NIST SPECIAL PUBLICATION 1800-32C

# Securing the Industrial Internet of Things:

## Cybersecurity for Distributed Energy Resources

**Volume C:**
**How-To Guides**

**Jim McCarthy**
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

**Don Faatz**
**Nik Urlaub**
**John Wiltberger**
**Tsion Yimer**
The MITRE Corporation
McLean, Virginia

September 2021

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/iiot

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.

While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder's responsibility to fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise, and the impact should the threat be realized before adopting cybersecurity measures such as this recommendation.

National Institute of Standards and Technology Special Publication 1800-32C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-32C, 65 pages, (September 2021), CODEN: NSPUE2

## FEEDBACK

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

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

Public comment period: September 21, 2021, through October 20, 2021

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 and operational 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 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

The Industrial Internet of Things (IIoT) refers to the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport, energy, and other critical infrastructure sectors. In the energy sector, distributed energy resources (DERs) such as solar photovoltaics including sensors, data transfer and communications systems, instruments, and other commercially available devices that are networked together. DERs introduce information exchanges between a utility's distribution control system and the DERs to manage the flow of energy in the distribution grid.

This practice guide explores how information exchanges among commercial- and utility-scale DERs and electric distribution grid operations can be monitored and protected from certain cybersecurity threats and vulnerabilities.

The NCCoE built a reference architecture using commercially available products to show organizations how several cybersecurity capabilities, including communications and data integrity, malware detection, network monitoring, authentication and access control, and cloud-based analysis and visualization can be applied to protect distributed end points and reduce the IIoT attack surface for DERs.

## KEYWORDS

*data integrity; distributed energy resource; industrial internet of things; malware; microgrid; smart grid*

## ACKNOWLEDGMENTS

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

| Name | Organization |
|---|---|
| Mike Brozek | Anterix |
| Mark Poulin | Anterix |
| Moin Shaikh | Bedrock Systems |
| John Walsh | Bedrock Systems |
| Michael Harttree | Cisco |
| Matthew Hyatt | Cisco |
| Peter Romness | Cisco |
| Shanna Ramirez | CPS Energy |
| Pete Tseronis | Dots and Bridges |
| TJ Roe | Radiflow |
| Gavin Nicol | Spherical Analytics |
| Chris Rezendes | Spherical Analytics |
| Jon Rezendes | Spherical Analytics |

| Name | Organization |
|---|---|
| Scott Miller | Sumo Logic |
| Doug Natal | Sumo Logic |
| Rusty Hale | TDi Technologies |
| Bill Johnson | TDi Technologies |
| Samantha Pelletier | TDi Technologies |
| Don Hill | University of Maryland |
| Kip Gering | Xage Security |
| Justin Stunich | Xage Security |
| Andy Sugiarto | Xage Security |

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 | Product |
|---|---|
| Anterix | LTE infrastructure and communications on wireless broadband |
| Cisco | Cisco Identity Services Engine; Cisco Cyber Vision; Cisco Firepower Threat Defense |
| Dots and Bridges | subject matter expertise |
| Radiflow | iSID Industrial Threat Detection |
| Spherical Analytics | Immutably™, Proofworks™, and Scrivener™ |

| Technology Partner/Collaborator | Product |
|---|---|
| Sumo Logic | Sumo Logic Enterprise |
| TDi Technologies | ConsoleWorks |
| University of Maryland | campus DER microgrid infrastructure |
| Xage Security | Xage Security Fabric |

# DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

# CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: energy_nccoe@nist.gov

# Contents

## List of Figures

# 1 Introduction

This volume of the guide shows information technology (IT) professionals and security engineers how we implemented the 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, these volumes show how we incorporated the products together in our environment.

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

## 1.1 How to Use this Guide

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference architecture and provides users with the information they need to use this architecture to ensure trustworthy information exchange between a utility's distribution operations systems and a microgrid control system. This reference architecture is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST Special Publication (SP) 1800-32A: Executive Summary
- NIST SP 1800-32B: Approach, Architecture, and Security Characteristics – what we built and why
- NIST SP 1800-32C: 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 1800-32A*, which describes the following topics:

- challenges utilities and microgrid operators can face in securely exchanging control and status information
- example solution built at the National Cybersecurity Center of Excellence (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 1800-32B*, 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 3.4.4, Security Control Map and Technologies, maps the security characteristics of this reference architecture to cybersecurity standards and best practices.

You might share the *Executive Summary, NIST SP 1800-32A*, with your leadership team members to help them understand the importance of adopting standards-based approaches to trustworthy information exchanges between distribution operations (distribution ops) and microgrid control systems.

**IT and operational technology (OT) 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 1800-32C*, to replicate all or parts of the example solution created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT and OT 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 the example solution to provide trustworthy information exchanges. Your organization's security experts should identify the products that will best integrate with your existing tools and OT infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 2, Product Installation Guides, lists the products that we used and explain how they are used in the example solution to implement the reference architecture.

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

## 1.2 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. |

## 1.3 Reference Architecture Summary

The reference architecture has three parts:

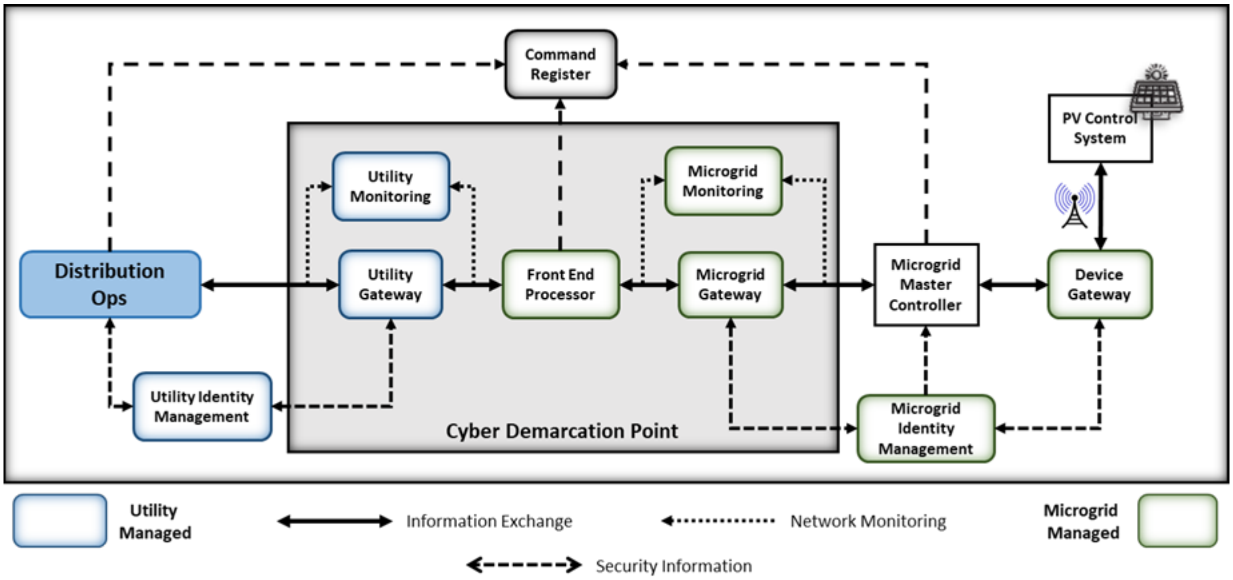
- information exchange, monitoring, and command register (Figure 1-1)
- log collection, data analysis and visualization (Figure 1-2)
- privileged user management (Figure 1-3)

The information exchange, monitoring, and command register portion of the architecture provides those gateway (GW) elements that ensure only authorized entities can exchange information, monitoring elements that detect anomalous and potentially malicious activities, and a command register that captures a complete record of all information exchanges. This portion of the reference architecture consists of:

- The **utility GW** component implements the utility's access policy.
- The **front-end processor** component receives information requests from the utility GW , records them in the command register, and forwards them to the microgrid GW.
- The **microgrid GW** component implements the microgrid access policy.
- The **utility cyber monitoring** component examines network and application traffic on the utility network and alerts utility cybersecurity personnel if anomalous activity is detected.

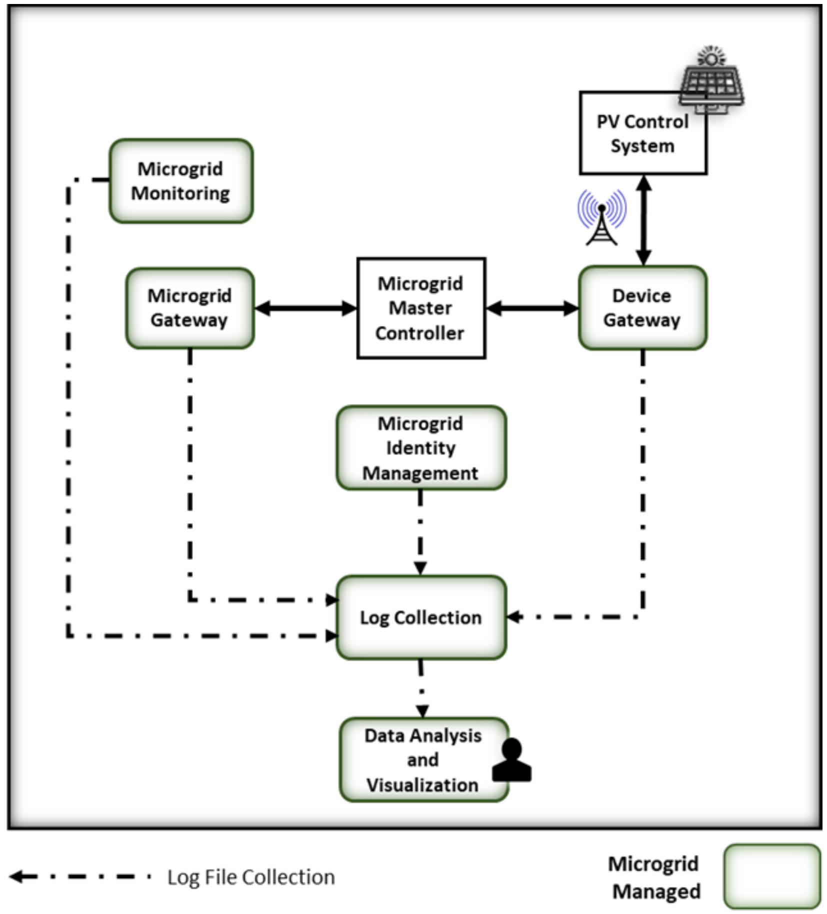
- The **microgrid cyber monitoring** component examines network and application traffic on the microgrid network and alerts microgrid cybersecurity personnel if anomalous activity is detected.
- The **distribution ops systems** record every information exchange they originate in the command register.
- The **microgrid master controller** records every information exchange it receives from the microgrid GW in the command register and forwards appropriate commands to the device GW.
- The **device GW** implements a device-specific access policy.
- * The **command register** records all information exchanges in a distributed ledger.
- The **PV control system** controls the photovoltaic (PV) Distributed Energy Resource (DER).

**Figure 1-1 Information Exchange, Monitoring, and Command Register**



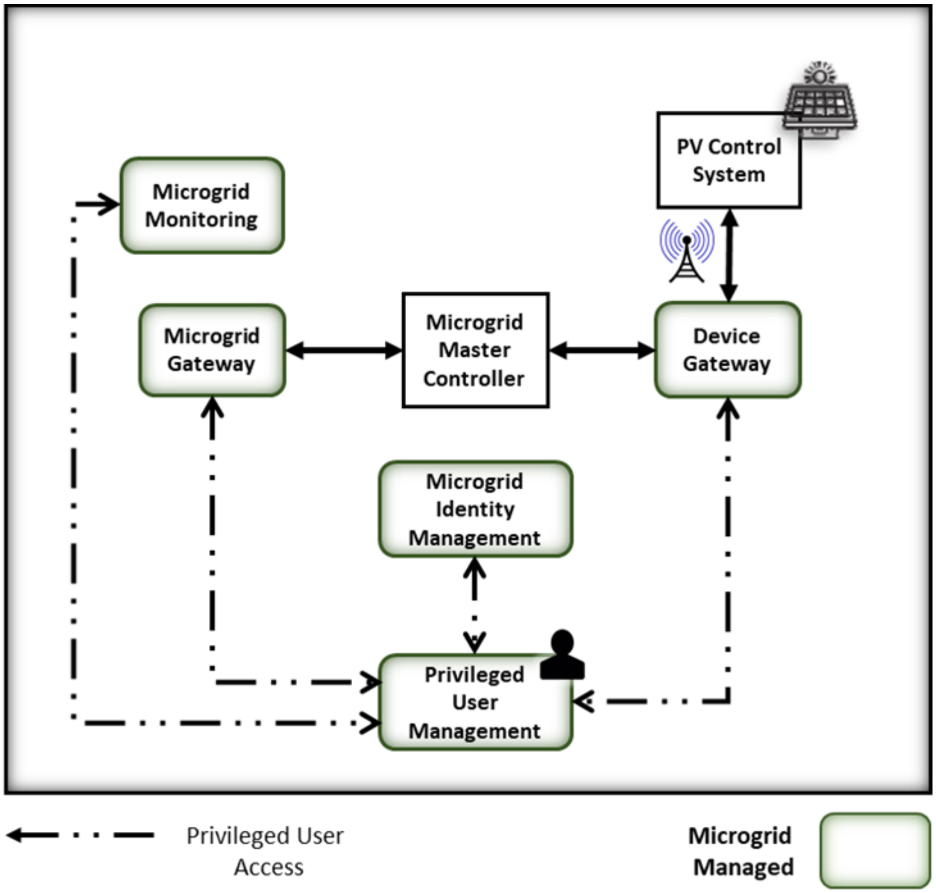
The log collection, data analysis and visualization portion of the reference architecture provides security information and event management capabilities for the microgrid operator and the ability to selectively share security-relevant information with the utility platform. The microgrid GW, microgrid monitoring device GW, and microgrid identity management elements of the reference architecture report event information to a log collection element. The log collection element forwards event information to an analysis and visualization capability that detects anomalies and reports them to microgrid operations personnel.

**Figure 1-2 Log Collection, Data Analysis, and Visualization**



The privileged user management portion of the reference architecture provides capabilities to manage the privileged users responsible for installation, configuration, operation, and maintenance of elements of the reference architecture. Privileged user management capabilities protect privileged access credentials, control access to management interfaces, and provide accountability for all privileged user actions in managing products on the microgrid.

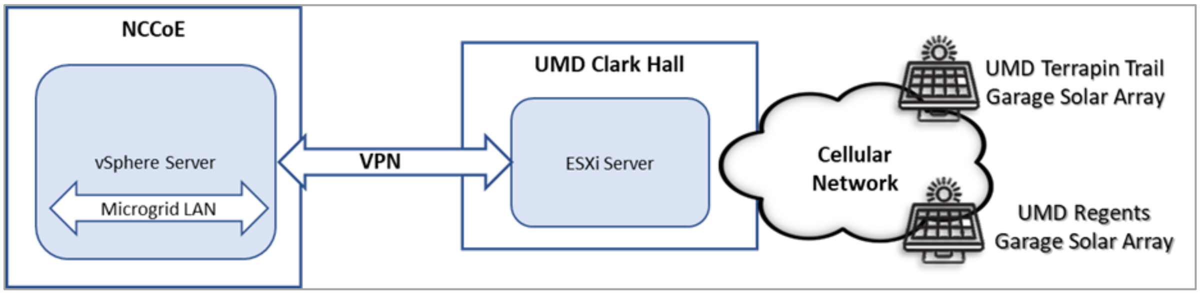
**Figure 1-3 Privileged User Management**



## 1.4 Laboratory Infrastructure

We constructed a laboratory prototype instance of the reference architecture, called the "example solution," to verify the design. The example solution is described in Section 1.5. The example solution consists of a combination of logical and physical infrastructure at the NCCoE and on the University of Maryland (UMD) campus. This section describes that laboratory infrastructure. Figure 1-4 presents a high-level overview of the project's lab infrastructure.

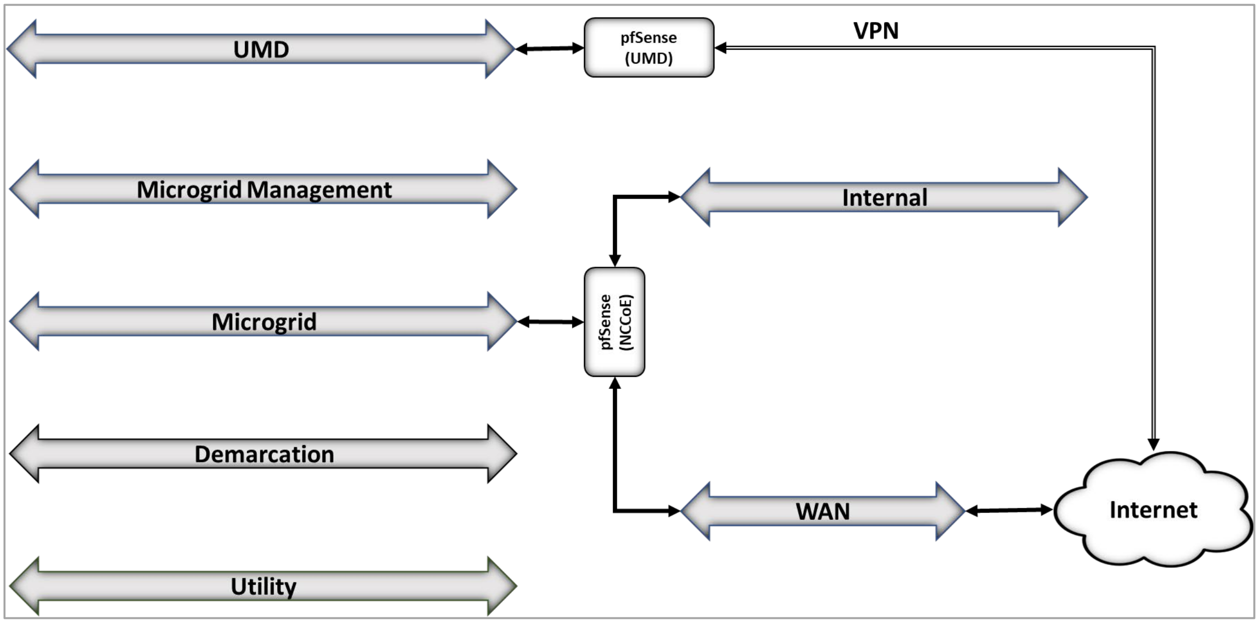
**Figure 1-4 Overview of Laboratory Infrastructure**



The core of our laboratory infrastructure is a virtual lab created in VMware vSphere 6.7. Within vSphere we defined several virtual networks. Each of these virtual networks represents a real-world network that would be part of a deployed instance of the reference architecture. Figure 1-5 illustrates these virtual networks.

A Virtual Private Network (VPN) connects the vSphere environment at NCCoE to UMD.

**Figure 1-5 Project Virtual Networks**

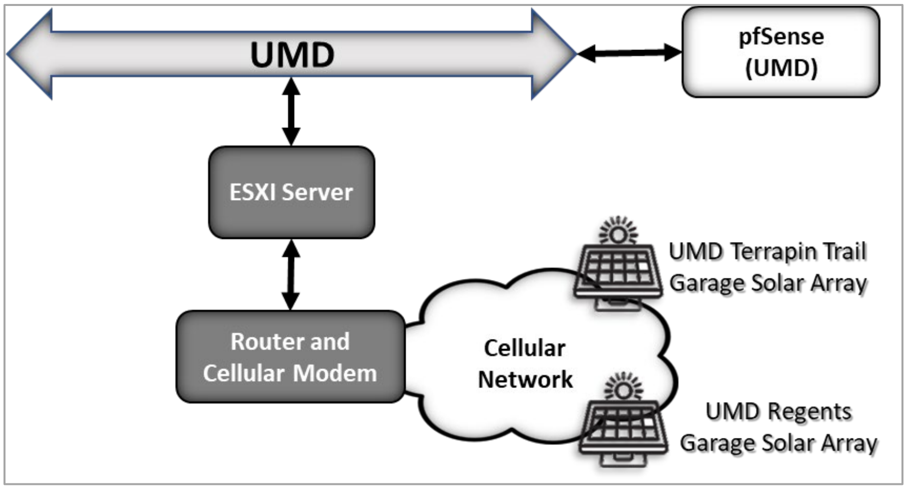


In addition to the core laboratory infrastructure, additional virtual and physical infrastructure was located at UMD's Clark Hall, Terrapin Trail parking garage, and Regents parking garage. Each of the parking garages has a rooftop solar array.

A vmWare ESXI server on the UMD campus network allows us to deploy software to UMD. A cellular network connects the ESXI server to the solar arrays on the two UMD parking garages.

Figure 1-6 illustrates the extended infrastructure at UMD.

**Figure 1-6 Project Infrastructure at UMD**


UMD
pfSense (UMD)
ESXI Server
Router and Cellular Modem
Cellular Network
UMD Terrapin Trail Garage Solar Array
UMD Regents Garage Solar Array

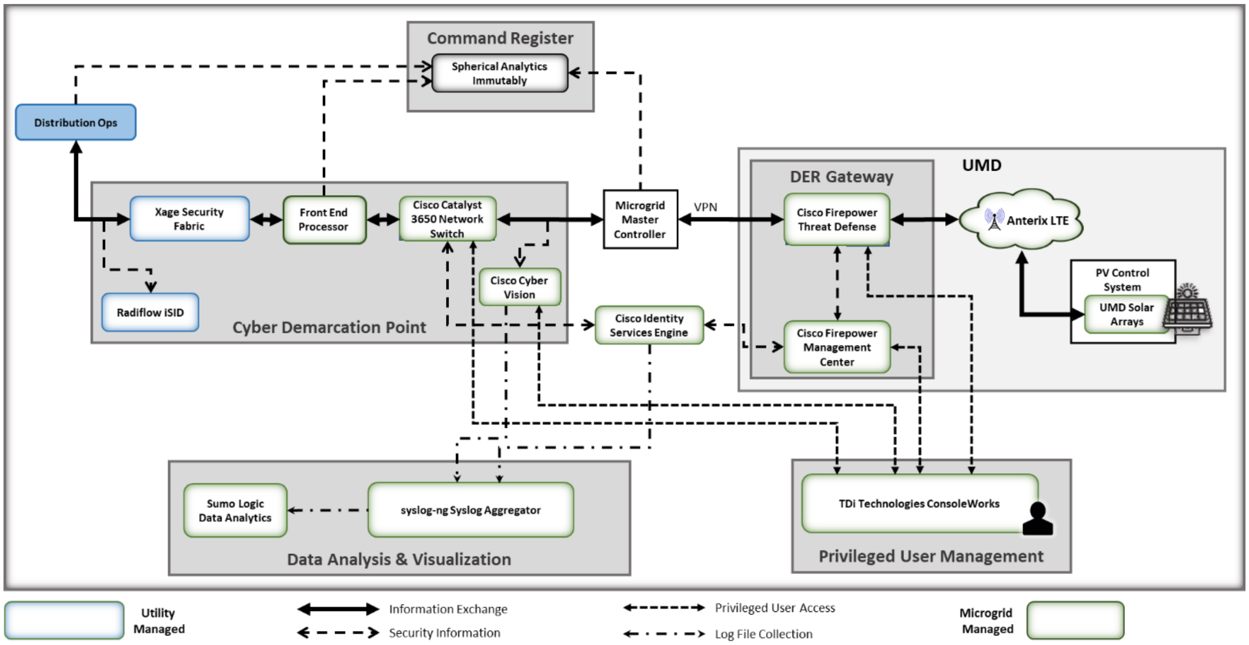
## 1.5 Example Solution Overview

Figure 1-7 shows how different products are integrated to create an implementation of the reference architecture referred to as the example solution.

The utility network and the cyber demarcation point of the reference architecture are represented in the example solution by virtual infrastructure in the NCCoE lab. The microgrid network is represented in the example solution by a virtual network in the NCCoE lab, the UMD campus network, and an LTE network installed on the UMD campus.

The components of the reference architecture's cyber demarcation are implemented using these products.

**Figure 1-7 Commercial Products Integrated into Example Solution**


Command Register
Spherical Analytics Immutably
Distribution Ops
Xage Security Fabric
Front End Processor
Cisco Catalyst 3650 Network Switch
Cisco Cyber Vision
Radiflow iSID
Cyber Demarcation Point
Microgrid Master Controller
VPN
UMD
DER Gateway
Cisco Firepower Threat Defense
Anterix LTE
PV Control System
UMD Solar Arrays
Cisco Identity Services Engine
Cisco Firepower Management Center
Sumo Logic Data Analytics
syslog-ng Syslog Aggregator
Data Analysis & Visualization
TDi Technologies ConsoleWorks
Privileged User Management
Utility Managed
Information Exchange
Security Information
Privileged User Access
Log File Collection
Microgrid Managed

The Xage Security Fabric is used to implement the utility identity management and utility GW component of the reference architecture. The Xage Security Fabric consists of five services, the Xage Broker, the Xage Manager, Xage Center nodes, a Xage Edge Node, and a Xage Enforcement Point. Installation and configuration of the Xage Security Fabric are described in Section 2.8.

Radiflow iSID is used to implement the utility monitoring component of the reference architecture. iSID is a single virtual appliance. Installation and configuration of Radiflow iSID are described in Section 2.4.1.

A Cisco Catalyst 3650 ISE-capable switch implements the microgrid GW component of the reference architecture. This switch requires the front-end processor to authenticate to connect. Further, the switch is policy enforcement point for access decisions made by ISE. ISE policy only allows the front-end processor to communicate with the Microgrid Master Controller.

A Cisco Firepower Threat Defense next-generation firewall implements the DER GW component of the reference architecture. This firewall requires the Microgrid Master Controller to authenticate to connect. Further, the firewall is a policy enforcement point for access decisions made by ISE. ISE policy only allows the Microgrid Master Controller to communicate with DERs.

Cisco Cyber Vision implements the microgrid monitoring component of the reference architecture. Cyber Vision is a single virtual appliance. Installation and configuration of Cisco Cyber Vision are described in Section 2.2.

The UMD solar arrays are not connected to the UMD campus network. Anterix designed and installed an LTE network to connect the solar arrays with our VPN enabling communication from the NCCoE lab to the solar arrays. Section 2.1 describes the Anterix design and implementation.

Cisco Identity Services Engine (ISE) provides the microgrid identity management component of the reference architecture. Authenticated identities and access policy decisions from Cisco ISE are enforced by the Cisco ISE-capable switches to control access to the Microgrid Master Controller and the DERs. Installation and configuration of Cisco ISE are described in Section 2.3.

Spherical Analytics Immutably implements the command register. Distribution ops systems, the front-end processor, and the microgrid master controller all send copies of information exchanges to Immutably's distributed ledger. Immutably is cloud-based software-as-a-service. Our configuration and use of Immutably are described in Section 2.5.

Distribution ops system, the front-end processor, and the microgrid master controller are emulated by NCCoE-developed software that sends copies of Modbus commands destined for the UMD solar arrays to Immutability.

The control systems of the UMD solar arrays represent the PV control system.

Sumo Logic implements the data analytics and visualization element of the reference architecture. Syslog data from the products and services in the cyber demarcation point and the microgrid are sent to Sumo Logic for aggregation, analysis, and visualization. Sumo Logic is a cloud-based software-as-a-service. Our configuration and use of Sumo Logic are described in Section 2.6.

TDi Technologies ConsoleWorks provides the privileged user management for products and services used on the microgrid. Access by privileged users to manage Cisco CyberVision and Cisco ISE is controlled by ConsoleWorks. Installation and configuration of ConsoleWorks are described in Section 2.7.

pfSense is used to create a virtual private network between the NCCoE lab and the UMD. pfSense is also used to control traffic out of the virtual lab to the Sumo Logic and Spherical Analytics cloud services. pfSense installation and configuration are described in Section 2.9.

syslog-ng is used to aggregate syslog data from products and services before sending the data to Sumo Logic. Installation and configuration of syslog-ng are described in Section 2.10.

# 2 Product Installation Guides

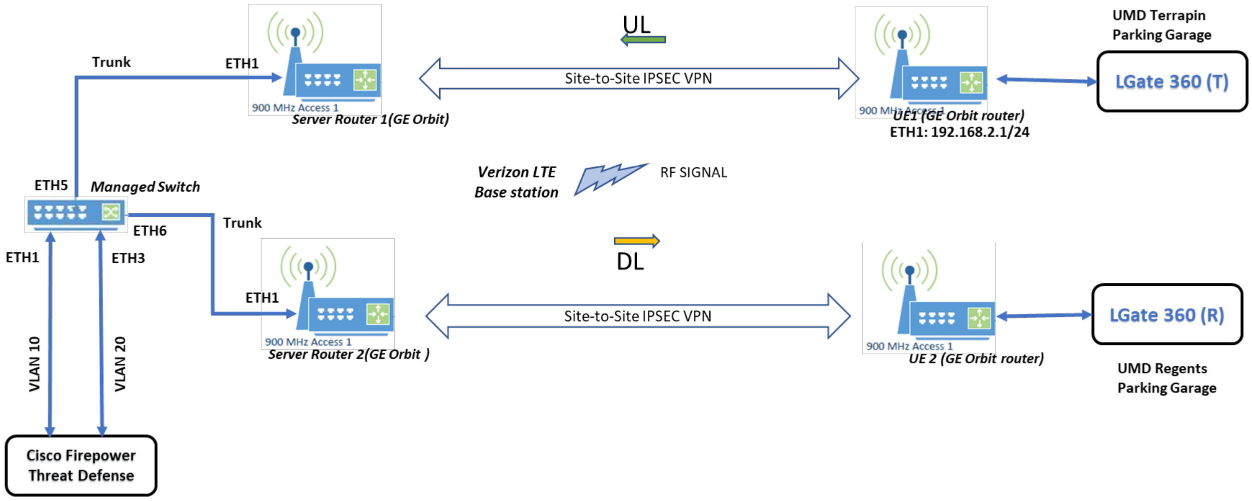
This section of the practice guide contains detailed instructions for installing and configuring all the products used in the example solution.

## 2.1 Anterix Long Term Evolution (LTE) Network

Anterix installed an LTE cellular network at UMD to provide connectivity from Clark Hall, where the NCCoE ESXI server is located, to the Regents and Terrapin Trail parking garages where the solar arrays are located. The installation included placing a router with a cellular interface at each parking garage and a managed network switch and two routers with cellular interfaces at Clark Hall. A point-to-point VPN is established over a cellular connection from a router in Clark Hall to a router at a parking garage.

A virtual Cisco Firepower Threat Defense next-generation firewallinstalled on  the NCCoE ESXI server at Clark Hall implements the reference architecture's device gateway. This firewall controls access to the Anterix-managed switch which provides connectivity to a cellular point-to-point VPN that connects to the solar arrays. The LGate 360s provide a connection point to the solar array control systems that implement the PV Control System of the reference architecture. Figure 2-1 illustrates the cellular network installation.

**Figure 2-1 Anterix Cellular Network Implementation**

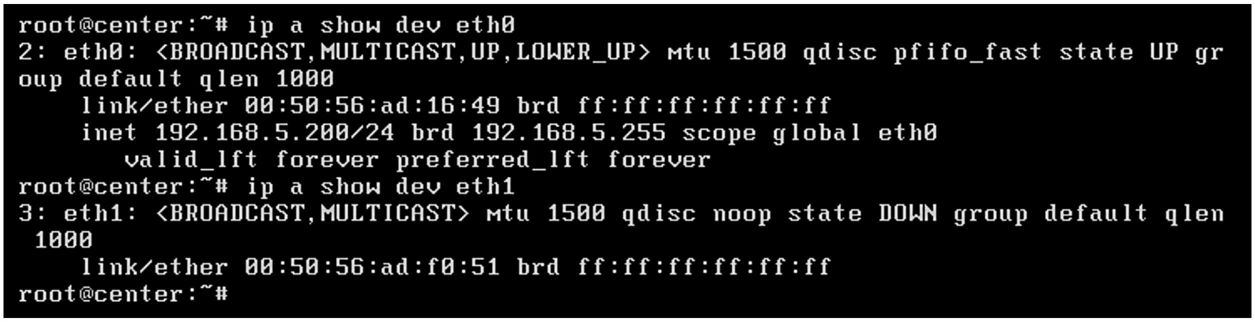


## 2.2 Cisco Cyber Vision

Cisco Cyber Vision implements the microgrid monitoring component of the reference architecture. It monitors the microgrid network for anomalous activity and provides alerts via syslog. These alerts are collected and sent to the data analysis and visualization component for presentation to microgrid operators.

