Dell Validated Design for Energy Edge

Design Guide with ABB and Forescout

H19725

Abstract

This document describes a validated design for substation automation and cybersecurity solutions in the energy and utilities industry. This is the result of a joint effort between Dell Technologies, ABB, and Forescout. The software from both of these industry-leading independent software vendors is fully validated on Dell hardware and platforms.

Dell Solutions

August 2023

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2023 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

1

Introduction

Topics:

Overview

The utility grid is transforming from passive to active, uni-directional to bi-directional. This transformation is changing the fundamental operation from a rigid Operational Technology (OT) centric, one-way energy flow model to a more dynamic, two-way, data-driven model supporting intermittent renewable resources and flexible customer loads. Due to this transformation, utilities are continuously facing challenges, both internal and external. A few of these challenges are :

- Cybersecurity
- Infrastructure modernization
- Declining knowledge base
- Predictive maintenance
- Regulatory uncertainty
- Renewable/EV management
- Climate change

Dell Validated Design for Energy Edge

The new Dell energy edge solution runs on PowerEdge XR12 servers and empowers utilities to modernize their legacy systems efficiently with virtualization that allows for seamless information technology (IT)/OT system integration, delivering a more resilient and agile grid. Substation virtualization is becoming increasingly popular in the power industry as it offers a more efficient and flexible approach to managing substations. Virtualized substations are vulnerable to cyberattacks, which can cause significant damage to the power system. This solution presents a novel approach for enhancing substation virtualization by incorporating layers of cybersecurity and high availability to ensure the security and reliability of the substation.

The proposed approach consists of three main components: secure virtualization, layered cybersecurity, and high availability. Secure virtualization involves the use of virtualization technologies that provide secure isolation of virtual machines, networks, and storage. Layered cybersecurity involves the implementation of multiple layers of cybersecurity controls, including firewalls, intrusion detection and prevention systems, and network segmentation. High availability involves the use of redundant hardware, software, and network components to ensure the availability of the substation in the event of hardware or software failures.

The Dell Validated Design for Energy Edge enables grid modernization and asset insights without compromising security.

Rugged and reliable hardware with a common operating platform provides flexibility for choice of software for multi-applications (varied utility applications) and Internet of Things (IoT) technologies. This flexibility enables customers to pick and choose (mix and match) their OT/IT vendors of choice for a reliable, integrated solution that enables fast and efficient data processing, which accelerates time to insight and increases operating efficiency. It also enables remote management of assets securely.

The digitized control system of the solution is compatible with traditional (copper wired) serial communications and modern TCP/IP-based communication, and the process bus is interoperable with IEC 61850. Integrated cybersecurity features facilitate secure, mission-critical monitoring and control while helping to reach regulatory requirements.

Use case: substation automation

The Dell Validated Design for Energy Edge is ideal for substation-based applications like data aggregation and substation/distribution automation, as well as sending data to a control center to aggregate data from multiple substations into an advanced distribution management system (ADMS) or energy management system (EMS).

With this solution, the concept of fail-safe operations can now be applied to IT/OT architectures. This helps to keep aging systems up to date with new technology while mitigating significant vulnerabilities due to: legacy issues, siloed data, multiple IT assets management, and disconnected applications.

Overall, this solution provides a comprehensive approach for enhancing substation virtualization by incorporating layers of cybersecurity and high availability. By adopting this approach, utilities can ensure the security and reliability of their virtualized substations and minimize the risk of cyberattacks that could cause significant damage to the power system. The proposed approach can also serve as a guideline for utilities that are considering virtualizing their substations, ensuring that they do so securely and with high availability.

To demonstrate the effectiveness this approach, a virtualized substation is presented as a solution. This Dell Validated Design shows how this approach can enhance the security and reliability of the substation by providing secure isolation, layered cybersecurity controls, and high availability.

2

Architecture

Topics:

- Architectural overview
- Architecture components

Architectural overview

The Dell Validated Design for Energy Edge consists of the following components:

- Dell PowerEdge servers with VMware Hypervisor (ESXi)
- Substation automation and visualization with ZEE600 from ABB
- Cybersecurity with Forescout
- Dell Edge Gateways
- IEDs and industrial controllers

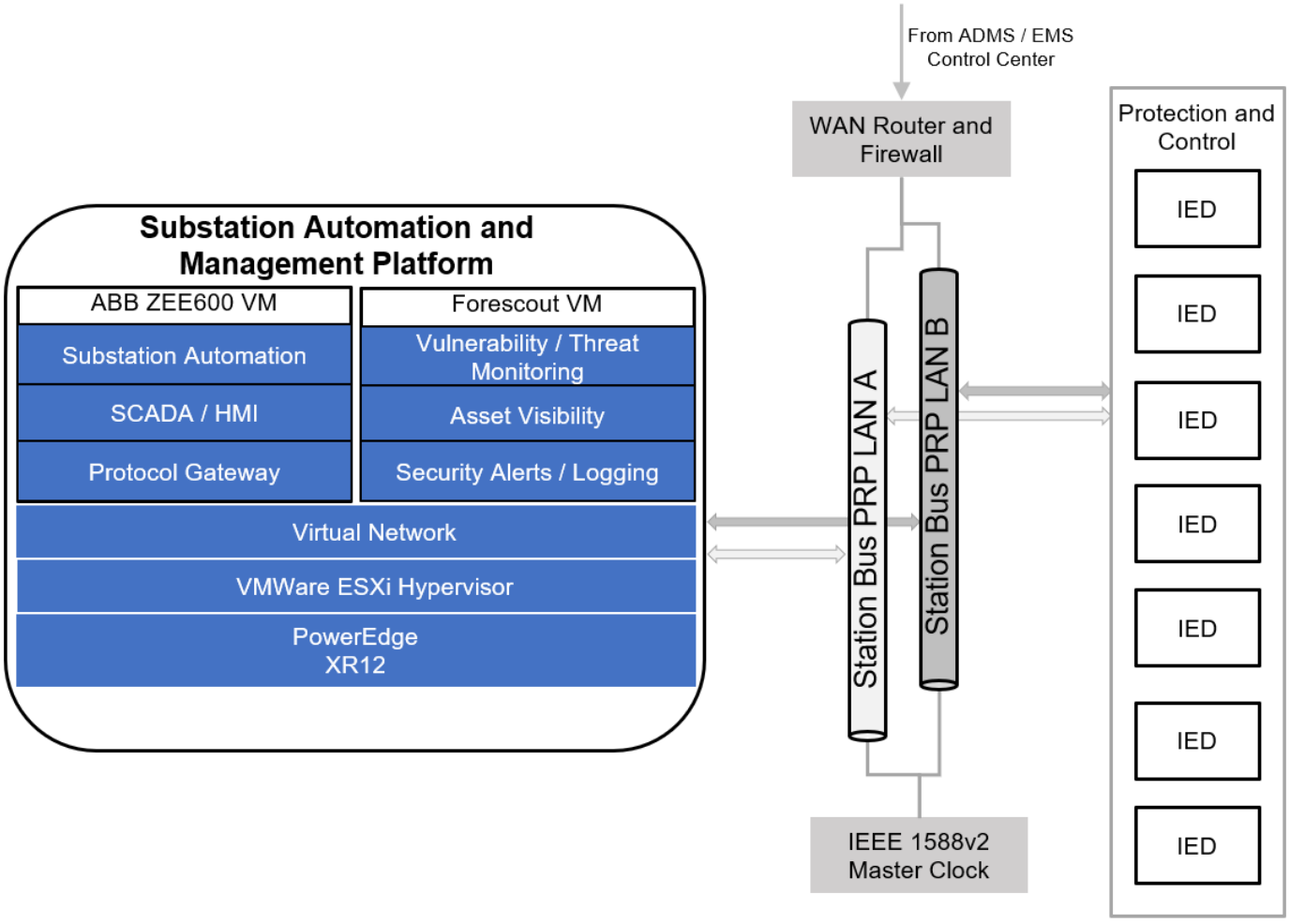


Figure 1. DVD for Energy Edge architecture

The architecture covered in this DVD for Energy Edge with ABB and Forescout addresses substation automation use cases by integrating the data handling, automation, and visualization offered by ABB ZEE600 along with the cybersecurity monitoring

and detection from Forescout. In this DVD, a substation, with downstream connections to IEDs (intelligent electronic devices) and upstream connections to a regional control center, is used to represent typical digital components of electrical distribution. This document describes the integration of Dell hardware, the VMware virtualized platform, and several independent software vendor (ISV) applications to validate the design and provide size and scaling guidance.

Some of the use cases this document addresses in detail are:

- Data aggregation
- Substation automation and SCADA
- Protocol gateway

The following figure shows the integrated architecture used in this validated design. It shows how the ISV applications connect to the devices found in a substation, how data flows through the system, and how the components work together to meet operational needs in a seamless and secure way.

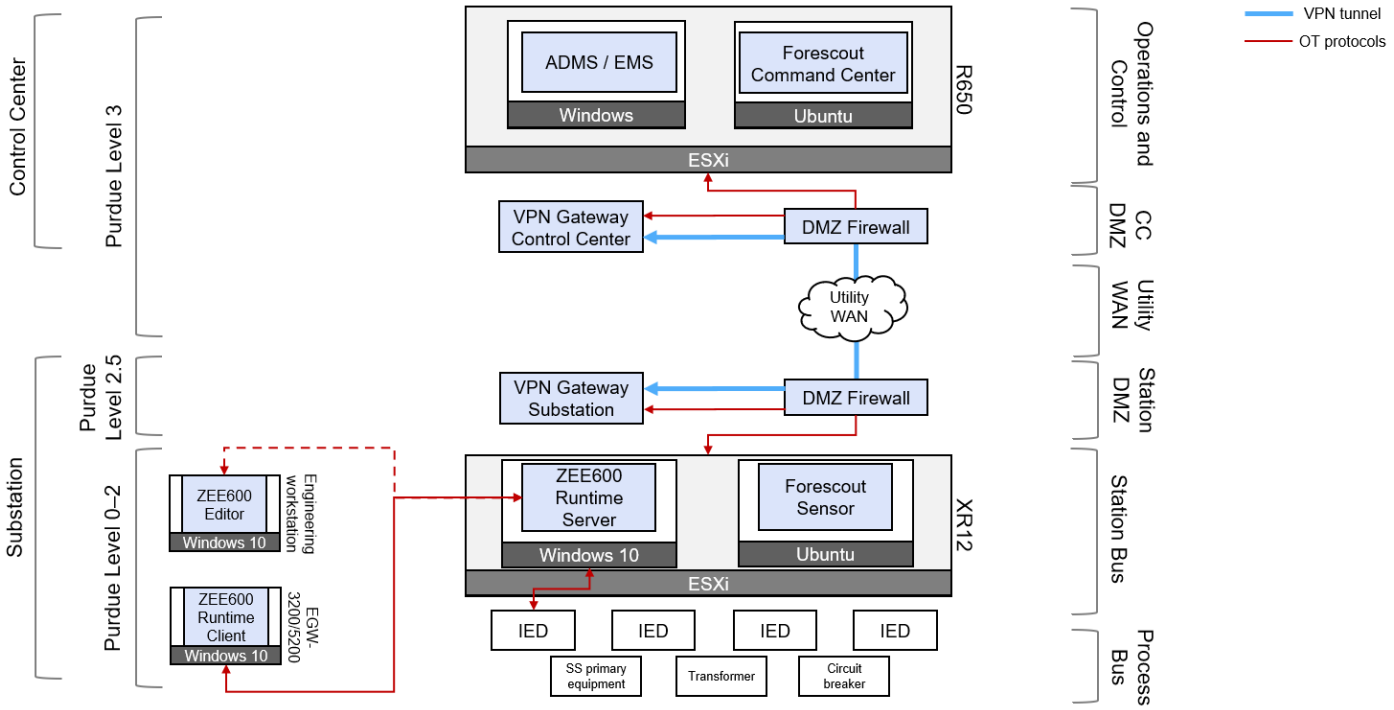


Figure 2. DVD for Energy Edge detailed application and hardware architecture

The following is a high-level description of the Dell Validated Design for Energy Edge:

- VMware vSphere and vSAN supported virtual machines for ABB ZEE600 and Forescout eyeInspect Sensor applications (Passive and Active) on Dell PowerEdge XR12 servers
- VMware vSphere and vSAN supported virtual machines for Forescout Command Center on Dell PowerEdge R660/R670 servers
- Dell Edge Gateways 3200 and 5200 running ABB ZEE600 Runtime HMI clients

Subsequent chapters describe each of the components in detail and discuss considerations and best practices.

Architecture components

The following sections describe the architecture components of the Dell Validated Design for Energy Edge.

PowerEdge

Dell PowerEdge servers are offered in this DVD as a standalone configuration. To enable future growth and to adapt to changing application demands, Dell PowerEdge servers offer adaptive computability depending on server application.

The intelligent autonomous compute infrastructure of PowerEdge servers features iDRAC (integrated Dell Remote Access Controller) and OpenManage Enterprise. This helps customers tame the complexity of their IT infrastructure by automating

the entire server management lifecycle, in addition to comprehensive monitoring of health status, statistics, connectivity, and system performance utilization.

In addition, proactive resilience is built into each PowerEdge server by design to protect, detect, and recover from cyberattacks—ensuring security from build to delivery to retirement.

Based on these three pillars, PowerEdge servers are designed to address customers' most challenging workloads, working autonomously and collaboratively across all of their IT environments.

PowerEdge hardware

The Dell PowerEdge product line offers third- and fourth-generation Intel Xeon scalable processors and are built for challenging environments, including energy, manufacturing, telecommunications, and retail. Some of the available configurations are ruggedized, MIL-STD, NEBS, and marine compliant. More configurations offer a full-featured enterprise server, designed to optimize and deliver outstanding performance for the most demanding workloads. Each server node includes the following technology:

- Single and dual Intel Xeon scalable Gen 3 and Gen 4 processors, with up to 56 cores per processor
- Memory capacity ranging from 128 GB to 8 TB per node, depending on the model
- A PCIe SAS disk drive controller supporting 12 GB SAS speeds, if applicable
- A mirrored pair of BOSS SATA M.2 cards used to boot VMware ESXi on the node
  - BOSS cards are not included in the IEC 61850-3 certified XR12 configuration for substations.
- Dual or quad 10 GbE or 25 GbE Network Daughter Cards (10 GbE can autonegotiate to 1 GbE)

A brief overview of each PowerEdge platform discussed in this solution is provided in the following sections. For more information, see the Dell Servers page.

Dell PowerEdge XR12

The Dell PowerEdge XR12 is recommended for processing and analyzing data locally at the edge. It offers third-generation Intel Xeon scalable processors and is built for challenging environments, including manufacturing, telecommunications, and energy. The XR12 is a ruggedized MIL-STD, NEBS, and marine compliant single-socket 2U server with support for up to two GPU cards.

Figure 3. Dell PowerEdge XR12

Dell PowerEdge R660

The Dell PowerEdge R660 is a 1U, dual-CPU rackmount server based on Intel's fourth-generation Xeon processors. Its robust performance and reliability make it well suited for a variety of workloads, including general purpose compute needs in energy control centers. It offers a range of configurations to cater to different performance requirements.

Figure 4. Dell PowerEdge R660

Dell PowerEdge R760

The Dell PowerEdge R760 is 2U rackmount server supporting two 4th generation Intel Xeon processors and up to 24 NVMe drives. The R760's extra height allows for additional storage options and offers two additional PCIe slots. It is intended for use as general purpose compute in energy control centers.

Figure 5. Dell PowerEdge R760

VMware Edge Compute Stack

This Dell Validated Design for Energy Edge is intended for use with VMware's Edge Compute Stack (ECS). VMware ECS provides a set of tools and technologies that enable a resilient, reliable, and cost-effective application runtime environment at the edge of the network, closer to the devices generating the data. This approach helps to reduce latency, bandwidth usage, and dependency on centralized data centers, making it especially beneficial for applications that require real-time data processing and low-latency response times.

VMware ECS is built on the foundational VMware vSphere hyper-converged infrastructure (HCI) technologies and provides a fully integrated edge platform. This validated design is built on the following core VMware technologies:

- vCenter for central management of the vSphere environment used to manage data center and edge hosts.
- vSphere and ESXi virtualization platform that abstracts computing, storage, and networking on server hosts.
- vSAN software-defined enterprise storage that is fully integrated with vSphere. vSAN aggregates data storage devices to create a single storage pool shared across all edge hosts in a cluster.
- vSphere HA and Distributed Resource Scheduler (DRS) to provide compute and storage high availability.

NOTE: For additional information about VMware ECS, see the Edge Compute Stack Introduction and Overview.

Gateways

Industrial gateways, deployed in Purdue model levels 0 through 2 of a facility, allow various factory devices and industrial protocols to communicate with the rest of the network. This communication is accomplished with software that interfaces with protocols. Industrial gateways differ from standard PCs or servers in that they are ruggedized to handle harsh environments.

NOTE: For more information about Dell Edge Gateway 3200 and 5200 systems, see Gateways.

IEDs and controllers

IEDs and other industrial devices are an integral source for edge data in the electrical utilities space. They track and control substation operations and provide vital information to understand the location's current status. With the current evolution of artificial intelligence (AI) and machine learning (ML), it is beneficial to obtain, aggregate, and then analyze this data to provide operational insights and optimization.

Dell Validated Design ISV application stack

The ISV application stack that is detailed in the following table runs on various Dell servers and operating systems running Windows or Linux.

Table 1. ISV application stack

Software component	Product
Operating systems	Windows Server 2019
	Windows 10 LTSC 2019
	Ubuntu 22.04
ABB	ZEE600 Editor
	ZEE600 Runtime (server and client)
Forescout	eyeInspect Sensor (Active and Passive)
	eyeInspect Command Center

The interactions of these applications can be seen in the DVD for Energy Edge detailed application and hardware architecture figure.

ABB applications

ZEE600 Editor

The ZEE600 Editor is the configuration software to build and compile Runtime projects. All devices, connections, tags, logic, and screens are configured with the Editor. The project components are compiled, and the resulting files are sent to the Runtime host machine for use in operations.

ZEE600 Runtime

The ZEE600 Runtime is where the substation device connections are made, automation is executed, and dashboards are hosted. The Runtime supports a client-server model, where the server hosts all the primary functions and hosts client connections so that multiple users can interface with the application.

Forescout applications

eyeInspect Sensor

Forescout eyeInspect incorporates a passive sensor as its primary data ingestion approach. This sensor is strategically positioned within the substation alongside assets. By configuring port mirroring on one of its interfaces, the sensor can be connected to a core switch that links to a significant portion of the substation assets. This strategic setup ensures that the sensor captures a significant portion of network traffic for comprehensive analysis.

eyeInspect Command Center

The eyeInspect Command Center serves as a visual representation of sensor-acquired data. This platform allows users to access all the information about substation assets obtained from the sensor, including fundamental details like MAC address, vendor type, OS, and IP address. Because eyeInspect is tailored for OT environments, the Command Center is equipped with a variety of tools to display and provide insight into the vulnerabilities, risks, and threats within your substation. While the software is pre-built with security-focused dashboards for monitoring and analysis, it also offers the flexibility to delve into more specific insights if needed.

Alerts and monitoring

ISV applications and VMware ECS offer an extensive set of configuration tools for alerts and monitoring. Various log levels can be configured for tracking events at the desired level of granularity. Simple Network Management Protocol (SNMP) traps can be configured to integrate with other network monitoring tools, such as Dell OpenManage.

Protocols

Communication protocols play an important role in the electrical utilities space to enable efficient and reliable data exchange between various IEDs, substation automation systems, and control centers. These protocols serve as a standardized messaging language that ensures seamless communication, allowing utilities to gather real-time data, monitor critical operations, and control switchgear in the substation.

These communication protocols range from legacy serial protocol Modbus RTU to more advanced DNP3, and finally to the modern IEC 61850 standard. This evolution of protocols enhanced the efficiency, reliability, and interoperability of systems in the electrical utilities space. This Dell Validated Design for Energy Edge supports integration of IEDs with the entire range of protocols. For further information on integration of IEDs with various protocols, see the System Design chapter.

3

System Design

Topics:

Overview

In this DVD for the Energy Edge, the ABB ZEE600 and the Forescout eyeInspect applications are deployed as virtual machines on Dell PowerEdge servers with VMware Edge Compute Stack (ECS). Low compute applications, such as the ZEE600 Runtime for Human Machine Interface (HMI) clients, are deployed on the Dell Edge Gateways.

The system design offers guidance on aspects of the solution such as platform, networking, security, and best practices based on the components within the solution. This chapter introduces considerations for a successful deployment of a solution for the energy edge. The following chapters provide more in-depth explanations for several topics covered here.

The considerations for the overall system design are broken out into hardware, software, networking, storage, high availability, and security aspects. Each section provides a high-level view of what needs to be planned and implemented to successfully deploy ISV applications. The sections also offer some insight into the various features of ECS that can be used to build an even more effective overall solution.

Hardware

The core hardware platforms discussed in this solution are Dell PowerEdge servers and Dell Edge Gateways. For in-depth detail on these platforms, see the Architecture chapter of this document.

VMware Edge Compute Stack overview

The VMware Edge Compute Stack (ECS) is comprised of the same functional components used in enterprise datacenters for years, now licensed and bundled in a smaller footprint for the edge. The core components and some of the value they provide are discussed in the following sections.

NOTE: For additional information about VMware ECS, see the VMware documentation, including the Edge Compute Stack Introduction and Overview.

vSphere and ESXi

- For more information about vSphere see the VMware vSphere product page.
- The ESXi hypervisor provides the ability to consolidate applications and virtual machines (VMs) onto shared hardware. It abstracts the physical hardware resources into pools, making them available for consumption and sharing among VMs.

vCenter

- vCenter provides centralized management of VMware ESXi hosts and clusters and enables various key features such as vMotion, Virtual Distributed Switches (vDS), vSAN, DRS, HA and many others.
- For more information about vCenter, see the VMware vCenter product page.

Features for 3-node configurations

The following features are relevant for the 3-node platform configurations, as described in the High availability overview section of this document.

vSAN

vSAN is integrated into the kernel of vSphere and provides the software-defined storage layer. A vSphere cluster is a collection of ESXi hosts configured to share resources. vSAN creates distributed shared storage by aggregating locally attached disks from the hosts that form the vSphere cluster. The following figure shows the vSAN high-level architecture:

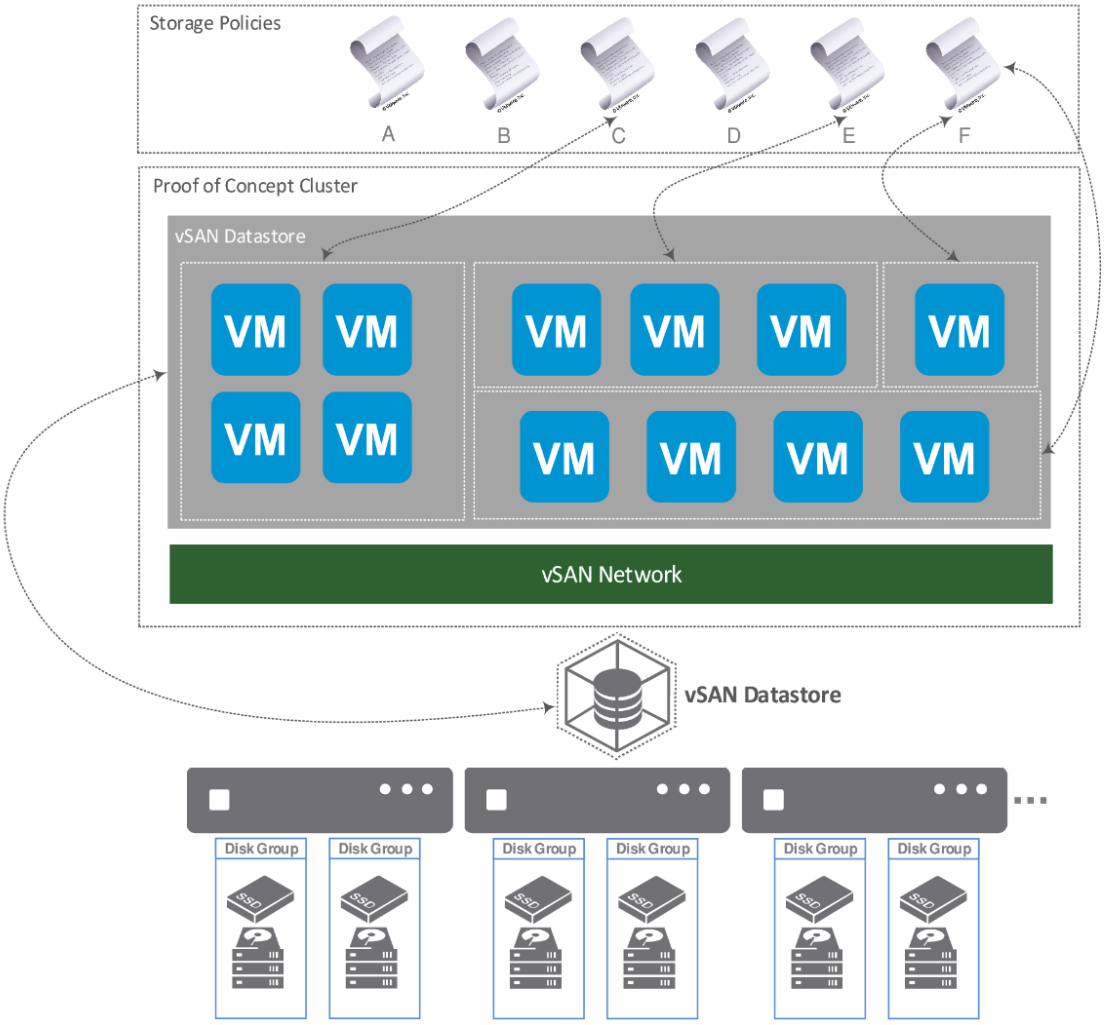


Figure 6. Developing a hyperconverged storage strategy

(Source: Developing a Hyper-Converged Storage Strategy)

NOTE: For more information about vSAN, see the VMware vSAN product page.

vMotion

- Provides the ability to perform live VM migrations:
  - Across ESXi hosts in the same (or different) clusters.
  - To separate vCenters or locations.
- Simplifies upgrades and maintenance by allowing VMs to move to and from servers during maintenance.
- For more information about vMotion see the VMware vMotion product page.

vSphere High Availability

- Policy-driven HA for virtual machines.
- Monitors ESXi hosts and clusters for various failure types and takes action (for example: restarts VMs on working hosts) if a failure occurs.
- For more information about HA, see How vSphere HA Works.

vSphere Distributed Resource Scheduler

- Leverages vMotion to automate and schedule VM migrations.
- Identifies optimal placement for a virtual machine within seconds.
- Policy-driven workload balancing can be tuned for equal distribution of workload across nodes in an ESXi cluster.
- For more information about Distributed Resource Scheduler (DRS), see the VMware Distributed Resource Scheduler product page.

Additional ECS components

Additional components not directly leveraged in this solution (but available as part of VMware) include:

- Tanzu Kubernetes—VMware's Kubernetes-related product suite
- Tanzu Mission Control—Centralized Kubernetes cluster management
- Edge Network Intelligence—AIOps solution for monitoring and analyzing various edge endpoints

Deployment models

The ISV applications in this Dell Validated Design can support multiple deployments and instances. CPU, memory, and storage requirements are determined based on the overall size and performance requirements of such deployments. Other factors to consider when deciding on the right deployment models for ISV applications for edge deployments are covered in detail in subsequent chapters.

High Availability and Disaster Recovery

The Dell Validated Design for Energy Edge encompasses VMs on VMware ECS with external data sources and devices that aggregate IoT traffic. High availability (HA) and disaster recovery (DR) leverage the VMware suite of tools and features to ensure the reliability and resilience of your edge infrastructure. Here are some design choices tailored to the VMware edge computing system:

- VMware vSphere High Availability—Enable vSphere HA on edge nodes to automatically restart virtual machines (VMs) on another host in the cluster if the original host fails, helping to minimize downtime.
- VMware vSphere Fault Tolerance (FT)—Consider using FT for critical VMs which creates a live shadow instance of a VM on a separate host, providing continuous availability in case the primary VM becomes unavailable.
- vSphere Distributed Resource Scheduler (DRS)—Enable DRS to automatically balance VM workloads across multiple edge hosts. This helps ensure optimal resource utilization and reduces the risk of performance bottlenecks.
- vSphere vMotion—Leverage vMotion to move VMs between edge hosts without disruption. This is useful for planned maintenance, load balancing, and improving overall system resilience.
- VMware vSAN (software-defined storage)—Deploy vSAN to provide highly available and resilient storage for your edge VMs. vSAN replicates VM data across multiple edge nodes, ensuring data integrity and availability.

