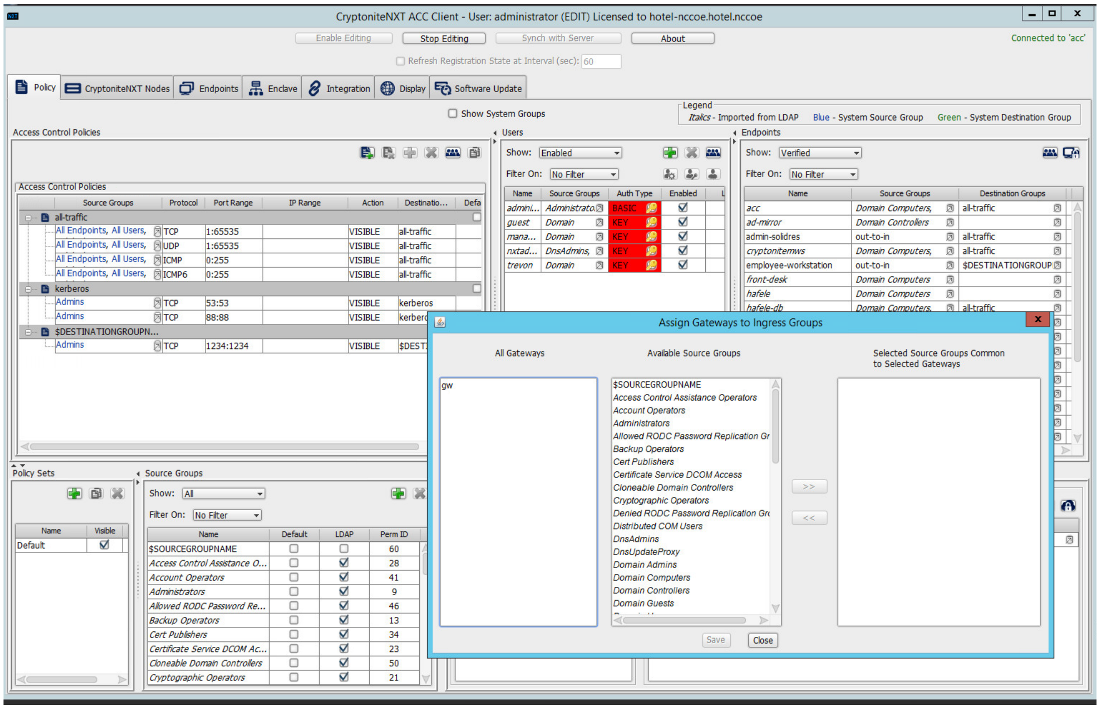
Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

4. Click **OK.**

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



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

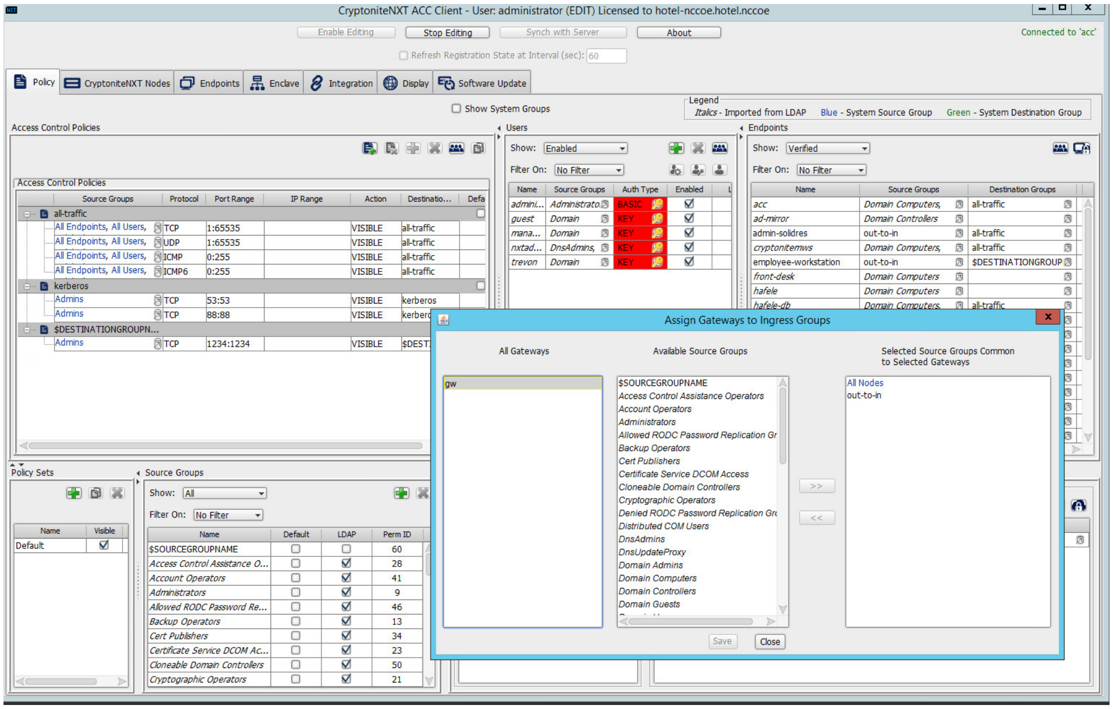
Assign Gateways to Ingress Groups

All Gateways
gw

Available Source Groups
$SOURCEGROUPNAME
Access Control Assistance Operators
Account Operators
Administrators
Allowed RODC Password Replication Gr
Backup Operators
Cert Publishers
Certificate Service DCOM Access
Cloneable Domain Controllers
Cryptographic Operators
Denied RODC Password Replication Gro
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests

Selected Source Groups Common to Selected Gateways

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



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

☐ Refresh Registration State at Interval (sec): 60

☐ Show System Groups

Legend: *Italics* - Imported from LDAP Blue - System Source Group Green - System Destination Group

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							☐
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							☐
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberc	
$DESTINATIONGROUPN...							
	Admins	TCP	1234:1234		VISIBLE	$DEST	

Users

Show: Enabled Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	*Administrato*	BASIC	☑
guest	*Domain*	KEY	☑
mana...	*Domain*	KEY	☑
nxtad...	*DnsAdmins,*	KEY	☑
trevon	*Domain*	KEY	☑

Endpoints

Show: Verified Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation	out-to-in	$DESTINATIONGROUP
front-desk	*Domain Computers*	
hafele	*Domain Computers*	
hafele-db	*Domain Computers,*	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: All Filter On: No Filter

Name	Default	LDAP	Perm ID
$SOURCEGROUPNAME	☐	☐	60
Access Control Assistance O...	☐	☑	28
Account Operators	☐	☑	41
Administrators	☐	☑	9
Allowed RODC Password Re...	☐	☑	46
Backup Operators	☐	☑	13
Cert Publishers	☐	☑	34
Certificate Service DCOM Ac...	☐	☑	23
Cloneable Domain Controllers	☐	☑	50
Cryptographic Operators	☐	☑	21

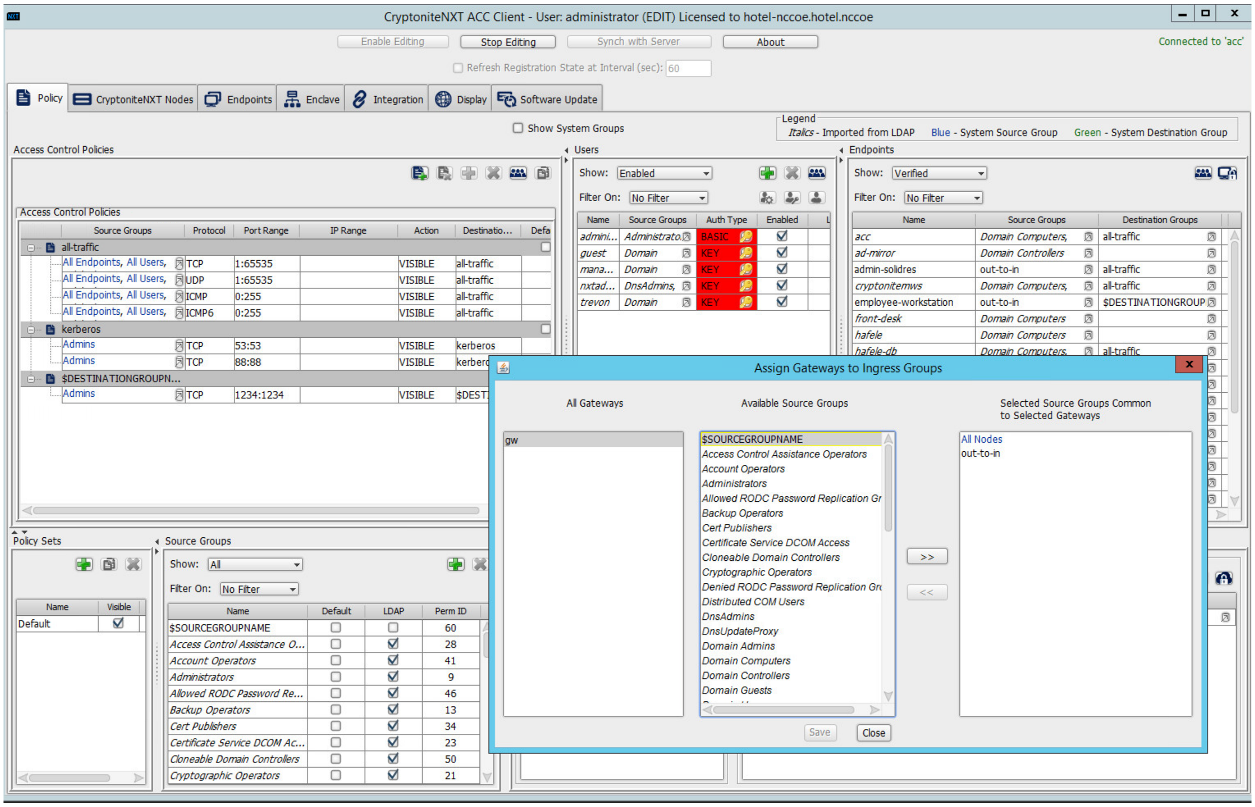
Assign Gateways to Ingress Groups

All Gateways:
gw

Available Source Groups:
$SOURCEGROUPNAME
Access Control Assistance Operators
Account Operators
Administrators
Allowed RODC Password Replication Gr
Backup Operators
Cert Publishers
Certificate Service DCOM Access
Cloneable Domain Controllers
Cryptographic Operators
Denied RODC Password Replication Gr
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests

Selected Source Groups Common to Selected Gateways:
All Nodes
out-to-in

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


CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe
Enable Editing
Stop Editing
Synch with Server
About
Connected to 'acc'
Refresh Registration State at Interval (sec): 60
Policy
CryptoniteNXT Nodes
Endpoints
Enclave
Integration
Display
Software Update
Show System Groups
Legend
Italics - Imported from LDAP
Blue - System Source Group
Green - System Destination Group

Access Control Policies

Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic						
All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos						
Admins	TCP	53:53		VISIBLE	kerberos	
Admins	TCP	88:88		VISIBLE	kerberc	
$DESTINATIONGROUPN...						
Admins	TCP	1234:1234		VISIBLE	$DEST	

Users

Show: Enabled

Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	Administrato...	BASIC	☑
guest	Domain	KEY	☑
mana...	Domain	KEY	☑
nxtad...	DnsAdmins,	KEY	☑
trevon	Domain	KEY	☑

Endpoints

Show: Verified

Filter On: No Filter

Name	Source Groups	Destination Groups
acc	Domain Computers,	all-traffic
ad-mirror	Domain Controllers	
admin-solidres	out-to-in	all-traffic
cryptonitemws	Domain Computers,	all-traffic
employee-workstation	out-to-in	$DESTINATIONGROUP
front-desk	Domain Computers	
hafele	Domain Computers	
hafele-db	Domain Computers,	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: All

Filter On: No Filter

Name	Default	LDAP	Perm ID
$SOURCEGROUPNAME	☐	☐	60
Access Control Assistance O...	☐	☑	28
Account Operators	☐	☑	41
Administrators	☐	☑	9
Allowed RODC Password Re...	☐	☑	46
Backup Operators	☐	☑	13
Cert Publishers	☐	☑	34
Certificate Service DCOM Ac...	☐	☑	23
Cloneable Domain Controllers	☐	☑	50
Cryptographic Operators	☐	☑	21

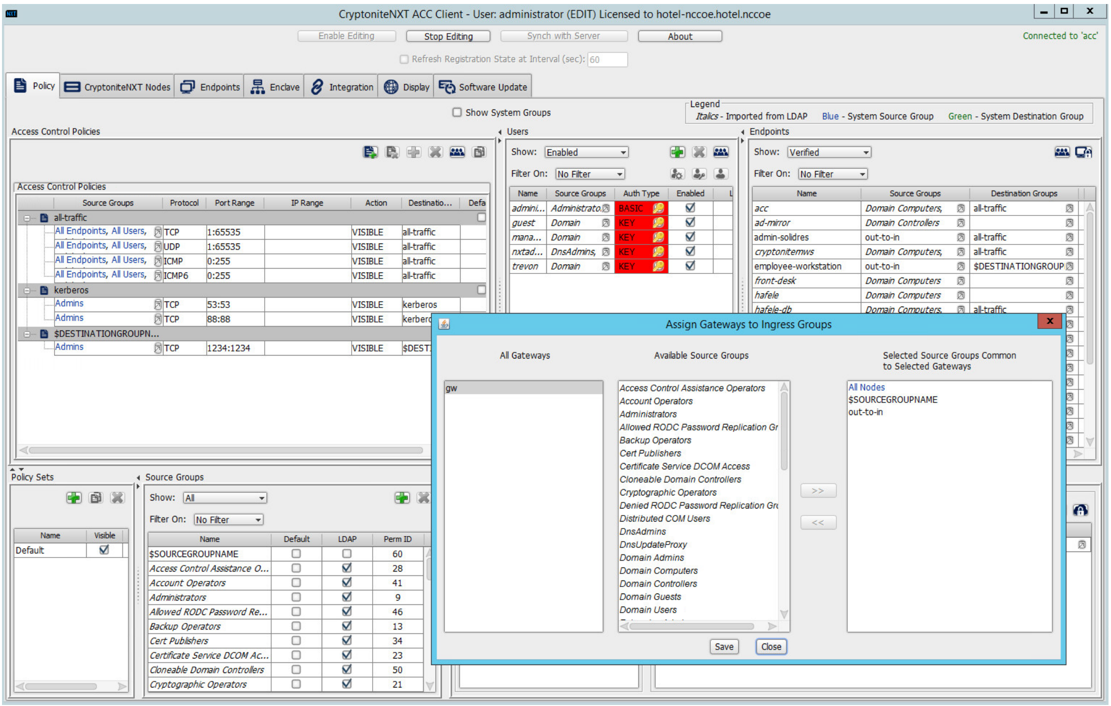
Assign Gateways to Ingress Groups

All Gateways:
gw

Available Source Groups:
$SOURCEGROUPNAME
Access Control Assistance Operators
Account Operators
Administrators
Allowed RODC Password Replication Gr
Backup Operators
Cert Publishers
Certificate Service DCOM Access
Cloneable Domain Controllers
Cryptographic Operators
Denied RODC Password Replication Gro
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests

Selected Source Groups Common to Selected Gateways:
All Nodes
out-to-in

8. Click **>>:**


CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe
Enable Editing
Stop Editing
Synch with Server
About
Connected to 'acc'
Refresh Registration State at Interval (sec): 60
Policy
CryptoniteNXT Nodes
Endpoints
Enclave
Integration
Display
Software Update
Show System Groups
Legend
Italics - Imported from LDAP
Blue - System Source Group
Green - System Destination Group
Access Control Policies
Users
Endpoints
Policy Sets
Source Groups
Assign Gateways to Ingress Groups
All Gateways
Available Source Groups
Selected Source Groups Common to Selected Gateways
>>
<<
Save
Close

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							□
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							□
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberc	
$DESTINATIONGROUPN...							
	Admins	TCP	1234:1234		VISIBLE	$DESTI	

Users — Show: Enabled; Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	*Administrato*	BASIC	☑
guest	*Domain*	KEY	☑
mana...	*Domain*	KEY	☑
nxtad...	*DnsAdmins,*	KEY	☑
trevon	*Domain*	KEY	☑

Endpoints — Show: Verified; Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation	out-to-in	$DESTINATIONGROUP
front-desk	*Domain Computers*	
hafele	*Domain Computers*	
hafele-db	*Domain Computers,*	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups — Show: All; Filter On: No Filter

Name	Default	LDAP	Perm ID
$SOURCEGROUPNAME	□	□	60
Access Control Assistance O...	□	☑	28
Account Operators	□	☑	41
Administrators	□	☑	9
Allowed RODC Password Re...	□	☑	46
Backup Operators	□	☑	13
Cert Publishers	□	☑	34
Certificate Service DCOM Ac...	□	☑	23
Cloneable Domain Controllers	□	☑	50
Cryptographic Operators	□	☑	21

Assign Gateways to Ingress Groups

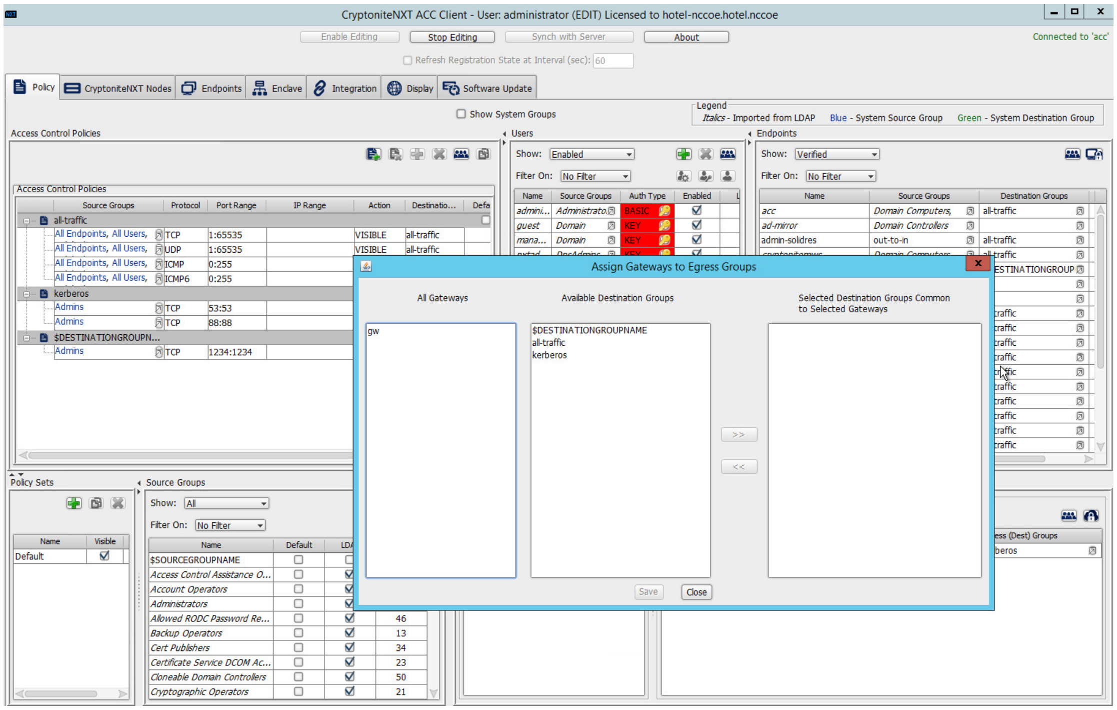
All Gateways:
gw

Available Source Groups:
Access Control Assistance Operators
Account Operators
Administrators
Allowed RODC Password Replication Gr
Backup Operators
Cert Publishers
Certificate Service DCOM Access
Cloneable Domain Controllers
Cryptographic Operators
Denied RODC Password Replication Gr
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users

Selected Source Groups Common to Selected Gateways:
All Nodes
$SOURCEGROUPNAME
out-to-in

9. Click **Save.**

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



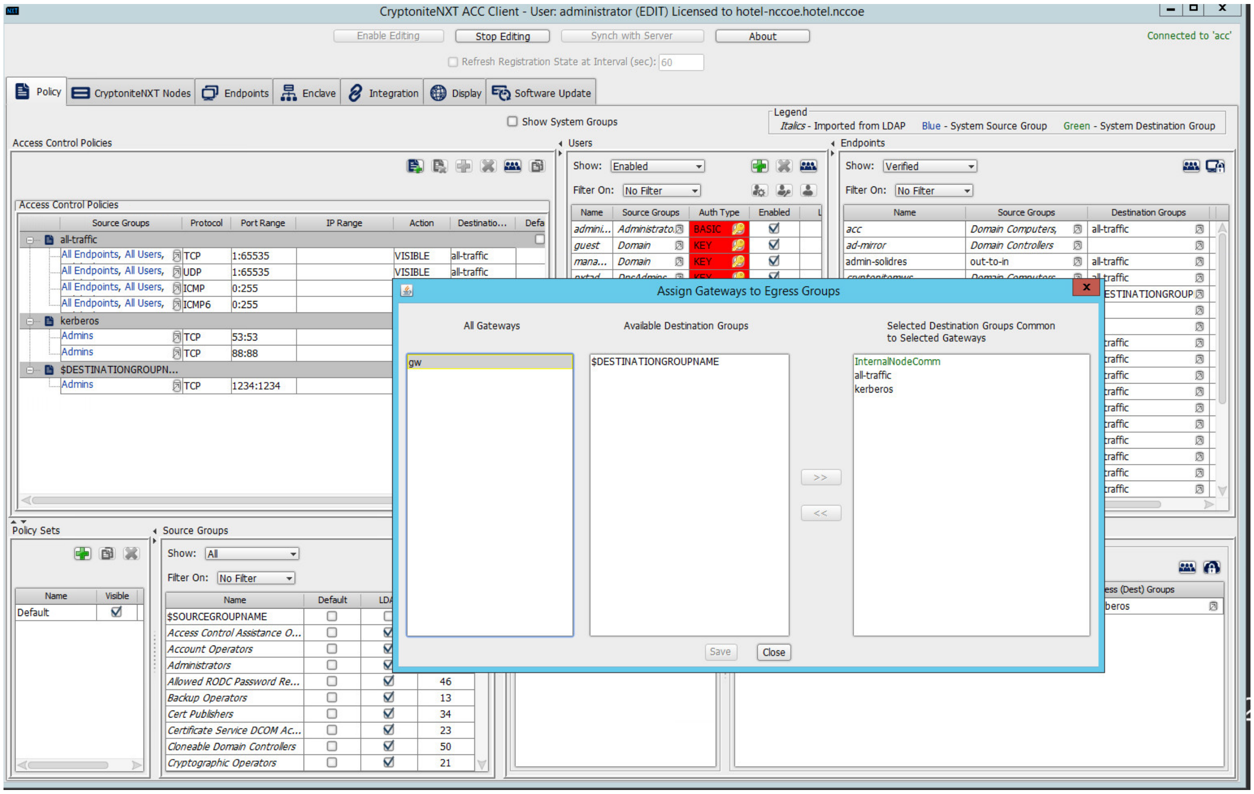
CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

Assign Gateways to Egress Groups

All Gateways	Available Destination Groups	Selected Destination Groups Common to Selected Gateways
gw	$DESTINATIONGROUPNAME all-traffic kerberos	

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



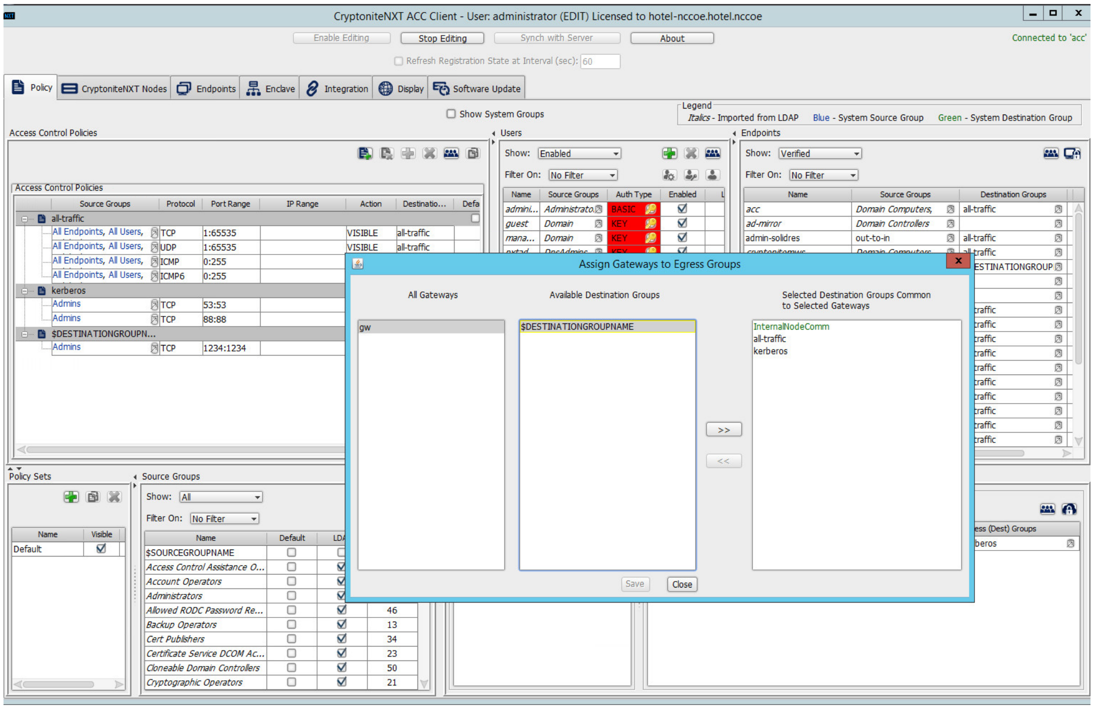
CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

Assign Gateways to Egress Groups

All Gateways	Available Destination Groups	Selected Destination Groups Common to Selected Gateways
gw	$DESTINATIONGROUPNAME	InternalNodeComm all-traffic kerberos

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

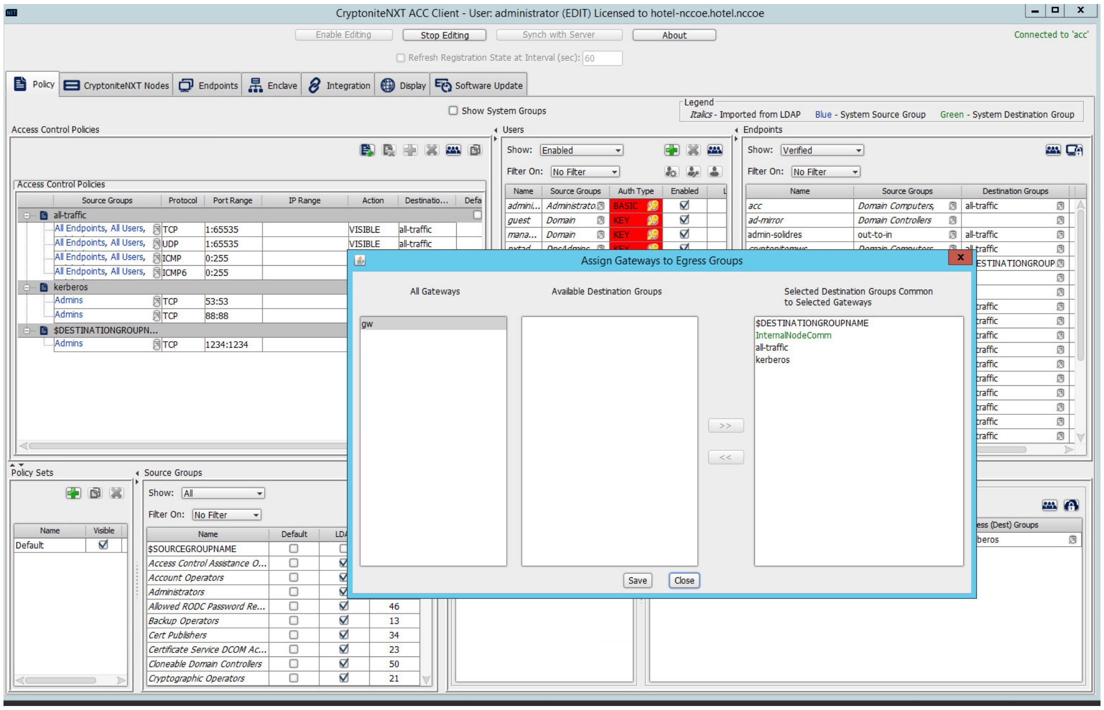

CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe
Enable Editing
Stop Editing
Synch with Server
About
Connected to 'acc'
Policy
CryptoniteNXT Nodes
Endpoints
Enclave
Integration
Display
Software Update
Assign Gateways to Egress Groups
All Gateways
Available Destination Groups
Selected Destination Groups Common to Selected Gateways
>>
<<
Save
Close

All Gateways: gw

Available Destination Groups: $DESTINATIONGROUPNAME

Selected Destination Groups Common to Selected Gateways:
InternalNodeComm
all-traffic
kerberos

13. Click **>>**:


CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe
Enable Editing
Stop Editing
Synch with Server
About
Connected to 'acc'
Policy
CryptoniteNXT Nodes
Endpoints
Enclave
Integration
Display
Software Update
Assign Gateways to Egress Groups
All Gateways
Available Destination Groups
Selected Destination Groups Common to Selected Gateways
>>
<<
Save
Close

All Gateways: gw

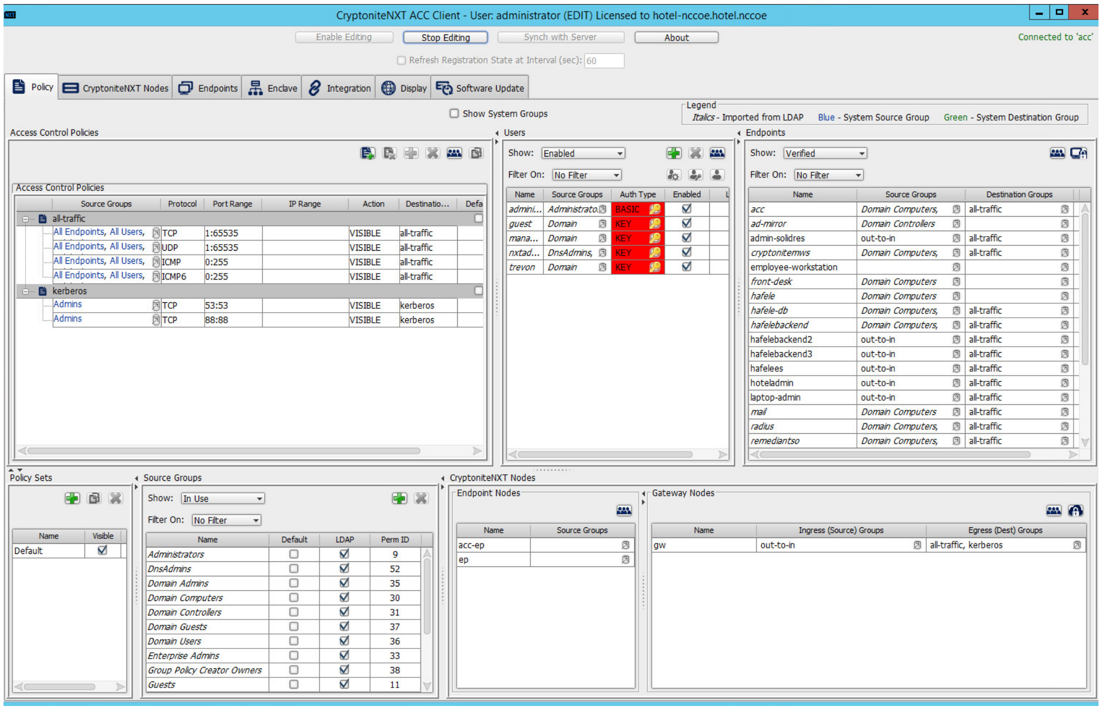
Selected Destination Groups Common to Selected Gateways:
$DESTINATIONGROUPNAME
InternalNodeComm
all-traffic
kerberos

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:**



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

□ Refresh Registration State at Interval (sec): 60

□ Show System Groups

Legend: *Italics* - Imported from LDAP Blue - System Source Group Green - System Destination Group

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							□
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							□
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	

Users

Show: Enabled
Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	*Administrato...*	BASIC	☑
guest	*Domain*	KEY	☑
mana...	*Domain*	KEY	☑
nxtad...	*DnsAdmins,*	KEY	☑
trevon	*Domain*	KEY	☑

Endpoints

Show: Verified
Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation		
front-desk	*Domain Computers*	
hafele	*Domain Computers*	
hafele-db	*Domain Computers,*	all-traffic
hafelebackend	*Domain Computers,*	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	*Domain Computers*	all-traffic
radius	*Domain Computers,*	all-traffic
remediantso	*Domain Computers,*	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use
Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	□	☑	9
DnsAdmins	□	☑	52
Domain Admins	□	☑	35
Domain Computers	□	☑	30
Domain Controllers	□	☑	31
Domain Guests	□	☑	37
Domain Users	□	☑	36
Enterprise Admins	□	☑	33
Group Policy Creator Owners	□	☑	38
Guests	□	☑	11

CryptoniteNXT Nodes

Endpoint Nodes

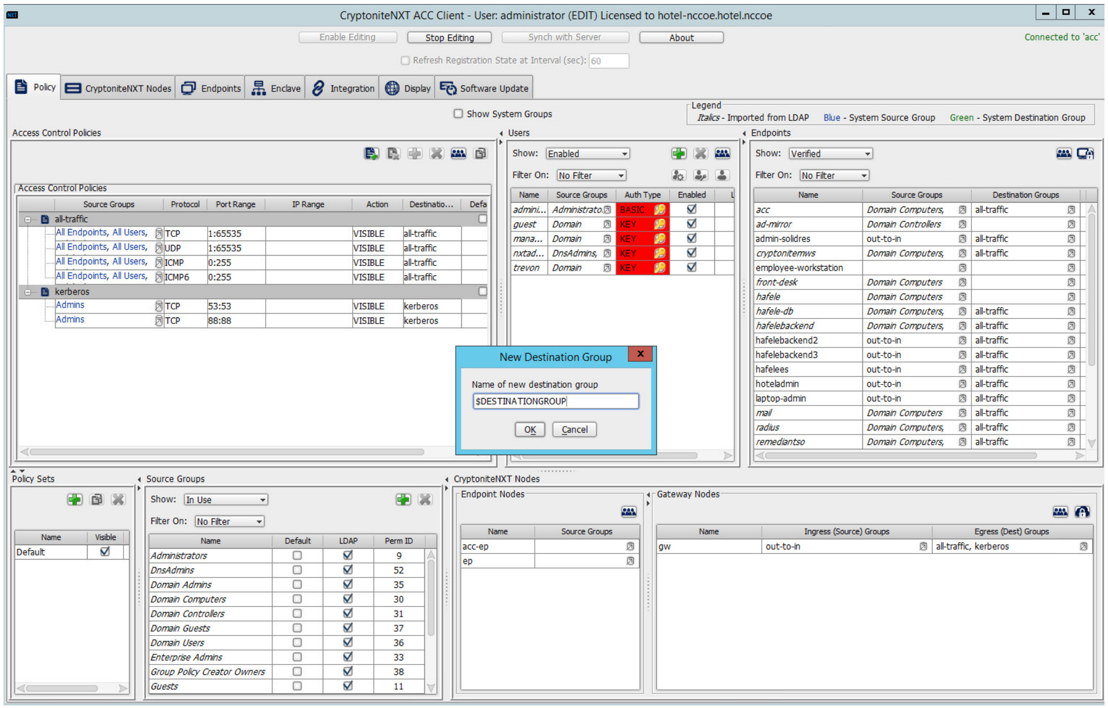
Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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:



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

□ Refresh Registration State at Interval (sec): 60

□ Show System Groups

Legend: *Italics* - Imported from LDAP; Blue - System Source Group; Green - System Destination Group

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							□
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							□
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	

Users

Show: Enabled
Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	*Administrato...*	BASIC	☑
guest	*Domain*	KEY	☑
mana...	*Domain*	KEY	☑
nxtad...	*DnsAdmins,*	KEY	☑
trevon	*Domain*	KEY	☑

Endpoints

Show: Verified
Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation		
front-desk	*Domain Computers*	
hafele	*Domain Computers*	
hafele-db	*Domain Computers,*	all-traffic
hafelebackend	*Domain Computers,*	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	*Domain Computers*	all-traffic
radius	*Domain Computers,*	all-traffic
remediantso	*Domain Computers,*	all-traffic

New Destination Group

Name of new destination group: $DESTINATIONGROUP

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use
Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	□	☑	9
DnsAdmins	□	☑	52
Domain Admins	□	☑	35
Domain Computers	□	☑	30
Domain Controllers	□	☑	31
Domain Guests	□	☑	37
Domain Users	□	☑	36
Enterprise Admins	□	☑	33
Group Policy Creator Owners	□	☑	38
Guests	□	☑	11

CryptoniteNXT Nodes

Endpoint Nodes

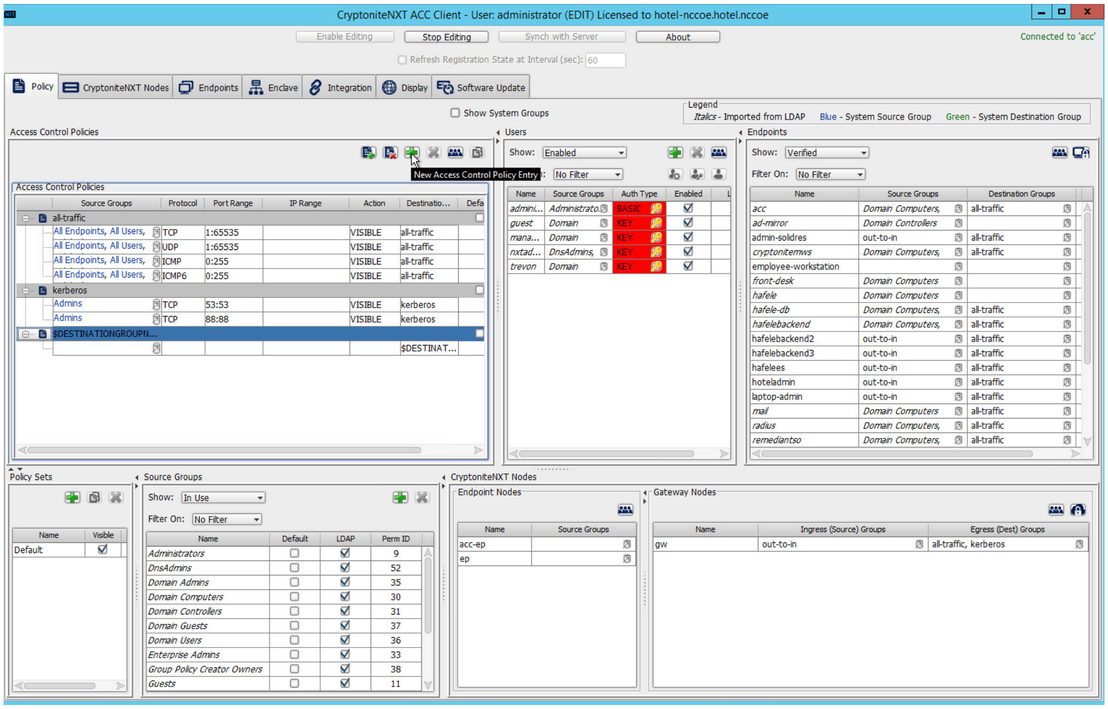
Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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):



Access Control Policies

Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic						☐
All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos						☐
Admins	TCP	53:53		VISIBLE	kerberos	
Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...						☐
					$DESTINAT...	

Users

Name	Source Groups	Auth Type	Enabled
admini...	Administrato...	BASIC	☑
guest	Domain	KEY	☑
mana...	Domain	KEY	☑
nxtad...	DnsAdmins,	KEY	☑
trevon	Domain	KEY	☑

Endpoints

Name	Source Groups	Destination Groups
acc	Domain Computers,	all-traffic
ad-mirror	Domain Controllers	
admin-solidres	out-to-in	all-traffic
cryptonitemws	Domain Computers,	all-traffic
employee-workstation		
front-desk	Domain Computers	
hafele	Domain Computers	
hafele-db	Domain Computers,	all-traffic
hafelebackend	Domain Computers,	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	Domain Computers	all-traffic
radius	Domain Computers,	all-traffic
remediantso	Domain Computers,	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

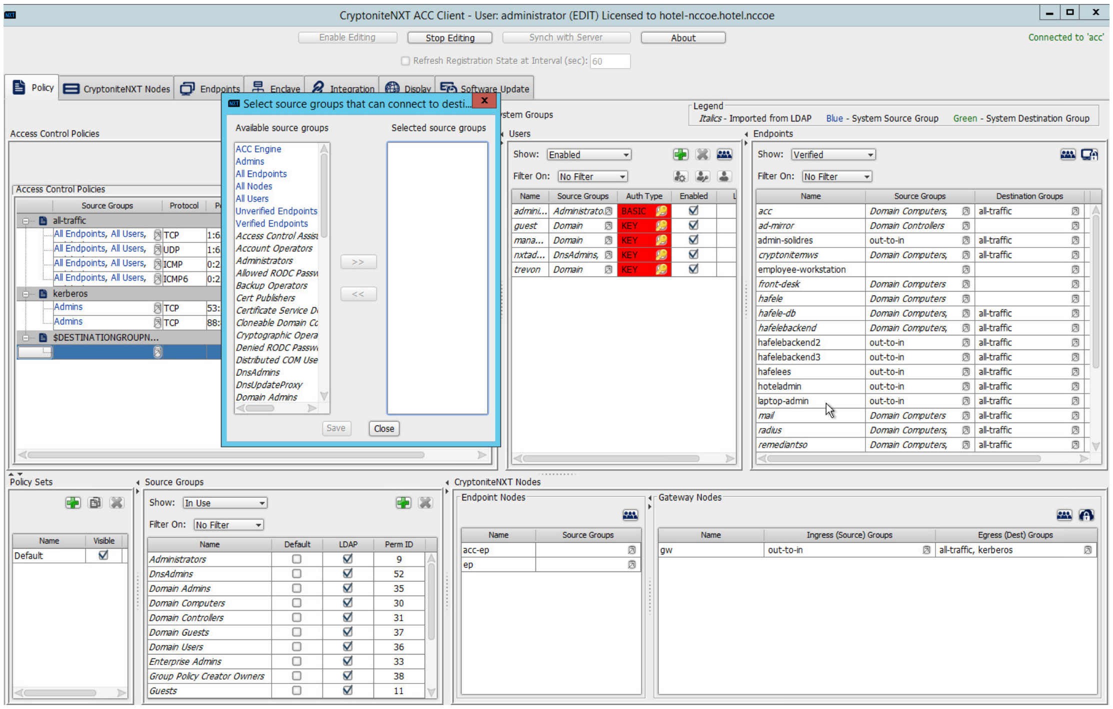
Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

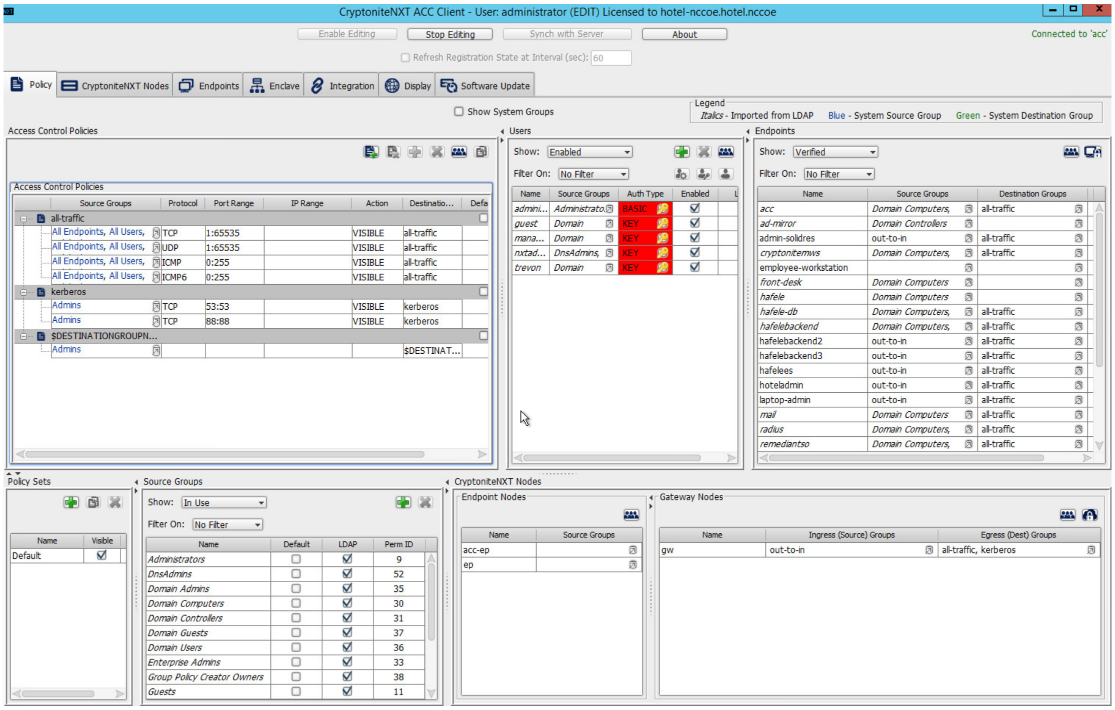
6. Click the small arrow icon in the **Source Groups** cell of the empty row (hover text: Click the arrow button to view/edit the source groups):


CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe
Enable Editing
Stop Editing
Synch with Server
About
Connected to 'acc'
Refresh Registration State at Interval (sec): 60
Select source groups that can connect to desti...
Available source groups
Selected source groups
>>
<<
Save
Close

Available source groups

- ACC Engine
- Admins
- All Endpoints
- All Nodes
- All Users
- Unverified Endpoints
- Verified Endpoints
- Access Control Assis
- Account Operators
- Administrators
- Allowed RODC Passw
- Backup Operators
- Cert Publishers
- Certificate Service D
- Cloneable Domain C
- Cryptographic Opera
- Denied RODC Passw
- Distributed COM Use
- DnsAdmins
- DnsUpdateProxy
- Domain Admins

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



☐ Refresh Registration State at Interval (sec): 60

☐ Show System Groups

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							☐
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							☐
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							☐
	Admins					$DESTINAT...	