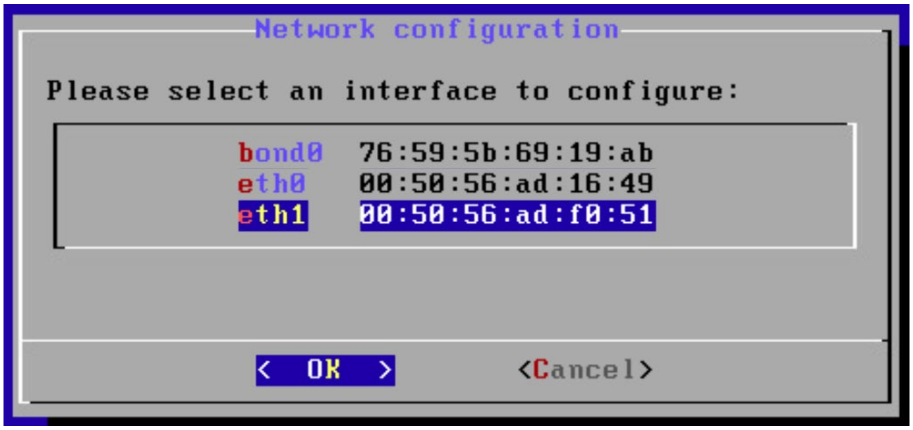
Cisco Cyber Vision was provided as a virtual appliance in an open virtualization appliance (OVA) file. The OVA file was deployed as a virtual machine in Sphere. We followed the instructions in Cisco's Cyber Vision All-in-One guide to complete the installation.

1. After the OVA has been deployed, check and verify the first network device (*eth0*) is used as the management interface by ensuring it has received an IP address. The second network device (*eth1*) should not have an IP address as that will be the monitoring port in this deployment. Note the MAC address (*link/ether* in the screenshot below) for *eth1* for the next step. When the MAC address is noted, type **`sbs-netconf`** to start the configuration process.

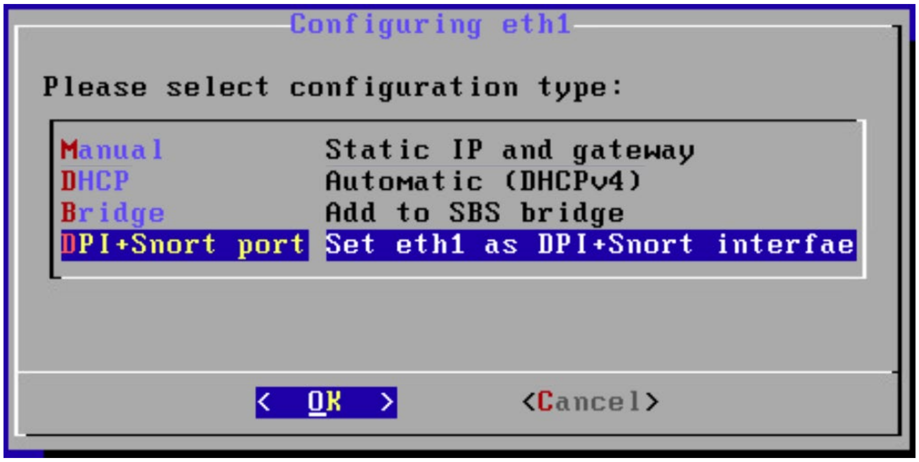


```
root@center:~# ip a show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 00:50:56:ad:16:49 brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.200/24 brd 192.168.5.255 scope global eth0
       valid_lft forever preferred_lft forever
root@center:~# ip a show dev eth1
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen
 1000
    link/ether 00:50:56:ad:f0:51 brd ff:ff:ff:ff:ff:ff
root@center:~#
```

2. Using the MAC address in the previous step, select the correct interface to activate the monitoring connection, then click **OK**.

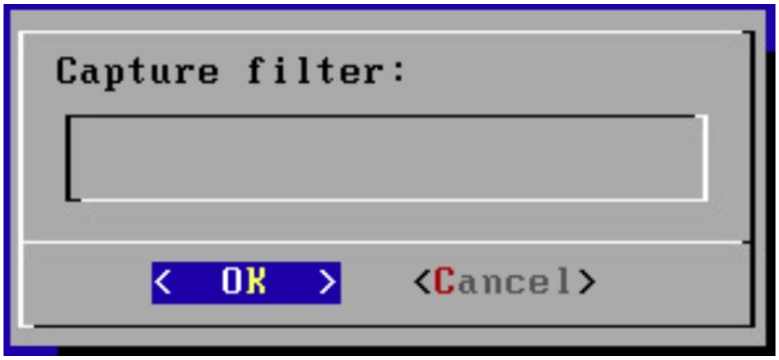


3. Select **DPI+Snort port** and click **OK**.

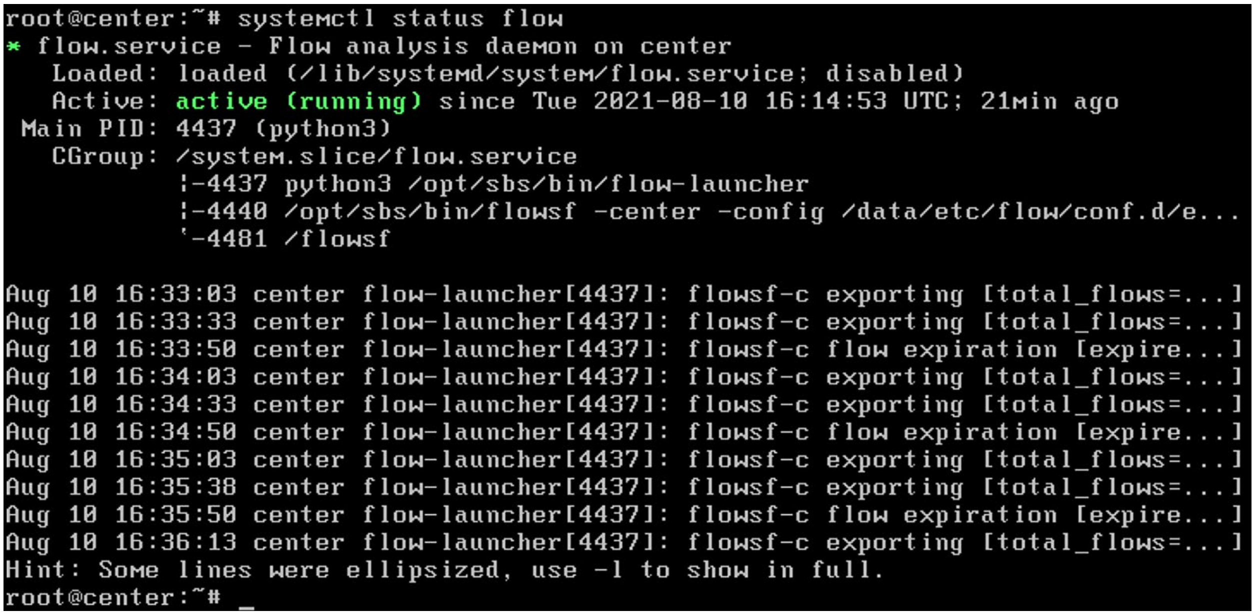


Configuring eth1
Please select configuration type:
Manual Static IP and gateway
DHCP Automatic (DHCPv4)
Bridge Add to SBS bridge
DPI+Snort port Set eth1 as DPI+Snort interfae
< OK >
<Cancel>

4. Leave the **Captur**e **filter**: block empty and click **OK.**

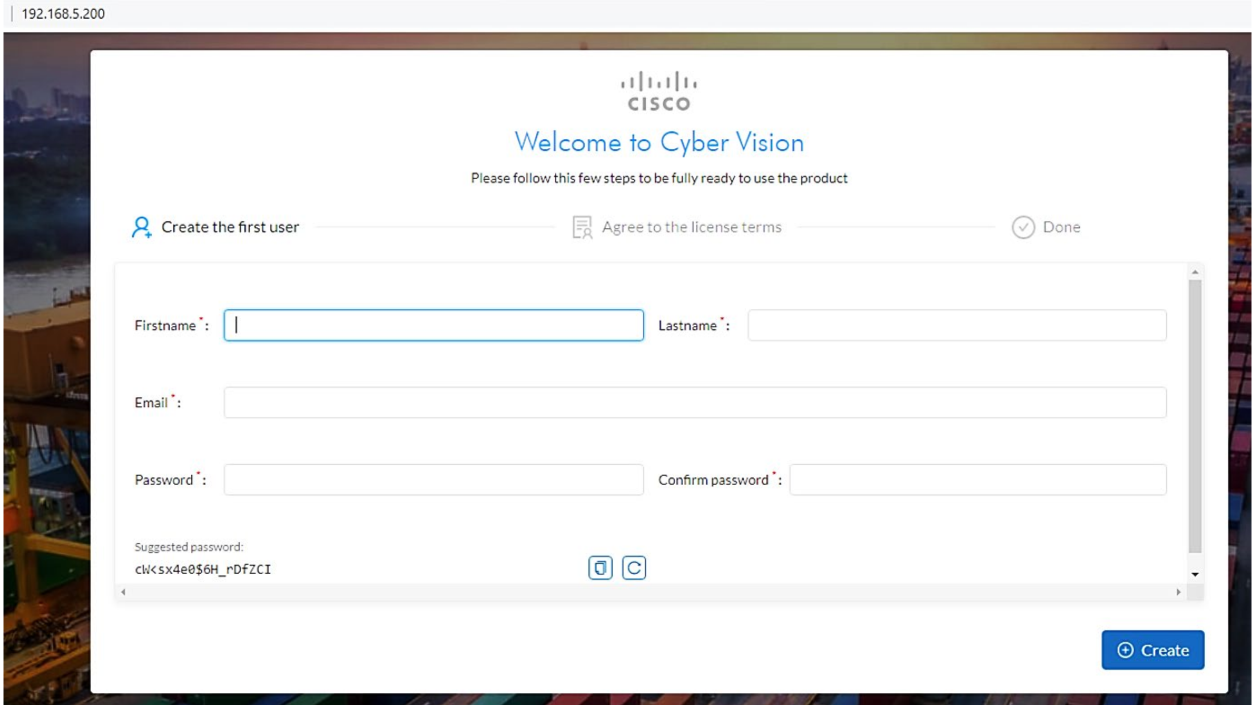


5. Verify that the service is running by typing **`systemctl status flow`** and verifying that the service is active and running.



```
root@center:~# systemctl status flow
* flow.service - Flow analysis daemon on center
   Loaded: loaded (/lib/systemd/system/flow.service; disabled)
   Active: active (running) since Tue 2021-08-10 16:14:53 UTC; 21min ago
 Main PID: 4437 (python3)
   CGroup: /system.slice/flow.service
           ├─4437 python3 /opt/sbs/bin/flow-launcher
           ├─4440 /opt/sbs/bin/flowsf -center -config /data/etc/flow/conf.d/e...
           └─4481 /flowsf

Aug 10 16:33:03 center flow-launcher[4437]: flowsf-c exporting [total_flows=...]
Aug 10 16:33:33 center flow-launcher[4437]: flowsf-c exporting [total_flows=...]
Aug 10 16:33:50 center flow-launcher[4437]: flowsf-c flow expiration [expire...]
Aug 10 16:34:03 center flow-launcher[4437]: flowsf-c exporting [total_flows=...]
Aug 10 16:34:33 center flow-launcher[4437]: flowsf-c exporting [total_flows=...]
Aug 10 16:34:50 center flow-launcher[4437]: flowsf-c flow expiration [expire...]
Aug 10 16:35:03 center flow-launcher[4437]: flowsf-c exporting [total_flows=...]
Aug 10 16:35:38 center flow-launcher[4437]: flowsf-c exporting [total_flows=...]
Aug 10 16:35:50 center flow-launcher[4437]: flowsf-c flow expiration [expire...]
Aug 10 16:36:13 center flow-launcher[4437]: flowsf-c exporting [total_flows=...]
Hint: Some lines were ellipsized, use -l to show in full.
root@center:~# _
```

6. Open up a browser on a system that is network routable to the Cyber Vision system and type the IP address into the URL. The **Welcome to Cyber Vision** screen shown below displays. Enter the user information and click **Create**.

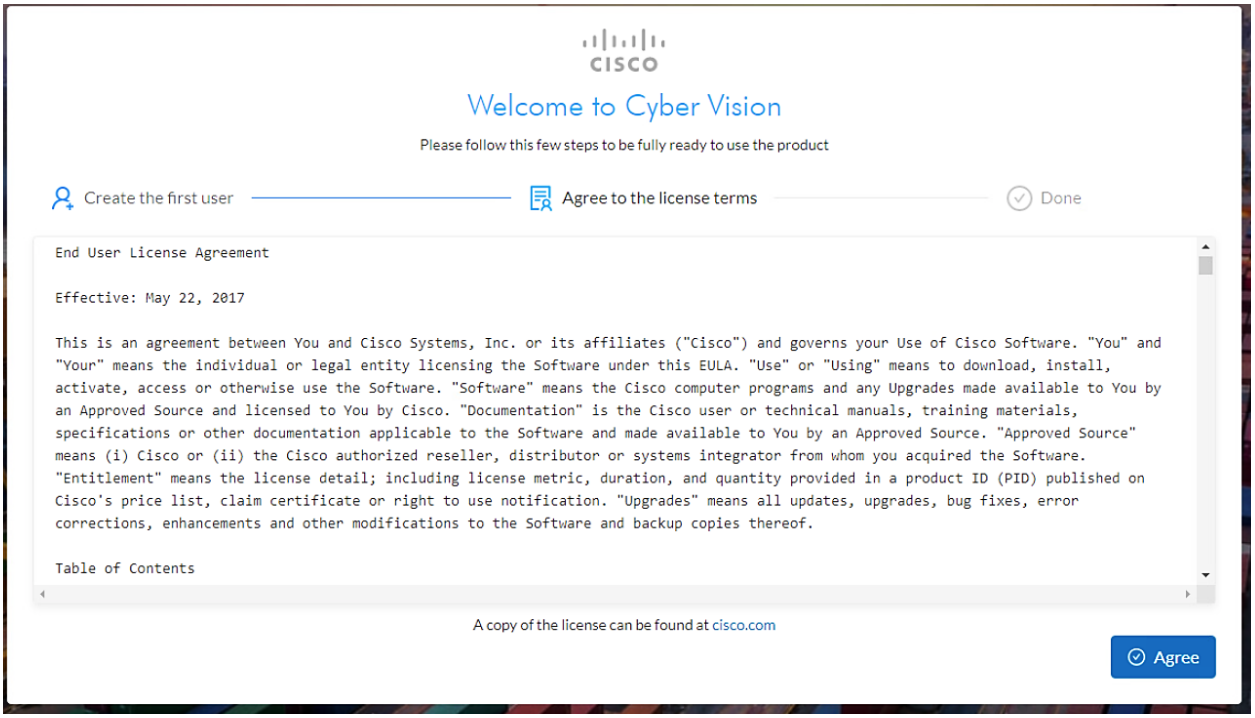


Welcome to Cyber Vision

Please follow this few steps to be fully ready to use the product

Suggested password:
cW<sx4e0$6H_rDfZCI

7. Read the EULA and click **Agree**.



Welcome to Cyber Vision

Please follow this few steps to be fully ready to use the product

End User License Agreement

Effective: May 22, 2017

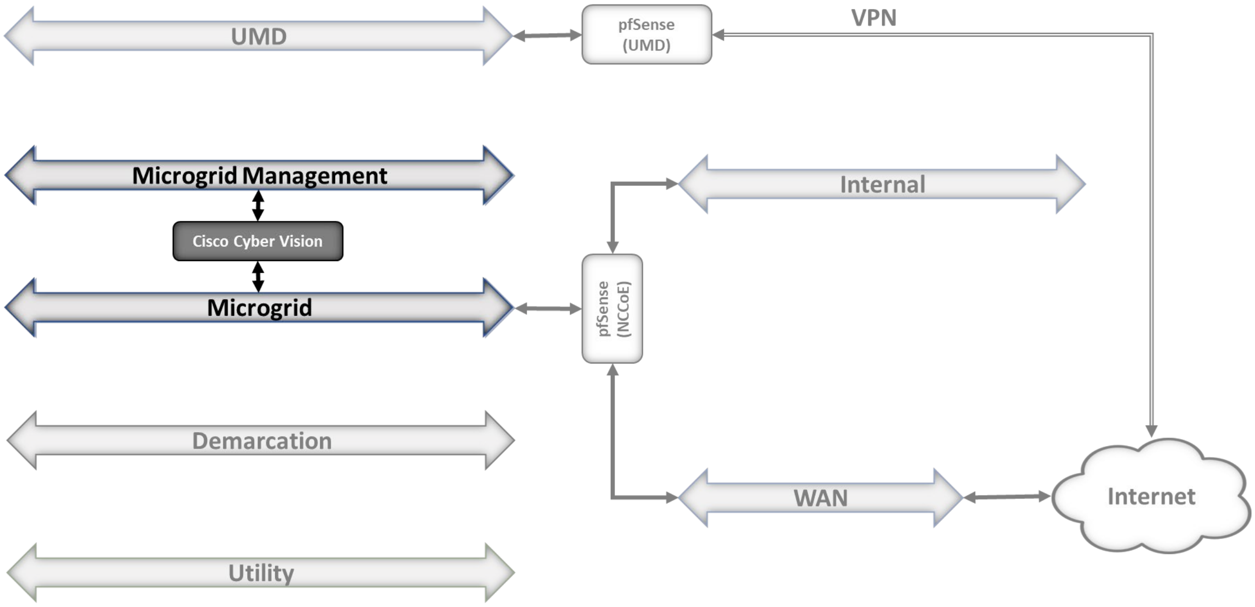
This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

Table of Contents

A copy of the license can be found at cisco.com

Figure 2-2 shows the location of Cisco Cyber Vision in the example solution.

**Figure 2-2 Cisco Cyber Vision in the Example Solution**



## 2.3 Cisco Identity Services Engine (ISE)

Cisco ISE provides the microgrid identity management component of the reference architecture. It works with Cisco ISE-enabled switches to provide authenticated identities that are used for access control.

### 2.3.1 Cisco ISE Installation and Configuration

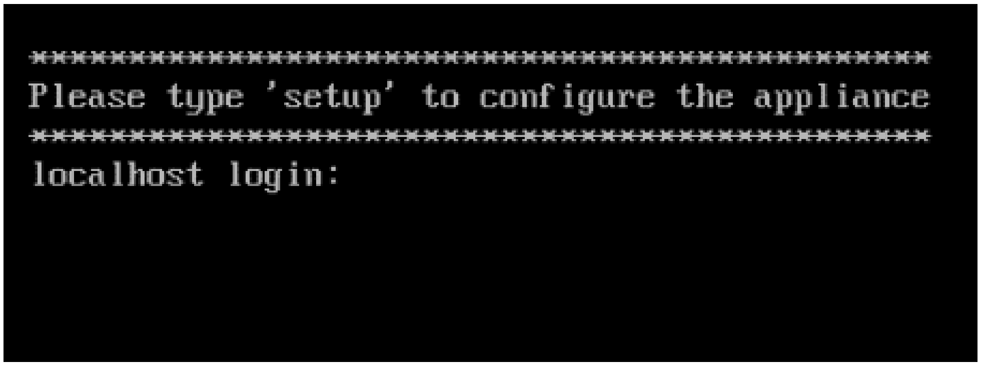
ISE was installed using the ISE 2.7 Installation Guide available at [https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/InstallGuide27/b_ise_InstallationGuide27/b_ise_InstallationGuide27_chapter_011.html#ID-1417-00000271](https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/InstallGuide27/b_ise_InstallationGuide27/b_ise_InstallationGuide27_chapter_011.html#ID-1417-00000271)

We followed steps 1 through 17 in the section titled “Configure a VMware Server” with the following selections:

- Step 8: Small, `16 cores`
- Step 12: `200Gb, thick-provisioned hard drive`

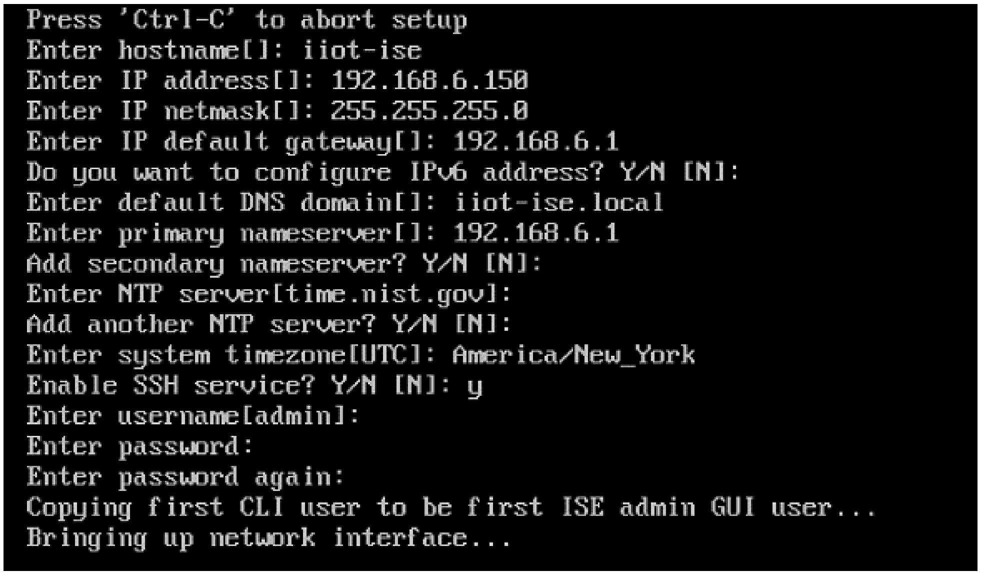
After completing the installation we used the setup guide at [https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/InstallGuide27/b_ise_InstallationGuide27/b_ise_InstallationGuide27_chapter_010.html#id_11096](https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/InstallGuide27/b_ise_InstallationGuide27/b_ise_InstallationGuide27_chapter_010.html#id_11096) to configure ISE.

1. Start up the VM for ISE that was created and type setup on the login screen:



```
**********************************************
Please type 'setup' to configure the appliance
**********************************************
localhost login:
```

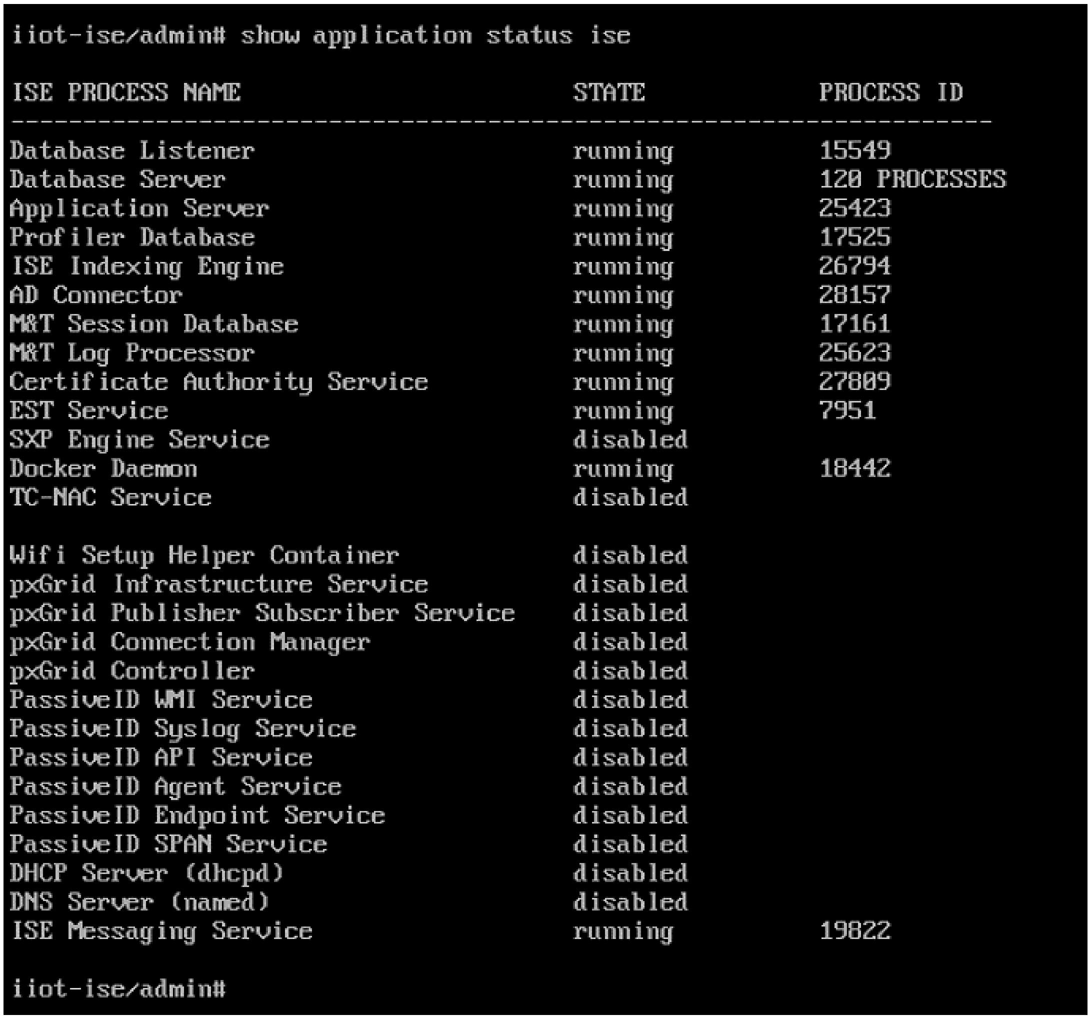
2. Fill in the appropriate information to configure the installation of ISE (as seen below):



```
Press 'Ctrl-C' to abort setup
Enter hostname[]: iiot-ise
Enter IP address[]: 192.168.6.150
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 192.168.6.1
Do you want to configure IPv6 address? Y/N [N]:
Enter default DNS domain[]: iiot-ise.local
Enter primary nameserver[]: 192.168.6.1
Add secondary nameserver? Y/N [N]:
Enter NTP server[time.nist.gov]:
Add another NTP server? Y/N [N]:
Enter system timezone[UTC]: America/New_York
Enable SSH service? Y/N [N]: y
Enter username[admin]:
Enter password:
Enter password again:
Copying first CLI user to be first ISE admin GUI user...
Bringing up network interface...
```

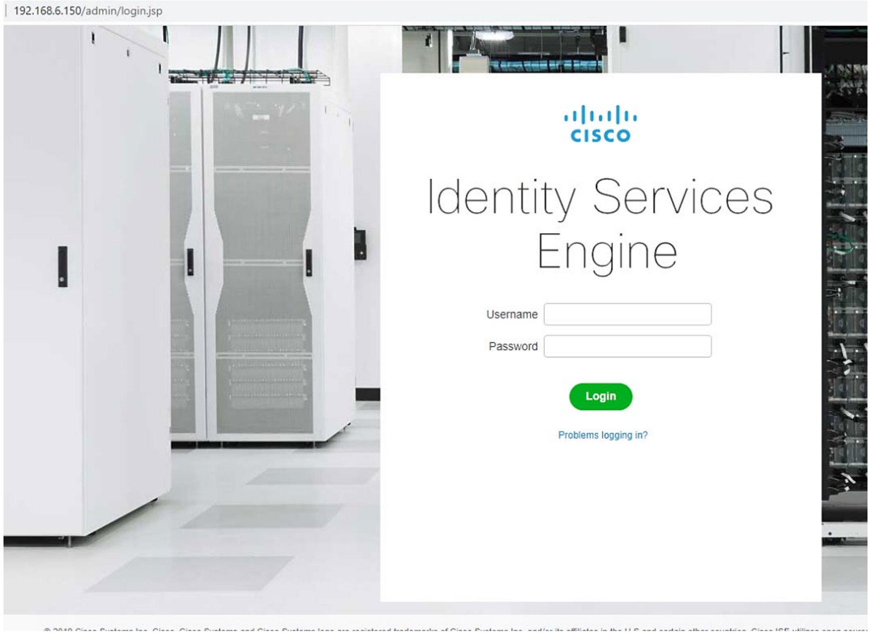
3. Once all configuration steps are complete, the ISE installation will begin. This may take several minutes.

4. Once installation is complete, log in to ISE and run **`show application status ise`** to verify ISE installation is complete.

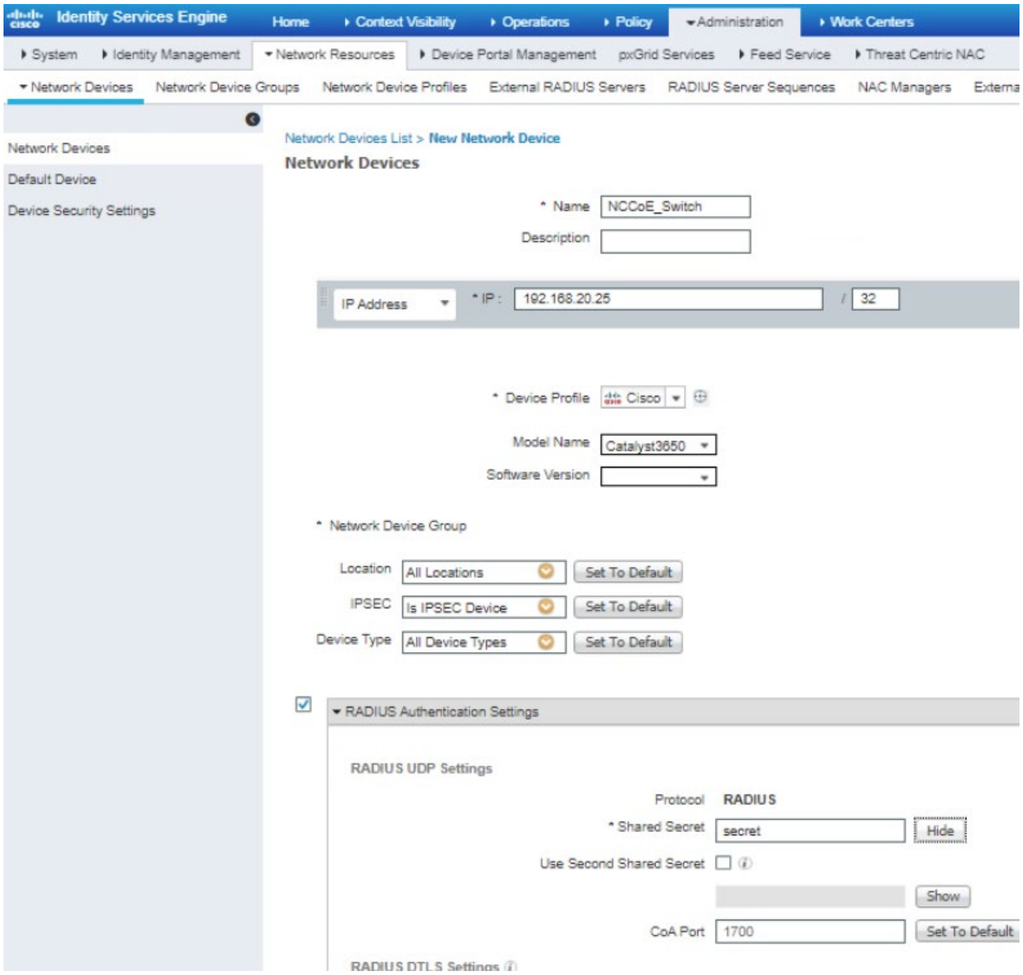


```
iiot-ise/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          15549
Database Server                        running          120 PROCESSES
Application Server                     running          25423
Profiler Database                      running          17525
ISE Indexing Engine                    running          26794
AD Connector                           running          28157
M&T Session Database                   running          17161
M&T Log Processor                      running          25623
Certificate Authority Service          running          27809
EST Service                            running          7951
SXP Engine Service                     disabled
Docker Daemon                          running          18442
TC-NAC Service                         disabled

Wifi Setup Helper Container            disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          19822

iiot-ise/admin#
```

5. Open a web browser and log into the Cisco ISE webserver.



6. Once complete, go to **Administration > Network Resources > Network Devices** and click **New Network Device**. Add the switch that will be configured to control access with the settings shown below.