- Rapid recovery mechanisms—For disaster recovery scenarios, enable application or VM backups for rapid recovery of services and data, minimizing downtime and data loss.
- Edge security—Ensure proper system hardening, adequate virus protection, and be certain that the necessary network and OS level securities are in place to prevent systems from malicious attacks or intrusions.
- Regular testing and maintenance—Conduct regular tests, failover drills, and maintenance activities to validate the effectiveness of the HA and DR design and identify areas for improvement.

NOTE: For more information, see the High Availability and Disaster Recovery chapter.

Latencies and throughput

The substation automation and SCADA systems should have very low latencies to address real-time monitoring and control of electrical substation assets and operations. Depending on the size of the substation, determined by factors such as number of bays, intelligent electronic devices (IEDs), and tags, the virtual machines in the solution should be assigned an appropriate set of compute, storage, and network resources to meet the latency and throughput requirements. Consider leveraging more CPU cores, higher memory, and high-performance storage for large deployments, as compared to medium or low deployments. See the Sizing and Scaling Guidance chapter for further information.

Industrial gateways have limited resources compared to VMs deployed on PowerEdge servers. Also, they may not have access to persistent resources locally. Hence, gateways can be leveraged to run low compute applications such as the ABB ZEE600 Runtime (HMI) clients.

IT and OT convergence

Information Technology (IT) and Operations Technology (OT) exist in two separate worlds, serving two distinct purposes. IT consists of computing systems for the processing and storage of data, while OT focuses on the hardware and software running and monitoring production systems – such as substation automation, SCADA (Supervisory Control and Data Acquisition), and Historians. Systems in the OT domain communicate with one or more intelligent electronic devices (IEDs), using their own bearers and protocols (for example, industrial or utilities protocols), and in turn they transmit data to a centralized control center.

The substation automation and SCADA systems that enable end-to-end solutions can be deployed in a virtual environment at electrical substations. The rise of edge computing and virtualization is accelerating this convergence.

The OT benefits from this integration with a more efficient, scalable, managed, and secured infrastructure onto which numerous applications are layered. These applications include substation automation and SCADA, as well as new cybersecurity asset visibility and threat detection applications. Benefits on the IT side include secure real-time communication with the enterprise's assets while retaining the requisite efficiency for creating, scaling, maintaining, and securing the infrastructure.

While allowing flexibility to both IT and OT management, the Dell Validated Design for Energy Edge offers a converged platform that provides service level management controls and governance for both IT and OT services.

Networking

This section introduces the various aspects of networking components to consider for an effective deployment of the system. It references the Dell VxRail Network Planning Guide, although VxRail is not discussed in this solution, as many of the networking concepts apply. This section covers best practices, recommendations, and requirements for both physical and virtual network environments

Top-of-Rack switches

A PowerEdge XR12 node (or cluster) running ESXi depends on adjacent physical switches, usually a Top-of-Rack (ToR) switch, to enable connectivity. In a typical configuration, the NICs on the XR12 nodes uplink to a pair of ToR switches. XR12 nodes can attach to any compatible network infrastructure using the four embedded LAN on motherboard (LOM) ports (25 GbE SFP+) or optional additional NICs with 1/10/25 GbE speeds with the option of SFP28 and BASE-T configurations. It is recommended in production environments to deploy dual ToR switches to avoid having a single point of failure. Layer 2 and Layer 3 connections are supported.

Consider switch performance and capabilities when selecting the best ToR switch solution. See the following section for details on common cabling and configuration.

vSphere networking

VMware networking centers on virtual switches. The preferred method is to use a virtual distributed switch (vDS), which can be shared among ESXi hosts and managed by a vCenter. The alternative is a virtual standard switch (vSwitch). However, a vSwitch is limited to a single ESXi host and typically only used when a vCenter is not available. Since VMware ECS includes vCenter, the focus here is on using a vDS. The design and configuration is similar with either option.

For the ESXi host (or cluster, in a multi-node configuration) to function, the following requirements must be followed. Configure critical infrastructure pieces such as DNS (Domain Name Server) and NTP (Network Time Protocol). These settings can be modified using vCenter for each ESXi host.

Designate Virtual LAN (VLAN) IDs in your network to be assigned to the networks. Each of these networks will be assigned to a port group on the vDS. The External Management network must be able to route to DNS and NTP services to provide communication between ESXi nodes and vCenter.

Some example port groups and VLANs that are commonly deployed are:

- External management (ESXi)
- Guest VM networks
- vSAN (for 3-node HA configurations)
- vMotion (for 3-node HA configurations)
- Server Out-of-Band (iDRAC)

A common configuration is to use two NICs and configure each of these port groups to use both uplinks, as shown in the following figure.

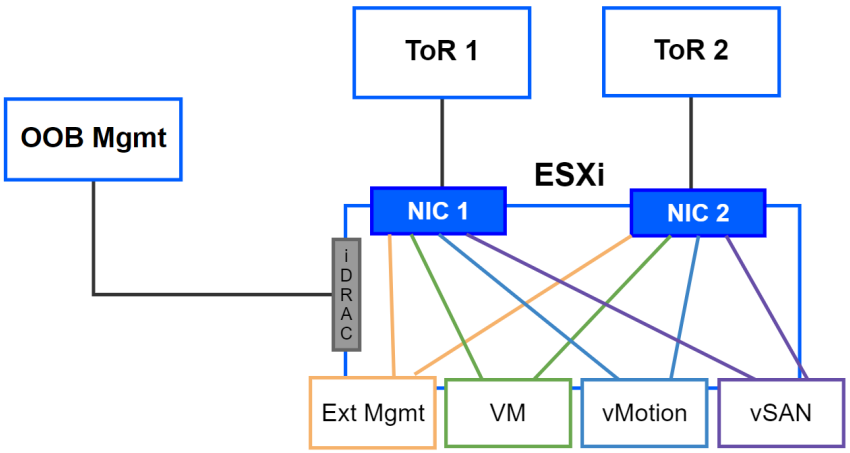


Figure 7. Two NICs configuration

Another common configuration is to use four NICs and separate management traffic from higher-bandwidth port groups such as vSAN and vMotion, as shown in the following figure.

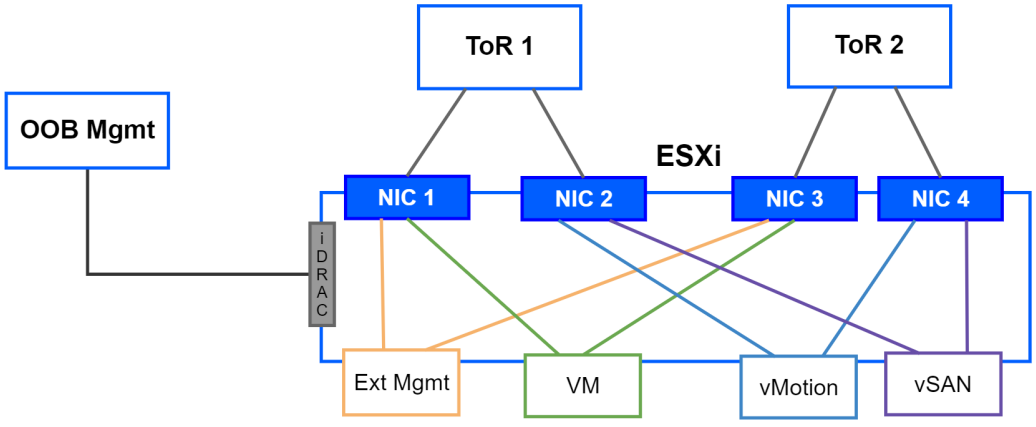


Figure 8. Four NICs configuration

These examples are common working configurations. For other options and additional details, see the Edge Designs documentation from VMware.

Network redundancy

To support high availability, better performance, and failover for the network, there must be at least two ToR switches deployed with a pair of cables connecting the switches. Additionally, configure link aggregation to enable features such as load balancing and failure protection. vSphere supports NIC teaming, which is a physical pairing of ports on the node. For network-intense workloads that require high availability, choose switches that support multi-chassis link aggregation, such as a virtual link trunking (VLT) port channel from Dell. vSphere also includes Link Aggregation Control Protocol (LACP) at the cluster level. The switches that support the ESXi host or cluster should support LACP for better manageability and broad load-balancing options.

For more information, see the High Availability and Disaster Recovery chapter.

Parallel Redundancy Protocol

Parallel Redundancy Protocol (PRP) is a standard for the high availability of Ethernet networks (IEC 62439-3 Clause 4). It provides seamless failover against failure of any network component.

Every PRP node has two network interfaces that are connected to two parallel networks of similar topology. Every sender on a PRP network sends duplicate Ethernet frames on both parallel networks. Every receiver on a PRP network accepts the first Ethernet frame and discards the second frames.

There are notable advantages of PRP over standard Ethernet:

- The redundancy is invisible to the application.
- There is zero down time or recovery time in the event of any single point of failure of any network component.
- PRP is suited for applications that require very short switchover time, such as protection and automation in electrical substations. For such applications, the recovery time of other commonly used Ethernet redundancy mechanisms (such as the Rapid Spanning Tree Protocol (RSTP), Linux NIC bonding, or Microsoft NIC teaming) is too long.

A PCIe-based PRP card or an external PRP Redundancy Box (RedBox) can be utilized with PowerEdge XR12 servers to add dual Ethernet interfaces with PRP capability. Similarly, an external RedBox can be utilized with Dell Edge Gateways to add PRP capability.

The following figure provides guidance on implementation of a PRP network with PowerEdge servers and Dell Edge Gateways.

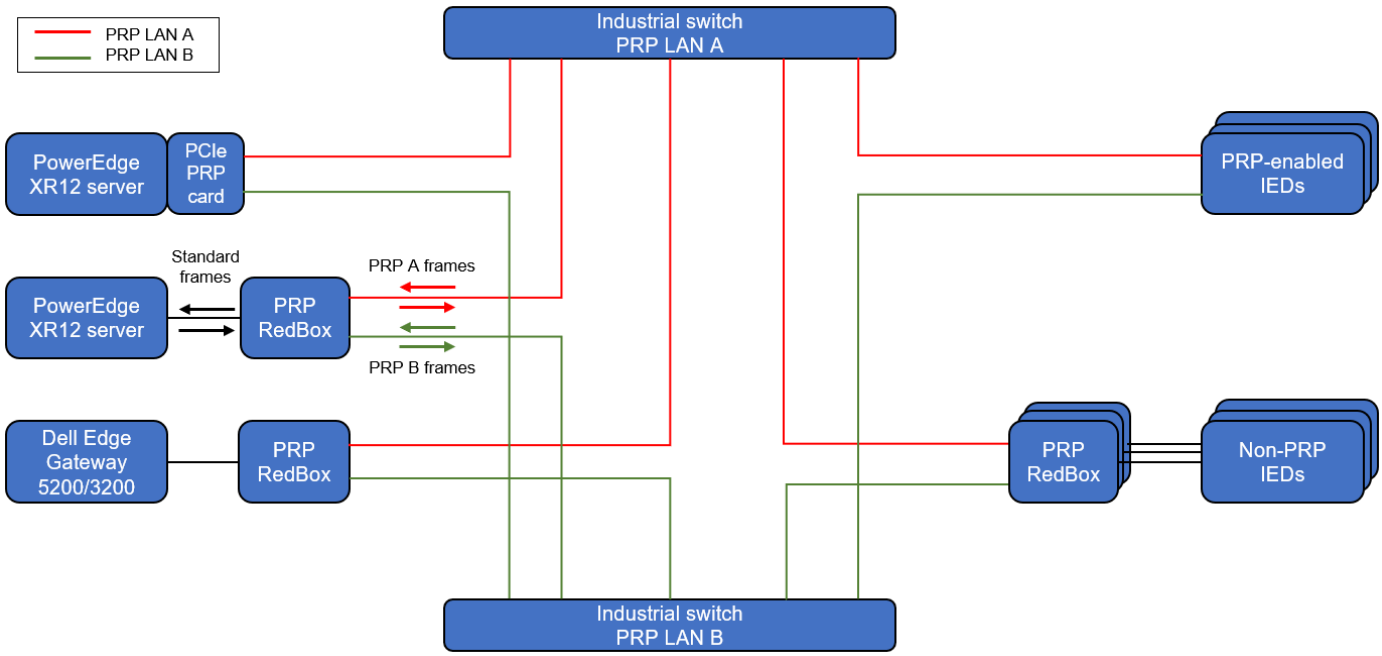


Figure 9. Parallel Redundancy Protocol

OT and IT protocols

It is important to recognize the common ports and protocols that are used in an industrial network. This helps to identify what should be seen and not seen within the network. Some of the industrial protocols inherently lack security features and can be susceptible to cyberattacks. Reduce risk by using segmentation to establish boundaries for the different protocols.

NOTE: See the ZEE600 Drivers documentation for the list of all protocols supported by the ZEE600.

The following table provides the common OT protocols used in the solution.

Table 2. OT protocols

Protocol	Ports
Modbus TCP	TCP/502
Modbus RTU	Serial
DNP3	TCP/20000, UDP/20000
DNP3 Serial	Serial
IEC 61850 MMS	TCP/102
IEC 61850 GOOSE	Ethernet EtherType/0x88B8
IEC 60870-5-101	Serial
IEC 60870-5-104	TCP/2404
IEC 60870-5-103	Serial
OPC UA	TCP/135, 4840, 4843, 40831, 49320

The following table lists the IT protocols and open ports used in this solution.

Table 3. IT protocols and open ports

Description	Source devices	Destination devices	Protocol	Ports
DNS	Host ESXi management interface, Dell iDRAC, VMware vCenter servers	DNS servers	UDP	53
NTP client	Host ESXi management interface, Dell iDRAC, VMware vCenter servers	NTP servers	UDP	123
Precision Time Protocol (PTP)	PTP grandmaster, master, or boundary clocks	PTP grandmaster, master, or boundary clocks	Ethernet	EtherType/ 0x88F7
Parallel Redundancy Protocol (PRP)	All doubly attached nodes (DAN) connected to PRP LAN A/B	All doubly attached nodes (DAN) connected to PRP LAN A/B	Ethernet	EtherType/ 0x88FB
Syslog	Host ESXi management interface, vRealize Log Insight	Syslog server	TCP	514
LDAP	VMware vCenter servers	LDAP server	TCP	389, 636
SMTP	SRS gateway VMs, vRealize Log Insight	SMTP servers	TCP	25
ESXi management	Administrators	Host ESXi management interface	TCP, UDP	902
Dell server management	Administrators	Dell iDRAC	TCP	623, 5900, 5901
SSH and SCP	Administrators	Host ESXi management, vCenter Server Appliance, Dell iDRAC port	TCP	22

Table 3. IT protocols and open ports (continued)

Description	Source devices	Destination devices	Protocol	Ports
Managed hosts to vCenter	Host ESXi management	vCenter server	TCP	443, 902, 5988,5989, 6500, 8000, 8001
Managed hosts to vCenter heartbeat	Host ESXi management	vCenter server	UDP	902

The ABB ZEE600 application opens various ports depending upon the use cases and the configuration. See Free ports under **Runtime** in the online help pages.

For the ports used by the Forescout eyeInspect application, see the DMZ firewall rules for Forescout table in the Cybersecurity chapter.

Security

It is imperative to consider security prior to implementation. Doing so ensures that all the pieces are in place to quickly and effectively implement cybersecurity as part of your industrial system architecture.

The Cybersecurity chapter covers the following topics:

- Industry standards—Leveraging guidelines provided by IEC 62443 and IEC 62351 standards to define and recommend security best practices for cybersecurity in energy and utility industrial systems.
- Platform security overview and considerations—The PowerEdge XR12 is well-suited for environments like substations, equipped with inherent cyber resilience to counter prevailing cybersecurity challenges. Additionally, key VMWare and vSAN factors that enhance the effectiveness and security of the deployment and lifecycle are discussed.
- OS security considerations—Recommended strategies to secure the host OS used by each ISV.
- Application-specific hardening guidance and validation—Validated test cases for implementing application hardening for each ISV. Focuses on key security areas such as authentication, authorization, confidentiality, integrity, accounting, and availability.
- Secure architecture implementation—Validation and implementation guidance on deploying the ISV application securely into an existing or new solution deployment. Provides validated firewall rules and details on secure routing between control center and substations using virtual private network (VPN) tunneling.

ABB ZEE600 system design

ZEE600 from ABB provides the substation HMI and automation systems, which connect the IEDs and devices within the substation as well as the offsite control center. This section examines the following aspects of system design related to ZEE600:

- ZEE600 components
- Use cases
- Substation edge deployment
- ZEE600 features

ABB ZEE600 refers to zenon Energy Edition (ZEE), which is built on COPA-DATA's zenon product suite. Throughout this documentation, the term ZEE600 includes both the underlying zenon functionality and ABB's augmented energy feature set.

ZEE600 components

The primary components of the ZEE600 software package are the Editor, which is used to create customized runtimes, and the Runtime, which is deployed on the wanted machine. Once deployed as a server, that same runtime can also be used to set up clients on other machines. There is also a set of tools that are included with ZEE600 that help manage, expand, or troubleshoot the deployment.

The following figure shows the components and features of ZEE600.

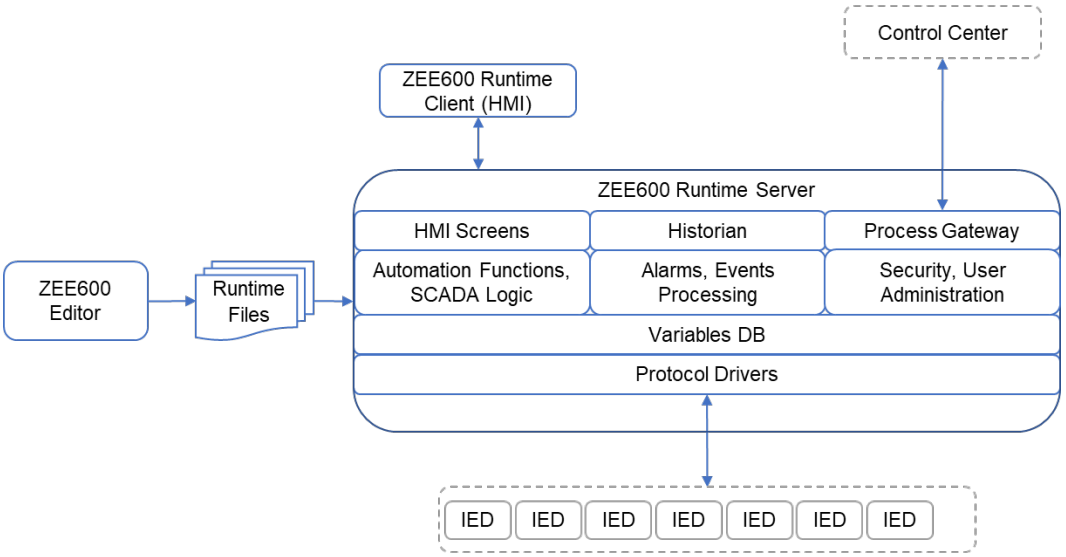


Figure 10. ZEE600 components and features

ZEE600 Editor

The Editor is used to configure a runtime for a specific substation. It is organized by Workspaces, which are a collection of projects the developer is working on. This workspace typically has an active project, which is the one being edited, and a start project, which is the project that starts when the run button is pressed. Projects can also be loaded from memory to view and edit them or unloaded from memory to free up resources.

The projects are composed of various components, such as drivers, variables, screens, and SCADA Logic. These components are covered in more detail later in this chapter and in subsequent chapters. These components can be edited, combined, exported, and imported to build the fully customized runtime.

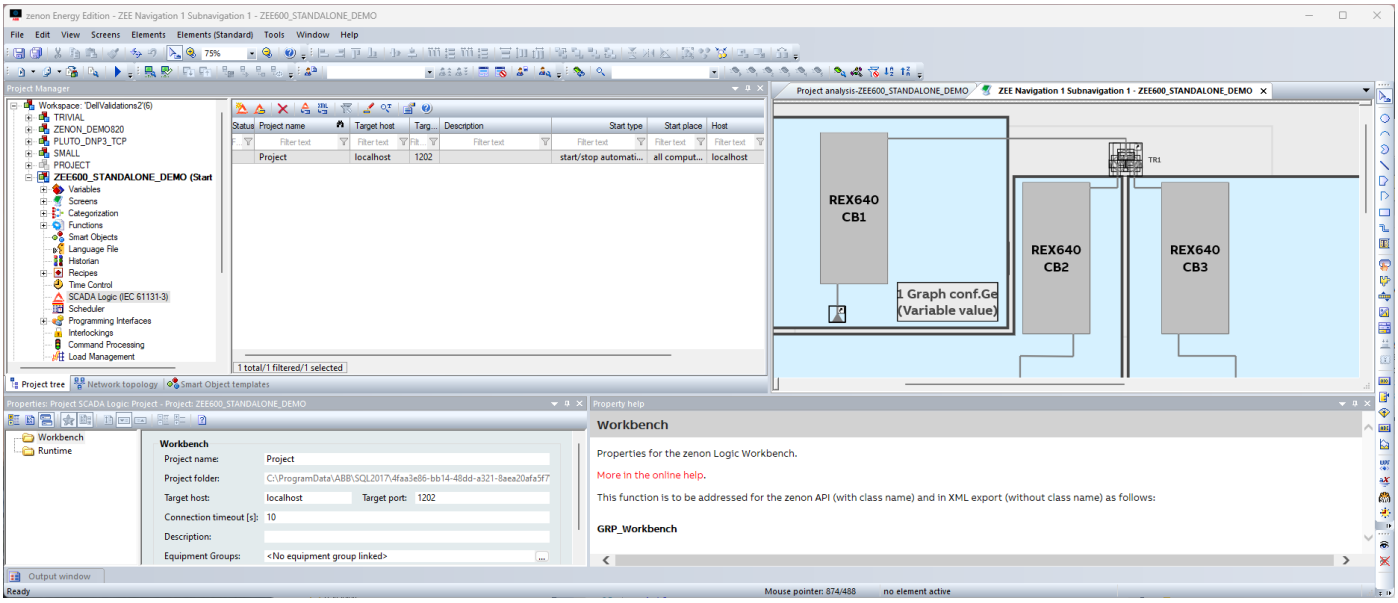


Figure 11. ZEE600 Editor

ZEE600 Runtime

The Runtime is the compiled project that is created with the Editor. It is a collection of all the files that are required to run the application on a given machine. The Runtime includes data ingestion from IEDS and other devices, automation and SCADA logic, dashboard navigation and visualizations, related security and administration, and the functionality to auto-launch additional components, like process gateways. Once created, it can be deployed on the required machine without the Editor or deployed remotely using the Editor.

Supplementary tools

Some of the supplementary tools that are used in the validation are shown in the following table.

Table 4. Supplementary tools

Tool	Use
Startup Tool	Launch all the other applications bundled with ZEE600.
License Manager	Add or release licenses and monitor the existing license configuration.
Diagviewer	View and search through logs.
Redundancy Management Tool	Configure redundant servers.
Process Gateway	Run a tool or application independently of the Runtime - can be configured to run automatically with the Runtime.

Application versions

The following application versions were used in validation, unless otherwise noted:

- ABB ZEE600 v2.0.1, containing:
  - zenon Startup Tool v8.20
  - zenon Editor v8.20
  - zenon Runtime v8.20
  - zenon Process Gateway v8.20

Use cases

A substation automation platform like ZEE600 plays a crucial role in electrical substations. It uses communication protocols and advanced automation applications to enhance substation monitoring and control operations.

The following are some use cases for ZEE600:

- Data aggregator—Collects measured values and state data from multiple downstream IEDs, such as protection relays, meters, and bay control units, using serial or TCP/IP-based communication protocols.
- Substation SCADA—Provides a local SCADA system in a substation, with features like HMI screens, Single Line Diagrams, a historian, reports, and alarms/events processing.
- Protocol gateway—Acts as a protocol gateway to send substation data to Advance Distribution Management System (ADMS) or Energy Management System (EMS) located in electrical utilities' control centers.
- Substation automation—Provides advanced automation features like interlocking, scheduler, and IEC 61131-3 programming. Utility customers can use these features to build customized automation applications that cater to their specific needs.

Substation edge deployment

This section discusses the deployment of ZEE600 components in a substation. All ZEE600 components are deployable on Windows machines-virtual machines for those components that are hosted on the virtualized VMware platform on PowerEdge XR12 servers and bare metal for those components that are hosted on the 3200 and 5200 Dell Edge Gateways.

Editor deployment

The Editor application is typically installed on an engineering workstation running Windows. This application only requires a network connection to the edge deployment when pushing changes to the Runtime files.

Runtime deployment

In this Dell Validated Design for Energy Edge, the customized ZEE600 Runtime is deployed to a VMware virtual machine running Windows 10 on an IEC 61850-3-certified Dell PowerEdge XR12 server at the substation.

ABB provides an easy-to-use installer application. The ZEE600 applications are easily selectable in the installer interface. For the distributed deployment used in this DVD, only the Runtime should be installed on the Dell PowerEdge XR12 virtual machine.

Deploying a project to the ABB Runtime

This Runtime is compiled in the Editor and can be pushed to the Runtime machine in two different ways:

1. The project files can be copied from the Editor host machine and placed on the Runtime VM.
2. The Runtime files can be pushed to the Runtime host from the Editor host over a secure network connection using the integrated Remote Transfer functionality. This allows a single user on the Editor machine to quickly make changes and push the updates to multiple runtime hosts with just a few clicks, eliminating the need to connect and log in to each Runtime host.

Runtime server

The ABB ZEE600 Runtime supports a client/server configuration, where IED connections and substation automation can be hosted on the Runtime server, and the HMI made available to operators can be viewed using the client machine.

This model provides flexibility on how the physical and digital security of devices is managed, how the respective workloads are distributed, and how HA/DR functionality is configured.

Runtime client

Other computers on the same network as the Runtime server can act as clients. While all devices, data, automation, and screens are hosted on the server, the client can host the interface used by operators and technicians.

Licensing

Every machine running an ABB ZEE600 component must have the appropriate license to gain the full functional value of the application. Demo mode is available prior to the activation of a license.

Licenses can be deployed to a host machine using either a hardware dongle that is attached to the host hardware or a software-based key that is added to the License Manager software on the machine. The activation of a license can be either online (see Online activation) or offline (see Offline activation), depending on the needs of the specific deployment.

Special consideration should be given to licensing Virtual machines—hardware dongles require a passthrough from the physical host to the VM, while software keys are tied to specific details of the host VM. Changing the VM, such as altering the computer resources, adding or removing network interfaces, or migrating the VM to a new host causes the software-based license to be invalidated. Therefore, software licenses should be returned using the License Manager prior to making any changes and then reactivated once the updates are complete. It is recommended to use the network licensing for virtual machines. For more information about this, see the Network dongles documentation.

For further details on licensing options and considerations, see Licensing.

NOTE: For information about USB passthrough in VMware, see Add USB Devices from an ESXi Host to a Virtual Machine.

ZEE600 features

Variables

Variables, also called process variables or data points, are the interface between a data source (IED, PLC, field bus, and so on) and the ZEE600. They represent certain measured values (line voltages, currents, frequency, and so on) or states of the field devices (circuit breaker, switch, and so on).

Variables can have many properties, including the specific address used by the driver, calculations for scaling, and limits. The following figure shows examples of ZEE600 variables and their typical properties.

Once a variable is defined and attached to a driver, it is available to other features of ZEE600 (HMI screens, functions, process gateways, and so on).