Users — Show: Enabled; Filter On: No Filter

Name	Source Groups	Auth Type	Enabled	L
admini...	*Administrato.*	BASIC	☑	
guest	*Domain*	KEY	☑	
mana...	*Domain*	KEY	☑	
nxtad...	*DnsAdmins,*	KEY	☑	
trevon	*Domain*	KEY	☑	

Endpoints — Show: Verified; Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation		
front-desk	*Domain Computers*	
hafele	*Domain Computers*	
hafele-db	*Domain Computers,*	all-traffic
hafelebackend	*Domain Computers,*	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	*Domain Computers*	all-traffic
radius	*Domain Computers,*	all-traffic
remediantso	*Domain Computers,*	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups — Show: In Use; Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

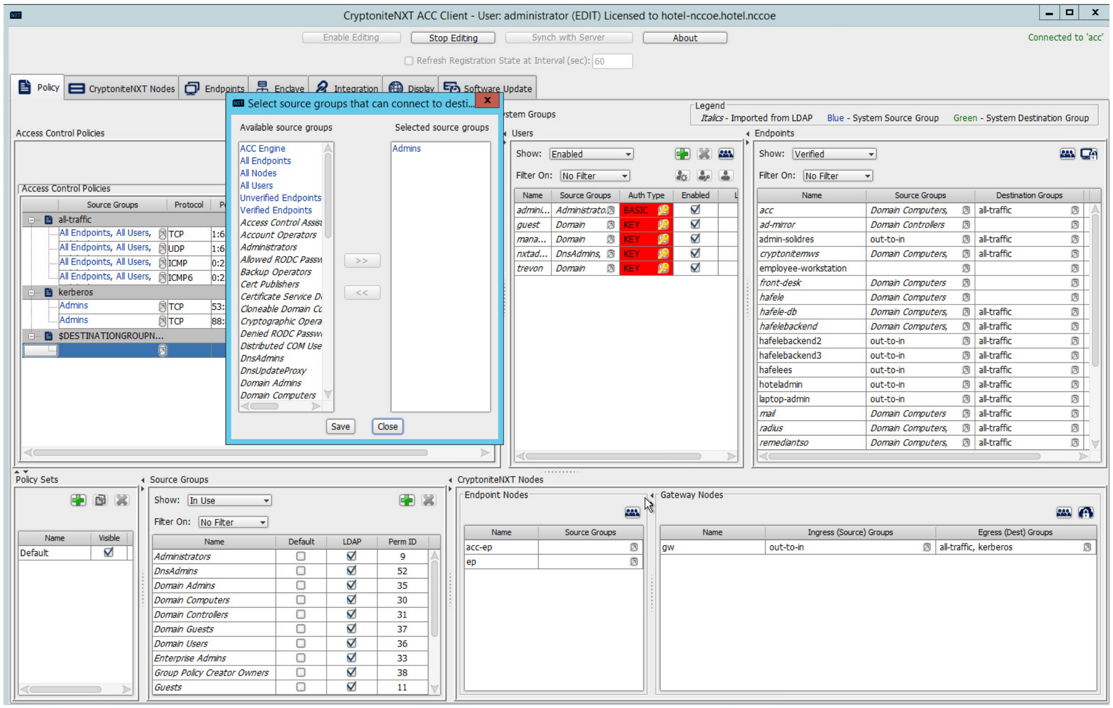
Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

8. Click **Save:**



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

☐ Refresh Registration State at Interval (sec): 60

Select source groups that can connect to desti...

Available source groups	Selected source groups
ACC Engine All Endpoints All Nodes All Users Unverified Endpoints Verified Endpoints *Access Control Assis* *Account Operators* *Administrators* *Allowed RODC Passw* *Backup Operators* *Cert Publishers* *Certificate Service D* *Cloneable Domain Co* *Cryptographic Opera* *Denied RODC Passw* *Distributed COM Use* *DnsAdmins* *DnsUpdateProxy* *Domain Admins* *Domain Computers*	Admins

Access Control Policies

	Source Groups	Protocol	P
all-traffic			
	All Endpoints, All Users,	TCP	1:6
	All Endpoints, All Users,	UDP	1:6
	All Endpoints, All Users,	ICMP	0:2
	All Endpoints, All Users,	ICMP6	0:2
kerberos			
	Admins	TCP	53:
	Admins	TCP	88:
$DESTINATIONGROUPN...			

Legend: *Italics* - Imported from LDAP   Blue - System Source Group   Green - System Destination Group

Users

Show: Enabled   Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	*Administrato*	BASIC	☑
guest	*Domain*	KEY	☑
mana...	*Domain*	KEY	☑
nxtad...	*DnsAdmins,*	KEY	☑
trevon	*Domain*	KEY	☑

Endpoints

Show: Verified   Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation		
front-desk	*Domain Computers*	
hafele	*Domain Computers*	
hafele-db	*Domain Computers,*	all-traffic
hafelebackend	*Domain Computers,*	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	*Domain Computers*	all-traffic
radius	*Domain Computers,*	all-traffic
remediantso	*Domain Computers,*	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use   Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

CryptoniteNXT Nodes

Endpoint Nodes

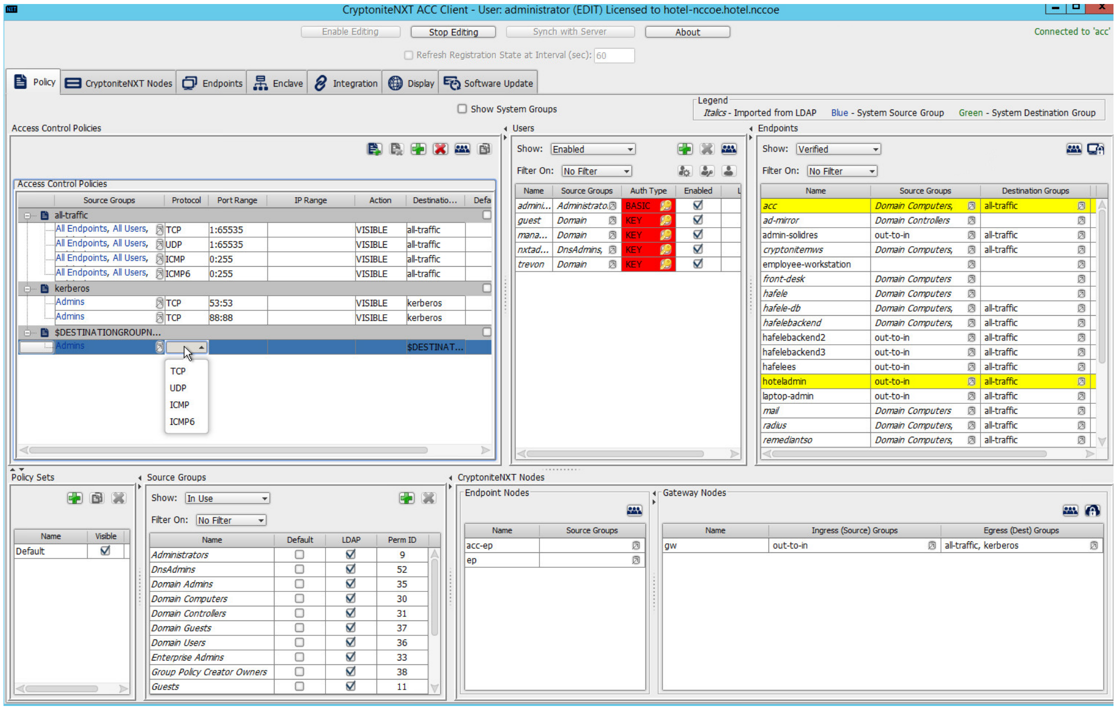
Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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

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



☐ Refresh Registration State at Interval (sec): 60

☐ Show System Groups

Legend: *Italics* - Imported from LDAP   Blue - System Source Group   Green - System Destination Group

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							☐
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							☐
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							☐
	Admins					$DESTINAT...	

Users — Show: Enabled; Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	*Administrato...*	BASIC	☑
guest	*Domain*	KEY	☑
mana...	*Domain*	KEY	☑
nxtad...	*DnsAdmins,*	KEY	☑
trevon	*Domain*	KEY	☑

Endpoints — Show: Verified; Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation		
front-desk	*Domain Computers*	
hafele	*Domain Computers*	
hafele-db	*Domain Computers,*	all-traffic
hafelebackend	*Domain Computers,*	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	*Domain Computers*	all-traffic
radius	*Domain Computers,*	all-traffic
remediantso	*Domain Computers,*	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups — Show: In Use; Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

Endpoint Nodes

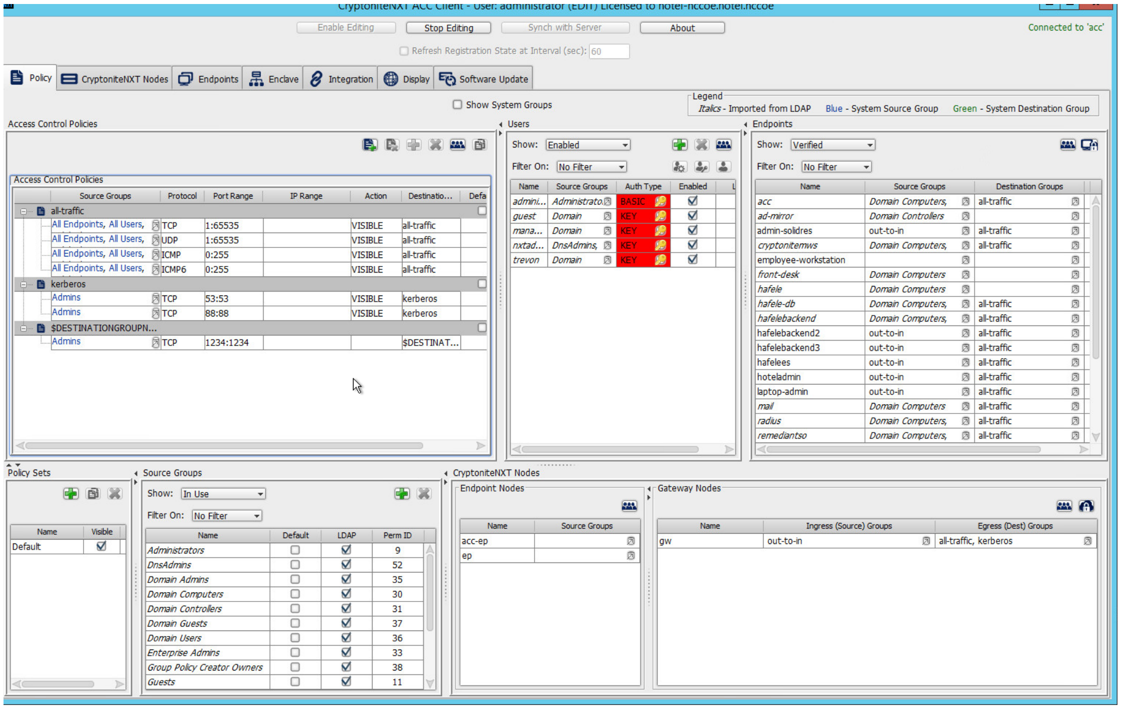
Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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

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



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe
Enable Editing
Stop Editing
Synch with Server
About
Connected to 'acc'
□ Refresh Registration State at Interval (sec): 60
Policy
CryptoniteNXT Nodes
Endpoints
Enclave
Integration
Display
Software Update
□ Show System Groups
Legend
Italics - Imported from LDAP
Blue - System Source Group
Green - System Destination Group

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							□
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							□
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							□
	Admins	TCP	1234:1234			$DESTINAT...	

Users

Show: Enabled

Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	Administrato...	BASIC	☑
guest	Domain	KEY	☑
mana...	Domain	KEY	☑
nxtad...	DnsAdmins,	KEY	☑
trevon	Domain	KEY	☑

Endpoints

Show: Verified

Filter On: No Filter

Name	Source Groups	Destination Groups
acc	Domain Computers,	all-traffic
ad-mirror	Domain Controllers	
admin-solidres	out-to-in	all-traffic
cryptonitemws	Domain Computers,	all-traffic
employee-workstation		
front-desk	Domain Computers	
hafele	Domain Computers	
hafele-db	Domain Computers,	all-traffic
hafelebackend	Domain Computers,	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	Domain Computers	all-traffic
radius	Domain Computers,	all-traffic
remediantso	Domain Computers,	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use

Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	□	☑	9
DnsAdmins	□	☑	52
Domain Admins	□	☑	35
Domain Computers	□	☑	30
Domain Controllers	□	☑	31
Domain Guests	□	☑	37
Domain Users	□	☑	36
Enterprise Admins	□	☑	33
Group Policy Creator Owners	□	☑	38
Guests	□	☑	11

CryptoniteNXT Nodes

Endpoint Nodes

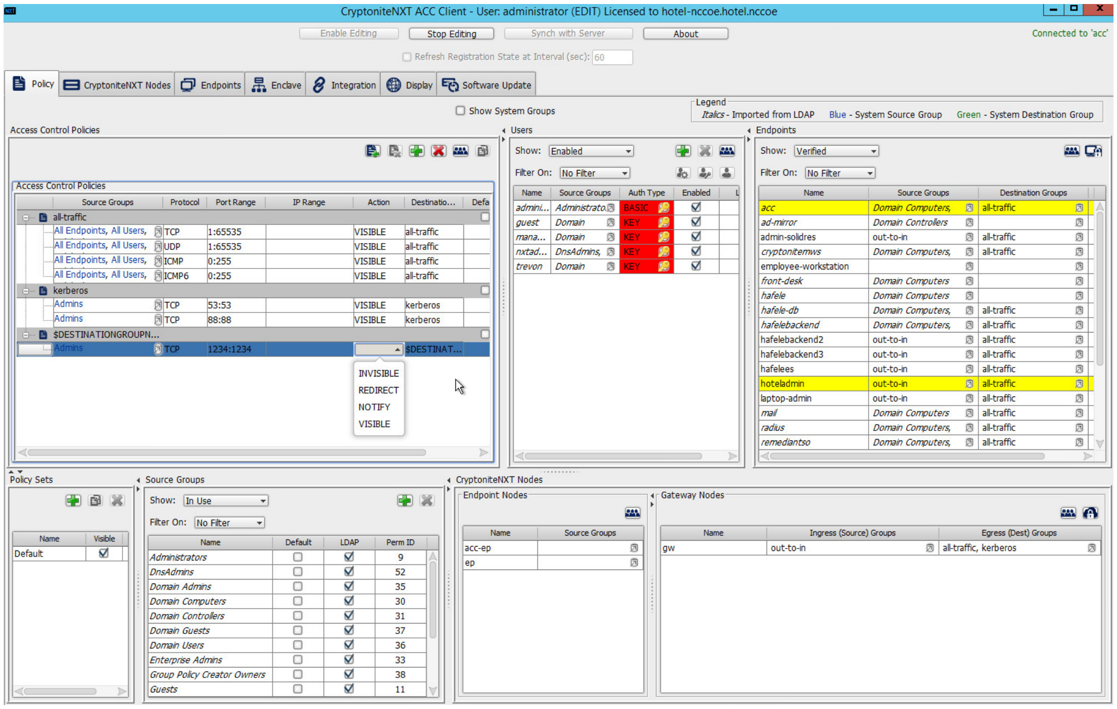
Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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

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


CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe
Enable Editing
Stop Editing
Synch with Server
About
Connected to 'acc'
☐ Refresh Registration State at Interval (sec): 60
Policy
CryptoniteNXT Nodes
Endpoints
Enclave
Integration
Display
Software Update
☐ Show System Groups
Legend
Italics - Imported from LDAP
Blue - System Source Group
Green - System Destination Group
INVISIBLE
REDIRECT
NOTIFY
VISIBLE

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							☐
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							☐
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							☐
	Admins	TCP	1234:1234			$DESTINAT...	

Users

Show: Enabled

Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	*Administrato.*	BASIC	☑
guest	*Domain*	KEY	☑
mana...	*Domain*	KEY	☑
nxtad...	*DnsAdmins,*	KEY	☑
trevon	*Domain*	KEY	☑

Endpoints

Show: Verified

Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation		
front-desk	*Domain Computers*	
hafele	*Domain Computers*	
hafele-db	*Domain Computers,*	all-traffic
hafelebackend	*Domain Computers,*	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	*Domain Computers*	all-traffic
radius	*Domain Computers,*	all-traffic
remediantso	*Domain Computers,*	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use

Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

CryptoniteNXT Nodes

Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

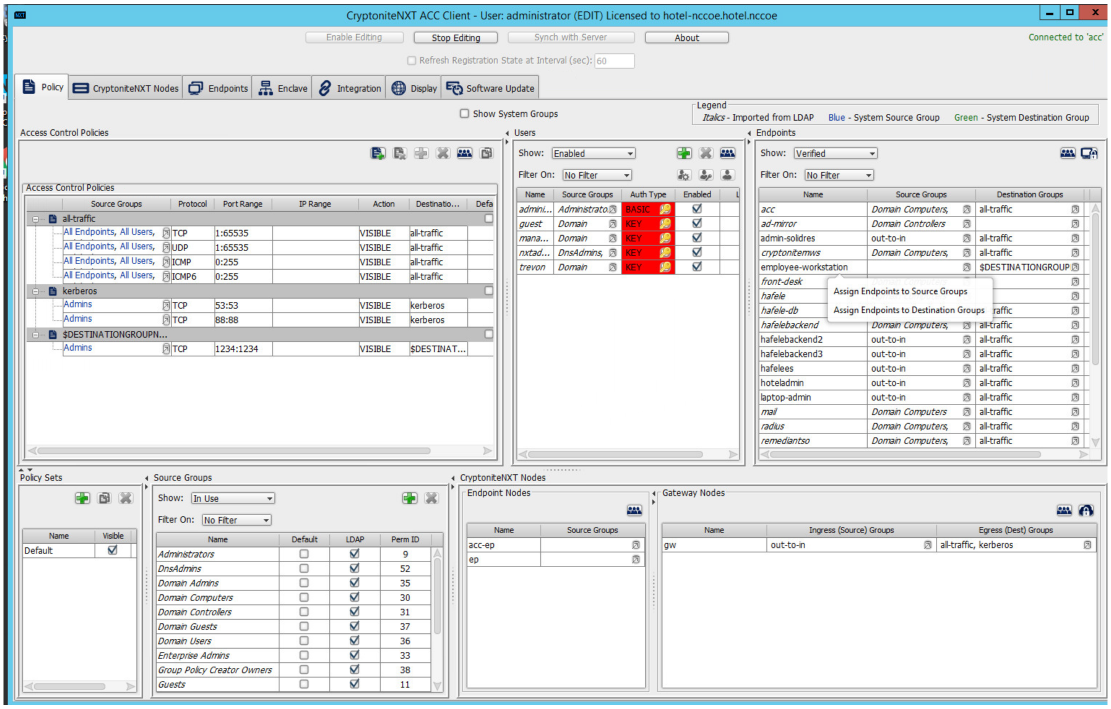
15. Set **Action** to VISIBLE to allow traffic of the described type; use INVISIBLE to block traffic of this type.

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:



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

Refresh Registration State at Interval (sec): 60

□ Show System Groups

Legend: *Italics* - Imported from LDAP   Blue - System Source Group   Green - System Destination Group

Access Control Policies

Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic						□
All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos						□
Admins	TCP	53:53		VISIBLE	kerberos	
Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...						□
Admins	TCP	1234:1234		VISIBLE	$DESTINAT...	

Users — Show: Enabled Filter On: No Filter

Name	Source Groups	Auth Type	Enabled
admini...	*Administrato*	BASIC	☑
guest	*Domain*	KEY	☑
mana...	*Domain*	KEY	☑
nxtad...	*DnsAdmins,*	KEY	☑
trevon	*Domain*	KEY	☑

Endpoints — Show: Verified Filter On: No Filter

Name	Source Groups	Destination Groups
acc	*Domain Computers,*	all-traffic
ad-mirror	*Domain Controllers*	
admin-solidres	out-to-in	all-traffic
cryptonitemws	*Domain Computers,*	all-traffic
employee-workstation		$DESTINATIONGROUP
front-desk		
hafele		
hafele-db		raffic
hafelebackend	*Domain Computers,*	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	*Domain Computers*	all-traffic
radius	*Domain Computers,*	all-traffic
remediantso	*Domain Computers,*	all-traffic

Assign Endpoints to Source Groups
Assign Endpoints to Destination Groups

Policy Sets

Name	Visible
Default	☑

Source Groups — Show: In Use Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	□	☑	9
DnsAdmins	□	☑	52
Domain Admins	□	☑	35
Domain Computers	□	☑	30
Domain Controllers	□	☑	31
Domain Guests	□	☑	37
Domain Users	□	☑	36
Enterprise Admins	□	☑	33
Group Policy Creator Owners	□	☑	38
Guests	□	☑	11

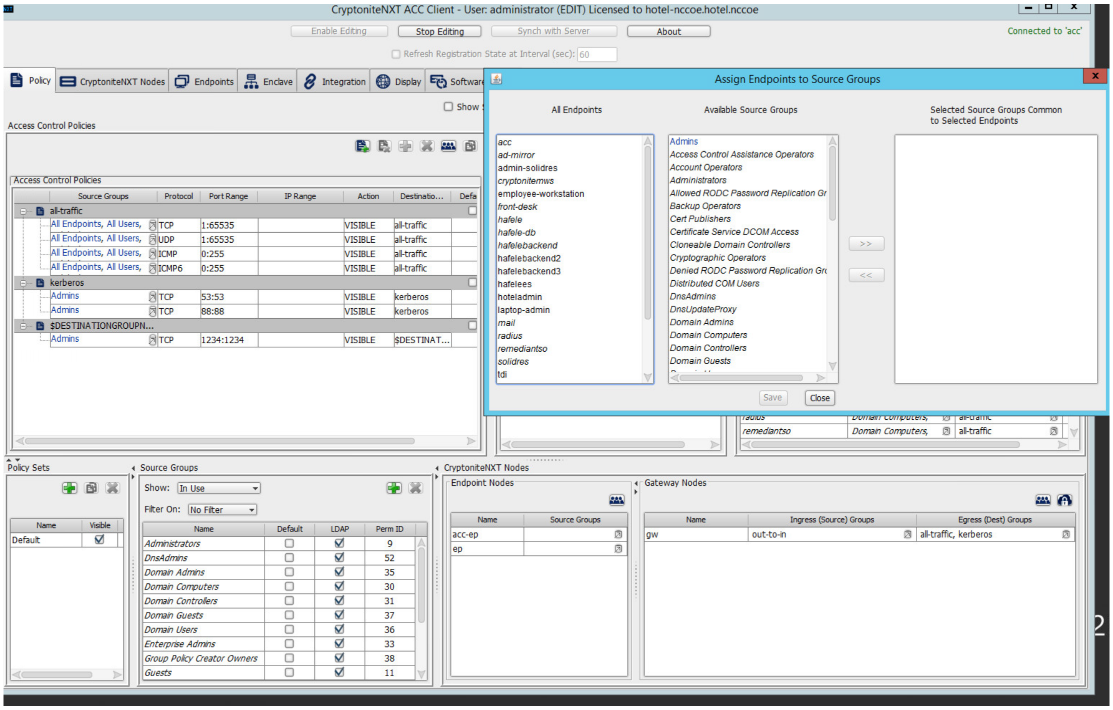
CryptoniteNXT Nodes — Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

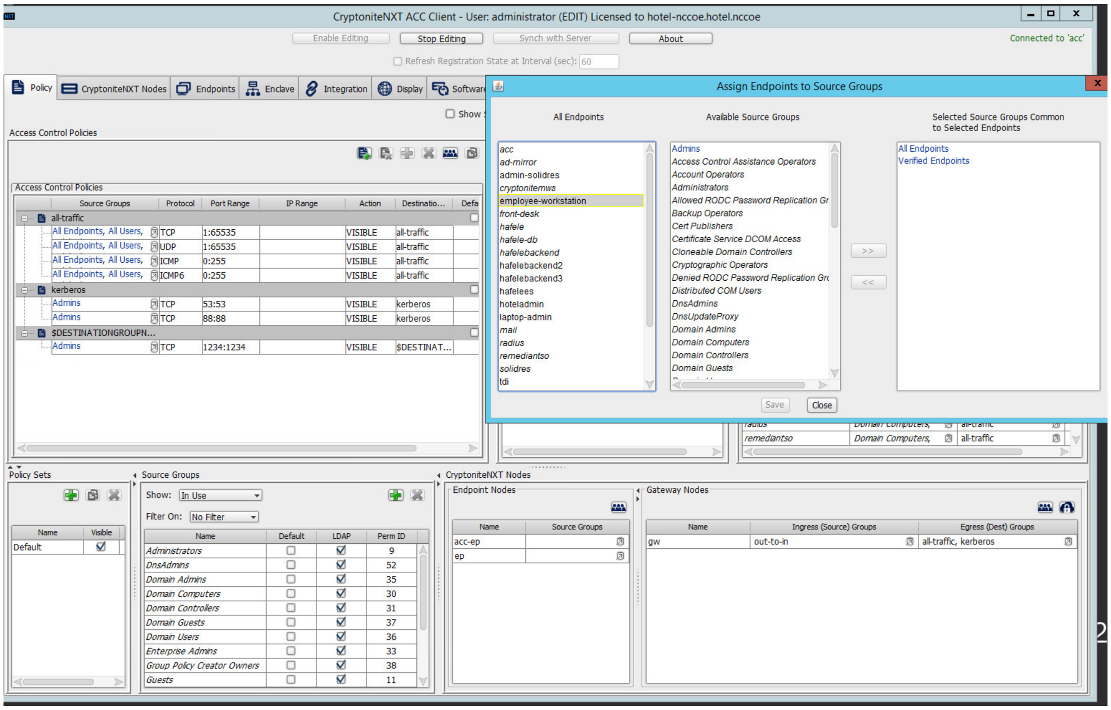
3. Select **Assign Endpoints to Source Groups:**



Assign Endpoints to Source Groups

All Endpoints	Available Source Groups	Selected Source Groups Common to Selected Endpoints
acc *ad-mirror* admin-solidres *cryptonitemws* employee-workstation *front-desk* *hafele* *hafele-db* *hafelebackend* hafelebackend2 hafelebackend3 hafelees hoteladmin laptop-admin *mail* *radius* *remediantso* *solidres* tdi	Admins *Access Control Assistance Operators* *Account Operators* *Administrators* *Allowed RODC Password Replication Gr* *Backup Operators* *Cert Publishers* *Certificate Service DCOM Access* *Cloneable Domain Controllers* *Cryptographic Operators* *Denied RODC Password Replication Gr* *Distributed COM Users* *DnsAdmins* *DnsUpdateProxy* *Domain Admins* *Domain Computers* *Domain Controllers* *Domain Guests*	

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



□ Refresh Registration State at Interval (sec): 60

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							□
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							□
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							□
	Admins	TCP	1234:1234		VISIBLE	$DESTINAT...	

All Endpoints

acc
ad-mirror
admin-solidres
cryptonitemws
employee-workstation
front-desk
hafele
hafele-db
hafelebackend
hafelebackend2
hafelebackend3
hafelees
hoteladmin
laptop-admin
mail
radius
remediantso
solidres
tdi

Available Source Groups

Admins
Access Control Assistance Operators
Account Operators
Administrators
Allowed RODC Password Replication Gr
Backup Operators
Cert Publishers
Certificate Service DCOM Access
Cloneable Domain Controllers
Cryptographic Operators
Denied RODC Password Replication Gr
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests

Selected Source Groups Common to Selected Endpoints

All Endpoints
Verified Endpoints

remediantso	Domain Computers,	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use

Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	□	☑	9
DnsAdmins	□	☑	52
Domain Admins	□	☑	35
Domain Computers	□	☑	30
Domain Controllers	□	☑	31
Domain Guests	□	☑	37
Domain Users	□	☑	36
Enterprise Admins	□	☑	33
Group Policy Creator Owners	□	☑	38
Guests	□	☑	11

CryptoniteNXT Nodes

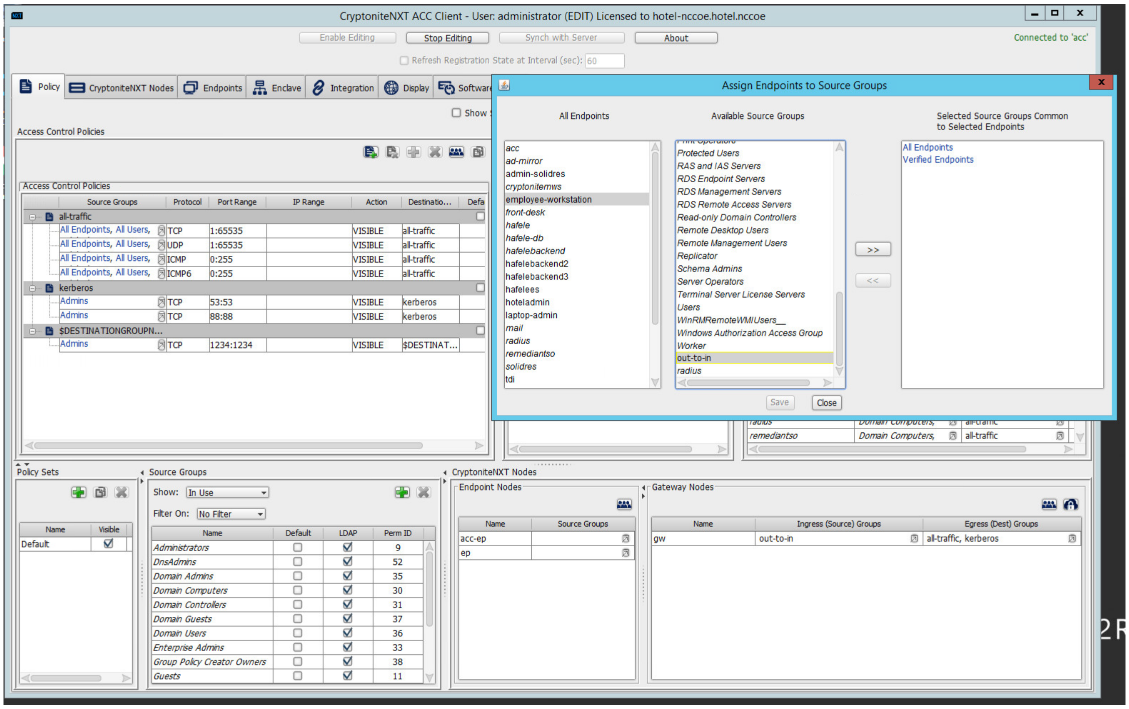
Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

☐ Refresh Registration State at Interval (sec): 60

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							☐
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							☐
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							☐
	Admins	TCP	1234:1234		VISIBLE	$DESTINAT...	

Assign Endpoints to Source Groups

All Endpoints: acc, ad-mirror, admin-solidres, cryptonitemws, employee-workstation, front-desk, hafele, hafele-db, hafelebackend, hafelebackend2, hafelebackend3, hafelees, hoteladmin, laptop-admin, mail, radius, remediantso, solidres, tdi

Available Source Groups: Print Operators, Protected Users, RAS and IAS Servers, RDS Endpoint Servers, RDS Management Servers, RDS Remote Access Servers, Read-only Domain Controllers, Remote Desktop Users, Remote Management Users, Replicator, Schema Admins, Server Operators, Terminal Server License Servers, Users, WinRMRemoteWMIUsers__, Windows Authorization Access Group, Worker, out-to-in, radius

Selected Source Groups Common to Selected Endpoints: All Endpoints, Verified Endpoints

remediantso	Domain Computers,	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use

Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

CryptoniteNXT Nodes

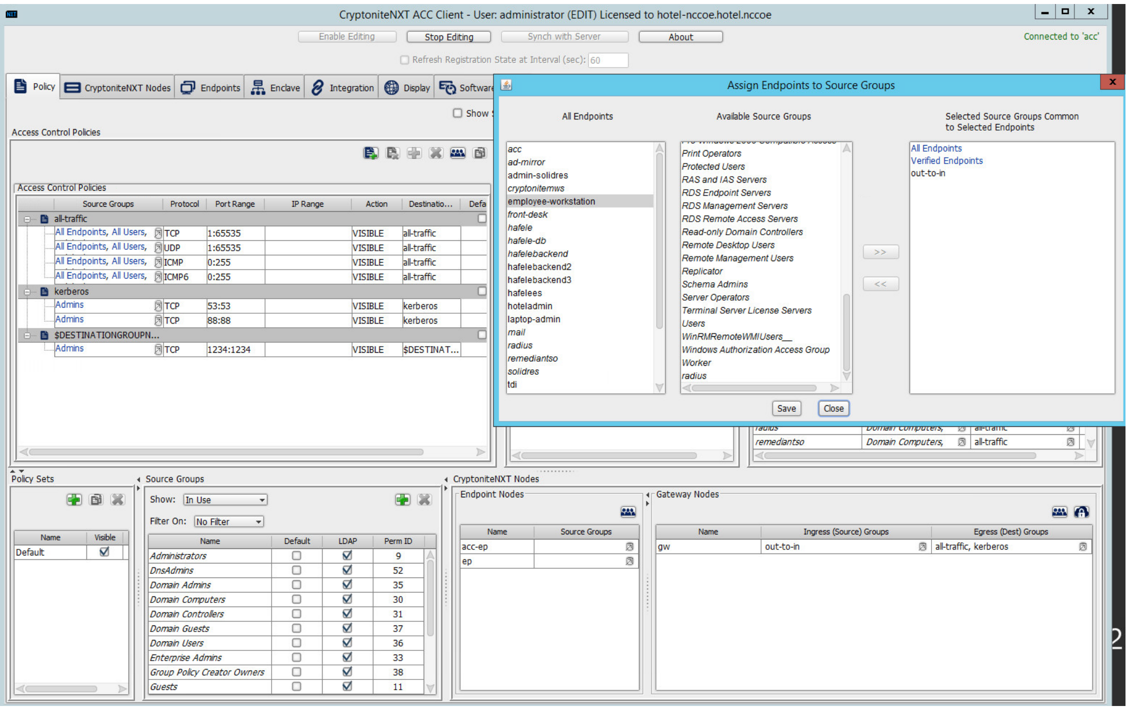
Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

6. Click **>>:**



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

☐ Refresh Registration State at Interval (sec): 60

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							☐
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							☐
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							☐
	Admins	TCP	1234:1234		VISIBLE	$DESTINAT...	

Assign Endpoints to Source Groups

All Endpoints: acc, ad-mirror, admin-solidres, cryptonitemws, employee-workstation, front-desk, hafele, hafele-db, hafelebackend, hafelebackend2, hafelebackend3, hafelees, hoteladmin, laptop-admin, mail, radius, remediantso, solidres, tdi

Available Source Groups: Print Operators, Protected Users, RAS and IAS Servers, RDS Endpoint Servers, RDS Management Servers, RDS Remote Access Servers, Read-only Domain Controllers, Remote Desktop Users, Remote Management Users, Replicator, Schema Admins, Server Operators, Terminal Server License Servers, Users, WinRMRemoteWMIUsers__, Windows Authorization Access Group, Worker, radius

Selected Source Groups Common to Selected Endpoints: All Endpoints, Verified Endpoints, out-to-in

remediantso	Domain Computers,	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use

Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

CryptoniteNXT Nodes

Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

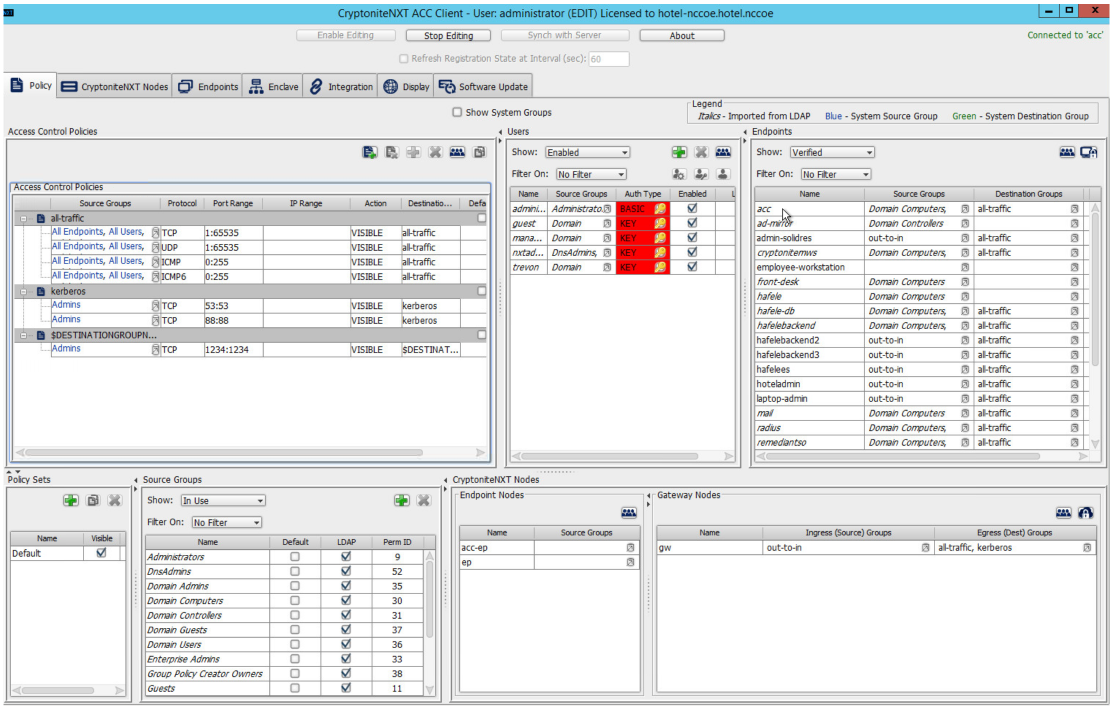
Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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:**



□ Refresh Registration State at Interval (sec): 60

□ Show System Groups

Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	Action	Destinatio...	Defa
all-traffic							□
	All Endpoints, All Users,	TCP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	UDP	1:65535		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP	0:255		VISIBLE	all-traffic	
	All Endpoints, All Users,	ICMP6	0:255		VISIBLE	all-traffic	
kerberos							□
	Admins	TCP	53:53		VISIBLE	kerberos	
	Admins	TCP	88:88		VISIBLE	kerberos	
$DESTINATIONGROUPN...							□
	Admins	TCP	1234:1234		VISIBLE	$DESTINAT...	

Users

Show: Enabled

Filter On: No Filter

Name	Source Groups	Auth Type	Enabled	L
admini...	Administrato...	BASIC	☑	
guest	Domain	KEY	☑	
mana...	Domain	KEY	☑	
nxtad...	DnsAdmins,	KEY	☑	
trevon	Domain	KEY	☑	

Endpoints

Show: Verified

Filter On: No Filter

Name	Source Groups	Destination Groups
acc	Domain Computers,	all-traffic
ad-mirror	Domain Controllers	
admin-solidres	out-to-in	all-traffic
cryptonitemws	Domain Computers,	all-traffic
employee-workstation		
front-desk	Domain Computers	
hafele	Domain Computers	
hafele-db	Domain Computers,	all-traffic
hafelebackend	Domain Computers,	all-traffic
hafelebackend2	out-to-in	all-traffic
hafelebackend3	out-to-in	all-traffic
hafelees	out-to-in	all-traffic
hoteladmin	out-to-in	all-traffic
laptop-admin	out-to-in	all-traffic
mail	Domain Computers	all-traffic
radius	Domain Computers,	all-traffic
remediantso	Domain Computers,	all-traffic

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use

Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	□	☑	9
DnsAdmins	□	☑	52
Domain Admins	□	☑	35
Domain Computers	□	☑	30
Domain Controllers	□	☑	31
Domain Guests	□	☑	37
Domain Users	□	☑	36
Enterprise Admins	□	☑	33
Group Policy Creator Owners	□	☑	38
Guests	□	☑	11

Endpoint Nodes

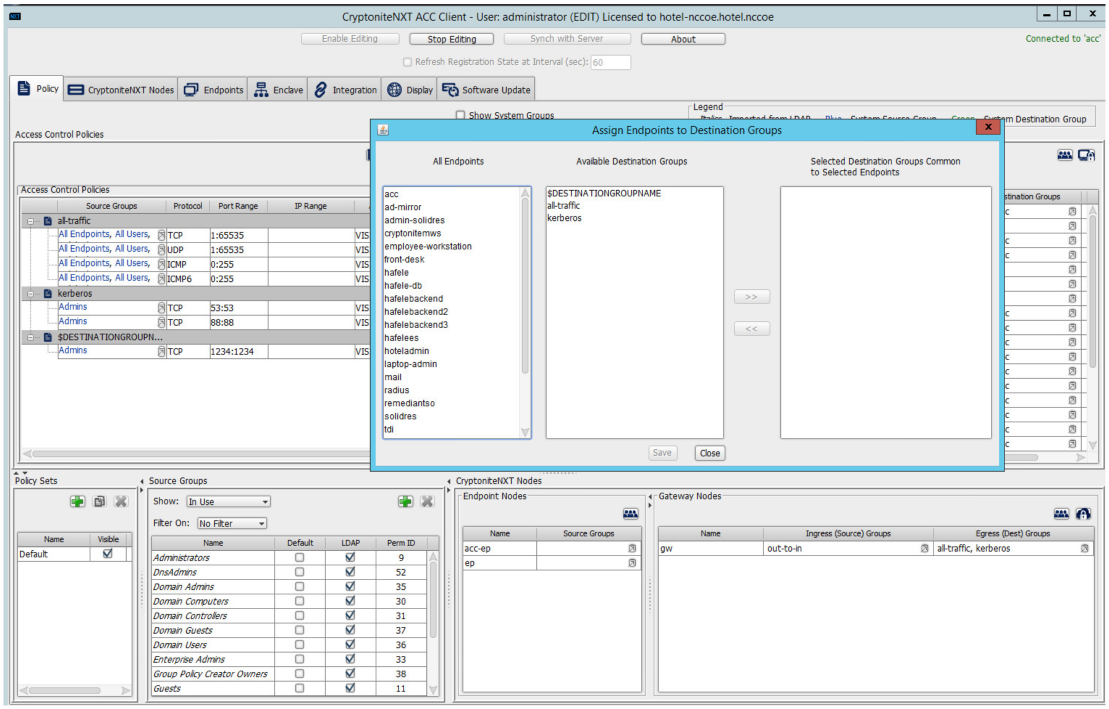
Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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:**



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

☐ Refresh Registration State at Interval (sec): 60

☐ Show System Groups

Access Control Policies

Source Groups	Protocol	Port Range	IP Range	
all-traffic				
All Endpoints, All Users,	TCP	1:65535		VIS
All Endpoints, All Users,	UDP	1:65535		VIS
All Endpoints, All Users,	ICMP	0:255		VIS
All Endpoints, All Users,	ICMP6	0:255		VIS
kerberos				
Admins	TCP	53:53		VIS
Admins	TCP	88:88		VIS
$DESTINATIONGROUPN...				
Admins	TCP	1234:1234		VIS

Assign Endpoints to Destination Groups

All Endpoints:
acc
ad-mirror
admin-solidres
cryptonitemws
employee-workstation
front-desk
hafele
hafele-db
hafelebackend
hafelebackend2
hafelebackend3
hafelees
hoteladmin
laptop-admin
mail
radius
remediantso
solidres
tdi

Available Destination Groups:
$DESTINATIONGROUPNAME
all-traffic
kerberos

Selected Destination Groups Common to Selected Endpoints

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use

Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

CryptoniteNXT Nodes

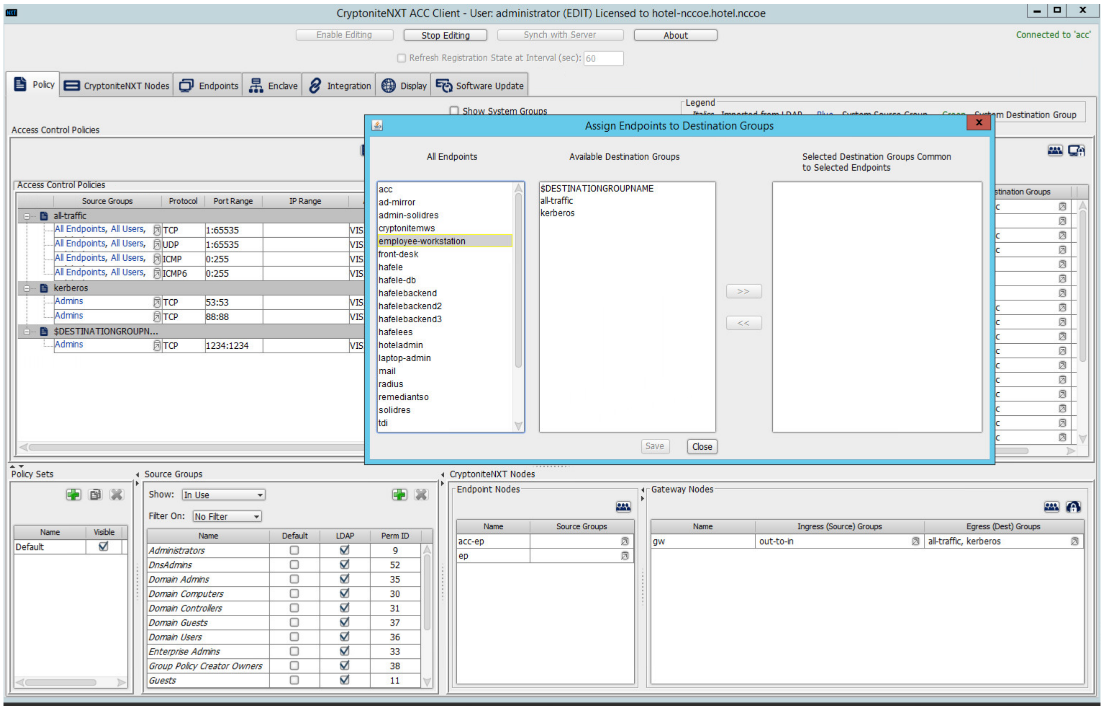
Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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



CryptoniteNXT ACC Client - User: administrator (EDIT) Licensed to hotel-nccoe.hotel.nccoe

Connected to 'acc'

☐ Refresh Registration State at Interval (sec): 60

☐ Show System Groups

Access Control Policies

Source Groups	Protocol	Port Range	IP Range	
all-traffic				
All Endpoints, All Users,	TCP	1:65535		VIS
All Endpoints, All Users,	UDP	1:65535		VIS
All Endpoints, All Users,	ICMP	0:255		VIS
All Endpoints, All Users,	ICMP6	0:255		VIS
kerberos				
Admins	TCP	53:53		VIS
Admins	TCP	88:88		VIS
$DESTINATIONGROUPN...				
Admins	TCP	1234:1234		VIS

Assign Endpoints to Destination Groups

All Endpoints:
acc
ad-mirror
admin-solidres
cryptonitemws
employee-workstation
front-desk
hafele
hafele-db
hafelebackend
hafelebackend2
hafelebackend3
hafelees
hoteladmin
laptop-admin
mail
radius
remediantso
solidres
tdi

Available Destination Groups:
$DESTINATIONGROUPNAME
all-traffic
kerberos

Selected Destination Groups Common to Selected Endpoints

Policy Sets

Name	Visible
Default	☑

Source Groups

Show: In Use

Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

CryptoniteNXT Nodes

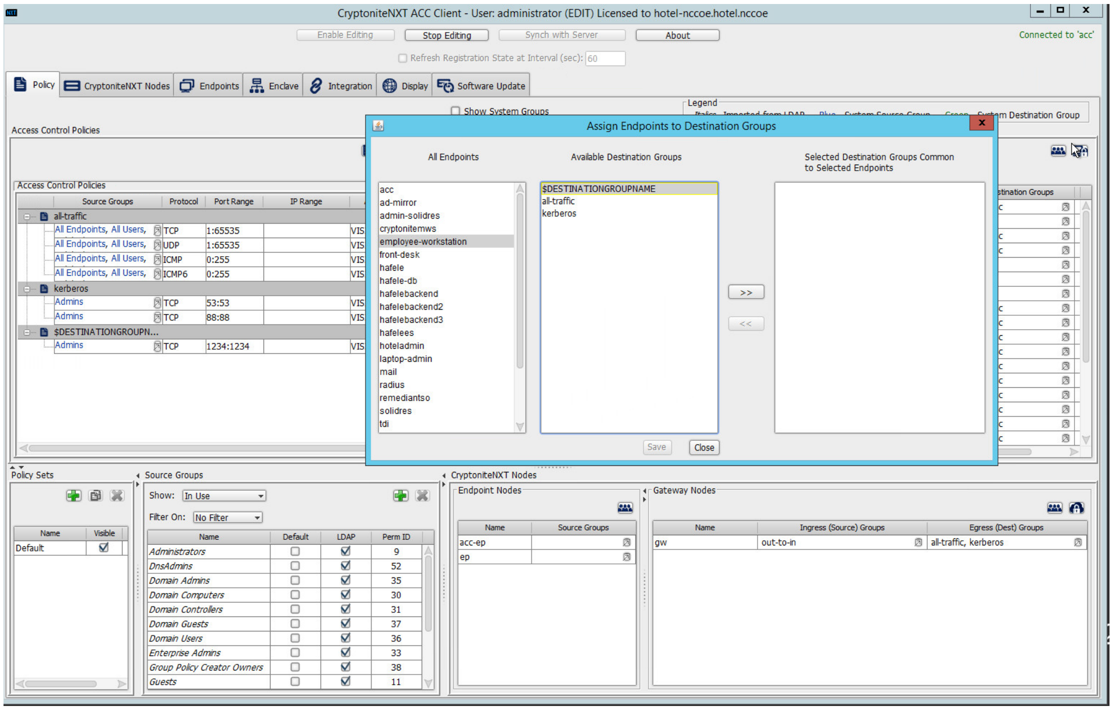
Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

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



Access Control Policies

	Source Groups	Protocol	Port Range	IP Range	
all-traffic					
	All Endpoints, All Users,	TCP	1:65535		VIS
	All Endpoints, All Users,	UDP	1:65535		VIS
	All Endpoints, All Users,	ICMP	0:255		VIS
	All Endpoints, All Users,	ICMP6	0:255		VIS
kerberos					
	Admins	TCP	53:53		VIS
	Admins	TCP	88:88		VIS
$DESTINATIONGROUPN...					
	Admins	TCP	1234:1234		VIS

All Endpoints:

acc
ad-mirror
admin-solidres
cryptonitemws
employee-workstation
front-desk
hafele
hafele-db
hafelebackend
hafelebackend2
hafelebackend3
hafelees
hoteladmin
laptop-admin
mail
radius
remediantso
solidres
tdi

Available Destination Groups:

$DESTINATIONGROUPNAME
all-traffic
kerberos

Policy Sets

Name	Visible
Default	☑

Source Groups — Show: In Use; Filter On: No Filter

Name	Default	LDAP	Perm ID
Administrators	□	☑	9
DnsAdmins	□	☑	52
Domain Admins	□	☑	35
Domain Computers	□	☑	30
Domain Controllers	□	☑	31
Domain Guests	□	☑	37
Domain Users	□	☑	36
Enterprise Admins	□	☑	33
Group Policy Creator Owners	□	☑	38
Guests	□	☑	11

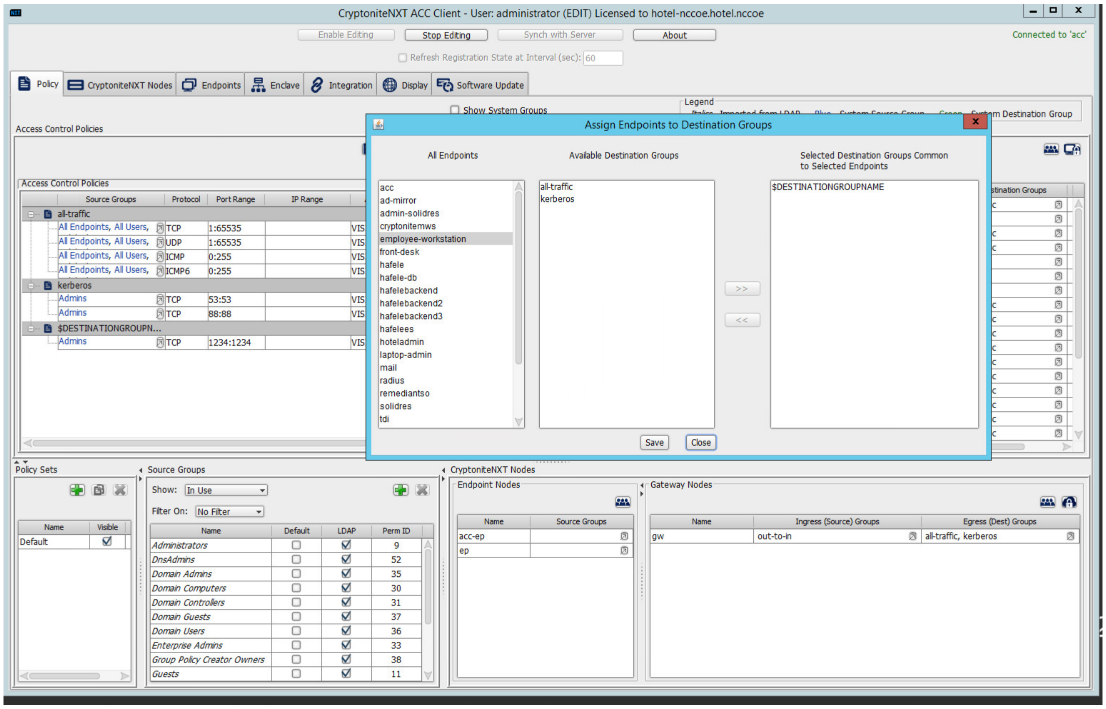
Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

6. Click **>>:**



Access Control Policies

Source Groups	Protocol	Port Range	IP Range	
all-traffic				
All Endpoints, All Users,	TCP	1:65535		VIS
All Endpoints, All Users,	UDP	1:65535		VIS
All Endpoints, All Users,	ICMP	0:255		VIS
All Endpoints, All Users,	ICMP6	0:255		VIS
kerberos				
Admins	TCP	53:53		VIS
Admins	TCP	88:88		VIS
$DESTINATIONGROUPN...				
Admins	TCP	1234:1234		VIS

All Endpoints:
acc
ad-mirror
admin-solidres
cryptonitemws
employee-workstation
front-desk
hafele
hafele-db
hafelebackend
hafelebackend2
hafelebackend3
hafelees
hoteladmin
laptop-admin
mail
radius
remediantso
solidres
tdi

Available Destination Groups:
all-traffic
kerberos

Selected Destination Groups Common to Selected Endpoints:
$DESTINATIONGROUPNAME

Policy Sets

Name	Visible
Default	☑

Source Groups

Name	Default	LDAP	Perm ID
Administrators	☐	☑	9
DnsAdmins	☐	☑	52
Domain Admins	☐	☑	35
Domain Computers	☐	☑	30
Domain Controllers	☐	☑	31
Domain Guests	☐	☑	37
Domain Users	☐	☑	36
Enterprise Admins	☐	☑	33
Group Policy Creator Owners	☐	☑	38
Guests	☐	☑	11

Endpoint Nodes

Name	Source Groups
acc-ep	
ep	

Gateway Nodes

Name	Ingress (Source) Groups	Egress (Dest) Groups
gw	out-to-in	all-traffic, kerberos

7. Click **Save.**

2.1.8 CryptoniteNXT Configuration for the PMS Reference Design

To gain the benefits of ZTA discussed in Volume B of this document, proper configuration of the CryptoniteNXT device is required. Non-use 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 destination groups shown in Table 2-1 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

Destination Group	Source Group	Protocol	Port Range
Solidres-Public	All Endpoints, All Users	TCP	80:80
	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

Apply the source and destination groups to the end points shown in Table 2-2 per instructions in Section 2.1.4 and Section 2.1.5. In some deployments, the adopting enterprise may have included an all-traffic or similar rule to facilitate installation of other devices in the protected zone. Remove all-traffic rules that allow elevated network privileges at this stage.