Network Devices

* Name: NCCoE_Switch

Description:

IP Address * IP: 192.168.20.25 / 32

* Device Profile: Cisco

Model Name: Catalyst3650

Software Version:

* Network Device Group

Location: All Locations

IPSEC: Is IPSEC Device

Device Type: All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: secret

Use Second Shared Secret ☐

CoA Port: 1700

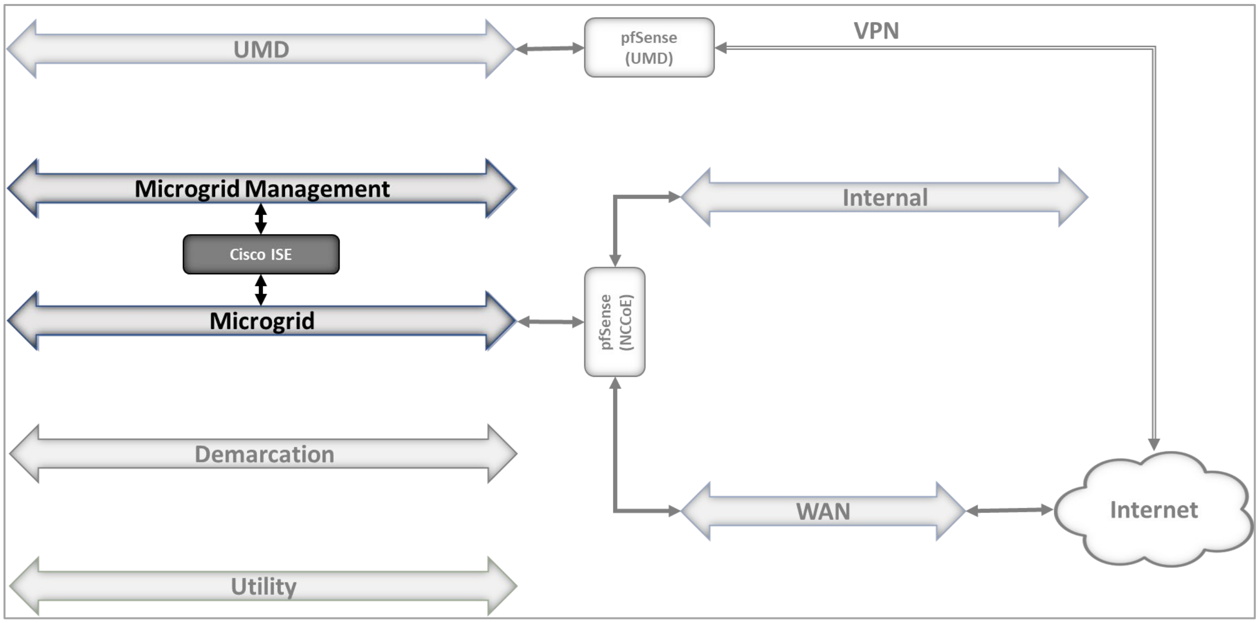
RADIUS DTLS Settings

7. We configured three identities in ISE:

- One identity was given access to both UMD solar arrays.
- One identity was given access to only one UMD solar array.
- One identity was given no access to the UMD solar arrays.

Figure 2-3 shows how Cisco ISE in positioned the example solution.

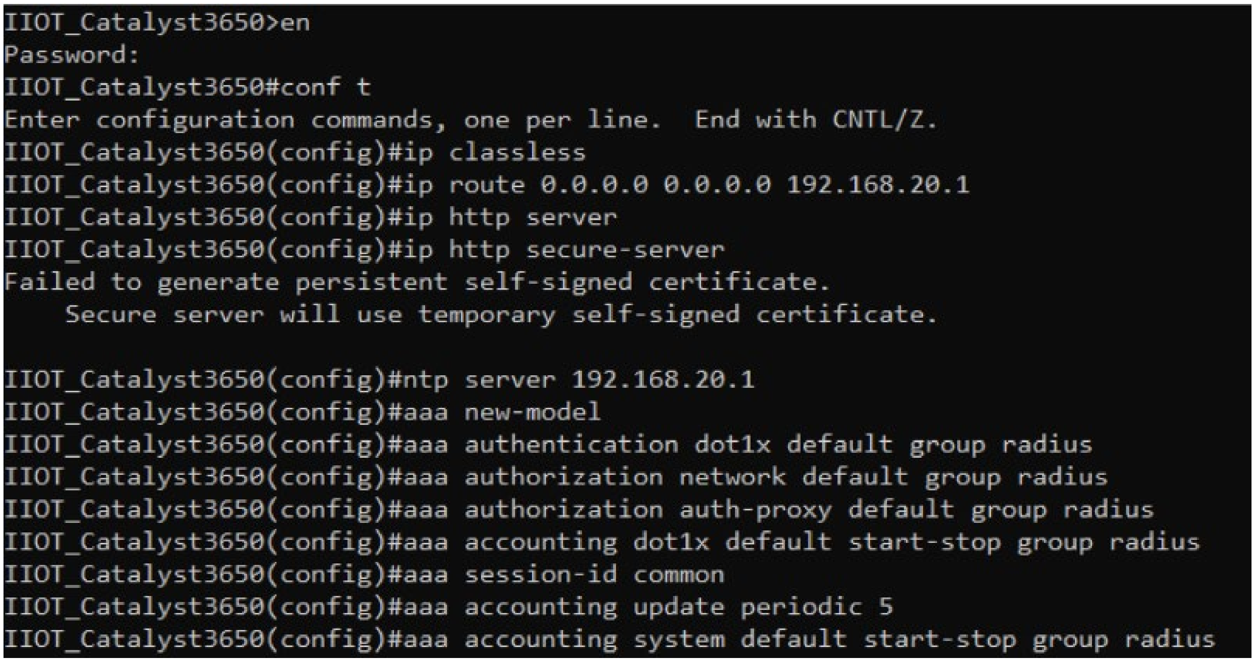
432 **Figure 2-3 Cisco ISE Position in the Example Solution**



433

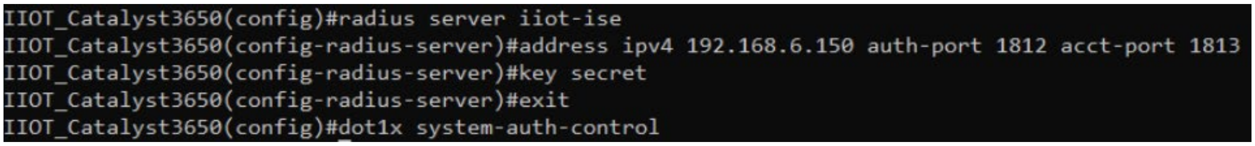
## 434 2.3.2 Cisco ISE Switch Settings

435 In order to integrate Cisco ISE with the switches in the NCCoE lab, switch configuration is required. Run 436 the required commands as shown in the following two screenshots.



```
IIOT_Catalyst3650>en
Password:
IIOT_Catalyst3650#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IIOT_Catalyst3650(config)#ip classless
IIOT_Catalyst3650(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.1
IIOT_Catalyst3650(config)#ip http server
IIOT_Catalyst3650(config)#ip http secure-server
Failed to generate persistent self-signed certificate.
    Secure server will use temporary self-signed certificate.

IIOT_Catalyst3650(config)#ntp server 192.168.20.1
IIOT_Catalyst3650(config)#aaa new-model
IIOT_Catalyst3650(config)#aaa authentication dot1x default group radius
IIOT_Catalyst3650(config)#aaa authorization network default group radius
IIOT_Catalyst3650(config)#aaa authorization auth-proxy default group radius
IIOT_Catalyst3650(config)#aaa accounting dot1x default start-stop group radius
IIOT_Catalyst3650(config)#aaa session-id common
IIOT_Catalyst3650(config)#aaa accounting update periodic 5
IIOT_Catalyst3650(config)#aaa accounting system default start-stop group radius
```

437



```
IIOT_Catalyst3650(config)#radius server iiot-ise
IIOT_Catalyst3650(config-radius-server)#address ipv4 192.168.6.150 auth-port 1812 acct-port 1813
IIOT_Catalyst3650(config-radius-server)#key secret
IIOT_Catalyst3650(config-radius-server)#exit
IIOT_Catalyst3650(config)#dot1x system-auth-control
```

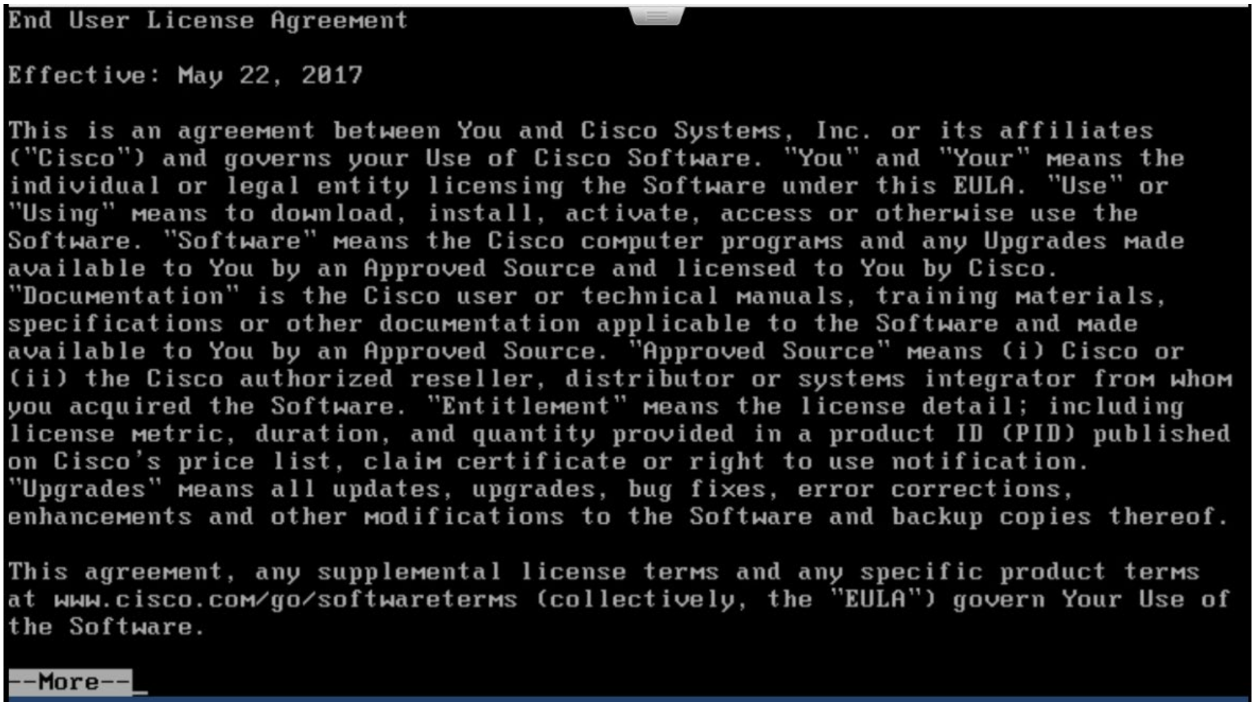
After completing the commands listed above, type exit then copy running-config startup-config to save the configuration to the switch.

## 2.3.3 Cisco Firepower Installation and Configuration

To handle identity authentication and authorization for protected resources at UMD, Cisco Firepower was utilized. Implementation included Firepower Management Center (FMC) and Firepower Threat Detection (FTD).

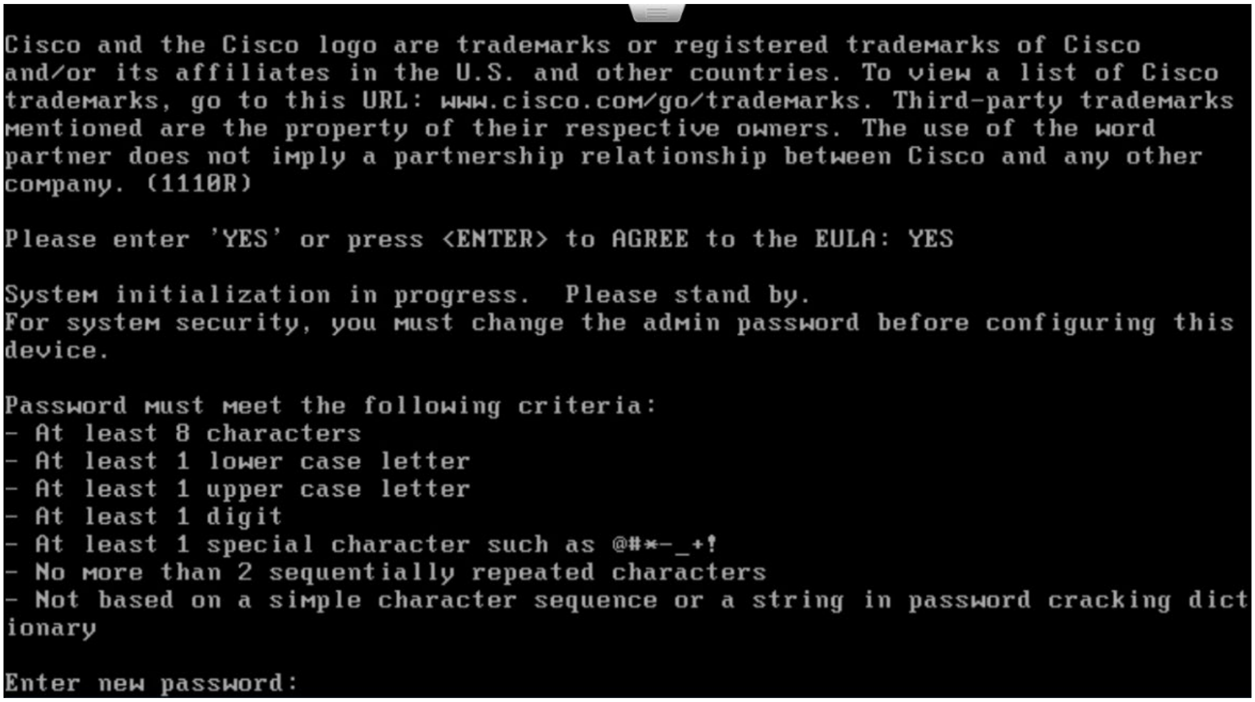
### *2.3.3.1 Cisco Firepower Threat Detection Installation and Configuration*

1. Obtain OVF and VMDK file from Cisco representative and deploy to virtual environment. Power on VM after deployment is completed.
2. Open VM Console and log in with username **admin** and password **Admin123**. Once logged in, view and accept the EULA.



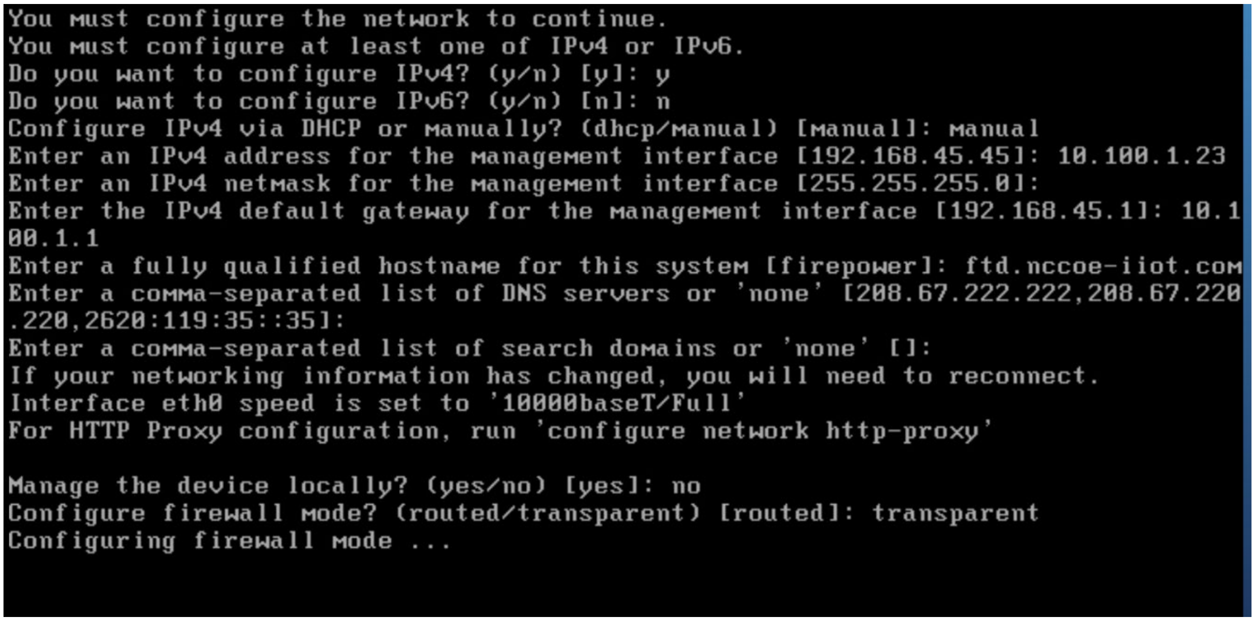
```
End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

This agreement, any supplemental license terms and any specific product terms
at www.cisco.com/go/softwareterms (collectively, the "EULA") govern Your Use of
the Software.

--More--_
```

3. Once completed, create a new password for the admin user.



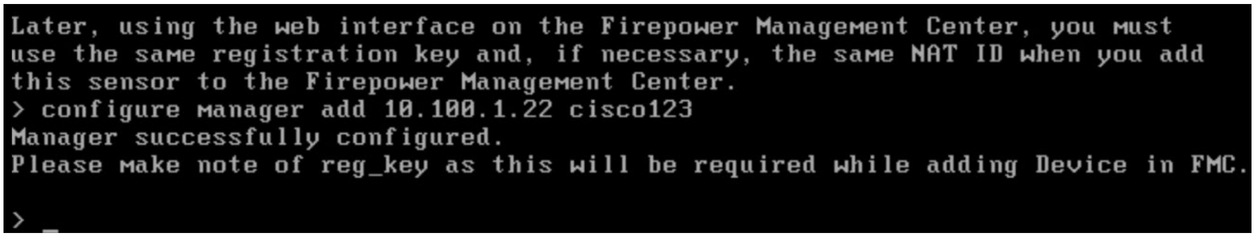
```
Cisco and the Cisco logo are trademarks or registered trademarks of Cisco
and/or its affiliates in the U.S. and other countries. To view a list of Cisco
trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks
mentioned are the property of their respective owners. The use of the word
partner does not imply a partnership relationship between Cisco and any other
company. (1110R)

Please enter 'YES' or press <ENTER> to AGREE to the EULA: YES

System initialization in progress.  Please stand by.
For system security, you must change the admin password before configuring this
device.

Password must meet the following criteria:
- At least 8 characters
- At least 1 lower case letter
- At least 1 upper case letter
- At least 1 digit
- At least 1 special character such as @#*-_+!
- No more than 2 sequentially repeated characters
- Not based on a simple character sequence or a string in password cracking dict
ionary

Enter new password:
```

4. Setup and configure network settings for FTD. Ensure that the device will not be managed locally and that the FTD system will run in transparent mode.



```
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.100.1.23
Enter an IPv4 netmask for the management interface [255.255.255.0]:
Enter the IPv4 default gateway for the management interface [192.168.45.1]: 10.1
00.1.1
Enter a fully qualified hostname for this system [firepower]: ftd.nccoe-iiot.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220
.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
Interface eth0 speed is set to '10000baseT/Full'
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]: transparent
Configuring firewall mode ...
```

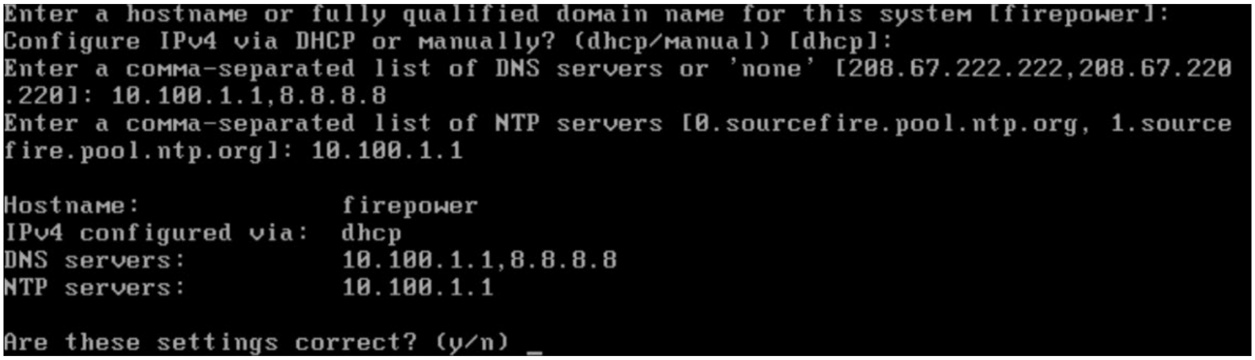
5. Configure the manager settings with the IP address of ISE and a registration key. The key opted to use in this build is **cisco123**. This key is required for integration into FMC.



```
Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
> configure manager add 10.100.1.22 cisco123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

> _
```

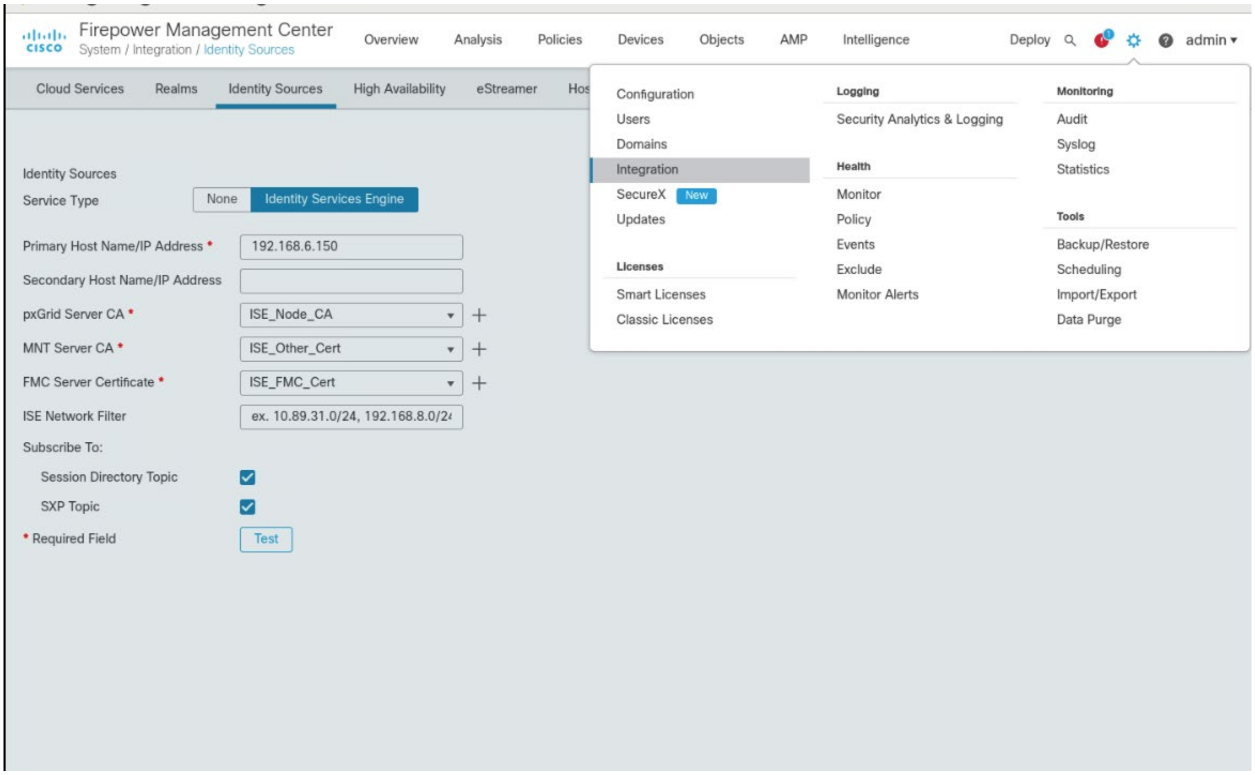
### 2.3.3.2 Cisco Firepower Management Center Installation and Configuration

1. Obtain OVF and VMDK file from Cisco representative and deploy to virtual environment. Power on VM after deployment is completed.
2. Open VM Console and log in with username **admin** and password **Admin123**. Once logged in, view and accept the EULA.
3. Configure network for FMC system. DHCP was utilized in this setup. Type **y** to verify configuration.



```
Enter a hostname or fully qualified domain name for this system [firepower]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [dhcp]:
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220
.220]: 10.100.1.1,8.8.8.8
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org, 1.source
fire.pool.ntp.org]: 10.100.1.1

Hostname:              firepower
IPv4 configured via:   dhcp
DNS servers:           10.100.1.1,8.8.8.8
NTP servers:           10.100.1.1

Are these settings correct? (y/n) _
```

4. Once logging in to the web interface for FMC, click the gear icon in the top left, then select **Integration.** Select the tab at the top entitled **Identity Sources**.



Identity Sources

Service Type: None | **Identity Services Engine**

Primary Host Name/IP Address *: 192.168.6.150

Secondary Host Name/IP Address:

pxGrid Server CA *: ISE_Node_CA

MNT Server CA *: ISE_Other_Cert

FMC Server Certificate *: ISE_FMC_Cert

ISE Network Filter: ex. 10.89.31.0/24, 192.168.8.0/2

Subscribe To:

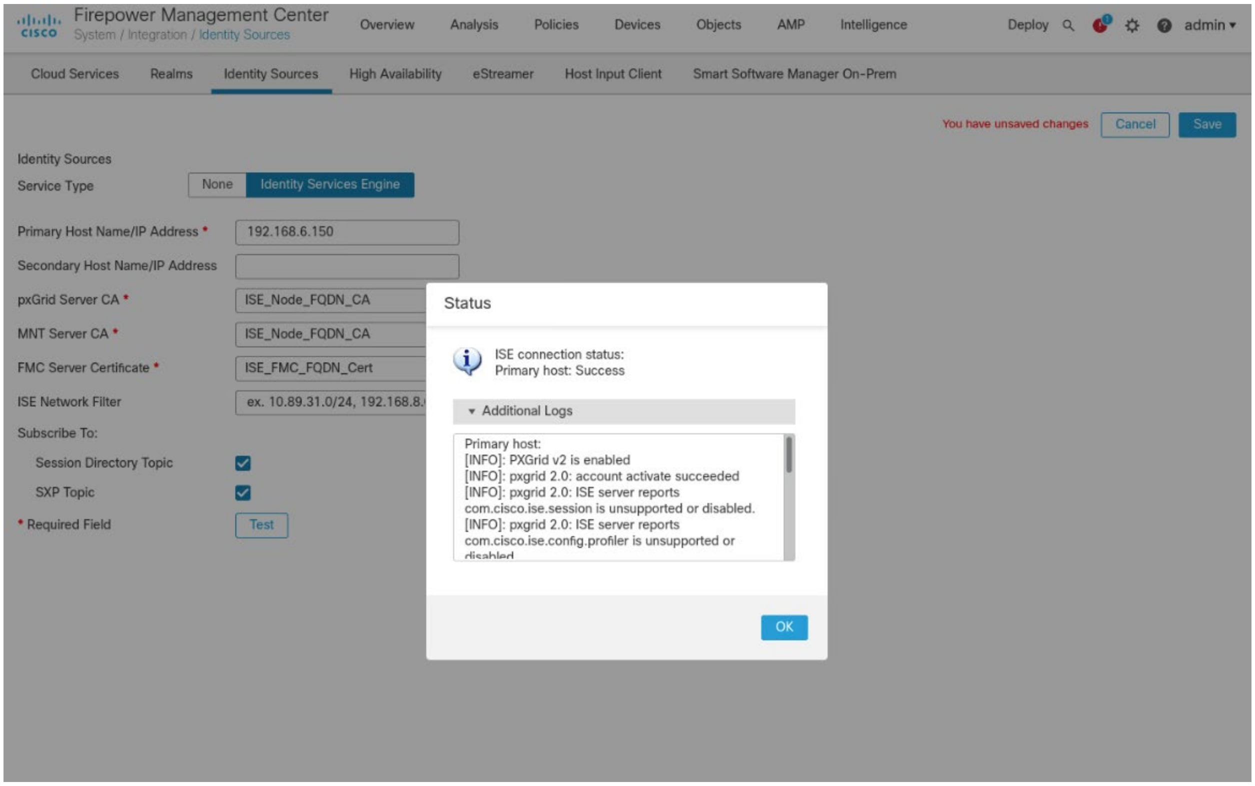
Session Directory Topic ☑

SXP Topic ☑

* Required Field

5. Fill out each line for the ISE instance. IP address or Fully Qualified Domain Name (FQDN), the pxGrid Server CA is the self-signed certificate in ISE, the same certificate is used for the MNT certificate, and the FMC Server Certificate is the certificate generated in ISE for the pxGrid. Ensure that the checkboxes for **Session Directory Topic** and **SXP Topic** are selected. Click **Test** to

verify successful connection, then click **Save**.



Identity Sources

Service Type: None | **Identity Services Engine**

Primary Host Name/IP Address *: 192.168.6.150

Secondary Host Name/IP Address:

pxGrid Server CA *: ISE_Node_FQDN_CA

MNT Server CA *: ISE_Node_FQDN_CA

FMC Server Certificate *: ISE_FMC_FQDN_Cert

ISE Network Filter: ex. 10.89.31.0/24, 192.168.8.

Subscribe To:

Session Directory Topic ☑

SXP Topic ☑

* Required Field

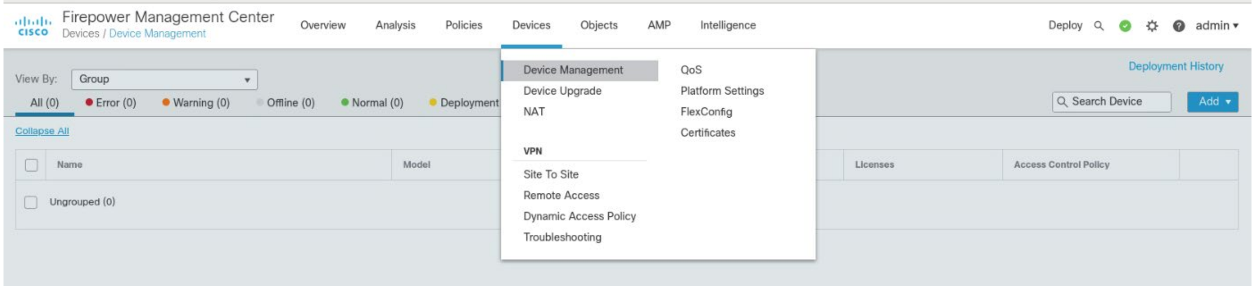
Status

ISE connection status:
Primary host: Success

Additional Logs

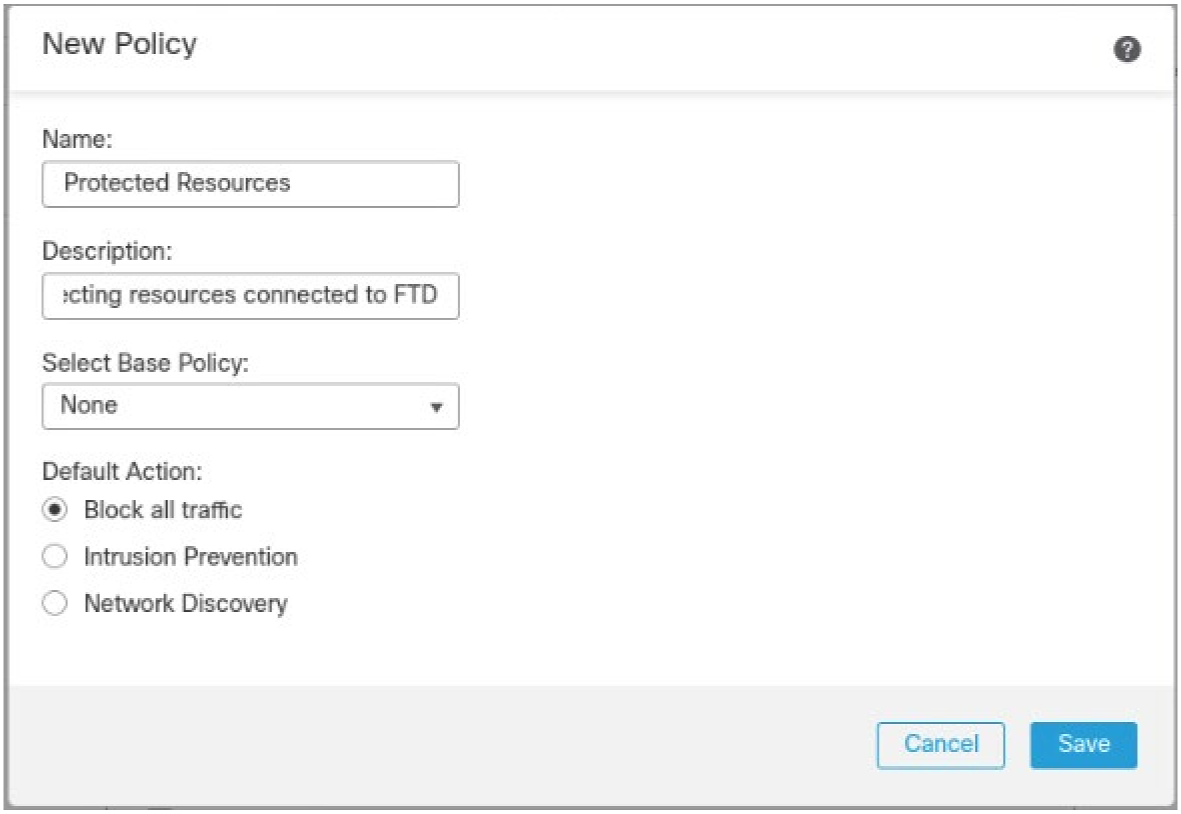
```
Primary host:
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: pxgrid 2.0: ISE server reports
com.cisco.ise.session is unsupported or disabled.
[INFO]: pxgrid 2.0: ISE server reports
com.cisco.ise.config.profiler is unsupported or
disabled
```

6. To add the FTD, select **Device** > **Device Management**, then click **Add**.



7. On the pop-up window, fill in all blanks, with the **Host** as the IP address of the FTD, a **Display Name**, and place copy the registration key created earlier to **Registration Key**. The lab used **cisco123** as the registration key. For **Access Control Policy**, click the drop-down box, then select **Create New Policy**. Give it a name, description, and ensure **Block all traffic** is selected as the

default action. Click **Save**.