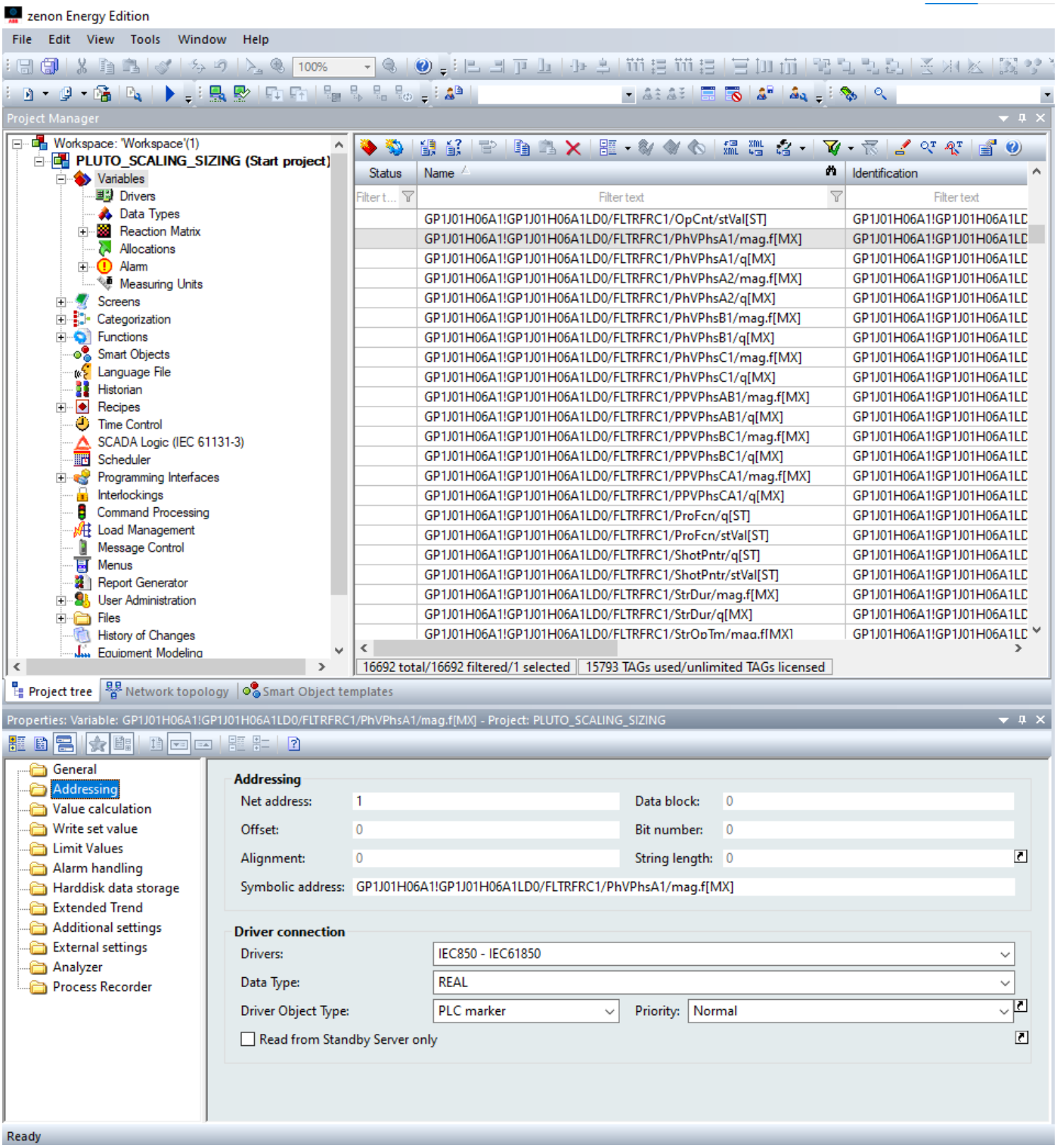


Figure 12. Example ZEE600 variables and their properties

Protocol drivers

A protocol driver establishes connection between an IED and ZEE600, and then fetches measured values and states. Each protocol driver implements a specific communications protocol in client mode. ZEE600 provides drivers for common protocols that are used in the energy industry, including DNP3, Modbus RTU and TCP/IP, IEC 61850, IEC 60870-5-101, IEC 60870-5-103, and IEC 60870-5-104.

The following steps are typically used to integrate an IED with ZEE600:

1. Create a driver and add the IED connection details. Configure its settings, like Serial Port, Baud Rate (for serial protocols) or IP Address of the IED, TCP port number (for network protocols).
2. Create variables for measured values and states available in the IED. Configure properties of the variables like driver addressing, datatype, scaling, and limits.
3. Map variables to HMI screens, functions, and process gateways.

See Variables in the ZEE600 manual for further details on configuring an IED connection in a protocol driver.

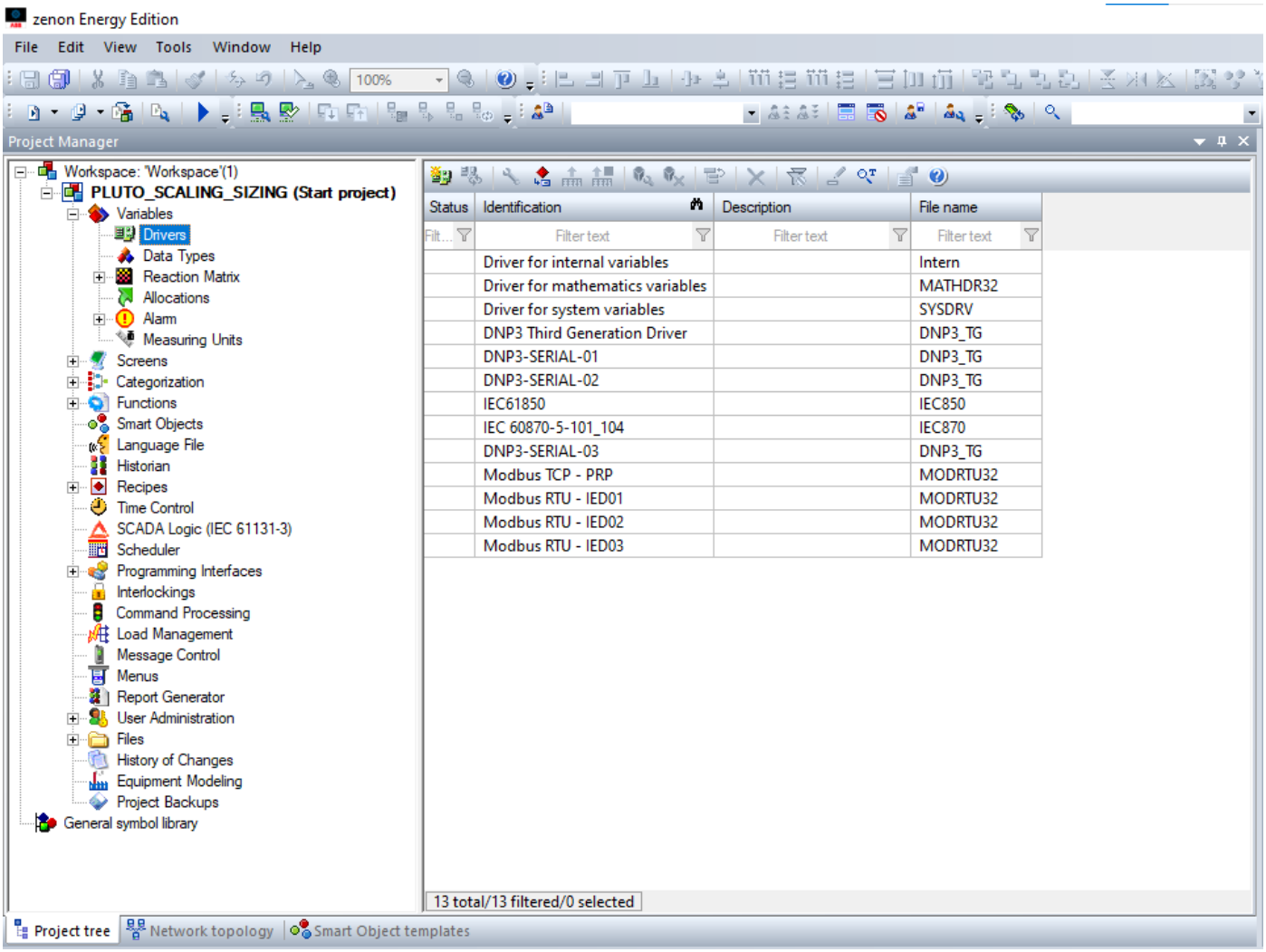


Figure 13. Example ZEE600 project with multiple protocol drivers

The following table lists the common protocol drivers that are used in the energy industry, and it includes links to driver manuals and integration strategies.

Table 5. Common protocol drivers in ZEE600

Protocol driver	Interface type	Driver manual	Recommended tools/Wizards for efficient integration of IEDs
Modbus/RTU	Serial	Link	• Use the Variable creation wizard to create multiple variables for a driver. • Use the CSV import tool to create multiple variables for a driver. • Use the XML import tool to export driver variables from one project and import into another.
Modbus/TCP	Network	Link	• Use the Variable creation wizard to create multiple variables for a driver.

Table 5. Common protocol drivers in ZEE600 (continued)

Protocol driver	Interface type	Driver manual	Recommended tools/Wizards for efficient integration of IEDs
			• Use the CSV import tool to create multiple variables for a driver. • Use the XML import tool to export driver variables from one project and import into another.
DNP3 Serial	Serial	Link	• Use the Online import steps to acquire variable information from an online IED and then add multiple variables. • Use the XML import tool to export driver variables from one project and import into another.
DNP3 TCP/UDP	Network	Link	• Use the Online import steps to acquire variable information from an online IED and then add multiple variables. • Use the XML import tool to export driver variables from one project and import into another.
IEC 60870-5-101	Serial	Link	• Use the Online import steps to acquire variable information from an online IED and then add multiple variables. • Use the XML import tool to export driver variables from one project and import into another.
IEC 60870-5-103	Serial	Link	• Use the XML import tool to export driver variables from one project and import into another.
IEC 60870-5-104	Network	Link	• Use the Online import steps to acquire variable information from an online IED and then add multiple variables. • Use the XML import tool to export driver variables from one project and import into another.
IEC 61850	Network	Link	• Use the IEC850 Driver Configuration Wizard to configure driver connections, RCB, Datasets, and variables, by importing an IEC 61850-6 SCL file (SCD, SSD, CID, and ICD). • Use the Online import steps to acquire variable information from an online IED and then add multiple variables. • Use the IEC 61850 SSD Import Wizard to create Single Line Diagram and other screens from the SSD project file.

NOTE: See the ZEE600 Drivers documentation for the list of all protocol drivers supported by ZEE600.

Process gateway

The process gateway in ZEE600 serves as a protocol server to higher-level systems, such as an ADMS or EMS in a control center. It mainly provides two use cases:

- Process data from ZEE600 Runtime can be forwarded to higher-level systems.
- Higher-level systems can write values or commands to the ZEE600 Runtime.

ZEE600 supports most protocol servers that are used in the energy industry: Modbus, DNP3, IEC 60870-5-101/104, OPC UA, and more. Furthermore, process gateways can be used to configure a syslog connection for central logging. For more information, see the Cybersecurity chapter.

The process gateway is intended as an add-on in the ZEE600 Runtime, and it maps variables from the Runtime by variable names in a project. Several process gateways can be started on one Runtime computer or virtual machine.

The following steps are typically required to configure a process gateway:

1. Module selection—In the first stage of configuration, select the module for the server protocol. The following figure shows the list of available protocol server modules.
2. Module-specific—Depending on the selected module, configure connection parameters and variable assignments.
3. Autostart—Create a function to start the process gateway and configure a script (like the prebuilt AUTOSTART script) to run the function on Runtime startup or on another automated condition.

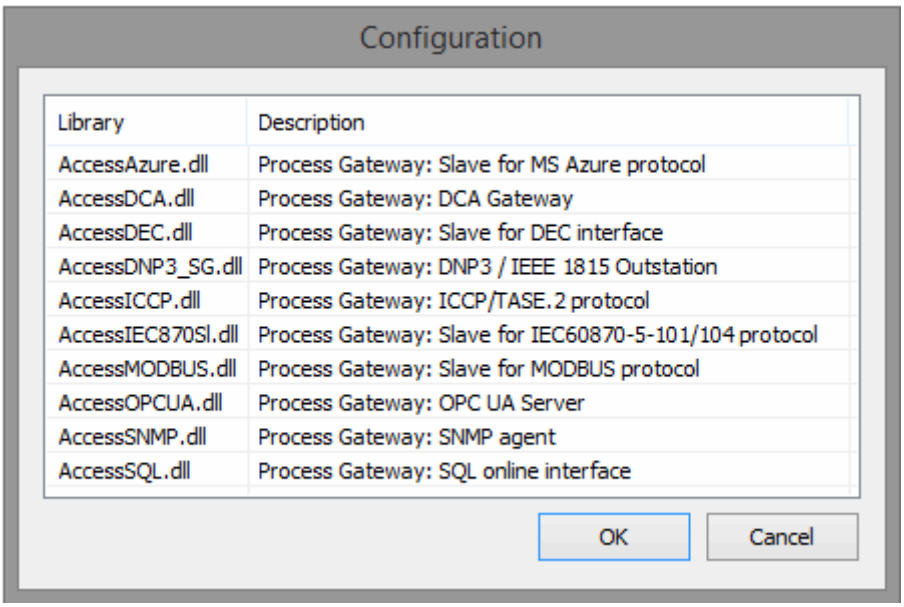


Figure 14. Process Gateway protocol modules

See the Process Gateway manual for the configuration details of the Process Gateway modules.

HMI features

Screens

The HMI is created by populating screens with the wanted elements. There are many basic elements available from the element toolbar, and those elements can be combined into symbols for reuse. Each element also has a list of properties, which are used to customize the element and link them to specific variables.

When building a ZEE600 project using the ABB ZEE600 Template Wizard, many screens and navigation interfaces are preconfigured to make customization quick and easy. A user login interface, alarm screen, menu navigation, and single line diagram screens are among the screens immediately available.

Further customization and standardization of the HMI can be achieved by using frames, font lists, styles, and color palettes.

Functions

Most HMI logic is encapsulated with functions, such as what happens when a button is pressed or when a variable changes. HMI navigation and opening pop-ups are handled through these functions.

Functions also play an important role in developing standardized HMIs. By using the Screen Switch function and replacing links or index parameters, all the variable links on a page can be changed dynamically. Then a single page can be used for multiple devices.

Historian

Variables which need to be tracked over time are added to the historian and grouped based on where and when the data is recorded. Data can also be set to expire after a fixed amount of time so that storage space is not overused.

This historical data can be displayed on the screen through the Trend Element or processed through SCADA logic.

For more details on HMI configuration, see the ZEE600 Manual.

Substation automation features

SCADA logic

Advanced automation can be added to any runtime by creating a SCADA logic project within the overall project. Doing this adds an internal driver to the Variables section and opens the SCADA Logic editor as seen in the following figure. Programs are written in any of the IEC 61131-3 languages and can execute cyclically or periodically.

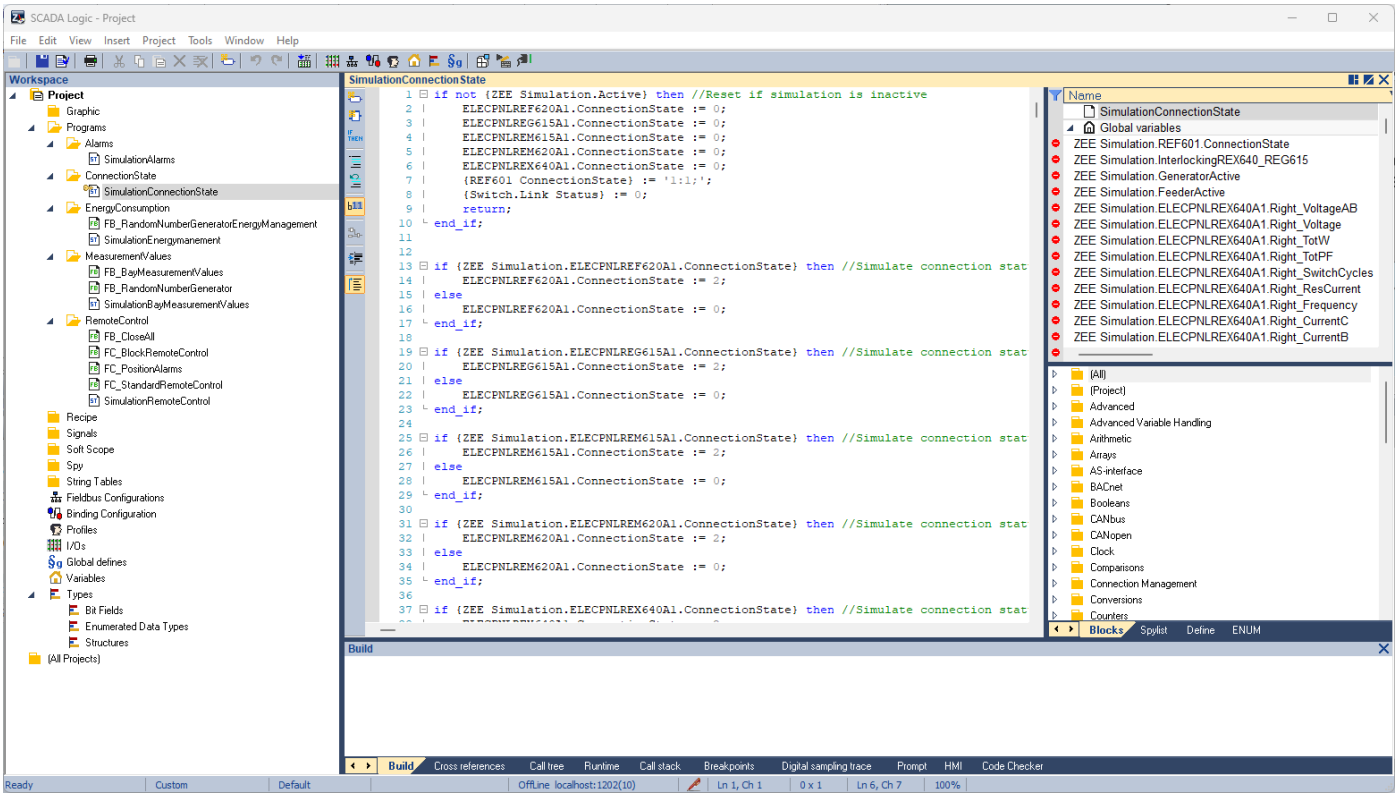


Figure 15. SCADA Logic editor window

By connecting to an active runtime, the SCADA Logic screen can be used to view the values of variables in real time and update the logic. This is useful while developing code and for troubleshooting.

This same interface is also available by creating a simulated driver as discussed in the Accelerated Time to Value chapter.

Command processing

The command processing component allows groups of variables to be connected for safe operation. This is an easier and more visible way to enforce intervariable logic than with a SCADA logic program and is most effective when combined with a Command Processing Screen (a template for this is already included in ZEE600 projects). For example, if a switch cannot be closed unless the *closed enable* variable is true, then this rule can be encapsulated in a command group. This supersedes any features in the HMI and reinforces safe operation.

Programming interfaces

All advanced programming, such as creating editor elements (wizards, graphics, and so on) are created in the programming interfaces option. This opens the VBA editor, or ideally Visual Studio with the appropriate add-on. By creating projects in VBA, the options to expand the functionality are limitless.

For further information about these and other available components, see the ZEE600 Manual.

Security features

ABB ZEE600 software has numerous security features available to secure data and restrict access to only authorized users.

Many of these security features are covered in detail in the Cybersecurity chapter.

User administration

This section of the Editor is where new users and user groups are created and configured. Users can be assigned authorization levels for security and organized into groups. Those groups can also be assigned authorization levels to make it easier to manage access for large numbers of users.

System design with Forescout

This section covers the overall system design for Forescout. This software platform supplies cybersecurity functionality, allowing visibility to assets and vulnerabilities of the assets in a substation. Forescout provides other applications which can be integrated with each other. Forescout eyeInspect was the focus of this validation. Topics include the overall functionality of this product, how to design and implement Forescout deployments, as well as functional use cases validated for eyeInspect.

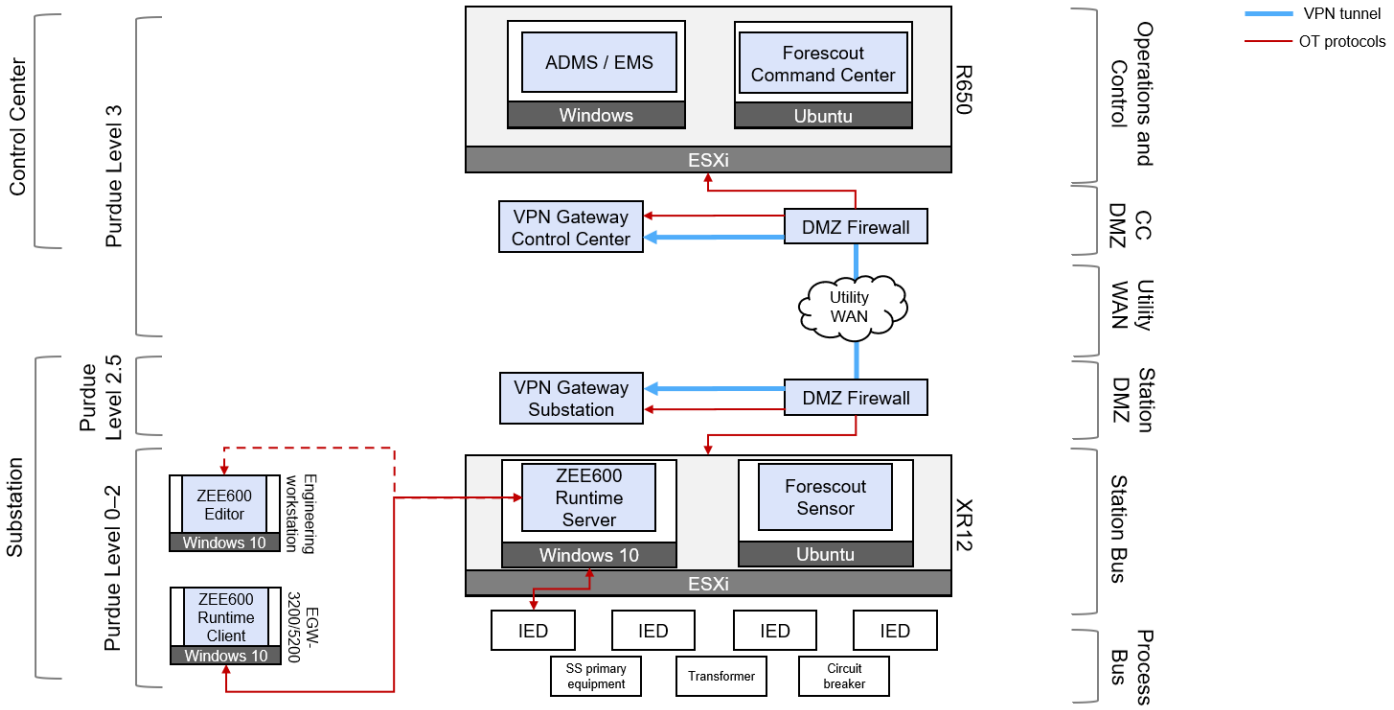


Figure 16. Validated architecture for secure communication in a substation and Control Center

Forescout eyeInspect

The primary objective of eyeInspect is to offer comprehensive visibility into the substation, which provides a holistic understanding of the substation network. Visibility is key as any oversight regarding assets or network segments could result in the failure to detect potential vulnerabilities or malicious activities.

Once eyeInspect has full visibility of assets and networks, the system can proactively address potential vulnerabilities, risks, alerts, threats, network communication mappings, baselines, process values, and more. Moreover, eyeInspect offers users valuable dashboards, highlighting assets with the most critical vulnerabilities and risks. This aids in prioritizing and addressing the most important issues, which is beneficial when dealing with a large number of potential risks and vulnerabilities.

Network deployment considerations

eyeInspect uses passive network monitoring as its primary method for gathering network and asset information. This validation was conducted for the use of eyeInspect's Passive Sensor strategically located at the substation. The sensor can be configured to ingest mirrored network traffic through methods such as the Switch Port Analyzer (SPAN) protocol. In the following figure, the sensor is shown to ingest SPAN data into its data interface while the sensor is managed and connected to the Command Center through its management (Mgmt.) interface.

eyeInspect can also ingest data through its Active Sensor which can be configured for various devices, including industrial-type devices like programmable logic controllers (PLCs) and workstations. The Active Sensor conducts safe scans to avoid potential disruptions to industrial devices, as they may not be equipped to handle traditional IT scanning methods. By doing so, eyeInspect ensures that critical industrial systems remain secure and stable, while simultaneously offering valuable insights into their security and performance.

Figure 17. Physical deployment with PowerEdge XR12

vCenter cluster networking considerations

There are some key considerations when deploying the sensor on a vCenter cluster. In a vCenter deployment, there is a virtual distributed switch (vDS) which acts as the main switch between all ESXi hosts in the cluster. For the sensor to passively ingest network traffic on a vCenter cluster, distributed port mirroring must be configured on the vDS. Overall, the user chooses the source of traffic to collect based on the virtual network port. The user then selects the destination port to send the traffic to. Users should be aware that there is a limitation where traffic cannot be mirrored across hosts, meaning from one ESXi host in the cluster to another. Follow the guidance in the subsequent sections for workarounds to this limitation.

NOTE: If configuring port mirroring on a single host/standard vSwitch, use promiscuous mode instead. More information can be found in the Configuring promiscuous mode on a virtual switch or portgroup (1004099) article from VMware.

NOTE: There are other methods to get around the port mirroring limitation beyond what is listed in this document, such as creating a separate vSwitch. Other methods may have trade-offs, such as the requirement of a dedicated physical port.

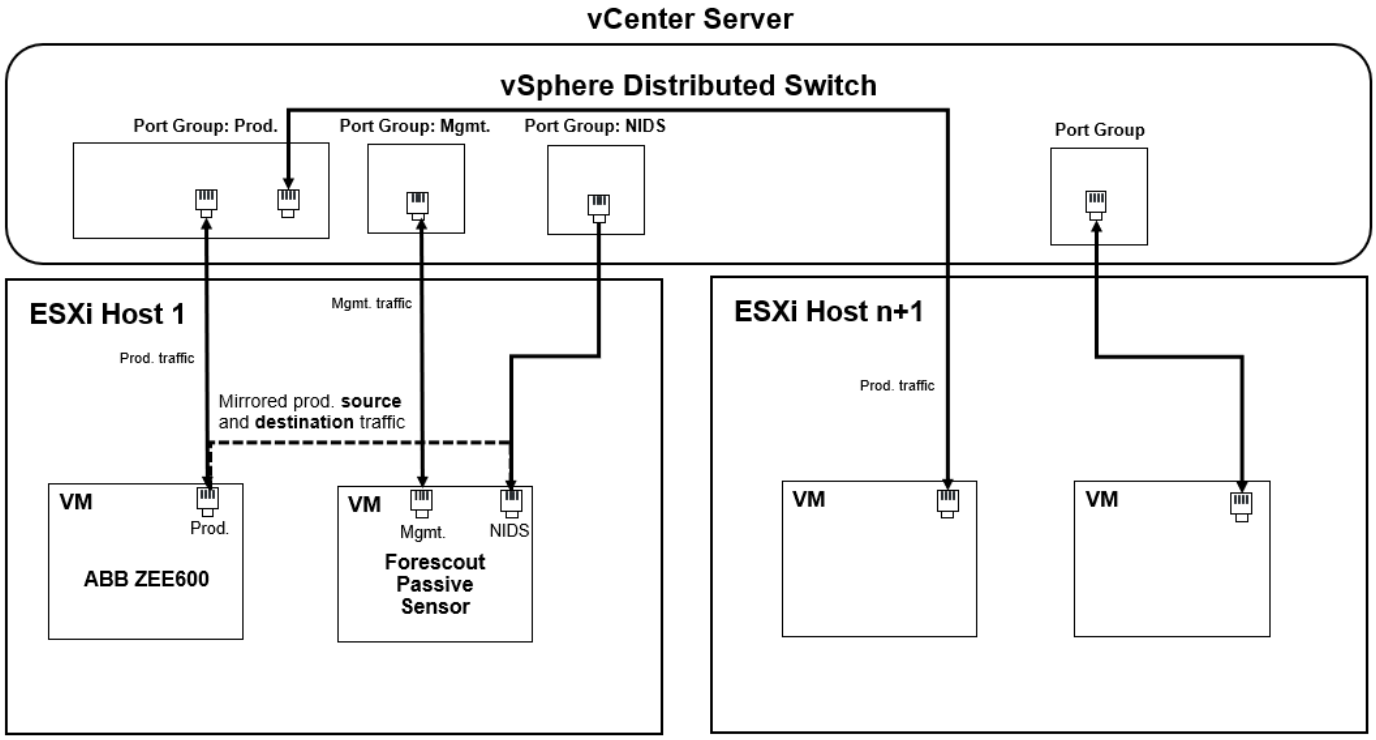


Figure 18. Example diagram of Distributed Port Mirroring on a vCenter cluster

PowerEdge XR12 deployment consideration

In certain scenarios, deploying eyeInspect software directly on a gateway can prove more efficient. This is advisable when the eyeInspect Sensor is in a separate network segment, distant from the Command Center server. As of the current date, the Dell PowerEdge XR12 has undergone validation to run the eyeInspect Sensor v5.1.0. For further details, see Platform hardening.