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 reference design and maps to the Identity and Access Management component of the ZTA.

2.2.1 Access Control Platform–TDi ConsoleWorks—Overview

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

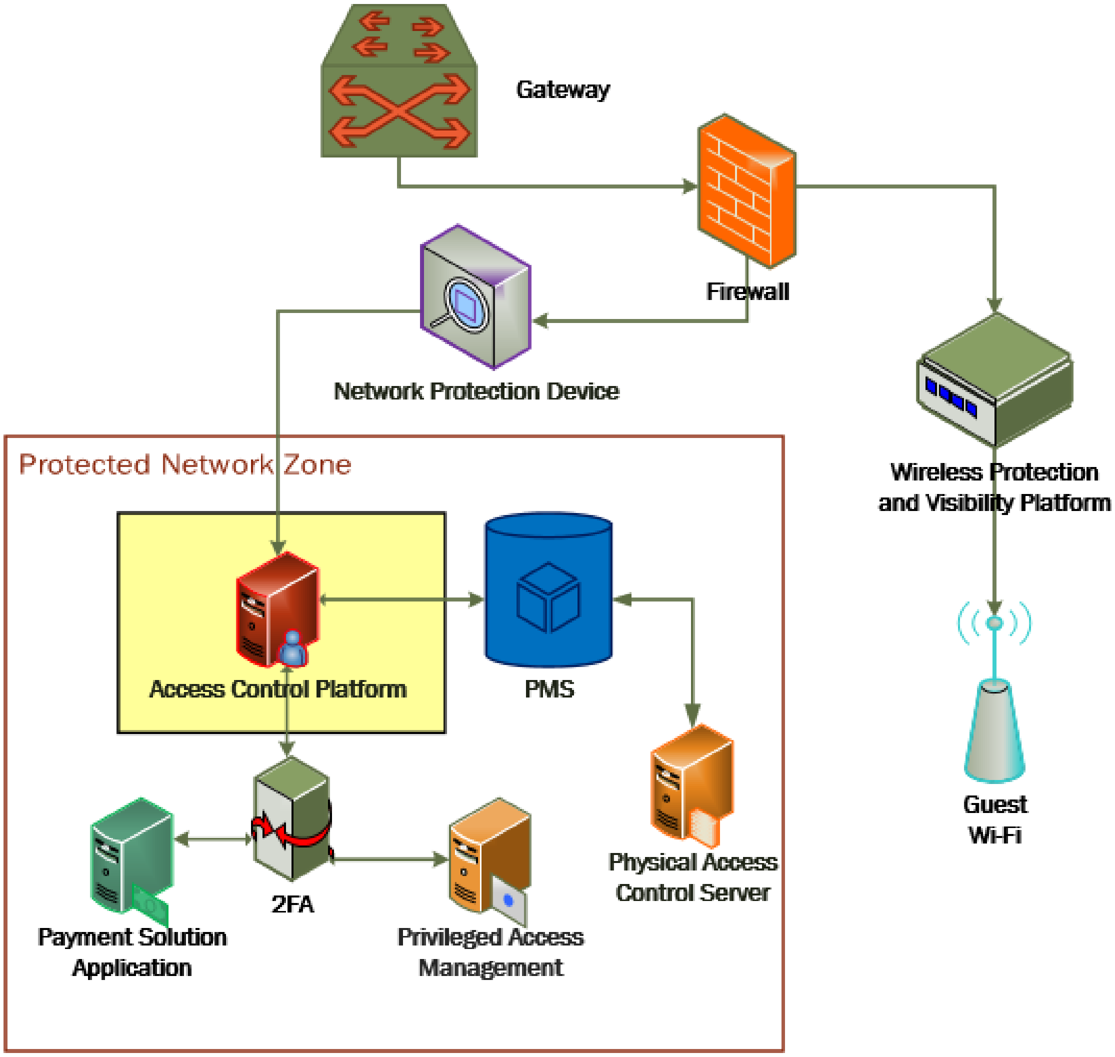
TDi ConsoleWorks was deployed as a virtual machine (VM) in the NCCoE hospitality lab. Installation instructions are available at the TDi Technologies support site, which may be useful if the adopting enterprise's deployment differs substantially from the one used for this project.

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.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

Figure 2-2 Access Control Platform in the Reference Architecture


Gateway
Firewall
Network Protection Device
Wireless Protection and Visibility Platform
Protected Network Zone
Access Control Platform
PMS
Guest Wi-Fi
2FA
Physical Access Control Server
Payment Solution Application
Privileged Access Management

2.2.2 Access Control Platform—TDi ConsoleWorks—Requirements

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

2.2.2.1 Hardware Requirements for Access Control Platform

TDi recommends amending hardware requirements for ConsoleWorks depending on the size of the 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 7.0, 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:

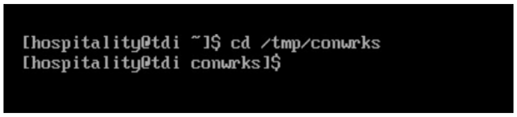
```
mkdir /tmp/conwrks
```

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:

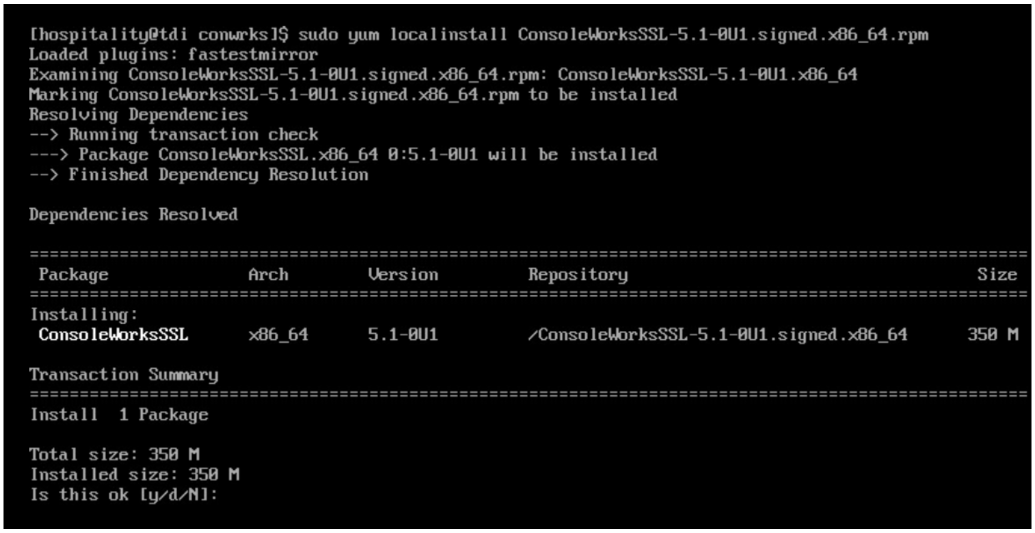
```
cd /tmp/conwrks
```



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

4. Execute the installation media:

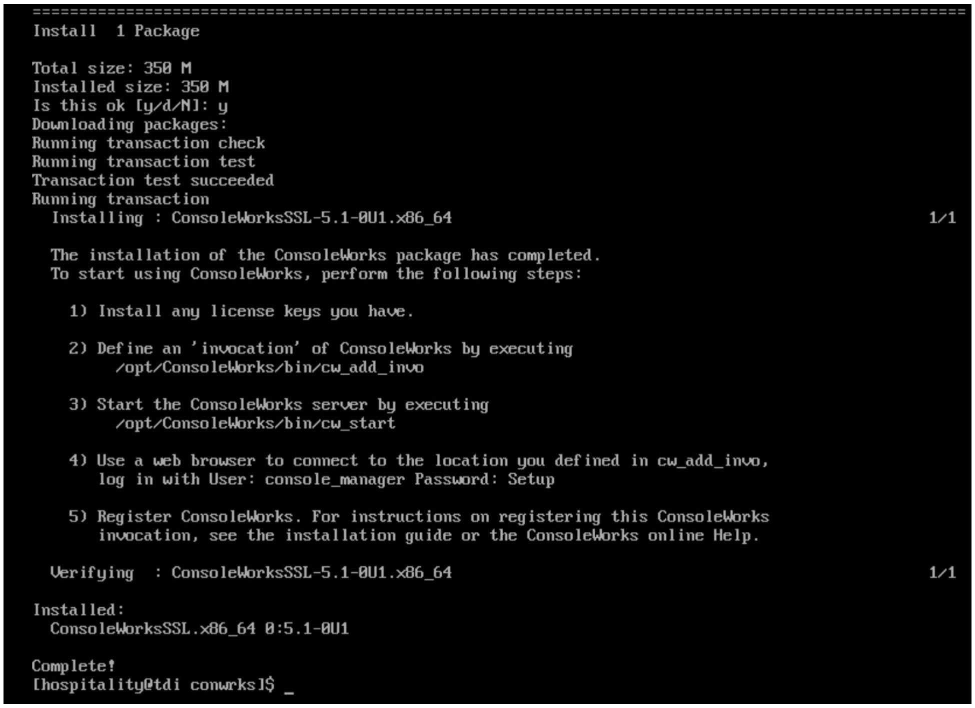
```
yum localinstall consoleworksssl-<version>_x86_64.rpm
```



```
[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:



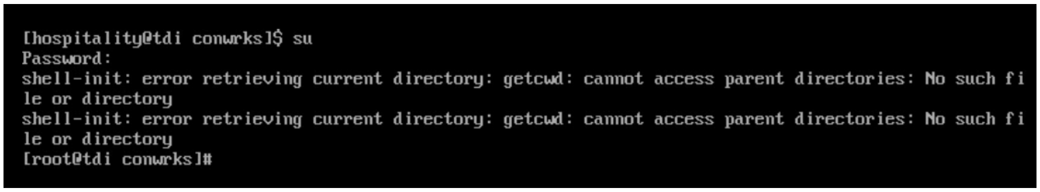
```
==================================================================================================
 Install  1 Package

 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]$ _
```

2.2.3.1 Create SSL Invocation

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

   `su`

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]#
```

3. Begin invocation creation with the following command:

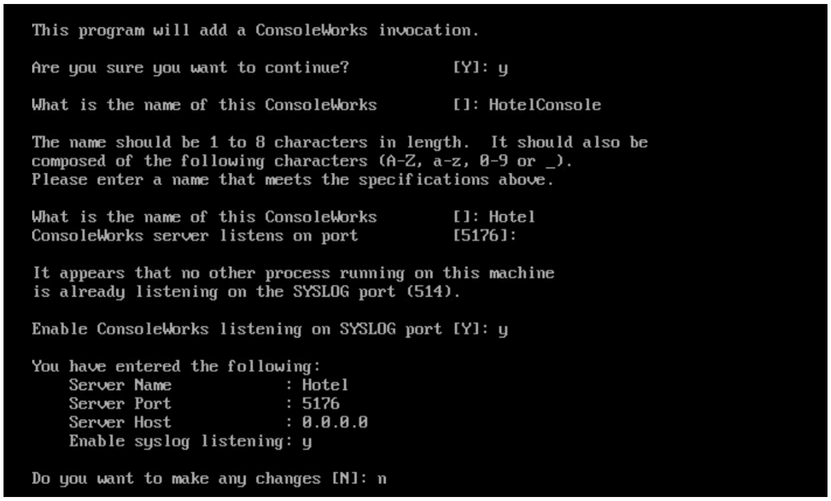
   `/opt/ConsoleWorks/bin/cw_add_invo`

4. Read the End User License Agreement. Accept by typing `y` followed by the enter key.

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

   a. desired console name [HotelConsole]
   b. web service port [5176]
   c. enabled syslog functionality [y]

6. Verify that the desired values have been entered:



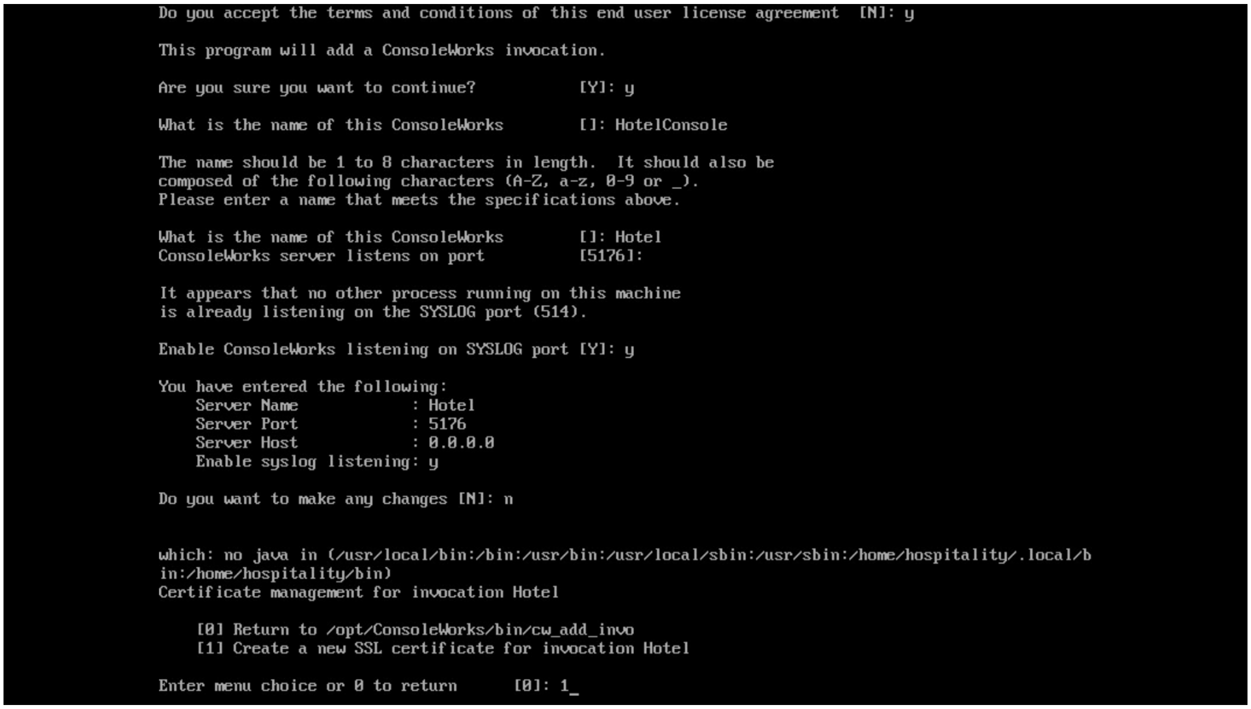
```
This program will add a ConsoleWorks invocation.

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
```

7. If satisfied, type `n` for no changes.

2.2.3.2 Create SSL Certificate

These instructions rely on execution of Section 2.2.3.1 and are a continuation of the invocation creation process. They are separated here for clarity.

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

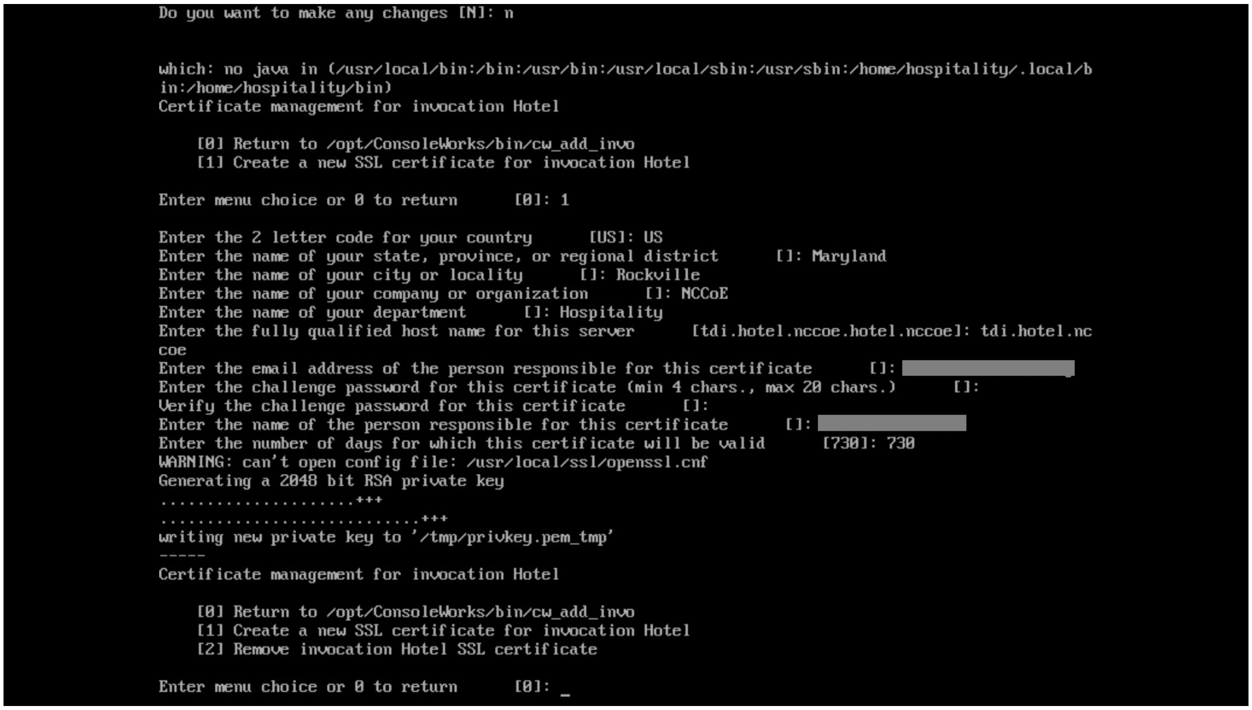
   g. email address of the person responsible for the certificate

   h. password to protect the certificate

   i. the same password to confirm

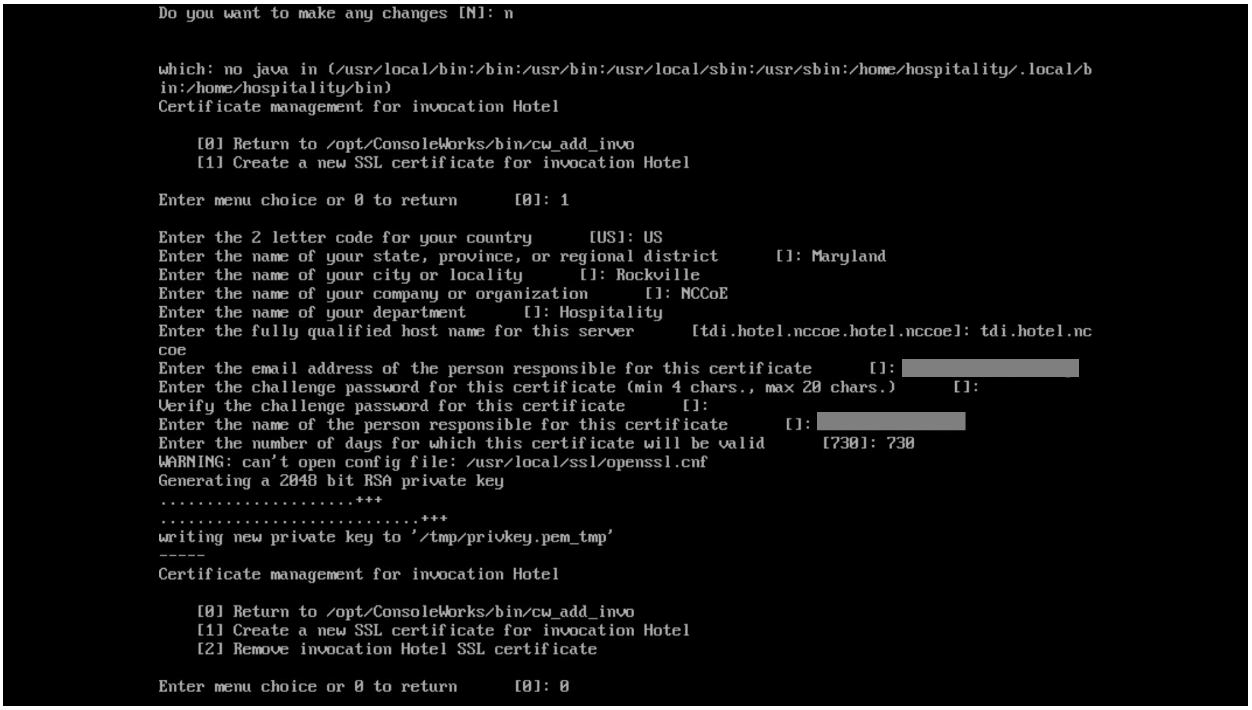
   j. name of the person responsible for the certificate

   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]: _
```

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

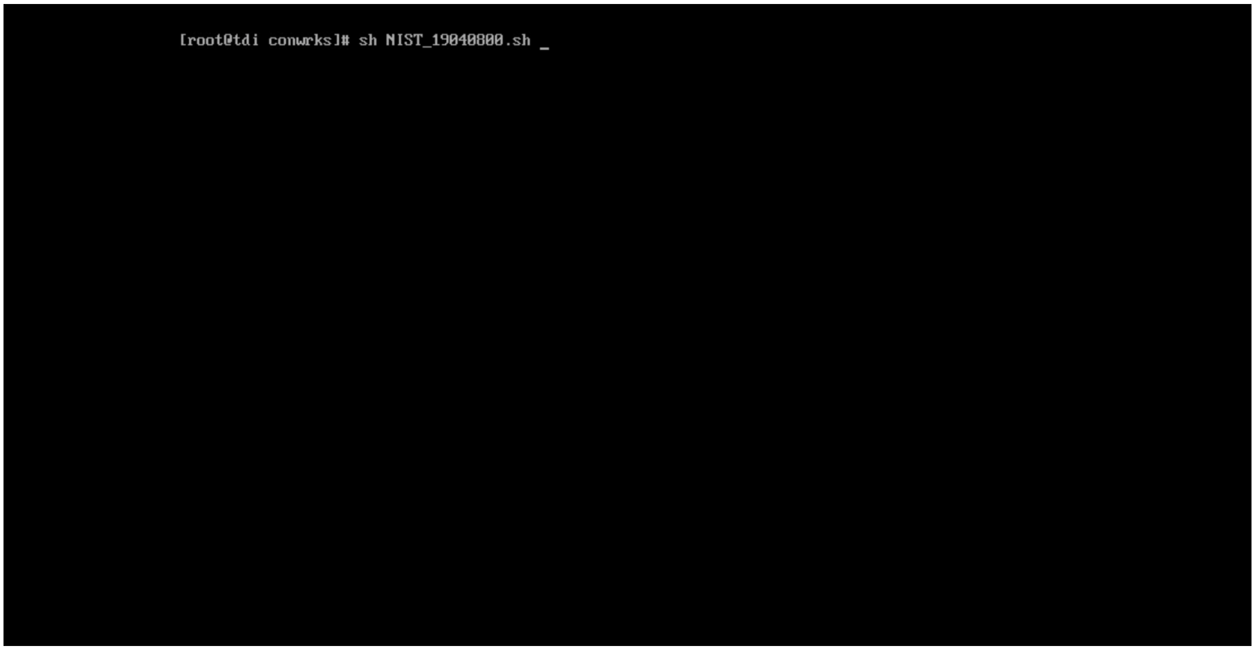


```
Do you want to make any changes [N]: n


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

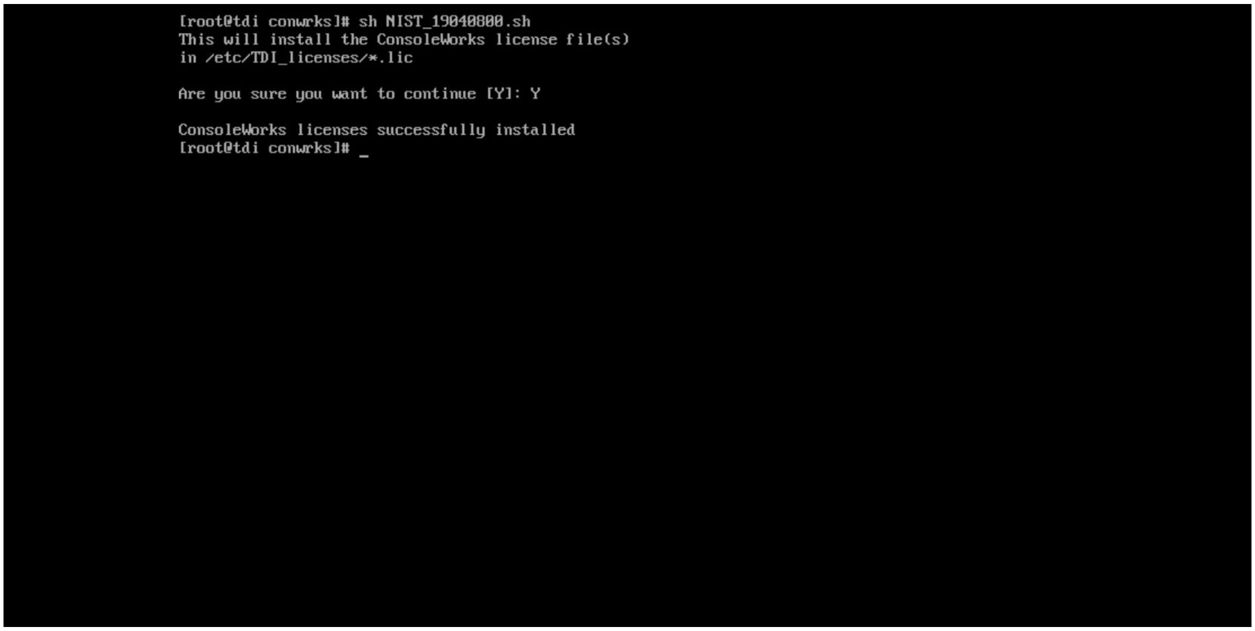
The following instructions rely on continued access to the CLI of the TDi ConsoleWorks device.

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



```
[root@tdi conwrks]# sh NIST_19040800.sh _
```

2. Input `Y`:

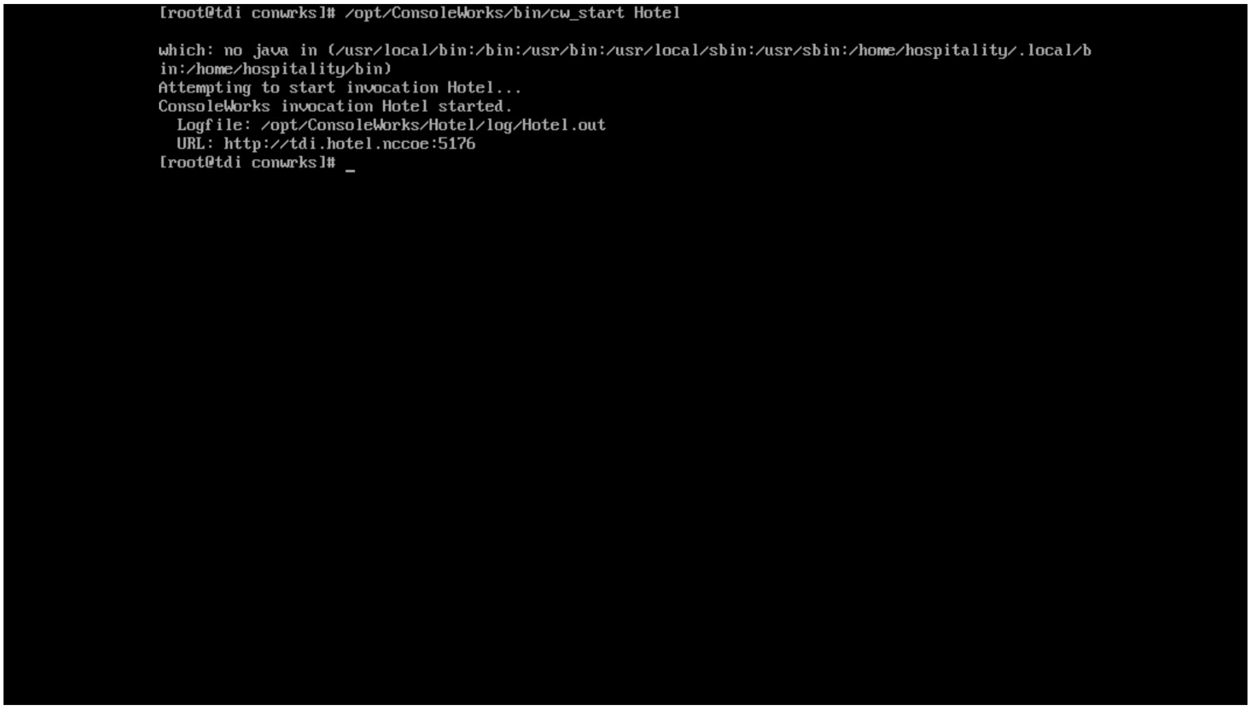


```
[root@tdi conwrks]# sh NIST_19040800.sh
This will install the ConsoleWorks license file(s)
in /etc/TDI_licenses/*.lic

Are you sure you want to continue [Y]: Y

ConsoleWorks licenses successfully installed
[root@tdi conwrks]# _
```

2.2.3.4 Start-Up

1. Execute the following command, and note the address and port provided in the console response:

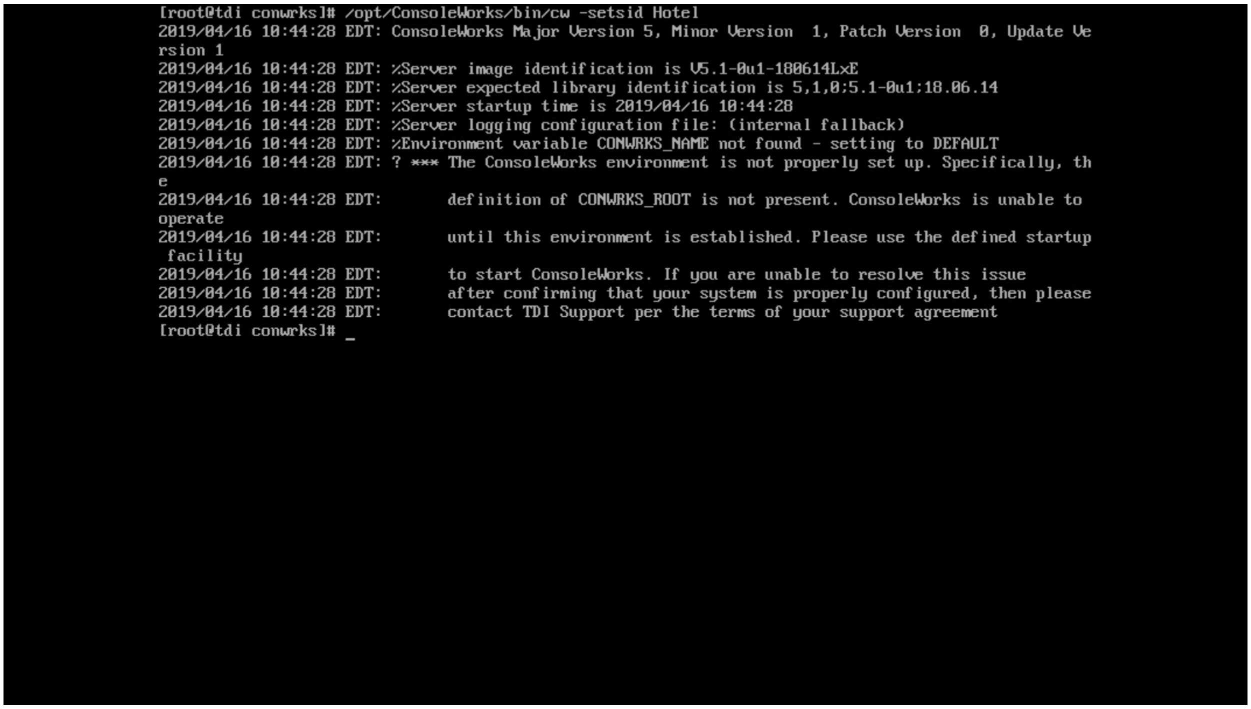
```
/opt/ConsoleWorks/bin/cw_start Hotel
```



```
[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]# _
```

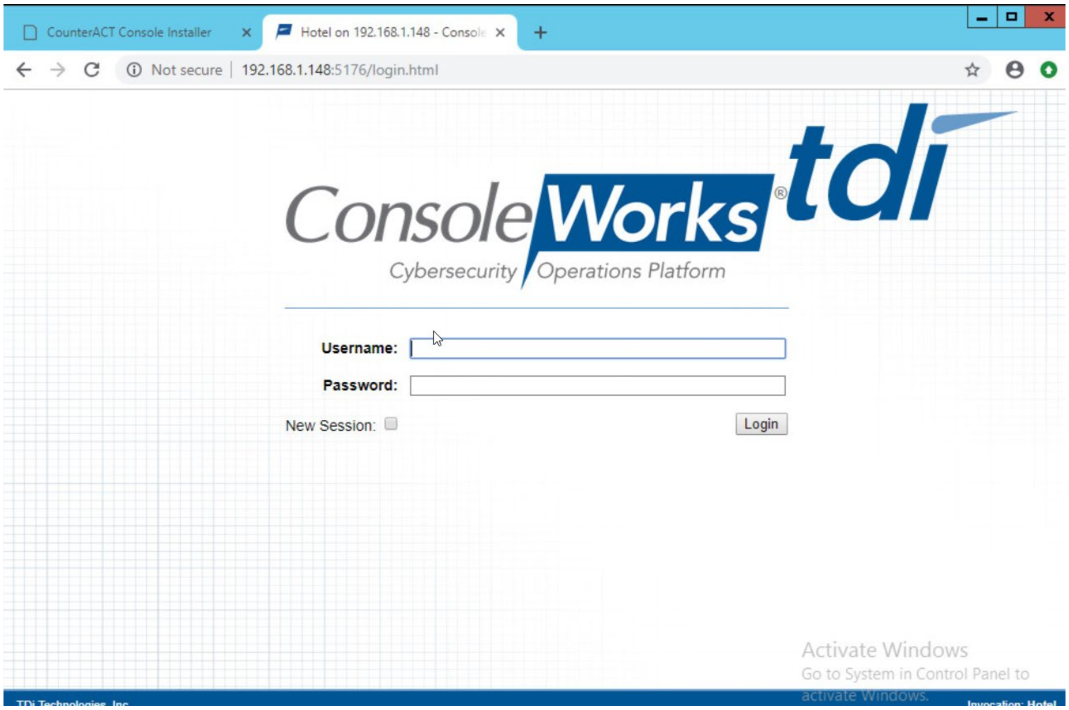
2. Execute the following command:

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

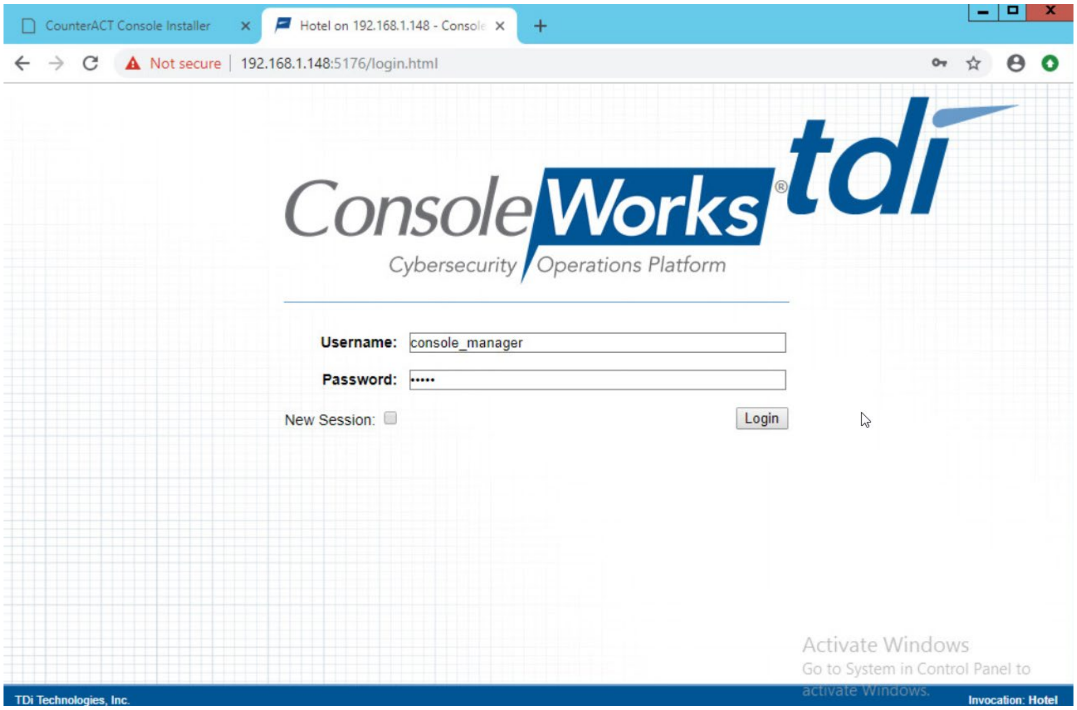


```
[root@tdi conwrks]# /opt/ConsoleWorks/bin/cw -setsid Hotel
2019/04/16 10:44:28 EDT: ConsoleWorks Major Version 5, Minor Version  1, Patch Version  0, Update Ve
rsion 1
2019/04/16 10:44:28 EDT: %Server image identification is V5.1-0u1-180614LxE
2019/04/16 10:44:28 EDT: %Server expected library identification 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]# _
```

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


CounterACT Console Installer
Hotel on 192.168.1.148 - Console
Not secure
192.168.1.148:5176/login.html
ConsoleWorks
tdi
Cybersecurity Operations Platform
Username:
Password:
New Session: □
Login
Activate Windows
Go to System in Control Panel to activate Windows.
TDi Technologies, Inc.
Invocation: Hotel

4. Log in with default credentials console_manager/Setup:



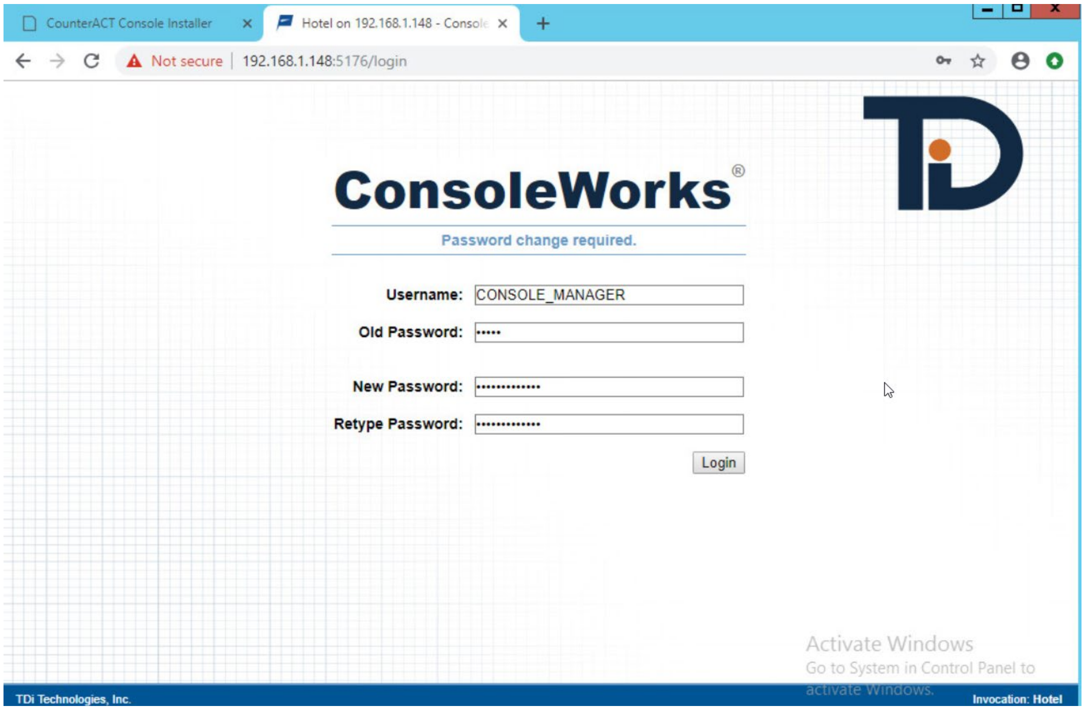
CounterACT Console Installer
Hotel on 192.168.1.148 - Console
Not secure
192.168.1.148:5176/login.html
ConsoleWorks
tdi
Cybersecurity Operations Platform
Login
TDi Technologies, Inc.
Invocation: Hotel
Activate Windows
Go to System in Control Panel to activate Windows.

Username: console_manager

Password: •••••

New Session: □

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



CounterACT Console Installer
Hotel on 192.168.1.148 - Console
Not secure
192.168.1.148:5176/login
ConsoleWorks®
TD

Password change required.