New Policy

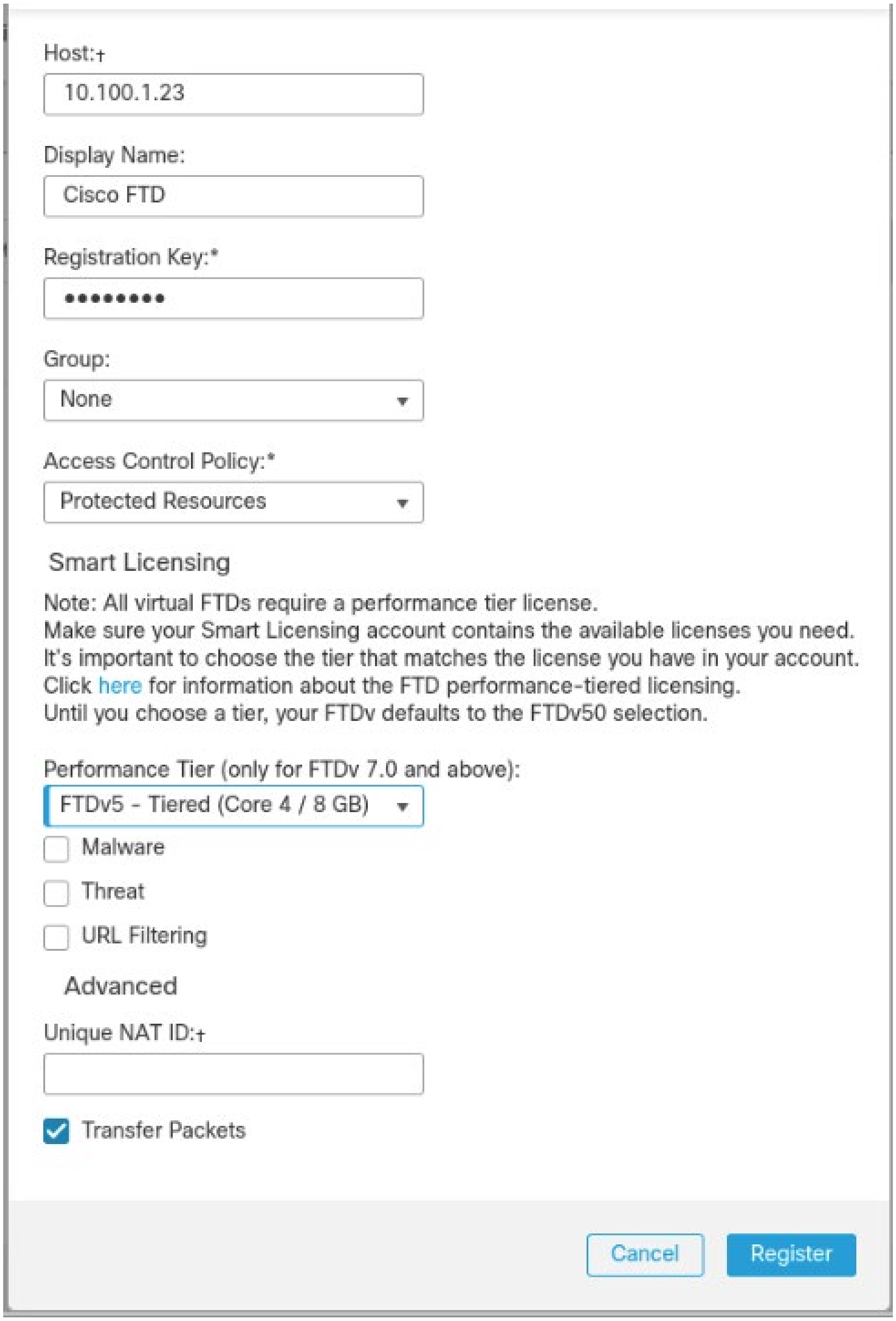
Name:
Protected Resources

Description:
:cting resources connected to FTD

Select Base Policy:
None

Default Action:
● Block all traffic
○ Intrusion Prevention
○ Network Discovery

8. Select **FTDv5** for the Performance Tier and click **Register**.



Host:†

10.100.1.23

Display Name:

Cisco FTD

Registration Key:*

●●●●●●●●●

Group:

None ▾

Access Control Policy:*

Protected Resources ▾

Smart Licensing

Note: All virtual FTDs require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the FTD performance-tiered licensing.
Until you choose a tier, your FTDv defaults to the FTDv50 selection.

Performance Tier (only for FTDv 7.0 and above):

FTDv5 - Tiered (Core 4 / 8 GB) ▾

□ Malware

□ Threat

□ URL Filtering

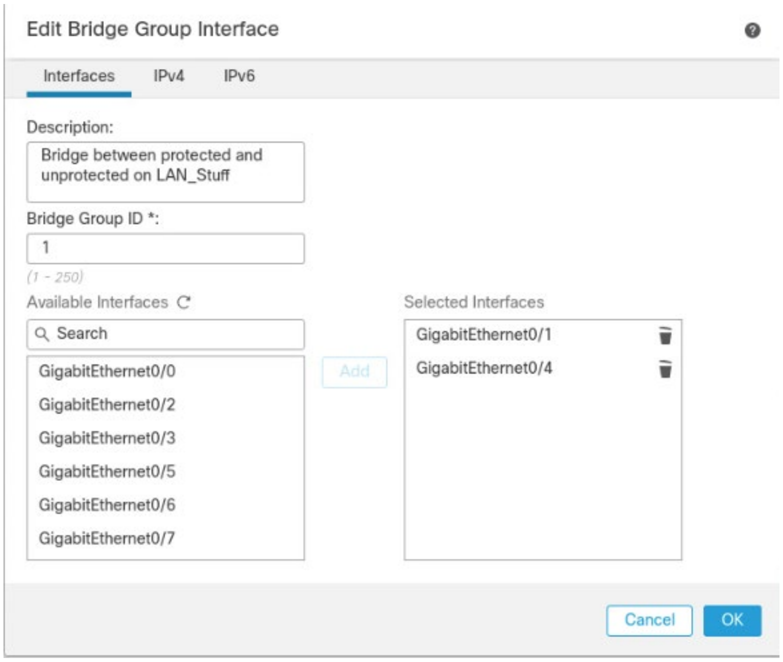
Advanced

Unique NAT ID:†

☑ Transfer Packets

9. The final setup required is to add a virtual interface. On the Device Management page, click the **Interfaces** tab if it is not already added, then click **Add Interfaces** on the left side of the screen. Then select **Bridge Group Interface**. Here we selected one interface for each side of the

transparent connection, then on the IPv4 tab assigned an IP address. The click **OK.**



Description:
Bridge between protected and unprotected on LAN_Stuff

Bridge Group ID *:
1
(1 - 250)

Available Interfaces
GigabitEthernet0/0
GigabitEthernet0/2
GigabitEthernet0/3
GigabitEthernet0/5
GigabitEthernet0/6
GigabitEthernet0/7

Selected Interfaces
GigabitEthernet0/1
GigabitEthernet0/4

## 2.4 Radiflow iSID

We implemented the utility cyber monitoring element of the reference architecture using Radiflow iSID. iSID is a passive monitoring, analysis, and detection platform that can be provided as either a physical or logical appliance. iSID learns the basic topology and behavior of the industrial control devices on the networks that it monitors. A typical deployment places an iSID appliance at a central location on the utility network and deploys iSAP smart collectors to various locations of interest on the utility network. In the example solution, for example, we could have placed smart collectors at UMD and in the NCCoE lab. To simplify the NCCoE lab example solution, a single virtual appliance was deployed in the NCCoE lab that acts as both the analysis and detection engine and the network collector.

iSID allows the utility operator to see all devices connected to the utility network, detect anomalous behavior on the network, and detect policy violations in communications occurring over the network. This information is made available to utility cyber analysts both through a collection of dashboards and through syslog data that can be collected by a Security Information and Event Management (SIEM) system.

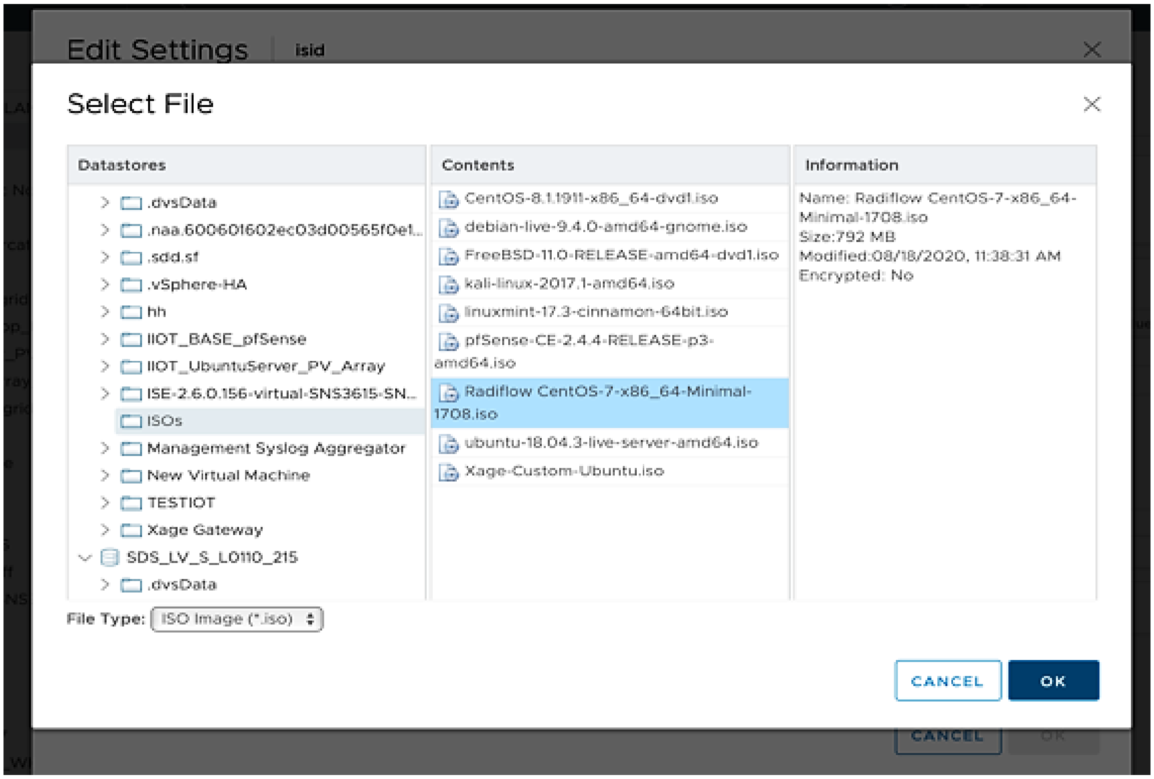
In the NCCoE example solution, iSID was placed on the utility virtual network (vLAN) between the distribution ops systems and the utility gateway. This placement provides information about traffic bound for the microgrid network from the utility network. Sensors could also be placed between the utility gateway and the front-end processor.

## 2.4.1 Radiflow iSID Installation and Configuration

This section discusses the Radiflow iSID installation and configuration procedures.

**Setup a Radiflow Installation Manager (RIM) Server**

1. Create a Radiflow virtual machine (VM) using CentOS 1708 minimal International Standards Organization (ISO) file – CentOS-7-x86_64-Minimal-1708.iso.



Edit Settings | isid

Select File

Datastores
- .dvsData
- .naa.600601602ec03d00565f0et...
- .sdd.sf
- .vSphere-HA
- hh
- IIOT_BASE_pfSense
- IIOT_UbuntuServer_PV_Array
- ISE-2.6.0.156-virtual-SNS3615-SN...
- ISOs
- Management Syslog Aggregator
- New Virtual Machine
- TESTIOT
- Xage Gateway
- SDS_LV_S_L0110_215
- .dvsData

Contents
- CentOS-8.1.1911-x86_64-dvd1.iso
- debian-live-9.4.0-amd64-gnome.iso
- FreeBSD-11.0-RELEASE-amd64-dvd1.iso
- kali-linux-2017.1-amd64.iso
- linuxmint-17.3-cinnamon-64bit.iso
- pfSense-CE-2.4.4-RELEASE-p3-amd64.iso
- Radiflow CentOS-7-x86_64-Minimal-1708.iso
- ubuntu-18.04.3-live-server-amd64.iso
- Xage-Custom-Ubuntu.iso

Information

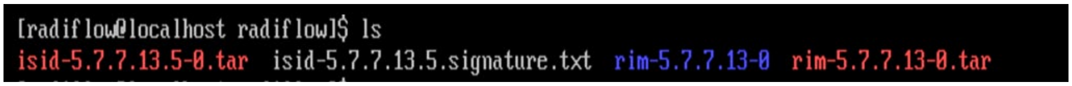
Name: Radiflow CentOS-7-x86_64-Minimal-1708.iso<br>
Size:792 MB<br>
Modified:08/18/2020, 11:38:31 AM<br>
Encrypted: No

File Type: ISO Image (*.iso)

2. Once the VM is up, use it to download the RIM from the download site.

3. Download the file from the website for install.

   We downloaded the file on the TEST machine, and then secure copied it to the Radiflow machine we created. Inside the Radiflow VM, files are uploaded into the 'radiflow' directory in the radiflow home directory (*cd/radiflow*). The files include iSID latest version – *isid-5.7.7.13.5-0.tar*, Radiflow Installation Manager (RIM) – *rim-5.7.7.13-0.tar* and iSID Signature file - *isid-5.7.7.13.5.signature.txt*– needed for installing iSID using RIM.



```
[radiflow@localhost radiflow]$ ls
isid-5.7.7.13.5-0.tar  isid-5.7.7.13.5.signature.txt  rim-5.7.7.13-0  rim-5.7.7.13-0.tar
```

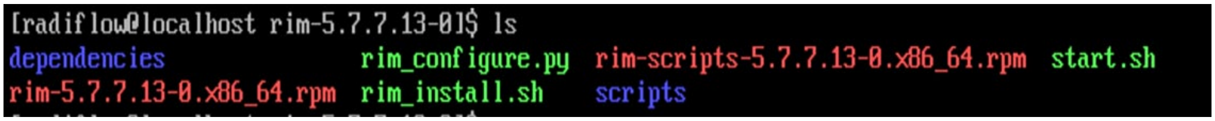
4. Extract RIM and run it.

```
tar -xvf rim-5.7.7.13-0.tar
```

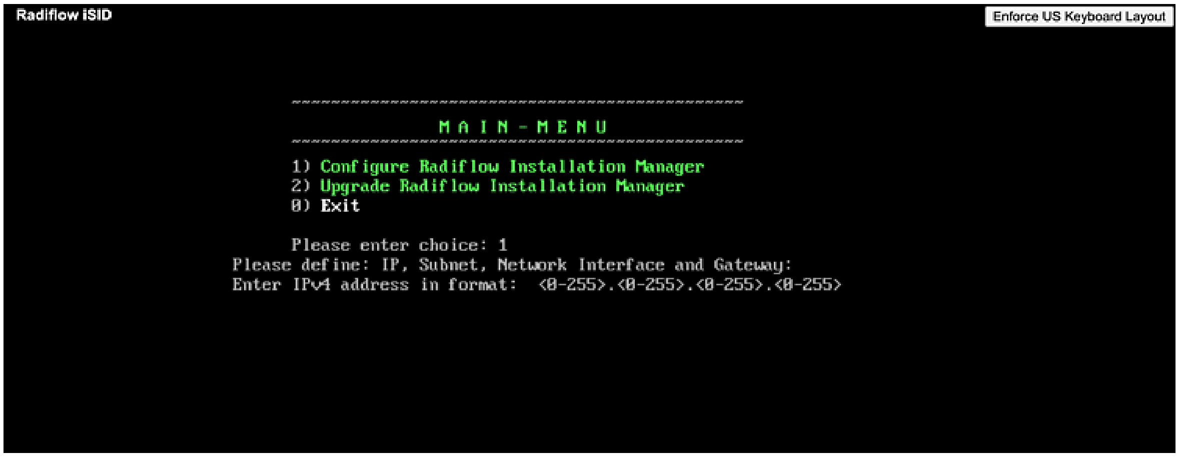
**cd rim-5.7.7.13-0**

**su root**

**./start.sh**



```
[radiflow@localhost rim-5.7.7.13-0]$ ls
dependencies               rim_configure.py  rim-scripts-5.7.7.13-0.x86_64.rpm  start.sh
rim-5.7.7.13-0.x86_64.rpm  rim_install.sh    scripts
```

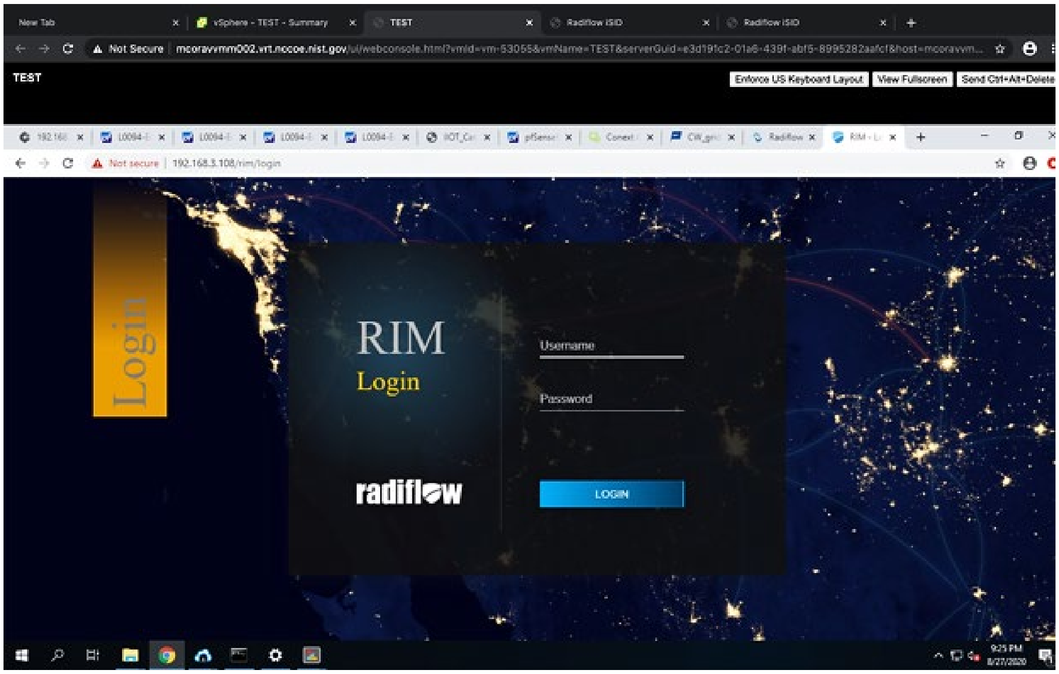


```
        ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
                      M A I N - M E N U
        ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
        1) Configure Radiflow Installation Manager
        2) Upgrade Radiflow Installation Manager
        0) Exit

        Please enter choice: 1
  Please define: IP, Subnet, Network Interface and Gateway:
  Enter IPv4 address in format:  <0-255>.<0-255>.<0-255>.<0-255>
```

5. Enter 1 to configure the RIM server with the following:
   - IP address: 192.168.3.108
   - Subnet mask: 255.255.255.0
   - Gateway: 192.168.3.1
   - Interface name: ens192

**Access and Test the RIM and iSID User Interface**

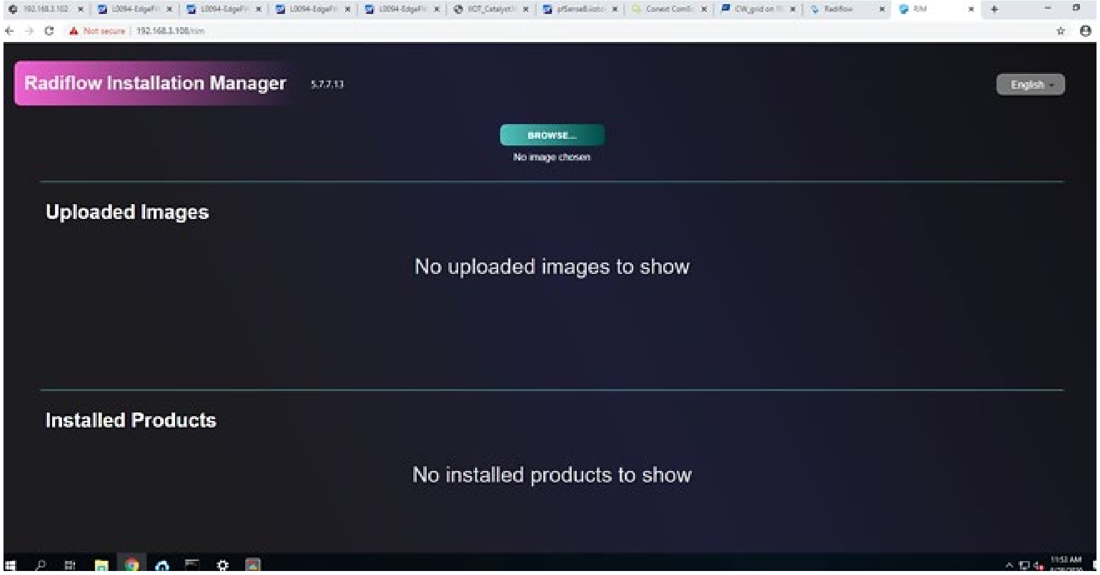
1. To access the RIM, open a web browser from the TEST VM (192.168.3.101) and navigate to the RIM server at https:192.168.3.108/rim.



2. To get access inside the RIM user interface login, enter the username and password:

   Username: **radiflow**

   Password: **Secured1492**



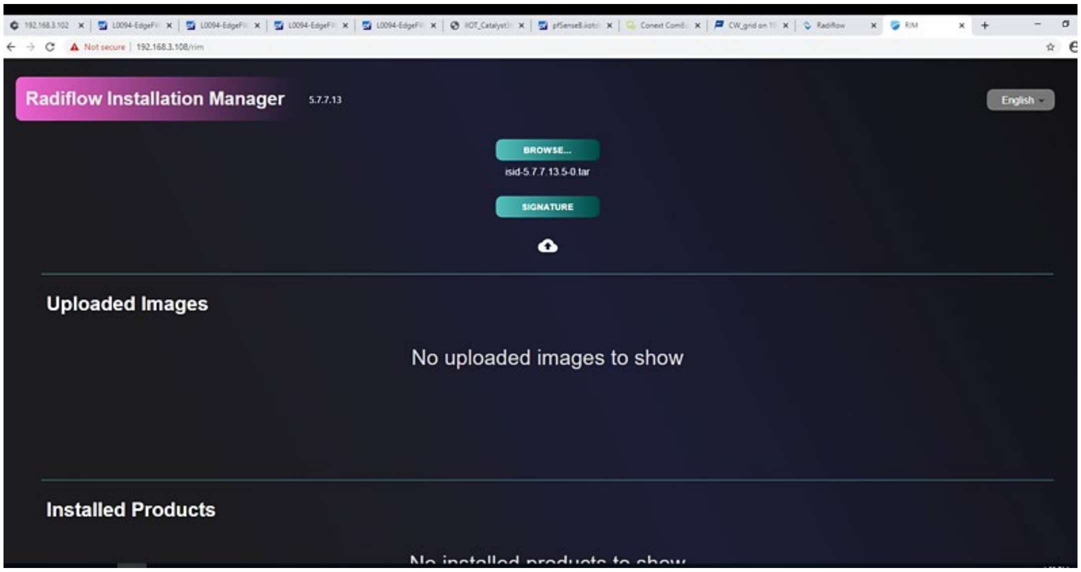
No uploaded images to show

No installed products to show

Inside this TEST machine, we have the files isid-5.7.7.13.5-0.tar and iSID Signature file isid-5.7.7.13.5.signature.txt

3. Click **Browse** and select the *isid-5.7.7.13.5-0.tar*.

4. Click **Add signature file** and select *isid-5.7.7.13.5.signature.txt*, then click **Upload**.

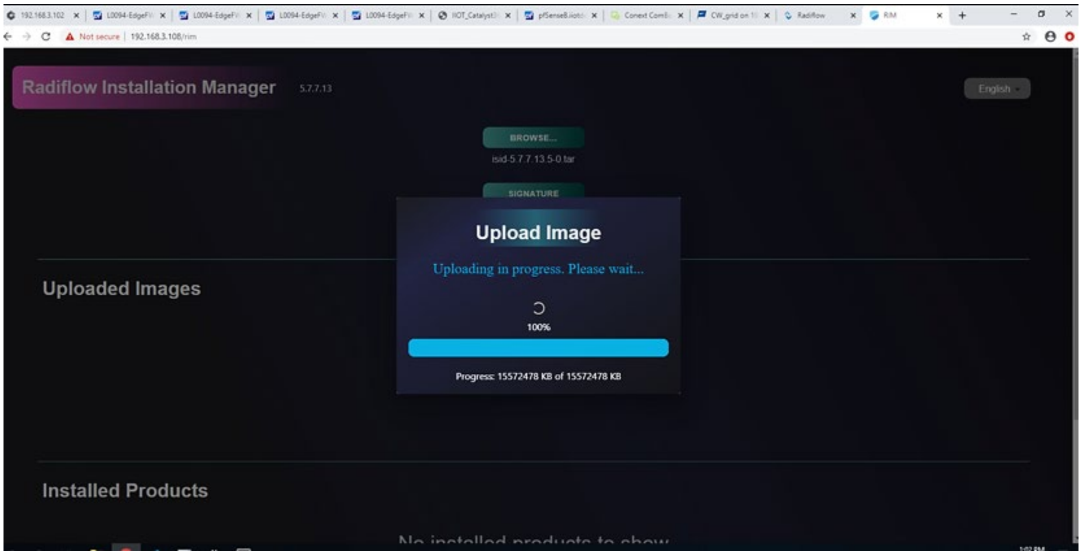


Uploaded Images

No uploaded images to show

Installed Products

No installed products to show



Upload Image

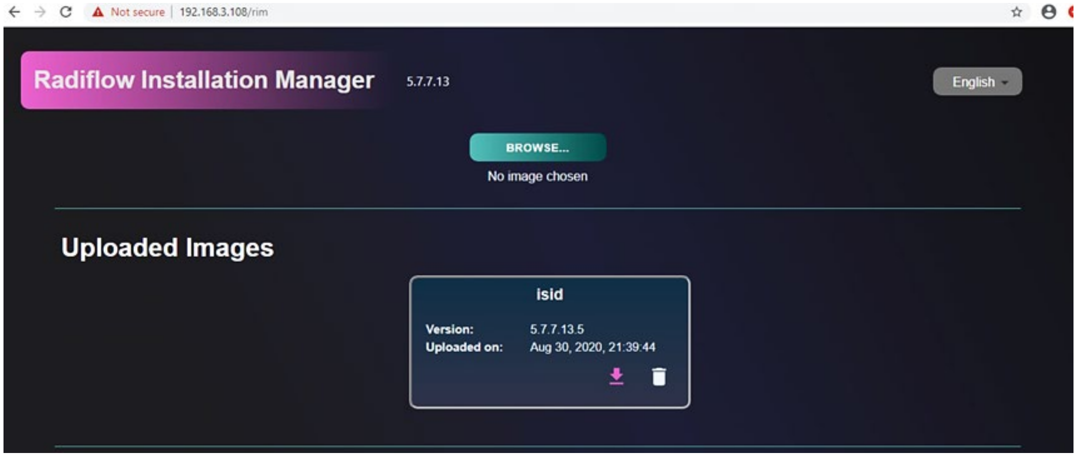
Uploading in progress. Please wait...

100%

Progress: 15572478 KB of 15572478 KB

No installed products to show

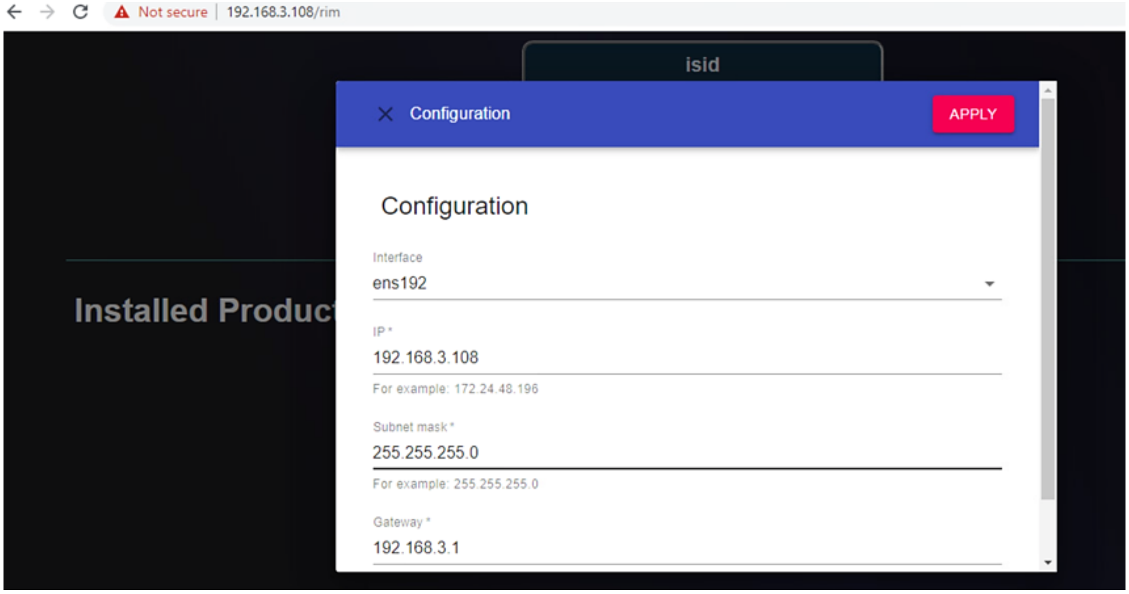
5. Successfully uploaded the image.