Test cases

Asset discovery

Forescout eyeInspect offers multiple methods to discover assets on the networks, such as passive and active sensors. The following test cases demonstrate the effectiveness of these features in allowing the utilities industry to gain insight into their network assets and reveal the underlying structure of the existing substation network.

Asset Passive Monitoring

Passive monitoring is the primary way data is ingested in Forescout eyeInspect. This is done by configuring Switch Port Analyzer Protocol (SPAN) on one of the Network adapters of the Passive Sensor and connecting it to switches at the substation. It is best to deploy on a core switch because if most traffic is traversing this switch, it is most efficient to collect data from one source. The sensor is deployed according to Forescout guidelines and then it is configured to connect to the Command Center. For the verification steps in Command Center, see *Monitor passive asset* in the Forescout tasks section.

The eyeInspect Passive Sensor offers **Asset Details** on each individual device and displays an asset map that shows asset locations on the Purdue model. It also provides a communication flow to highlight inbound and outbound traffic from the asset. Users can access asset properties such as IP, OS, and MAC address, along with the corresponding asset risk information.

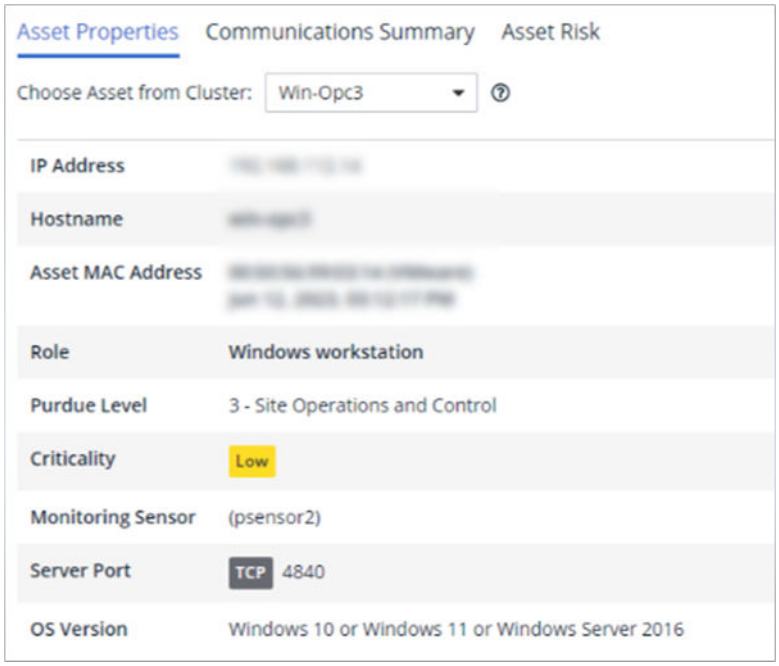


Figure 19. Asset Properties window

Asset Active Scanning

The primary role of Active Sensors is to collect data that cannot be easily accessed through passive monitoring. This can lead to the discovery of additional information about known assets, or identify assets that are not actively communicating or reside in networks that are not monitored by passive sensors. Active Sensors play a crucial role in providing a more thorough view of the network, complementing the insights obtained from passive monitoring. The sensor is deployed according to Forescout guidelines, then it is configured to connect to the Command Center. For the verification steps in Command Center, see *Scan active asset* in the Forescout tasks section.

The eyeInspect Active Sensor conducts scans on one or multiple hosts to identify active IP addresses, thereby discovering new assets within the network. It assesses the operating system, identifies open ports that may pose risks to an asset, and recognizes open OT-specific ports to ascertain the historical communication protocols of an asset. Additionally, the Active Sensor captures details like IED hardware and firmware information, among other relevant data points.

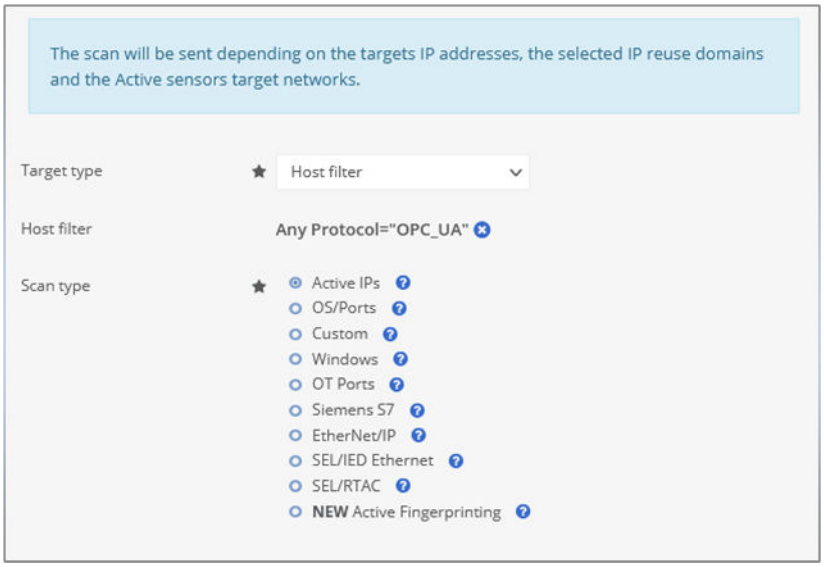


Figure 20. Active scan policies and configuration

Network visibility and architecture

Having a clear understanding of an organization's network architecture and topology is essential in locating and identifying network issues. It is crucial to ensure that devices adhere to standardized models, such as the Purdue Model for substations. Having this sort of visibility can validate that assets are logically in the proper location, and unauthorized devices are not jumping operational levels to communicate with other devices, which can pose security risks.

By gaining visibility into the network architecture, organizations can anticipate potential threat scenarios and align their architecture models with standardized business practices for enhanced security and operational efficiency.

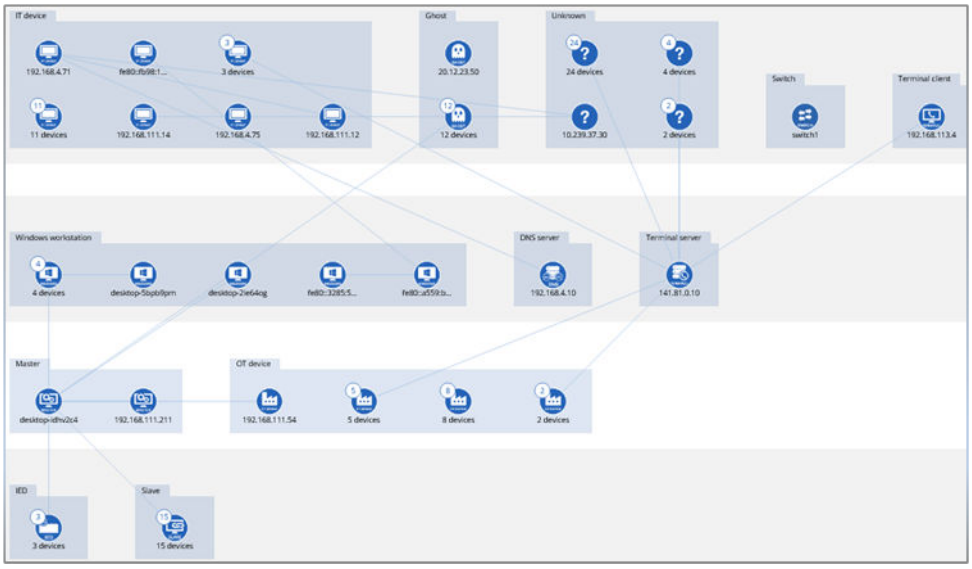


Figure 21. Visibility of network topology

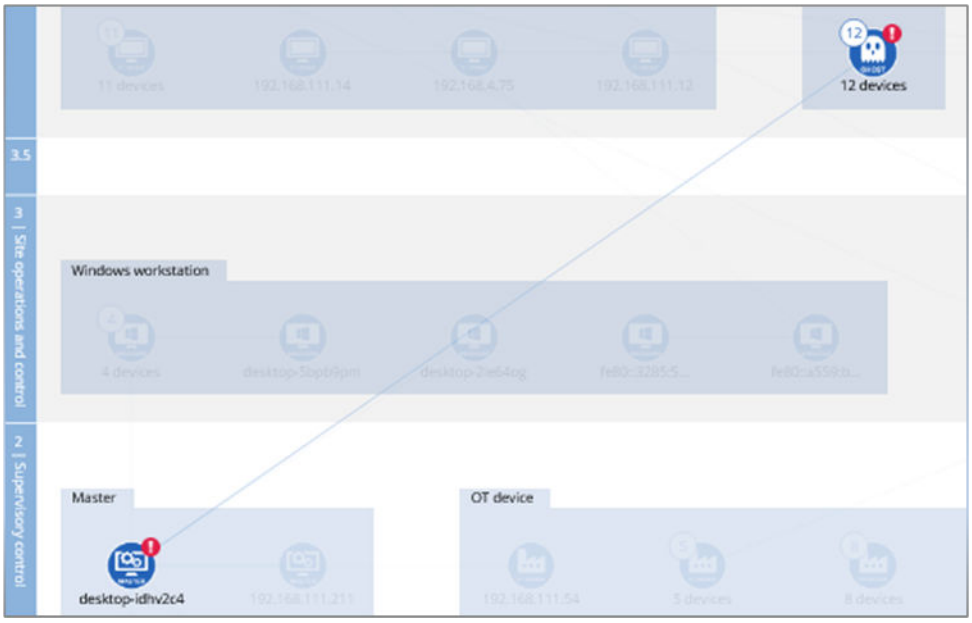


Figure 22. Visibility of possible threat scenario

Asset visibility customization

Substations often consist of numerous assets, and there may be instances where the focus needs to be narrowed down to a specific type of asset. EyeInspect offers the flexibility to customize dashboards in the **Assets** tab, enabling users to access detailed information about specific types of assets.

This capability enhances the user's ability to obtain purposeful insights and effectively monitor the wanted assets. This allows for well-informed decision-making for asset management.

Investigation and detection

Detecting network communications can be effective in applying configuration management. Capturing and correctly identifying network communication establishes a baseline and helps to also detect any anomalous or suspicious behavior.

Detect network communications

Gaining insight into the network communications of the substation plays a crucial role in identifying suspicious requests and transfers. The Passive Sensors are equipped with Event Logging modules, which require activation. Once activated, these modules search for specific actions on network communication protocols.

Enabling all these features ensures that eyeInspect maximizes its capability to capture and detect rogue events, bolstering the network's security and effectively mitigating potential threats.

Event name	Status	Category	Protocols	Severity	Description
		(NOT SET)		(NOT SE	
Name query	Enabled	Name resolution	DNS		A name resolution query wa
Name resolved	Enabled	Name resolution	DNS		A name query issued by a n
File access error	Enabled	File operation	FTP, SMB, SPLUS		An error was reported durir
File access error: file not found	Enabled	File operation	SMB		A file not found error was re

Figure 23. Example event log

Risk and vulnerabilities

Forescout sensors offer valuable insights into the assets present at your substation, which include vulnerabilities and risks. In conventional terms, a vulnerability represents a weakness, while a risk refers to the probability of that vulnerability being

exploited. This section demonstrates how eyeInspect can reveal vulnerabilities and risks to the cybersecurity of the substation network and provide a comprehensive means to view and effectively manage risks that are present.

Detecting vulnerabilities

Within its monitored network, eyeInspect incorporates a network intelligence framework with detection engines that monitor and alert for scenarios that are related to security, networking, and operations. The Passive Sensor is equipped with an Industrial Threat Library (ITL) which examines assets for weaknesses and outputs vulnerabilities specific to each asset type in the **Assets Details** tab. The ITL aligns with common vulnerabilities and exposures (CVEs) tailored to the substation, ensuring operators receive relevant vulnerability information, avoiding unnecessary alerts unrelated to their operations.

This targeted approach streamlines security monitoring and allows operators to prioritize focus on critical issues.

Figure 24. Display of vulnerabilities

Generating insight of risks

eyeInspect offers a quantified approach to assessing asset vulnerabilities by assigning risk scores for both operational and security risks. These risk scores can be configured to be continuously updated through periodic polling, enabling real-time risk evaluation in fast-paced operational environments.

This dynamic capability fortifies the system's ability to proactively identify and address potential risks, providing valuable insights for effective risk management and informed decision making.

Risk calculation

eyeInspect incorporates a robust integrated risk calculation method, developed through years of experience and extensive research on substation threats. Since each substation is unique, operators and administrators have the flexibility to customize risk calculations, prioritizing attributes that contribute to the risk score as percentages.

This tailored approach empowers organizations to adapt to their specific security needs, enhancing the effectiveness of risk assessment and management that is closely aligned to their security posture.

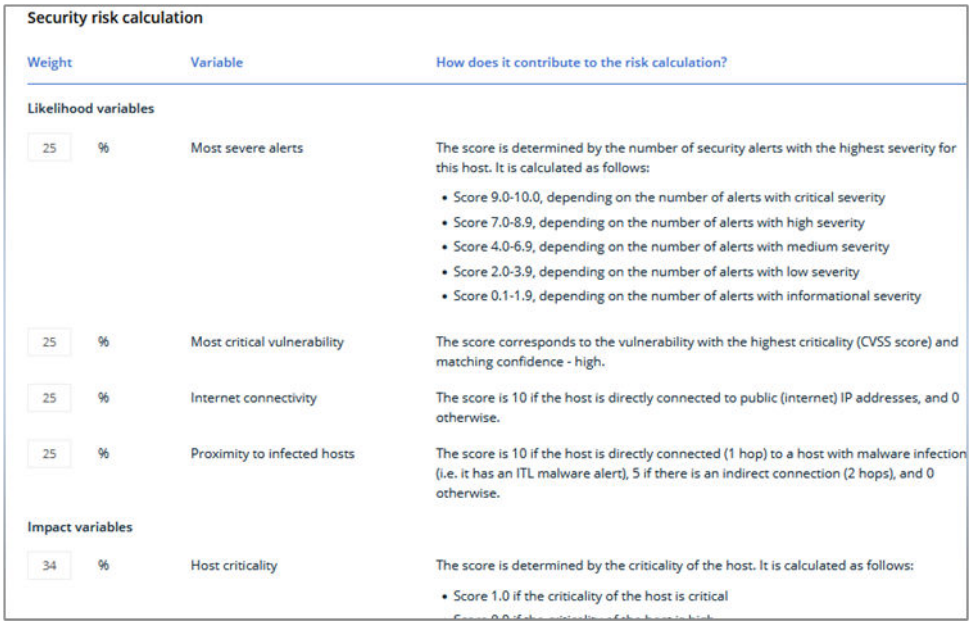


Figure 25. Security risk calculation

Risk visualization

By representing risks in a visual format, administrators can quickly identify critical areas that require immediate attention and prioritize their efforts accordingly. This visual representation enables better decision making, facilitates effective risk mitigation strategies, and enhances overall cybersecurity measures. Forescout eyeInspect provides dashboards on the home landing page for visualizing assets at higher risk at-a-glance, and further customization is possible in the **Analytics** tab, allowing operators to create graphs depicting assets and their risk levels (operational or security) in relation to other variables.

Visualizing risks helps administrators identify, communicate, and track the security status of the substation in a more intuitive and accessible manner, allowing for a better understanding and support for security initiatives.

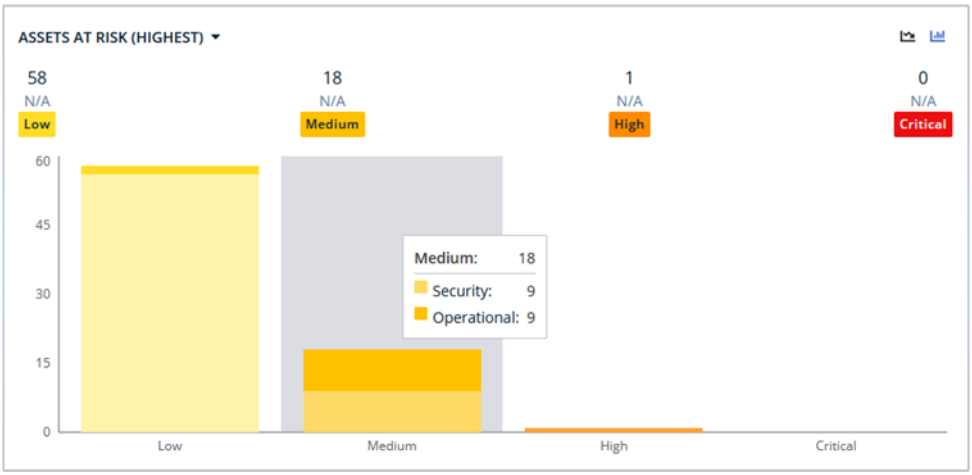


Figure 26. Risk prioritization dashboard

Threat detection

Forescout sensors also provide useful insight into potential threats to a substation. Conventionally, a threat is an event or scenario that can cause data to be damaged, leaked, stolen, or disrupted. eyeInspect can enable visibility into substation network security threats and allow end customers to evaluate threats they are concerned about.

Threat definition updates

eyeInspect's Command Center (CC) offers the capability to update CVEs and indicators of compromise (IoCs) tailored for substation environments. This feature is vital, as threats are consistently detected and require regular updates. Forescout regularly provides CVEs that specifically target the substation through its Partner Portal. Administrators have the option to manually upload the new threat definitions that are provided by Forescout to the CC and are encouraged to download updates frequently. By going to **Events** > **Network Logs** > **IoC Scan Page**, you can upload the updated files that contain the new CVEs and IoC definition.

This proactive approach enhances the ability of the system to stay current with emerging threats, bolstering the cybersecurity posture of substations, and ensuring effective threat mitigation.

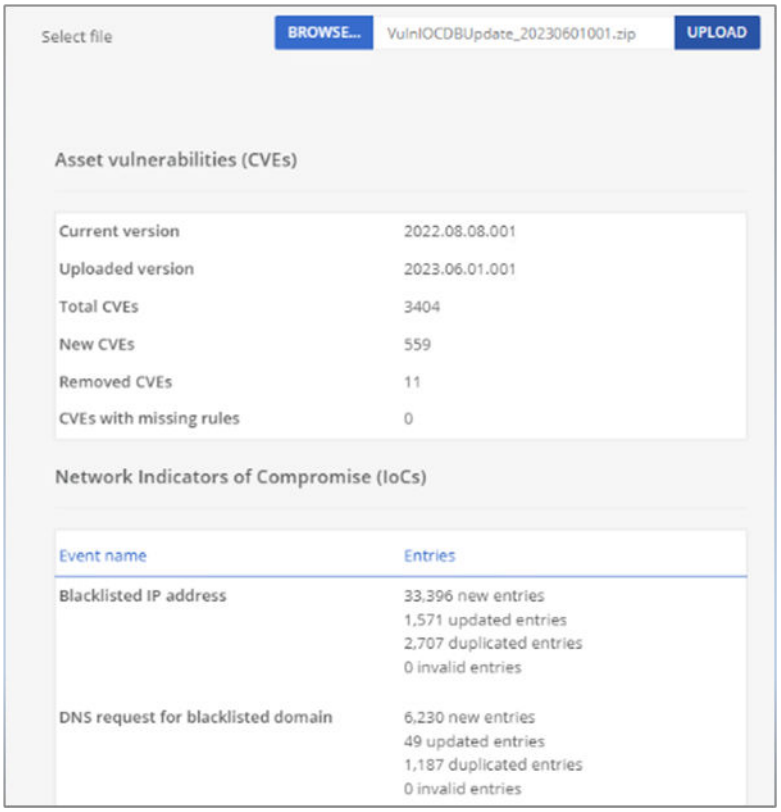


Figure 27. Upload to Command Center threat definition library

Threat monitoring and discovery

eyeInspect incorporates an Industrial Threat Library, which enables the identification of asset actions as potential threats. A list of all potential threats along with general alerts can be found in the **Events** > **Alerts** tab. When an event is identified as a threat, an in-depth alert summary is presented, featuring the communicating assets, associated sensors, and a brief description. Additional tabs offer more detailed information such as ports, protocols, and timestamps for the event.

The CC also provides ICS adversarial tactics, techniques, and common knowledge (ATT&CK) category matches for the events, explaining the tactics and techniques used by attackers for the matched threat. This valuable information helps organizations to understand attack patterns and helps them take appropriate measures to counter potential threats. Lastly, the discovered threat outputs the sensor's trigger details, providing the lowest level of information about the event.

This multifaceted approach ensures a comprehensive and granular understanding of detected threats, facilitating efficient threat management and response.

Threat visibility customization

Just as with creating dashboards for assets with specific attributes, eyeInspect enables the creation of dashboards for events that pose potential threats to substations while reviewing related **Alerts**. This functionality empowers operators to monitor and analyze events more effectively, ensuring timely responses to potential security risks and enhancing the overall threat detection capabilities of the system. For example, if there is a threat that coincides with assets communicating through the DNP3 protocol, you can create a dashboard to filter the alerts of **L7 Protocol: DNP3**.

#	Event Type	Timestamp	Alert Cat...	Severity
32 (29.4%)	DNP3 device lost all DNP3 connections (itl_ops_lec_dnp3)	07/27/2023 - 07/26/2023	Operational	High
25 (22.9%)	DNP3 invalid reserved bit (pars_psc_dnp3_iv_rb)	07/27/2023 - 07/27/2023	Anomalies	High
18 (16.5%)	DNP3 object type and function code mismatch (pars_psc_dnp3_m_otfc)	07/27/2023 - 07/27/2023	Anomalies	High
4 (3.7%)	Invalid field value (pars_ops_iv_ci)	07/27/2023 - 07/27/2023	Anomalies	High
3 (2.8%)	Invalid field length (pars_ops_il_bob)	07/27/2023 - 07/27/2023	Anomalies	High
6 (5.5%)	Unexpected restart(s) of DNP3 field device (itl_ops_md_dnp3_restart)	07/27/2023 - 07/27/2023	Operational	Low
5 (4.6%)	DNP3 field device with event buffer full (itl_ops_md_dnp3_buf_overflow)	07/27/2023 - 07/27/2023	Operational	Low
16 (14.7%)	DNP3 device restored DNP3 connections (itl_ops_lec_dnp3_restored)	07/27/2023 - 07/27/2023	Operational	Informational

Figure 28. Filtering of alerts by DNP3 protocol

Cases

In eyeInspect, operators have the capability to create **Cases** in the **Events** > **Alerts** tab. This feature groups related alerts and instructs the system to automatically assign new instances of those alerts to the designated case. This can help segment alerts related to an ongoing investigation or process. This functionality can also help to streamline threat monitoring, allowing operators to concentrate on new threats emerging on the network while efficiently managing and analyzing existing issues within designated cases.

Alert cases improve operational efficiency by providing a structured approach to handle and prioritize security incidents in real time.

Baselining and deviation

In OT environments, uptime and reliability are often prioritized, leaving minimal time to address system security. The Passive Sensors can be equipped with the Local Area Network Connection Profiler (LAN CP), which tracks and analyzes TCP and UDP communication patterns among network devices. Regular communication patterns are recorded in an editable safelist. The LAN CP can be set to **Learning** mode to establish a baseline of communication traffic. Once configured, the profiler switches to **Detecting** mode, alerting on unfamiliar communications to identify potential rogue devices or anomalies on the network.

This proactive approach aids in enhancing the security posture of OT environments and mitigating potential risks effectively. LAN CP can be toggled between **Learning** and **Detecting** mode to establish a new baseline if needed; however, this privilege should be restricted to administrators to allow for proper change management.

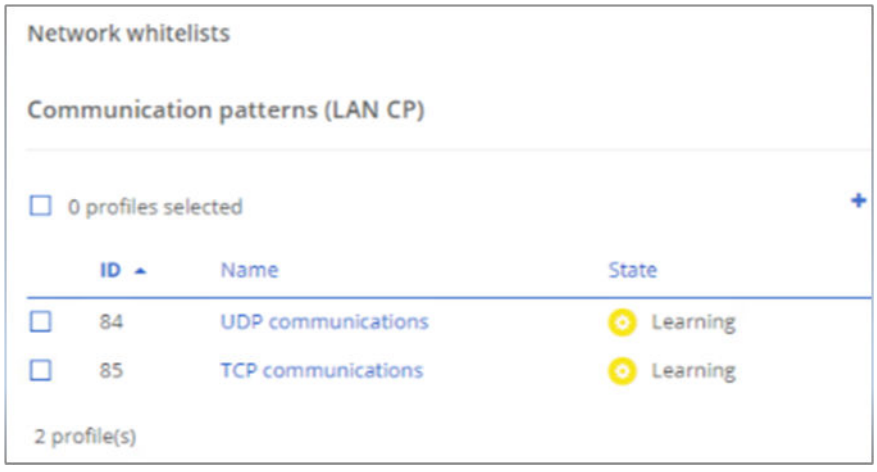


Figure 29. Network safelist

Incidence response and alerting

Forescout eyeInspect primarily functions as an intrusion detection system, providing incident response for network access concerns through alerting. It seamlessly integrates with security information and event management (SIEM) for log forwarding and can generate incident reports for forensics without disrupting Forescout operations. Moreover, eyeInspect harmoniously

integrates with other Forescout applications, thereby creating a robust cybersecurity ecosystem that elevates threat detection and response capabilities.

Viewing alerts

eyeInspect generates alerts when it detects suspicious events in the network traffic. These alerts are assigned severity levels, allowing administrators to prioritize their response. Alerts can be triggered by:

- Network communications
- Anomalies when eyeInspect observes deviations from a set baseline
- Security and operational events when potential threats or disruptions are matched to tactics and techniques of known threats
- Informational alerts that notify of nonthreatening events in the system

All alerts can be conveniently viewed in the **Events** > **Alerts** tab, providing administrators with real-time insights to effectively manage and respond to security incidents.

Timestamp	Event Type	Alert Category	Severity	Source IP Ad...	Destination ...	L7 Protocol	Des
Jun 30, 2023, 03:34:12 PM	Use of insecure protocol (...	Security	High	[redacted]	192.168.112.37	TELNET	23
Jun 30, 2023, 03:33:25 PM	Use of insecure protocol (...	Security	High	[redacted]	192.168.112.36	TELNET	23
Jul 05, 2023, 03:55:35 AM	Host not receiving answe...	Networking	Low	[redacted]	10.239.37.96	DNS	53
Jul 05, 2023, 03:39:33 AM	Host not receiving answe...	Networking	Low		255.255.255.255	DHCP	67
Jul 04, 2023, 03:48:05 AM	Host not receiving answe...	Networking	Low	[redacted]	10.239.37.96	DNS	53
Jul 03, 2023, 03:39:19 PM	Host not receiving answe...	Networking	Low		255.255.255.255	DHCP	67

Figure 30. Details in the Alerts tab

Generating reports

eyeInspect offers the capability to export host information and alert details to an editable .docx document. Users can create management reports that provide an overview of assets and identified threats on the network. Additionally, eyeInspect allows for generating detailed reports for offline analysis and mitigation purposes.

Figure 31. Generate report icon

In eyeInspect's Command Center, every tab offers the capability to generate and export CSV files. Whether it is a comprehensive list of assets and their essential details or specific assets with vulnerabilities, this feature ensures convenient data export for various purposes.

Within the **Events > Alerts** tab, when selecting a specific alert, locate the three vertical dots on the right. There is submenu item **Download PCAP** which presents the opportunity to retrieve a packet capture (PCAP) file encompassing the unprocessed network traffic that is linked to the alert. This feature empowers analysts to conduct an investigation into the origins and outcomes of the identified anomalous behavior. The PCAP file further serves as a resource for forensic analysis.

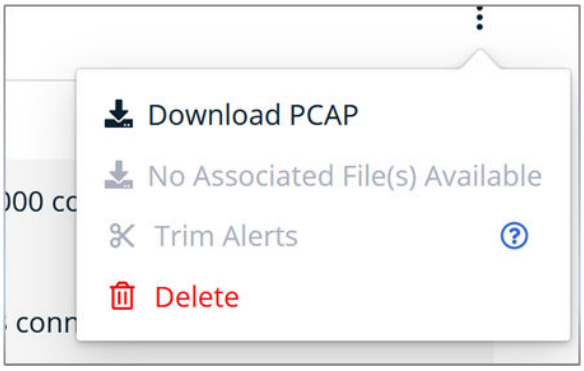


Figure 32. Download PCAP in asset alerts

Integrating with SIEM

Forescout eyeInspect specializes in incident response by alerting for events and potential threats. Its sister software, eyeSight, seamlessly integrates with external products like ServiceNow, streamlining incident response workflows. eyeInspect can automatically take action to resolve incidents by connecting to eyeSight. Additionally, it can integrate with SIEM solutions using the syslog protocol, enhancing security threat detection, analysis, and response for organizations. Forescout can forward alerts, network logs, active scans, and Command Center's health status to the SIEM.