Username: CONSOLE_MANAGER

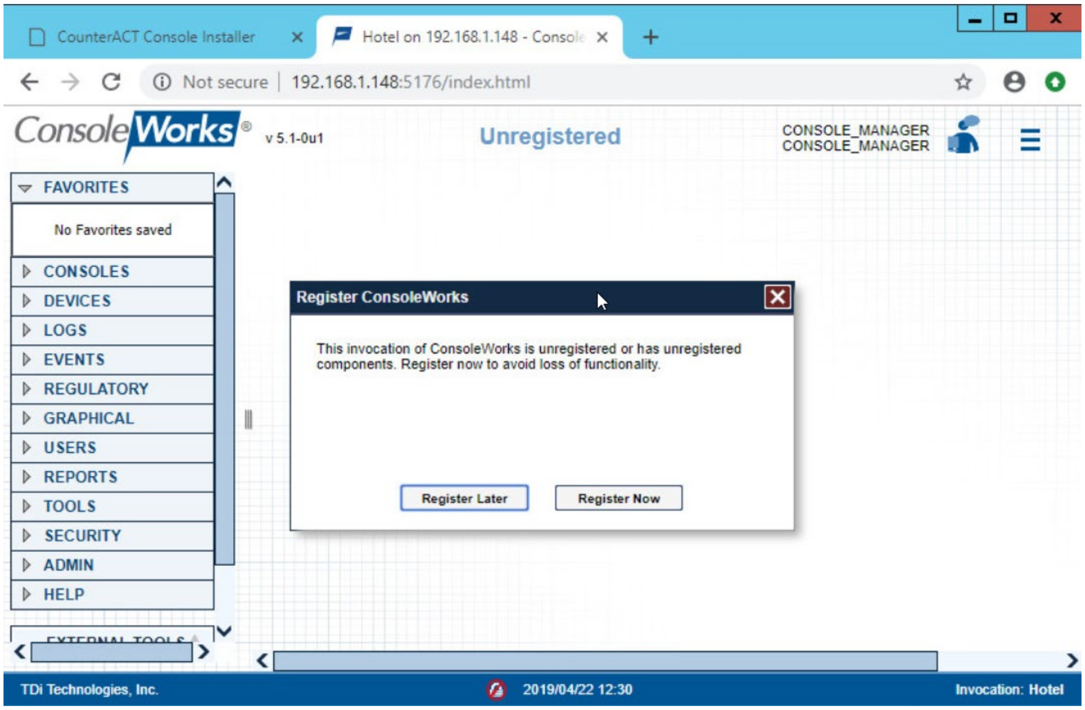
Old Password: •••••

New Password: •••••••••••••

Retype Password: •••••••••••••

Login
Activate Windows
Go to System in Control Panel to activate Windows.
TDi Technologies, Inc.
Invocation: Hotel

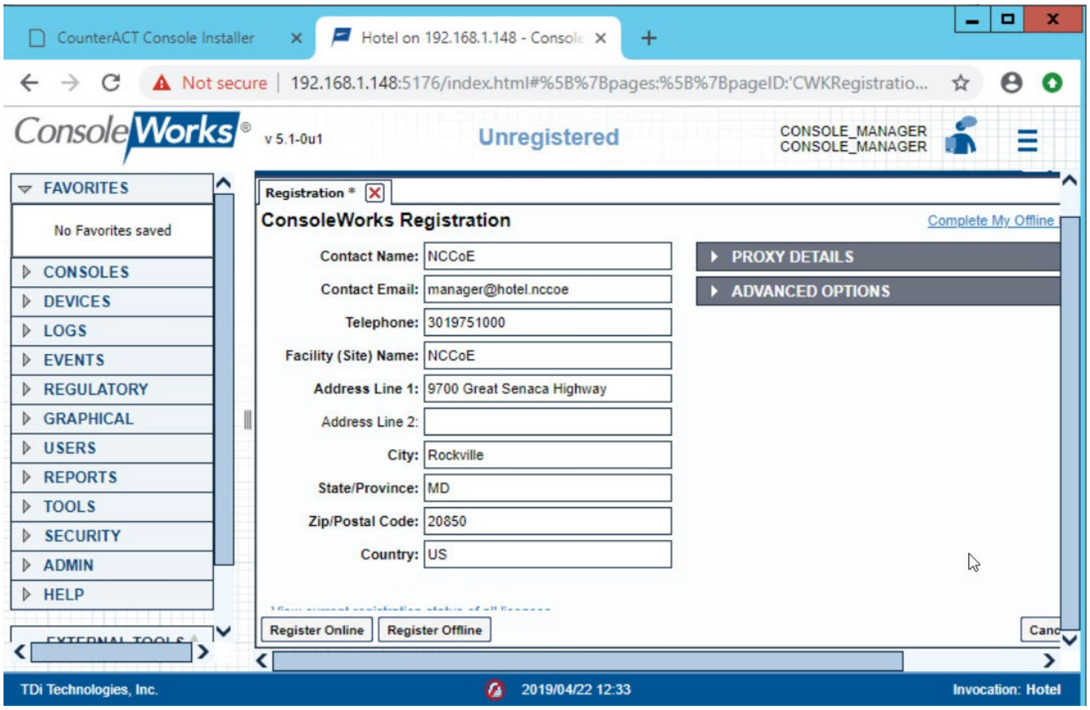
6. Click **Register Now:**



Register ConsoleWorks

This invocation of ConsoleWorks is unregistered or has unregistered components. Register now to avoid loss of functionality.

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



ConsoleWorks Registration

Contact Name: NCCoE

Contact Email: manager@hotel.nccoe

Telephone: 3019751000

Facility (Site) Name: NCCoE

Address Line 1: 9700 Great Senaca Highway

Address Line 2:

City: Rockville

State/Province: MD

Zip/Postal Code: 20850

Country: US

2.2.3.5 GUI Gateway Installation

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

    -freerdp-libs

    -uuid

    -cairo

    -libvncserver

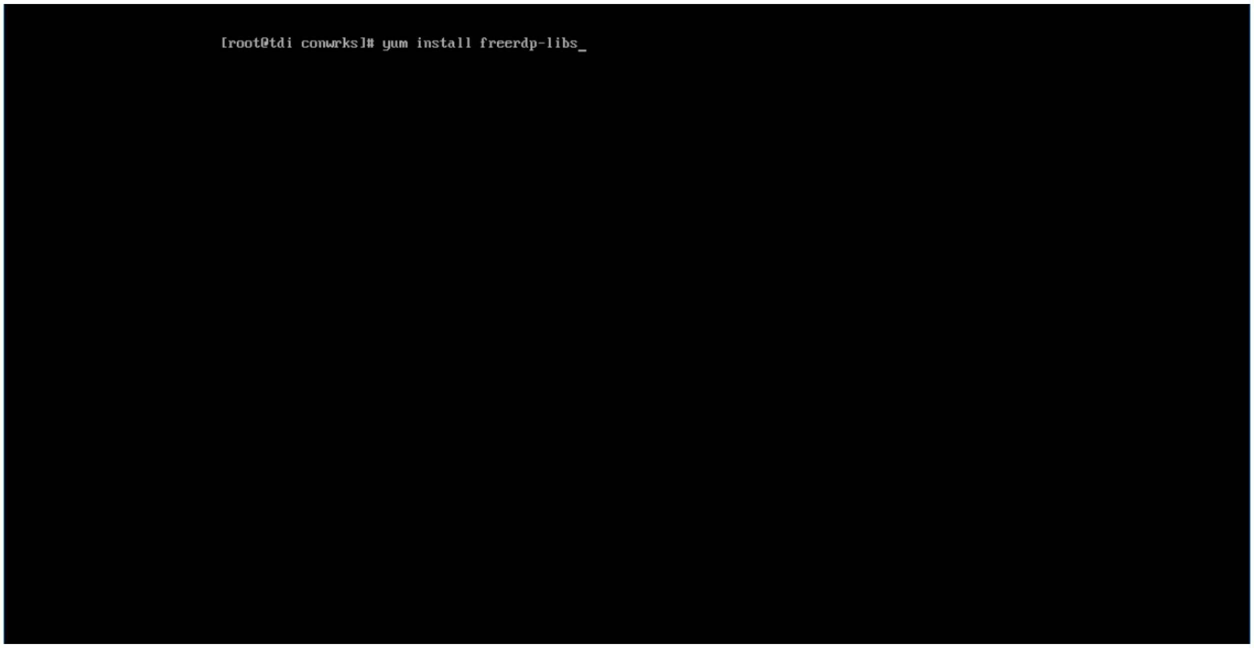
    -libpng12

    -freerdp-plugins

    -net-tools

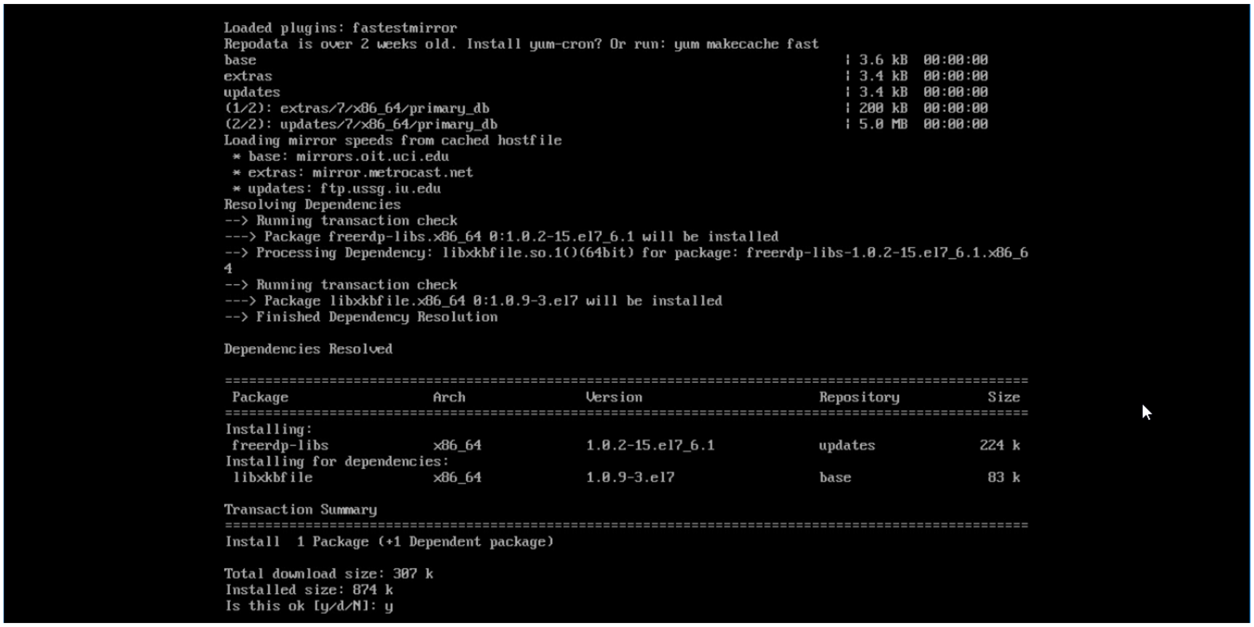
    -openssh-clients

    -open-vm-tools



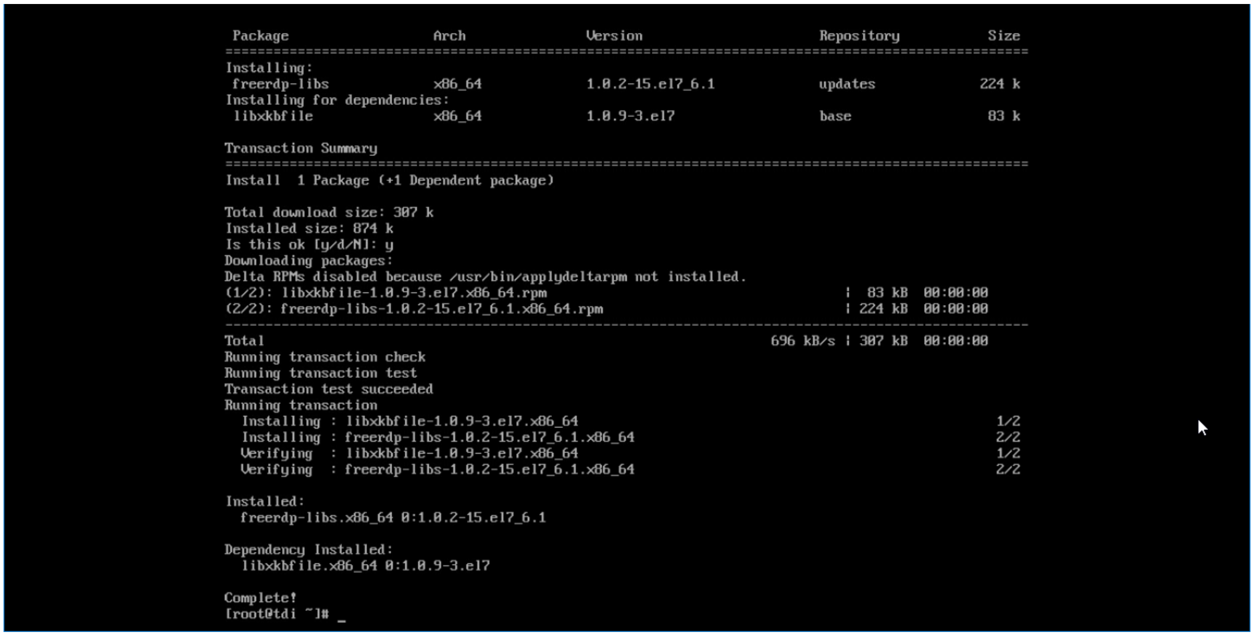
```
[root@tdi conwrks]# yum install freerdp-libs_
```

2. Type y to allow installation:



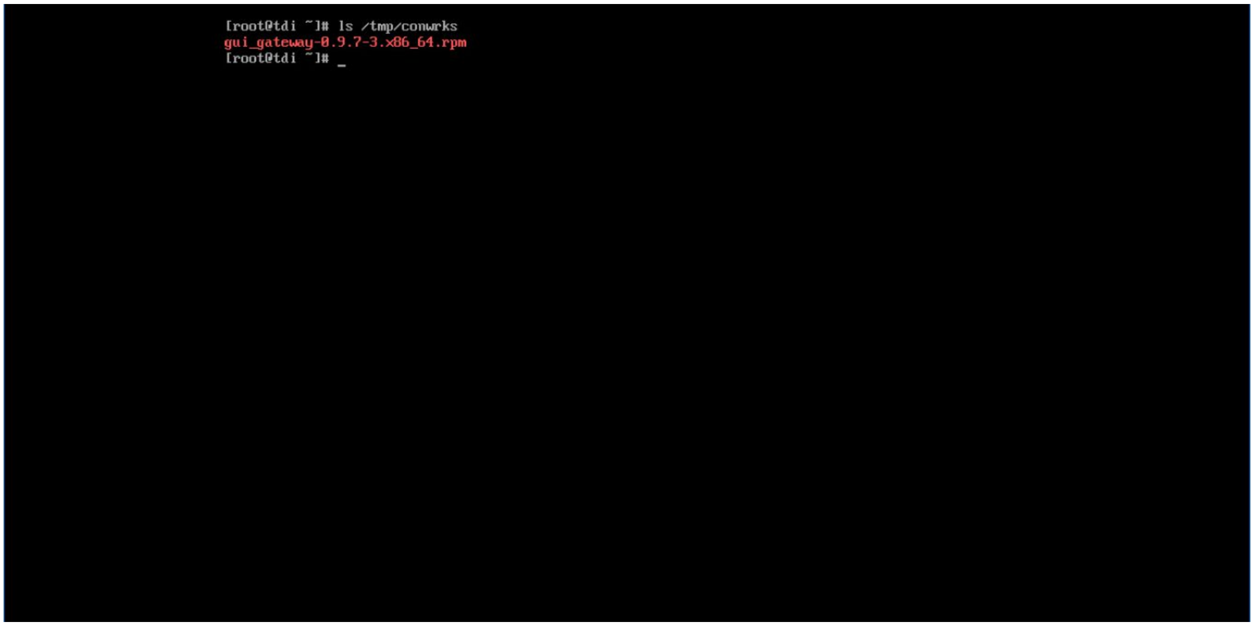
```
Loaded plugins: fastestmirror
Repodata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
base                                                                     ¦ 3.6 kB  00:00:00
extras                                                                   ¦ 3.4 kB  00:00:00
updates                                                                  ¦ 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
```

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 ~]# _
```

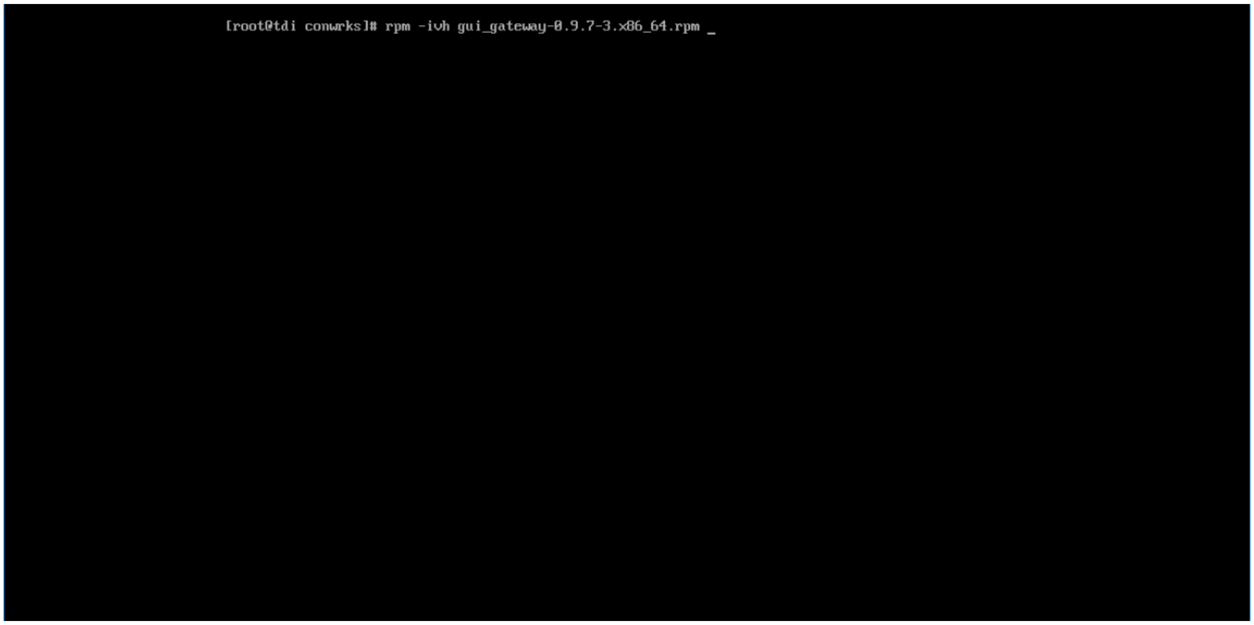
4. Download *gui_gateway-0.9.7-3.x86_64.rpm* (or the latest version), and place on the TDi back-end server:



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

5. Install with this command:

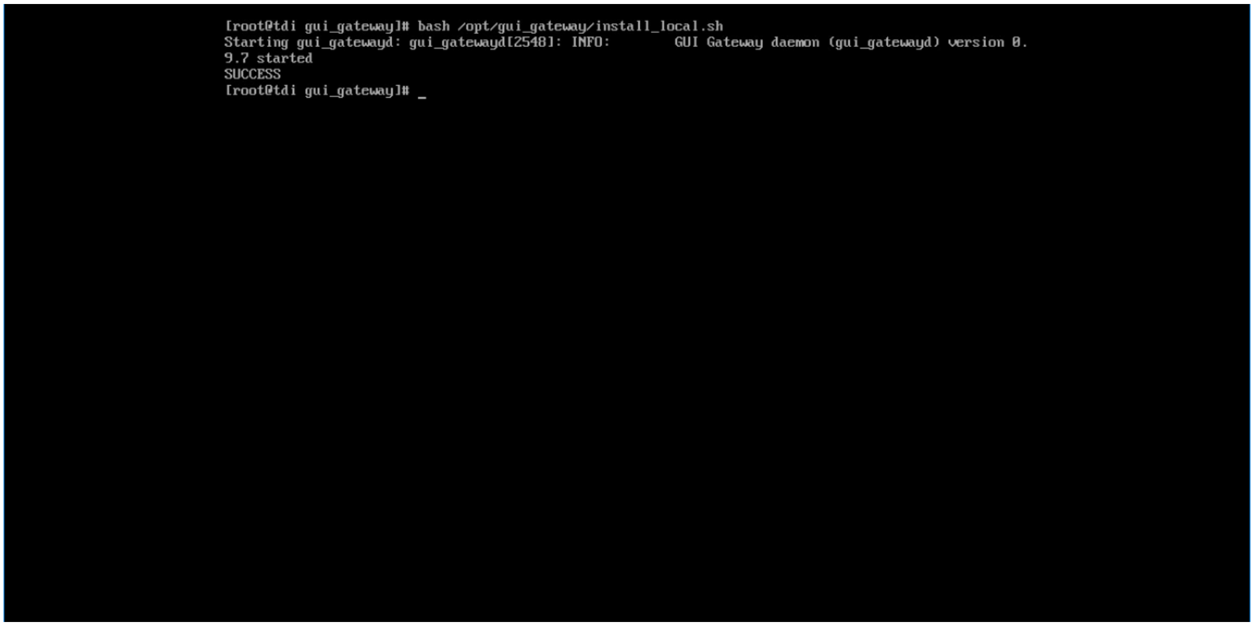
```
rpm -ivh gui_gateway-0.9.7-3.x86_64.rpm
```



```
[root@tdi conwrks]# 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:

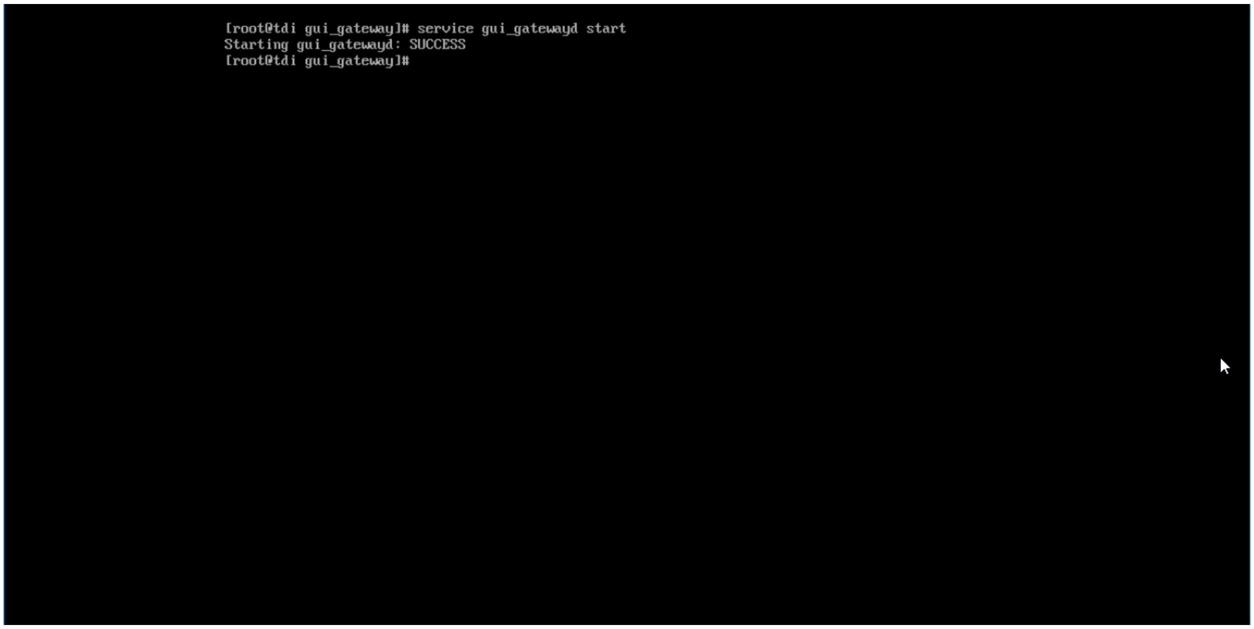
```
/opt/gui_gateway/install_local.sh
```



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

7. Execute the following to start the gateway:

```
service gui_gatewayd start
```



```
[root@tdi gui_gateway]# service gui_gatewayd start
Starting gui_gatewayd: SUCCESS
[root@tdi gui_gateway]#
```

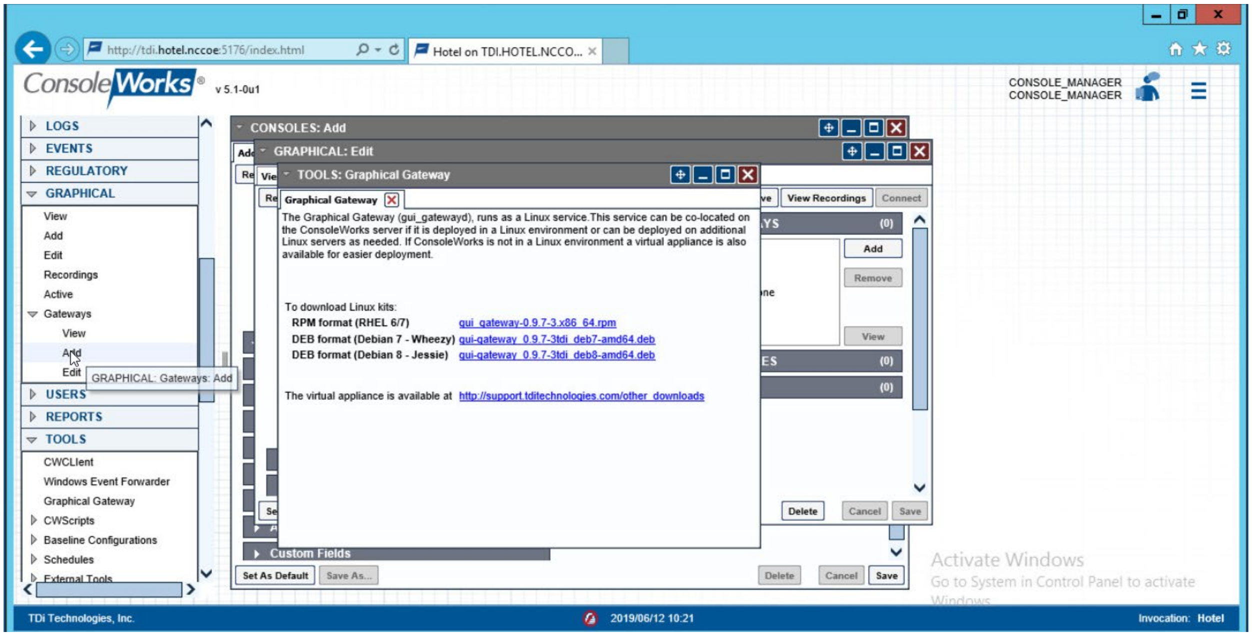
2.2.4 Add Gateway to GUI

The instructions below are executed on a separate virtual or physical machine that has network access to the TDi ConsoleWorks back-end server through the previously configured web port. The web service is accessed through a web browser. The user must navigate to `[TDi Domain Name].[Hotel Domain]:[Port Number]` if DNS has been configured for the enterprise or to `[TDi IP Address]:[Port Number]` if DNS has not been configured.

1. Authenticate to the web portal with the `console_manager` account.

2. Once authenticated, expand the side menu by clicking **Graphical** and then **Gateways.** Click **Add:**

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.



The Graphical Gateway (gui_gatewayd), runs as a Linux service.This service can be co-located on the ConsoleWorks server if it is deployed in a Linux environment or can be deployed on additional Linux servers as needed. If ConsoleWorks is not in a Linux environment a virtual appliance is also available for easier deployment.

To download Linux kits:

RPM format (RHEL 6/7)	gui_gateway-0.9.7-3.x86_64.rpm
DEB format (Debian 7 - Wheezy)	gui-gateway_0.9.7-3tdi_deb7-amd64.deb
DEB format (Debian 8 - Jessie)	gui-gateway_0.9.7-3tdi_deb8-amd64.deb

The virtual appliance is available at http://support.tditechnologies.com/other_downloads

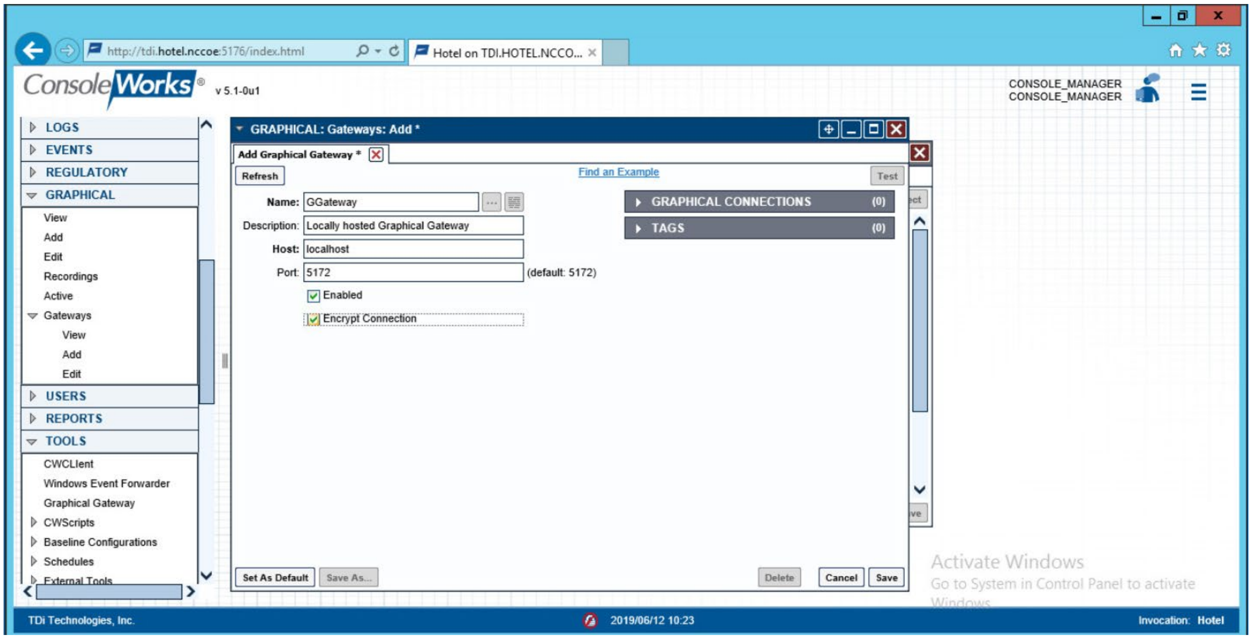
3. Enter the desired values for the graphical gateway. The values used for this architecture are provided but may not be the correct values for your enterprise.

    a. Name [GGateway]

    b. Description [Locally hosted Graphical Gateway]

    c. Host [localhost]

    d. Port [5172]



Name: GGateway

Description: Locally hosted Graphical Gateway

Host: localhost

Port: 5172 (default: 5172)

☑ Enabled

☑ Encrypt Connection

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]

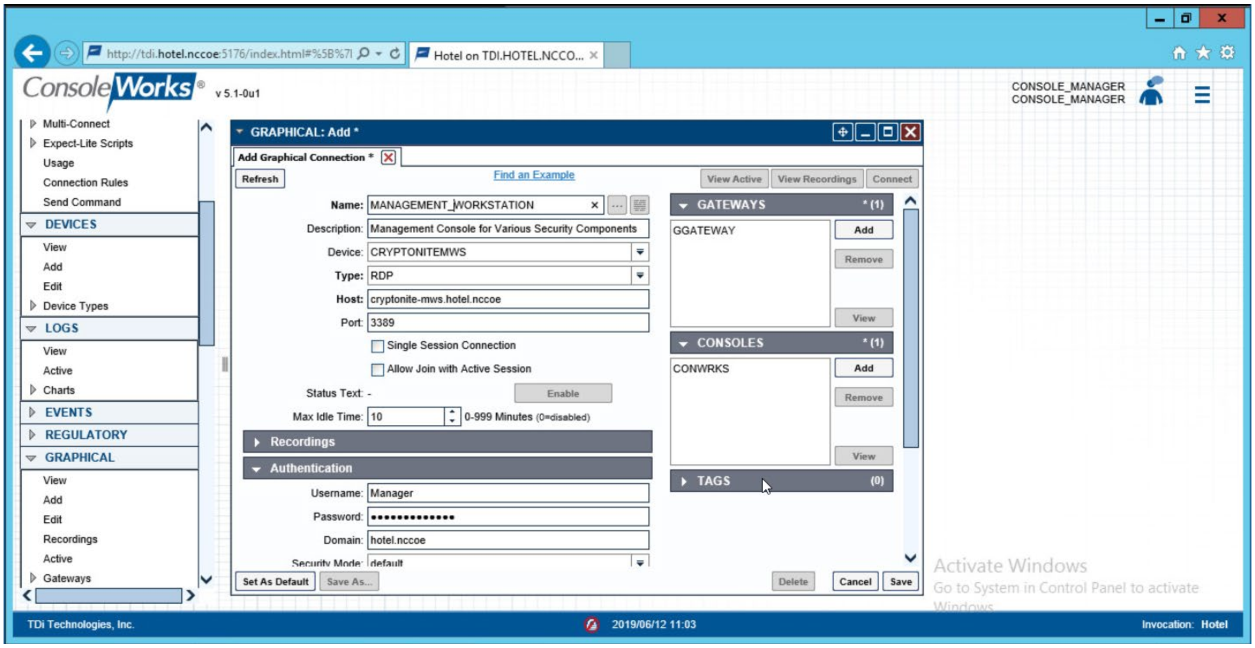
    e. DNS Host Information [cryptonite-mws.hotel.nccoe]

    f. Port number [3389]

    g. Username [Administrator]

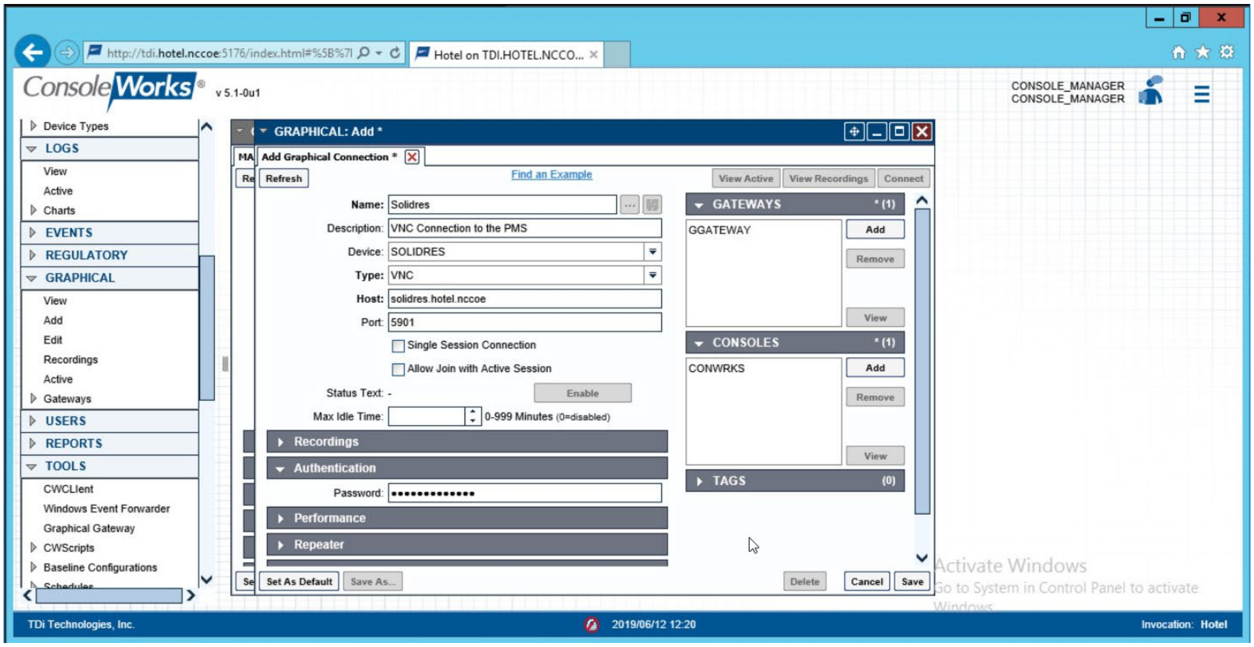
    h. Password

    i. Domain [hotel.nccoe]



Name: MANAGEMENT_WORKSTATION
Description: Management Console for Various Security Components
Device: CRYPTONITEMWS
Type: RDP
Host: cryptonite-mws.hotel.nccoe
Port: 3389
☐ Single Session Connection
☐ Allow Join with Active Session
Status Text: -
Max Idle Time: 10 0-999 Minutes (0=disabled)
Username: Manager
Password: •••••••••••••
Domain: hotel.nccoe
Security Mode: default
GATEWAYS * (1): GGATEWAY
CONSOLES * (1): CONWRKS
TAGS (0)

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



Name: Solidres
Description: VNC Connection to the PMS
Device: SOLIDRES
Type: VNC
Host: solidres.hotel.nccoe
Port: 5901
☐ Single Session Connection
☐ Allow Join with Active Session
Status Text: -
Max Idle Time: 0-999 Minutes (0=disabled)
Password: •••••••••••••
GATEWAYS * (1): GGATEWAY
CONSOLES * (1): CONWRKS
TAGS (0)

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 reference design. It is the only component that we purchased for this project. The PMS and the data it contains are enterprise resources in the ZTA.

2.3.1 Property Management System Overview

The Solidres PMS provides the back-end enterprise functionality of a hotel in the PMS reference design.

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
   ```

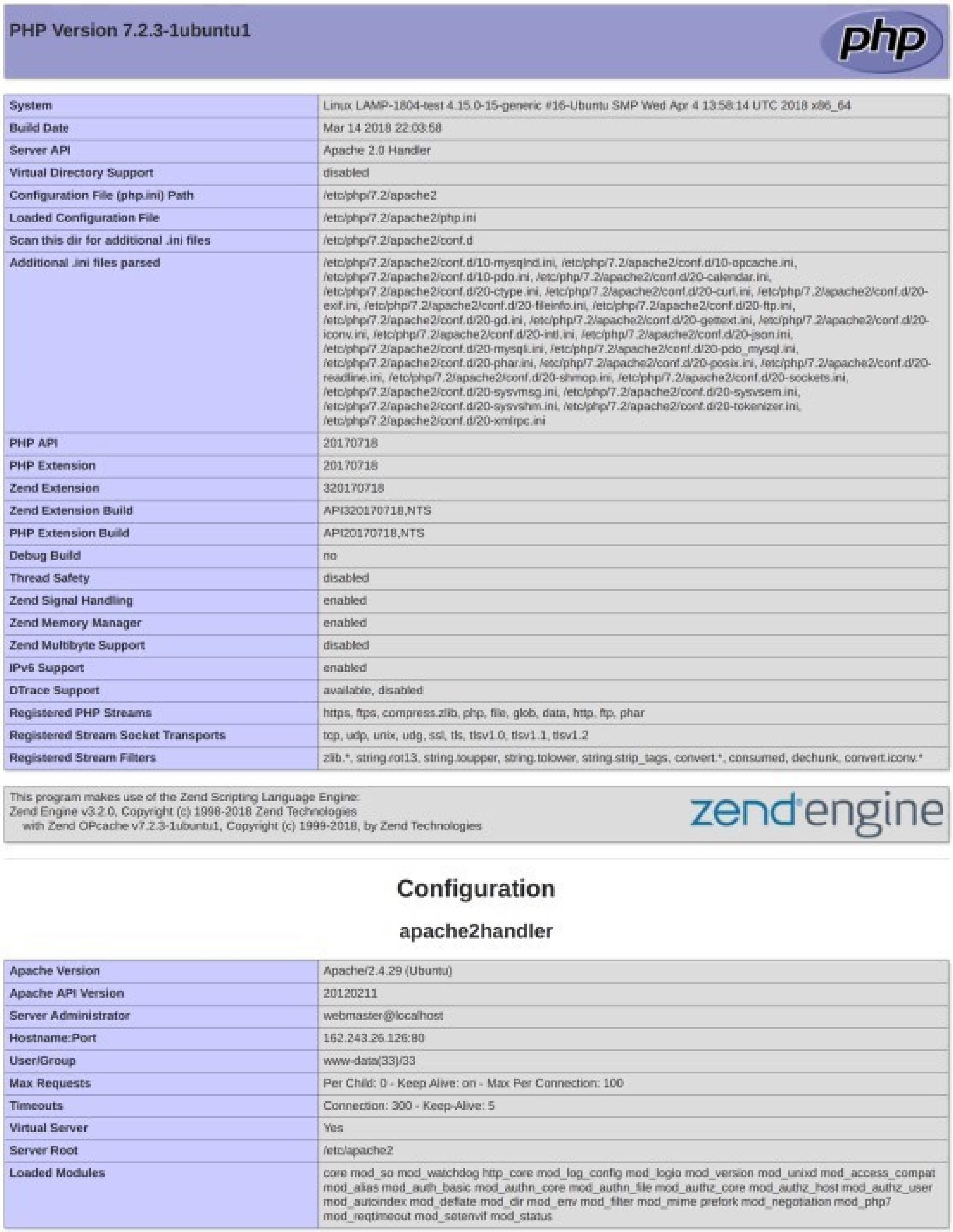
2. Run the following command to install the NGINX web server and Hypertext Preprocessor (PHP) dependencies:

   ```
   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

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

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

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

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

```
<?php

phpinfo():

?>
```

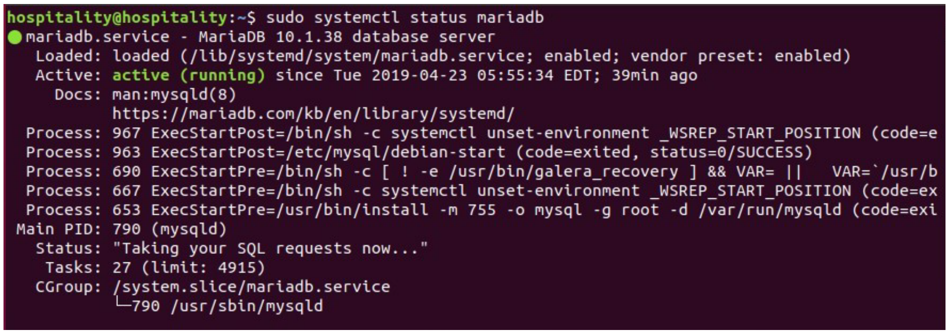
   c. Navigate a web browser to http://localhost/info.php.

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
```



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

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:

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

   b. Set root password? [Y/n]. Press **Y.**

   c. Enter a secure password twice.

   d. Remove anonymous users? [Y/n]. Press **Y.**

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

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

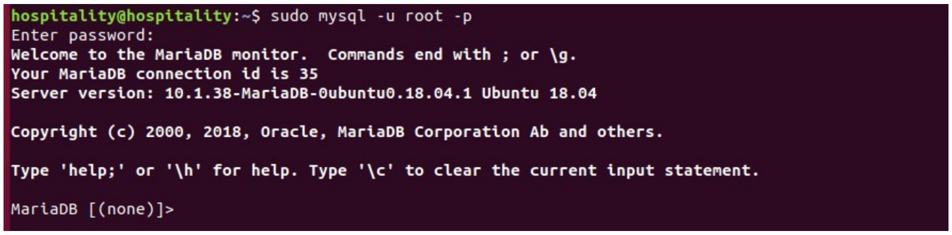
g. Reload privilege tables now? [Y/n]. Press **Y.**

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 9c 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:



```
hospitality@hospitality:~$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 35
Server version: 10.1.38-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

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;
```

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

```
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:

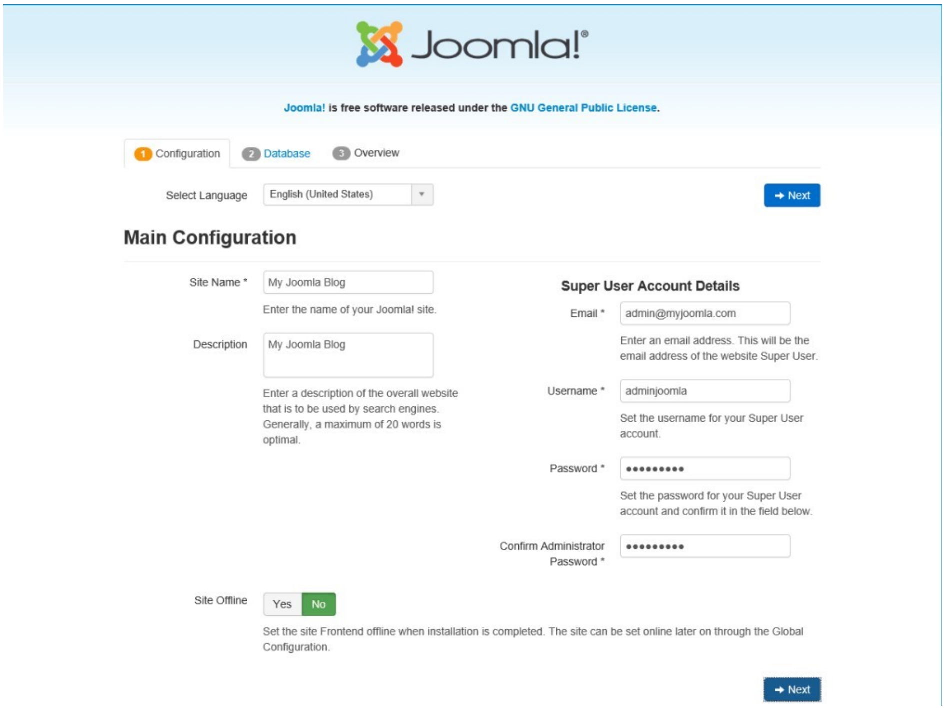
```
sudo systemctl restart nginx php7.1-fpm
```

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:**



Joomla! is free software released under the GNU General Public License.

Select Language: English (United States)

Main Configuration

Site Name *: My Joomla Blog
Enter the name of your Joomla! site.

Description: My Joomla Blog
Enter a description of the overall website that is to be used by search engines. Generally, a maximum of 20 words is optimal.

Super User Account Details

Email *: admin@myjoomla.com
Enter an email address. This will be the email address of the website Super User.

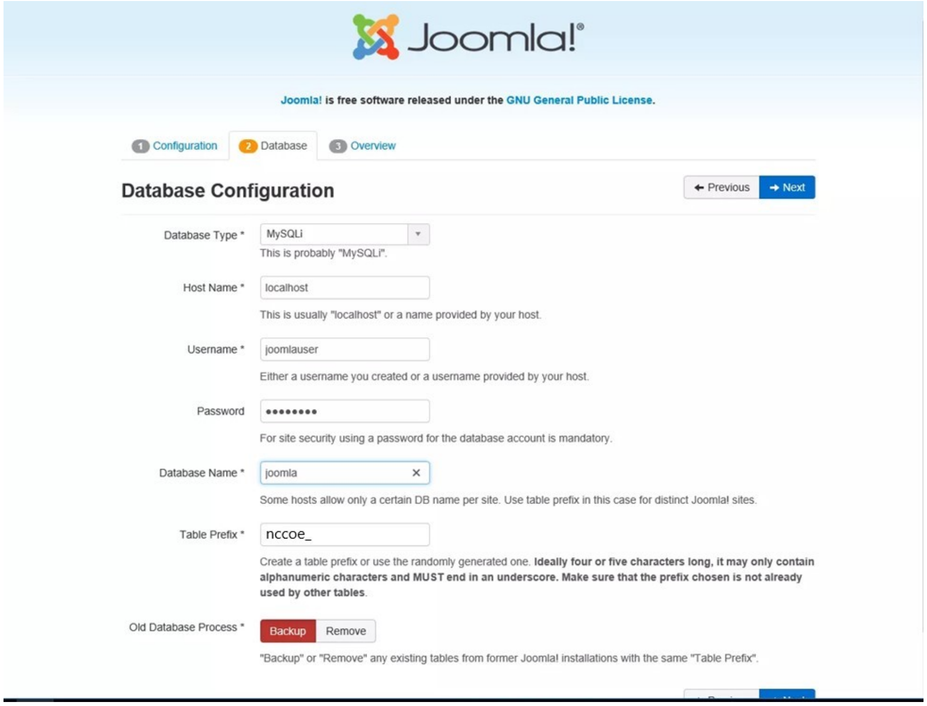
Username *: adminjoomla
Set the username for your Super User account.