Version: 5.7.7.13.5
Uploaded on: Aug 30, 2020, 21:39:44

6. Install the uploaded image.

**Note:** If you configured the RIM server from step 6 above, then there is no need to reconfigure.



Interface: ens192

IP *: 192.168.3.108

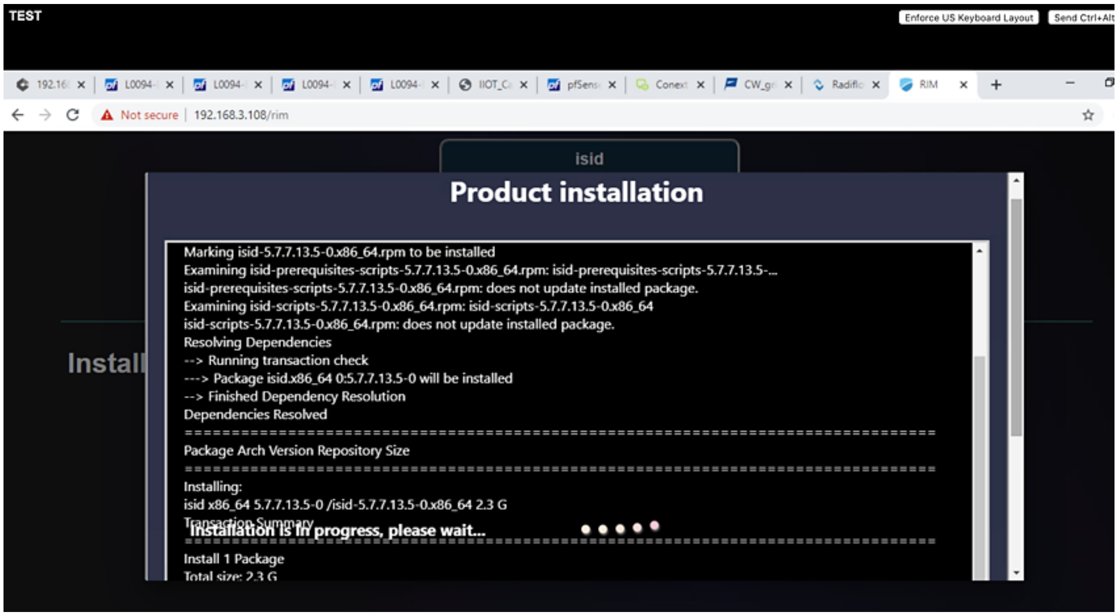
For example: 172.24.48.196

Subnet mask *: 255.255.255.0

For example: 255.255.255.0

Gateway *: 192.168.3.1

Product installation window:

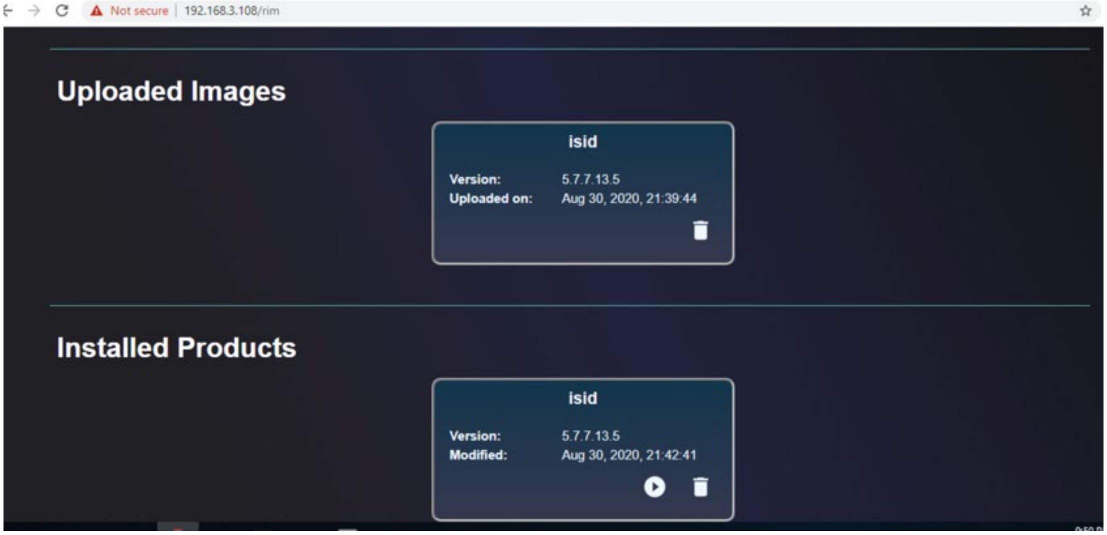


Product installation

```
Marking isid-5.7.7.13.5-0.x86_64.rpm to be installed
Examining isid-prerequisites-scripts-5.7.7.13.5-0.x86_64.rpm: isid-prerequisites-scripts-5.7.7.13.5-...
isid-prerequisites-scripts-5.7.7.13.5-0.x86_64.rpm: does not update installed package.
Examining isid-scripts-5.7.7.13.5-0.x86_64.rpm: isid-scripts-5.7.7.13.5-0.x86_64
isid-scripts-5.7.7.13.5-0.x86_64.rpm: does not update installed package.
Resolving Dependencies
--> Running transaction check
---> Package isid.x86_64 0:5.7.7.13.5-0 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
Package Arch Version Repository Size
================================================================================
Installing:
isid x86_64 5.7.7.13.5-0 /isid-5.7.7.13.5-0.x86_64 2.3 G
Transaction Summary
================================================================================
Install 1 Package
Total size: 2.3 G
```

Installation is in progress, please wait...

7. Once the installation is complete, the installed iSID image displays.



Uploaded Images

isid

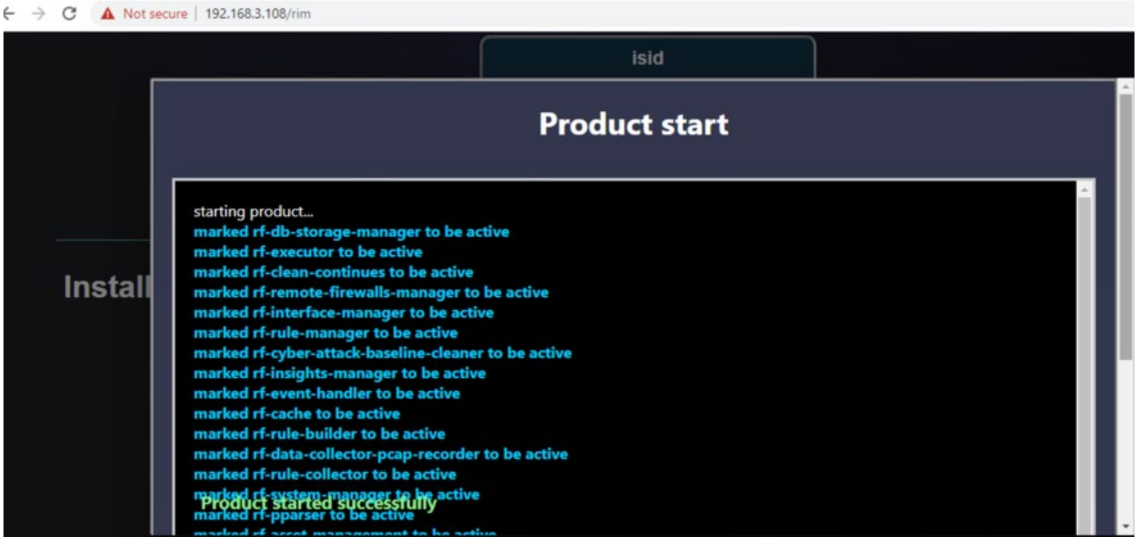
Version: 5.7.7.13.5
Uploaded on: Aug 30, 2020, 21:39:44

Installed Products

isid

Version: 5.7.7.13.5
Modified: Aug 30, 2020, 21:42:41

8. Run an installed iSID image, click **Finish** when it is complete.



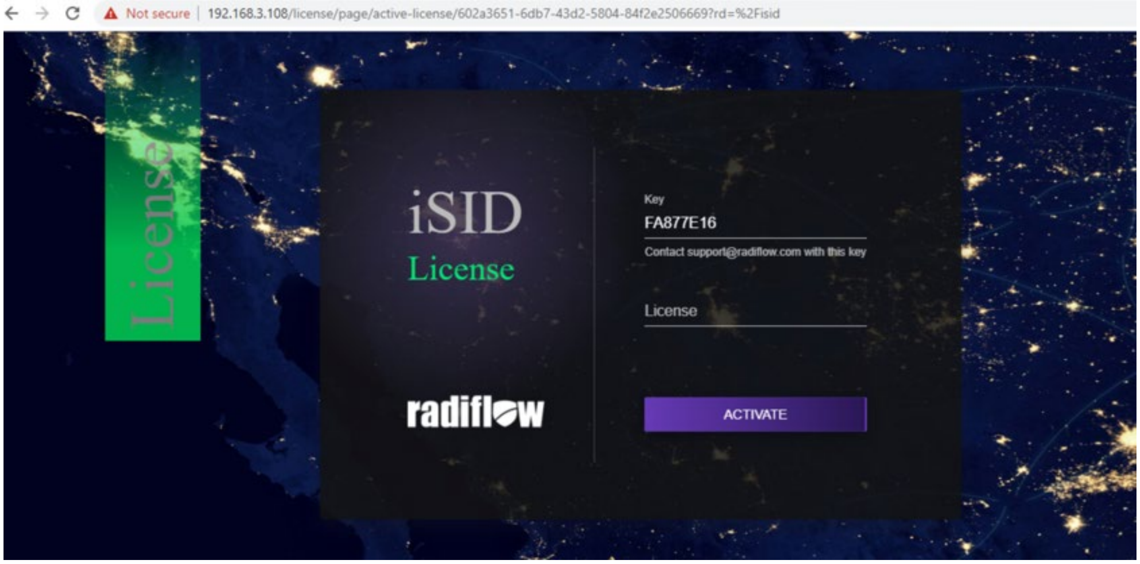
Product start

```
starting product...
marked rf-db-storage-manager to be active
marked rf-executor to be active
marked rf-clean-continues to be active
marked rf-remote-firewalls-manager to be active
marked rf-interface-manager to be active
marked rf-rule-manager to be active
marked rf-cyber-attack-baseline-cleaner to be active
marked rf-insights-manager to be active
marked rf-event-handler to be active
marked rf-cache to be active
marked rf-rule-builder to be active
marked rf-data-collector-pcap-recorder to be active
marked rf-rule-collector to be active
marked rf-system-manager to be active
Product started successfully
marked rf-pparser to be active
marked rf-asset-management to be active
```

9. Test the installed and running iSID.

10. Navigate to https://192.168.3.108/isid to enter the activation key:

11. Contact Radiflow to get the license and enter the license key and select Activate. We need to enter: **E7ICAMY8.**


192.168.3.108/license/page/active-license/602a3651-6db7-43d2-5804-84f2e2506669?rd=%2Fisid
License
iSID
License
radiflow
ACTIVATE

Key
FA877E16
Contact support@radiflow.com with this key

License

12. Enter the following credentials for iSID:

- Username: **radiflow**
- Password: safe@Rad1flow

13. View the Radiflow iSID web application.

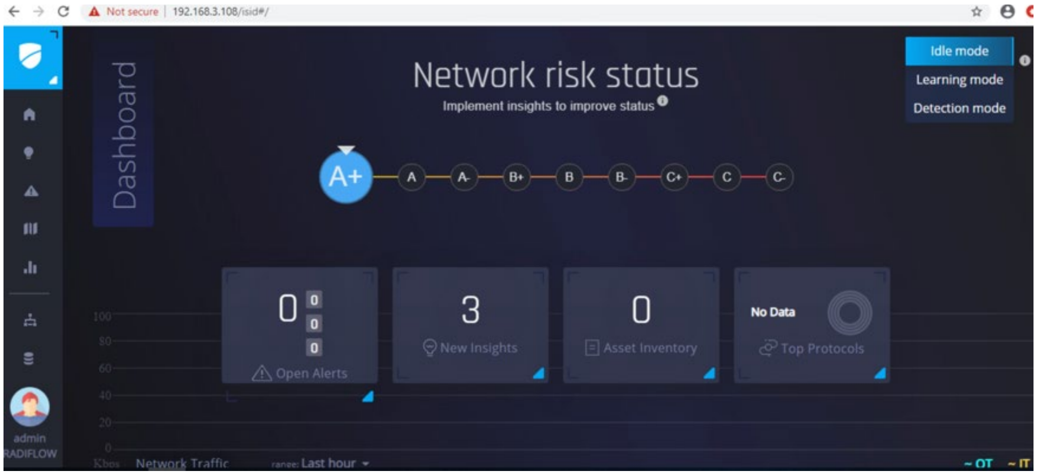
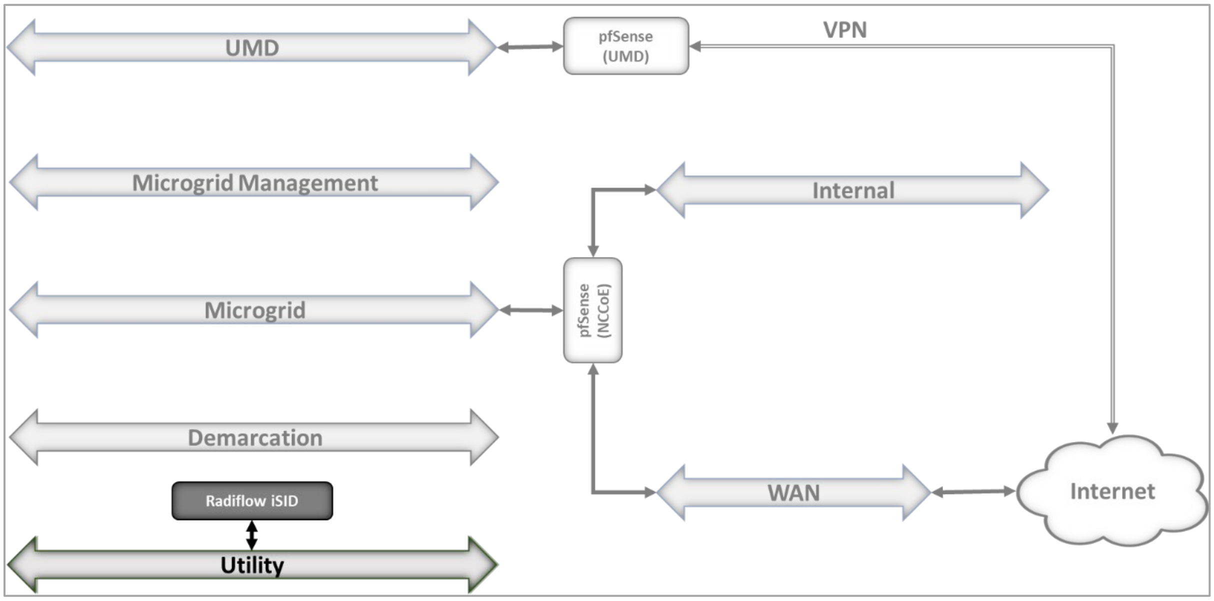


Figure 2-3 shows the location of Radiflow iSID in the example solution.

**Figure 2-4 Radiflow iSID position in the example solution**



## 2.5 Spherical Analytics Immutably ™

We implemented the command register element of the reference architecture using the Spherical Analytics Immutably service. Immutably receives records of information exchanges from the distribution ops systems, the front-end processor, and the microgrid master controller. It digitally signs the records, augments them with information from notaries providing time stamps and source information, and places them on a distributed ledger. This ledger provides an immutable audit trail of information exchanges between the utility and microgrid DER devices.

The records in the ledger are cryptographically chained together to provide tamper detection. The utility and all participating microgrid operators can read and verify the audit trail maintained by the Immutably distributed ledger.

### 2.5.1 Spherical Analytics Immutably Installation and Configuration

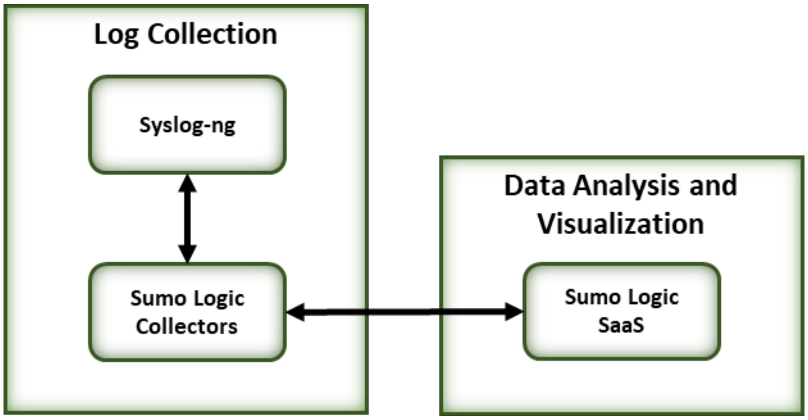
Immutably is a software-as-a-service product and no installation was required. We developed three pieces of software to send data to Immutably. The source for this software is provided in Appendix B.

The records are sent using an Immutably representational state transfer (REST) application programming interface.

## 2.6 Sumo Logic

Sumo Logic provides a cloud-based SIEM capability for analyzing and visualizing security information and events that implement the data analysis and visualization elements of the reference architecture. Sumo Logic data analytics and visualization are software-as-a-service products. No installation was required for the analytic and visualization services. Figure 2-5 shows Sumo Logic's role in the reference architecture.

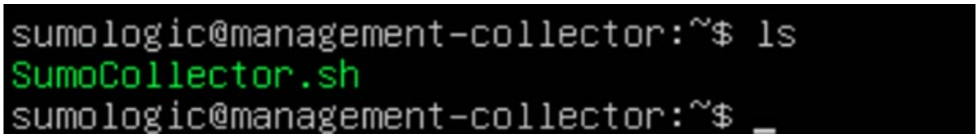
**Figure 2-5 Sumo Logic Role in the Example Solution**



### 2.6.1 Sumo Logic syslog Collector Installation

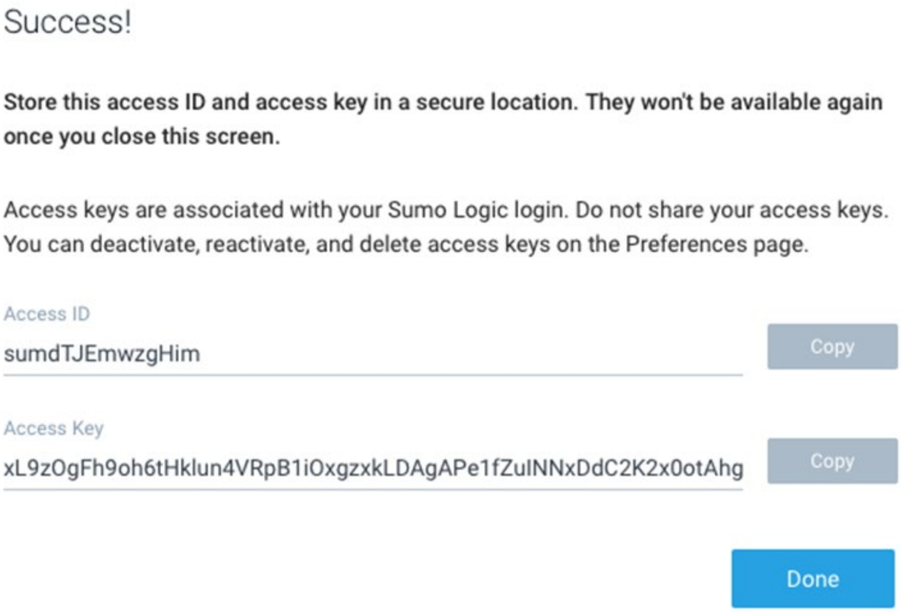
We installed the Sumo Logic syslog collector on a Linux system to send syslog data to Sumo Logic for analysis. The Sumo Logic collector provides one of the two parts that make up the log collection element of the reference architecture. We combined the Sumo Logic syslog collector with the open-source version of syslog ng to create the log collector element of the reference architecture.

1. We set up an Ubuntu Linux VM and installed the collector using a command provided by Sumo Logic:
    a. sudo wget “https://collectors.us2.sumologic.com/rest/download/linux/64” -O SumoCollector.sh && sudo chmod +x SumoCollector.sh && sudo ./SumoCollector.sh && chmod +x SumoCollector.sh



```
sumologic@management-collector:~$ ls
SumoCollector.sh
sumologic@management-collector:~$ _
```

2. Next, an authentication method is required to get the access key and access ID or installation token strings from the Sumologic account, which will be used to register installed collectors. Navigate to Preferences from the menu options.
    a. Click **Add Access Key** and add a username for your collector.
    b. Click **Create Key** to see the access ID and Access Key you created.



Success!

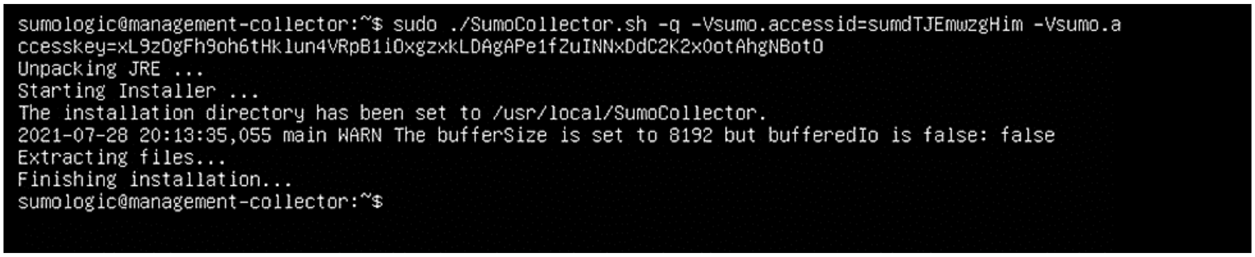
**Store this access ID and access key in a secure location. They won't be available again once you close this screen.**

Access keys are associated with your Sumo Logic login. Do not share your access keys. You can deactivate, reactivate, and delete access keys on the Preferences page.

Access ID
sumdTJEmwzgHim

Access Key
xL9zOgFh9oh6tHklun4VRpB1iOxgzxkLDAgAPe1fZuINNxDdC2K2x0otAhg

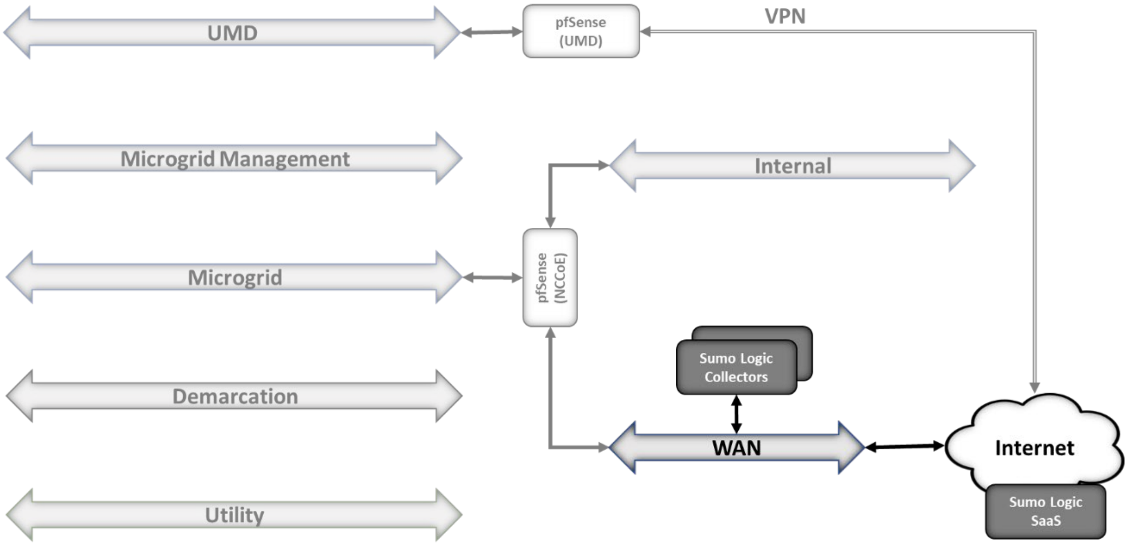
3. Run the command:
    a. sudo ./SumoCollector.sh -q -Vsumo.accessid=<accessId> -Vsumo.accesskey=<accessKey> -Vsources=<filepath>



```
sumologic@management-collector:~$ sudo ./SumoCollector.sh -q -Vsumo.accessid=sumdTJEmwzgHim -Vsumo.a
ccesskey=xL9zOgFh9oh6tHklun4VRpB1iOxgzxkLDAgAPe1fZuINNxDdC2K2x0otAhgNBotO
Unpacking JRE ...
Starting Installer ...
The installation directory has been set to /usr/local/SumoCollector.
2021-07-28 20:13:35,055 main WARN The bufferSize is set to 8192 but bufferedIo is false: false
Extracting files...
Finishing installation...
sumologic@management-collector:~$
```

Figure 2-5 shows the location of Sumo Logic collectors and Sumo Logic SaaS in the example solution.

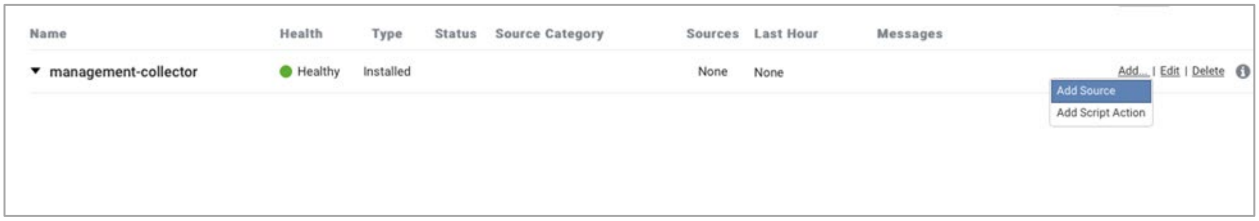
**Figure 2-6 Sumo Logic Location in the Example Solution**



## 2.6.2 Configuring Sources for syslog Collectors

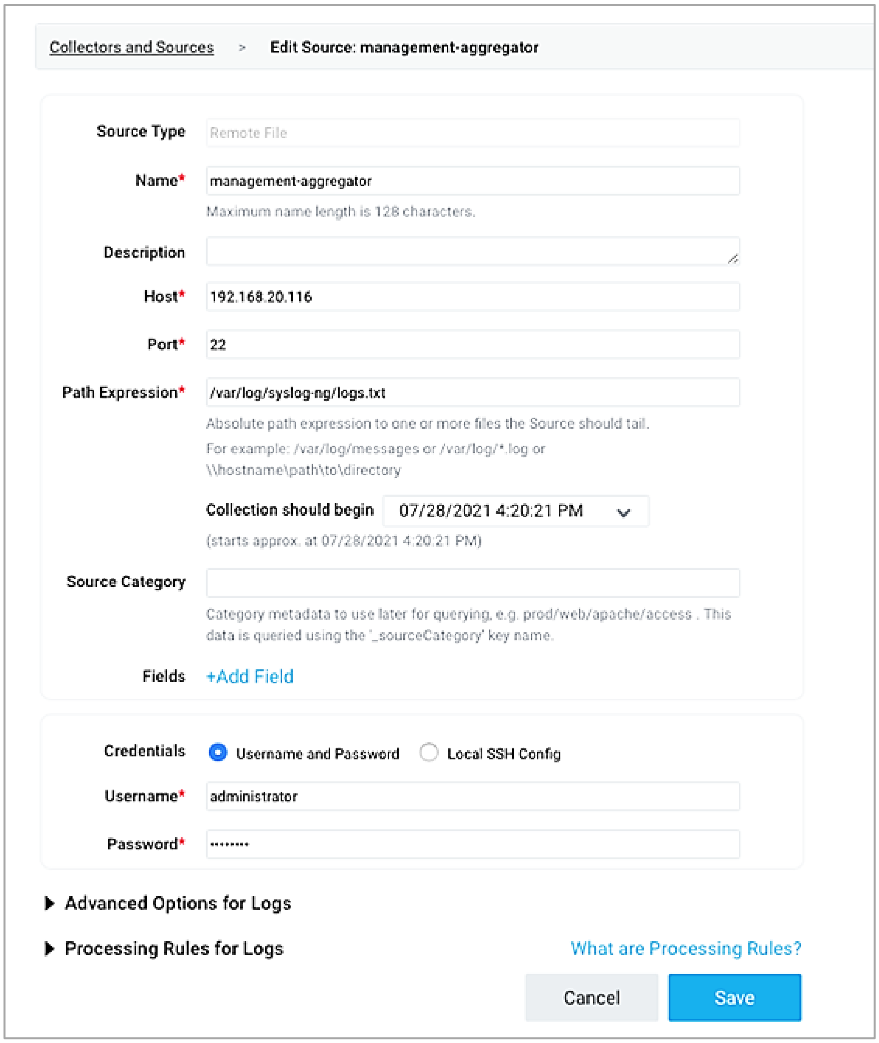
For each installed collector, we are using Syslog or remote file as our source type. Each product's log data goes to a syslog aggregator, implemented with Syslog ng, before reaching the Sumo Logic collector. Installation and configuration guide for Syslog-ng is described in section 2.10.

1. Navigate to **Manage Data > Collection** on the **Collector** menu.
2. Click **Add Source** for Collector management-collector.



| Name | Health | Type | Status | Source Category | Sources | Last Hour | Messages |
|---|---|---|---|---|---|---|---|
| ▼ management-collector | ● Healthy | Installed | | | None | None | |

3. Select the **Remote File** source and provide the following information for source and destination:
   a. Name: `management-aggregator`
   b. Host: `193.168.20.116`
   c. Port: `22`
   d. Path Expression: `cd /var/log/syslog-ng/logs.txt`



Collectors and Sources > Edit Source: management-aggregator

Source Type: Remote File

Name*: management-aggregator

Maximum name length is 128 characters.

Description:

Host*: 192.168.20.116

Port*: 22

Path Expression*: /var/log/syslog-ng/logs.txt

Absolute path expression to one or more files the Source should tail.
For example: /var/log/messages or /var/log/*.log or
\\hostname\path\to\directory

Collection should begin: 07/28/2021 4:20:21 PM

(starts approx. at 07/28/2021 4:20:21 PM)

Source Category:

Category metadata to use later for querying, e.g. prod/web/apache/access . This data is queried using the '_sourceCategory' key name.

Fields: +Add Field

Credentials: ● Username and Password ○ Local SSH Config

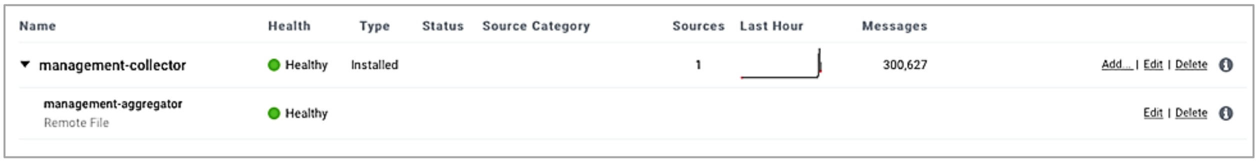
Username*: administrator

Password*: ••••••••

▸ Advanced Options for Logs
▸ Processing Rules for Logs
What are Processing Rules?
Cancel
Save

636

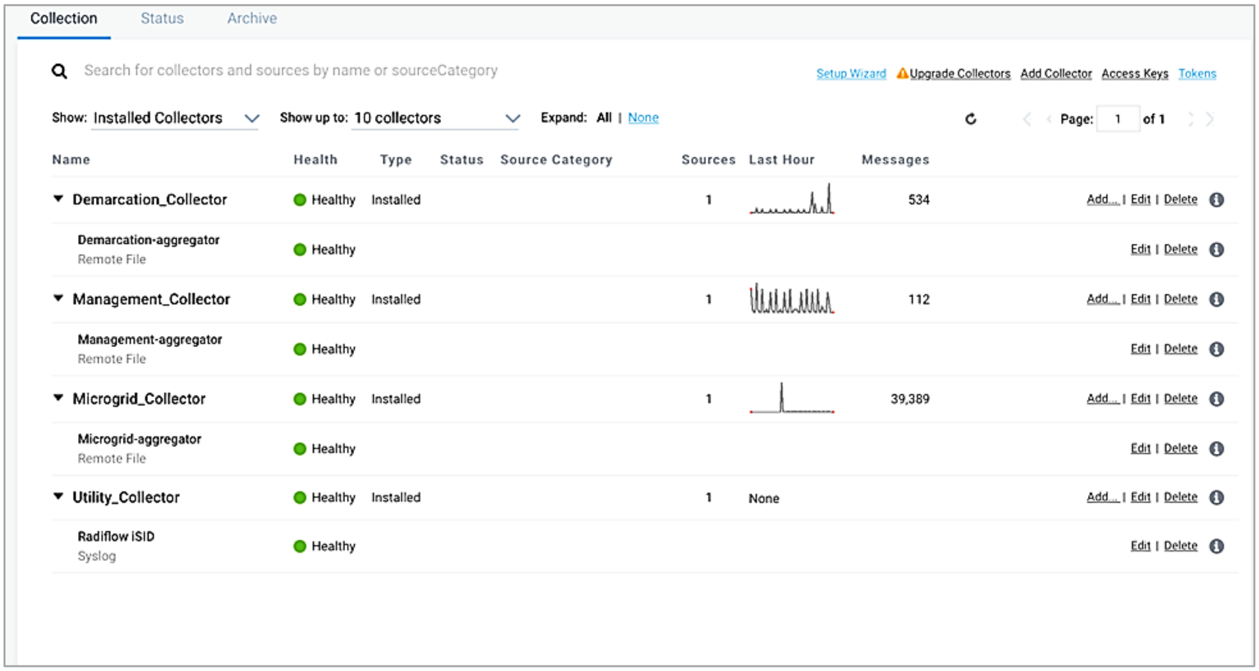
637 4. Click **Save.**



| Name | Health | Type | Status | Source Category | Sources | Last Hour | Messages | |
|---|---|---|---|---|---|---|---|---|
| ▾ management-collector | ● Healthy | Installed | | | 1 | | 300,627 | Add... \| Edit \| Delete |
| management-aggregator<br>Remote File | ● Healthy | | | | | | | Edit \| Delete |

638

639 We configured four collectors, one for each of the eight networks used in the example solution, 640 microgrid, microgrid management, demarcation, and utility. This configuration is shown below.