Forescout's integrations strengthen its ecosystem's security posture and incident response abilities, providing a more complete approach to security management.

Detect and read OT process values in a unified architecture

eyeInspect was validated along with ABB ZEE600 following the architecture that is displayed in the Validated architecture for secure communication in a substation and Control Center figure. Utilizing a few of the more common substation protocols, the integration of Forescout eyeInspect provided valuable insights into assets engaged in protocol-based communication. Upon asset detection, eyeInspect conducted a risk assessment and established its logical architectural position. The following figures show a few of the protocols that were used and eyeInspect's discovery and representation of them.

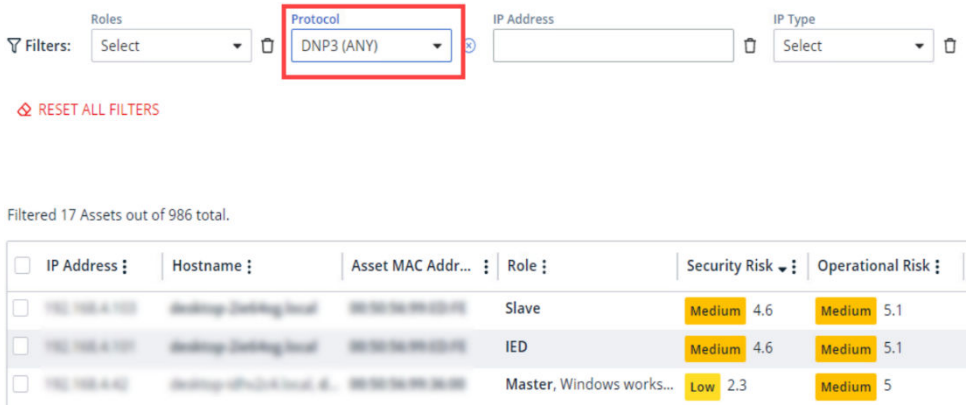


Figure 33. eyeInspect discovering assets communicating through DNP3

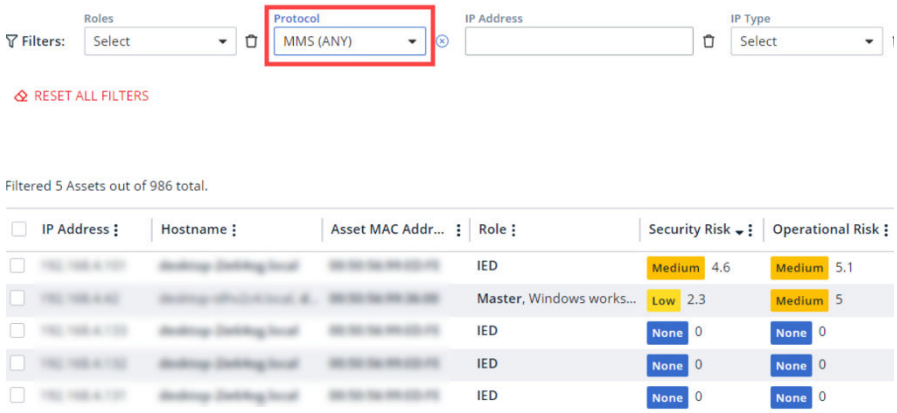


Figure 34. eyeInspect discovering assets communicating through MMS

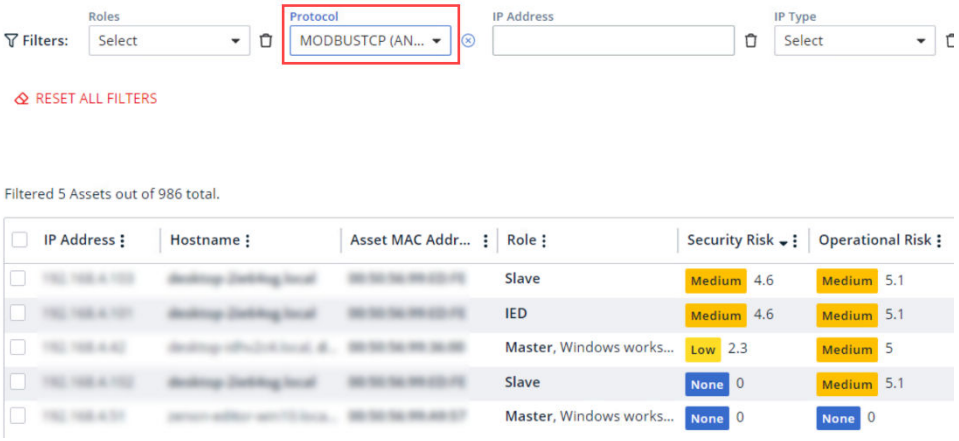


Figure 35. eyeInspect discovering assets communicating through MODBUS/TCP

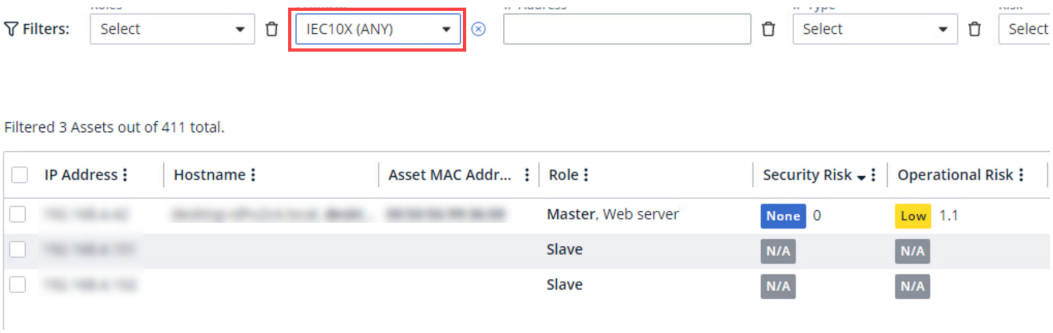


Figure 36. eyeInspect discovering assets communicating through IEC 104

eyeInspect's passive sensor has a feature similar to the Local Area Network Connection Profiler (LAN CP) feature, Deep Packet Behavior Inspection (**DPBI**) to learn the normal range of protocol behavior/values per asset. After the protocol behavior had been observed and recorded, the DPBI monitor was set to detect mode, promptly alerting on any values outside the range of values learned from the device output.

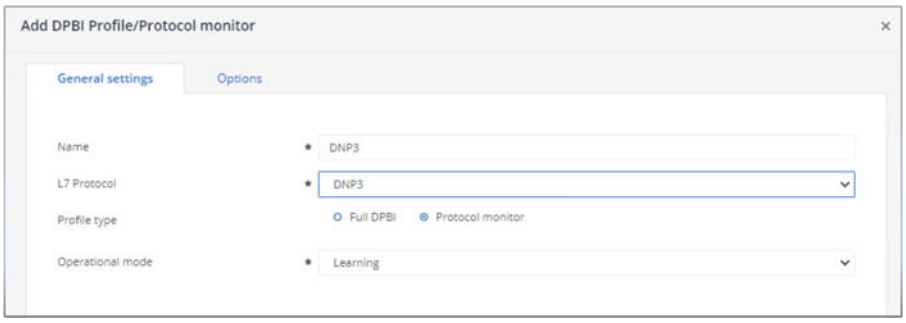


Figure 37. DPBI to monitor specific protocols

Unforeseen variations such as voltage fluctuations can disrupt operational continuity within substations. Detecting when values deviate from the anticipated range proves invaluable in the forensic analysis of trends. In the event of such incidents, eyeInspect promptly alerts and designates the numerical anomalies as **Anomalies**, aiding in timely response and resolution.

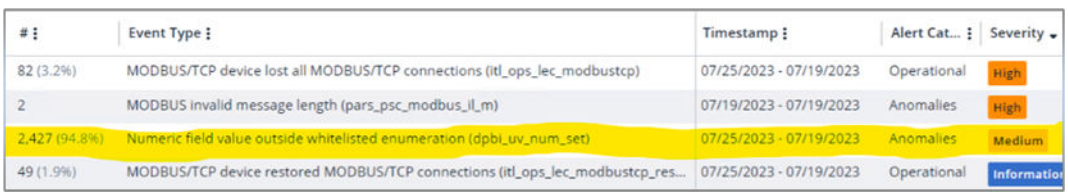


Figure 38. Alert of a baseline deviation anomaly

Forescout tasks

Configure distributed port mirroring

About this task

This is an example of how to configure distributed port mirroring to send traffic from a port or set of ports to the sensor VM. The sensor hosts have at least two ports (network adapters), where one is designated for management purposes only, and the other for mirrored network data as shown in Validated architecture for secure communication in a substation and Control Center. Make sure to send traffic to the appropriate data ingest port.

Steps

1. Log in to the vCenter vSphere Client.
2. Navigate to **Inventory** > **Networking**.
3. Click the distributed switch.
4. Navigate to **Configure** > **Port mirroring**.
5. Click **NEW...**.
6. Select **Distributed Port Mirroring** and click **NEXT**.
7. On the **Edit properties** options, set the following at a minimum:
   a. **Name:** *<Descriptive name>*
   b. **Status:** Enabled
8. Click **NEXT**.
9. In the table of port groups, select the source port group. This designates the ports for which traffic is copied from.
10. Select the port group(s) and click **NEXT**.
11. In the table of port groups, select the destination port group. This designates the port(s) that will receive the mirrored traffic.
12. Select the port group(s) and click **NEXT**.
13. Click **FINISH**.

Example

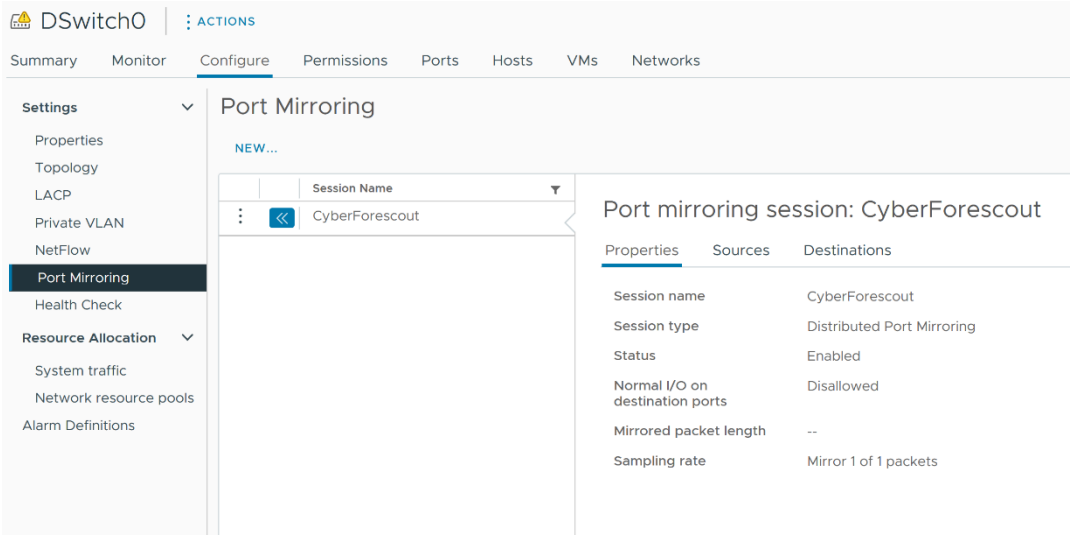


Figure 39. Example of configured port mirroring showing destination port groups for the specific rule

Monitor passive asset

Prerequisites

- Command Center deployment
- Ubuntu 20.04 LTS iso image

- Two network adapters
- SPAN Port enabled on one network adapter port

Steps

1. In Command Center: Navigate to **Sensor** > **New Sensor** > **Enrollment overview**.
2. Once you see the sensor that you just configured show up under a Pending enrollment status:
   a. Double check the device UUID.
   b. If the Passive Sensor does not show up in the enrollment guide:
      i. Re-run the sudo nids-cc-mgmt command (from the Installation guide).
      ii. Reboot the sensor.
      iii. Refresh the Command Center page.
3. Once the request is visible with a Pending Enrollment Status, click on **Actions** > **Accept Request**.

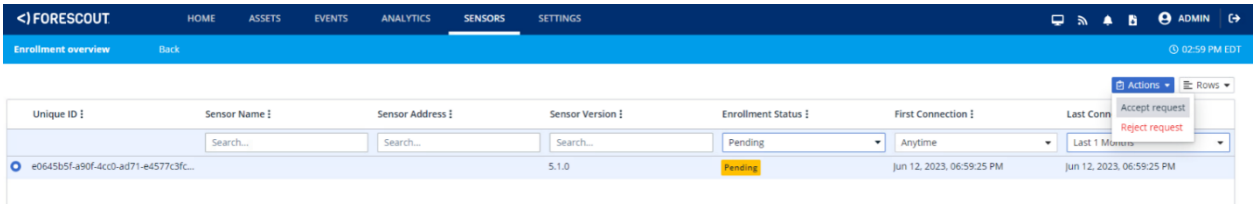


Figure 40. Add new sensor in Enrollment overview

Next steps

Helpful tips and links:

- Forescout OT Hardware Guidelines
- eyeInspect Installation Guide
- Make sure the Passive Sensor is on a network that is discoverable by the Command Center.
- Do not clone the sensor VMs, as CC needs a unique ID to connect sensors to its UI.

Scan active asset

Prerequisites

- Command Center deployment
- Ubuntu 20.04 LTS iso image
- Active sensor deployed according to user guide

Steps

1. Log in into Command Center as an admin, and navigate to **Sensor** > **Sensor Overview**.
   You should see the sensor that you just configured show up under **Active Sensors**.
2. If the sensor state is in deployment for too long, navigate to the Command Center command line and run the `sudo docker restart icsp-core` command and refresh the Command Center page.

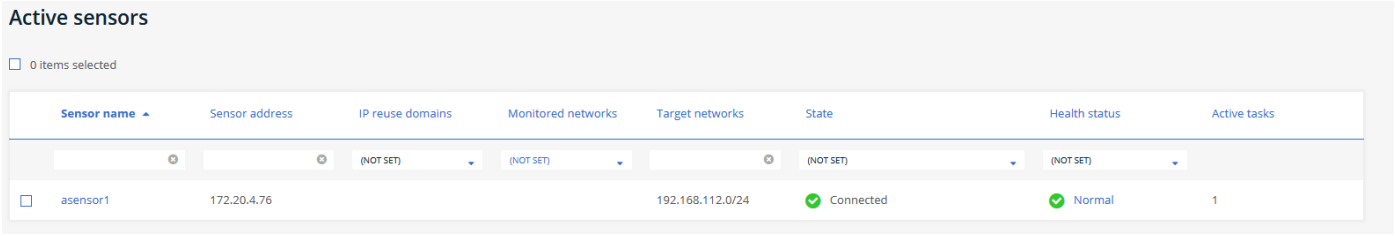


Figure 41. Active sensor is visible

Next steps

Helpful links:

- Forescout OT Hardware Guidelines
- eyeInspect Installation Guide

4

Accelerated Time to Value

Topics:

Overview

The Dell Validated Design for Energy Edge helps create high-performance, robust, and expandable substation automation systems. It also contains a variety of features that reduce development time and enhance the quality of the deployment. This chapter explores those features in more depth.

Service level management

Service level management means meeting the performance, scale, workflow, user base, and data services requirements according to pre-defined service levels. In consolidated environments servicing a multitude of substation devices, operational workflows, and users, service level requirements for various segments of the environments are varied. They may range from mission-critical environments to mid-tier operations and even low-tier environments used for reporting, QA, and development.

Service level management ensures that the right set of resources are available to service the needs of these diverse environments which can dynamically scale up and down with shifting priorities. Service level management planning encompasses a range of components and operational details to ensure high-performing and efficient substation operations that meet the demand for the application service levels.

More emphasis can be given to critical processes to ensure the highest service levels compared to mid-tier and low-tier environments, which are assigned less importance.

For the Dell Validated Design for Energy Edge, the following service level management aspects are considered:

- Data ingest sources, frequencies, and user base
- Size and number of ISV application instances
- Compute, storage, and memory allocations for virtual machines and edge gateways
- Number of virtual machines and their clone copies
- Number of configured objects, visualizations, and their data rates for reads and writes
- Real-time and historical analytics operations and affected data sets

Data ingest sources, frequencies, and user base

Substations have a variety of devices that produce data. The speed at which this data needs to be collected and processed varies based on the specific operation, priority, and analytics.

The type and value of information also differs based on the device producing it. The number of users connected to such systems varies based on the amount of automation or complexity of the operation.

Size and number of ISV application instances

The sizing of ISV application instances depends on the number of data sets that they need to manage. Based on the scale and sizing requirements, multiple instances can be configured on the supported infrastructure by this DVD, and it is important to evaluate data service requirements for various instances to ensure ease of management, desired availability, and user experience.

Using a large number of small instances may pose operational challenges and result in lower overall efficiency. But small instances also allow for smaller copy sizes, ease of backup and restore due to finer granularity, ease of migration for changes in the scale as the application demands change, all resulting in better overall system management.

Alternatively, keeping a small number of large instances may make adding new systems easier due to the extra capacities these instances have. But large instances make it difficult to manage due to higher complexity and the number of underlying systems supported by them. It is important to plan the deployment with current and future growth in mind and to consider the overall complexity of the OT and IT systems.

For more information, see the Sizing and Scaling Guidance chapter.

Number of configured objects and their data rates for reads and writes

The number of configured connections, external data tables, devices and tags, and visualizations is accountable for the system load and performance profile at a given point in time. The data rates vary according to their size and frequency, and they put stress on the system in the event of spikes. For example, when the users are first connecting, running some analytics operations, or configuring new objects, the system needs to handle the additional level of workloads. Some of them result in heavy writes or some heavy reads, or a combination of both, which stresses the entire system as various components compete for the available resources.

Scaling up environments to manage growth

As utility operations mature and support a broad range of services, workflows, and user base, it becomes necessary to scale up the environments. Similarly, old applications may retire, operations may get consolidated, and the systems used for processing may move into a lower tier to support QA and reporting, all of which may require downscaling of those environments. This section covers the considerations for infrastructure updates and data or system migration aspects. Specific tasks may vary based on the environments, but it helps to follow the general guidance provided in this section.

Scale and sizing guidance to meet demand of workflows

The system size and resources required for a given ISV deployment vary based on the expected load, required performance, and configuration options selected.

The following are parameters to consider when making sizing decisions:

- The number of connected sensors and equipment (referred to as devices)
- The number of tags collected, the data types of the tags, and frequency of data collection
- The number and type of applications and dashboards
- The number of locations and facilities
- The requirements for local data processing and for high-performance configurations
- The applications running real-time and historical analytics using telemetry data

Deploying the DVD for Energy Edge solution on VMware comes with the significant benefit that—if load or performance requirements should change in the future—CPU, storage, and memory configuration changes can be made easily in the VM's settings. Some of these changes can even be made on the fly, with no production downtime.

NOTE: For more information, see Sizing and Scaling Guidance.

Collect VMware ECS and application performance data and tune the environment

The vCenter system monitoring dashboard provides detailed insights into compute, network, and storage consumption at the VM level. PowerCLI, which is tightly integrated with Windows PowerShell, can be used to collect such monitoring data at various granularities and frequencies. CSV files can be generated from the PowerCLI-collected dataset, and it can be used for further analytics and charting for identifying bottlenecks and tuning the environment. Application and VM-level performance data can also be collected, using tools like Windows Performance Monitor (Perfmon), IOstat, and others, to compare vCenter-reported data with application-level performance for further application-level guidance and tuning.

Infrastructure requirements for scaling

Evaluation of the performance of the system and future operational needs may require proactively updating the environments to meet the changing demands. These are the key points for consideration for infrastructure changes. The points below are based on the service level priorities of the target environments, and not all of the points have the same impact for all environments.

- Consider the service level changes needed with the new scale and plan the environment as per the guidance from earlier section.
- Based on the expected data growth rate, plan for some extra capacity.
- Consider the data services requirements. Some of the factors include writes per second and reads per second rates, number of connected users, size, and type of the data set to estimate the throughput requirements, desired latency based on the service levels of the environment, and data retention period.
- Add enough data and log devices and increase their count for scaling up for performance as well as concurrency.
- Use separate VMware paravirtualized SCSI controller for each device to minimize contention for IO operations.
- Analytics tools require heavy reads and may span various database tables making them very memory and I/O intensive. Such operations also feed the results to other tiered services to augment the decisions or provide additional capabilities. Consider the type of analytics operations to run on the data and the locality of that on edge, core, and cloud with the data exchange and security requirements.
- Identify the data protection needs, high availability, and mechanisms to recover the environments in the event of failures and corruption.
- This DVD also works across functional edge, far edge, and near edge, and several ISV applications are purpose-built for specific edge deployments. Dell Edge Gateways, PowerEdge servers, and VMware systems are among other products and services that offer a broad range of options to meet the needs of these environments. Consider ISV application-specific scaling and sizing to optimize the performance at all of these layers for the best return on investment and efficiency.
- This DVD also covers multiple ISV applications and allows cross-ISV application deployment to address a variety of use cases. Scale and sizing should also consider how multiple ISV applications interact with each other, what use cases they are addressing, and the components of these ISV applications. For example, small sizing for one ISV application may be different from small sizing for another ISV application, or when multiple ISV applications are combined.
- This DVD takes into account ISV-specific scale and sizing guidance, but the flexibility that Dell infrastructure products and services offer allows updating the scale and sizing as the application demands change.

Migration requirements for scaling

- Use a pre-tested clone from the source environment to seed the new target environment. Once that is complete, all industrial connection and network configurations can be updated to confirm the data flow onto the target environment. These are the steps to adhere to new scale requirements:
  1. Configure the appropriate directory structure and files as per the desired scale. New data files and log files can be added as necessary to support data growth requirements at the application, databases, and support file levels.
  2. Introduce these new files to the application ecosystem using application mechanisms.

  NOTE: See the Licensing section for important information about ZEE600 licensing on VMs.
- Test the backup or clone available from the source environment, which can be used to revert the changes, if necessary.
- Migration may also involve moving to a different hardware type, different data services, or consolidation of multiple systems into larger systems, or splitting the applications across multiple systems. Ensure that the intricacies of the applications are properly considered when planning for such migrations.

Tuning the environment for higher performance

Whenever instantiating a database for storage on a hyperconverged infrastructure, it is best practice to create separate disks for the host OS, for the data, and for the database logs.

In VMware, the configuration steps are simple. In the settings of the VM, add additional hard disks, typically assigning the largest amount of storage for the data disk. Leave the boot disk for the host OS. Create one SCSI controller per disk, and assign it as the **VMware Paravirtual** type. Once the controllers are created, adjust the hard disk settings such that each hard disk has a dedicated SCSI controller.

Upon booting the VM and depending on the host OS, complete the partitioning, mounting, and formatting of the additional disks. Update the database configuration to point to the correct paths for these disks. The steps will vary depending on the OS and selected database.

If working on an existing database, follow proper procedures for backup and migration.

NOTE: Before making any configuration changes, ensure that there is access to a recent backup of the VM.

Creating templates to rapidly deploy new environments

Once a deployment is set up as documented in this guide, there are several ways to rapidly deploy new environments. The following are important guidelines to consider:

- Clone an existing VM to create another, using the same configuration as the original one. In this way, any number of new environments can be rapidly deployed with very little intervention. VM resources, operating systems, database disks, and so on are automatically configured on new machines. Users simply need to change the network configuration, update the connectivity between various applications, and then customize any environmental details for the facility.
- If further customization is needed, new database disks, scale, and other aspects can be configured. Such customization requires following database migration best practices, adding customized devices and tags for the desired scale, and enabling additional services for new environments.

Leveraging analytics for optimized operations

Analytics and tools to incorporate

Several tools can be utilized at various hierarchical levels to track and analyze system needs and performance.

At the cluster level, performance parameters are leveraged to track compute, latency, and more, down to the physical disk.

The vSphere client portal is part of the VMware suite. It provides out-of-the-box charts to view real-time and historical VM performance of:

- CPU
- Memory
- Memory rate
- Disk and network traffic

Complex analytics can be developed using a rich set of tools, including Grafana, REST API, Python, Java Scripting, and database-level analytics tools like PowerBI, Tableau, and others.

Grafana is a software platform that can be used to aggregate and consolidate performance metrics from various endpoints, such as vCenter, Windows, Linux, Kubernetes, Docker, and many others. There are various versions, including open-source, cloud, and enterprise versions that can be leveraged for consolidating and visualizing metrics in dashboards. Many prebuilt dashboards are available directly from the Grafana open-source community. Dashboards can also be easily customized to display the most important information in the environment. See the Grafana website for more details.

Different ISV applications also offer visualization and analytics using the ISV's native capabilities. They can be leveraged to have better synergies with existing processes for those applications.

ESXi system performance metrics

The VMware vSphere UI or Windows PowerShell with VMware PowerCLI integration can be used to collect performance metrics including the SCSI controller, CPU and memory consumption of individual VMs, disk latencies, and throughput information.

NOTE: See Windows PowerShell and VMware PowerCLI documentation for details.

OS performance metrics on Windows

At the OS level, many tools are available to track performance metrics. These tools and metrics vary based on OS.

In a Windows systems, the built-in Performance Monitor application provides an easy-to-use graphical user interface (GUI) to configure jobs that can collect specified data on demand. These metrics track compute performance, memory use, and storage use, broken down by disk. These jobs can also be exported as a template to quickly configure multiple machines.

NOTE: For more information, see the Windows Performance Monitor Overview from Microsoft.

OS performance metrics on Linux

Linux systems offer comparable statistics with select packages. The sysstat package offers system performance tools that are comparable to those in Performance Monitor on Windows, including CPU utilization and disk I/O statistics. This package can be installed on both Debian and CentOS Linux systems, though the installation varies between them.

After installing the sysstat package, execute the `iostat` command to output a set of real-time system statistics including CPU use, memory use, and disk use. Details on command options and the collected metrics are available on the iostat man page.

These metrics can be easily output to a file for tracking and analysis.

Ensuring time zone consistency across devices

For continuity of data, intentionally set the times and time zones used on all machines responsible for generating and storing data. Syncing all machines to an NTP server is a reliable way to accomplish this.

Accelerated time to value with ABB ZEE600

Along with functionality, an important consideration when developing substation software solutions is how quick and simple it is to customize the application for each substation. ABB ZEE600 is based on the zenon SCADA software and contains the features that accelerate development found in the base software, as well as a variety of features specific to the energy industry.

These include:

- ZEE600 project templates
- Automatic line coloring
- IEC and ANSI standard symbols
- ZEE600 device import wizard
- Object import and export
- Driver simulation

ZEE600 project template

The ZEE600 New Project wizard dramatically reduces the time to create a substation project from scratch and ensures a consistent structure throughout all projects.

The general structure of this HMI is to have four sections: single line diagrams, system diagnostics, plant automation, and reporting. Each of these sections can then have up to 12 pages, depending on the size and complexity of the substation. There are also various pop-up screens that are automatically created to enable switching users, viewing and responding to alarms, real-time configuration of the HMI, and various other functions.

Navigation of the HMI is also handled in the project template, through an always-present navigation bar at the top of the screen and an interactive information bar at the bottom. The previously mentioned pop-ups are all accessible, either directly by using the icons on these bars, such as the alarm icon in the top right, or by opening the main menu through the menu icon in the top right and then selecting the desired item.

During the template setup process, there is an option to enter contact details and a customer logo. This logo is displayed at the bottom of the HMI, and the contact details show up in the **Utilities** pop-up from the main menu. This is a great opportunity for integrators to add their brand to the HMI and show availability for support and development needs.

Automatic line coloring

The central page of a substation HMI is the single line diagram. This is where an operator can immediately see which lines are live and how all the different substation components relate to one another. ZEE600 includes a feature called automatic line coloring to speed up the development of this crucial component.

The way this works is that all the basic single line diagram symbols are assigned a role, such as Source, Transformer, and so on, and any line attached to that component inherits the appropriate color. This includes the correct voltage color when active, as defined by either IEEE or ANSI standards, and it changes dynamically depending on the status of the connected components. This allows for very complicated single line diagrams to be created without the need to configure every line.