Password *: •••••••••
Set the password for your Super User account and confirm it in the field below.

Confirm Administrator Password *: •••••••••

Site Offline: Yes [✓ No]
Set the site Frontend offline when installation is completed. The site can be set online later on through the Global Configuration.

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


Joomla!®
Joomla! is free software released under the GNU General Public License.
1 Configuration
2 Database
3 Overview
Previous
Next

Database Configuration

Database Type * MySQLi
This is probably "MySQLi".

Host Name * localhost
This is usually "localhost" or a name provided by your host.

Username * joomlauser
Either a username you created or a username provided by your host.

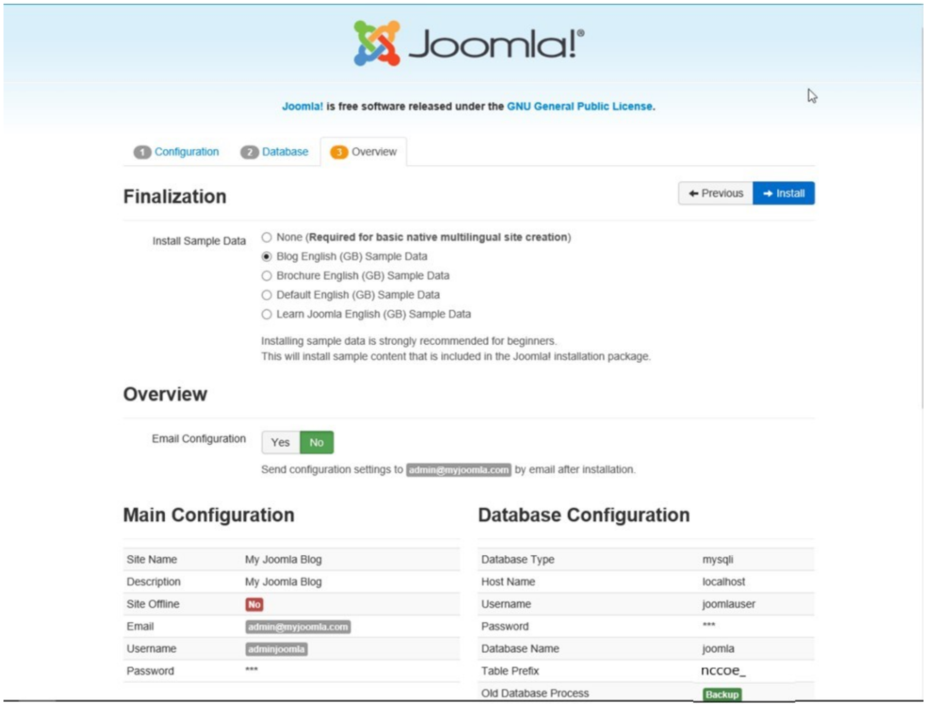
Password ••••••••
For site security using a password for the database account is mandatory.

Database Name * joomla
Some hosts allow only a certain DB name per site. Use table prefix in this case for distinct Joomla! sites.

Table Prefix * nccoe_
Create a table prefix or use the randomly generated one. **Ideally four or five characters long, it may only contain alphanumeric characters and MUST end in an underscore. Make sure that the prefix chosen is not already used by other tables.**

Old Database Process * [✓ Backup] Remove
"Backup" or "Remove" any existing tables from former Joomla! installations with the same "Table Prefix".

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


Joomla!®
Joomla! is free software released under the GNU General Public License.
1 Configuration
2 Database
3 Overview
Previous
Install

Finalization

Install Sample Data
○ None (**Required for basic native multilingual site creation**)
● Blog English (GB) Sample Data
○ Brochure English (GB) Sample Data
○ Default English (GB) Sample Data
○ Learn Joomla English (GB) Sample Data

Installing sample data is strongly recommended for beginners.
This will install sample content that is included in the Joomla! installation package.

Overview

Email Configuration Yes [✓ No]
Send configuration settings to admin@myjoomla.com by email after installation.

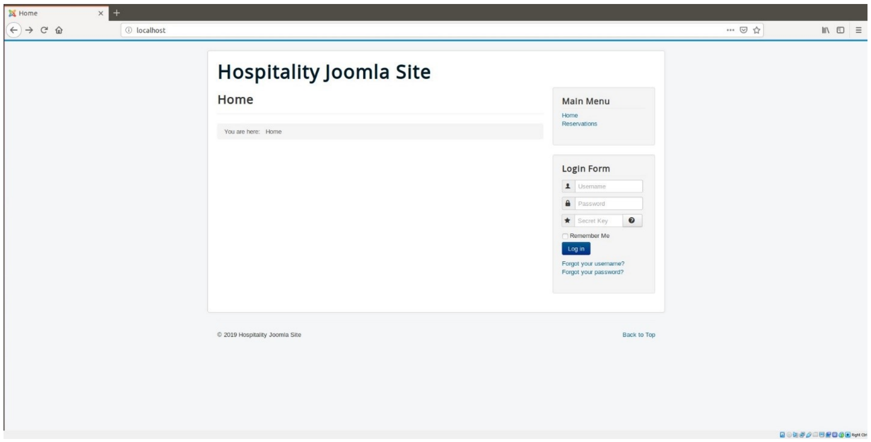
Main Configuration

Site Name	My Joomla Blog
Description	My Joomla Blog
Site Offline	No
Email	admin@myjoomla.com
Username	adminjoomla
Password	***

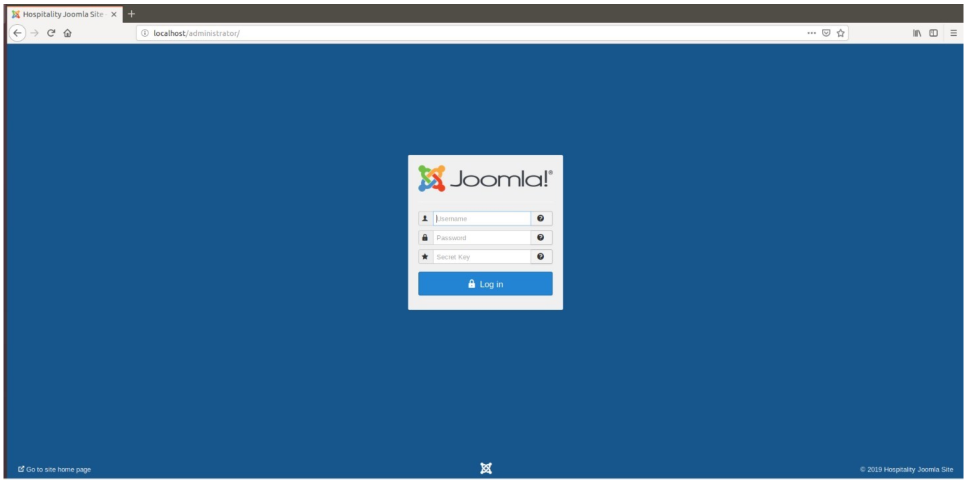
Database Configuration

Database Type	mysqli
Host Name	localhost
Username	joomlauser
Password	***
Database Name	joomla
Table Prefix	nccoe_
Old Database Process	Backup

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



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



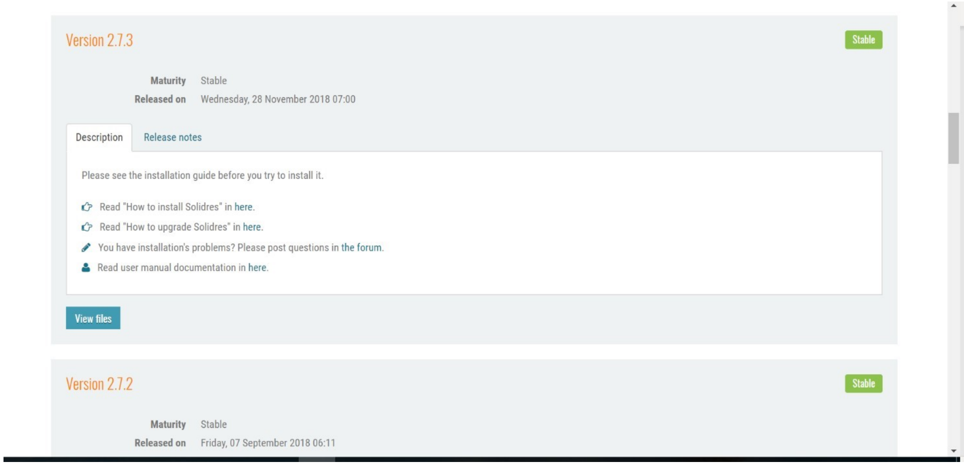
6. First, start by making sure that the system has versions of the required Solidres components that are at least as recent as the versions listed on the following Solidres website:

   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:



Version 2.7.3

Maturity Stable
Released on Wednesday, 28 November 2018 07:00

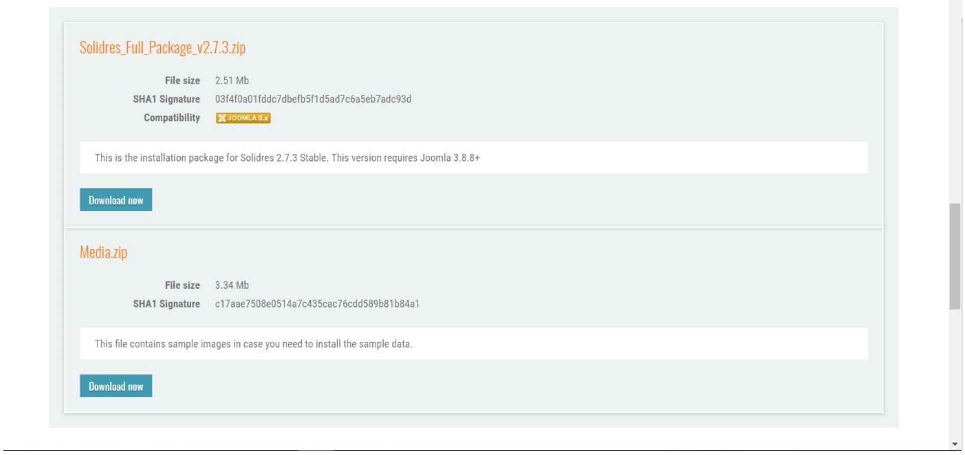
Please see the installation guide before you try to install it.

- Read "How to install Solidres" in here.
- Read "How to upgrade Solidres" in here.
- You have installation's problems? Please post questions in the forum.
- Read user manual documentation in here.

Version 2.7.2

Maturity Stable
Released on Friday, 07 September 2018 06:11

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:



Solidres_Full_Package_v2.7.3.zip

File size 2.51 Mb
SHA1 Signature 03f4f0a01fddc7dbefb5f1d5ad7c6a5eb7adc93d
Compatibility JOOMLA 3.x

This is the installation package for Solidres 2.7.3 Stable. This version requires Joomla 3.8.8+

Media.zip

File size 3.34 Mb
SHA1 Signature c17aae7508e0514a7c435cac76cdd589b81b84a1

This file contains sample images in case you need to install the sample data.

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
```

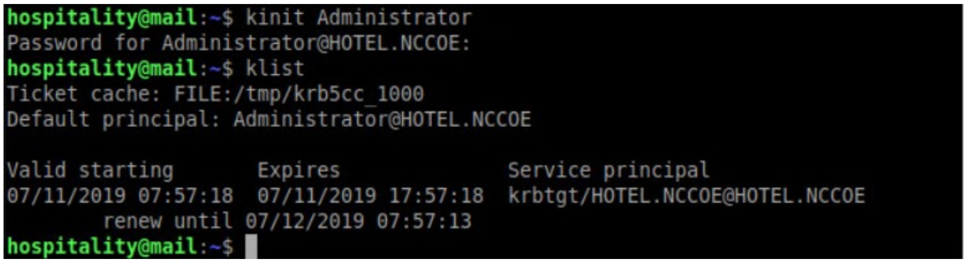
   NOTE: This may apply if the samba-common-bin back end depends on samba on your system:

```
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:



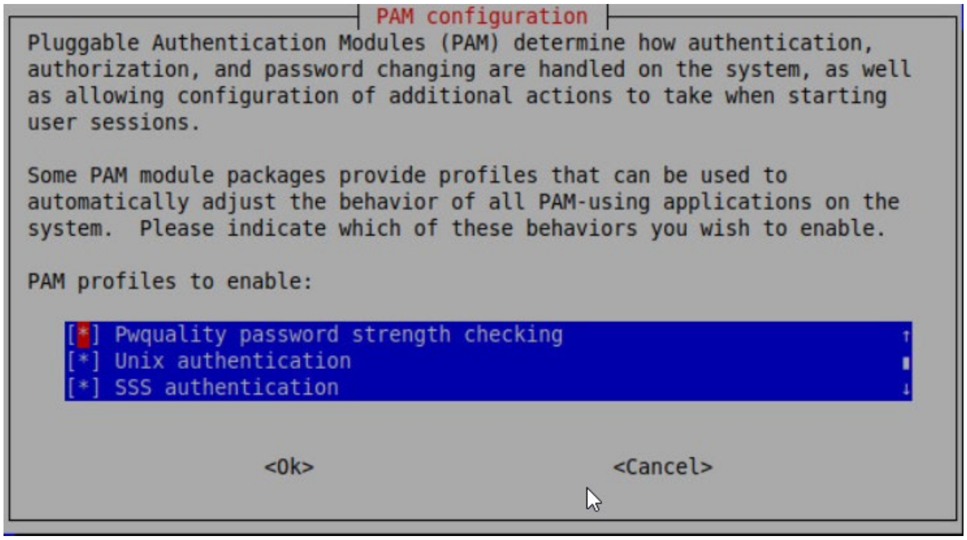
```
hospitality@mail:~$ kinit Administrator
Password for Administrator@HOTEL.NCCOE:
hospitality@mail:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: Administrator@HOTEL.NCCOE

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
```



```
PAM configuration
Pluggable Authentication Modules (PAM) determine how authentication,
authorization, and password changing are handled on the system, as well
as allowing configuration of additional actions to take when starting
user sessions.

Some PAM module packages provide profiles that can be used to
automatically adjust the behavior of all PAM-using applications on the
system.  Please indicate which of these behaviors you wish to enable.

PAM profiles to enable:

    [*] Pwquality password strength checking
    [*] Unix authentication
    [*] SSS authentication
```

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 Tellaro Appliance

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. The StrongKey vault and the credit card data it contains are enterprise resources in the ZTA.

2.4.1 Data Tokenization Appliance–StrongKey–Overview

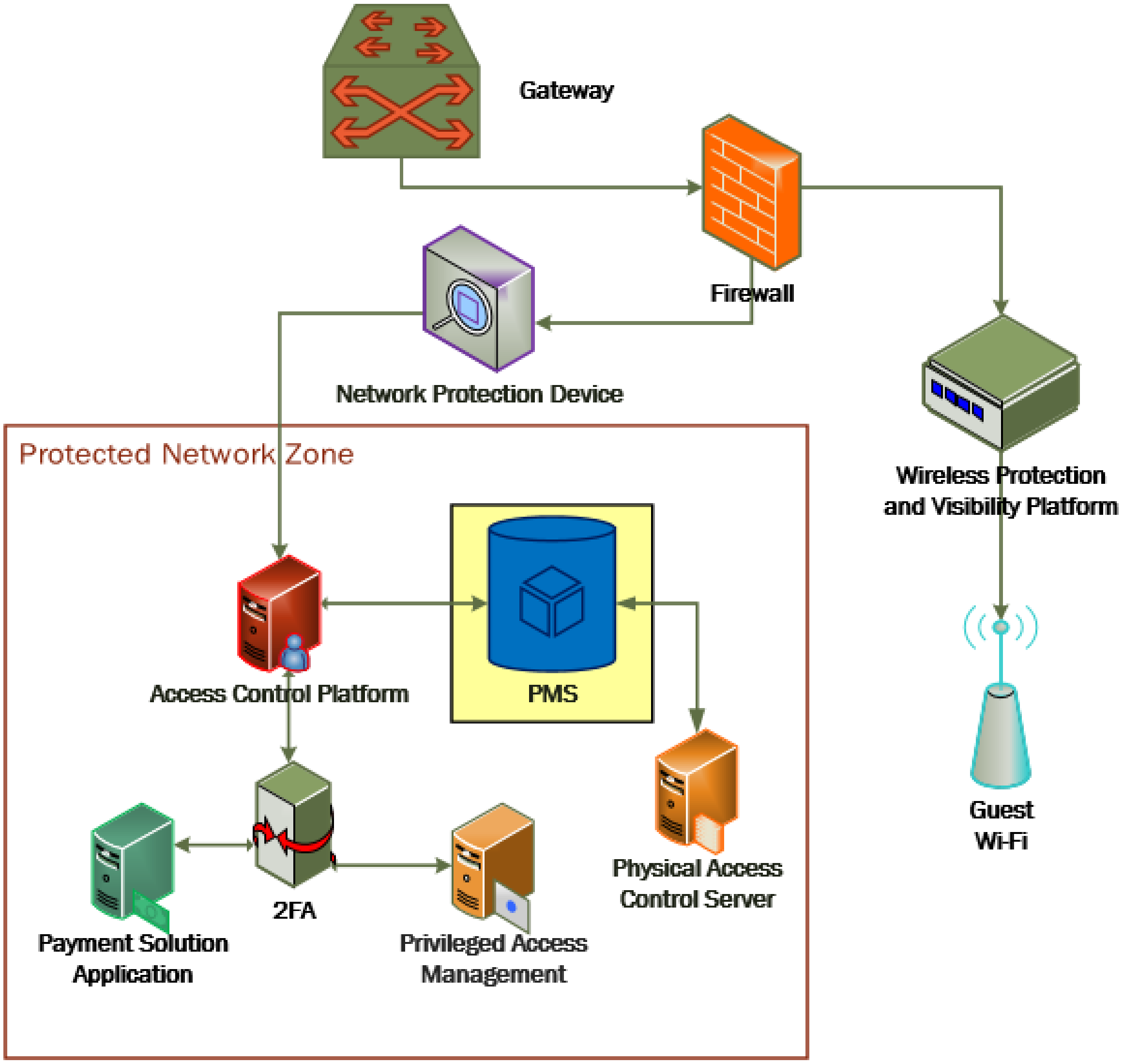
The data tokenization appliance from StrongKey performs tokenization and secure storage in the PMS reference design.

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 Figure 2-3 below.

Figure 2-3 Data Tokenization Appliance in the Reference Architecture


Gateway
Firewall
Network Protection Device
Wireless Protection and Visibility Platform
Protected Network Zone
Access Control Platform
PMS
Physical Access Control Server
Guest Wi-Fi
2FA
Payment Solution Application
Privileged Access Management

2.4.2 Data Tokenization Appliance–StrongKey–Requirements

The following subsections document the software, hardware, and network requirements for the data 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://uploads-ssl.webflow.com/5f6d3df5a0fd5f37d95b79a6/6010468e3216552d3eca3d18_KA_Demo_Client_Guide.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 StrongAuth tokenization suite and modified the offline card of Solidres. In our reference design 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 and represents an Asset and an Enterprise resource in a ZTA.

2.5.1 Physical Access Control System–Häfele Dialock–Overview

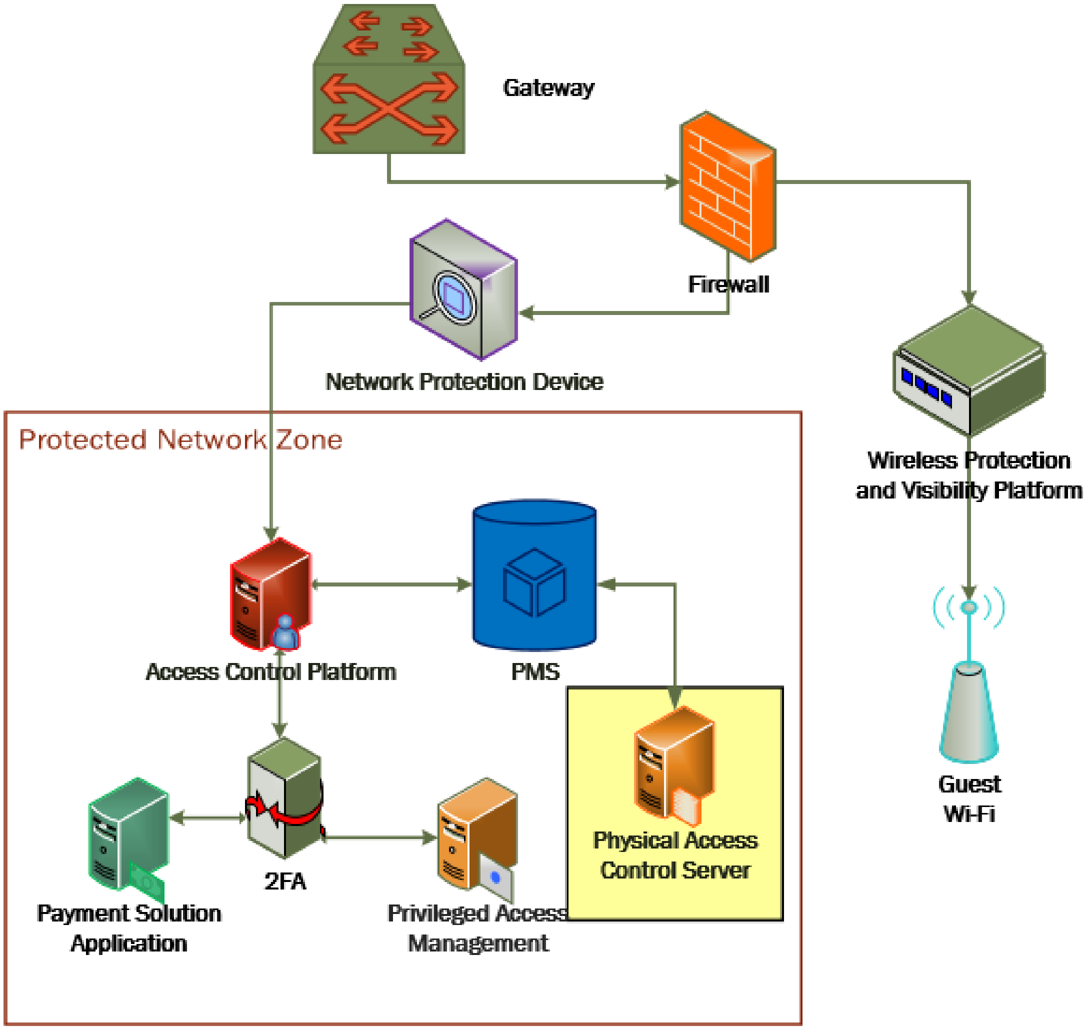
The physical access control system from Häfele provides the physical access systems and the means to administer them in the PMS reference design.

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.

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


Gateway
Firewall
Network Protection Device
Wireless Protection and Visibility Platform
Protected Network Zone
Access Control Platform
PMS
Guest Wi-Fi
2FA
Payment Solution Application
Privileged Access Management
Physical Access Control Server

2.5.2 Physical Access Control System–Häfele Dialock–Requirements

The following subsections document the software, hardware, and network requirements for the physical 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:

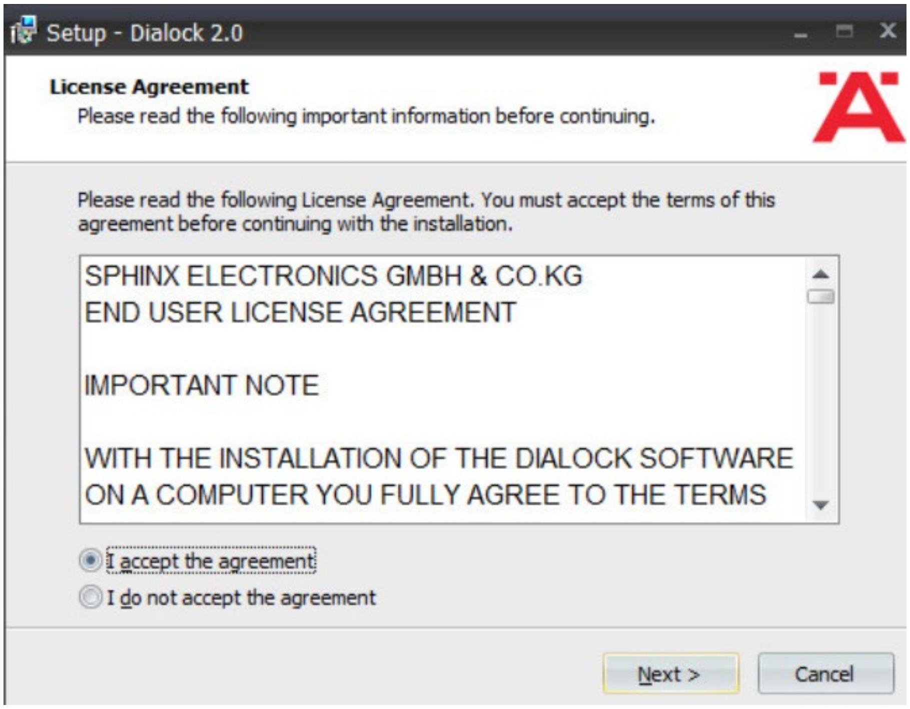
1. Run the installation media on the back-end server.
2. Log in to the web portal to change the password and apply a license.
3. Add the encoding station to the back-end server.
4. Add the MDU to the back-end server.
5. Set up a guest room and a physical access control area.
6. Provision access to terminals.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

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

2.5.4 Server Installation

1. Run the installation media.

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



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

SPHINX ELECTRONICS GMBH & CO.KG
END USER LICENSE AGREEMENT

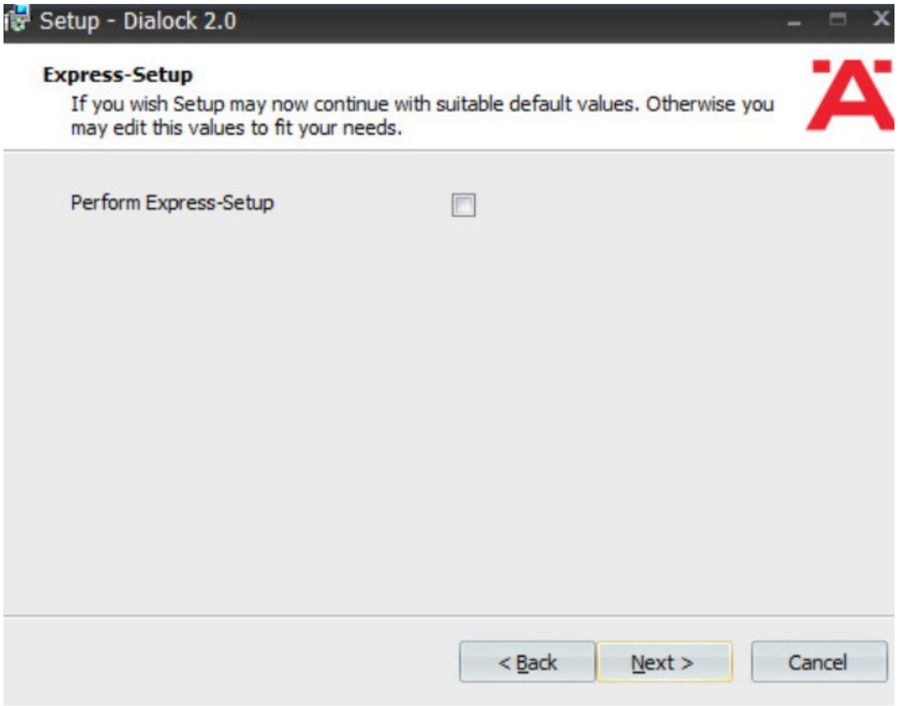
IMPORTANT NOTE

WITH THE INSTALLATION OF THE DIALOCK SOFTWARE ON A COMPUTER YOU FULLY AGREE TO THE TERMS

● I accept the agreement
○ I do not accept the agreement

3. Click **Next.**

4. Uncheck Perform Express-Setup:



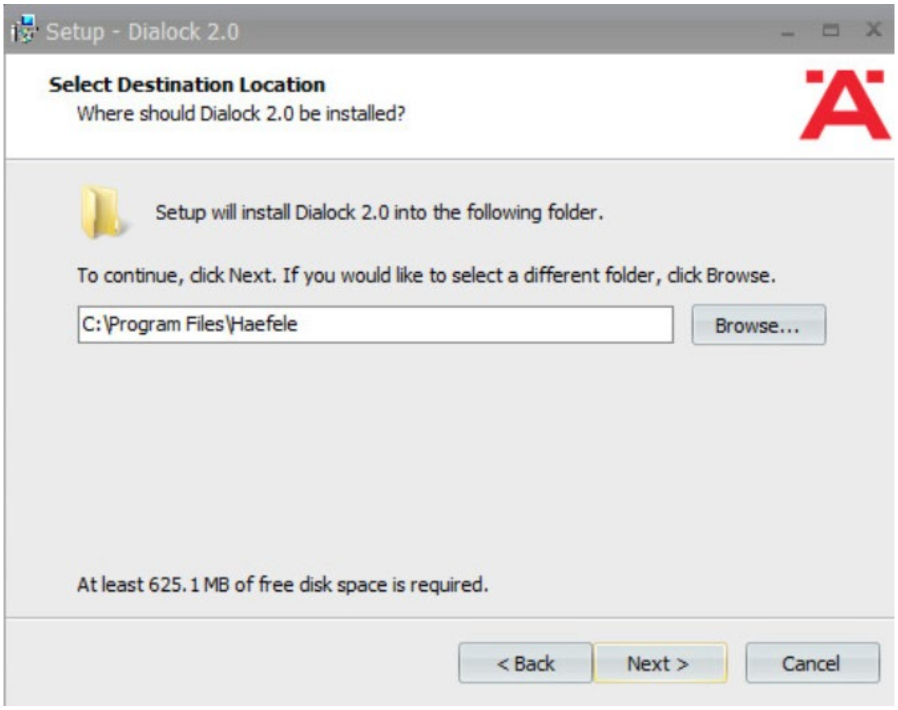
Setup - Dialock 2.0

Express-Setup

If you wish Setup may now continue with suitable default values. Otherwise you may edit this values to fit your needs.

Perform Express-Setup □

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



Setup - Dialock 2.0

Select Destination Location

Where should Dialock 2.0 be installed?

Setup will install Dialock 2.0 into the following folder.

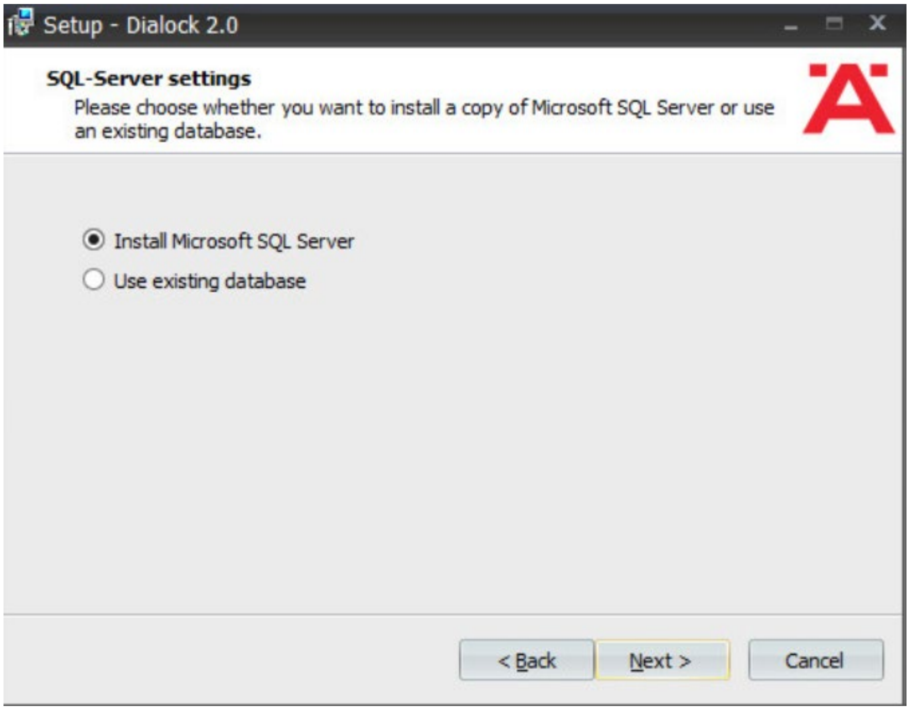
To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Haefele

At least 625.1 MB of free disk space is required.

7. Click **Next.**

8. If you wish to utilize an existing database, select **Use existing database.** Otherwise, leave Install Microsoft SQL Server selected:



SQL-Server settings

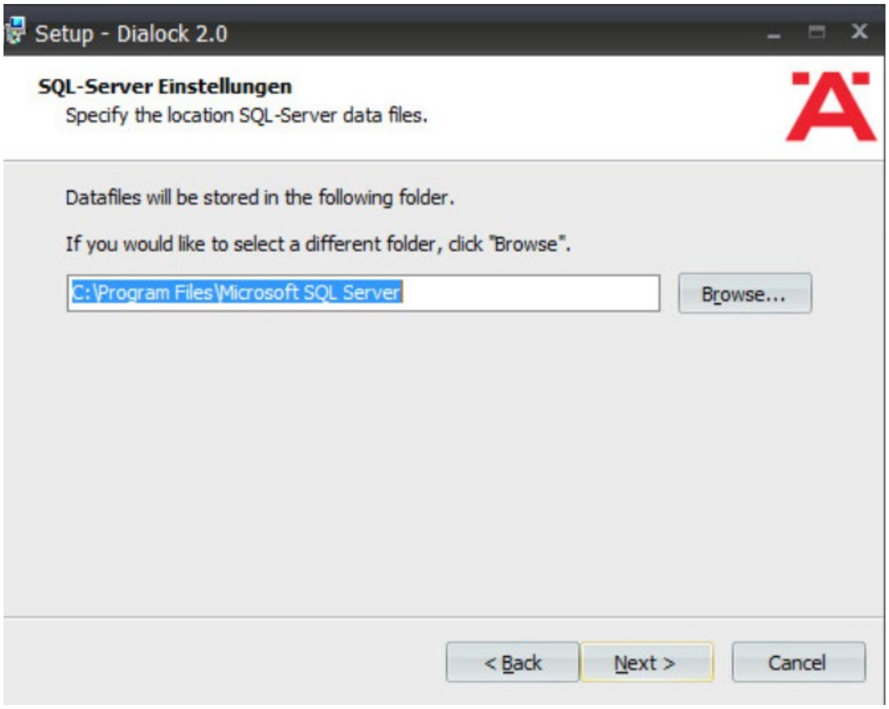
Please choose whether you want to install a copy of Microsoft SQL Server or use an existing database.

● Install Microsoft SQL Server

○ Use existing database

9. Click **Next.**

10. Change the installation directory for Microsoft SQL Server if desired:



Setup - Dialock 2.0

SQL-Server Einstellungen

Specify the location SQL-Server data files.

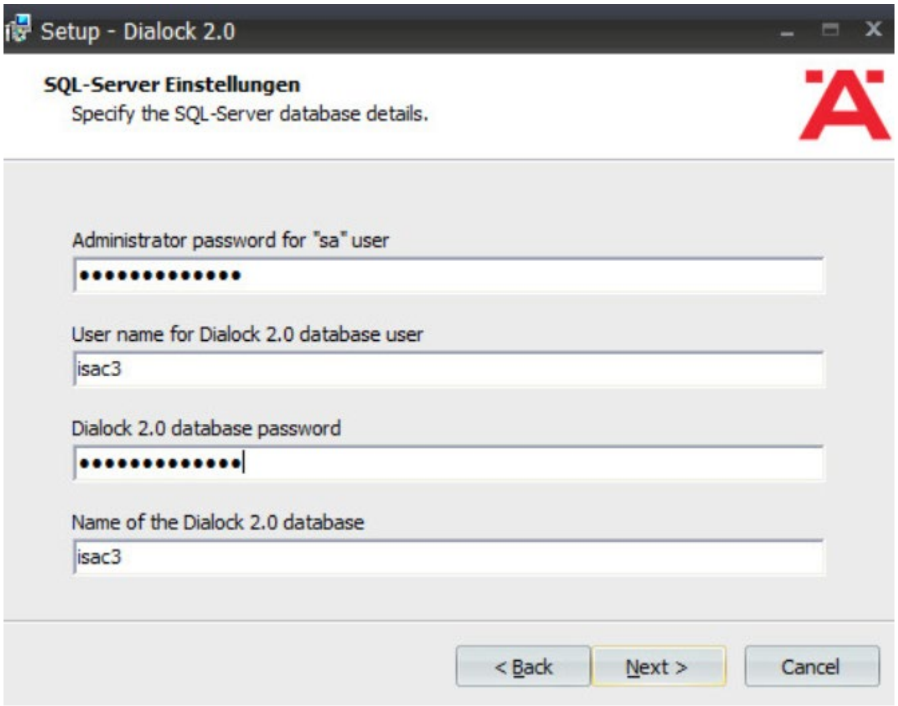
Datafiles will be stored in the following folder.

If you would like to select a different folder, click "Browse".

C:\Program Files\Microsoft SQL Server

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:



SQL-Server Einstellungen

Specify the SQL-Server database details.

Administrator password for "sa" user

••••••••••••••

User name for Dialock 2.0 database user

isac3

Dialock 2.0 database password

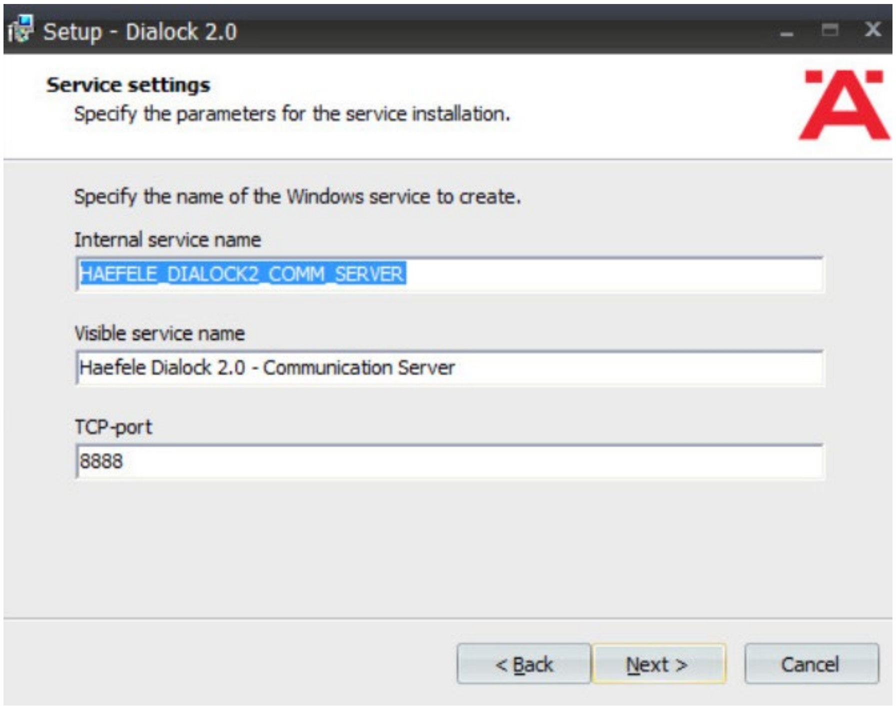
••••••••••••••

Name of the Dialock 2.0 database

isac3

13. Click **Next.**

14. Change the communication server service information if desired:



Service settings

Specify the parameters for the service installation.

Specify the name of the Windows service to create.

Internal service name

HAEFELE_DIALOCK2_COMM_SERVER

Visible service name

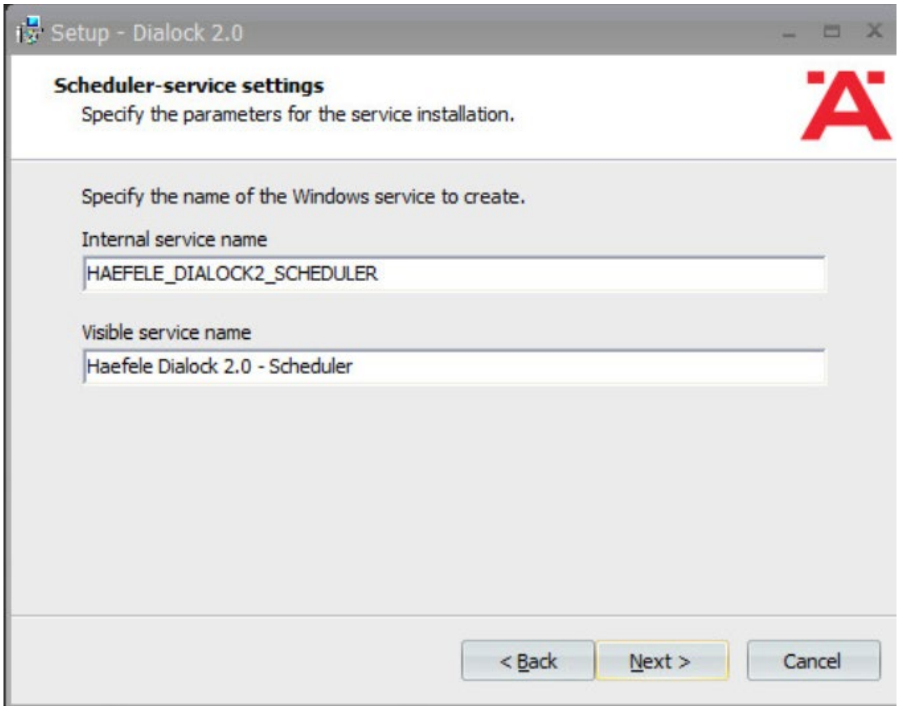
Haefele Dialock 2.0 - Communication Server

TCP-port

8888

15. Click **Next.**

16. Change the schedule service information if desired.



Scheduler-service settings

Specify the parameters for the service installation.

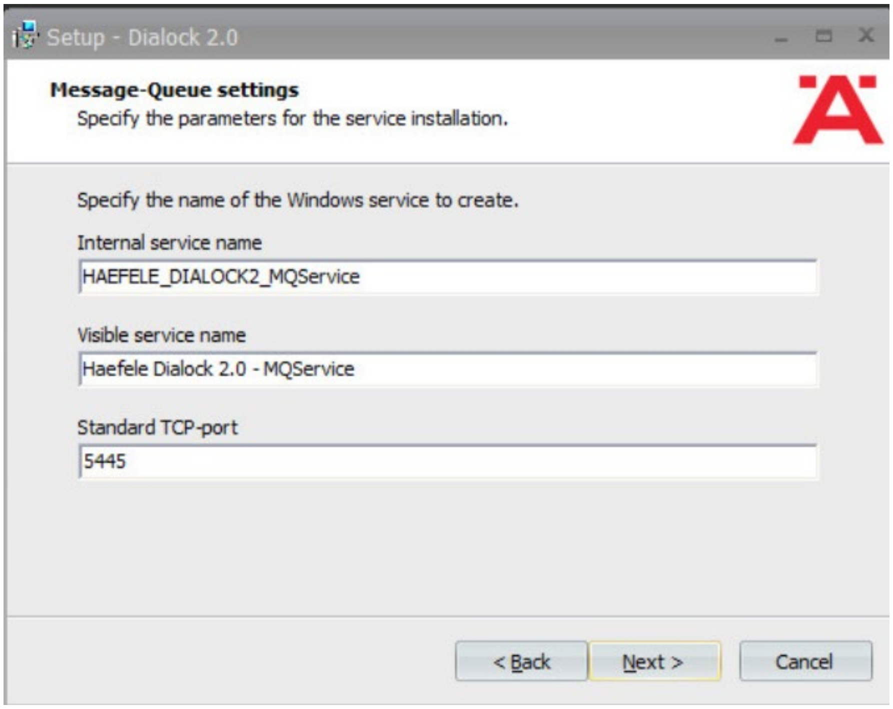
Specify the name of the Windows service to create.

Internal service name: HAEFELE_DIALOCK2_SCHEDULER

Visible service name: Haefele Dialock 2.0 - Scheduler

17. Click **Next.**

18. Change the message queue service information if desired:



Message-Queue settings

Specify the parameters for the service installation.

Specify the name of the Windows service to create.

Internal service name

HAEFELE_DIALOCK2_MQService

Visible service name

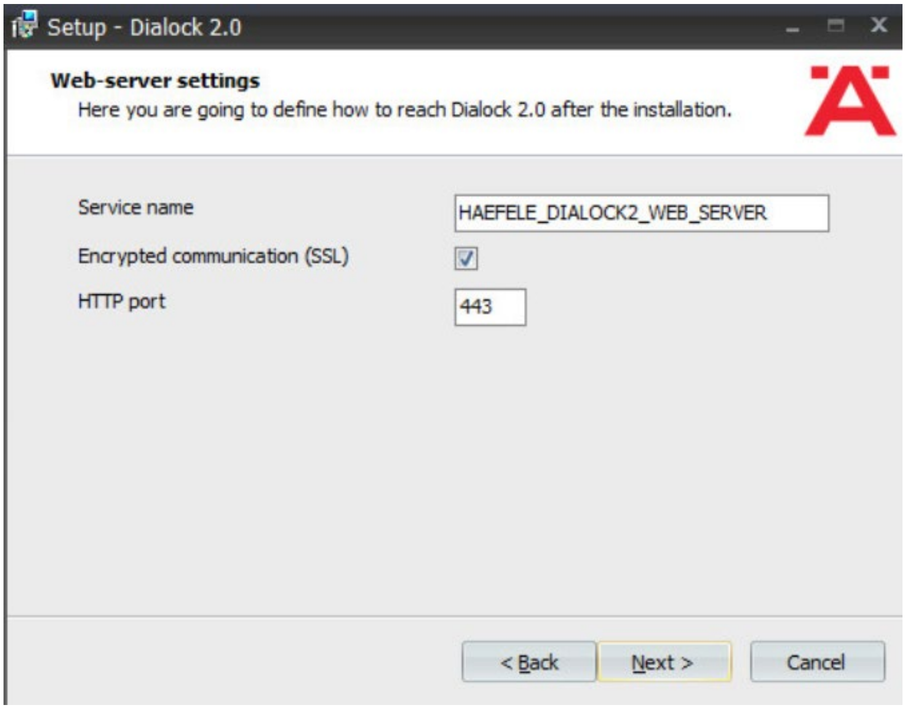
Haefele Dialock 2.0 - MQService

Standard TCP-port

5445

19. Click **Next.**

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



Web-server settings

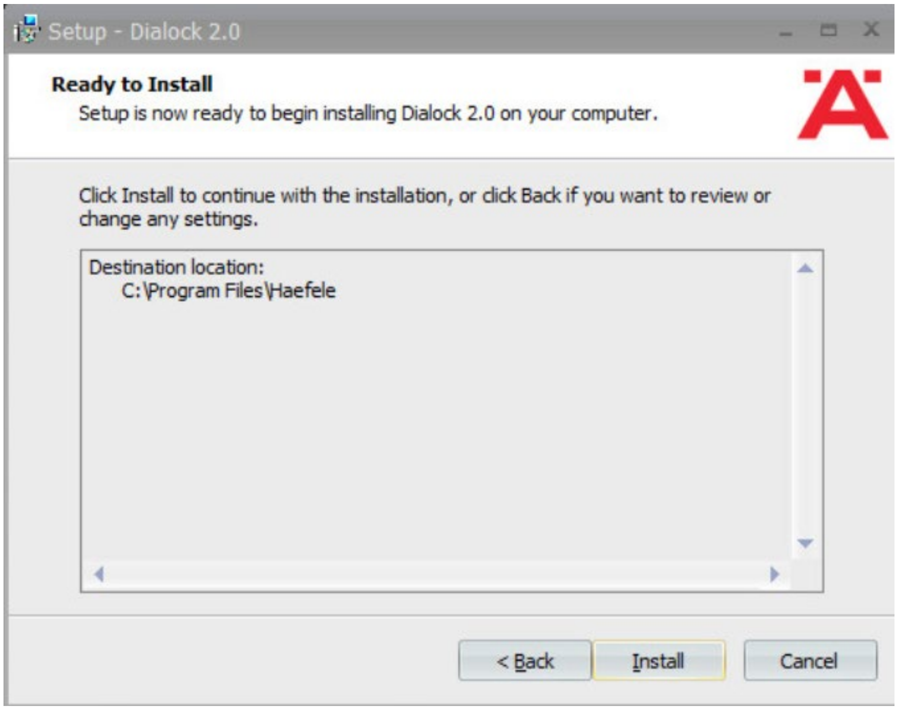
Here you are going to define how to reach Dialock 2.0 after the installation.