Show: Installed Collectors  Show up to: 10 collectors  Expand: All | None  Page: 1 of 1

| Name | Health | Type | Status | Source Category | Sources | Last Hour | Messages | |
|---|---|---|---|---|---|---|---|---|
| ▼ Demarcation_Collector | ● Healthy | Installed | | | 1 | | 534 | Add... \| Edit \| Delete |
| Demarcation-aggregator<br>Remote File | ● Healthy | | | | | | | Edit \| Delete |
| ▼ Management_Collector | ● Healthy | Installed | | | 1 | | 112 | Add... \| Edit \| Delete |
| Management-aggregator<br>Remote File | ● Healthy | | | | | | | Edit \| Delete |
| ▼ Microgrid_Collector | ● Healthy | Installed | | | 1 | | 39,389 | Add... \| Edit \| Delete |
| Microgrid-aggregator<br>Remote File | ● Healthy | | | | | | | Edit \| Delete |
| ▼ Utility_Collector | ● Healthy | Installed | | | 1 | None | | Add... \| Edit \| Delete |
| Radiflow iSID<br>Syslog | ● Healthy | | | | | | | Edit \| Delete |

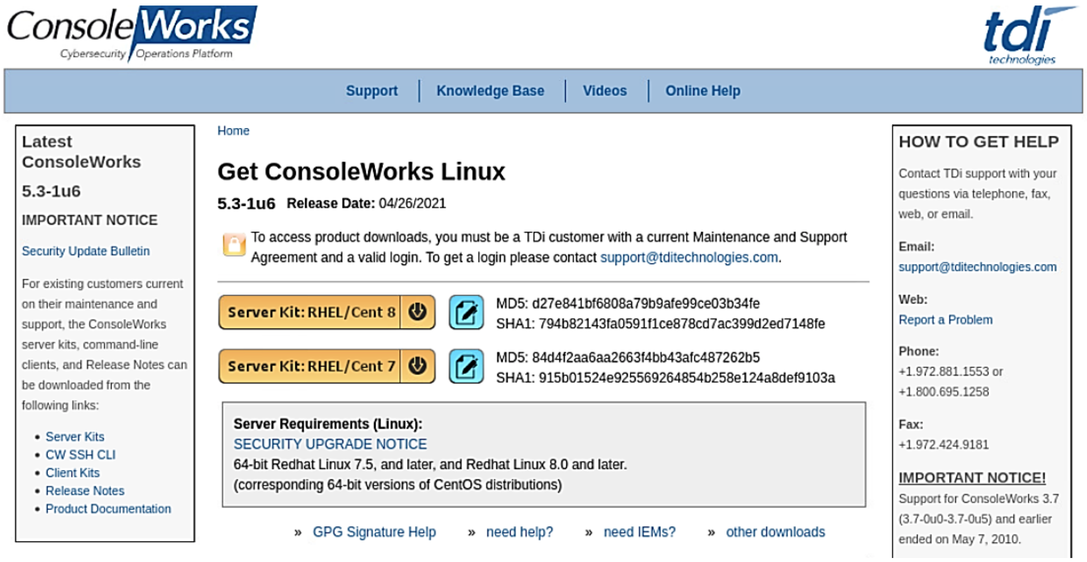
## 2.7 TDi Technologies ConsoleWorks

TDi Technologies ConsoleWorks serves as a ”jump box” to control privileged user access to the management interfaces of Cisco ISE and Cisco Cyber Vision. ConsoleWorks maintains the credentials used to access the dedicated management interfaces of these products. Privileged users have credentials that allow them to access ConsoleWorks. ConsoleWorks uses “user profiles” to define the management interfaces that each privileged user is allowed to access, and the credentials used to access that interface. ConsoleWorks authenticates authorized users to product management interfaces and records all privileged user actions in an audit trail.

### 2.7.1 Console Works Installation and Configuration

Create a virtual machine running Centos 7.5 with one network interface, dynamic host configuration protocol disabled, and an IP address `192.168.20.109`, then:

1. Download the installation kit from the Tdi website at http://support.tditechnologies.com. A username and password are required. Contact Tdi Support at support@tditechnologies.com to request a username and password. You will also need a unique link from Tdi Technologies for the ConsoleWorks License ZIP file. Download this file (do not unzip it) to your chosen directory.



Latest ConsoleWorks

5.3-1u6

IMPORTANT NOTICE

Security Update Bulletin

For existing customers current on their maintenance and support, the ConsoleWorks server kits, command-line clients, and Release Notes can be downloaded from the following links:

- Server Kits
- CW SSH CLI
- Client Kits
- Release Notes
- Product Documentation

Home

Get ConsoleWorks Linux

**5.3-1u6** **Release Date:** 04/26/2021

To access product downloads, you must be a TDi customer with a current Maintenance and Support Agreement and a valid login. To get a login please contact support@tditechnologies.com.

MD5: d27e841bf6808a79b9afe99ce03b34fe
SHA1: 794b82143fa0591f1ce878cd7ac399d2ed7148fe

MD5: 84d4f2aa6aa2663f4bb43afc487262b5
SHA1: 915b01524e925569264854b258e124a8def9103a

**Server Requirements (Linux):**
SECURITY UPGRADE NOTICE
64-bit Redhat Linux 7.5, and later, and Redhat Linux 8.0 and later.
(corresponding 64-bit versions of CentOS distributions)

» GPG Signature Help » need help? » need IEMs? » other downloads

HOW TO GET HELP

Contact TDi support with your questions via telephone, fax, web, or email.

**Email:**
support@tditechnologies.com

**Web:**
Report a Problem

**Phone:**
+1.972.881.1553 or
+1.800.695.1258

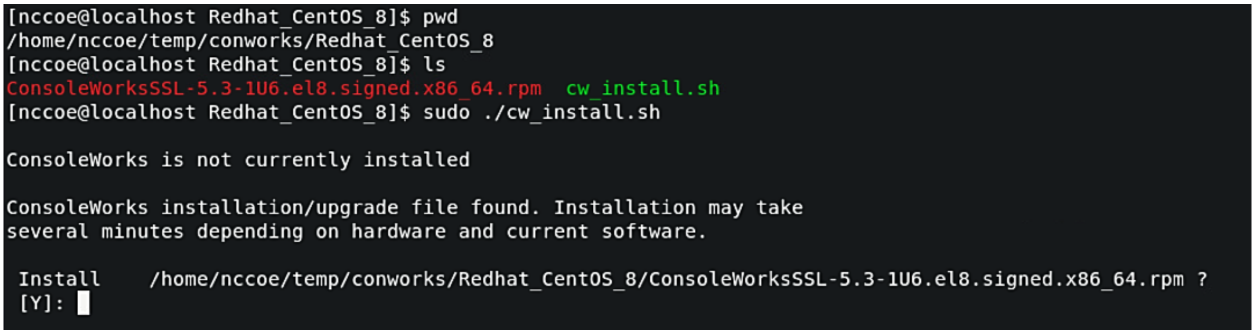
**Fax:**
+1.972.424.9181

IMPORTANT NOTICE!

Support for ConsoleWorks 3.7 (3.7-0u0-3.7-0u5) and earlier ended on May 7, 2010.

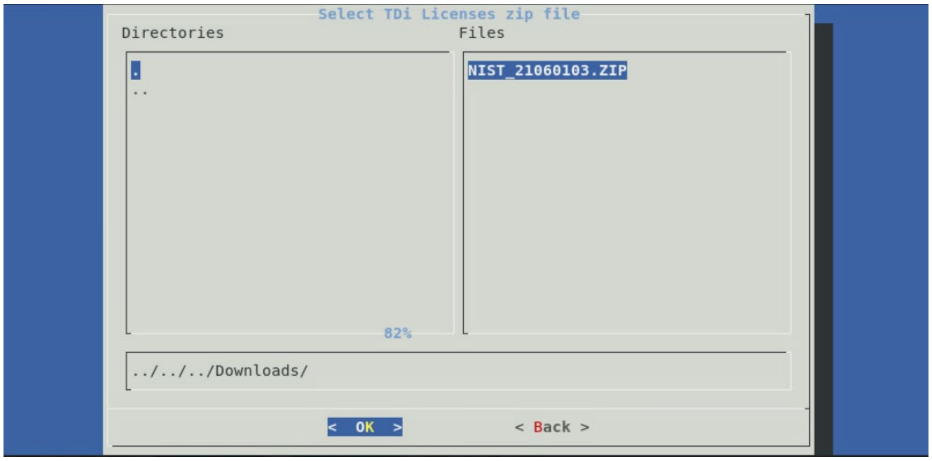
2. Create a directory to contain the ConsoleWorks installation files: `$mkdir -p temp/conworks`.

3. Inside the new directory, run the install script: `$sudo ./cw_install.sh`.



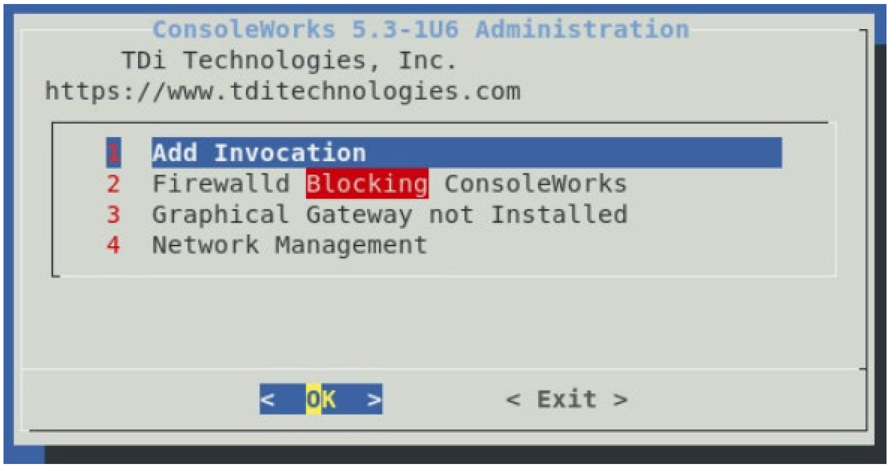
```
[nccoe@localhost Redhat_CentOS_8]$ pwd
/home/nccoe/temp/conworks/Redhat_CentOS_8
[nccoe@localhost Redhat_CentOS_8]$ ls
ConsoleWorksSSL-5.3-1U6.el8.signed.x86_64.rpm  cw_install.sh
[nccoe@localhost Redhat_CentOS_8]$ sudo ./cw_install.sh

ConsoleWorks is not currently installed

ConsoleWorks installation/upgrade file found. Installation may take
several minutes depending on hardware and current software.

 Install    /home/nccoe/temp/conworks/Redhat_CentOS_8/ConsoleWorksSSL-5.3-1U6.el8.signed.x86_64.rpm ?
 [Y]:
```

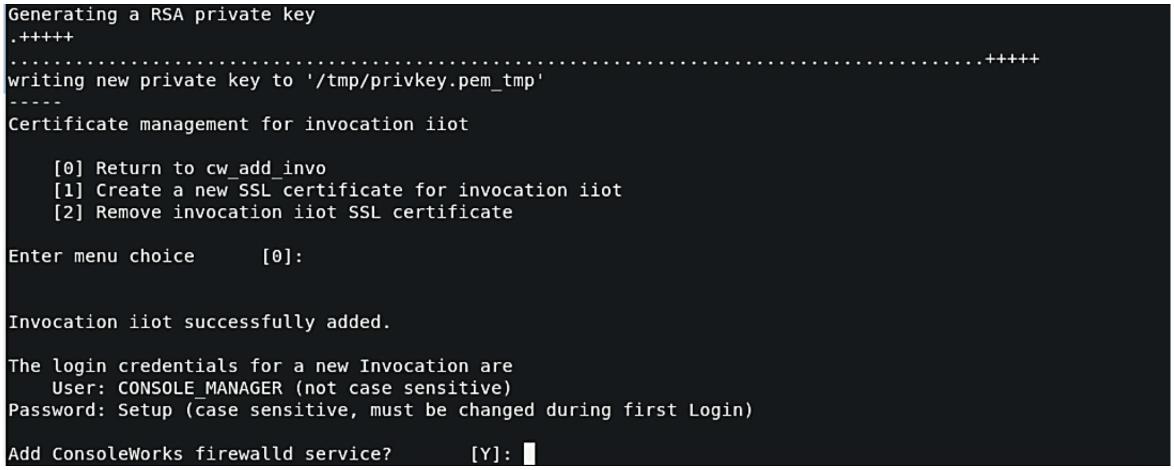
4. Follow the installer script to select the previously downloaded license file.



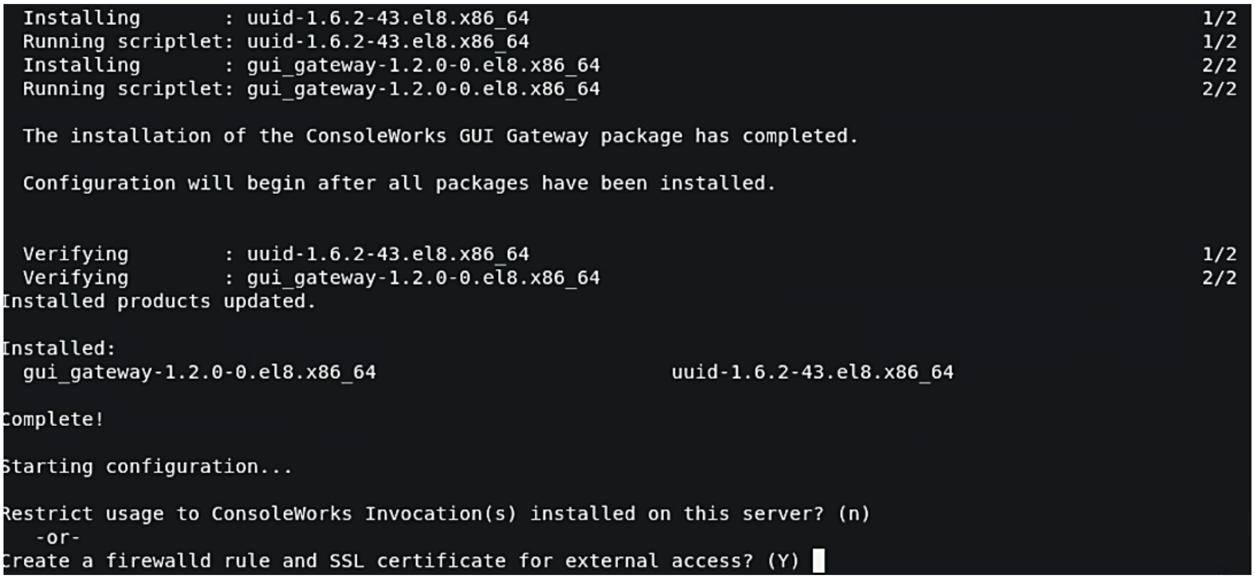
```
../../../Downloads/
```

5. Follow the prompts to add an invocation, configure the firewall, install the Graphical Gateway, and any other network management settings.

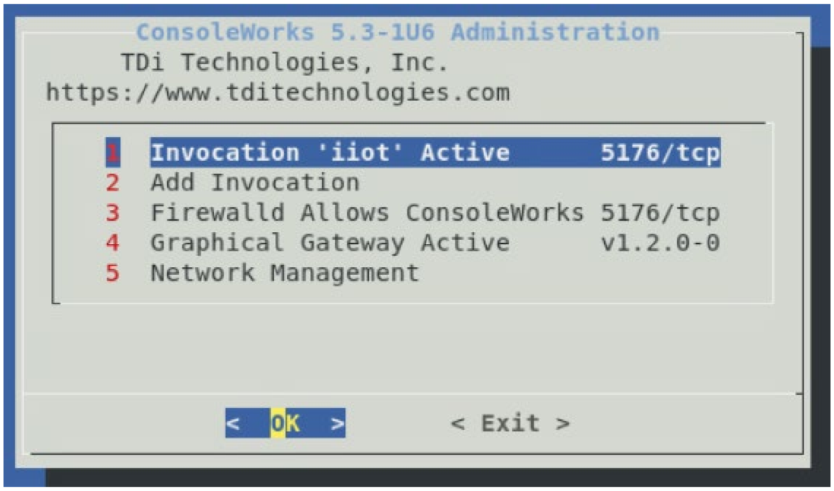

ConsoleWorks 5.3-1U6 Administration
TDi Technologies, Inc.
https://www.tditechnologies.com
1 Add Invocation
2 Firewalld Blocking ConsoleWorks
3 Graphical Gateway not Installed
4 Network Management
< OK >
< Exit >



```
Generating a RSA private key
.+++++
.........................................................................................+++++
writing new private key to '/tmp/privkey.pem_tmp'
-----
Certificate management for invocation iiot

    [0] Return to cw_add_invo
    [1] Create a new SSL certificate for invocation iiot
    [2] Remove invocation iiot SSL certificate

Enter menu choice      [0]:


Invocation iiot successfully added.

The login credentials for a new Invocation are
    User: CONSOLE_MANAGER (not case sensitive)
Password: Setup (case sensitive, must be changed during first Login)

Add ConsoleWorks firewalld service?       [Y]:
```



```
  Installing       : uuid-1.6.2-43.el8.x86_64                                                  1/2
  Running scriptlet: uuid-1.6.2-43.el8.x86_64                                                  1/2
  Installing       : gui_gateway-1.2.0-0.el8.x86_64                                            2/2
  Running scriptlet: gui_gateway-1.2.0-0.el8.x86_64                                            2/2

  The installation of the ConsoleWorks GUI Gateway package has completed.

  Configuration will begin after all packages have been installed.


  Verifying        : uuid-1.6.2-43.el8.x86_64                                                  1/2
  Verifying        : gui_gateway-1.2.0-0.el8.x86_64                                            2/2
Installed products updated.

Installed:
  gui_gateway-1.2.0-0.el8.x86_64                         uuid-1.6.2-43.el8.x86_64

Complete!

Starting configuration...

Restrict usage to ConsoleWorks Invocation(s) installed on this server? (n)
   -or-
Create a firewalld rule and SSL certificate for external access? (Y)
```

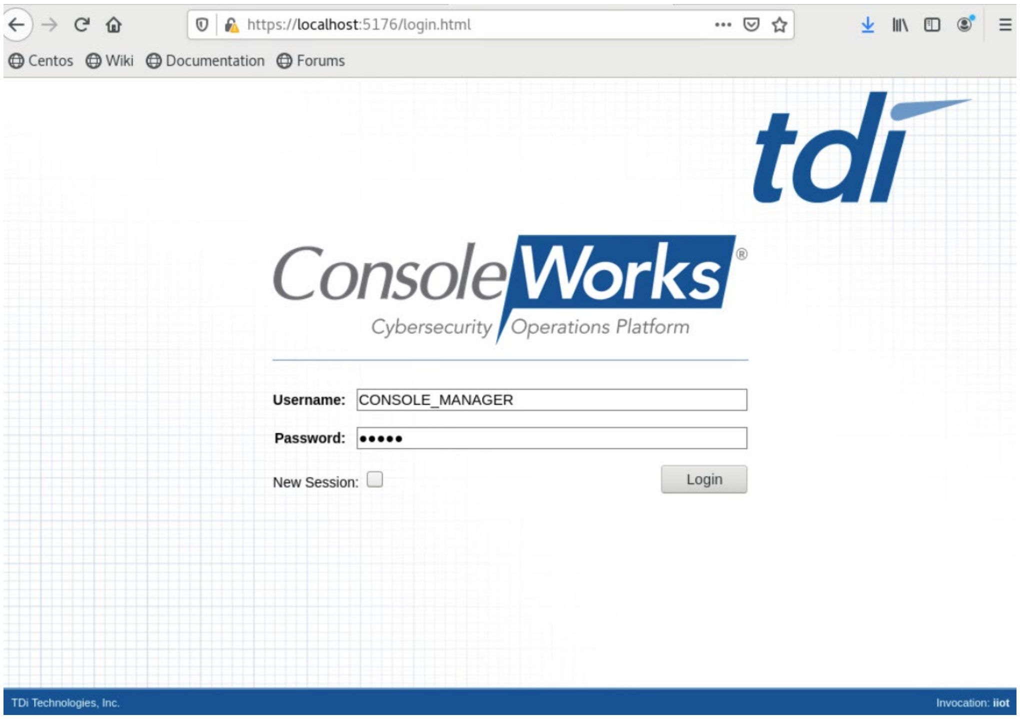


```
ConsoleWorks 5.3-1U6 Administration
     TDi Technologies, Inc.
 https://www.tditechnologies.com

      1  Invocation 'iiot' Active      5176/tcp
      2  Add Invocation
      3  Firewalld Allows ConsoleWorks 5176/tcp
      4  Graphical Gateway Active      v1.2.0-0
      5  Network Management

              <  OK  >        < Exit >
```

6. When the ConsoleWorks Administration script shows the details of the invocation and firewall settings, installation is complete. Select Exit to close the script.

7. If ConsoleWorks did not autostart, run the following command: `# /opt/ConsoleWorks/bin/cw_start <invocation name>`.

8. Log in to the ConsoleWorks local instance at `https://localhost:5176` (or a different port number if configured) with the username *CONSOLE_MANAGER* and the password "Setup". You will be required to set up a new password when complete.



Username: CONSOLE_MANAGER

Password: •••••

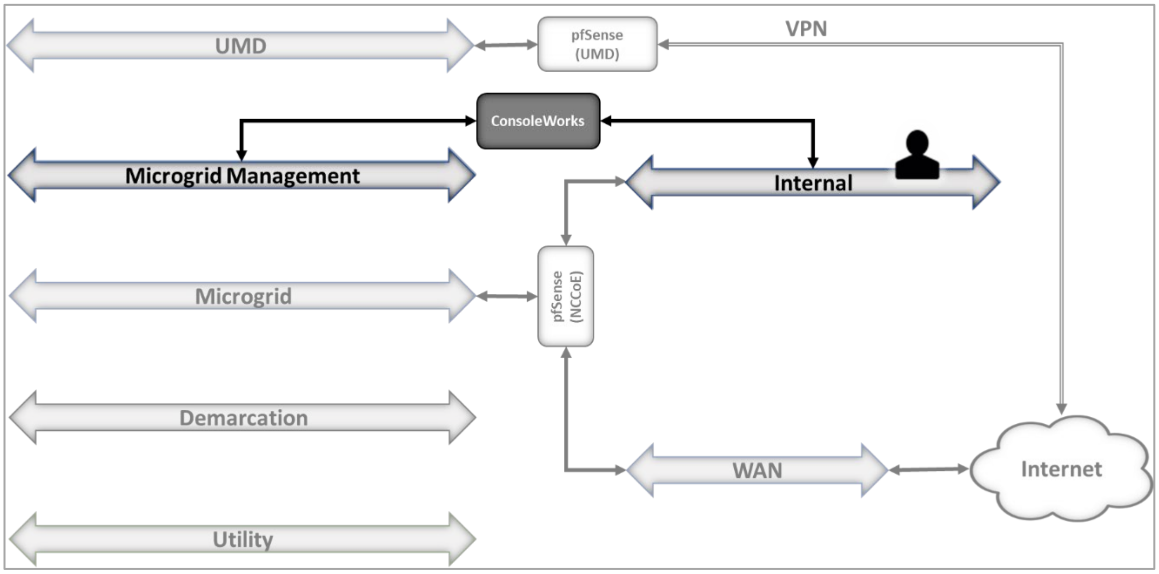
New Session: □

Three privileged users were defined in ConsoleWorks:

- One user has permission and credentials to access Cisco Cyber Vision
- One user has permission and credentials to access Cisco ISE
- One user has permission and credentials to access both Cisco Cyber Vision and Cisco ISE

Figure 2-7 shows ConsoleWorks position in the example solution.

**Figure 2-7 ConsoleWorks Position in the Example Solution**



## 2.8 Xage Security Fabric

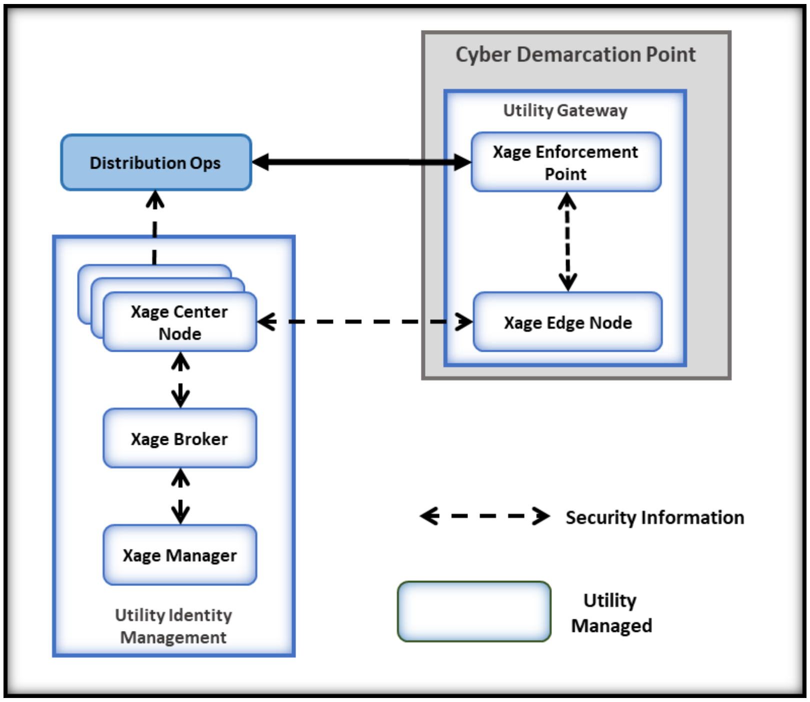
The Xage Security Fabric implements the utility identity management and utility GW elements of the reference architecture. The fabric consists of five services, the Xage Manager, Xage Broker, Xage Cener Fabric Node, the Xage Edge Node, and the Xage Enforcement Point. The Xage Manager, Xage Broker, and Xage Center Nodes combine to implement the utility identity management element. The Xage Edge Node and Xage Enforcement Point implement the utility GW.

- The Xage Manager configures users, devices, and access policies. The policies are then sent to Xage Broker. There is one Xage Manager operated by the utility and used to configure security policies for access to all DERs.
- The Xage Broker is a liaison between the Xage Manager and the Xage Center Nodes. The broker copies information such as identities and credentials from the Xage Manager to the Xage Edge nodes. In the NCCoE example solution, there is one Xage Broker operated by the utility to distribute access policies for all DERs via the distributed ledger operated on the Xage Center Nodes.
- The Xage Center Nodes use a distributed ledger to provide a geographically distributed information store that is tamperproof. The Xage Broker distributes policy information to the

Xage Center Nodes. This distributed information store provides policy information for the Xage Edge Nodes.

- A Xage Edge Node is in the cyber demarcation point at each microgrid operator site. The Xage Edge Node retrieves security information for its site from the Xage Center Nodes and stores it locally within the cyber demarcation point.
- The Xage Enforcement Point (XEP) in the cyber demarcation point uses the security information to allow or deny access to the front-end processor.

**Figure 2-8 Xage Implementation of Reference Architecture Elements**



## 2.8.1 Xage Installation and Configuration

Xage provides a Linux ISO file configured with all the packages needed by the Xage services. We used this ISO to create all the VMs needed by the installation.

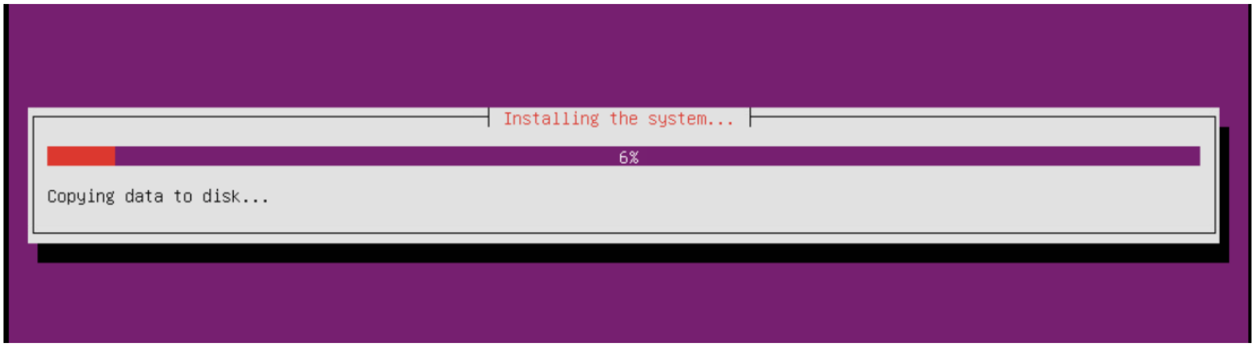
We followed the instructions in the XSG_Release_3.3_Install guide provided by Xage.

1. Starting on page 7 of the guide, we used Xage Built ISOs (2.1.1)
2. Starting on page 13, the install happens.
    a. We created the VM for the Xage Manager using the provided ISO
        i. The Xage Manager IP address id 192.168.3.102.
        ii. We then created three more VMs using the Xage-provided ISO, one each for
            1. Xage Broker

2. Xage Center Fabric Node
3. Xage Edge Node

iii. During the install starting on page 13, we configure the Xage manager with the IP addresses of the three different VMs, and the Xage manager deploys the appropriate software to those other VMs.

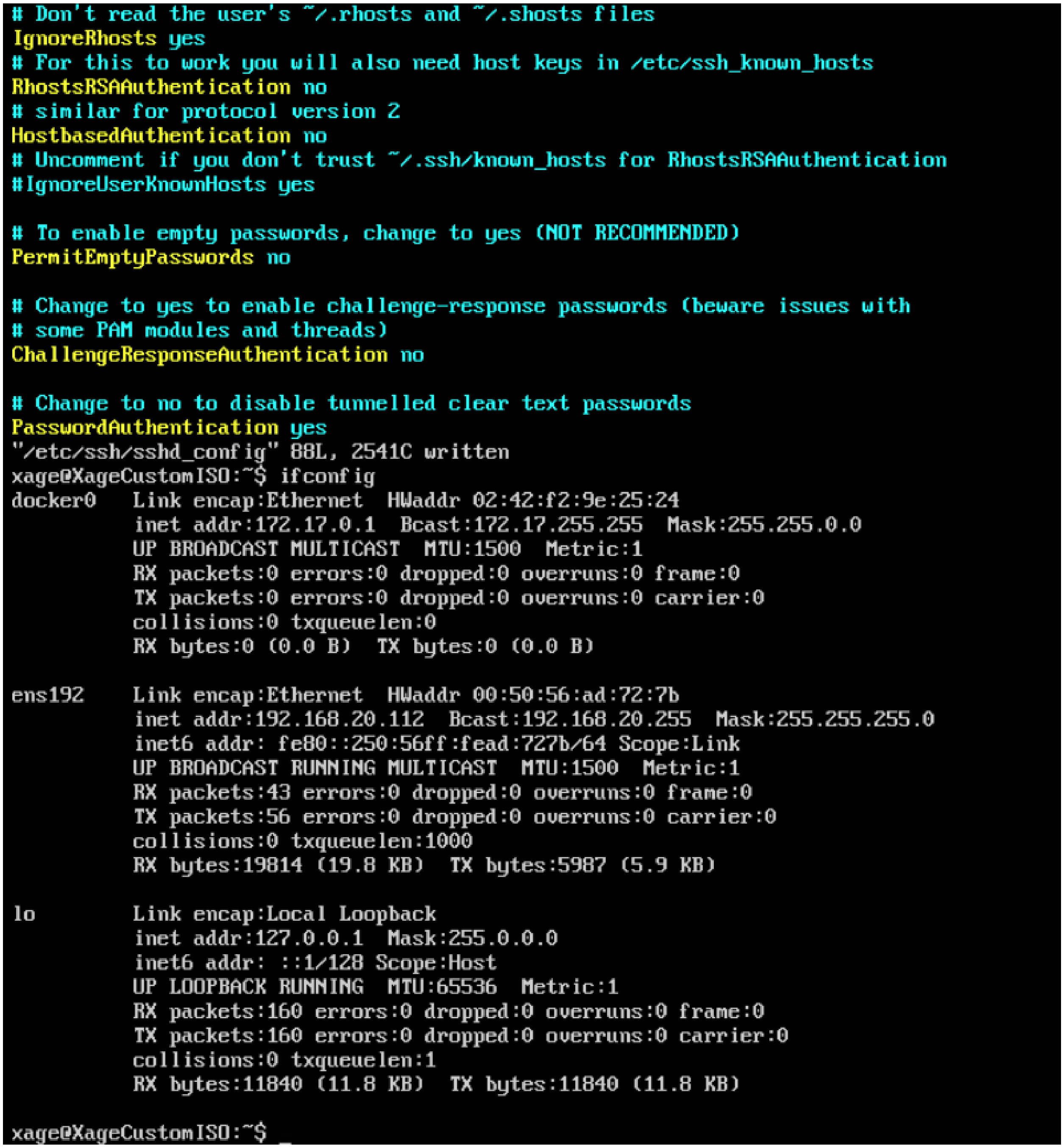
3. Begin the install and follow the Custom ISO install guide: Create a VM with 2 cores in the CPU, 8Gb RAM, and 60Gb Hard Drive size. Load the Xage Custom ISO into the virtual CD Drive and start the installer. Once completed, continue with the install.



```
Installing the system...
6%
Copying data to disk...
```

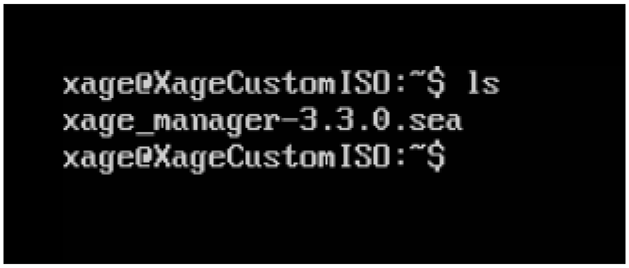
3. During the install, Xage creates a user that is used with the username **xage** and password **secret**. Log in to the VM using these credentials.