Standardized IEC and ANSI substation symbols

Most substations are required to follow either IEC or ANSI standards, depending on the country. This includes a specific set of symbols to represent different components in the single line diagram. ZEE600 makes developing these single line diagrams easier by including all the necessary symbols pre-configured so that they can be easily added to the single line diagrams.

Since the same ZEE600 symbols are designed to be used regardless of standard, they can even be switched dynamically. Therefore, as long as standard icons are used, the same project can be deployed in substations that use IEEE and ANSI without any change.

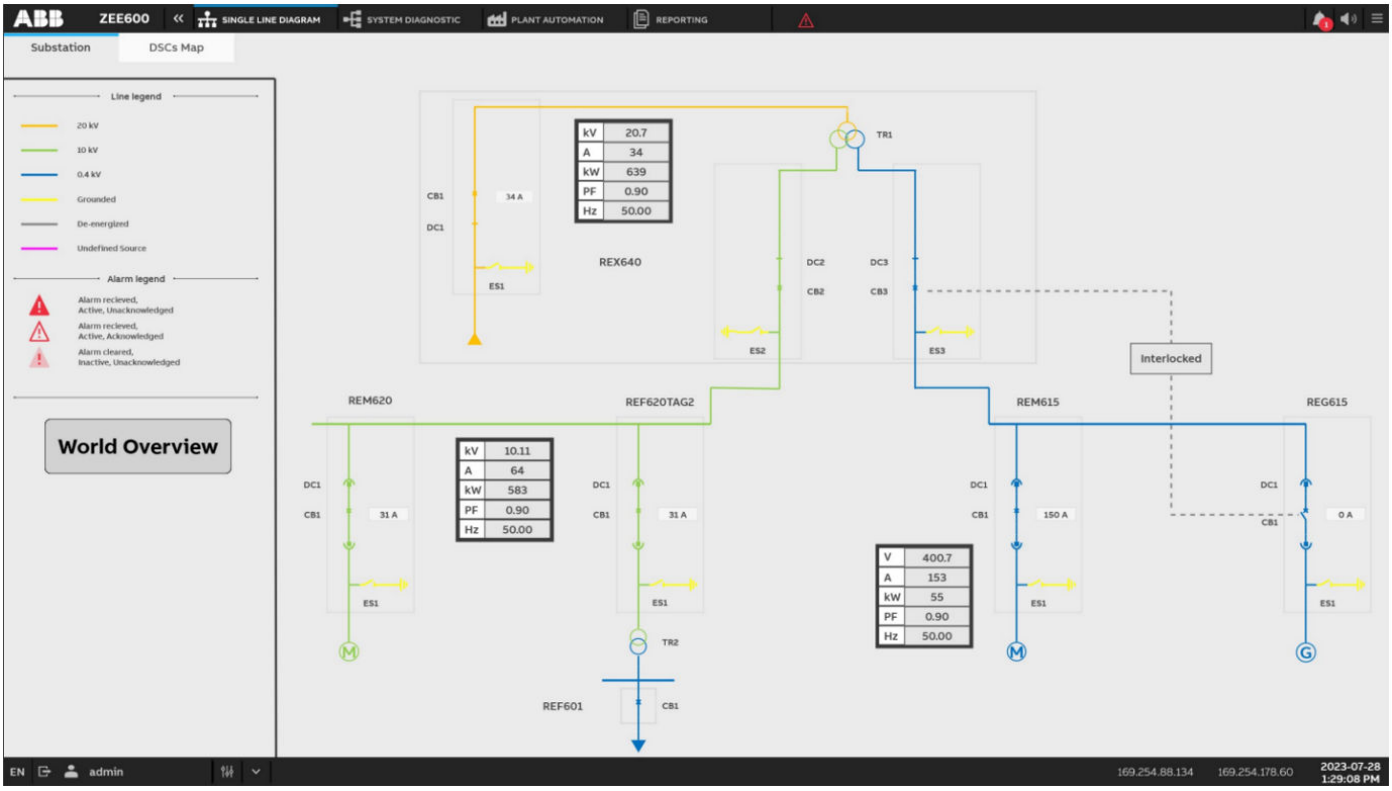


Figure 42. Sample single line diagram with legend

ZEE600 object import wizard

A major stage of developing substation automation is to connect specific devices through an IED and create appropriate graphics. ZEE600 makes this task much easier by including an object import wizard.

The first step in this wizard is to define the substation structure by identifying the substation name, voltage level, and bay ID. Use this information when naming components to simplify filtering. This bay structure is then stored in the **Equipment Modeling** section and can be used to assign authorization or aggregate alarms according to the defined hierarchy.

Once the bay structure is complete, components are then individually added to each bay. The pre-configured ones include circuit breakers, transformers with tap changers, metering devices, and ABB SWICOM devices. After selecting the category of device, the specific symbol can be chosen and assigned to a specific single line diagram (where multiples exist). If no preconfigured symbol exists, a generic object can be created and later connected to objects on the screen.

At the time of writing, the only objects that can be imported through the wizard are those that use either Modbus or IEC 61850 communication. For other devices, such as DNP3, it is still possible to take advantage of the wizard by creating a temporary Modbus device, and later updating the communication configuration.

Object import and export

Virtually all objects (tags, pages, functions, and so on) can be exported to an XML file format using the **Export selected as xml** option found by right-clicking on the object in the project manager. This is useful for scaling up development as you can export the xml, use a text editor to replace key values (such as communication addresses), and then import the xml as a new device. This also allows for easy development of a single project in parallel amongst multiple engineers because each engineer is responsible for their specific component xml file and can set up their project as they choose.

Furthermore, configuring hundreds of tags for various protocol drivers can be a tedious process. ZEE600 allows the export of a single tag or a few tags to a CSV file format, where these template tags can quickly and easily be replicated programmatically or based on a pattern. This extended CSV file can then be imported back into the ZEE600 project to rapidly scale the data ingest configuration.

Simulated drivers

One of the best features for accelerating time to deployment and improving quality is the built-in option to simulate drivers. This enables HMI and automation development and testing without the need for actual hardware. When the hardware becomes available, a simple switch makes it easy to test and use actual hardware communications.

For relatively simple projects, the option to set a driver to **Constant** or **Counting** is sufficient. For the **Constant** setting, all tags are set to their initial value (this typically defaults to 0 for all number types). The values can then be changed through the HMI or through automation programming. If **Counting** is selected, the tags start at their initial value and increase by one every second for numeric tags or alternate between true and false for binary tags. This is useful for situations where seeing a number change is important, such as with trend lines.

For most projects however, it is worth developing a simulated driver. This allows for realistic variable values, expected variable interactions, and appropriate use of automation and alarms. Setting up these simulated drivers is done by right-clicking on the driver and selecting **new / edit simulation**. This brings up the programming interface, and code can be written in any of the IEC 61131 languages.

Accelerated time to value with Forescout eyeInspect

Managing the ever-evolving landscape of cybersecurity threats can be challenging when conventional security tools often lack the specialization to comprehend OT networks and protocols, resulting in the potential oversight of vulnerabilities, risks, and threats. Offering a portfolio of software applications designed for OT environments, Forescout provides a versatile array of methods to collect network information, respond to network events, and at-glance analytics into systems. By creating solutions that simplify the process to acquire an in-depth understanding of their OT networks, optimize their prioritization strategies, and execute timely actions, users can swiftly achieve an accelerated time to value in safeguarding their industrial environments.

eyeInspect

Forescout eyeInspect simplifies network visibility for users, providing a comprehensive overview of their network activities and facilitating the identification of top-priority concerns. Users have the opportunity to leverage eyeInspect's granularity to drill

down deeper into the insights the Sensors and Command Center discover and present on the dashboards. In each subsequent section, we delve into specific eyeInspect features and their role in accelerating time to value.

Deployment

As part of this validation process, eyeInspect's two components, Sensor and Command Center, were isolated into separate networks. These components can be deployed on bare metal servers or as virtual machines (VMs). Forescout also offers a hybrid deployment option where the Sensor and Command Center are combined into a single VM. While deploying the Sensor and Command Center individually is not excessively time-consuming, opting for the hybrid solution expedites both deployment and configuration processes. Both the Sensor and Command Center installations are executed through the Ubuntu terminal, and the necessary installation files are accessible in the Forescout Partner Portal.

Sensor Template—During the configuration of a Passive Sensor with a command center, a unique Universal Unique Identifier (UUID) is required by the Command Center to identify each instance. If a Passive Sensor is cloned, there is a risk of having the same UUID, which can lead to complications in sensor configuration.

Prior to running the Passive Sensor installation file, users can create a virtual machine template on vSphere. This approach eliminates the need for repetitive deployment tasks, and only running a single command per virtual machine. Sensor networking settings can be adjusted afterwards to prevent potential IP conflicts.

Risk Realization

Forescout eyeInspect Command Center makes it easy to view the overall risk of the network at a high level. This visibility is achieved through informative graphs that enable users to swiftly assess their cybersecurity status. The risk score is categorized into two distinct aspects: Security and Operational. Security risk assesses the likelihood of an asset posing a security threat based on various factors such as alerts, Internet connectivity, proximity to vulnerable hosts, and existing vulnerabilities. Operational risk gauges the likelihood of an asset causing operational issues based on factors like logical location, network impact, and related alerts.

eyeInspect allows users to view individual asset risk scores presented on an asset map and represented by color-coded dots. The risk score is a combination of the security and operational risks, which helps users to quickly identify critical assets and high-risk network levels. This aids administrators in concentrating their efforts in these areas of concern.

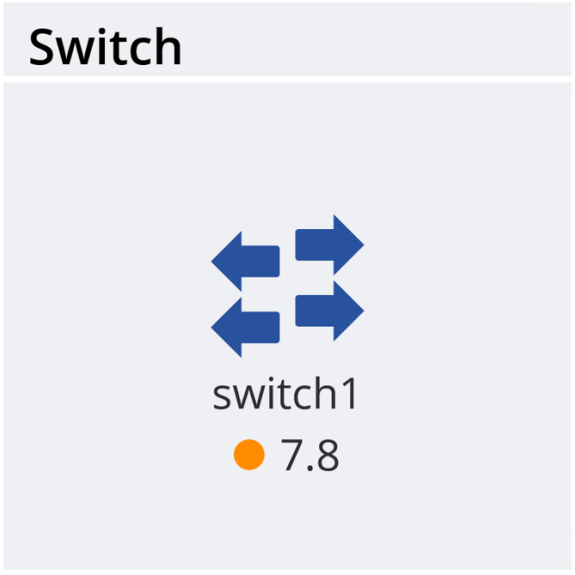


Figure 43. Color-coded risk calculation identifying risky assets on an asset map

Enterprise Command Center—eyeInspect also includes an Enterprise Command Center (ECC). The ECC was not a part of the validation, but it is a software solution that empowers eyeInspect administrators to retain local or regional control over their eyeInspect Command Center installations while achieving centralized visibility for their OT infrastructure.

This provides security analysts with an instant overview of potential issues and threats within specific regions. Analysts are presented with visual and tabular representation of vulnerabilities, alerts, and operational health status for OT networks and assets across multiple deployments of ECC. In cases where multiple Command Center deployments exist within a region, the ECC localizes each geographic area and provides summarized insights into your OT systems.

Data ingest

A crucial element of eyeInspect revolves around data ingestion, a vital consideration for effective substation management. Enhanced visibility contributes to a comprehensive overview and minimizes the risk of overlooking crucial events. eyeInspect provides multiple pathways for data ingestion that can be customized to accelerate the processes involved in data visualization.

Passive Network Monitoring—End users must configure their network devices (for example, switches or virtual switches in vSphere) to mirror network traffic to the Passive Sensor. Sensors connect to the Command Center server over TCP/IP. This adaptive approach caters to environments constrained by network traffic mirroring capabilities.

In hybrid deployments of Command Center and sensor, the option emerges to directly mirror traffic to the eyeInspect server when combined with Command Center, eliminating the requirement for a distinct sensor setup.

Packet Captures (PCAPS)—PCAPs are files containing network packet data. eyeInspect allows users to replay PCAP files in the sensor so that the sensor can ingest the network data from that file and add it to its pre-existing dataset on the connected Command Center.

As mentioned before, Forescout offers a hybrid deployment, bundling its Command Center and sensor into one VM. Within these bundled configurations, the Command Center introduces the capability for traffic captures (PCAPs) to be reenacted through the UI, facilitated by PCAP Replay Sensors. The PCAP Replay Sensor parallels the functionality of a monitoring sensor, with the sole distinction being its inability to monitor real-time traffic.

5

High Availability and Disaster Recovery

Topics:

What is high availability?

Utility operators are evaluated based on their ability to meet established reliability objectives. The operational efficiency of substations is of paramount importance as they play a vital role in upholding consistent and dependable electrical services. These services rely on high availability (HA) of operations applications to provide sophisticated protection and control functions to ensure uninterrupted functionality. The ability of these systems to maintain an agreed-upon level of uptime is critical for smooth operations. Similarly, HA systems should be configured so that the operations and workflows with lower importance (also known as noisy neighbors) do not interfere with mission critical operations. Systems with proper high availability practices allow administrators to use applications with minimal involvement, improving productivity and reliability.

High availability overview

The Dell Validated Design for Energy Edge includes single-node, 2-node, and 3+ node cluster options, depending on workload needs and HA requirements. A single-node configuration provides the necessary hardware to run multiple application virtual machines (VMs) but without HA and will incur downtime when host failures happen. The 2-node and 3+ node configurations provide the necessary redundancy to offer a highly available processing environment with the 3+ node option providing both infrastructure and workload HA. See the System Design chapter for a complete list of components and the Bill of Materials for hardware specifications. For vSphere documentation, see the VMware vSphere Documentation.

Resiliency of the ISV application stack on VMware

As described earlier, there are several components involved in the solution, and all of them offer varying degrees of resiliency.

ISV application services are automatically started when the VM fails over or migrates to another node in the VMware cluster, making the entire stack ready to use without user intervention. As user connectivity relies on access to the web services—other than a momentary glitch—there is no impact to the users.

Role-based HA management for devices, users, and applications

ISV applications may not offer the role-based service level management needed to ensure that a certain set of mission-critical applications, users, and devices have higher availability compared to other noncritical users. Role-based HA management is important to ensure that high-priority applications remain available and continue to perform. This requires application deployment with proper understanding of the application, user load, connected devices, and priorities.

There are several ways to address the needs for role-based HA management:

- Based on the prioritized grouping of the ISV application components, a separate set of VMs and database VMs can be used for deployment. Such physical separation allows configuration of a different set of policies to ensure higher availability.

VMware DRS allows fully automated, partially automated, and manual placement for load balancing and resource scheduling. VMware HA offers host rules to keep a user-defined set of VMs together. ISV application VMs can be configured with specific host rules to ensure consistency of performance and availability across all application components. This separation of the application stack also allows the use of independent database services and storage devices with additional policies.

- Such role-based configurations assist in identifying the requirements for additional VMware ECS clusters, ISV applications, and related components.
- Similarly, other policies like security, alerts and monitoring, database snapshots, backup and recovery can also be employed differently when considering role-based availability of ISV applications.

RPO and RTO management

For 24/7 industrial environments, the ability to quickly troubleshoot a failure, and more importantly, recover from a failure situation, are key considerations. Different users, applications, and devices can have a different Recovery Point Objective (RPO)—which brings the application state to the last good state for continued operations—and Recovery Time Objective (RTO). RTO is the time it takes to bring the entire application stack to the last good state. ISV applications depend on continuous availability of database services, and various backup and recovery options are available to ensure availability of the application stack. Thus, ISV applications running on VMware help to manage and improve RPO and RTO.

Aggregating data sources and supporting multiple use cases at scale

Edge applications aggregate data from a diverse set of sensors, devices, and gateways that support various network topologies and use different protocols for northbound traffic to edge systems. ISV applications support a large set of such protocols and communication channels. It is common to have multiple layers of gateways supporting a large set of sensors. ISV applications support many protocols for northbound traffic and can communicate with multiple application instances. By deploying multiple instances, and aggregating and storing data from diverse data sources, users can realize HA and also provide an additional set of services from multiple instances.

For example, one ISV application instance can be used for analytics and predictive maintenance, whereas another can be used for reporting overall health of the system and time series data.

Isolation and multitenant network management

Many edge devices provide multiple physical interfaces to connect to multiple northbound IP addresses that support various ISV applications. VMware infrastructure and network switches support multiple network interfaces. Such redundancies in the network configuration offer HA, and if any network paths go down, operations are not impacted. Such networks can be configured with independent VLANs to isolate traffic for multitenant environments, improving overall availability and allowing effective noisy neighbor management.

HA considerations

RPO, RTO, and tracking the last known good state of the system

Applications can keep track of the last known good state of the system in various ways: journaling, logging, periodic snapshots, and so on. This tracking determines the RPO. Also, the amount of time it takes to start from the known state to a good restart point will determine RTO. These two are important measures for the HA capabilities of a system. This section covers configuration, operation, and recovery aspects.

- Configuration data
  - Edge devices may allow configuration related to data collection type and frequency, ability to send alerts and notification in specific conditions, period reports, and integration with external APIs. When failures occur, such configurations can be backed up to restore the configuration to a working state, or to quickly make replacement devices operational. Such configurations can be exported and stored on resilient folders on vSAN datastores.

    NOTE: For more details, see the device-specific documentation.
  - Several ISV applications can back up their configuration. Even if such back-up practices are in place, it may be useful to use vSAN datastores for backups as well for an additional level of protection and availability.

NOTE: For more details, see the ISV-specific documentation in References.

- Operational data
  - Edge devices collect and aggregate time series data and send them to the ISV application stack on which utilities operations depend. Edge devices depend on data services and analytics systems for operational intelligence.

Although the VMware virtual infrastructure that ISV applications run on provides a high degree of resiliency, edge devices operate independently and may not have the same resiliency as the VMware environment. They generally have multiple network ports, and using the available ports allows redundant communication channels and improves RPO and RTO.

Edge devices also operate under harsh conditions with excessive temperature, vibration, and other factors; and at times they need to operate in disconnected environments. Edge devices must be physically hardened and secured to work in such environments. Such devices accumulate data in a disconnected situation according to the available local resources. By ensuring appropriate bandwidth when the connection is re-established, they can improve RPO and RTO and contribute to the overall health of the infrastructure.

Many edge devices need to be portable and must connect to different networks and end devices quickly to ensure continuity. Edge devices need to support plug-and-play to allow communication with new devices, and to quickly discover and connect to available network interfaces for continued operation.

Non-disruptive updating and working in a non-uniform environment

Systems with effective HA should allow functioning in a non-uniform fashion. Even if all the components are not at the same software revision level, the system should continue to function. One premise of HA is to allow specific components to be updated transparently so that applications continue to run within another set of working components. The DVD for Energy Edge on VMware enables independent updating of standalone and clustered ISV applications. Updates are not applied automatically, so customers can have full control. The system also allows independent, non-disruptive updating for all its components, with administrative control over when to apply each update.

OT and IT user personas in regard to HA

OT personnel are looking for real-time access to production assets to improve efficiency, and they need the ability to connect to other facilities, global suppliers, employees, and partners. They are responsible for industrial automation control systems (IACS), Supervisory Control and Data Acquisition (SCADA), historians, and asset management. They are concerned with HA and the security of these systems, but lack the control and knowledge of infrastructures, data services, and networks that these systems use—which are managed by IT. HA for edge infrastructure ensures maximum availability for both OT and IT systems, with minimal interaction or impact on either side of the edge infrastructure. ISV applications on the Dell Validated Design for Energy Edge offer such capabilities by providing control, flexibility, and workflows for HA needed by OT and IT. They support a multiprotocol environment encompassing both OT and IT systems, and provide a policy-driven, single pane of control for HA for industrial automation systems.

How an HA system recovers

When components in the HA system go down, it is important to understand when and how those components can be brought up so that the HA system returns to its full functional capability. Understanding the degraded state of the system is helpful. If the system functions in the degraded state for a long time, surviving components will eventually go down and result in increased downtime. The following are some of the considerations for HA for ISV applications on VMware ECS:

- VMs supporting ISV applications should use VMware capabilities like Dynamic Resource Scheduler, vMotion, and HA rules to ensure optimal performance with policy-based user controls.
- VMware vSAN datastores perform with the highest level of availability.

VMware ECS nodes already offer storage and compute clusters for ISV applications. This solution can support multiple deployments of ISV applications with minimum Operating Expense (OpEx), allowing the separation of various production workflows, with better multitenancy controls with desired service levels. Separate deployments can also leverage independent datastores controlled by different policies. When failures occur, it is easy to identify, troubleshoot, and recover impacted components. This kind of deployment improves overall availability and performance with less management overhead.

What is disaster recovery?

A disaster recovery plan is a grouping of policies and procedures for how an organization responds and recovers from an event that negatively affects business operations. This plan should provide business continuity for essential infrastructure following a natural or human-induced disaster.

If an infrastructure is designed to provide high availability, then it may not achieve the goal of disaster recovery. A system that is considered highly available is fault tolerant, which is usually accomplished with redundancy. If a component in the system fails, it can seamlessly and automatically switch (failover) to a secondary backup. Disaster recovery aims to have an alternate site up and running when the primary site is offline due to an unforeseen event. A solution with both high availability and disaster recovery is crucial for business continuity if there is a component failure or disaster.

Disaster defined

The most common disasters that can impact critical infrastructure include the following:

- Natural disasters—Tornadoes, hurricanes, earthquakes, landslides, floods, and wildfires are some of the types of disasters that nature can produce. These unpredictable events can be catastrophic. A solid business continuity and disaster recovery plan are essential to avoid a complete collapse of the business.
- Cyberattacks—Humans can cause disasters. Data can be stolen, corrupted, or deleted. Identifying cyberattacks, knowing how they can affect business, and knowing how to recover from such attacks is crucial to the return of operations.
- Hardware failures—Many scenarios involving hardware failures are dealt with by having a dependable high availability plan in place. Redundancy in the system can help avoid data loss and unexpected downtime. These scenarios can be disastrous in the absence of proper planning.

  NOTE: For more information, see High availability overview.

DR overview

The Dell Validated Design for Energy Edge provides both business continuity and data loss prevention if a disaster occurs. By consolidating most ISV application services on a resilient VMware infrastructure, we provide a single dashboard for managing a successful disaster recovery (DR) solution. VMware simplifies the infrastructure stack by allowing compute, network, and storage resources to be managed as a single, shared pool. It provides a simple, scale-out architecture, leveraging vSphere and vSAN to provide server virtualization and software-defined storage, with simplified deployment, upgrades, and maintenance through vSphere vCenter.

NOTE: For more information, see the VMware vSphere Documentation.

VMware ISV application disaster recovery considerations

Before deciding on a disaster recovery strategy for an ISV application deployment, customers must have a business continuity plan. This plan is unique for a given business, and it should specify the metrics of RPO and recovery time objective RTO. RPO refers to the amount of data you can afford to lose before business operations are impacted. RTO is the timeframe in which the application and systems must be restored after an outage. Both RPO and RTO are typically determined by negotiating a service level agreement (SLA) with the business.

Recovering from a disaster is generally accomplished by using alternative production sites or cloud services. These alternate locations may operate in an active/active or active/passive fashion. A virtualized ISV application deployment provides multiple data protection options for every level of protection. The Dynamic Resource Scheduling (DRS) and High Availability (HA) features of VMware protect all components of the application stack, without complicated database or application-level cluster configurations.

If such a configuration is desired, application-level clusters can be configured. Such a configuration involves additional components and load balancers to create a clustered multisite environment. Beyond the integrated VMware HA/DR configuration, options are available for a more robust disaster recovery solution.

NOTE: See the ISV-specific chapters for more information about such deployments.

HA and DR with ABB

The previous sections highlighted the various sizing options tailored to specific workload needs and HA requirements. All sizing options include DR capabilities, but for a highly available processing setup, the 2-node and 3+ node configurations are the recommended choices as they offer a robust redundancy mechanism, ensuring a highly available processing environment.

This section explores the ABB ZEE600 features that contribute to building a more HA/DR-aligned far edge deployment, including:

- Types of HA redundancy
- Project Backup and restore functions

Types of HA redundancy

In a 3+ node deployment, the VMware ECS nodes form a single cluster to create a redundant pool of compute and storage capacity. vSAN and vSphere HA should be enabled on the cluster to provide highly available compute and storage for the VMs and the applications running on these VMs. In the 2-node configuration, where features such as vSAN and vSphere HA are unavailable, the network functionality of the ABB ZEE600 Runtime makes it possible to enable seamless redundancy in situations where the primary server experiences a failure.

For a redundant ABB ZEE600 system in a 2-node deployment scenario, a distinction is made between

- Software redundancy—The primary server communicates with the controller on a two-way basis; the standby server is read only.
- Hardware redundancy—Both servers communicate on a two-way basis with the respective connected controller. This is usually applied in conjunction with controllers connected in series.

NOTE: For either redundancy option, consider backup mechanisms and failover solutions to ensure consistent and reliable communication between virtual machines and any physically connected serial devices if applicable.

ABB ZEE600 software redundancy

A software redundant system consists of a controller and two redundant servers (primary and standby). Both servers must be connected to the IED. In normal operation, one server acts as primary and one as secondary. All other servers are clients. If the primary server fails, the standby server automatically recognizes the failure and takes on this role. All clients connect to the new primary server. Any on-premises configuration data is also protected, as it is duplicated on the standby server. For additional information and detailed steps to configure software redundancy, see the Redundancy section of the online help page.

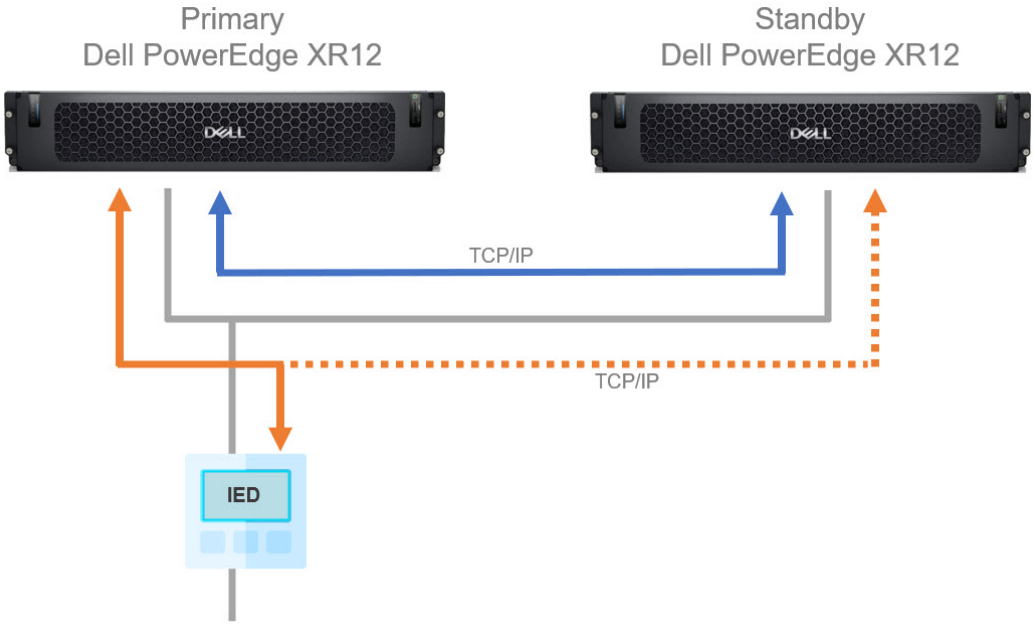


Figure 44. Example 2-node Dell PowerEdge XR12 deployment with software redundancy

ABB ZEE600 hardware redundancy

A hardware redundant system must have two controllers and two servers, in contrast to software redundancy. Hardware redundancy is primarily used in conjunction with controllers connected using serial. Both servers must be connected to the IED. In normal operation, the system consists of two redundant IEDs and two redundant control system servers. Each server communicates bidirectionally with one IED. Both computers and both IEDs synchronize their data. If one component in the first system crashes, the second system takes over. For additional information and detailed steps to configure hardware redundancy, see the Redundancy section of the online help page.