Service name: HAEFELE_DIALOCK2_WEB_SERVER

Encrypted communication (SSL): ☑

HTTP port: 443

21. Click **Next:**



Ready to Install

Setup is now ready to begin installing Dialock 2.0 on your computer.

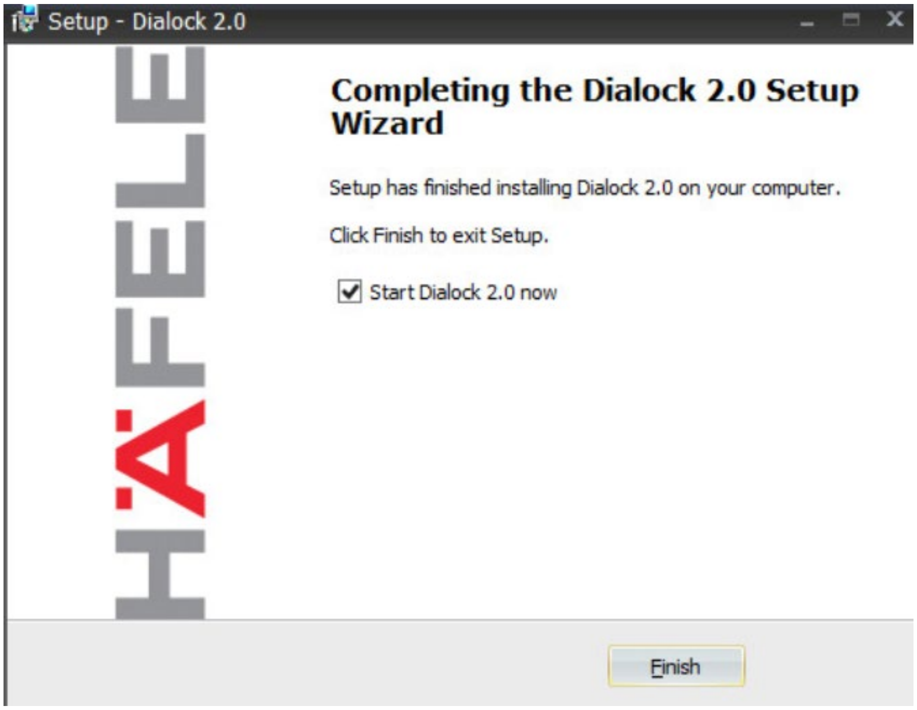
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files\Haefele

22. Click Install.

23. Wait for the installation to complete.

24. Verify that “Start Dialock 2.0 now” is checked:



Completing the Dialock 2.0 Setup Wizard

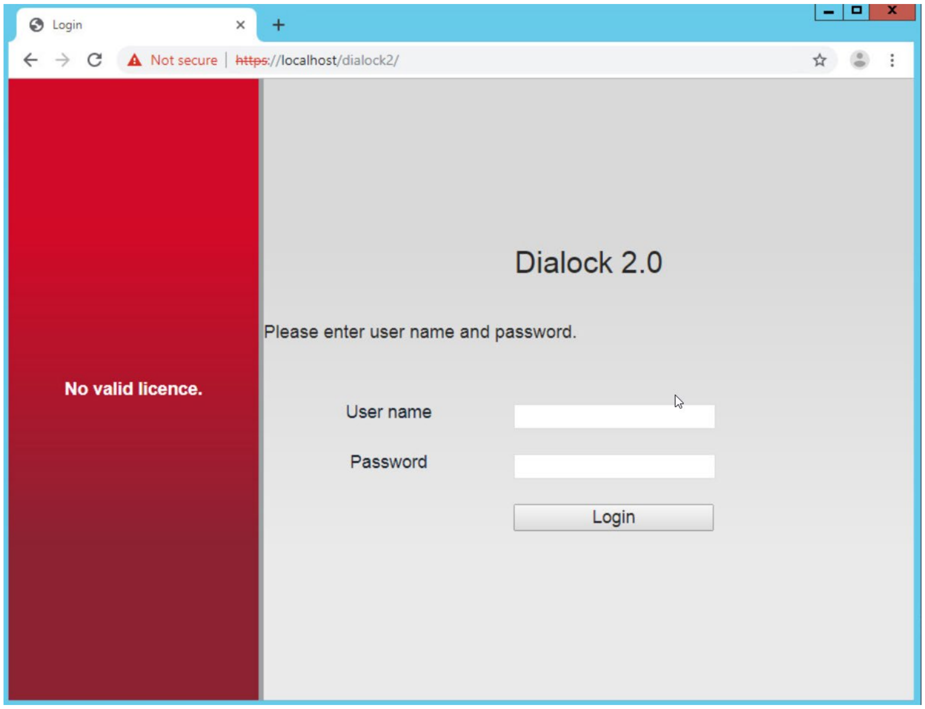
Setup has finished installing Dialock 2.0 on your computer.

Click Finish to exit Setup.

☑ Start Dialock 2.0 now

25. Click **Finish.**

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



Dialock 2.0

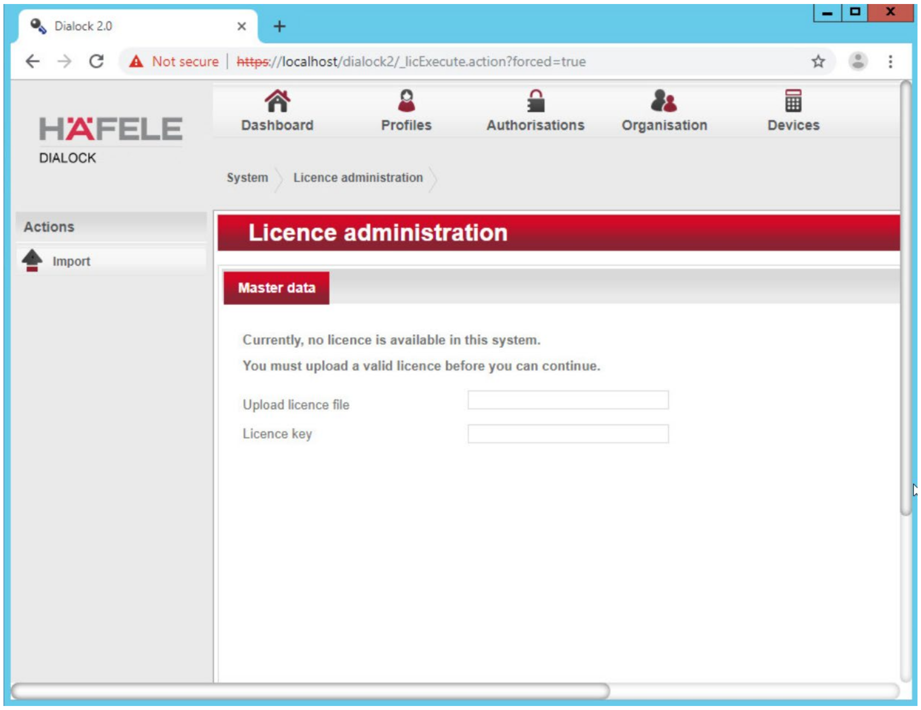
Please enter user name and password.

No valid licence.

User name

Password

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



Licence administration

Master data

Currently, no licence is available in this system.

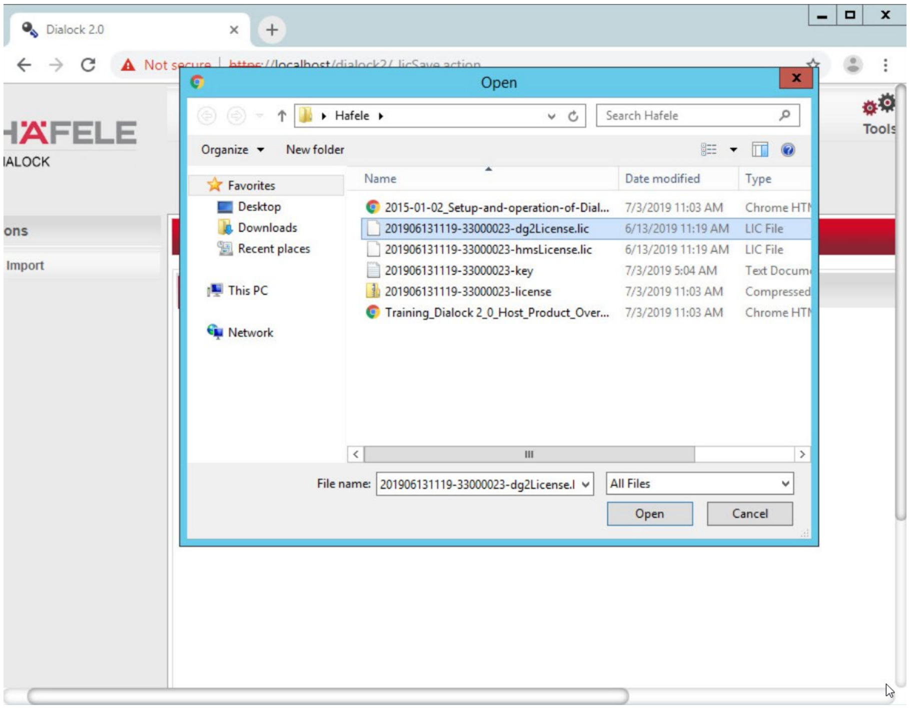
You must upload a valid licence before you can continue.

Upload licence file

Licence key

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

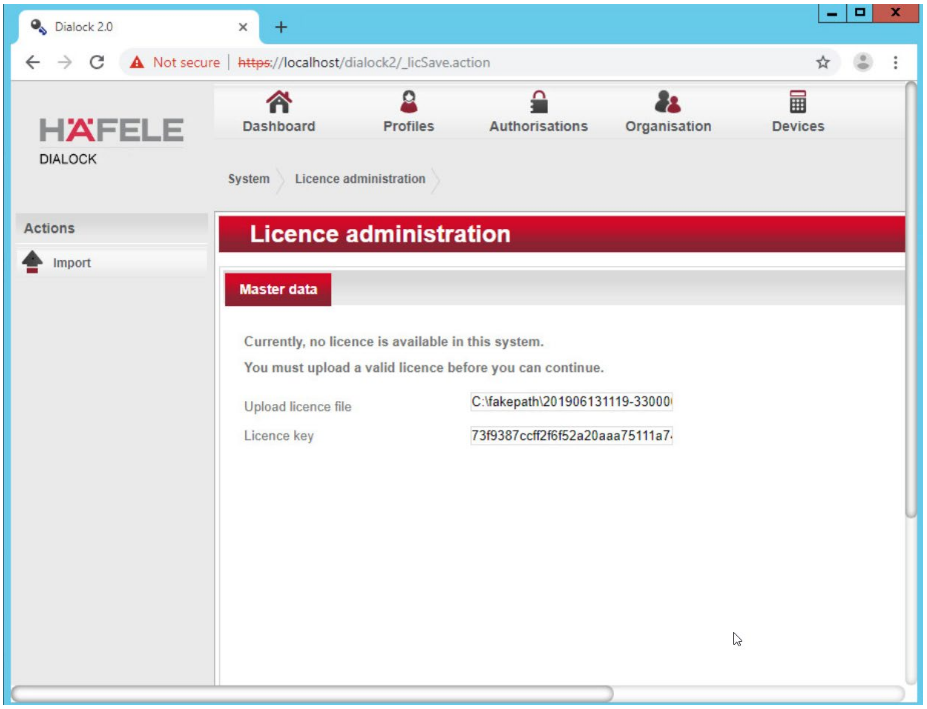
29. Locate the license file for dialock2 and click **Open:**



Name	Date modified	Type
2015-01-02_Setup-and-operation-of-Dial...	7/3/2019 11:03 AM	Chrome HTI
201906131119-33000023-dg2License.lic	6/13/2019 11:19 AM	LIC File
201906131119-33000023-hmsLicense.lic	6/13/2019 11:19 AM	LIC File
201906131119-33000023-key	7/3/2019 5:04 AM	Text Docum
201906131119-33000023-license	7/3/2019 11:03 AM	Compressed
Training_Dialock 2_0_Host_Product_Over...	7/3/2019 11:03 AM	Chrome HTI

File name: 201906131119-33000023-dg2License.l

30. Input the provided license key:



Licence administration

Master data

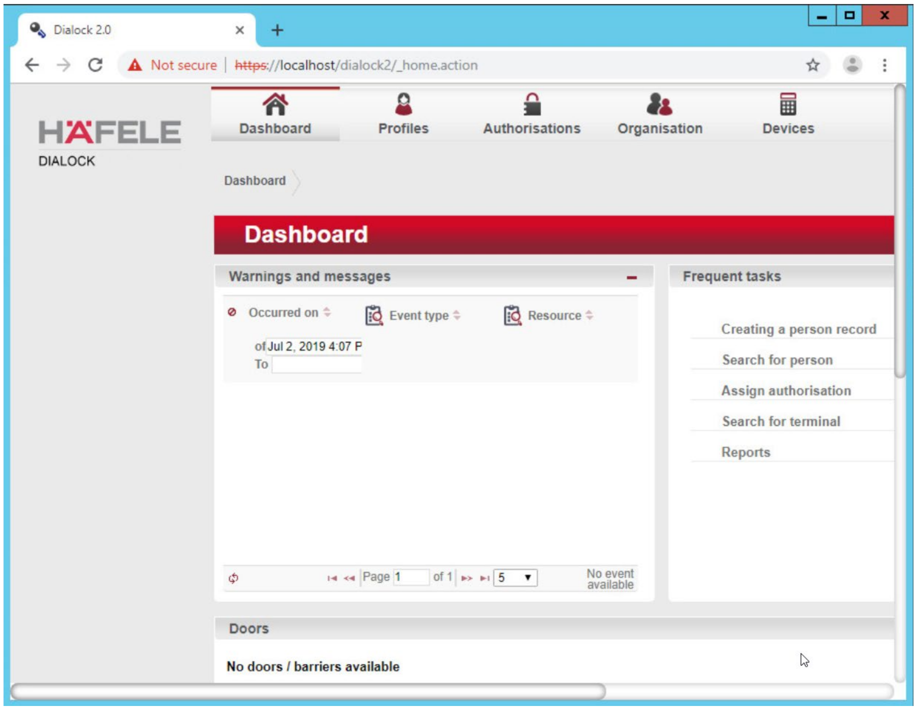
Currently, no licence is available in this system.

You must upload a valid licence before you can continue.

Upload licence file C:\fakepath\201906131119-33000

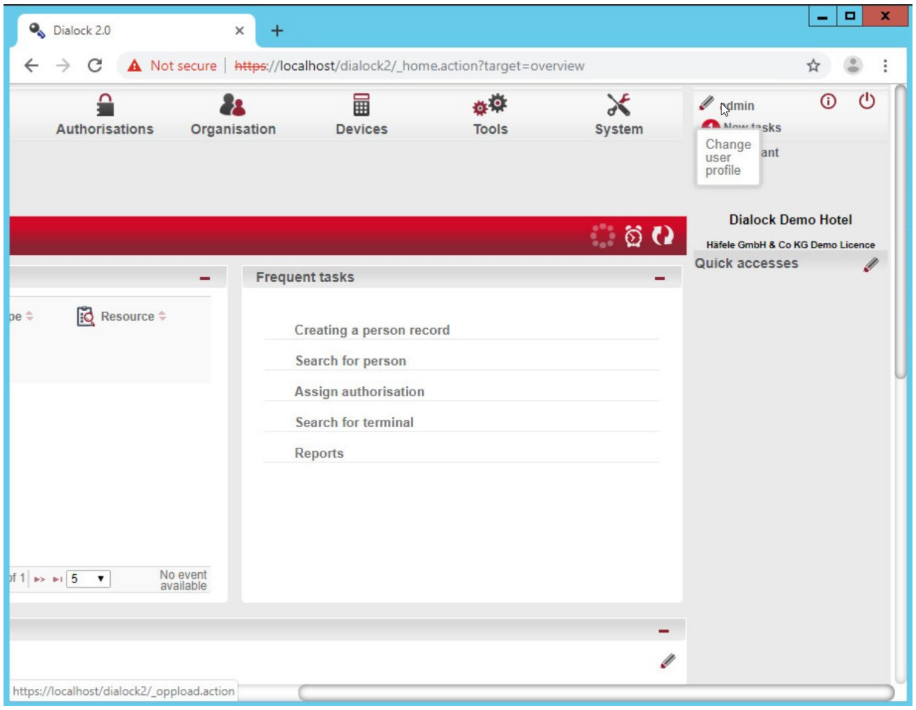
Licence key 73f9387ccff2f6f52a20aaa75111a7

31. Click **Import:**



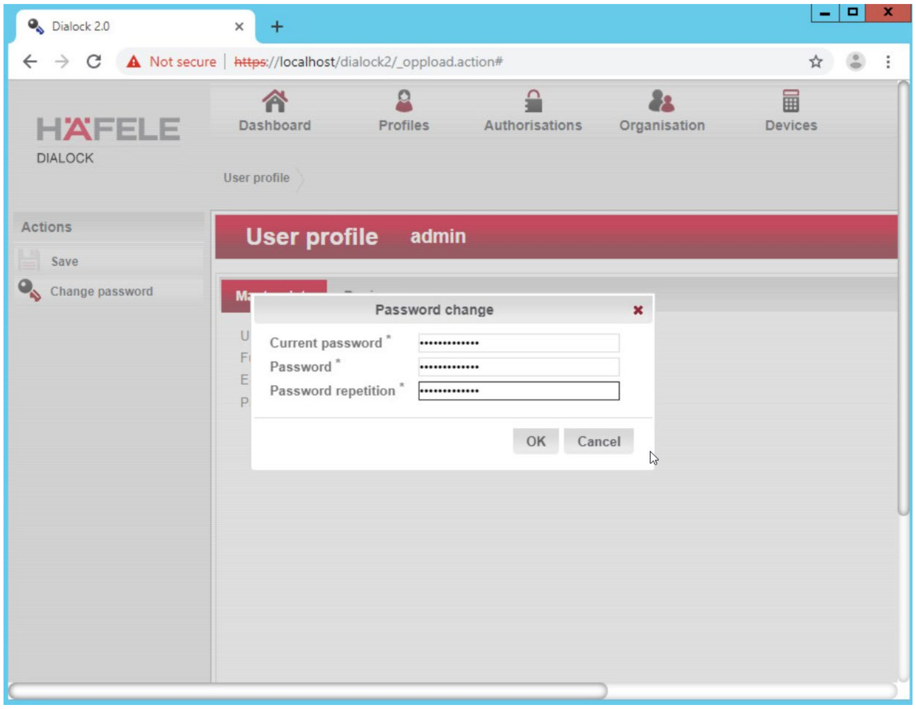
No doors / barriers available

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:



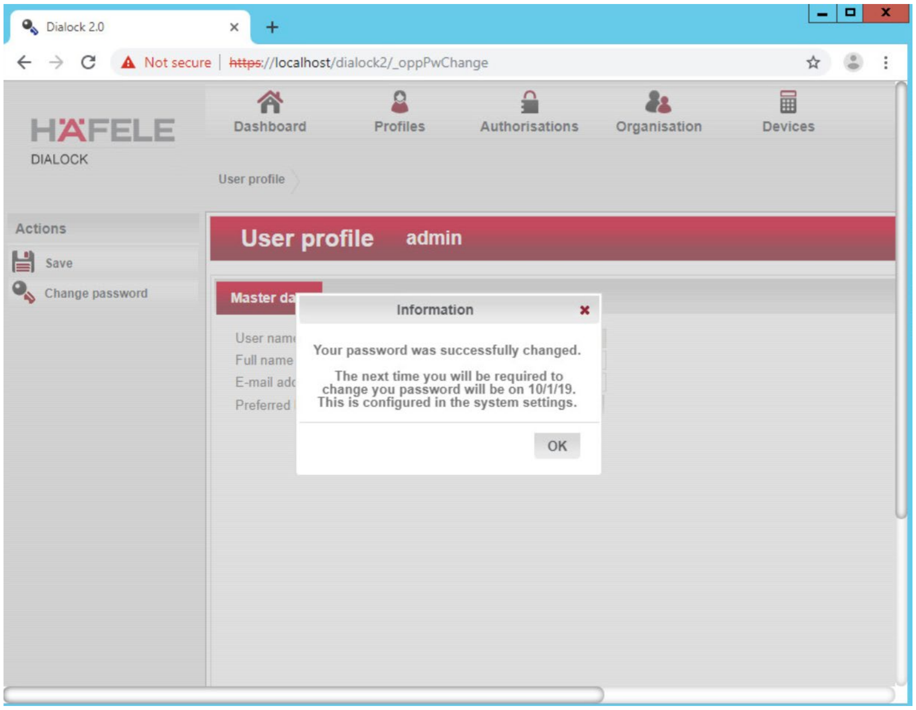
Password change

Current password * ••••••••••••••

Password * ••••••••••••••

Password repetition * ••••••••••••••

35. Click **OK:**



Information

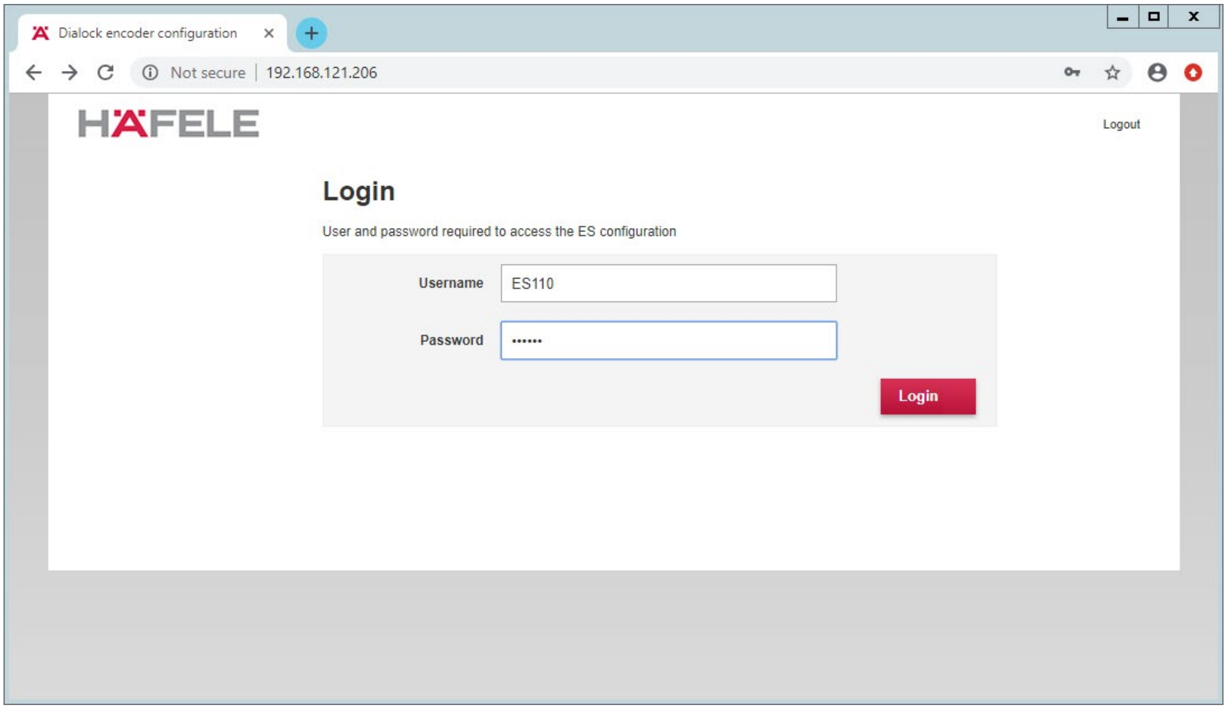
Your password was successfully changed.

The next time you will be required to change you password will be on 10/1/19. This is configured in the system settings.

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.



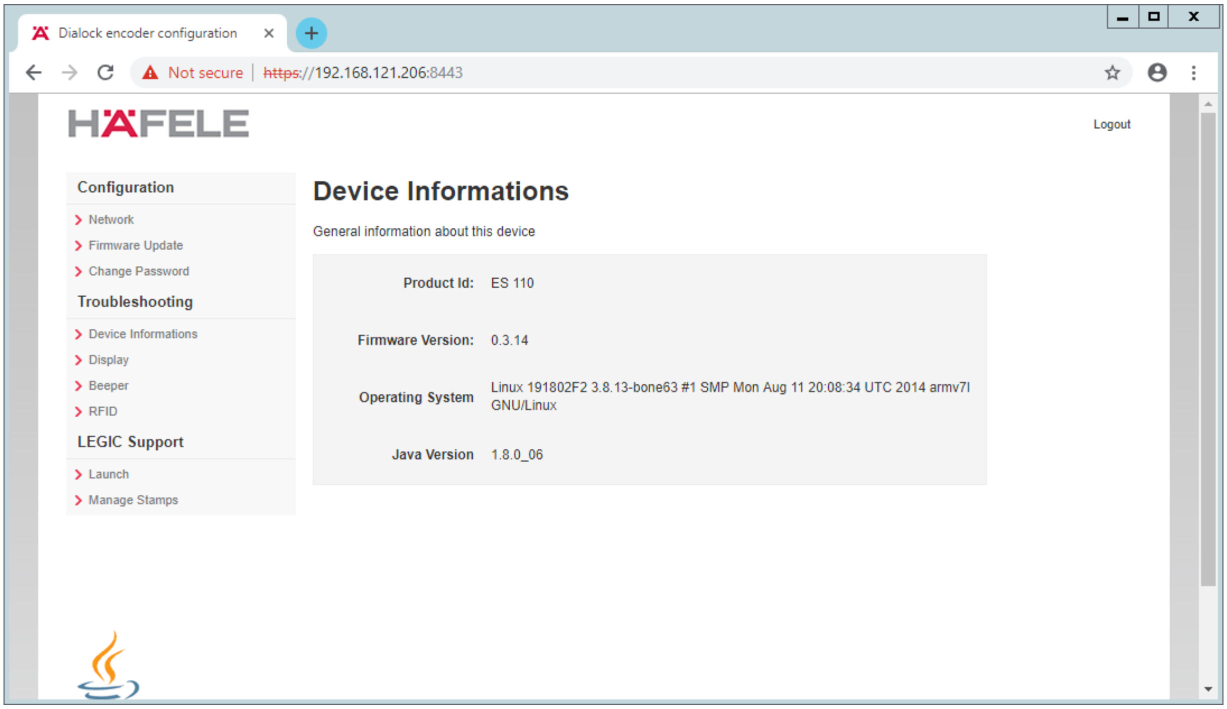
Login

User and password required to access the ES configuration

Username: ES110

Password: ••••••

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



Device Informations

General information about this device

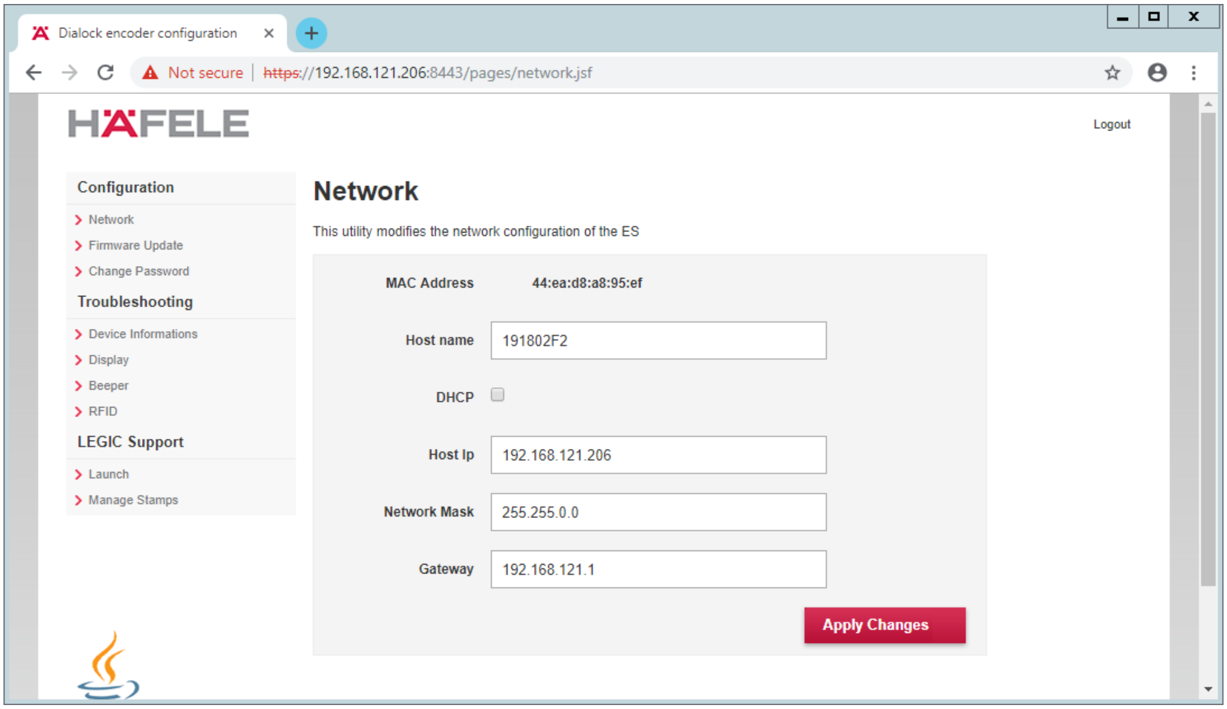
Product Id: ES 110

Firmware Version: 0.3.14

Operating System Linux 191802F2 3.8.13-bone63 #1 SMP Mon Aug 11 20:08:34 UTC 2014 armv7l GNU/Linux

Java Version 1.8.0_06

6. Select **Network:**



Network

This utility modifies the network configuration of the ES

MAC Address 44:ea:d8:a8:95:ef

Host name 191802F2

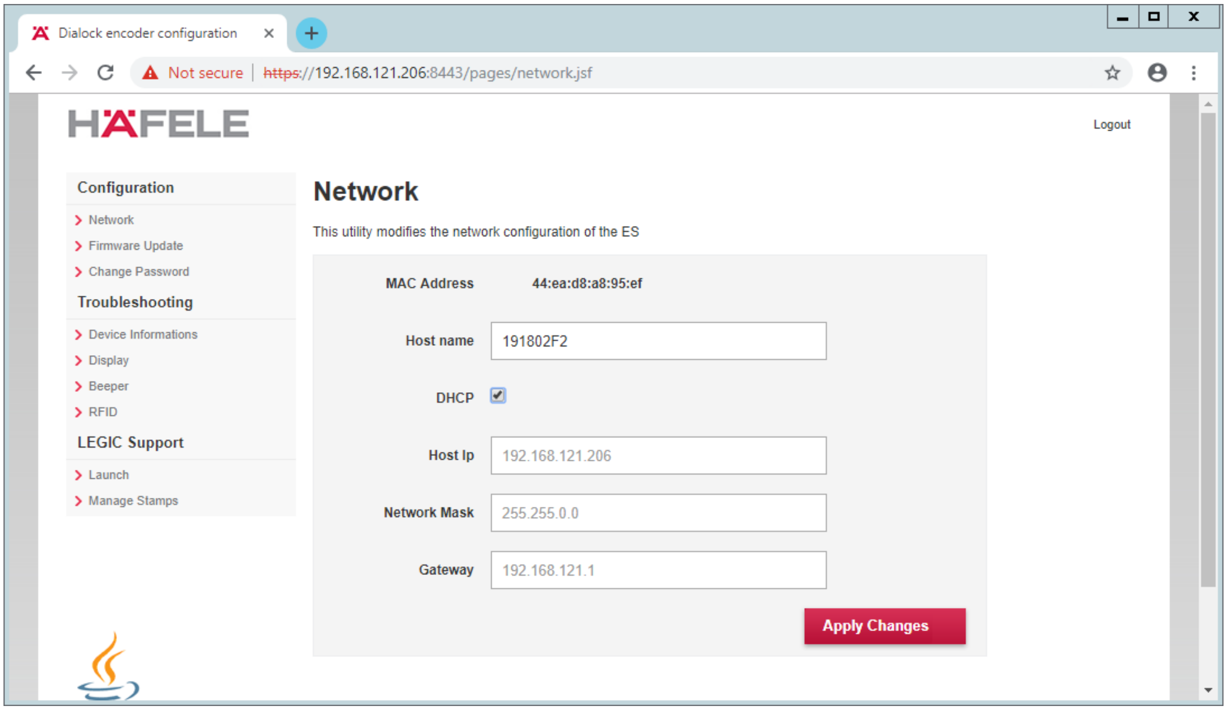
DHCP □

Host Ip 192.168.121.206

Network Mask 255.255.0.0

Gateway 192.168.121.1

7. Check **DHCP:**



Network

This utility modifies the network configuration of the ES

MAC Address 44:ea:d8:a8:95:ef

Host name 191802F2

DHCP ☑

Host Ip 192.168.121.206

Network Mask 255.255.0.0

Gateway 192.168.121.1

8. Click **Apply Changes.**

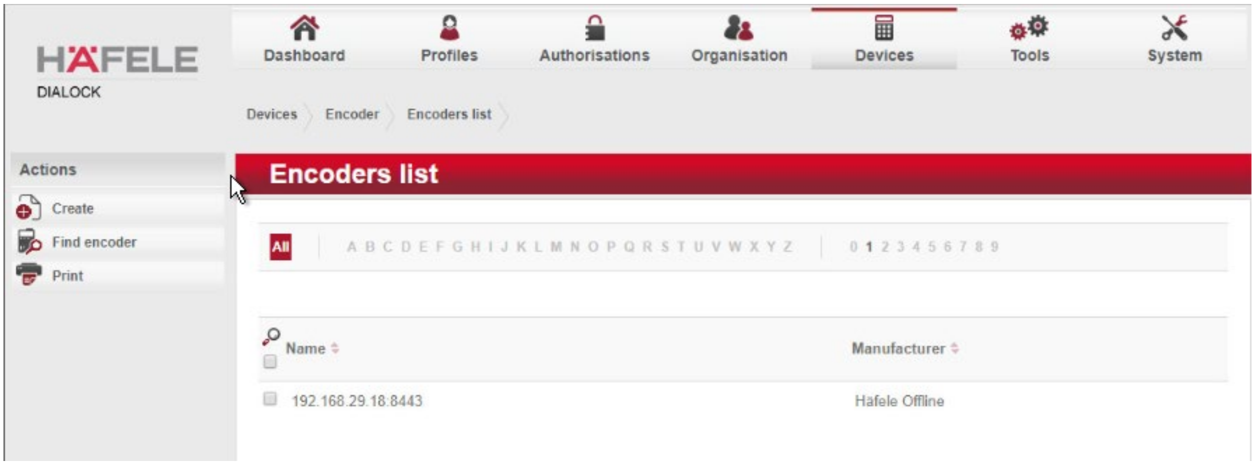
9. The new IP address should be visible on the encoding station device.

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.

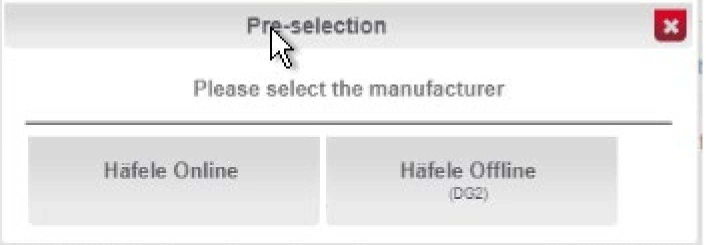
2. From there, you will see a menu titled **Encoders list.** If you see your networked device as shown below, you can proceed to the next step. If not, continue following the instructions.



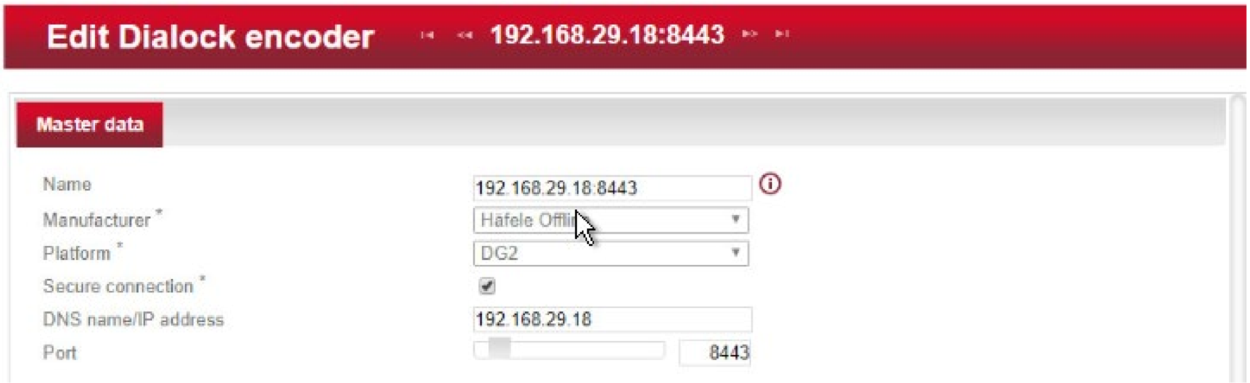
Name	Manufacturer
□ 192.168.29.18:8443	Häfele Offline

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:



Edit Dialock encoder 192.168.29.18:8443

Name: 192.168.29.18:8443
Manufacturer *: Häfele Offli
Platform *: DG2
Secure connection *: ☑
DNS name/IP address: 192.168.29.18
Port: 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.

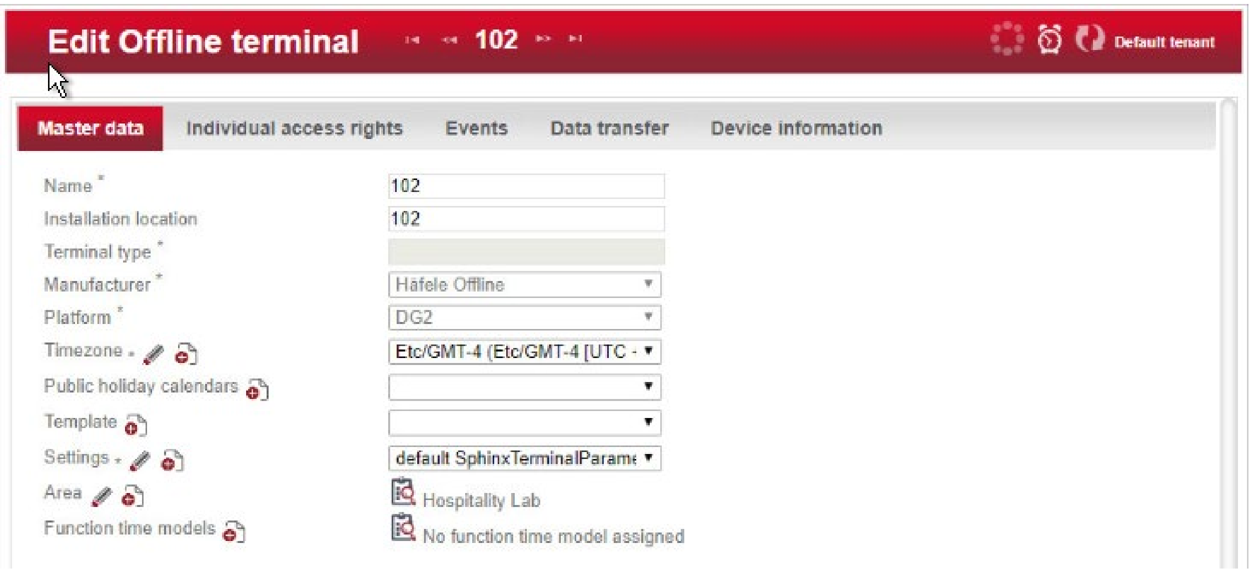
2.5.6.2 Adding the MDU

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.

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

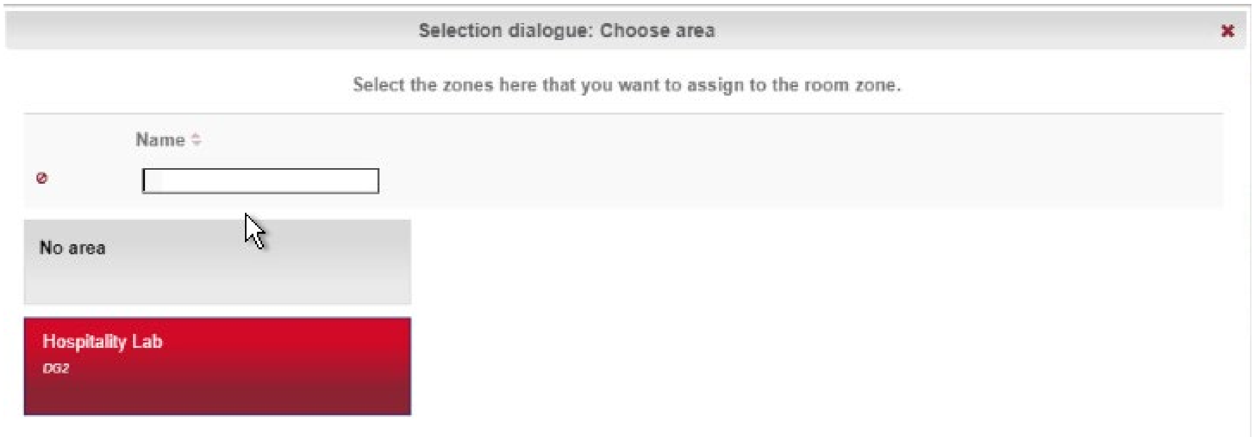
1. Navigate to **Devices > Terminal.**
2. In this menu, select the **create menu item** located under Actions on the left side of the screen. In the preselection pop-up dialogue, select **Häfele Offline (DG2).**
3. The grayed-out fields contain unconfigurable preset terms.
4. **Name** is a required field. 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:



Name *	102
Installation location	102
Terminal type *	
Manufacturer *	Häfele Offline
Platform *	DG2
Timezone	Etc/GMT-4 (Etc/GMT-4 [UTC -
Public holiday calendars	
Template	
Settings	default SphinxTerminalParame
Area	Hospitality Lab
Function time models	No function time model assigned

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.



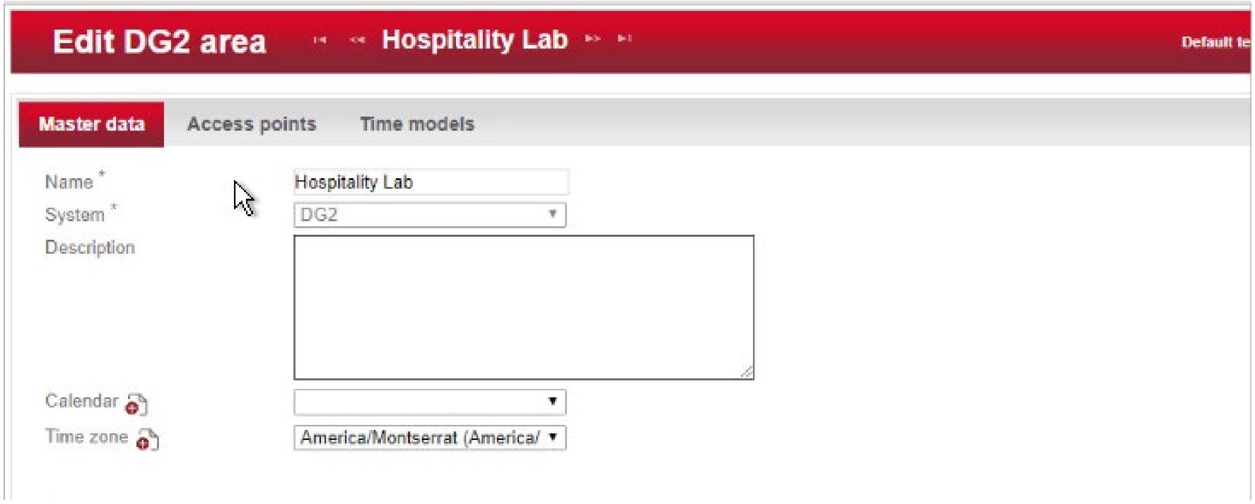
Selection dialogue: Choose area
Select the zones here that you want to assign to the room zone.
Name
No area
Hospitality Lab
DG2

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:



Edit DG2 area — Hospitality Lab

Name *: Hospitality Lab
System *: DG2
Description:
Calendar:
Time zone: America/Montserrat (America/

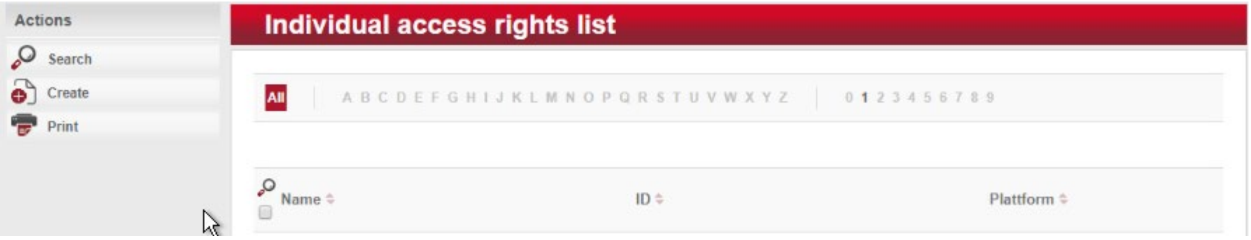
2. Be sure to save the created area. After this is complete, refer to the previous step to add the area to the terminal.

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:



Individual access rights list

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

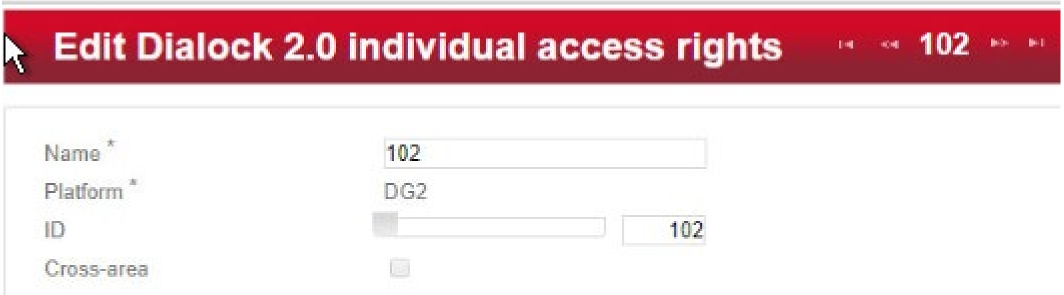
3. The window **Create Dialock 2.0 individual access rights** opens.