5. Type *sudo vi /etc/ssh/sshd_config* (or a different text editor) and ensure **PubkeyAuthentication** and **PasswordAuthentication** are uncommented and are set to **yes**. Then run *ifconfig* to get the IP address from the ethernet device.



```
# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
PasswordAuthentication yes
"/etc/ssh/sshd_config" 88L, 2541C written
xage@XageCustomISO:~$ ifconfig
docker0   Link encap:Ethernet  HWaddr 02:42:f2:9e:25:24
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

ens192    Link encap:Ethernet  HWaddr 00:50:56:ad:72:7b
          inet addr:192.168.20.112  Bcast:192.168.20.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fead:727b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19814 (19.8 KB)  TX bytes:5987 (5.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)

xage@XageCustomISO:~$ _
```

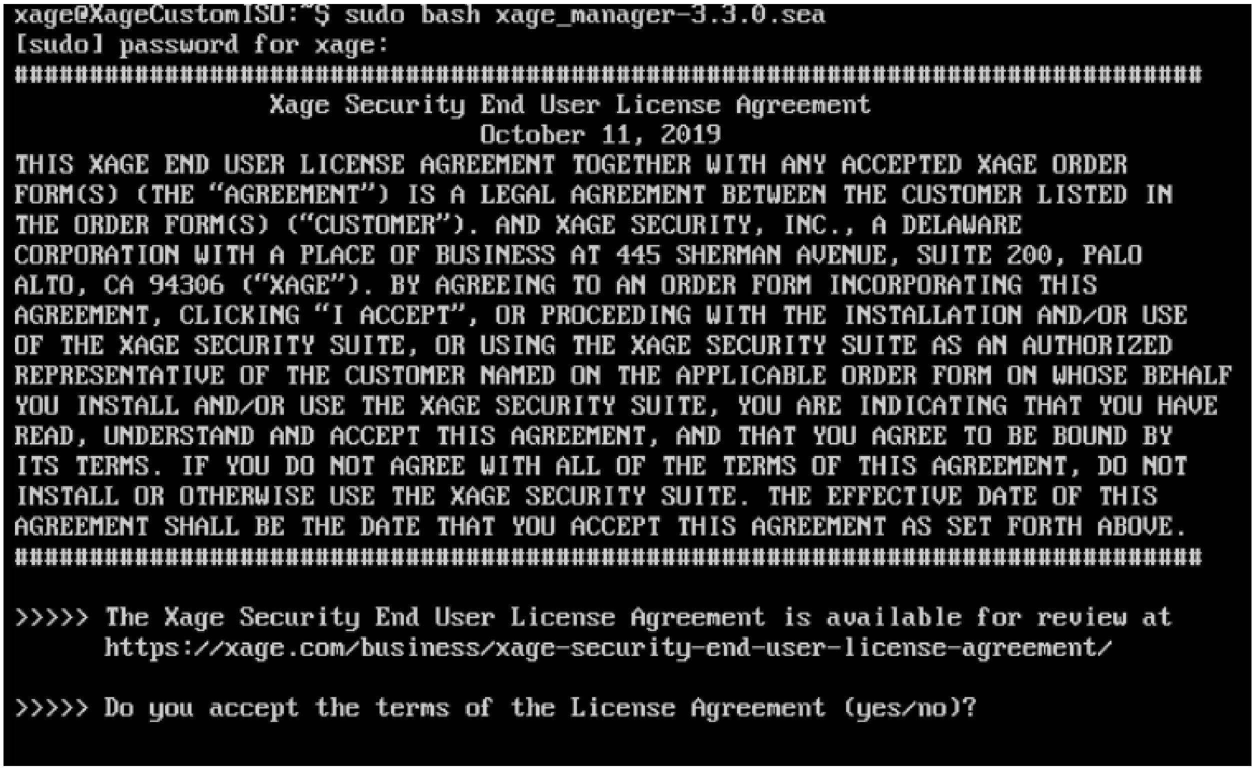
6. Using secure copy (SCP), copy the xage SEA file for installation to the Xage home drive.



```
xage@XageCustomISO:~$ ls
xage_manager-3.3.0.sea
xage@XageCustomISO:~$
```

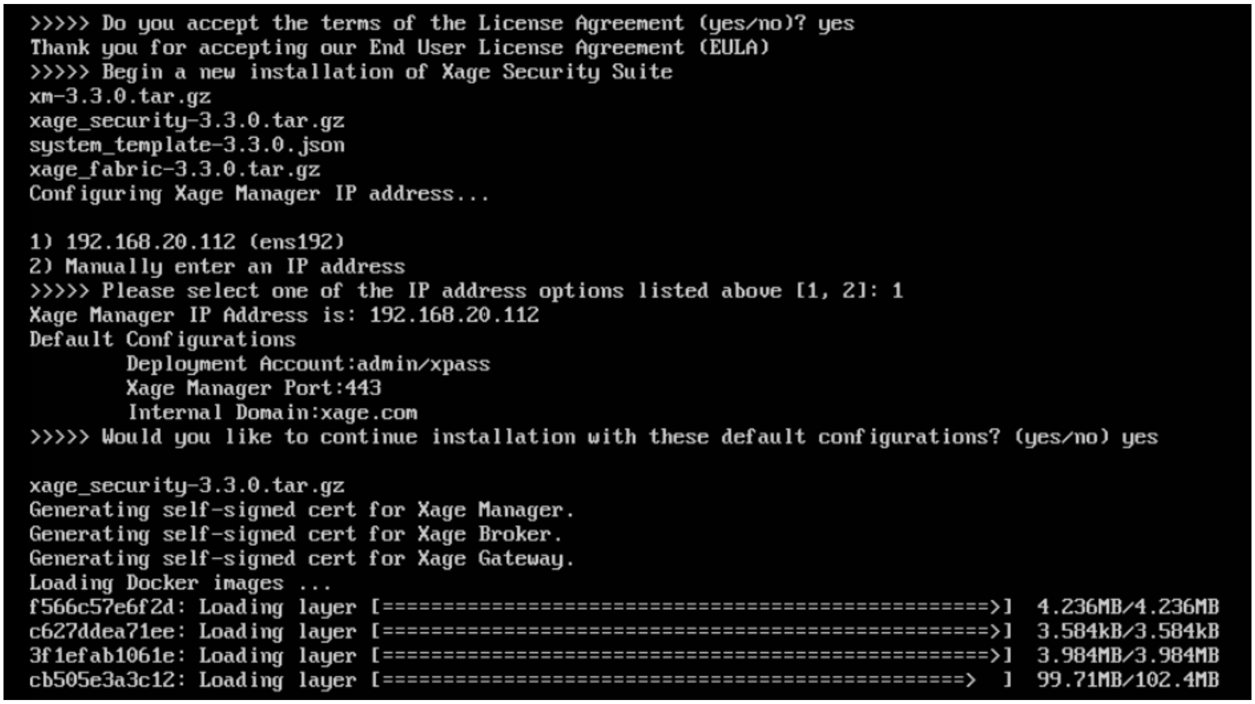
7. Beginning with the install guide, we opted to utilize Xage for managing users and user groups internally (as opposed to LDAP or Active Directory).

8. Begin installation by running *sudo bash xage_manager-3.3.0.sea* and accepting the EULA. Xage will then extract all the files.



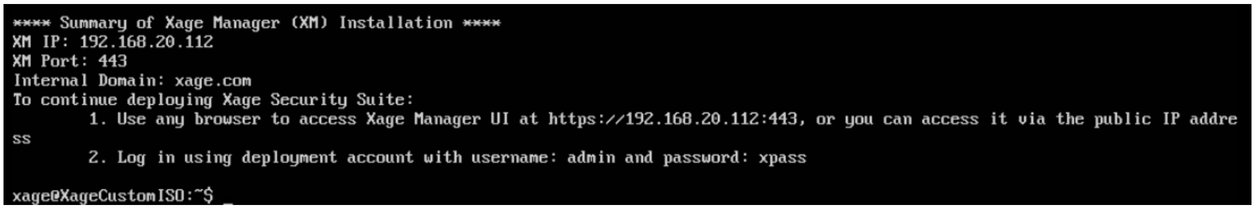
```
xage@XageCustomISO:~$ sudo bash xage_manager-3.3.0.sea
[sudo] password for xage:
###############################################################################
                 Xage Security End User License Agreement
                              October 11, 2019
THIS XAGE END USER LICENSE AGREEMENT TOGETHER WITH ANY ACCEPTED XAGE ORDER
FORM(S) (THE "AGREEMENT") IS A LEGAL AGREEMENT BETWEEN THE CUSTOMER LISTED IN
THE ORDER FORM(S) ("CUSTOMER"). AND XAGE SECURITY, INC., A DELAWARE
CORPORATION WITH A PLACE OF BUSINESS AT 445 SHERMAN AVENUE, SUITE 200, PALO
ALTO, CA 94306 ("XAGE"). BY AGREEING TO AN ORDER FORM INCORPORATING THIS
AGREEMENT, CLICKING "I ACCEPT", OR PROCEEDING WITH THE INSTALLATION AND/OR USE
OF THE XAGE SECURITY SUITE, OR USING THE XAGE SECURITY SUITE AS AN AUTHORIZED
REPRESENTATIVE OF THE CUSTOMER NAMED ON THE APPLICABLE ORDER FORM ON WHOSE BEHALF
YOU INSTALL AND/OR USE THE XAGE SECURITY SUITE, YOU ARE INDICATING THAT YOU HAVE
READ, UNDERSTAND AND ACCEPT THIS AGREEMENT, AND THAT YOU AGREE TO BE BOUND BY
ITS TERMS. IF YOU DO NOT AGREE WITH ALL OF THE TERMS OF THIS AGREEMENT, DO NOT
INSTALL OR OTHERWISE USE THE XAGE SECURITY SUITE. THE EFFECTIVE DATE OF THIS
AGREEMENT SHALL BE THE DATE THAT YOU ACCEPT THIS AGREEMENT AS SET FORTH ABOVE.
###############################################################################

>>>>> The Xage Security End User License Agreement is available for review at
      https://xage.com/business/xage-security-end-user-license-agreement/

>>>>> Do you accept the terms of the License Agreement (yes/no)?
```

9. The installer will then prompt for IP addresses. Select the default. Enter "yes" to accept the default configurations. Xage finishes the installation.



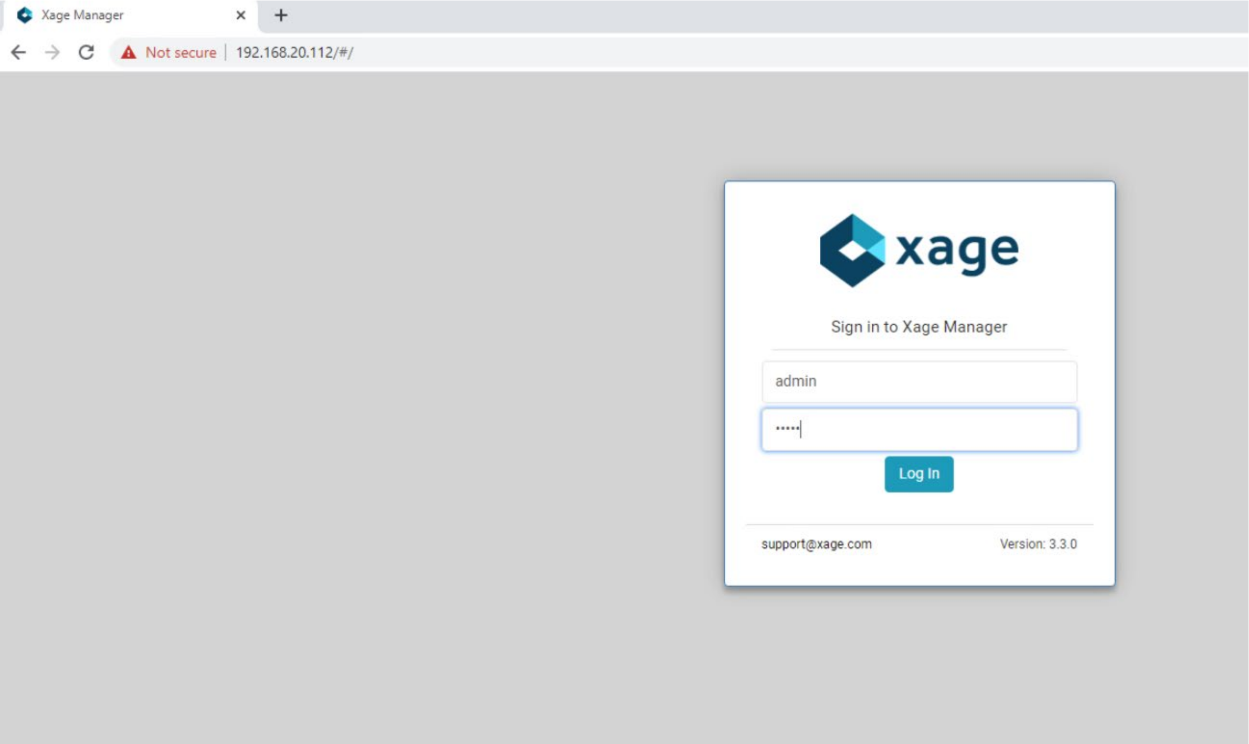
```
>>>>> Do you accept the terms of the License Agreement (yes/no)? yes
Thank you for accepting our End User License Agreement (EULA)
>>>>> Begin a new installation of Xage Security Suite
xm-3.3.0.tar.gz
xage_security-3.3.0.tar.gz
system_template-3.3.0.json
xage_fabric-3.3.0.tar.gz
Configuring Xage Manager IP address...

1) 192.168.20.112 (ens192)
2) Manually enter an IP address
>>>>> Please select one of the IP address options listed above [1, 2]: 1
Xage Manager IP Address is: 192.168.20.112
Default Configurations
        Deployment Account:admin/xpass
        Xage Manager Port:443
        Internal Domain:xage.com
>>>>> Would you like to continue installation with these default configurations? (yes/no) yes

xage_security-3.3.0.tar.gz
Generating self-signed cert for Xage Manager.
Generating self-signed cert for Xage Broker.
Generating self-signed cert for Xage Gateway.
Loading Docker images ...
f566c57e6f2d: Loading layer [==================================================>]  4.236MB/4.236MB
c627ddea71ee: Loading layer [==================================================>]  3.584kB/3.584kB
3f1efab1061e: Loading layer [==================================================>]  3.984MB/3.984MB
cb505e3a3c12: Loading layer [================================================>  ]  99.71MB/102.4MB
```

10. Once completed, Xage will give information on how to log in with a web server.



```
**** Summary of Xage Manager (XM) Installation ****
XM IP: 192.168.20.112
XM Port: 443
Internal Domain: xage.com
To continue deploying Xage Security Suite:
        1. Use any browser to access Xage Manager UI at https://192.168.20.112:443, or you can access it via the public IP addre
ss
        2. Log in using deployment account with username: admin and password: xpass

xage@XageCustomISO:~$ _
```

11. Log in to the web server at the IP address listed with the username and password listed.



Xage Manager

Not secure | 192.168.20.112/#/

xage

Sign in to Xage Manager

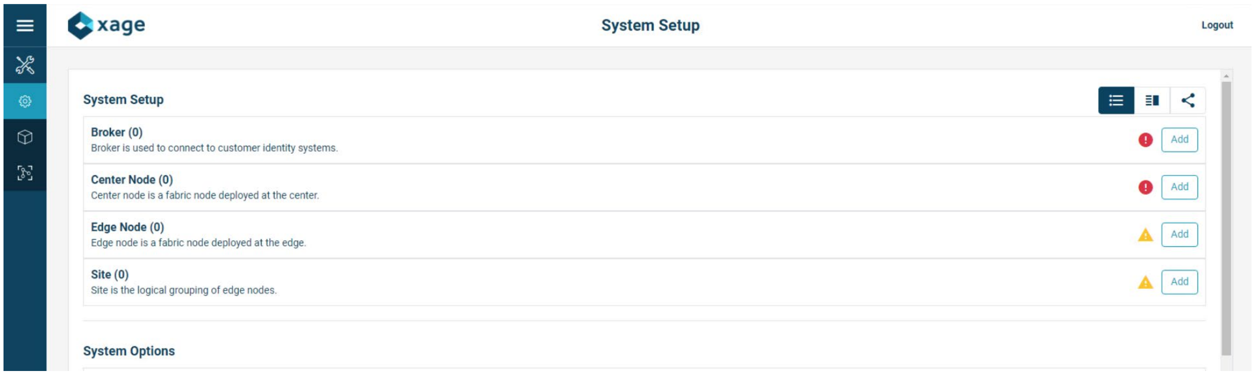
admin

•••••

Log In

support@xage.com Version: 3.3.0

12. After logging in, you will be prompted to add a Xage Broker, Xage Center Node, and Xage Edge Node. These need to be VMs installed in the environment, using the Xage Custom ISO. Following Step 3 of this section will install required base operating systems, then use those IP addresses for the individual installations.



xage System Setup Logout

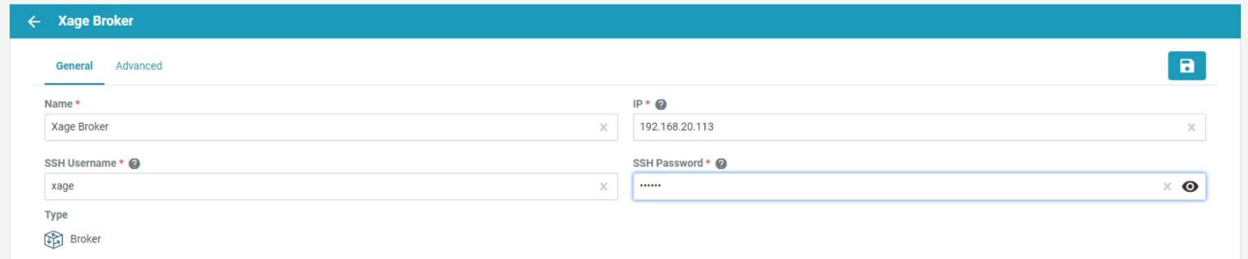
System Setup

| | |
|---|---|
| **Broker (0)**<br>Broker is used to connect to customer identity systems. | Add |
| **Center Node (0)**<br>Center node is a fabric node deployed at the center. | Add |
| **Edge Node (0)**<br>Edge node is a fabric node deployed at the edge. | Add |
| **Site (0)**<br>Site is the logical grouping of edge nodes. | Add |

System Options

13. Gather the IP addresses of the devices that will be added. In this installation, the IP addresses are as follows:
    a. Broker: 192.168.20.113
    b. Center Nodes (four is the minimum): 192.168.20.114, 192.168.20.117, 192.168.20.118, 192.168.20.119
    c. Edge Node: 192.168.20.115

14. Starting with the Xage Broker, click **Add** on the far right of the **Broker** row. Fill in the required information and click the create icon in the top right of the frame.



Name * Xage Broker

IP * 192.168.20.113

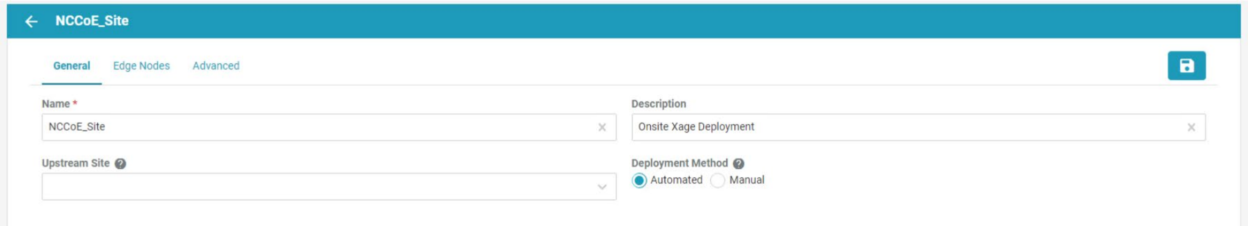
SSH Username * xage

SSH Password * ••••••

Type Broker

15. Repeat the previous step for Center Node and Edge Node.

16. Click **Add** on the far right of the **Site** row to add a new site. The **General Configuration** screen opens. Fill in the information as needed.



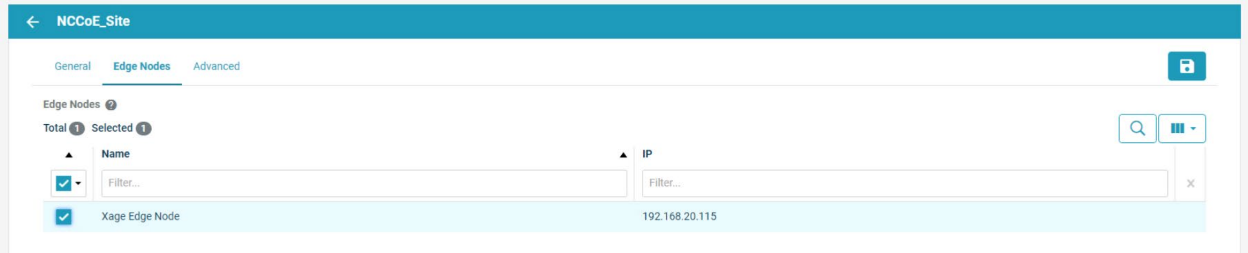
Name * NCCoE_Site

Description Onsite Xage Deployment

Upstream Site

Deployment Method ● Automated ○ Manual

17. Next, click **Edge Nodes** on the top bar and select the Xage Edge Node created earlier then, click **Create**.

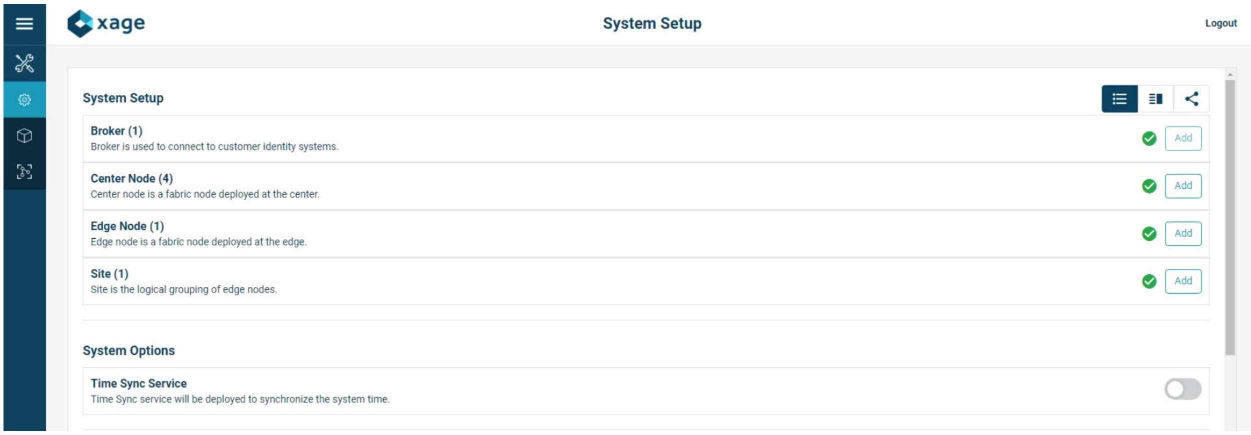


Edge Nodes

Total 1 Selected 1

| | Name | IP |
|---|---|---|
| ☑ | Filter... | Filter... |
| ☑ | Xage Edge Node | 192.168.20.115 |

18. Once all devices are configured completely, the **System Setup** page displays all green checks.



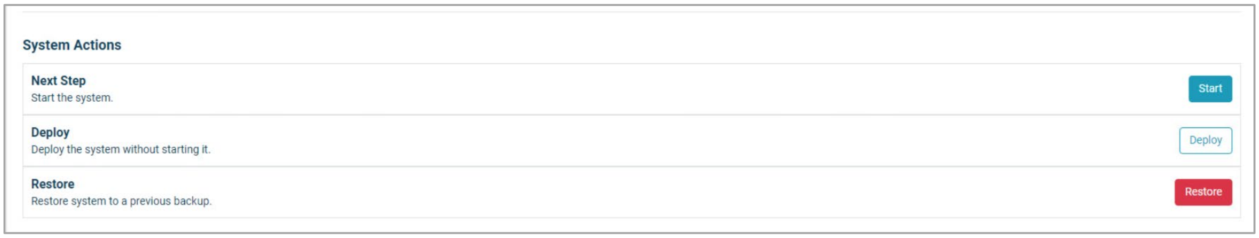
System Setup

| | | |
|---|---|---|
| **Broker (1)**<br>Broker is used to connect to customer identity systems. | ✓ | Add |
| **Center Node (4)**<br>Center node is a fabric node deployed at the center. | ✓ | Add |
| **Edge Node (1)**<br>Edge node is a fabric node deployed at the edge. | ✓ | Add |
| **Site (1)**<br>Site is the logical grouping of edge nodes. | ✓ | Add |

System Options

**Time Sync Service**
Time Sync service will be deployed to synchronize the system time.

19. At the bottom of the screen, Click **Start** to start the system. Then click **Start** again to confirm.



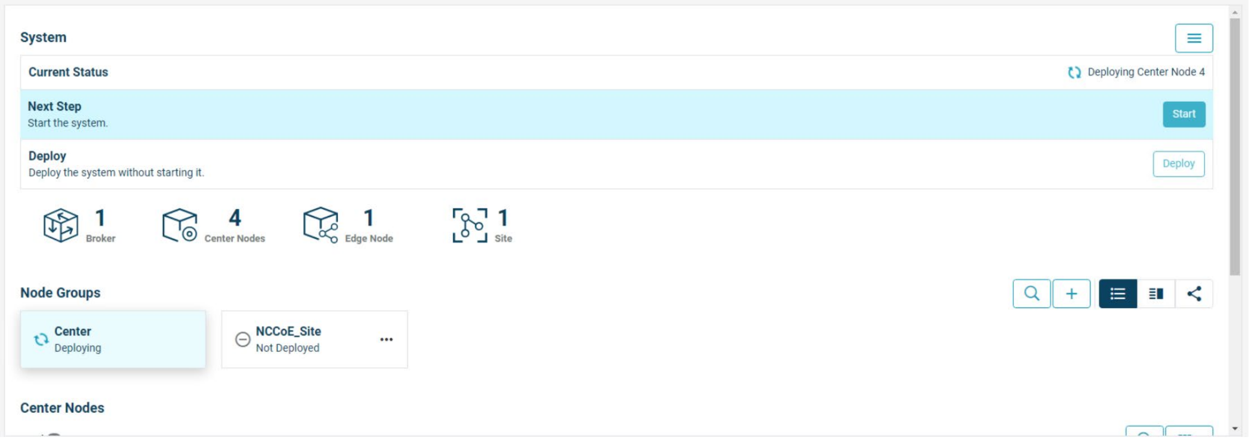
System Actions

Next Step
Start the system. Start

Deploy
Deploy the system without starting it. Deploy

Restore
Restore system to a previous backup. Restore

20. Starting will begin for the system, including deploying all nodes. **Current Status** will show what the system is currently doing.



System

Current Status — Deploying Center Node 4

Next Step
Start the system. Start

Deploy
Deploy the system without starting it. Deploy

1 Broker | 4 Center Nodes | 1 Edge Node | 1 Site

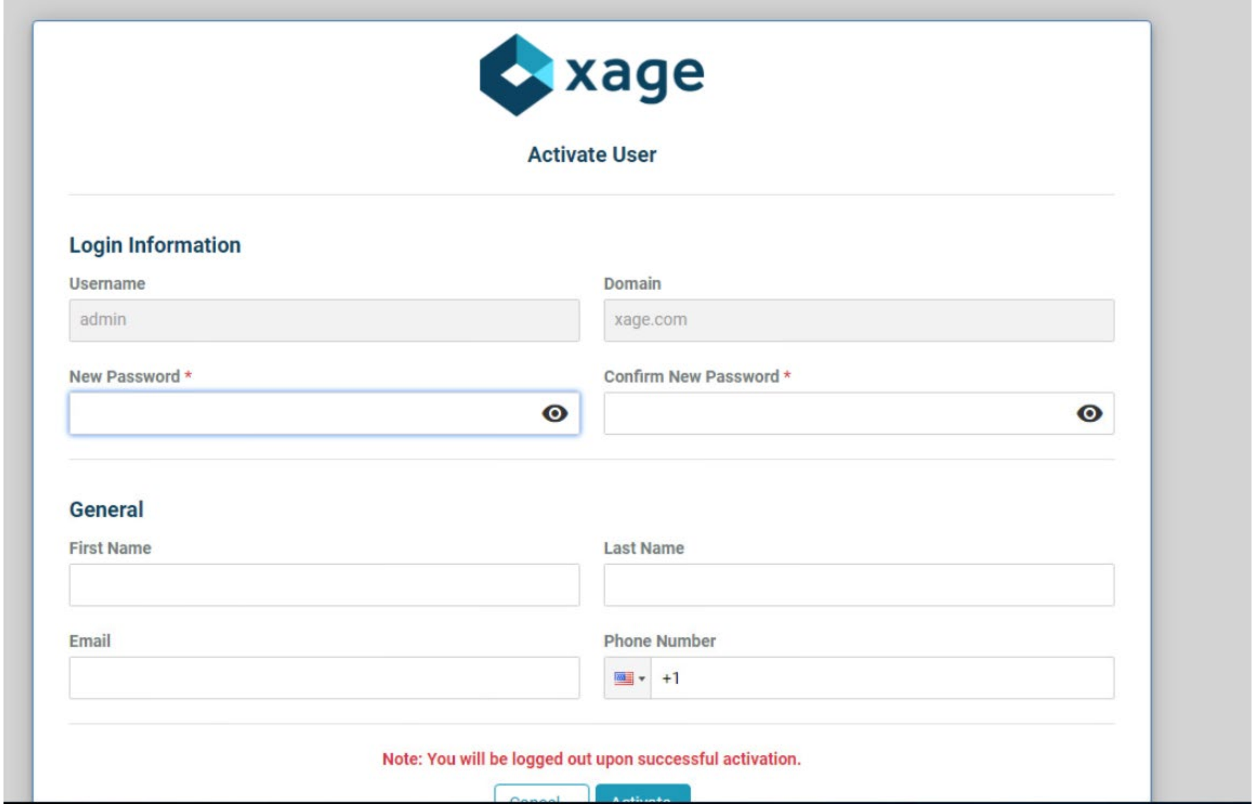
Node Groups

Center — Deploying

NCCoE_Site — Not Deployed

Center Nodes

21. After deployment is finished, you will have to login again and change your password to activate the manager.



**Login Information**

Username: admin

Domain: xage.com

New Password *

Confirm New Password *

**General**

First Name

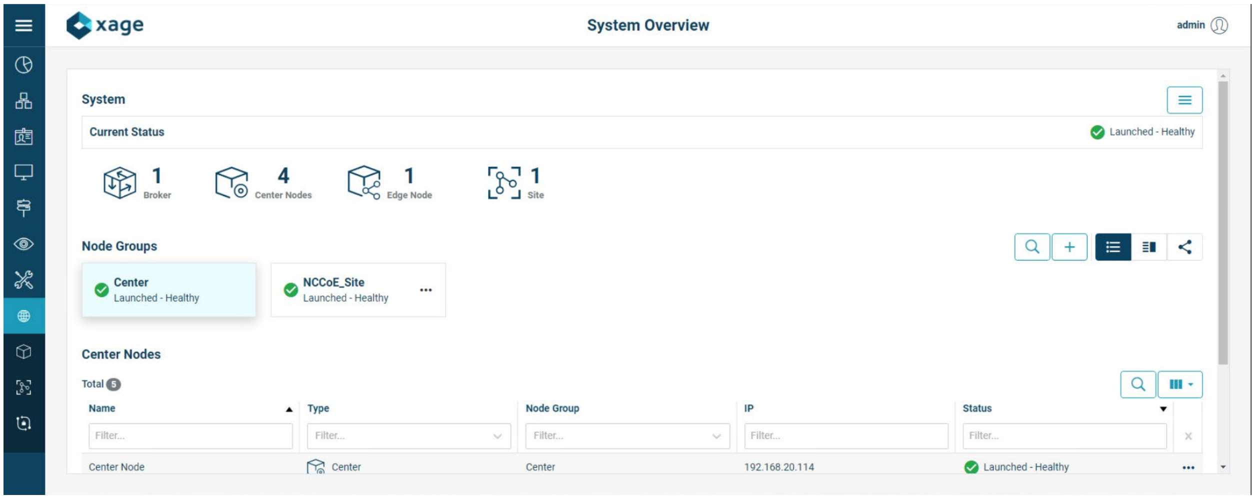
Last Name

Email

Phone Number: +1

Note: You will be logged out upon successful activation.