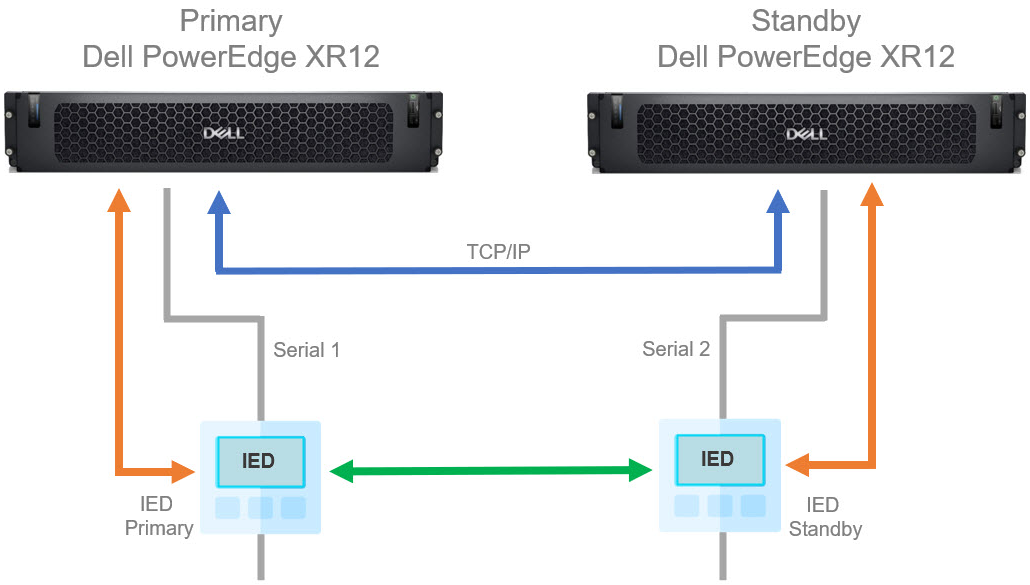


Figure 45. Example 2-node Dell PowerEdge XR12 deployment with hardware redundancy

Redundancy Management Tool

The Redundancy Management Tool is used on the server to monitor the network adapter and its connection to the network. If the server loses the connection to the network, the Redundancy Management Tool stops the Runtime. When the connection to the network is reestablished, the Redundancy Management Tool restarts the Runtime. For detailed configuration steps, see the Redundancy Management Tool section in the online help.

Project Backup and restore

In addition to full VM backup solutions, the ABB ZEE600 configuration can also be copied using the **Project Backup** functionality through the Editor. This is important for disaster recovery because a project backup can be restored and used to duplicate the configuration on an additional node in the case of a hardware failure, or to restore the configuration on a node where software was corrupted or an unintended change to the configuration was made.

Project backups can be exported and stored at a secure offsite location to ensure data protection and disaster recovery. Based on the desired RPO, the customer should decide the frequency at which backups are taken and the retention period for those backups. For more information and detailed steps, see the Project Backup section of the online help.

NOTE: When changing the parameters of a virtual machine, such as the number of CPU cores, RAM, MAC addresses, or in the event of a disaster where the host server is replaced, the license becomes invalid. It is thus recommended that you use network licensing for virtual machines. For more information, see the Licensing section of the online help.

HA and DR with Forescout

When running Forescout components as VM s on vSphere, it is recommended to leverage the existing features on the vSphere cluster that provide HA and DR capabilities. For instance, DRS automatically migrate s the Forescout VMs to a separate host if the current ESXi host fails. More information on about how to leverage vSphere HA and DR capabilities , see the High availability overview and DR overview sections.

In the two-node deployment scenario, where features such as DRS and vSphere HA are unavailable, itis essential to ensure network visibility remains intact during failover events. To achieve this, each ABB ZEE600 Runtime instance should be accompanied by a corresponding eyeInspect Passive Sensor on the same ESXi host. This deployment strategy guarantees the continuity of network monitoring and analysis.

For each eyeInspect Passive Sensor, a designated port-mirror configuration is necessary. You can find detailed instructions on how to set up a port mirroring session for the eyeInspect Passive Sensor in the System Design chapter.

Backup and restore with Forescout

The following tasks cover the backup and restore procedures for recovering eyeInspect data in case of permanent or temporary system failure. By using these procedures, all the data and most of the settings of eyeInspect can be safeguarded.

Before initiating a backup, it is essential to verify that the backup storage medium has ample space available. Keep in mind that a single backup might necessitate several gigabytes of storage capacity. For enhanced data security and recovery options, consider storing the eyeInspect backups at a secure offsite location.

The frequency of backups and the retention period for these backups should be determined by the customer based on their desired RPO. This help s to align the backup strategy with the specific needs of the customer's data management.

When it comes to restoring eyeInspect components, ensure that the versions of the components being restored match the version of the backup. This guarantees a seamless restoration process and minimizes compatibility issues.

Backup and restore tasks

Back up a Command Center

Steps

1. Log into the Command Center server using SSH.
2. Run the Command Center Backup and Restore Script by issuing the following command:

```
sudo /opt/sdconsole/scripts/backup-cc.sh -backup <path/location of your backup>
```

NOTE: The backup file is named cc-backup-<*timestamp*>, for example cc-backup-20220801164121.

Back up a Passive Sensor

Steps

1. Log into the Passive Sensor server using SSH.
2. Run the Passive Sensor Backup and Restore Script by issuing the following command:

```
sudo /opt/nids-docker/bin/backup-passive-sensor.sh -backup <path/location of your backup>
```

NOTE: The backup file is named passive-sensor-backup-<*timestamp*>, for example passive-sensor-backup-20220801164121.

Back up an Enterprise Command Center

Steps

1. Log into the Enterprise Command Center server using SSH.
2. Run the Enterprise Command Center Backup and Restore Script by issuing the following command:

```
sudo /opt/ecc/scripts/backup-ecc.sh -backup <path/location of your backup>
```

NOTE: The backup file is named ecc-backup-*<timestamp>*, for example ecc-backup-20220801164121.

Restore a Command Center

Steps

1. Log in to the Command Center server using SSH.
2. Run the Command Center Backup and Restore Script by issuing the following command:

```
sudo /opt/sdconsole/scripts/backup-cc.sh -restore <path/location of your backup>
```

Restore a Passive Sensor

Steps

1. Log in to the Passive Sensor server using SSH.
2. Run the Passive Sensor Backup and Restore Script by issuing the following command:

```
sudo /opt/nids-docker/bin/backup-passive-sensor.sh -restore <path/location of your
backup>
```

Restore an Enterprise Command Center

Steps

1. Log in to the Enterprise Command Center server using SSH.
2. Run the Enterprise Command Center Backup and Restore Script by issuing the following command:

```
sudo /opt/ecc/scripts/backup-ecc.sh -restore <path/location of your backup>
```

6

Cybersecurity

Topics:

Security considerations

This chapter starts with an overview of IEC 62351 and IEC 62443, an international set of industrial cybersecurity standards which can be used as a framework to secure energy and utilities systems. Next, the document demonstrates the importance of core security concepts such as hardening and defense-in-depth. This chapter ends with additional cybersecurity recommendations and considerations for power system deployments. Each concept is given a brief overview and explanation of how it applies to the DVD solution components.

IEC 62351 overview

IEC 62351 is a series of cybersecurity standards for the smart grid, also known as power (energy) systems. This series of standards is specifically designed to help with the security of the TC 57 series of protocols (as shown in the gray box in the following figure). At a high level, IEC 62351 helps to secure both the data communications and the overall operations of power systems. The following list of IEC 62351 standards focuses on both general introductory materials and the security of the TC 57 series of protocols.

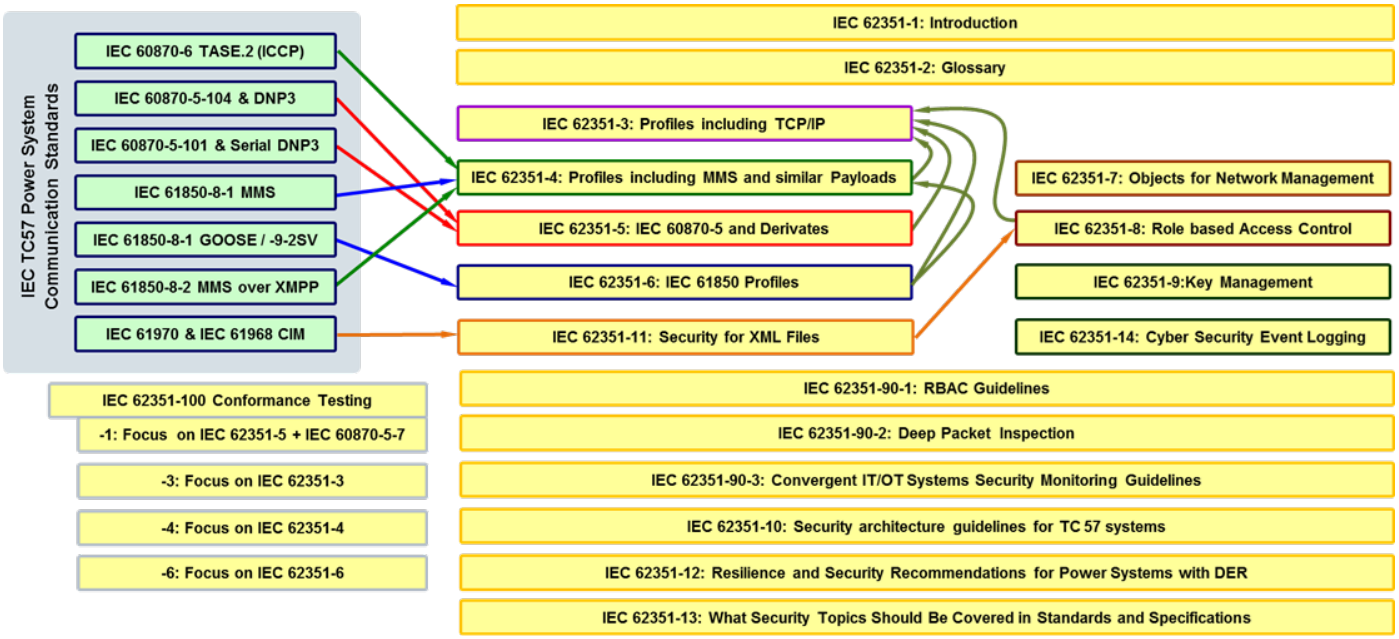


Figure 46. IEC 62351 series of standards mapped to IEC TC57 standards

- IEC 62351-1: Introduction—This provides the background for overall security in power system operations among other introductory information.
- IEC 62351-2: Glossary—Provides a glossary of terms and acronyms used throughout the series of standards.
- IEC 62351-3: Profiles Including TCP/IP—Data and communication security guidance for power system-based protocols that leverage TCP/IP communications. These include IEC 60870-6, IEC 60870-5-104, DNP3 over TCP/IP, and IEC 61850 over TCP/IP.
- IEC 62351-4: Profiles Including MMS and similar Payloads—Data and communication guidance to secure MMS and other similar payload types. Specifically, IEC 60870-6, IEC 61850-8-1, and IEC 61850-8-2.
- IEC 62351-5: IEC 60870-5 and Derivatives—Data and communication security guidance for IEC 60870-5-101, IEC 60870-5-104, and DNP3 protocols.
- IEC 62351-6: IEC 61850 Profiles—Data and communication security guidance for IEC 61850, specifically peer-to-peer profiles (IEC 61850 that does not use TCP/IP such as GOOSE).

Other than security guidance for energy specific protocols such as DNP3 and IEC 61850, IEC 62351 offers further general cybersecurity standards to keep the overall power system secure. The following are the additional standards in IEC 62351:

- IEC 62351-7: Objects for Network Management—Guidance on network and system management (for example, use of SNMP) for the power system network and information infrastructure.
- IEC 62351-8: Role based Access Control—Guidance on authorization such as users and roles with their associated permissions as it relates specifically to power system operations.
- IEC 62351-9: Key Management—Guidance on managing digital certificates and cryptographic keys.
- IEC 62351-10: Security architecture guidelines for TC 57 systems—Provides guidelines for a power system security architecture using various security controls.
- IEC 62351-11: Security for XML files—Guidelines for securely exchanging XML-based documents, which are used as part of IEC 61970 and in aspects of IEC 61850.
- IEC 62351-12: Resilience and Security Recommendations for Power Systems with DER—Targeted for Distributed Energy Resources (DER) systems with guidance on how to implement resilience and other cybersecurity considerations in these types of systems.
- IEC 62351-13: What Security Topics Should Be Covered in Standards and Specifications—Guidance for the personnel who develop the policies and standards for cybersecurity. Provides information about which security controls to include or what security topics to cover, especially as it pertains to power systems.
- IEC 62351-14: Cyber Security Event Logging—Guidance based on Syslog for the implementation of security logging in power systems.

The previous figure shows how the different power system communication standards (protocols) map to the different standards within IEC 62351. Further information on IEC 62351 can be found on the IEC 62351 Overview site.

IEC 62443 overview

There are multiple industry frameworks to help create and maintain a secure industrial control system (ICS) environment. Some of the industrial cybersecurity standards include IEC 62443 (International Electrotechnical Commission), NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection), and NIST 800-82 (National Institute of Standards and Technology - Guide to Industrial Control Systems (ICS) Security). IEC 62443 is a series of standards and technical reports that are developed by the International Society of Automation (ISA) and the IEC. This is the recommended framework to follow for the DVD for Energy Edge and was used as a reference when validating components of this solution. This series of standards provides a road map for improving the overall cybersecurity posture of an ICS environment. The scope of IEC 62443 is defined as any software, hardware, personnel, and policies that are involved in or have influence over the safety, security, and reliability of the ICS operations. Since ICS components can be physical systems, IEC 62443 stresses the importance of safety. Specifically, a compromise of these physical systems can lead to risk of human life or safety, damage to machinery, financial impact, and harm caused to the environment.

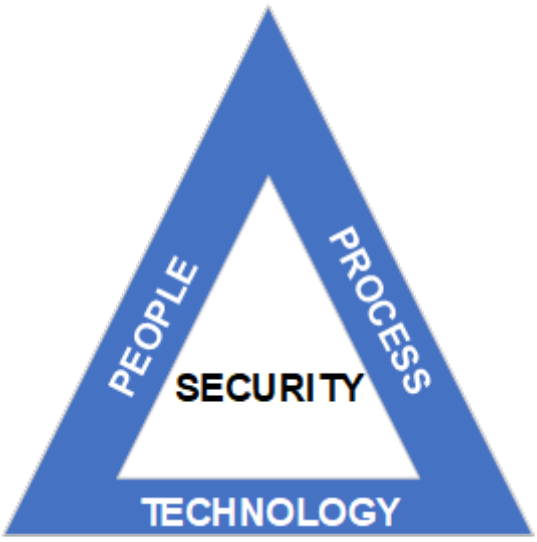


Figure 47. IEC 62443 Security Triad

IEC 62443 is broken up into documents and technical reports that are grouped into four families of standards: 1) General, 2) Policies and Procedures, 3) System, and 4) Component. Also, IEC 62443 defines roles of those who are involved in the overall operations of an ICS. These roles consist of the Asset Owner, Maintenance Service Provider, Integration Service Provider, and the Product Supplier. In addition, listed below are some of the fundamental concepts within IEC 62443:

- **Security program**—Specific to Part 2-1, this program covers details on policies and procedures, technical capabilities, and maintenance of personnel within ICS.
- **Risk Management**—Specific to Part 3-2, this program starts with a risk assessment to help understand the current level of risk within the ICS environment. Going through the risk assessment helps identify how to manage the risk through tasks such as identifying assets, Security Levels, and by establishing Zones and Conduits.
- **Security Levels**—Measure of how well an ICS component is protected from a certain level of threat and potential vulnerabilities. The following table gives an overview of each security level with some examples of potential threats and their associated skills and effort.

Table 6. IEC 62443 Security Level details

Security level	Protection against	Threat actor example	Threat actor skills	Threat actor resources	Threat actor means	Threat actor motivation
1	Casual or coincidental events or violations	Accidental, or casual	Simple or none	Low, usually an individual	Simple and sometimes non-intentional	Low or mistakes
2	Intentional violation by using simple means	Hacker	Low	Low, usually individual with resources	Simple	Low

Table 6. IEC 62443 Security Level details (continued)

Security level	Protection against	Threat actor example	Threat actor skills	Threat actor resources	Threat actor means	Threat actor motivation
3	Intentional violations using sophisticated means of attack	Terrorist or hacktivist	Moderate, ICS-specific	Moderate, can be a group	Sophisticated attack	Moderate
4	Sophisticated attack with extended resources	Nation-state	High, ICS-specific	High, can be highly trained teams	Sophisticated and coordinated attack	High

- **Zones and conduits**—Zones are groups of physical or logical assets that are grouped based upon criteria such as risk, function, or physical/logical location. Conduits are logical groupings of communications channels that share common security requirements when connecting zones.
- **Defense-in-depth**—A principle in which multiple layers of security are built into the overall system architecture so that if one level of security is broken, the rest of the system is not compromised. An example of this is if physical security is compromised, all communication over the network is encrypted so it cannot be easily read.

As mentioned previously, IEC 62443 is broken up into a family of standards that applies to different areas of industrial control systems. For example, IEC 62443-3-3 (System security requirements and security levels) describes overall requirements for an ICS-based system and mainly targets asset owners, suppliers, or integrators of the system.

Standards IEC 62443-4-1 and IEC 62443-4-2 are at the component level. Since this is at the component level, both standards provide more detailed and specific applicable controls. IEC 62443-4-1 is a standard that focuses on the security development life cycle requirements for control system suppliers.

IEC 62443-4-2 focuses on components within the ICS and is broken up into different categories such as embedded devices or host devices.

As an example, to align with IEC 62443-3-3, the organization must go through a certain set of steps. The steps can include the organization having identified their OT assets and conducted an organizational risk analysis to help identify criticality of system components. Once this is done, the organization can leverage this information to create zones and conduits. Security target levels (SL-T) can then be assigned to each zone and conduit, identifying how secure each should be. The organization assesses achieved security levels (SL-A) to then obtain a list of systems where the SL-A is less than the SL-T, which translates to the capability level (SL-C). The SL-C describes to what security level a system can be configured. If an SL-T cannot be achieved, the organization should consider compensatory controls, such as changing equipment.

Security Levels help narrow down the scope for what security controls to apply. The following table is an example of a set of controls and their associated security levels for a component's identification and authentication capabilities. This table shows how higher security levels, which are mapped to components or systems with higher criticality levels, apply more stringent security controls. A higher security level (SL-2 or SL-3 in this case) assumes application of lower security levels. In summary, this section aims to provide an overview of the different components of IEC 62443 and an introduction of how to understand it and start to leverage the family of standards.

Table 7. Example of identification and authentication security controls mapped to security levels

Security level	Example requirement	Example control
1	Identification and authentication of all users	All users are identified (example: username) and then authenticated (example: password) prior to gaining access to the system.
2	Users must be uniquely identified and authenticated	Each user has a unique identifier such as a username that can only be used for a single user.
3	Use multifactor authentication	All users must be authenticated using multifactor authentication such as providing something they know (example: password) and something they have (example: token).

Defense-in-depth

If there is only one defense mechanism within the network, and it is compromised, the rest of the environment is potentially exposed to the threat. To avoid these types of scenarios, a defense-in-depth architecture is deployed within the network. Defense-in-depth includes implementing multiple security controls such as training programs or technical controls. If one line of defense is compromised, the next layer within the architecture is there to stop or to slow down the attack from spreading

further. The following figure illustrates the different layers and gives some examples of what defense techniques can be implemented at each layer.

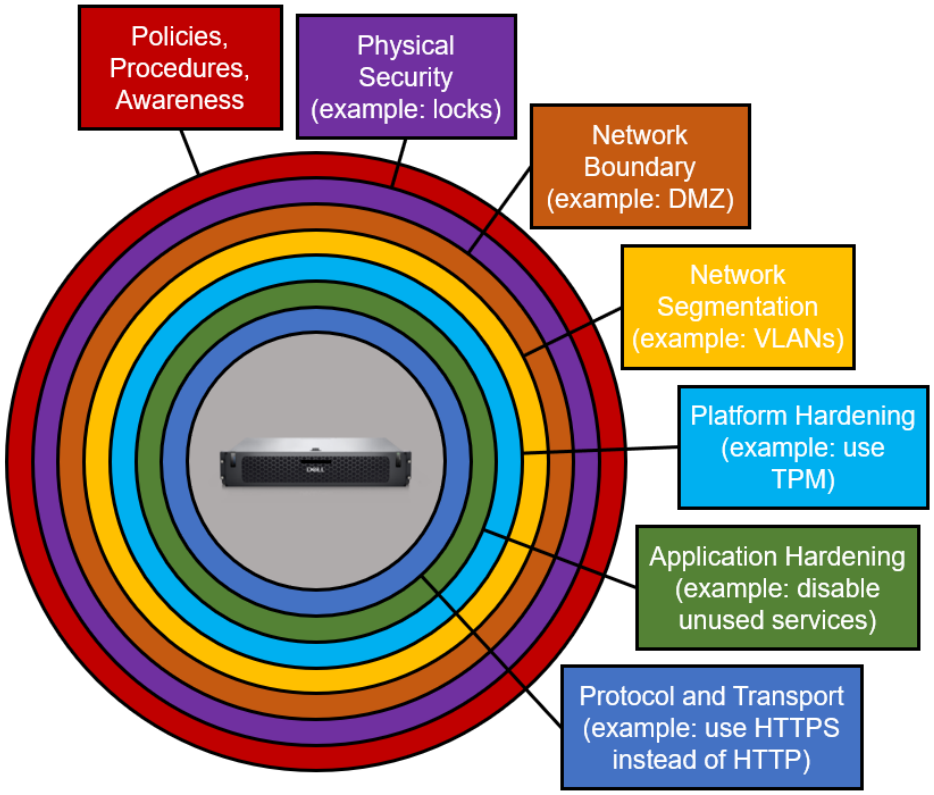


Figure 48. Defense-in-depth layers

The DVD solution has been validated to support the defense-in-depth principal. An example of this is how all software components are validated for hardening while the solution also validates functionality with a secure architecture. These two security practices help to create multiple layers of security around the solution. For instance, if a threat actor finds a way through the network boundary, such as a demilitarized zone (DMZ), then the use of authentication, encryption, and authorization all help to mitigate any further potential compromises.

Network segmentation

This solution has been validated to run with a certain set of firewall access-list rules that restrict the flow of data between the control center and substation networks to only allow traffic for basic functionality between ISV components and for access to ISV resources. Users must consider any unique requirements for their environments, as well as the list of expected ports, protocols, and services for each software component in the solution. Additionally, it is essential to confirm and test different use cases once network segmentation has been implemented. It is also recommended to define a baseline of expected traffic to further enhance these rules or define additional rules.

In Information Technology (IT) environments, the DMZ is used to segment between external and internal networks to prevent direct access between the two network zones. The DMZ can host publicly accessible services such as web servers. The same principal can be applied in industrial based networks. This can be achieved using firewalls and technologies like proxies or VPN tunneling.

Hardening

Hardening a device, system or component can greatly help reduce the attack surface. An example of physical hardening is to seal or monitor ports on a server. Also, hardening software can be done by disabling unused or unnecessary ports and services (for example, disabling SSH when not being used).

The following are some of the security configuration settings that are validated in this DVD:

- Identification and authentication of users and integration with central authentication servers (for example, Active Directory)
- Authorization for users based on Role-Based Access Control (RBAC)
- Logging and auditing settings
- Using secure versions of protocols (for example, using HTTPS instead of HTTP)

NOTE: This DVD does not cover all possible security configuration settings. Validated security settings were chosen based on the overall use cases for this DVD.

Platform hardening

This section covers hardening details for the different platform offerings of the solution. This includes PowerEdge security considerations, which can be applied to the XR12, as well as security configuration details for the different VMware components.

PowerEdge security overview

The PowerEdge team continuously evolves the security controls, features, and solutions to meet the ever-growing threat landscape. A key security foundation is Silicon Root of Trust. The White Paper: Cyber Resilient Security in Dell PowerEdge Servers details the security features built into the PowerEdge Cyber Resilient Platform, many of which are enabled by the integrated Dell Remote Access Controller (iDRAC9). Many new security features have been added, which span from access control to data encryption to supply chain assurance. These features include:

- Live BIOS scanning
- UEFI Secure Boot Customization
- RSA SecurID Multi Factor Authentication
- Secure Enterprise Key Management (SEKM)
- Secured Component Verification (SCV)
- Enhanced System Erase
- Automatic Certificate Enrollment and Renewal
- Cipher Select
- Commercial National Security Algorithm (CNSA) support

Further details on iDRAC security can be found in the iDRAC9 Security Configuration Guide.

VMware vSphere security overview

The *VMware vSphere Security Configuration Guide* is the baseline for hardening and auditing guidance for vSphere itself. Started more than a decade ago, the SCG has served as a reference for vSphere administrators as they work to protect their infrastructure.

Dell Technologies has validated several test cases to develop a set of vSphere validated security configuration settings. There are test cases for deployments with and without a vCenter-managed deployment. This is important to note, as some ESXi configurations are not applicable when managed by vCenter. The goal is to provide validated security settings that can be applied to the DVD deployment to provide simplified guidance.

For more information, see the following documents:

- VMware vSphere Security Configuration Guide 7
- Dell Validated Design Security Configurations for Edge Solutions using VMware vSphere v7.0 - Configuration Guide
- VMware vSphere Security Configuration Guide 8
- Dell Validated Design Security Configurations for Edge Solutions using VMware vSphere v8.0 - Configuration Guide

VMware vSAN encryption

To further secure your data, encrypt data in transit in your vSAN cluster and encrypt data at rest in your vSAN datastore. vSAN can encrypt data in transit across hosts in the vSAN cluster. Data-in-transit encryption protects data as it moves around the vSAN cluster. vSAN can encrypt data at rest in the vSAN datastore. Data-at-rest encryption protects data on storage devices, in case a device is removed from the cluster. When you enable data-at-rest encryption, vSAN encrypts everything in the vSAN datastore. All files are encrypted, which protects all VMs and their corresponding data. Only administrators with encryption privileges can perform encryption and decryption tasks. For more information, see Using Encryption in a vSAN Cluster.

OS hardening

Consider hardening the host OS as it presents possible additional vulnerabilities to the network. In general, it is recommended to run the minimum required services and applications to support the required functionality and help reduce the attack surface. This can be done by creating baselines and by conducting periodic port and OS scans to obtain a list of open ports and services. Conducting periodic vulnerability scans is also highly recommended as it identifies any potential vulnerabilities that are related to the OS itself or any vulnerabilities that are introduced by underlying applications or its dependencies.

There is a common set of considerations for each type of OS to keep the environment more secure and to reduce the potential attack surface. The items listed below are some general considerations for securing an OS:

- Ensure that only those who are required have access to the OS.
- Ensure that any user or service account has the minimum set of privileges necessary to carry out the required tasks.
- Use strong passwords.
- Configure host OS firewall rules (access lists) for managing traffic coming into and leaving the host.
- Integrate authentication with an existing central authentication system when possible.
- Keep up with the latest patches and ensure that they are applied only after being tested and approved.
- Disable unused or unnecessary services.
- Configure the system to use NTP.
- Configure logging settings and integrate with a central logging system or security information and event management (SIEM) when possible.
- Conduct credentialed vulnerability scanning regularly (per organizational policy).
- Deploy endpoint security software, such as anti-virus, to detect potential threats on the OS.

NOTE: There could be new vulnerabilities since the tests were conducted for this solution. It is highly recommended for the organization to conduct their own vulnerability assessment after implementing the DVD solution.

Substation VPN

Connectivity between substations and the control center often requires connectivity over WAN connections. In many cases, the WAN connections can pose a major risk to the substation because of potentially untrusted activity on the WAN network. To defend against threats from outside the substation network, a secure architecture using a VPN tunnel has been validated for this solution. The VPN tunnel encrypts traffic between the substation and the control center, ideally terminating at the DMZ network of each location. The VPN tunnel protects any data that is transmitted over the WAN and it also applies best-practice routing using a DMZ so that there is no direct communication between the substation and external networks. The following figure illustrates an example of the validated secure architecture with both ABB ZEE600 and Forescout eyeInspect.