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:



Edit Dialock 2.0 individual access rights 102

Name * 102
Platform * DG2
ID 102
Cross-area □

2.5.6.5.2 Configuring the Terminal

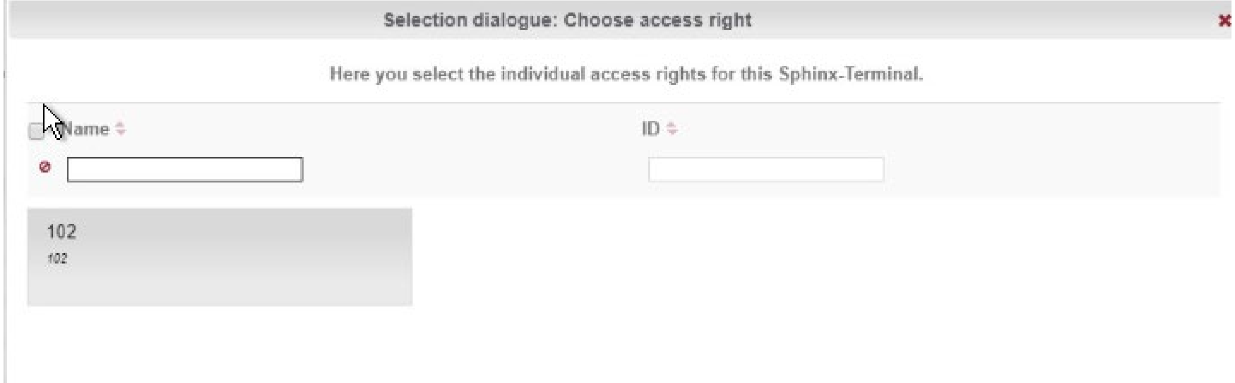
This step completes the individual terminal setup and assigns the previously created individual access rights to the respective terminals.

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:



Selection dialogue: Choose access right

Here you select the individual access rights for this Sphinx-Terminal.

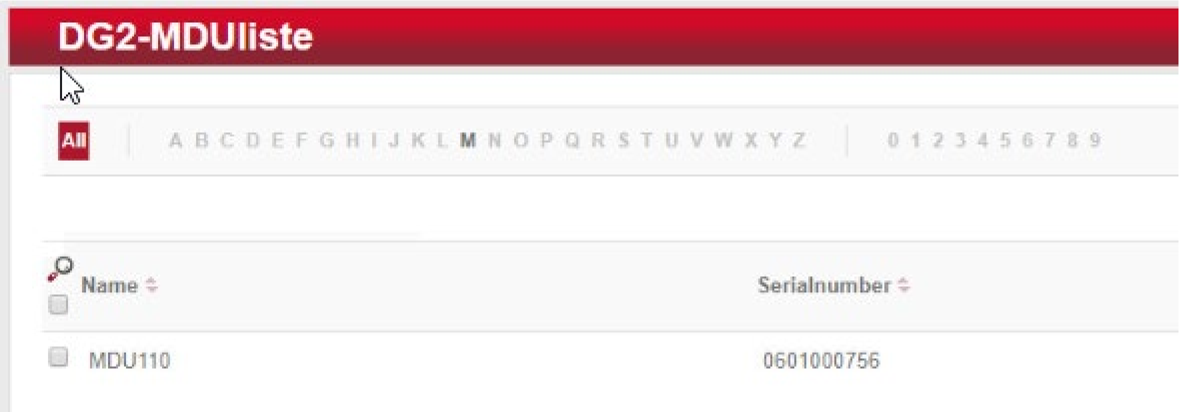
□ Name | ID

102
102

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:



□ Name	Serialnumber
□ MDU110	0601000756

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.

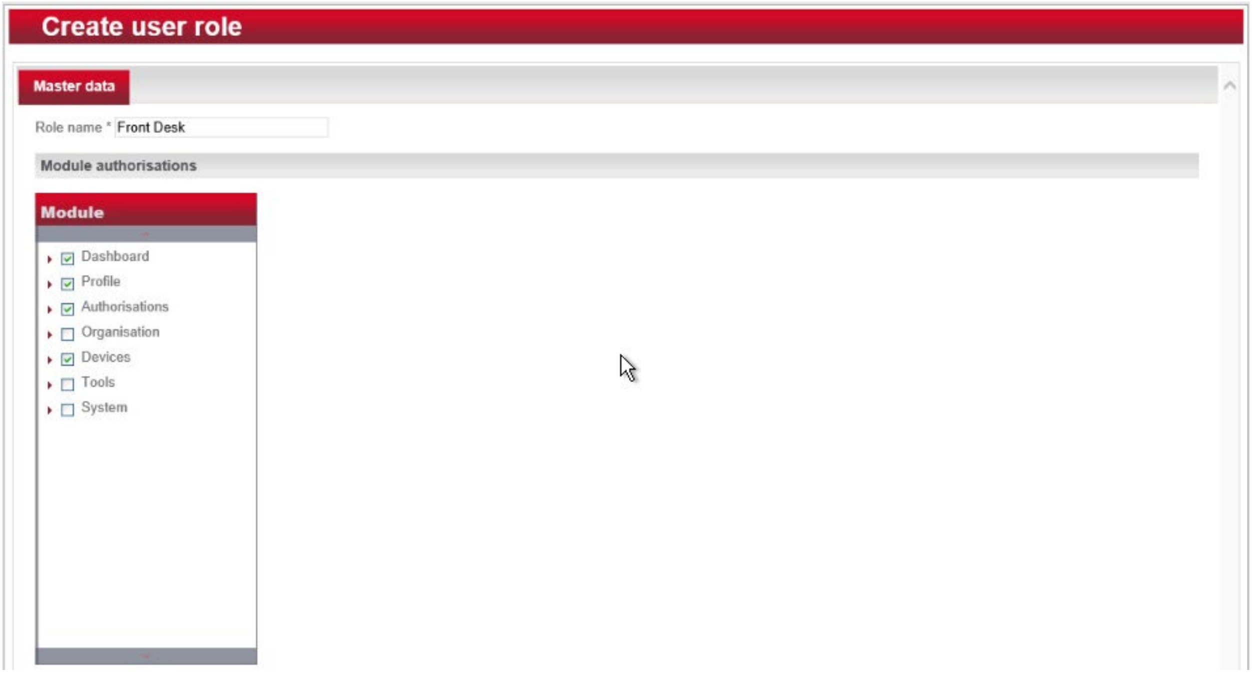
6. Click **OK.** You can now begin to program physical access points utilizing the MDU.

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:



Create user role

Master data

Role name * Front Desk

Module authorisations

Module

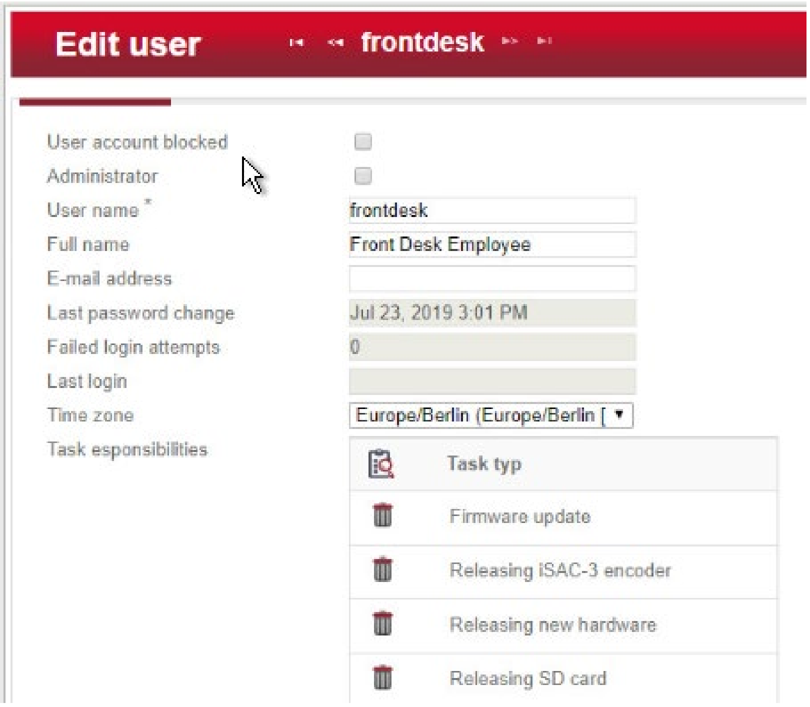
- ☑ Dashboard
- ☑ Profile
- ☑ Authorisations
- □ Organisation
- ☑ Devices
- □ Tools
- □ System

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:**



Edit user ⏮ ◀ frontdesk ▶ ⏭

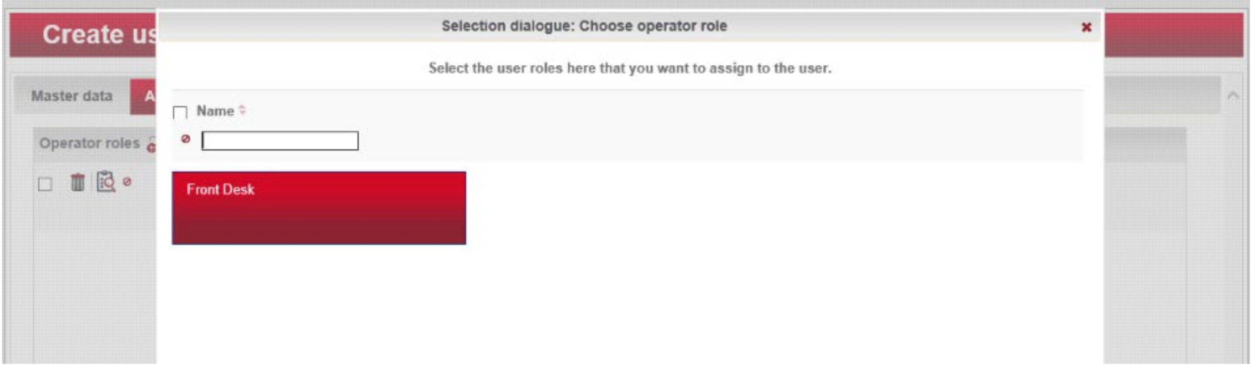
User account blocked □
Administrator □
User name * frontdesk
Full name Front Desk Employee
E-mail address
Last password change Jul 23, 2019 3:01 PM
Failed login attempts 0
Last login
Time zone Europe/Berlin (Europe/Berlin [▾
Task esponsibilities

	Task typ
🗑	Firmware update
🗑	Releasing iSAC-3 encoder
🗑	Releasing new hardware
🗑	Releasing SD card

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.



Create us

Selection dialogue: Choose operator role ×

Select the user roles here that you want to assign to the user.

□ Name

Front Desk

Remediant SecureONE is the privileged access management solution within the reference architecture. Additionally, it maps to the Security Analytics component of the ZTA.

2.6.1 Privileged Access Management System–Remediant SecureONE–Overview

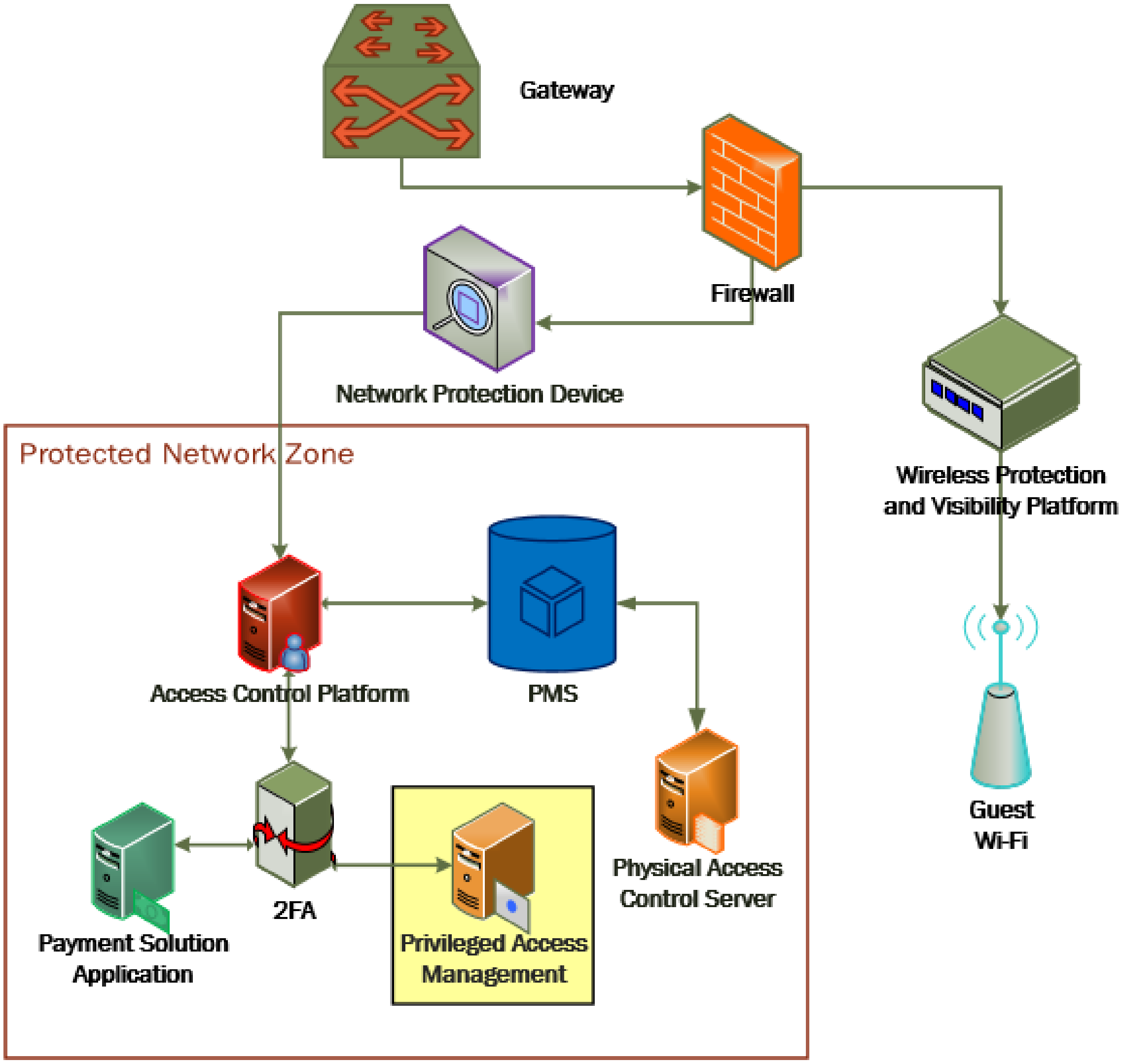
Remediant SecureONE provides detection and response capabilities for violations of privileged access within the enterprise.

In the PMS reference design, 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 Figure 2-5 below.

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


Gateway
Firewall
Network Protection Device
Wireless Protection and Visibility Platform
Protected Network Zone
Access Control Platform
PMS
Guest Wi-Fi
2FA
Physical Access Control Server
Payment Solution Application
Privileged Access Management

2.6.2 Privileged Access Management System–Remediant SecureONE–Requirements

The following subsections document the software, hardware, and network requirements for the PAM system Remediant SecureONE. Both the hardware and software requirements were included in the 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 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.

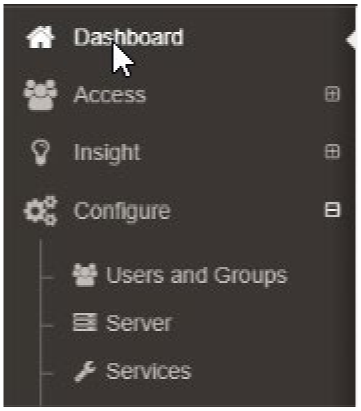
2.6.4 Initial Configuration

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/

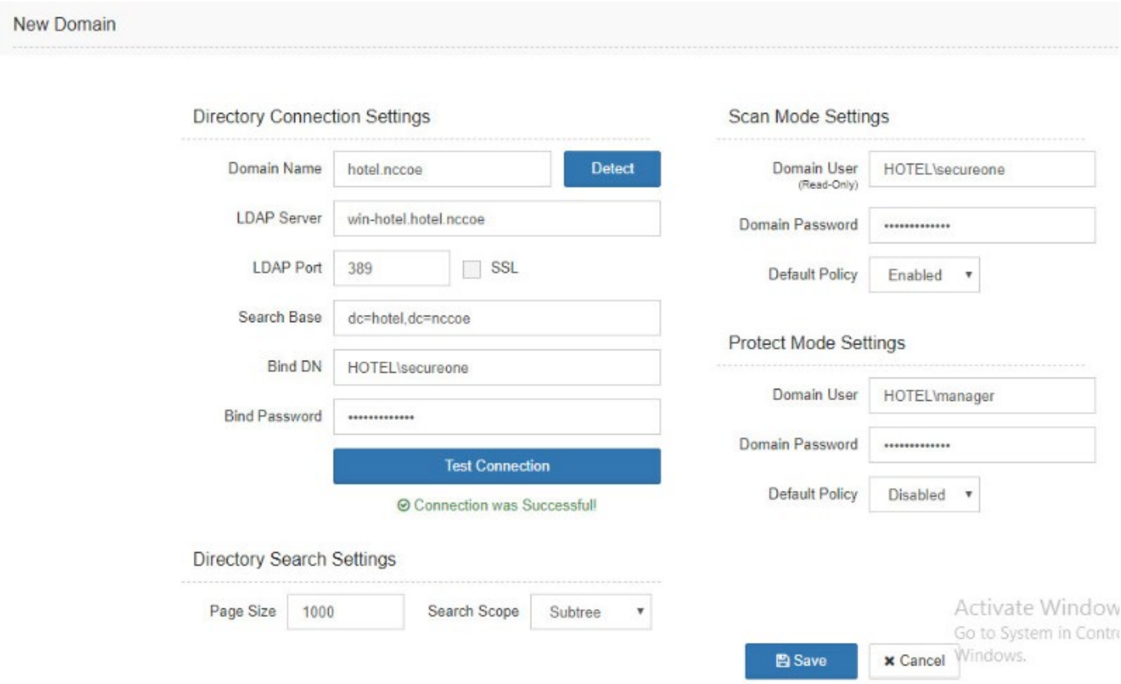
2. To log in to the SecureONE appliance, navigate in a web browser to the IP of the machine, and use the provided credentials to sign in.

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:



New Domain

Directory Connection Settings

Domain Name: hotel.nccoe [Detect]

LDAP Server: win-hotel.hotel.nccoe

LDAP Port: 389 ☐ SSL

Search Base: dc=hotel,dc=nccoe

Bind DN: HOTEL\secureone

Bind Password: •••••••••••••

[Test Connection]

Connection was Successful!

Directory Search Settings

Page Size: 1000 Search Scope: Subtree

Scan Mode Settings

Domain User (Read-Only): HOTEL\secureone

Domain Password: •••••••••••••

Default Policy: Enabled

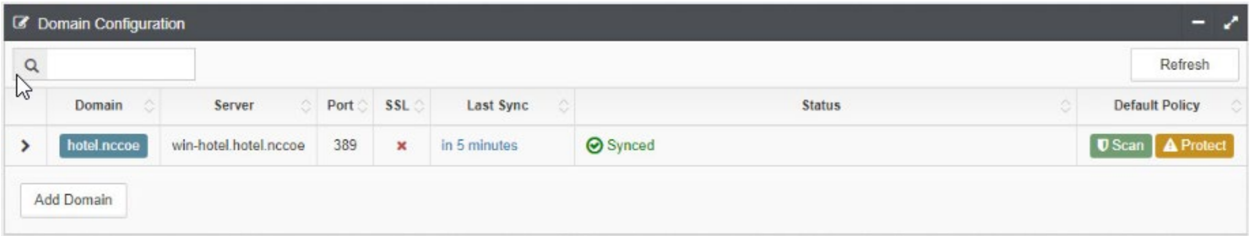
Protect Mode Settings

Domain User: HOTEL\manager

Domain Password: •••••••••••••

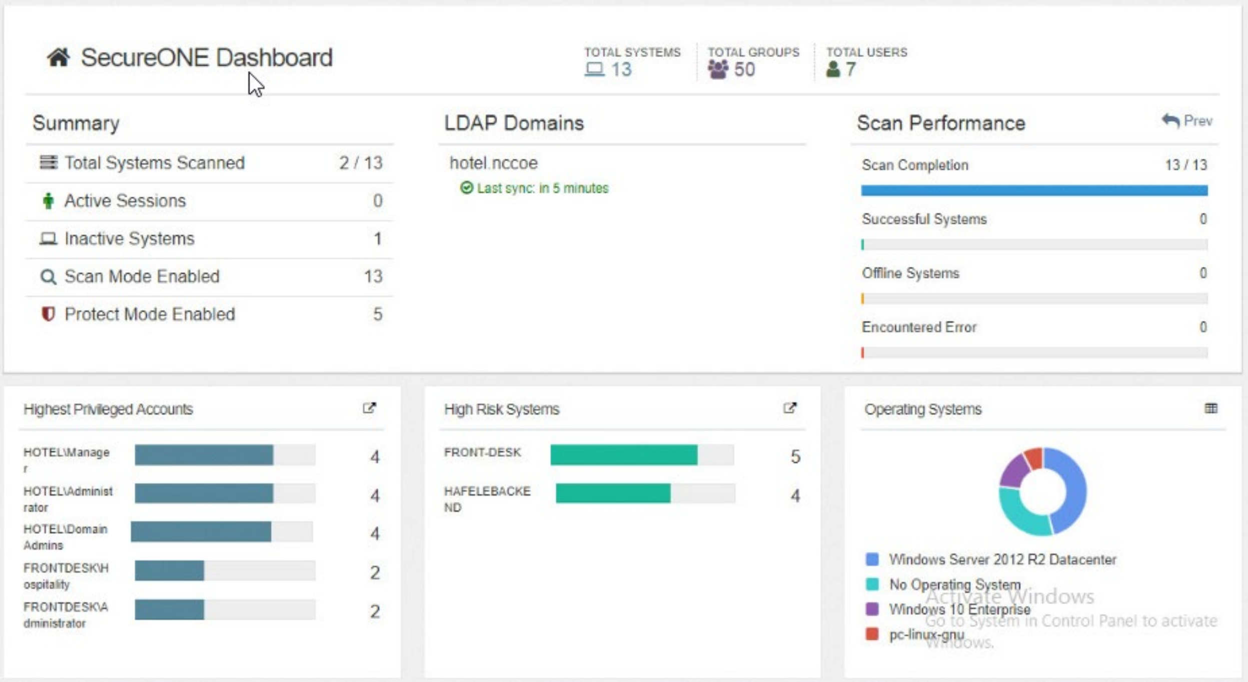
Default Policy: Disabled

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



	Domain	Server	Port	SSL	Last Sync	Status	Default Policy
>	hotel.nccoe	win-hotel.hotel.nccoe	389	✗	in 5 minutes	Synced	Scan Protect

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



Summary

Total Systems Scanned	2 / 13
Active Sessions	0
Inactive Systems	1
Scan Mode Enabled	13
Protect Mode Enabled	5

LDAP Domains

hotel.nccoe
Last sync: in 5 minutes

Scan Performance

Scan Completion	13 / 13
Successful Systems	0
Offline Systems	0
Encountered Error	0

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. It covers a role in the ZTA that is similar to CryptoniteNXT, except in our implementation it is used exclusively to protect the wireless network.

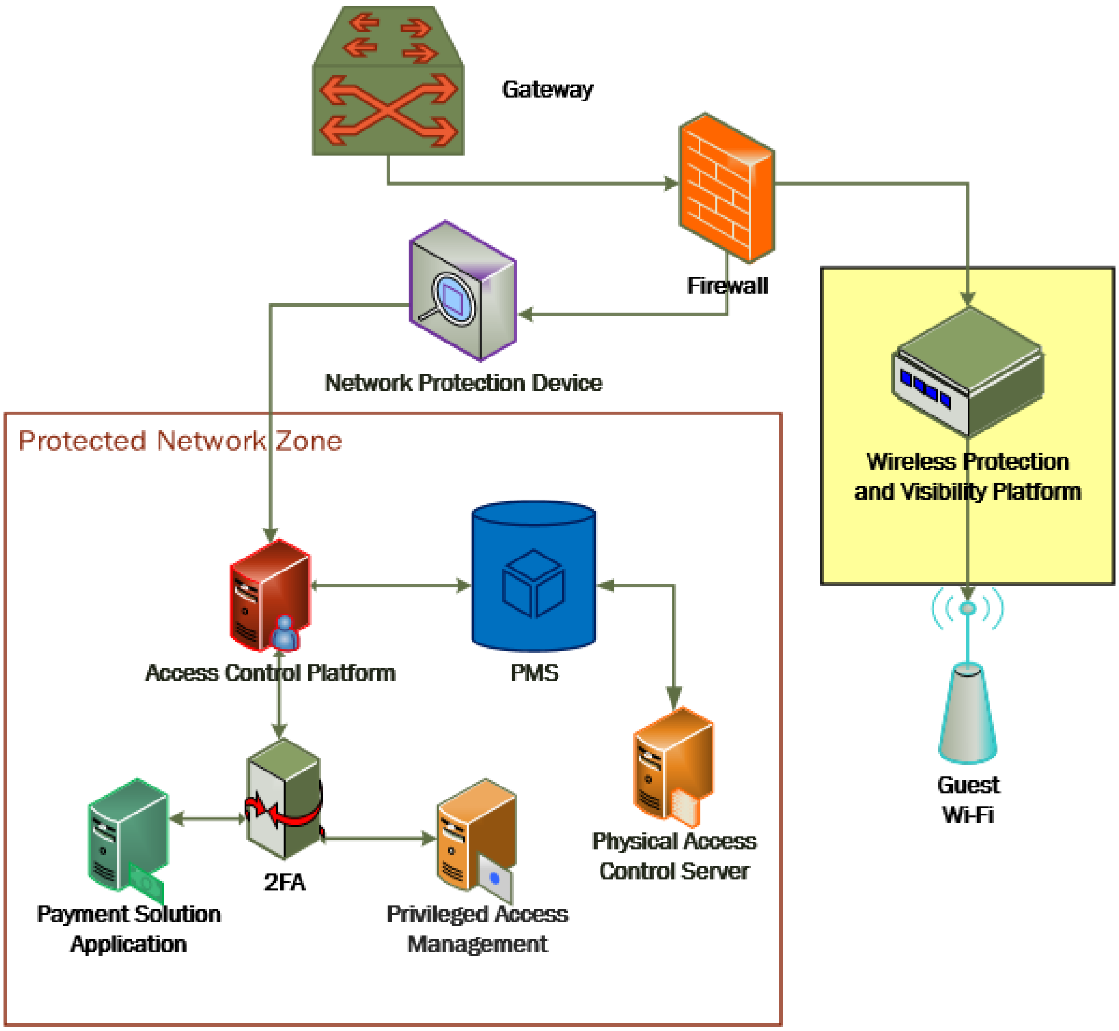
2.7.1 Wireless Network Management–Forescout CounterACT–Overview

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

Forescout CounterACT authenticates hotel guest 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 Figure 2-6 below.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-27.

Figure 2-6 Wireless Network Management in the Reference Architecture


Gateway
Firewall
Network Protection Device
Wireless Protection and Visibility Platform
Protected Network Zone
Access Control Platform
PMS
Physical Access Control Server
2FA
Payment Solution Application
Privileged Access Management
Guest Wi-Fi

2.7.2 Wireless Network Management–Forescout CounterACT–Requirements

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

2.7.2.1 Hardware Requirements for Wireless Network Management

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

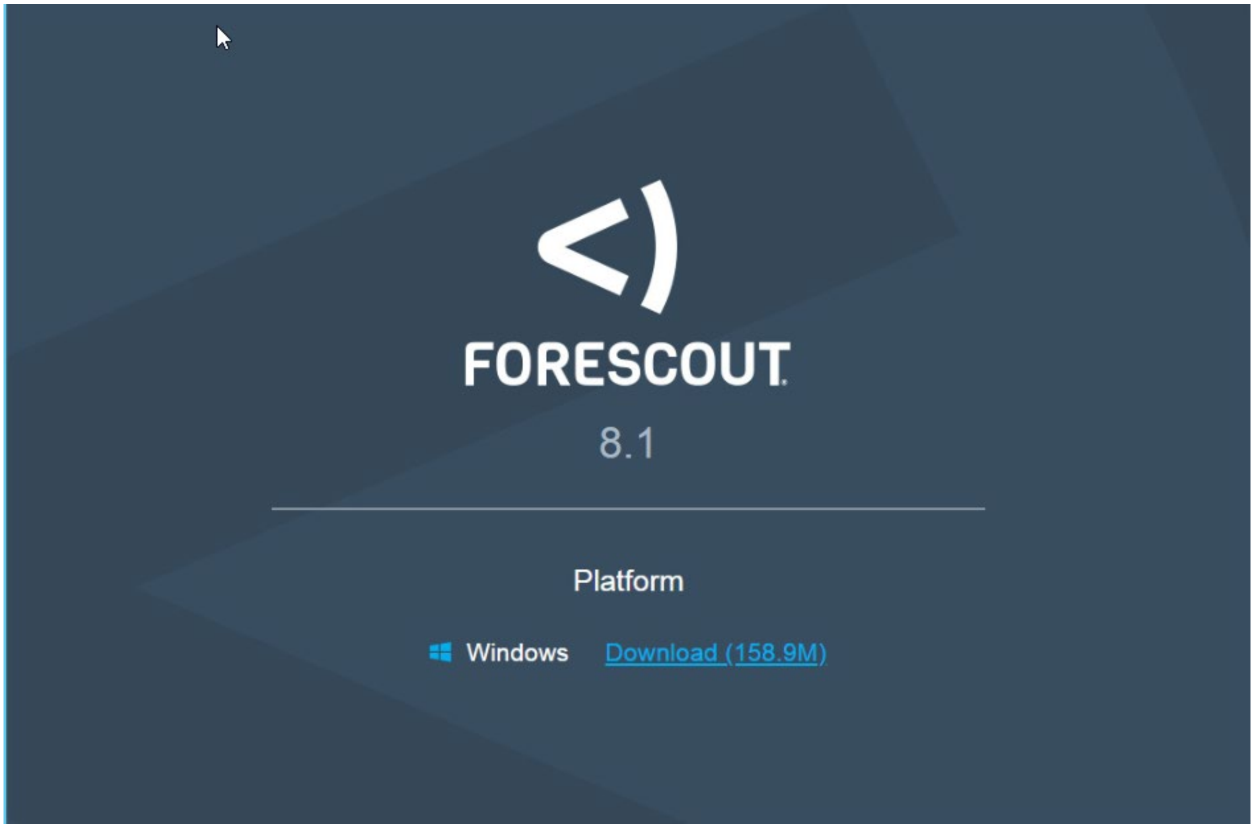
This installation occurred on a deployed CentOS 7 VM that the vendor provided.

2.7.2.3 Network Requirements for Wireless Network Management

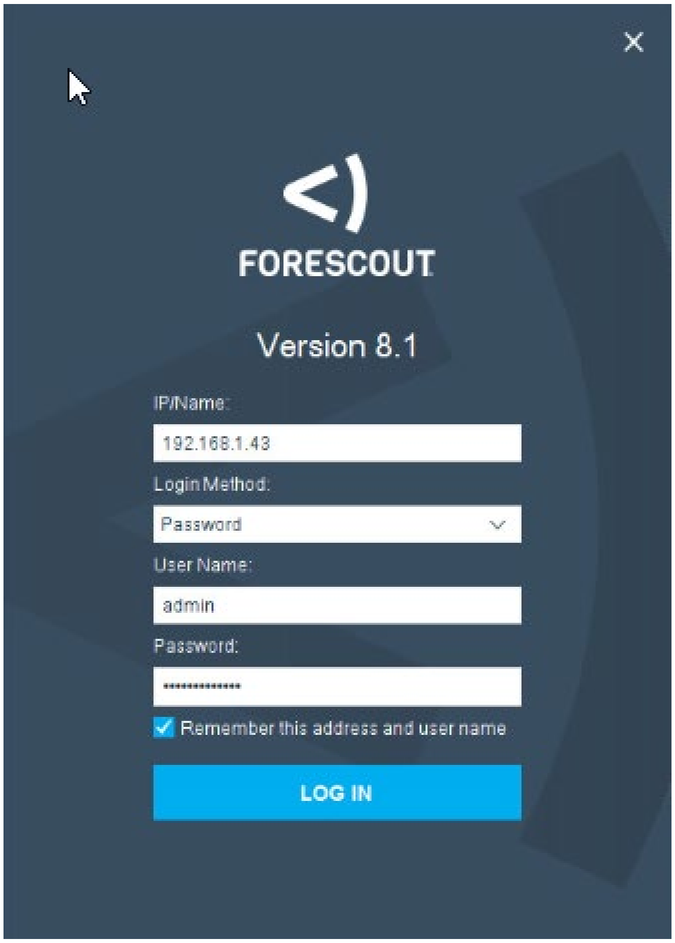
Forescout CounterACT requires the capability to monitor network traffic on the network it is administering. Network connectivity is also required on the system administrator user workstation that will run the Forescout CounterACT console.

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:



IP/Name: 192.168.1.43

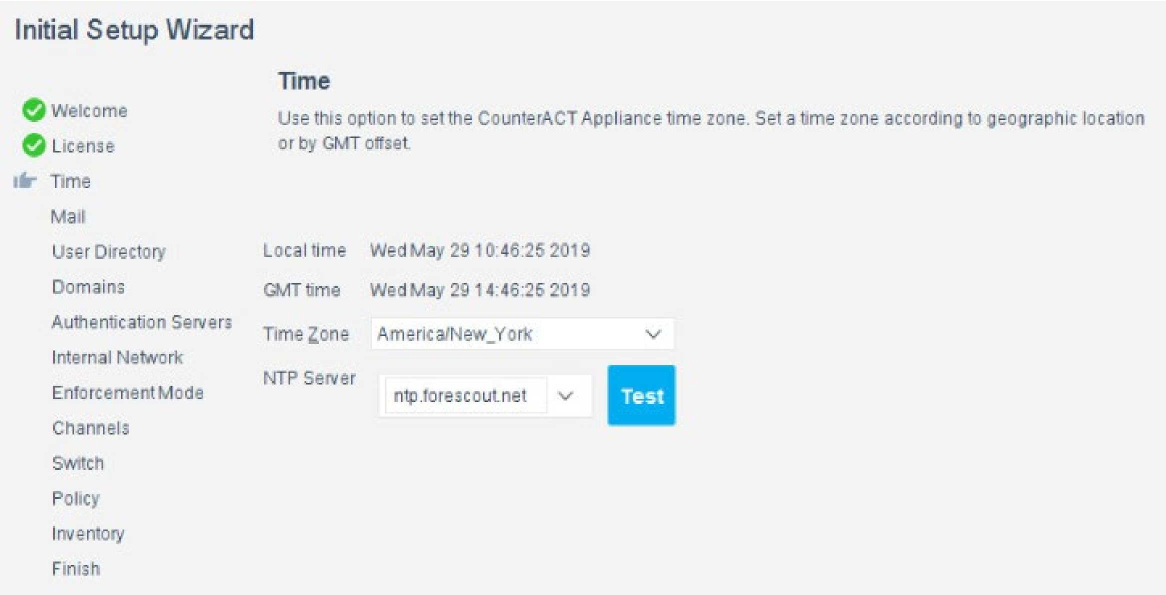
Login Method: Password

User Name: admin

Password: **************

☑ Remember this address and user name

3. Navigate through the Initial Setup Wizard when the console launches. Verify that the NTP (Network Time Protocol) server is configured as desired.



Initial Setup Wizard

Time

Use this option to set the CounterACT Appliance time zone. Set a time zone according to geographic location or by GMT offset.

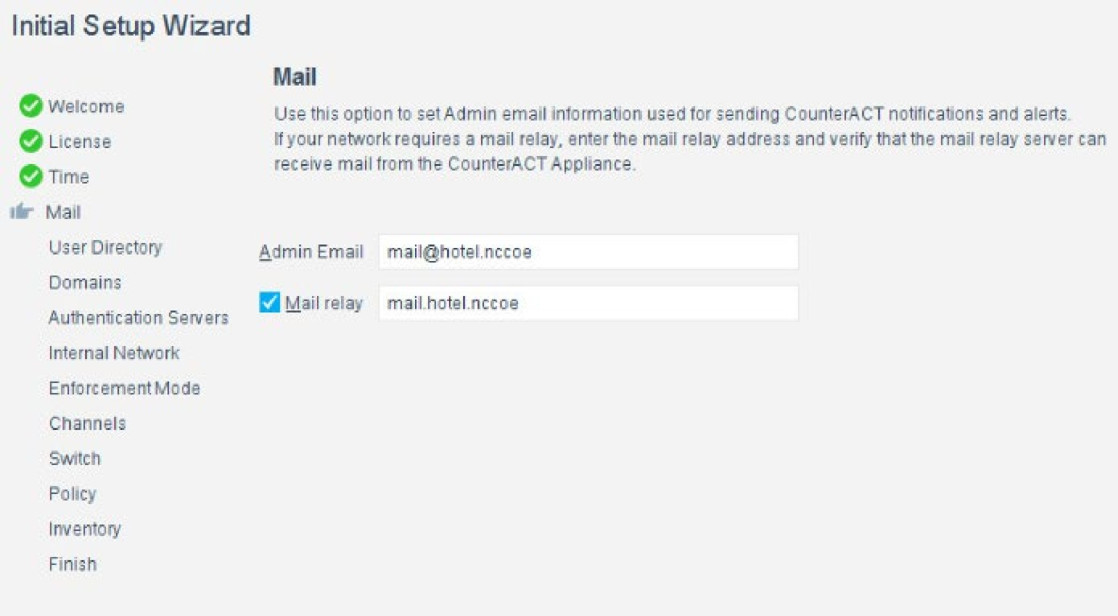
Local time Wed May 29 10:46:25 2019

GMT time Wed May 29 14:46:25 2019

Time Zone America/New_York

NTP Server ntp.forescout.net

4. Input the email account where you wish to receive notifications and alerts:



Initial Setup Wizard

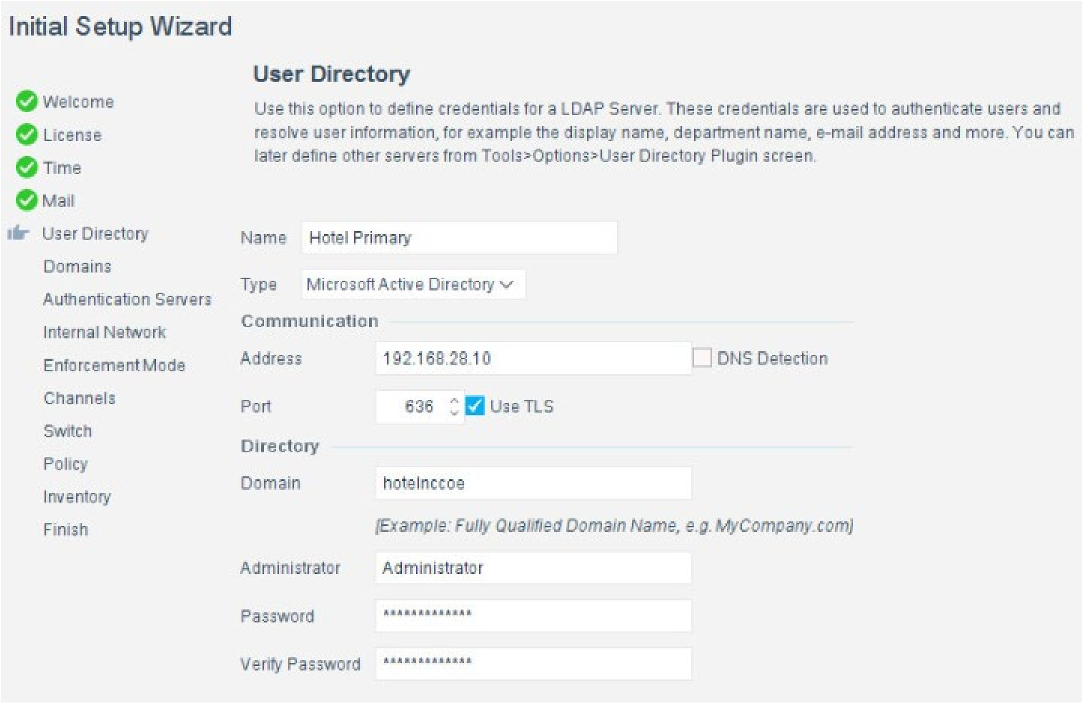
Mail

Use this option to set Admin email information used for sending CounterACT notifications and alerts. If your network requires a mail relay, enter the mail relay address and verify that the mail relay server can receive mail from the CounterACT Appliance.

Admin Email mail@hotel.nccoe

☑ Mail relay mail.hotel.nccoe

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



User Directory

Use this option to define credentials for a LDAP Server. These credentials are used to authenticate users and resolve user information, for example the display name, department name, e-mail address and more. You can later define other servers from Tools>Options>User Directory Plugin screen.

Name: Hotel Primary

Type: Microsoft Active Directory

Communication

Address: 192.168.28.10 □ DNS Detection

Port: 636 ☑ Use TLS

Directory

Domain: hotelnccoe

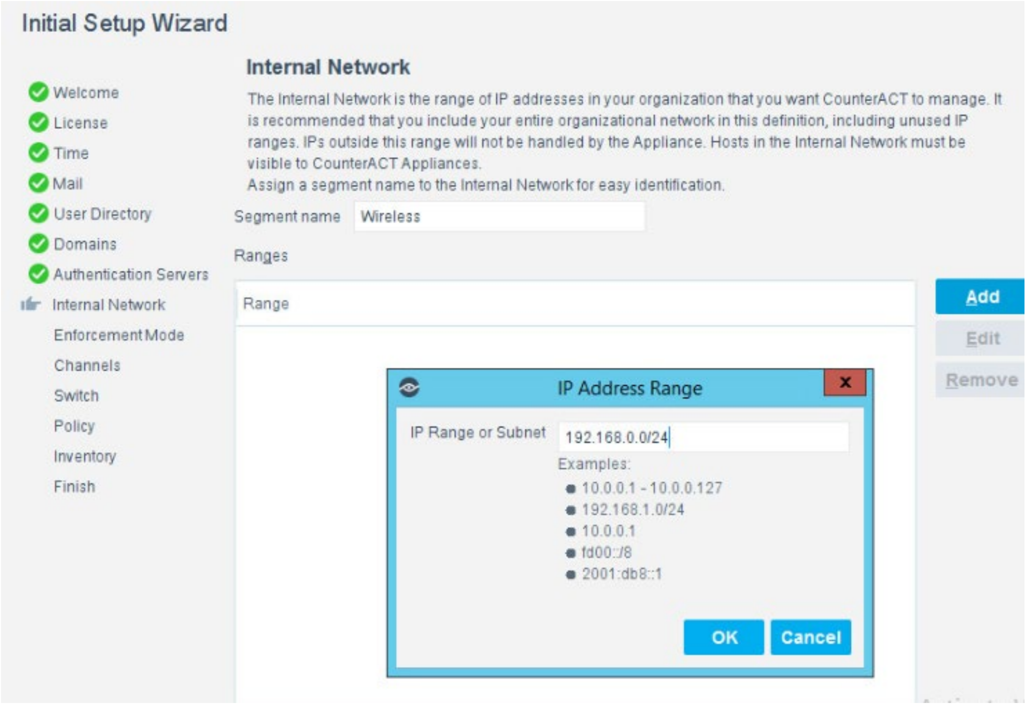
[Example: Fully Qualified Domain Name, e.g. MyCompany.com]

Administrator: Administrator

Password: *************

Verify Password: *************

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



Internal Network

The Internal Network is the range of IP addresses in your organization that you want CounterACT to manage. It is recommended that you include your entire organizational network in this definition, including unused IP ranges. IPs outside this range will not be handled by the Appliance. Hosts in the Internal Network must be visible to CounterACT Appliances.

Assign a segment name to the Internal Network for easy identification.

Segment name: Wireless

Ranges

Range

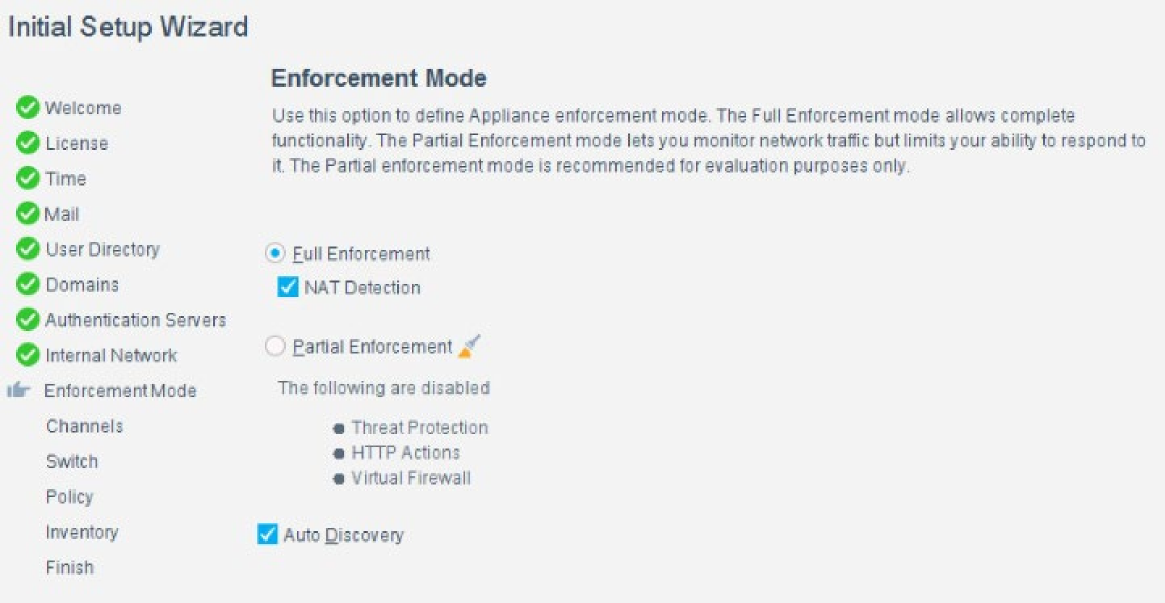
IP Address Range

IP Range or Subnet: 192.168.0.0/24

Examples:

- 10.0.0.1 - 10.0.0.127
- 192.168.1.0/24
- 10.0.0.1
- fd00::/8
- 2001:db8::1

7. Set the enforcement options desired for this deployment. For our lab, **Full Enforcement, NAT Detection** (Network Address Translation) and **Auto Discovery** were employed:



Initial Setup Wizard

Enforcement Mode

Use this option to define Appliance enforcement mode. The Full Enforcement mode allows complete functionality. The Partial Enforcement mode lets you monitor network traffic but limits your ability to respond to it. The Partial enforcement mode is recommended for evaluation purposes only.