22. Once logged back in, Xage will show a green check mark labeled **Launched – Healthy**.



Current Status: ✓ Launched - Healthy

Node Groups: ✓ Center Launched - Healthy; ✓ NCCoE_Site Launched - Healthy

Center Nodes Total 5

| Name | Type | Node Group | IP | Status |
|---|---|---|---|---|
| Center Node | Center | Center | 192.168.20.114 | ✓ Launched - Healthy |

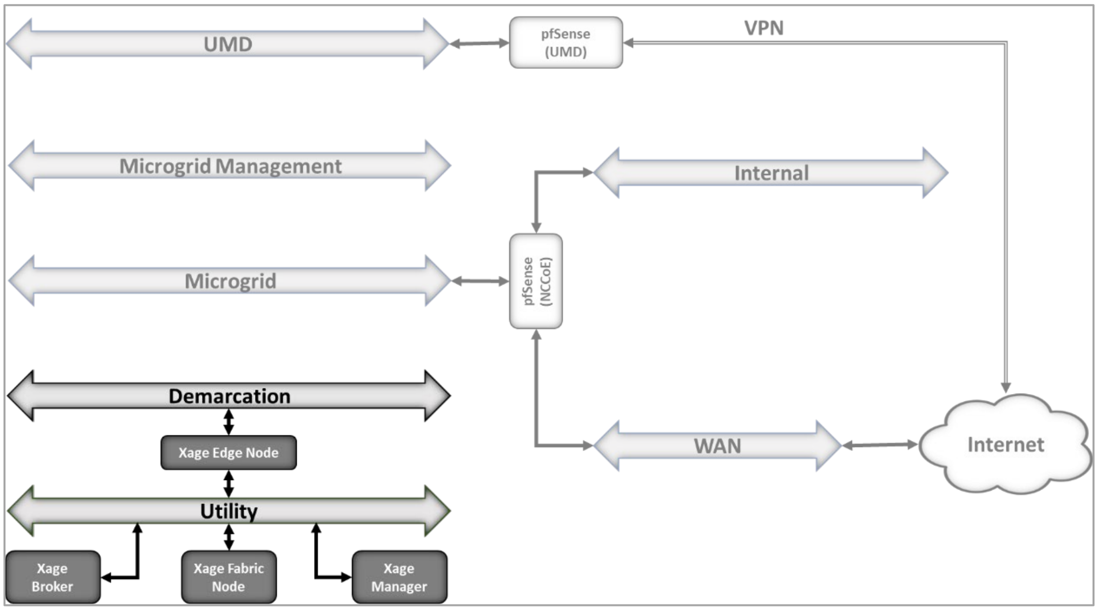
We configured three identities and two devices in the Xage Security Fabric using the Xage manager:

- One device was configured for each solar array at UMD.
- Three identities were configured:
  - One identity was given access to both UMD solar arrays.
  - One identity was given access to only one UMD solar array.

- One identity was given no access to the UMD solar arrays.

Figure 2-9 shows the location of the Xage components in the example solution.

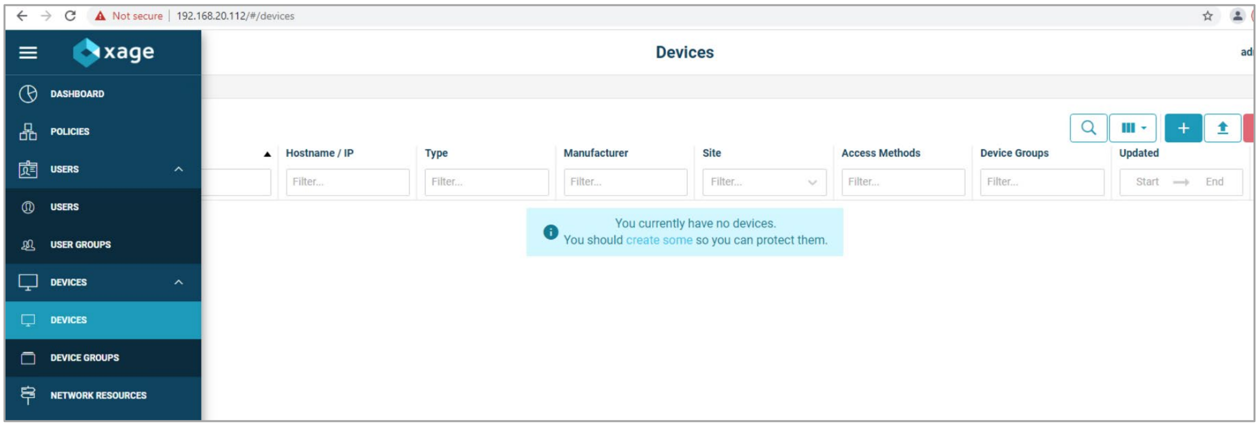
Figure 2-9 Xage Location in the Example Solution



## 2.8.2 Configure Xage Devices

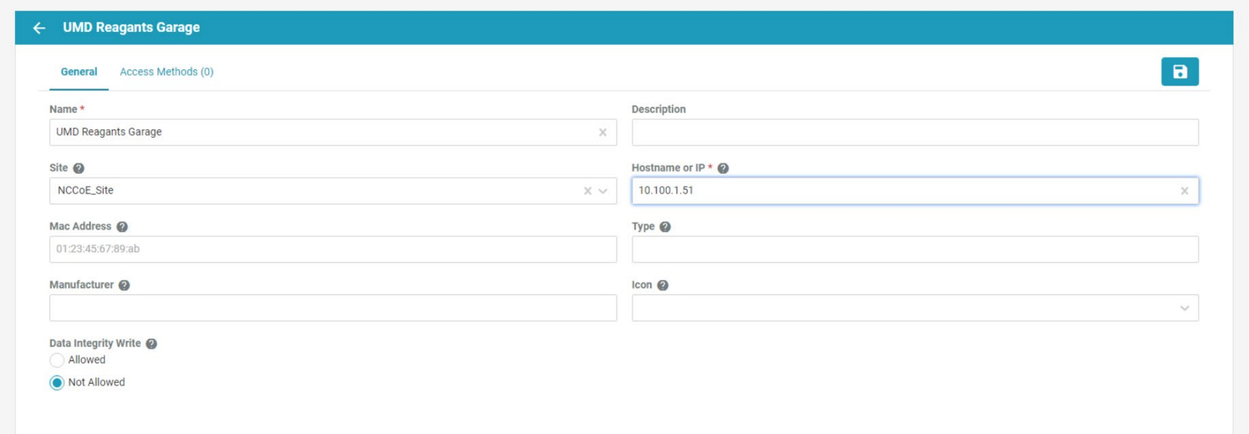
Follow these steps to configure Xage devices:

1. From the main Xage System Overview page, select **Devices > Devices** to create new devices for Xage.



You currently have no devices.
You should create some so you can protect them.

2. Click the **+** to create a new device, then fill in the details for that device.



Name * UMD Reagants Garage

Description

Site NCCoE_Site

Hostname or IP * 10.100.1.51

Mac Address 01:23:45:67:89:ab

Type

Manufacturer

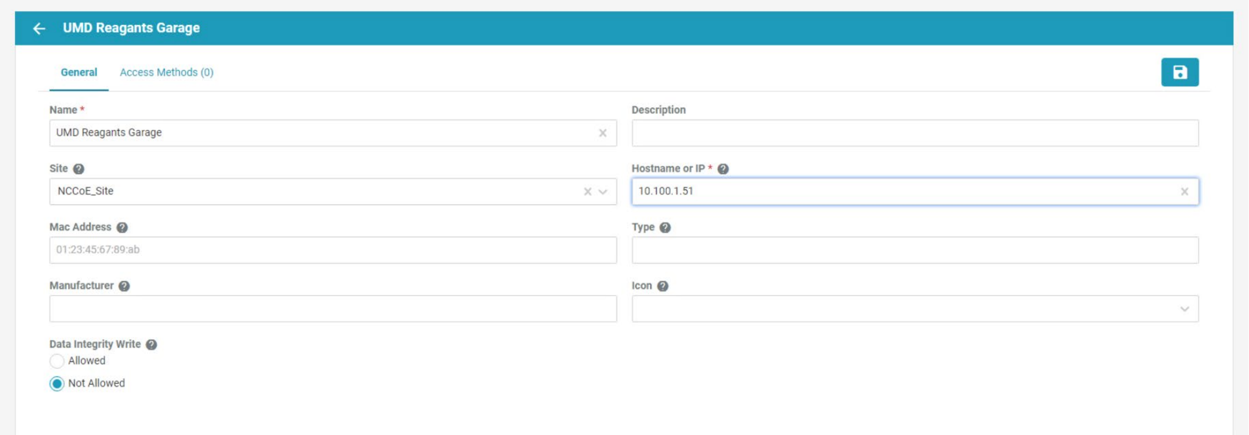
Icon

Data Integrity Write

○ Allowed

● Not Allowed

3. Click the **Access Methods** tab and fill in the details for an HTTP Proxy. Then click the **Create** button.



Name * UMD Reagants Garage

Description

Site NCCoE_Site

Hostname or IP * 10.100.1.51

Mac Address 01:23:45:67:89:ab

Type

Manufacturer

Icon

Data Integrity Write

○ Allowed

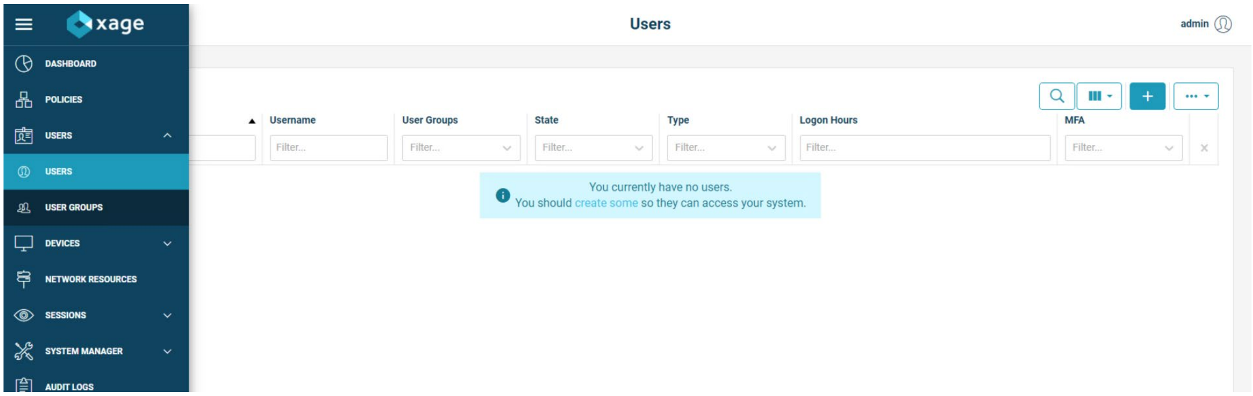
● Not Allowed

4. Repeat this method for the second device.

### 2.8.3 Configure Xage Identities

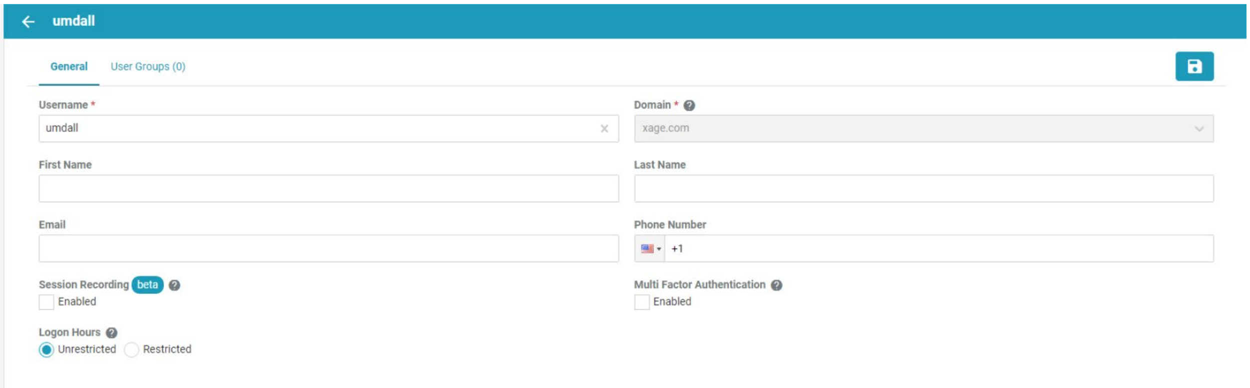
Follow these steps to configure Xage identities:

1. From the main Xage System Overview page, select **Users > Users** to create new identities for Xage.



You currently have no users.
You should create some so they can access your system.

2. Click the **+** to create a new user, then fill in the details for that user. This example shows a user that does not use session recording and does not restrict logon hours. The user also does not use multi-factor authentication. When finished, click the **create** button.



Username *
umdall

Domain *
xage.com

First Name

Last Name

Email

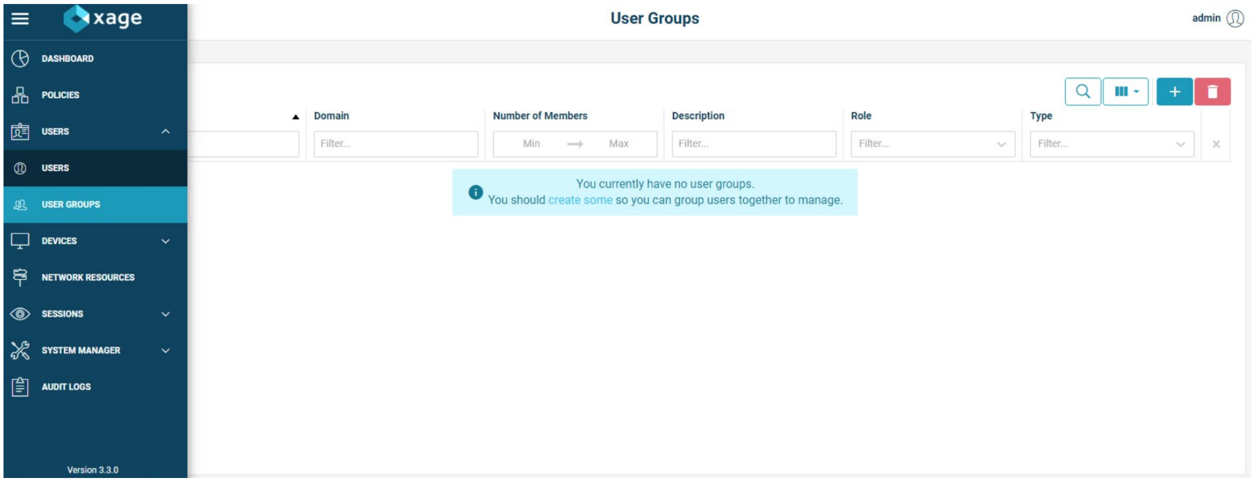
Phone Number
+1

Session Recording
□ Enabled

Multi Factor Authentication
□ Enabled

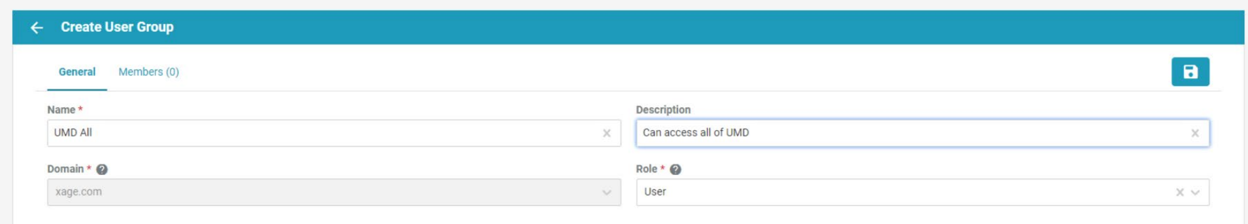
Logon Hours
● Unrestricted ○ Restricted

3. Add in other users as needed.
4. The next step is to create user groups for the users. Go to **Users > User Groups** and click the **+** sign.



You currently have no user groups.
You should create some so you can group users together to manage.

5. Add in details for the **General** tab, then move to the **Members** tab.



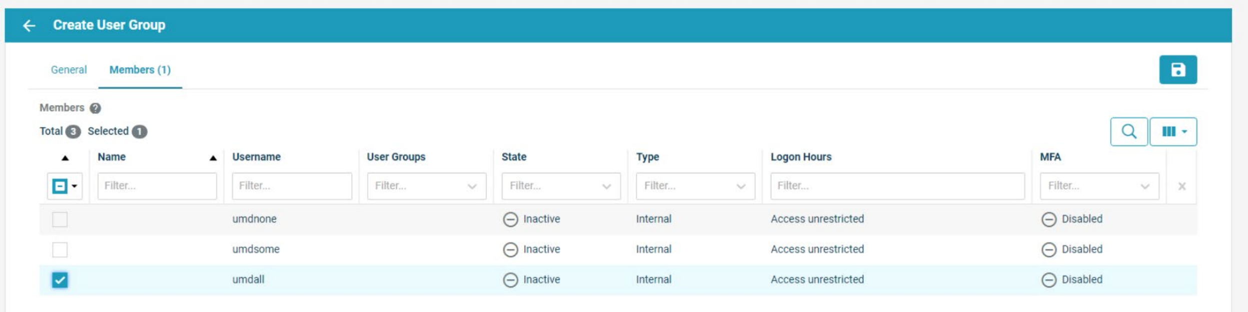
Name * UMD All

Description Can access all of UMD

Domain * xage.com

Role * User

6. Select users for addition to the current group, then click the create button. Repeat for all necessary groups.



Total 3 Selected 1

| | Name | Username | User Groups | State | Type | Logon Hours | MFA |
|---|---|---|---|---|---|---|---|
| □ | | umdnone | | Inactive | Internal | Access unrestricted | Disabled |
| □ | | umdsome | | Inactive | Internal | Access unrestricted | Disabled |
| ☑ | | umdall | | Inactive | Internal | Access unrestricted | Disabled |

## 2.9 pfSense Open-source Firewall

pfSense is an open-source firewall/router used to create a site-to-site VPN tunnel between the NCCoE lab and the UMD campus network.

We installed pfSense using the installation guide at https://docs.netgate.com/pfsense/en/latest/install/download-installer-image.html. We installed pfSense in a Linux virtual machine in our virtual lab using the ISO installation media option.

We used the instructions at https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/index.html to configure the VPN.

## 2.10 Syslog-ng Open-Source Log Management

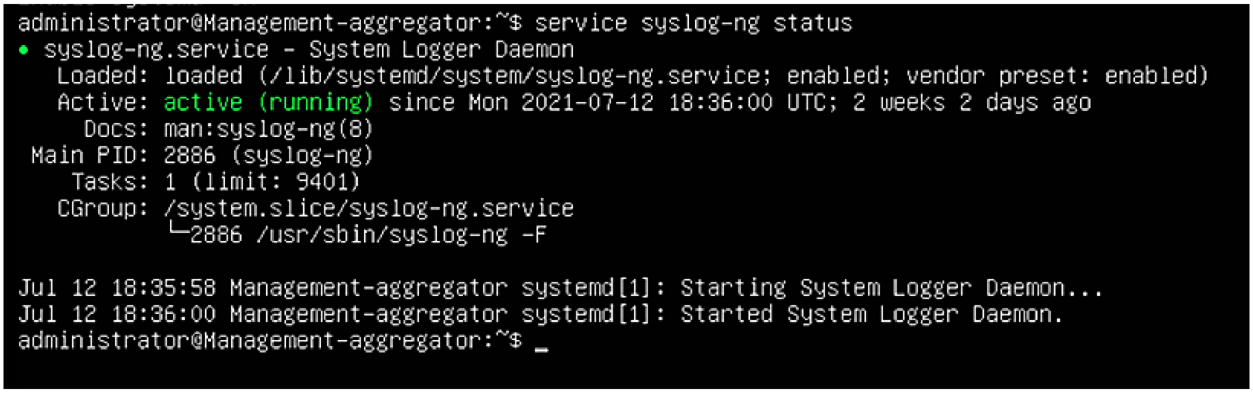
Syslog-ng is an open source log server (https://github.com/syslog-ng/syslog-ng). Syslog ng provides the second part of the log collector component of the reference architecture. Syslog ng serves as a syslog aggregator. Cisco ISE and Cisco Cyber Vision send their syslog data to syslog ng. Syslog ng then sends the aggregated data to the Sumo Logic syslog collector for transport to the Sumo Logic software-as-a-service analysis and visualization capabilities to process. Figure 8 shows syslog-ng implementing the reference architecture log aggregator element.

We used Linux Centos 8 VMs to host our syslog-ng instances -ng.

### 2.10.1 Installing Syslog-ng

Follow these steps to install Syslog-ng:

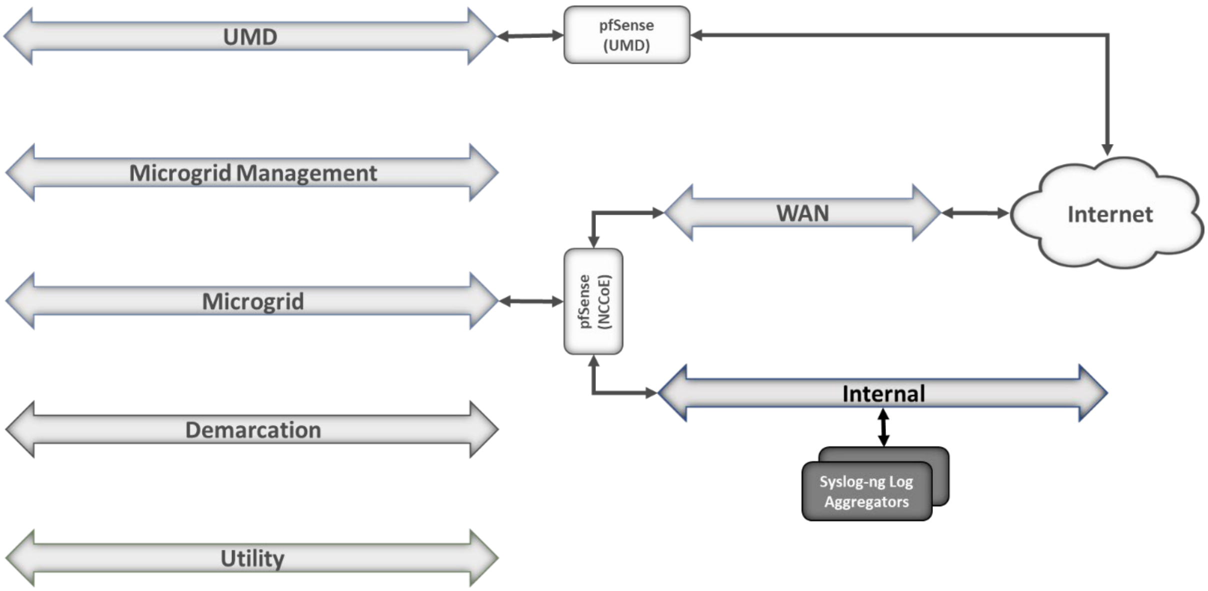
1. On a VM that will host syslog-ng, run the command `sudo apt-get install syslog-ng -y`.
2. When this completes, check the syslog-ng version with the command `syslog-ng –version`.
3. Verify syslog-ng is running with the command `syslog-ng status`.



```
administrator@Management-aggregator:~$ service syslog-ng status
● syslog-ng.service - System Logger Daemon
   Loaded: loaded (/lib/systemd/system/syslog-ng.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-07-12 18:36:00 UTC; 2 weeks 2 days ago
     Docs: man:syslog-ng(8)
 Main PID: 2886 (syslog-ng)
    Tasks: 1 (limit: 9401)
   CGroup: /system.slice/syslog-ng.service
           └─2886 /usr/sbin/syslog-ng -F

Jul 12 18:35:58 Management-aggregator systemd[1]: Starting System Logger Daemon...
Jul 12 18:36:00 Management-aggregator systemd[1]: Started System Logger Daemon.
administrator@Management-aggregator:~$ _
```

Figure 2-10 shows the location of the syslog-ng log aggregators in the example solution.

**Figure 2-10 syslog-ng Location in the Example Solution**

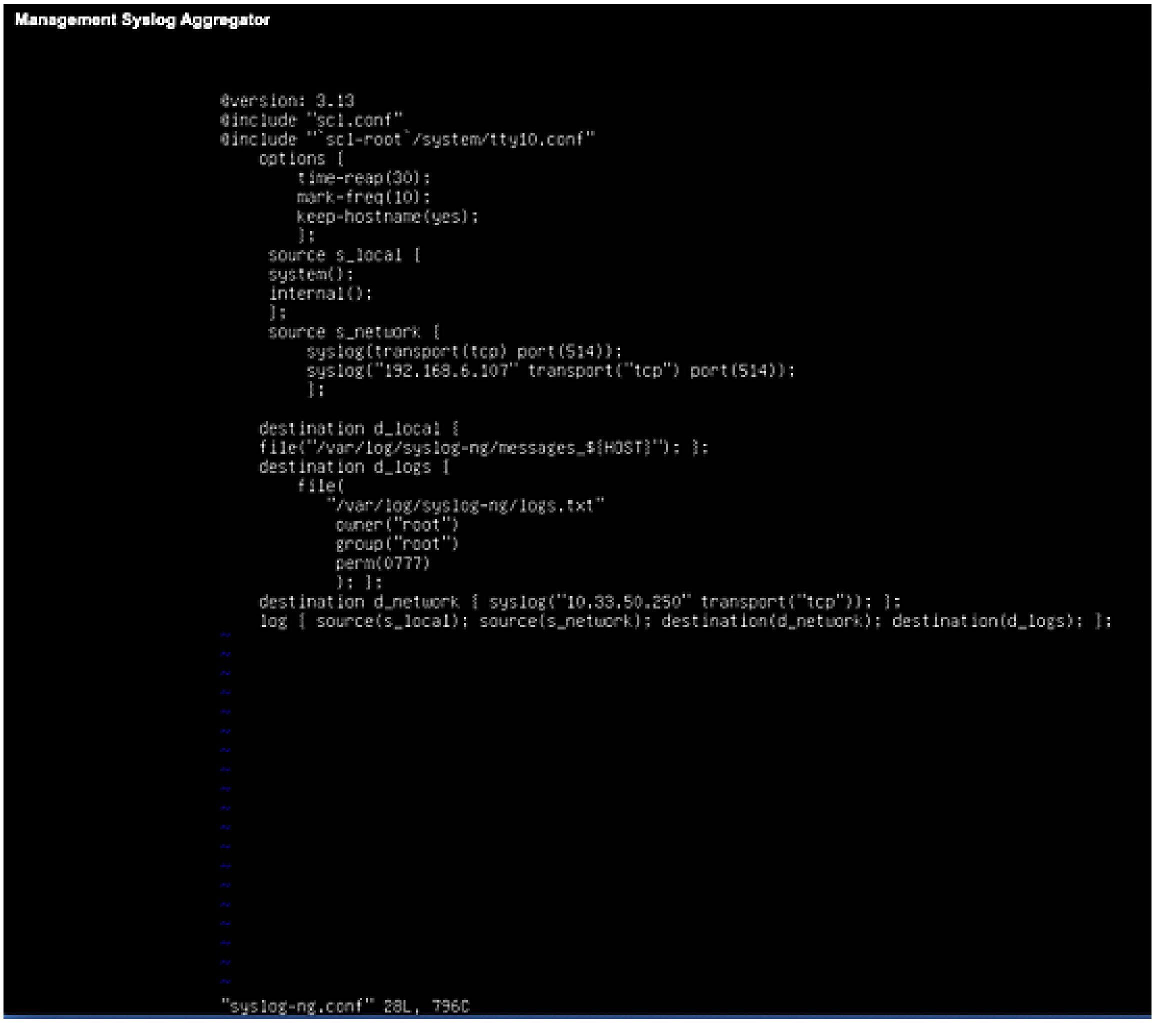


## 2.10.2 Configuring Syslog-ng

Follow these steps to configure Syslog-ng:

1. Navigate to the `/etc/syslog-ng` directory using the command `cd /etc/syslog-ng` and run the command `vim syslog-ng.conf` to configure `scl.conf`.

2. For each product that sends log data to syslog-ng, edit the source and destination configuration information to add the IP address, protocol, and port number.



Management Syslog Aggregator

```
@version: 3.13
@include "scl.conf"
@include "`scl-root`/system/tty10.conf"
    options {
        time-reap(30);
        mark-freq(10);
        keep-hostname(yes);
        };
     source s_local {
     system();
     internal();
     };
     source s_network {
         syslog(transport(tcp) port(514));
         syslog("192.168.6.107" transport("tcp") port(514));
         };

    destination d_local {
    file("/var/log/syslog-ng/messages_${HOST}"); };
    destination d_logs {
        file(
           "/var/log/syslog-ng/logs.txt"
            owner("root")
            group("root")
            perm(0777)
            ); };
    destination d_network { syslog("10.33.50.250" transport("tcp")); };
    log { source(s_local); source(s_network); destination(d_network); destination(d_logs); };
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"syslog-ng.conf" 28L, 796C
```

# Appendix A List of Acronyms

| | |
|---|---|
| **CA** | Certificate Authority |
| **DER** | Distributed Energy Resource |
| **GW** | Gateway |
| **IP** | Internet Protocol |
| **ISO** | Optical disk image in International Standards Organization 9660 format |
| **IT** | Information Technology |
| **LAN** | Local Area Network |
| **LTE** | Long Term Evolution |
| **NCCoE** | National Cybersecurity Center of Excellence |
| **NIST** | National Institute of Standards and Technology |
| **OT** | Operational Technology |
| **OVA** | Open Virtualization Appliance |
| **PV** | Photovoltaic |
| **SaaS** | Software as a Service |
| **SIEM** | Security Information and Event Management |
| **SP** | Special Publication |
| **TAC** | Transport Access Control |
| **vLAN** | Virtual Local Area Network |
| **VM** | Virtual Machine |
| **UMD** | University of Maryland |

# Appendix B Software for Using Immutably

This appendix presents the software used to send records to the command register. This same software, with minor variations, is used in the distribution ops system, front end processor, and microgrid master controller.

```
import requests

import json

from requests_oauthlib import OAuth1, OAuth1Session

from pyModbusTCP.client import ModbusClient

from pyModbusTCP.server import ModbusServer, DataBank

from time import sleep



class Proofworks:

    def __init__(self):

        self.host = 'https://immutably.client.cxl.io/api'

        self.key = 'kXHeHvHnwEDeGFPOmjTs39Oest42WxmXz62y1LfJ'

        self.secret = 
'GiXxoeWk26DnFUloSn3rQQ97tZHm7SGdK86au5bLqTJtIHuzrzK6nd0J4lqArYrI'

        self.realm = '74b8e784-242b-11e8-b467-0ed5f89f718b.0d091c52-2431-11e8-b467-
0ed5f89f718b.fee64f24-f8c5-4406-953e-3705cccd9c3c'

        self.project_id = 'b269de55-8c42-482f-a0cb-2077c3f9be9f'

        self.session = None

    def login(self):

        payload = json.dumps({
          "key": self.key,
          "secret": self.secret,
          "realm": self.realm
        })

        headers = {
          'Content-Type': 'application/vnd.io.cxl.credentials.consumer-key+json',
          'Authorization': 'OAuth
realm="realm",oauth_consumer_key="key",oauth_signature_method="HMAC-
SHA1",oauth_timestamp="1504127763",oauth_nonce="6ULC6xT4Fxi",oauth_version="1.0",
oauth_signature="%2BegGM2djZ032sy7MyTwpfnqByZg%3D"'
        }

        oauth = OAuth1(self.key, client_secret=self.secret)
        response = requests.request("POST", f"{self.host}/authc/login", auth=oauth,
headers=headers, data=payload)
        token = str(response.json()['access-token'])

        self.session = OAuth1Session(self.key, client_secret=self.secret,
resource_owner_key=token, realm=self.realm)

    def get_total_proofs_in_project(self):
        response = self.session.get(
            f"{self.host}/proofworks/projects/{self.project_id}/proofs", timeout=10,
           )
        r = response.json()
        return r.get('count')

    def create_proof(self, source, NetRealEnergy, V_LL, Current, Frequency):
```

```
headers = {
        "Content-Type": "application/json"
    }

proof = json.dumps([
  {"==": ["source: ", source]},
  {"==": ["Real Energy - Net: ", NetRealEnergy]},
  {"==": ["Voltage - L-L: ", V_LL]},
  {"==": ["Current: ", Current]},
  {"==": ["Frequency: ", Frequency]}
])

response = self.session.post(
        f"{self.host}/proofworks/projects/{self.project_id}/proofs",
        data=proof,
        timeout=10,
        headers=headers,
    )
```

# Appendix C References

[1] Xage Security, Xage Security Fabric Installation Guide, Version 3.2.0, February 2021.