● Full Enforcement

☑ NAT Detection

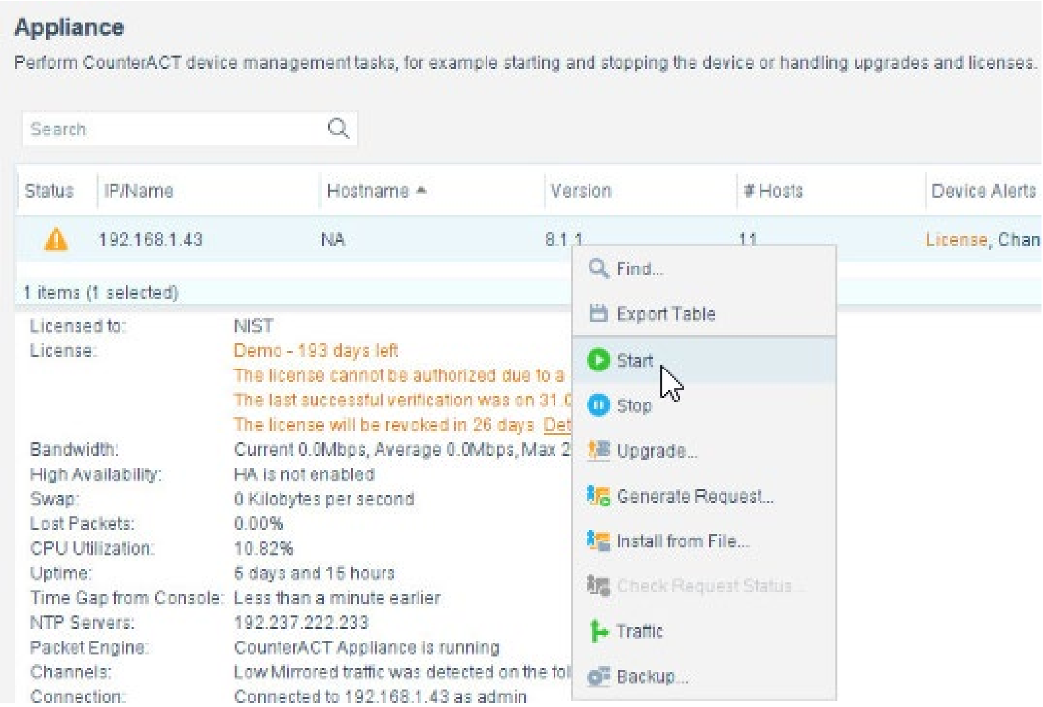
○ Partial Enforcement

The following are disabled

- Threat Protection
- HTTP Actions
- Virtual Firewall

☑ Auto Discovery

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



Appliance

Perform CounterACT device management tasks, for example starting and stopping the device or handling upgrades and licenses.

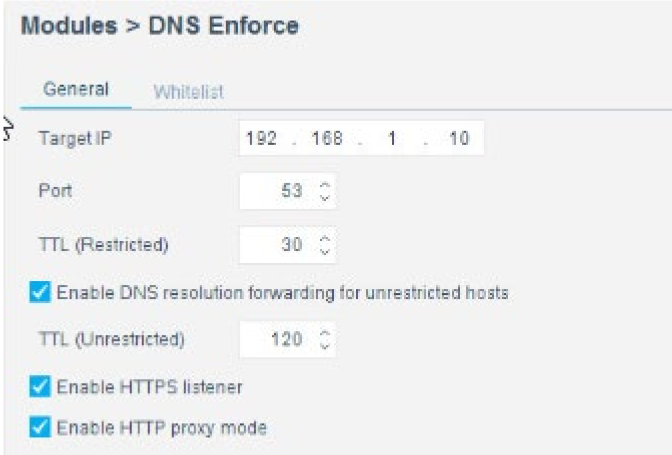
Status	IP/Name	Hostname ▲	Version	# Hosts	Device Alerts
⚠	192.168.1.43	NA	8.1.1	11	License, Chan

1 items (1 selected)

Licensed to: NIST
License: Demo - 193 days left
The license cannot be authorized due to a
The last successful verification was on 31.0
The license will be revoked in 26 days. Det
Bandwidth: Current 0.0Mbps, Average 0.0Mbps, Max 2
High Availability: HA is not enabled
Swap: 0 Kilobytes per second
Lost Packets: 0.00%
CPU Utilization: 10.82%
Uptime: 6 days and 16 hours
Time Gap from Console: Less than a minute earlier
NTP Servers: 192.237.222.233
Packet Engine: CounterACT Appliance is running
Channels: Low Mirrored traffic was detected on the fol
Connection: Connected to 192.168.1.43 as admin

2.7.4 DNS Enforcement

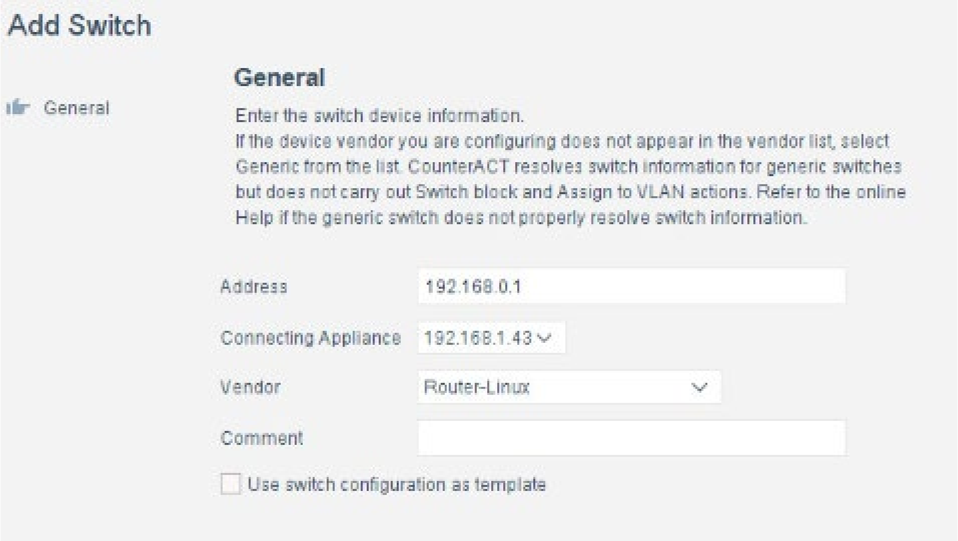
In the **options** menu, select the drop-down for modules, then select **DNS Enforce.** In this menu, configure the IP used for the DNS enforcement. It should look like the screenshot below:



Target IP: 192 . 168 . 1 . 10
Port: 53
TTL (Restricted): 30
☑ Enable DNS resolution forwarding for unrestricted hosts
TTL (Unrestricted): 120
☑ Enable HTTPS listener
☑ Enable HTTP proxy mode

2.7.5 Switch Plug-In

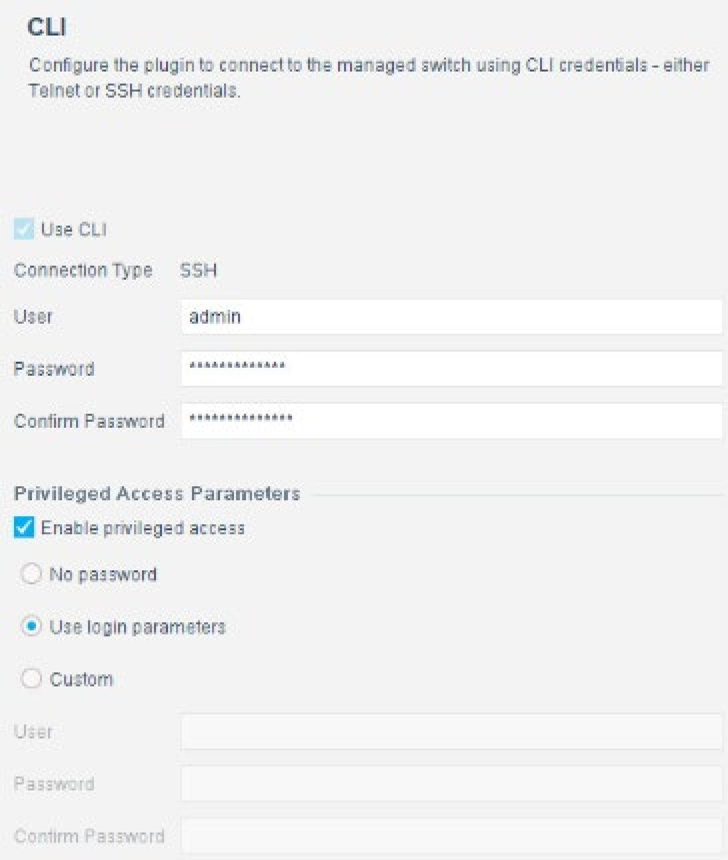
1. In the **options** menu, select the **switch** menu icon in the left scrolling menu. Here, we are adding our VyOS switch:
   - Select **Add.**
   - Enter the address of the switch.
   - Select **Router-Linux** as the vendor:



Enter the switch device information.
If the device vendor you are configuring does not appear in the vendor list, select Generic from the list. CounterACT resolves switch information for generic switches but does not carry out Switch block and Assign to VLAN actions. Refer to the online Help if the generic switch does not properly resolve switch information.

Address: 192.168.0.1
Connecting Appliance: 192.168.1.43
Vendor: Router-Linux
Comment:
□ Use switch configuration as template

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



CLI

Configure the plugin to connect to the managed switch using CLI credentials - either Telnet or SSH credentials.

☑ Use CLI

Connection Type SSH

User admin

Password *************

Confirm Password **************

Privileged Access Parameters

☑ Enable privileged access

○ No password

● Use login parameters

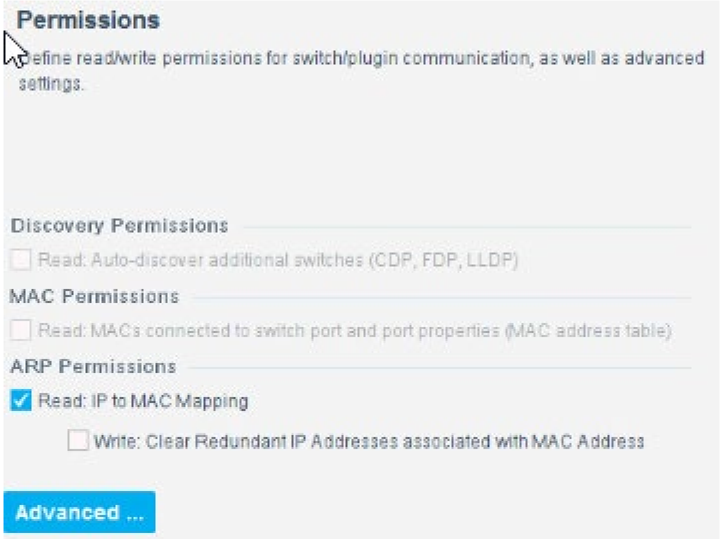
○ Custom

User

Password

Confirm Password

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



Permissions

Define read/write permissions for switch/plugin communication, as well as advanced settings.

Discovery Permissions

☐ Read: Auto-discover additional switches (CDP, FDP, LLDP)

MAC Permissions

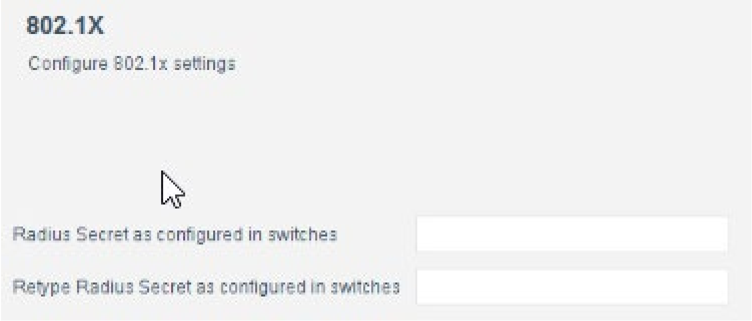
☐ Read: MACs connected to switch port and port properties (MAC address table)

ARP Permissions

☑ Read: IP to MAC Mapping

☐ Write: Clear Redundant IP Addresses associated with MAC Address

4. Configure 802.1X per organizational specification:



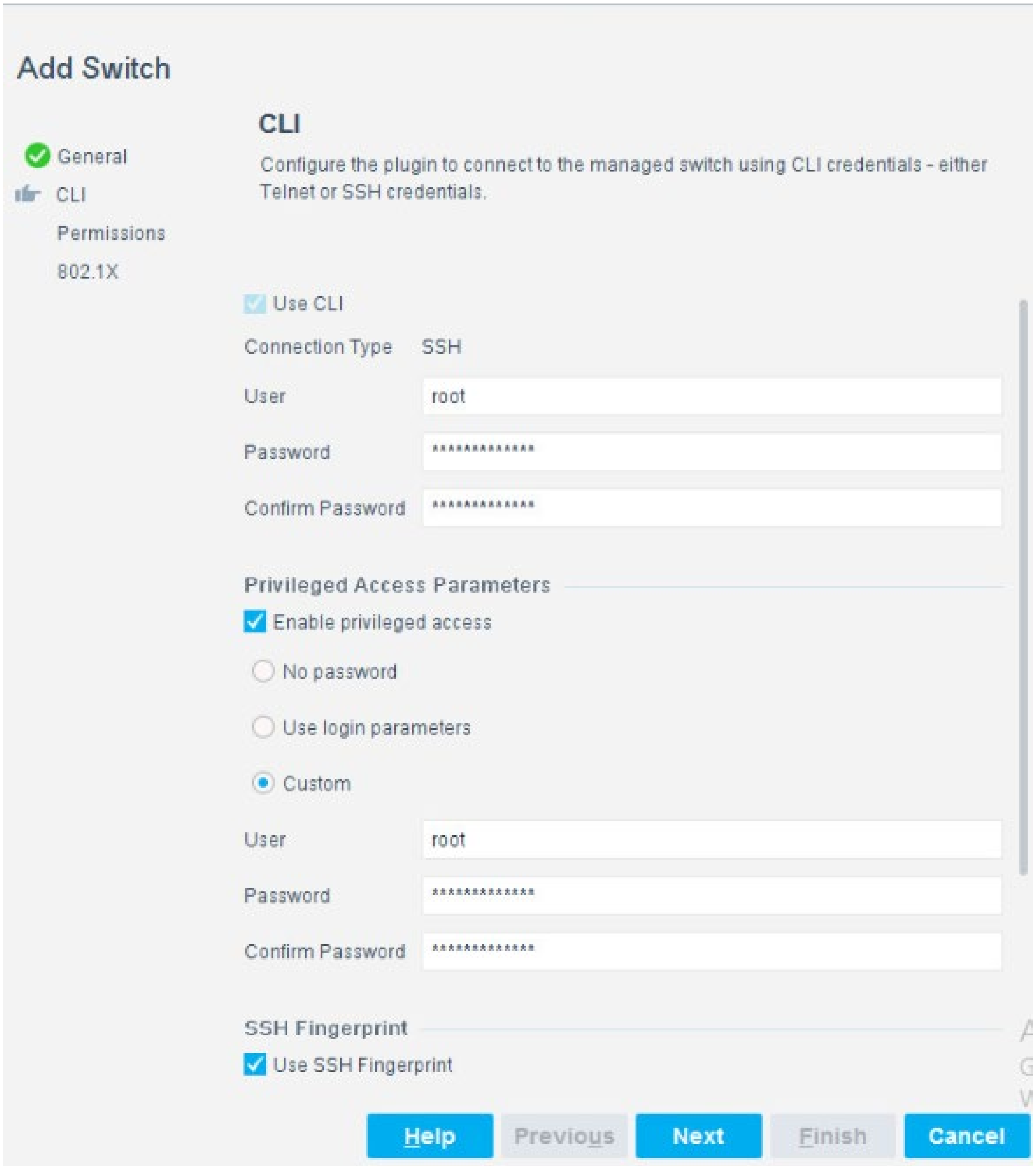
802.1X

Configure 802.1x settings

Radius Secret as configured in switches

Retype Radius Secret as configured in switches

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



Add Switch

CLI

Configure the plugin to connect to the managed switch using CLI credentials - either Telnet or SSH credentials.

☑ Use CLI

Connection Type SSH

User: root

Password: *************

Confirm Password: *************

Privileged Access Parameters

☑ Enable privileged access

○ No password

○ Use login parameters

● Custom

User: root

Password: *************

Confirm Password: *************

SSH Fingerprint

☑ Use SSH Fingerprint

2.7.6 Guest Policy

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

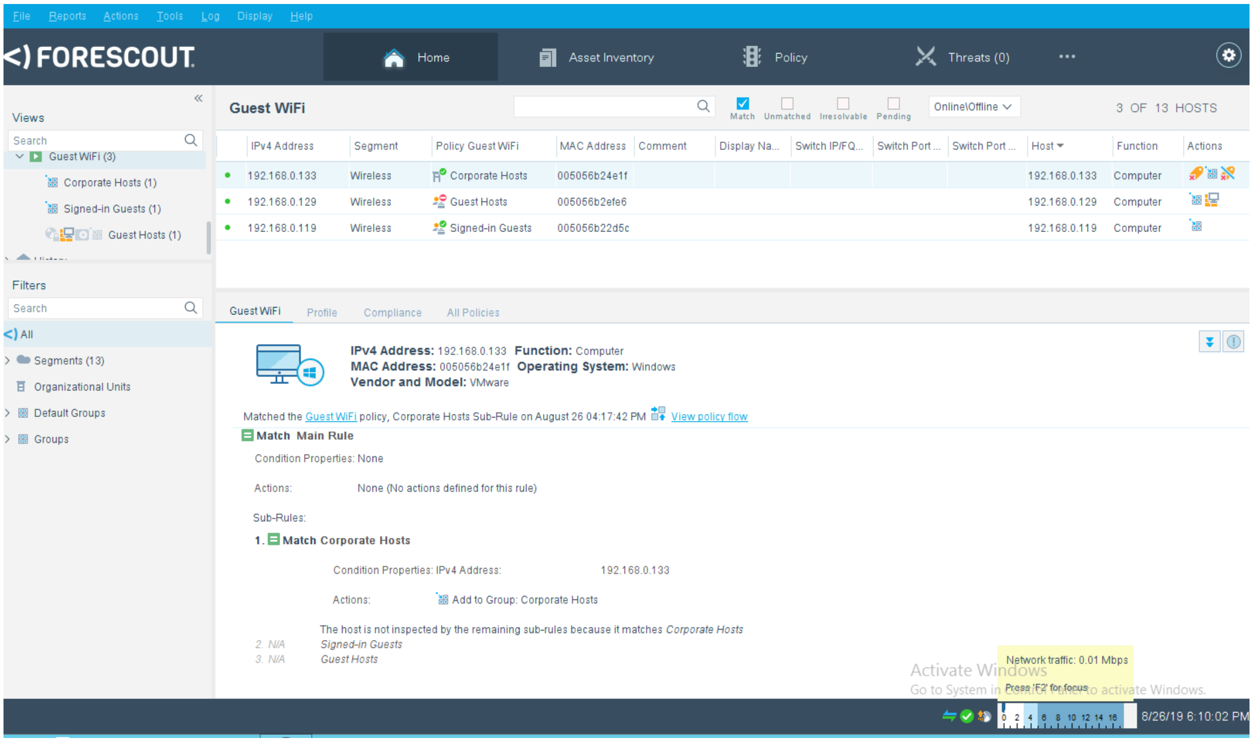
This Forescout policy is designed to detect a device when it joins the Guest WiFi, query that device for the result of its authentication process, and assign settings to the Forescout virtual firewall that provide the appropriate network access to that device. Due to lab limitations, the query process 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:



Guest WiFi

☑ Match ☐ Unmatched ☐ Irresolvable ☐ Pending Online\Offline 3 OF 13 HOSTS

	IPv4 Address	Segment	Policy Guest WiFi	MAC Address	Comment	Display Na...	Switch IP/FQ...	Switch Port ...	Switch Port ...	Host	Function	Actions
●	192.168.0.133	Wireless	Corporate Hosts	005056b24e1f						192.168.0.133	Computer	
●	192.168.0.129	Wireless	Guest Hosts	005056b2efe6						192.168.0.129	Computer	
●	192.168.0.119	Wireless	Signed-in Guests	005056b22d5c						192.168.0.119	Computer	

IPv4 Address: 192.168.0.133 **Function:** Computer
MAC Address: 005056b24e1f **Operating System:** Windows
Vendor and Model: VMware

Matched the Guest WiFi policy, Corporate Hosts Sub-Rule on August 26 04:17:42 PM View policy flow

Match Main Rule

Condition Properties: None

Actions: None (No actions defined for this rule)

Sub-Rules:

1. **Match Corporate Hosts**

Condition Properties: IPv4 Address: 192.168.0.133

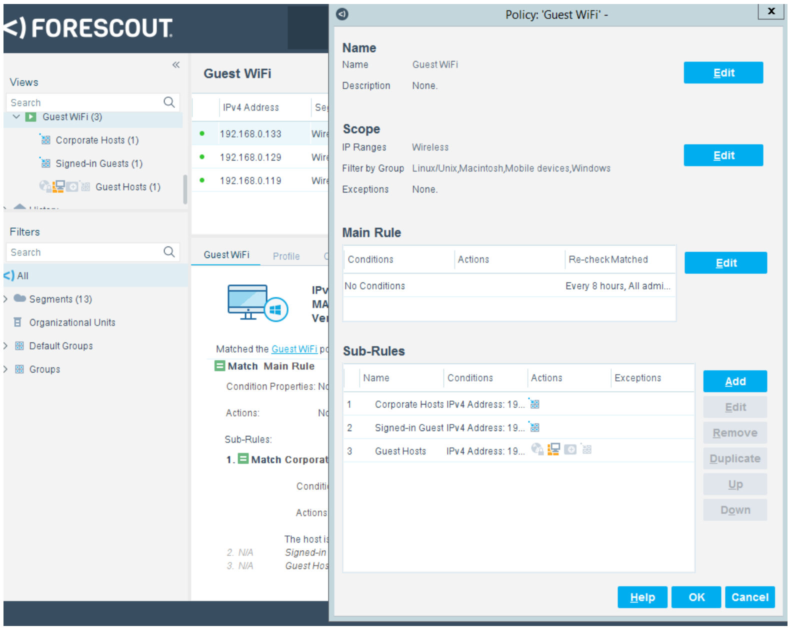
Actions: Add to Group: Corporate Hosts

The host is not inspected by the remaining sub-rules because it matches *Corporate Hosts*

2. N/A *Signed-in Guests*

3. N/A *Guest Hosts*

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



Policy: 'Guest WiFi' -

Name

Name Guest WiFi

Description None.

Scope

IP Ranges Wireless

Filter by Group Linux/Unix,Macintosh,Mobile devices,Windows

Exceptions None.

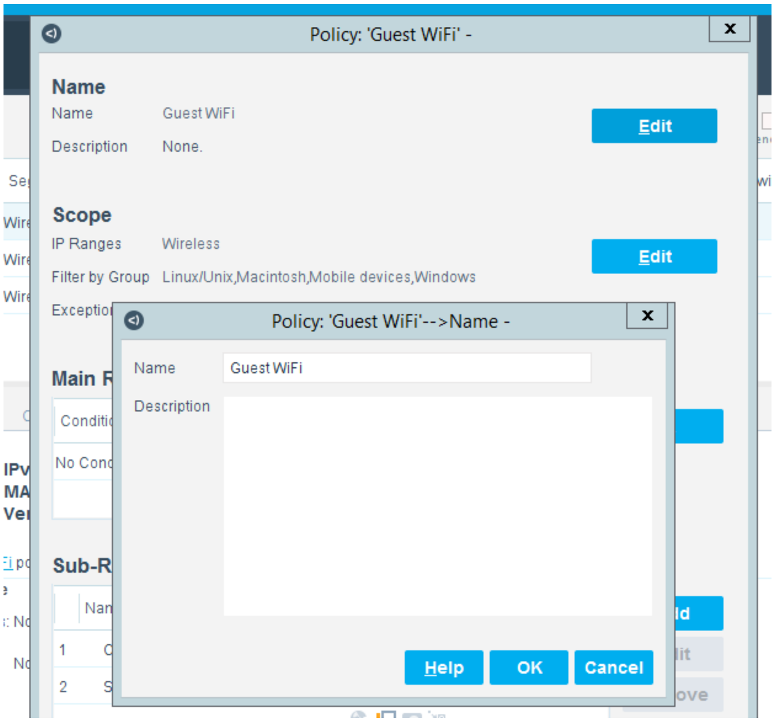
Main Rule

Conditions	Actions	Re-check Matched
No Conditions		Every 8 hours, All admi...

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	Corporate Hosts	IPv4 Address: 19...		
2	Signed-in Guest	IPv4 Address: 19...		
3	Guest Hosts	IPv4 Address: 19...		

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



Policy: 'Guest WiFi' -

Name

Name Guest WiFi

Description None.

Scope

IP Ranges Wireless

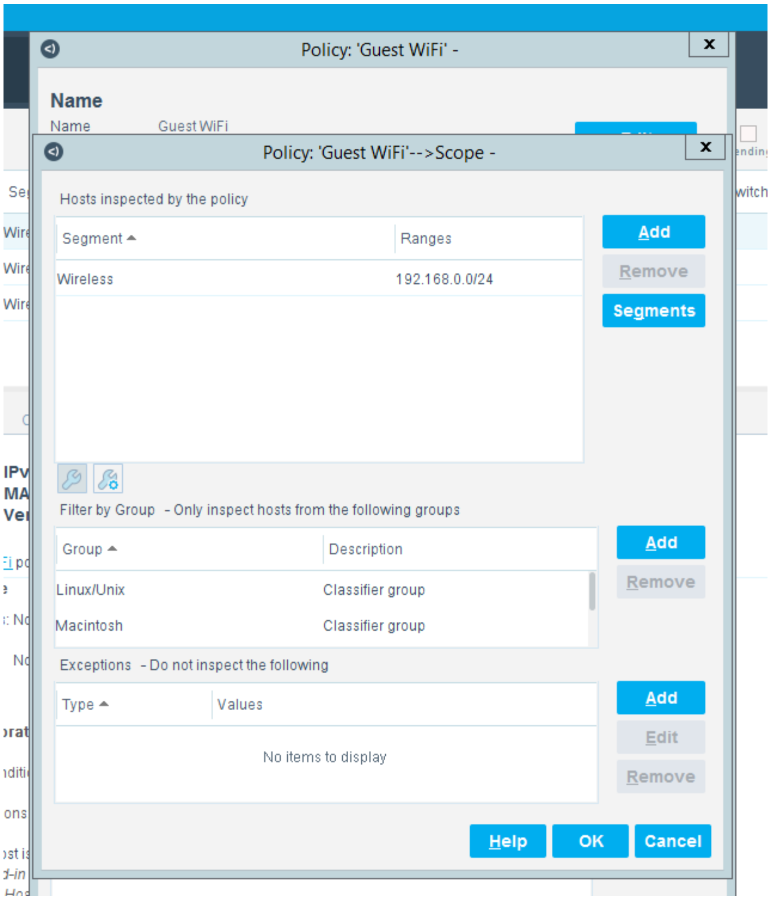
Filter by Group Linux/Unix,Macintosh,Mobile devices,Windows

Policy: 'Guest WiFi'-->Name -

Name: Guest WiFi

Description:

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

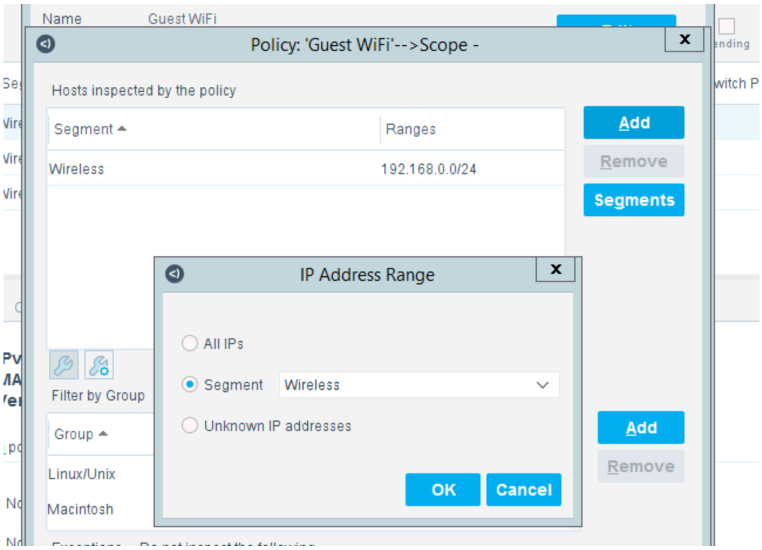
Filter by Group - Only inspect hosts from the following groups

Group ▲	Description
Linux/Unix	Classifier group
Macintosh	Classifier group

Exceptions - Do not inspect the following

Type ▲	Values
No items to display	

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



Name Guest WiFi

Policy: 'Guest WiFi'-->Scope -

Hosts inspected by the policy

Segment	Ranges
Wireless	192.168.0.0/24

IP Address Range

○ All IPs

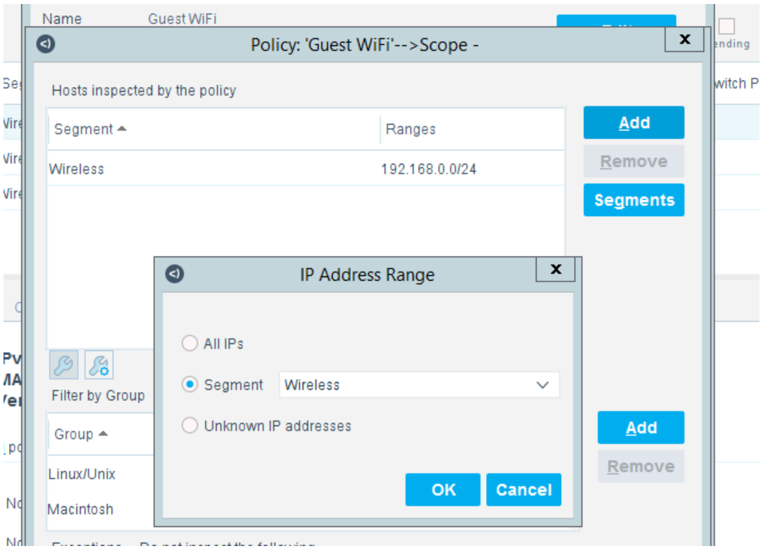
● Segment Wireless

○ Unknown IP addresses

Filter by Group

Group
Linux/Unix
Macintosh

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



Name Guest WiFi

Policy: 'Guest WiFi'-->Scope -

Hosts inspected by the policy

Segment	Ranges
Wireless	192.168.0.0/24

IP Address Range

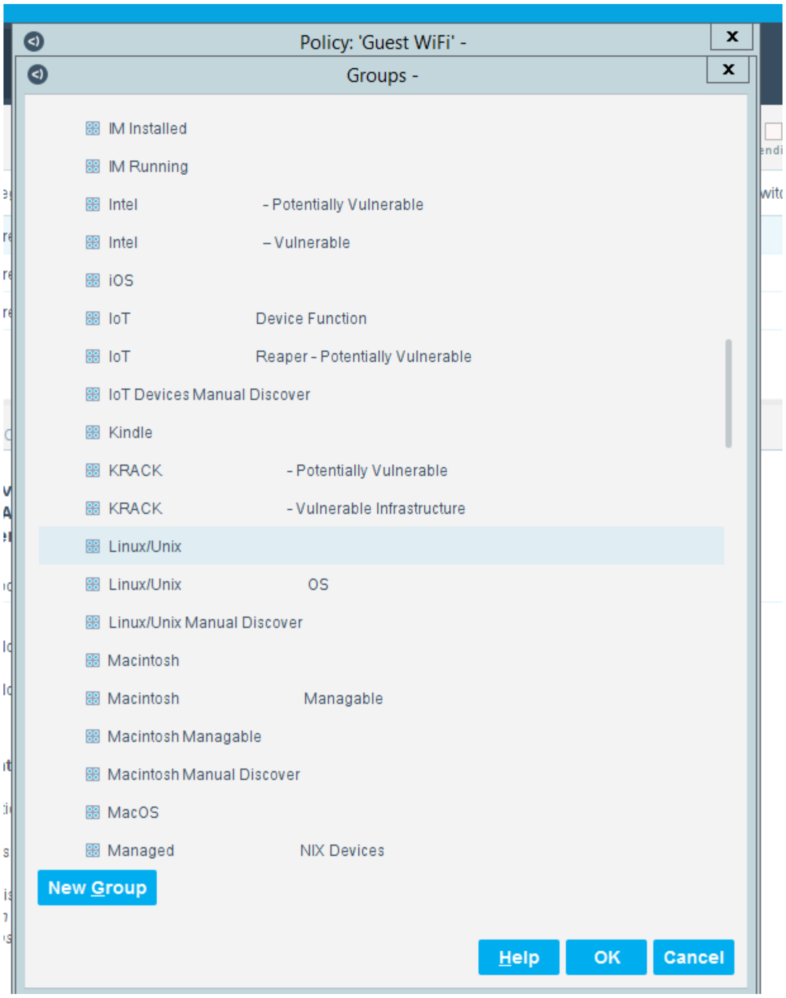
○ All IPs

● Segment Wireless

○ Unknown IP addresses

Filter by Group

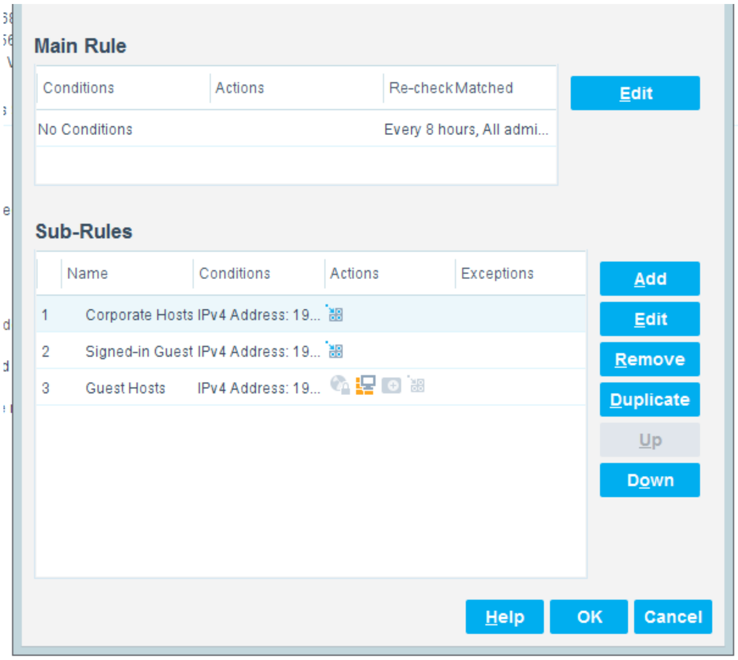
Group
Linux/Unix
Macintosh



IM Installed
IM Running
Intel - Potentially Vulnerable
Intel – Vulnerable
iOS
IoT Device Function
IoT Reaper - Potentially Vulnerable
IoT Devices Manual Discover
Kindle
KRACK - Potentially Vulnerable
KRACK - Vulnerable Infrastructure
Linux/Unix
Linux/Unix OS
Linux/Unix Manual Discover
Macintosh
Macintosh Managable
Macintosh Managable
Macintosh Manual Discover
MacOS
Managed NIX Devices

After the Name and Scope have been defined, consider defining the Main Rule section. For this lab, the Main Rule was left in the default No Conditions value. Only the Sub-Rules were used.

1. Highlight a Sub-Rule and click **Edit** to open the **Sub-Rule Edit** window.



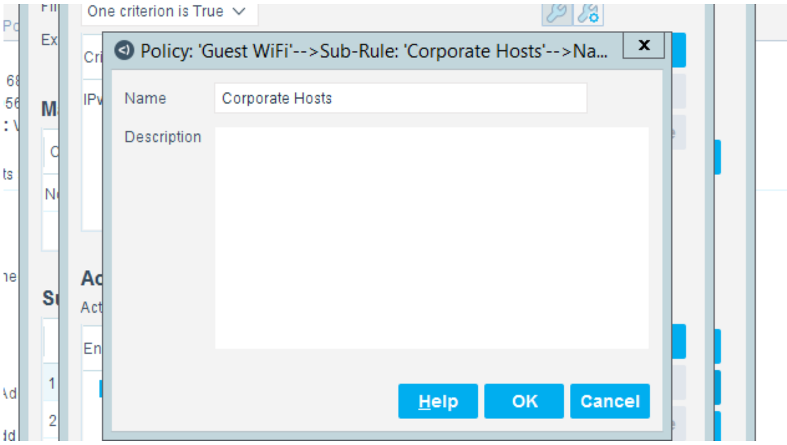
Main Rule

Conditions	Actions	Re-check Matched
No Conditions		Every 8 hours, All admi...

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	Corporate Hosts	IPv4 Address: 19...		
2	Signed-in Guest	IPv4 Address: 19...		
3	Guest Hosts	IPv4 Address: 19...		

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



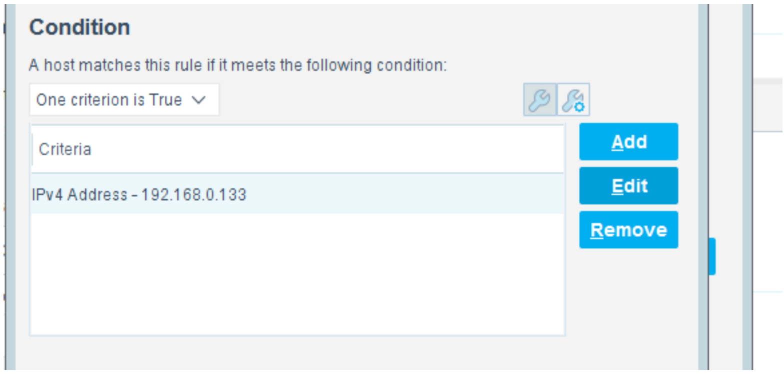
Policy: 'Guest WiFi'-->Sub-Rule: 'Corporate Hosts'-->Na...

Name: Corporate Hosts

Description:

3. In the Condition section of the **Sub-Rule Edit** window, click the drop-down arrow, and select the **condition type.**

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



Condition

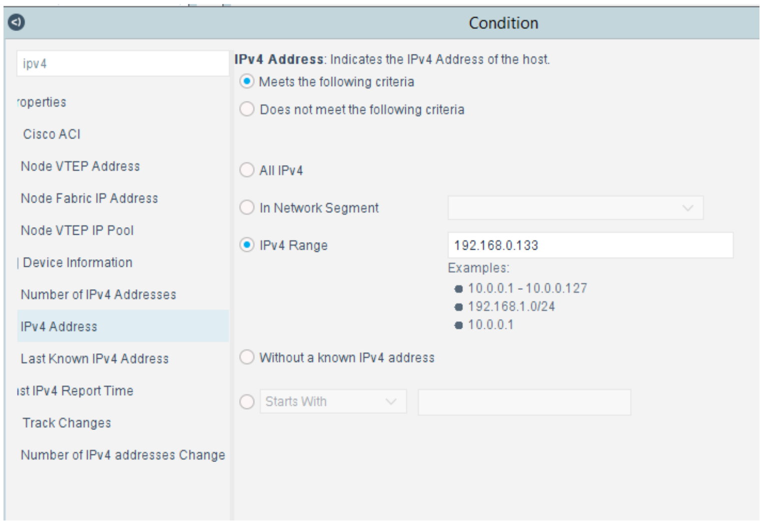
A host matches this rule if it meets the following condition:

One criterion is True

Criteria
IPv4 Address - 192.168.0.133

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:



Condition

ipv4

'operties
Cisco ACI
Node VTEP Address
Node Fabric IP Address
Node VTEP IP Pool
| Device Information
Number of IPv4 Addresses
IPv4 Address
Last Known IPv4 Address
ıst IPv4 Report Time
Track Changes
Number of IPv4 addresses Change

IPv4 Address: Indicates the IPv4 Address of the host.

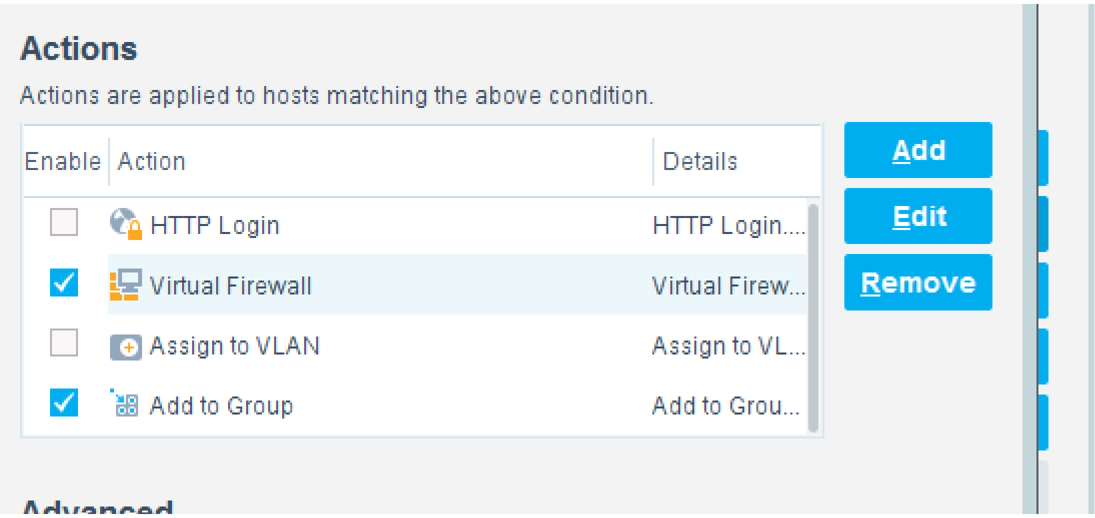
● Meets the following criteria
○ Does not meet the following criteria

○ All IPv4
○ In Network Segment
● IPv4 Range 192.168.0.133

Examples:
- 10.0.0.1 - 10.0.0.127
- 192.168.1.0/24
- 10.0.0.1

○ Without a known IPv4 address
○ Starts With

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:

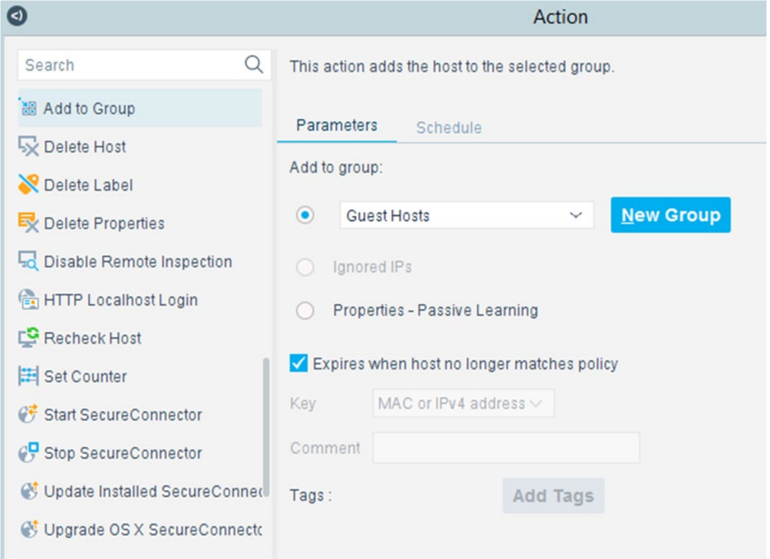


Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
☐	HTTP Login	HTTP Login....
☑	Virtual Firewall	Virtual Firew...
☐	Assign to VLAN	Assign to VL...
☑	Add to Group	Add to Grou...

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:



This action adds the host to the selected group.

Add to group:

● Guest Hosts

○ Ignored IPs

○ Properties - Passive Learning

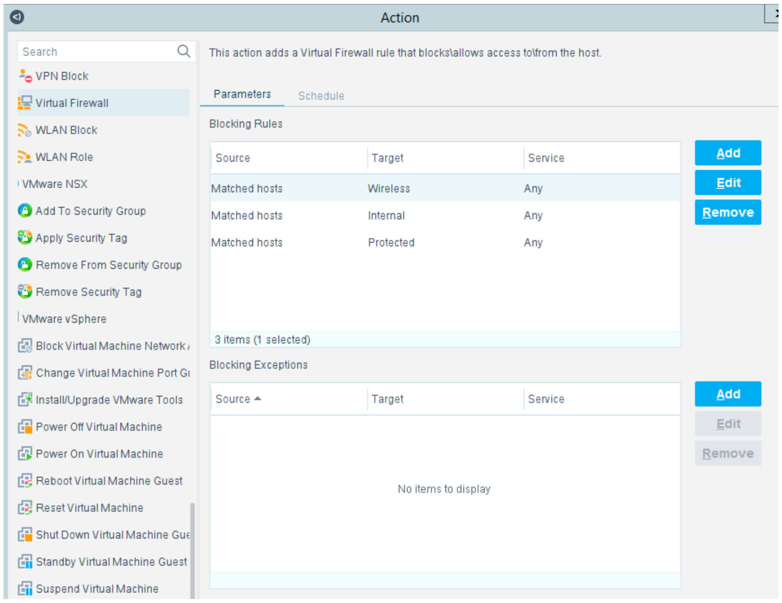
☑ Expires when host no longer matches policy

Key: MAC or IPv4 address

Comment:

Tags :

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:



This action adds a Virtual Firewall rule that blocks\allows access to\from the host.

Blocking Rules

Source	Target	Service
Matched hosts	Wireless	Any
Matched hosts	Internal	Any
Matched hosts	Protected	Any

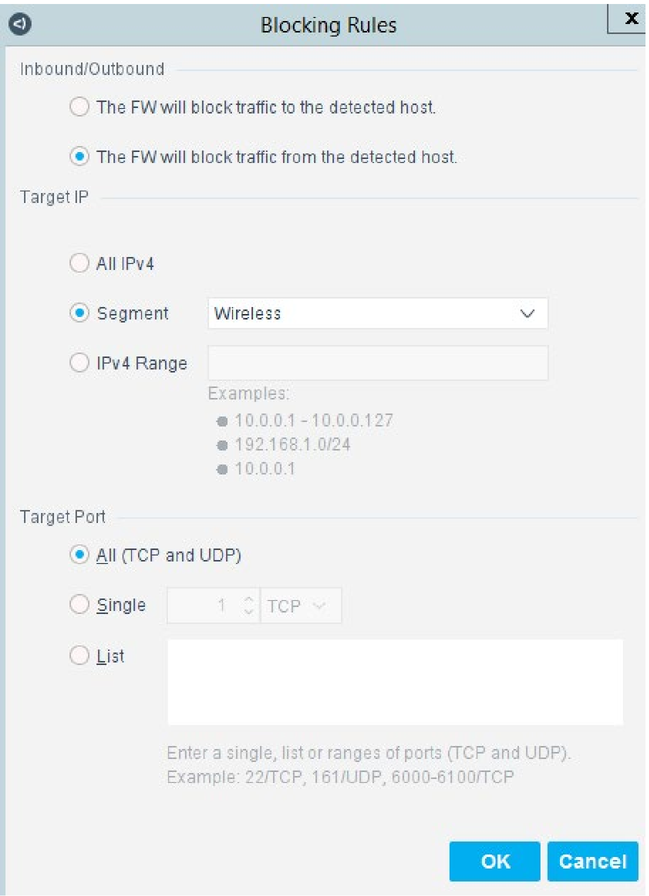
3 items (1 selected)

Blocking Exceptions

Source ▲	Target	Service

No items to display

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



Blocking Rules

Inbound/Outbound

○ The FW will block traffic to the detected host.

● The FW will block traffic from the detected host.

Target IP

○ All IPv4

● Segment Wireless

○ IPv4 Range

Examples:
- 10.0.0.1 - 10.0.0.127
- 192.168.1.0/24
- 10.0.0.1

Target Port

● All (TCP and UDP)

○ Single 1 TCP

○ List

Enter a single, list or ranges of ports (TCP and UDP).
Example: 22/TCP, 161/UDP, 6000-6100/TCP

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 default-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 reference design 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

2FA	Multifactor Authentication
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
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PCI	Payment Card Industry
PHP	Hypertext Preprocessor
PMS	Property Management System
RDP	Remote Desktop Protocol

SAKA	StrongAuth KeyAppliance
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transport Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
ZTA	Zero Trust Architecture

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

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