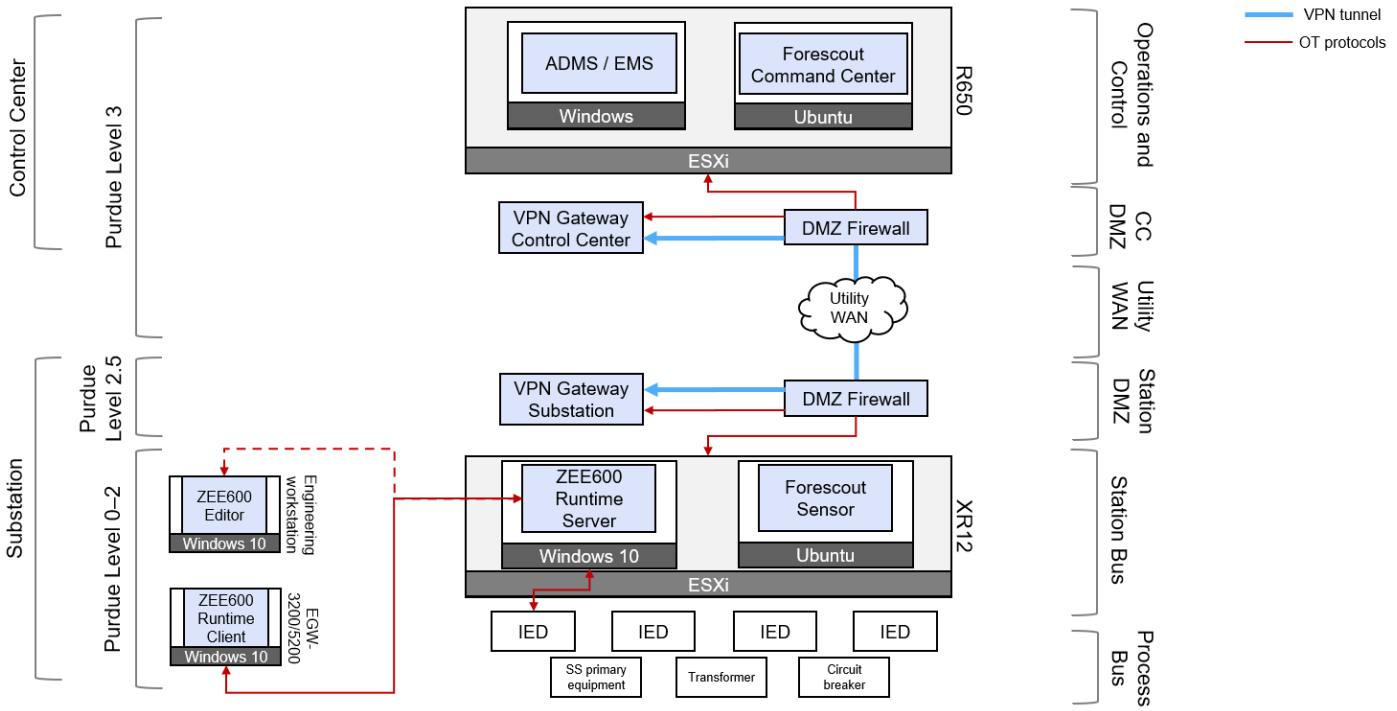


Figure 49. Security architecture

The following table lists firewall rules that can be applied at the substation DMZ firewall to allow the VPN traffic to establish between the VPN endpoints.

Table 8. Firewall rules

Description	Source network/Host	Source device	Destination network	Destination device	Port
Allow the substation DMZ VPN client to connect to control center DMZ VPN server to establish a VPN tunnel.	Substation	Substation VPN client	WAN	Control center VPN server	TCP/ UDP ###[a]

a. The destination port and protocol depend on the vendor-specific VPN implementation.

NOTE: The firewall rules that are shown here assume that routing is configured so that control center and substation hosts are routed using the VPN tunnel to reach each other. These rules and validated architecture also assume that the VPN server at the control center has a WAN interface and that the VPN client at the substation is hosted in the substation DMZ. Actual deployments vary, but the same architecture can be applied by modifying source/destination networks or by implementing other network techniques like NAT.

Another important factor to consider is the routing between the substation and control center. Traffic originating in the control center must know to use the VPN server to reach the substation network. The same is true for the hosts in the substation network, where traffic must be forwarded into the VPN client at the substation to be tunneled to the control center.

Lastly, firewall rules also have to be added in this architecture to allow traffic from the control center into the substation, and in reverse for traffic originating from the substation destined for the control center. To support these use cases, see the DMZ sections in the following ABB and Forescout cybersecurity sections.

Additional power system security considerations

Power systems are unique in how they function and communicate. With this fact in mind, there are some security best practices to consider when implementing security in these types of deployments.

- Ensure that cybersecurity governance is in place to support activities such as risk management and to help meet regulatory compliance requirements. It is especially important that organizational leadership is aware of these requirements and support these activities so that they are implemented successfully.
- Restrict Internet access to deployed solutions or implement the solution in a way that Internet connectivity is not required. If necessary, develop procedures or workarounds to help disable Internet connectivity.
- Implement proper logging and monitoring for the solution. Ideally, implement a central logging system to aggregate all logs. Provide and collect details such as what is logged and where it is logged and plan for log retention such as archiving.
- Implement integrity checks for the processes and software that are a part of the solution. For software, which includes firmware as well, verify that the software is authentic and has not been tampered (for example, cryptographic integrity checks). Follow the same recommendation for operational processes, such as when implementing third-party technology into the network to help verify its supply chain integrity.
- Consider physical security for the location of the solution in the power system (substation). This includes implementing controls like monitoring, badged access, and locks for server racks.
- Consider the software life cycle of the solution. For example, determine if the developer of the software solution follows security life cycle best practices. Learn about which security standards the supplier of the solution follows (for example, OWASP). It can also be helpful to verify that the solution supplier follows best practices such as conducting independent audits of their cybersecurity posture.
- Verify that any implemented solution follows security best practices like user access and the principal of least privilege. Additionally, verify that the solution can function in a secure architecture where only authorized communications are allowed to and from the solution.
- Consider the security of the information systems involved with the solution. Examples include implementing data replication, consideration for backup and recovery, and other considerations like operational monitoring.
- Consider whether the supplier of the solution has an incident management plan. Learn about the incident management of the supplier, especially for notifications and remediation processes for any incidents that may occur.
- Verify that the supplier of the solution has a valid vulnerability management framework and explains how to monitor the output so that vulnerabilities can be mitigated as soon as possible.
- Learn about the solutions patch management process and how to ensure the integrity of all patches that are applied to the software.
- Ensure that the solution undergoes appropriate cybersecurity testing, such as penetration testing, so that vulnerabilities are properly identified.
- Verify that the solution supplier has all required documentation and support, as this may be critical to compliance requirements.

Cybersecurity with ABB ZEE600

Cybersecurity is a critical consideration when deploying any new computing technology. The physical environment, system criticality, hardware, and software that is used should all be considered when deciding what to deploy and how to securely deploy it.

This section covers security considerations when deploying ABB ZEE600 in a utilities substation environment.

NOTE: Keep in mind that implementing security features, like encryption, can affect system performance.

Application hardening

Authentication

Authentication-focused security controls involve any feature that addresses the issue of a user identifying themselves prior to accessing or editing a system.

ABB's ZEE600 has several features to help add authentication measures to your deployment.

Local users

Locally created and managed users can be added to a ZEE600 project in the **User Administration** section of the Editor. These can be configured without any dependence on external systems, which can be the best choice if those systems are not configured, or if they cannot be reliably reached by a remote deployment.

Local users can easily be created in ZEE600, and these users have several settings that can be leveraged to secure the deployment:

- A user's credentials can be given an expiration—if a user only requires temporary access for a specific task, take advantage of this feature.
- Credentials can be locked—if a user's credentials are not needed for a period of time, but will be needed in the future, use this setting.
- Username and password rules—ZEE600 enforces that user names must be unique (which is helpful for accounting) and enforces password requirements to prevent using insecure passwords.
- Credentials can be deleted—any credentials that have no future use should be deleted to prevent unauthorized access.

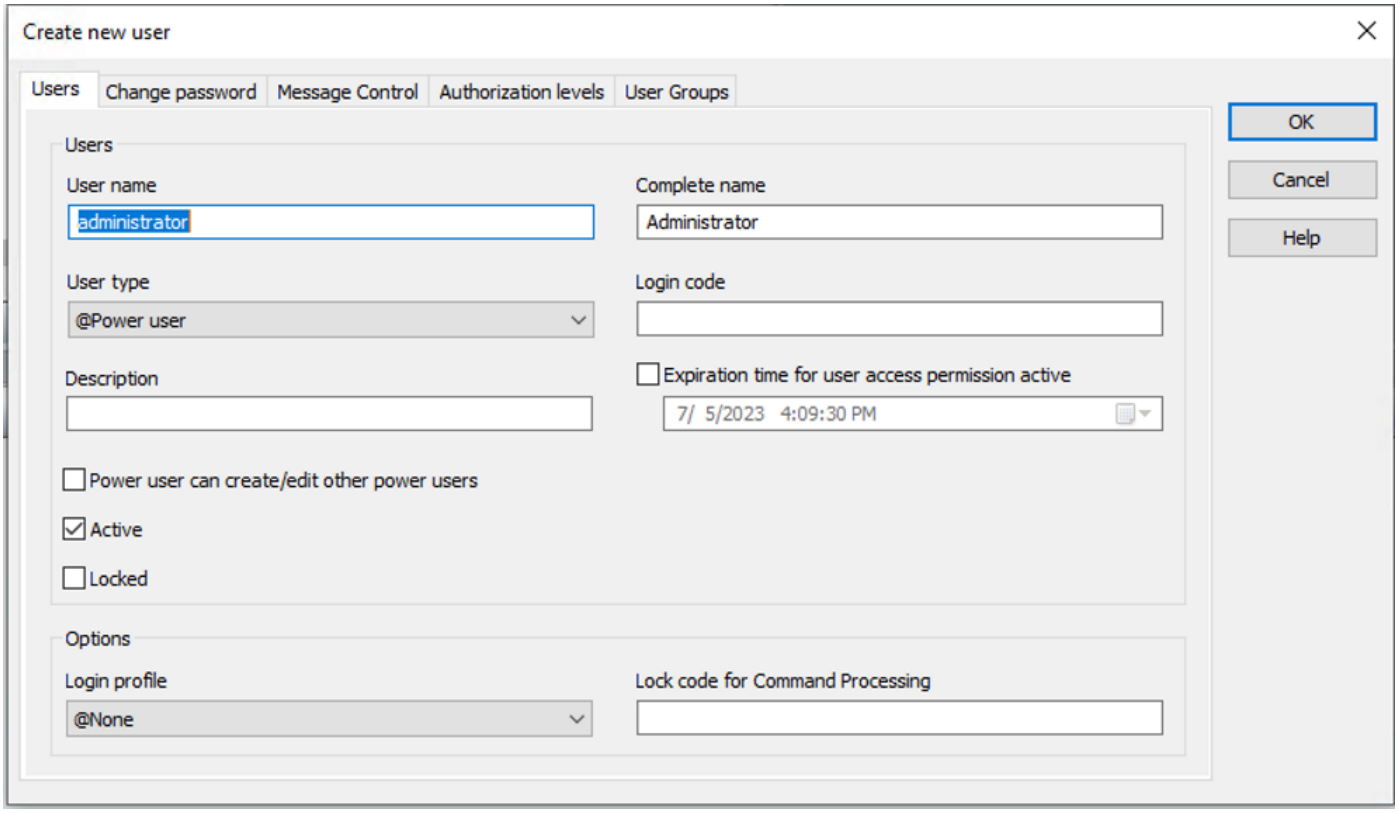


Figure 50. Create new user window

Active Directory integration

ZEE600 supports an Active Directory (AD) integration. This allows the ZEE600 Runtime to use the users and groups that are already managed in an active directory system for login, rather than requiring management of a separate set of users.

Users, passwords, and their assigned roles are all inherited from the AD server. This offers several advantages over a locally managed user set, and is typically recommended when feasible.

Benefits include:

- Each user only needs to remember their AD credentials, rather than a new set of credentials. This reduces the chance that a password needs to be written down or otherwise kept in an unsecure manner.
- Users who are created or deleted in the AD server automatically have their ZEE600 access created or deleted accordingly.
- Administrators and security personnel can view, audit, and manage credentials in a single central location.

To configure the connection to an AD server, the Runtime host must be a member of the domain, and AD details are pulled automatically from the provided domain. The AD configuration options are set by selecting the target project in the Editor, and navigating to the **Active Directory/AD LDS** section of the **Project Properties**.

Session management

Session management features enforce that a user must re-authenticate after a certain period of time, based on the configuration. This reauthentication protects against a user forgetting to log out, accidentally leaving the application unattended, and so on.

ZEE600 projects have an automatic logout time parameter. By default, this is set to 5 minutes, but is configurable for each project in the **Project Properties** area. After the user is inactive for the configured time, the user is automatically logged out, and must reenter their credentials.

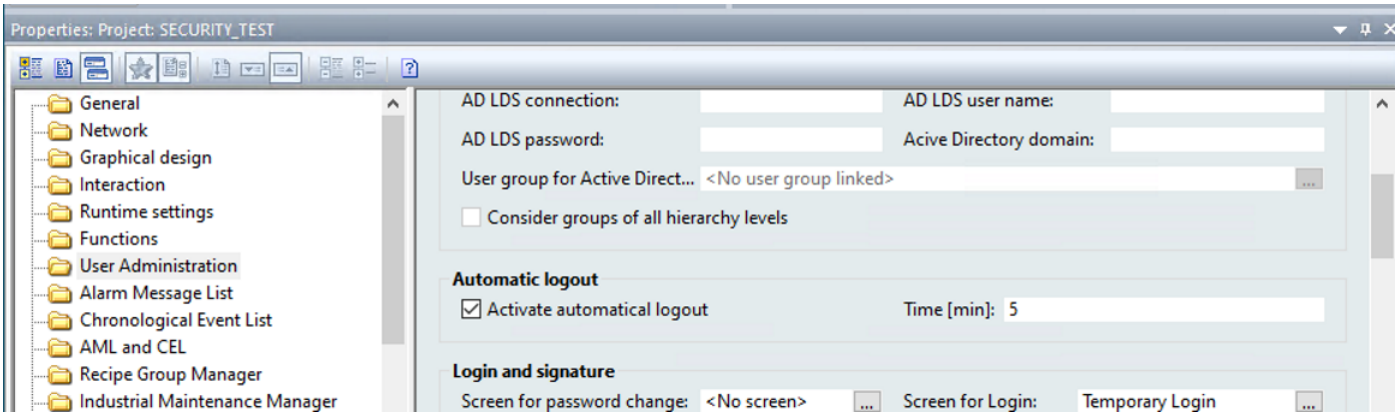


Figure 51. Activate automatic logout

To prevent leaving an authenticated session open, when a user is finished with their Runtime session, they can use the integrated logout button or they can close the Runtime to end their session.

Authorization and control

By considering authorization and control features, you can ensure that only authorized users have access to specific data and settings and ensure that each user only has access to the information that they require for their role, thus abiding by the principal of least privilege.

Several of the most common features offered by ZEE600 to address proper authorization are discussed here.

Default Runtime access

By default, when a ZEE600 Runtime is launched, no user is logged in and most views and actions are available. To restrict this access, two steps should be taken.

First, ensure that nothing is available to a user before logging in. One way to accomplish this is to set the login screen as the start screen that is shown on Runtime startup. Then credentials must be provided before any dashboards, status information, or actions are available.

Second, ensure that all functions are reviewed to ensure the proper authorization level is set, restricting the feature to only those who require access. Continue reading for more information about authorization levels.

User groups

User groups are used to assign permissions to users based on their access requirements. User groups are typically created based on roles or tasks. The **Operators**, **Maintenance**, and **Administrators** user groups are created automatically in all ZEE600 projects.

A user can be a member of multiple user groups, and they inherit the permissions of each group. User groups are assigned specific authorization levels, which specify what members of the user group can see and do. It is recommended that a user is only assigned to groups that they must be a part of and nothing more.

Authorization levels

Authorization levels are permission codes that are assigned to specific actions within a ZEE600 project. Each function, including functions that open screens, is assigned a single authorization level.

Only users with the authorization level assigned directly to them or who are members of a user group with the authorization level assigned to the group may execute the function. This is an effective way to limit access to dashboards or specific settings to only specific users or user groups.

To make managing authorization levels easier, they can be named. This simplifies keeping track of what permissions are associated with a particular authorization level.

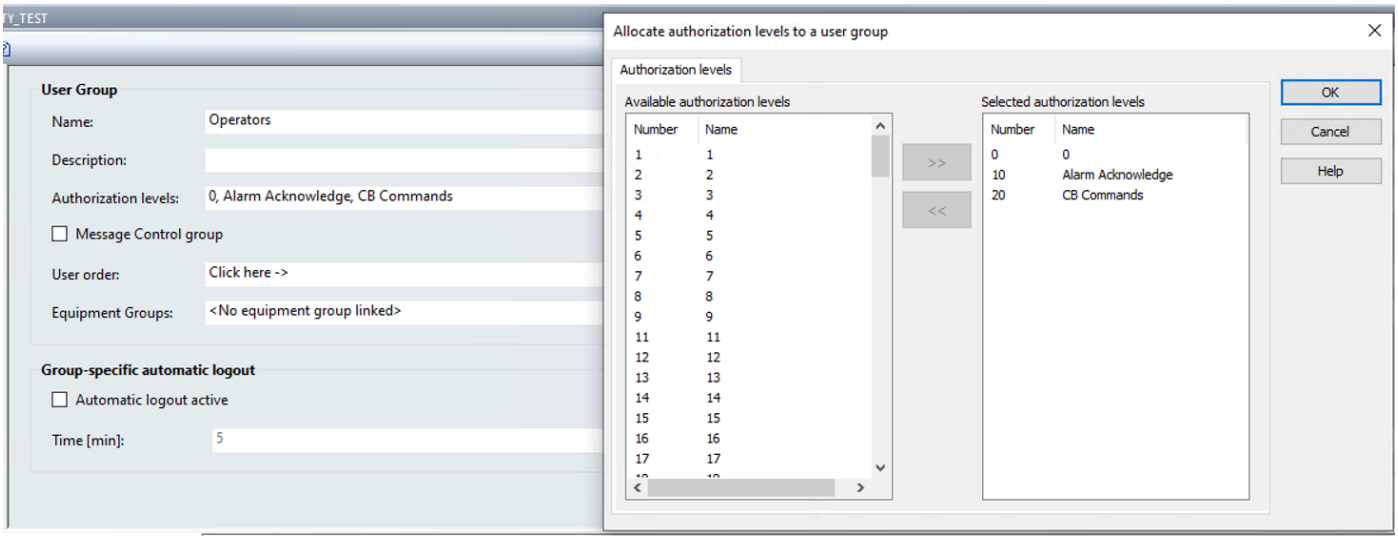


Figure 52. Authorization levels

Confidentiality

Confidentiality in cybersecurity addresses concerns of data and other transmissions being exposed to unintended persons. It applies to both the movement of information between systems and to the accessibility of confidential data within a system.

Securing the transmission of data and commands is a vital part of ensuring confidentiality. This DVD employs a VPN to encrypt transmissions between a substation and a centralized control center. Beyond that, ABB ZEE600 offers options to secure data at the application level, if the protocol supports a secured option.

For example, ZEE600 supports secured OPC UA communications from the OPC UA server hosted in a ZEE600 Process Gateway to an OPC UA client hosted in the Command Center. The security options include the use of **Sign** or **Sign and Encrypt**, and the option to require non-anonymous connections.

NOTE: If using an encrypted OT protocol within the station bus, Forescout eyeSight is not able to obtain full information about the traffic.

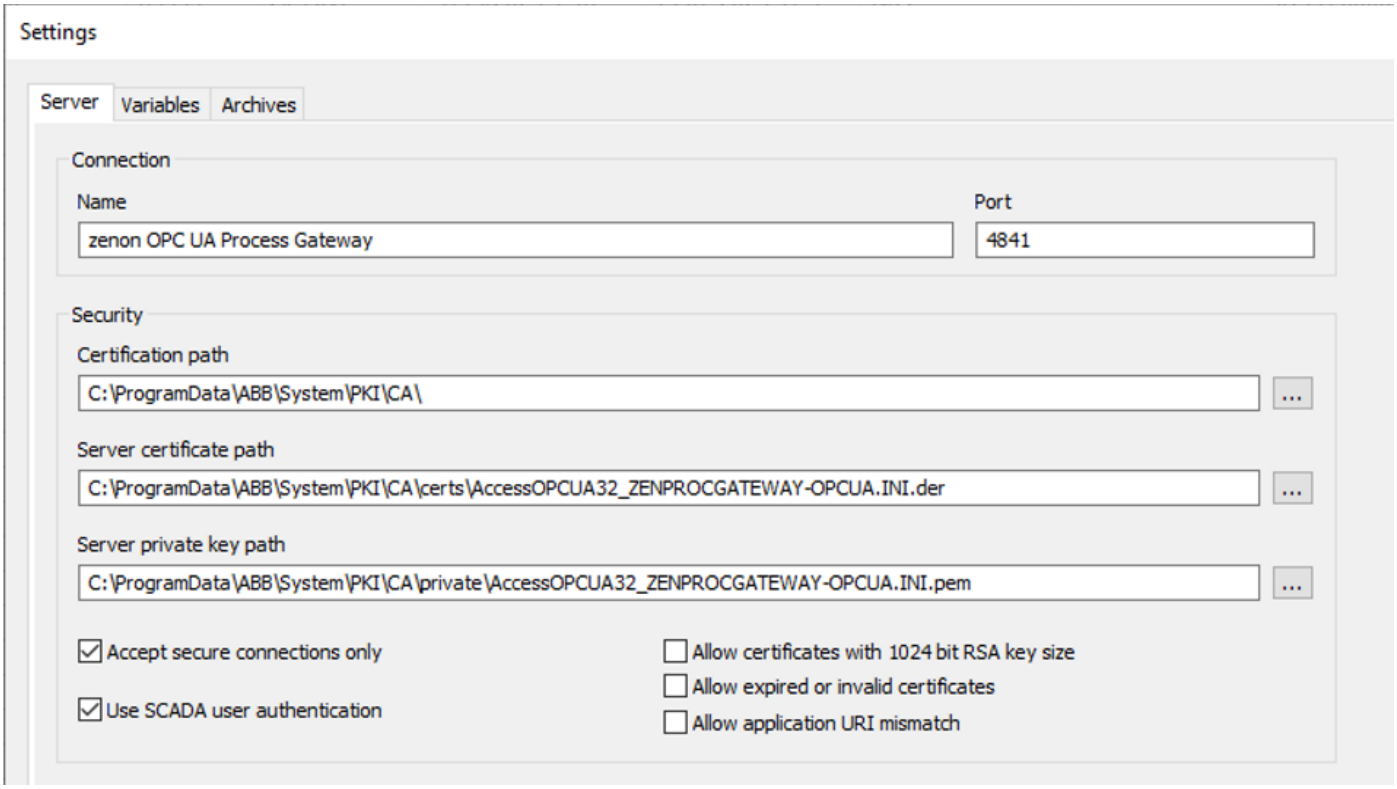


Figure 53. Security configuration in Settings

Accounting

In terms of cybersecurity, accounting allows for the tracking of user actions and system activity, which can be vital information in building processes and performing investigations.

NTP server connection

An important aspect for tracking actions on a production system is ensuring that the timestamp that is associated with an event is meaningful. Syncing all systems to a centralized clock ensures that all applications, operating systems, and peripherals are tracking actions in a reliable and standardized way.

ZEE600 supports syncing with an NTP (network time protocol) server. By configuring the Windows OS host to sync with an NTP server, you can ensure that the ZEE600 application is using the same time as all other systems that are part of the industrial deployment. Among other timestamps, those on the ZEE600 audit log can be correlated to actions in other systems, like computer logins, badge swipes, and so on.

Local audit log

An audit log is a system that logs user and systems actions. In the ZEE600 Runtime, the chronological event list (CEL) captures most of these actions, such as a user logging in or logging out and the Runtime starting or stopping. Actions that are related to alarms, like a user acknowledging an alarm, are visible on the **Alarms** page.

Both the Alarms and CEL functionality and pages are prebuilt as part of creating a ZEE600 project. What information and how it is displayed can be further configured based on the needs of the deployment.

See Chronological Event List (CEL) for more information.

Syslog integration

To take the standardization of logging across a system to the next level, consider implementing a centralized syslog server. All applications that support a syslog server integration can send their event logs to a single location, where alerts can be configured, patterns tracked, and events analyzed for deeper insights.

ZEE600 supports a syslog integration using the process gateway functionality.

See Syslog for more details.

DMZ architecture and validation

A demilitarized zone is a vital buffer to insulate the substation from unwanted network intrusions. It is recommended to implement a firewall at this external interface to limit traffic to only expected and approved sources and protocols.

Architecture

The Security architecture figure shows the DVD architecture and its security components.

VPN tunnel

An important feature of this architecture is the VPN tunnel which is used to encrypt traffic between the substation and the control center. Even in the case where an OT protocol does not support its own secure connection, the VPN can provide the needed confidentiality.

DMZ firewall

Of particular importance is the firewall that is hosted on the substation DMZ. All traffic initiated externally is routed through this firewall, and it is the first line of defense against intrusion. It is important to configure this DMZ such that all necessary traffic, and only intended traffic, is permitted through.

In the following section, see a list of potential firewall rules to be implemented for ZEE600 to function properly. Consider that each deployment has its own required communications, and the list may not be representative of your use case.

DMZ firewall rules

NOTE: The firewall rules that are shown here are illustrative using default ports. Part of a defense-in-depth approach to security is to avoid using default ports.

Table 9. DMZ firewall rules for ABB ZEE600

Description	Source network	Source device	Destination network	Destination device	Port	Application
Allow the DNP3 client at the control center to connect to the DNP3 server at the substation.	Control Center	DNP3 client	Station bus	DNP3 server (ZEE600 process gateway)	TCP 20000	TCP
Allow the OPC UA client at the control center to connect to OPC UA server at the substation.	Control Center	OPC UA client	Station bus	OPC UA server (ZEE600 process gateway)	TCP 4841	TCP
Allow the IEC 104 client at the control center to connect to IEC 104 server at the substation.	Control Center	IEC 104 client	Station bus	IEC 104 server (ZEE600 process gateway)	TCP 2404	TCP

NOTE: These firewall rules assume that the VPN endpoint in the substation does not use network address translation (NAT). If it does, the source is within the DMZ.

Cybersecurity with Forescout eyeInspect

As technology evolves, so do the threats that can compromise the integrity and reliability of a power distribution network. Cybersecurity at a substation is to protect and safeguard critical infrastructure that facilitates the distribution and transmission of electricity. It prevents power disruption and unauthorized access, detects potential threats, and helps to maintain the reliability and stability of the power grid that we depend on.

Forescout eyeInspect offers end-to-end cyber resiliency for your operational technology (OT) network with the following features:

- Comprehensive assets risk framework
- Ongoing automated asset management
- Compliance monitoring
- Threat detection

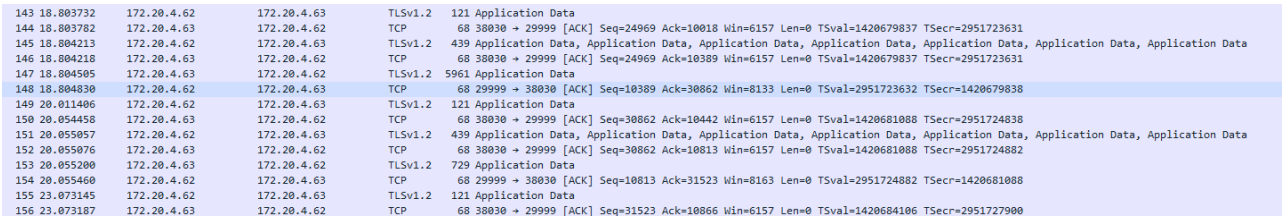
Confidentiality

OT personnel must safeguard confidential data such as network configurations, security protocols, and other operational details from unauthorized access at substations. If such sensitive data was to be leaked, it could compromise the integrity of the substation operations.

Secure connection between CC and sensor

To ensure the communication between the command center and sensors (end-to-end), networks are encrypted to prevent eavesdropping and data tampering. Using security protocols like TLS can effectively safeguard against malicious activities. Utilities like Wireshark and tcpdump can be used to validate whether critical network traffic is encrypted.

Implementing confidentiality enhances the privacy, security, and reliability of interactions between devices.



143	18.803732	172.20.4.62	172.20.4.63	TLSv1.2	121 Application Data
144	18.803782	172.20.4.63	172.20.4.62	TCP	68 38030 → 29999 [ACK] Seq=24969 Ack=10018 Win=6157 Len=0 TSval=1420679837 TSecr=2951723631
145	18.804213	172.20.4.62	172.20.4.63	TLSv1.2	439 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
146	18.804218	172.20.4.63	172.20.4.62	TCP	68 38030 → 29999 [ACK] Seq=24969 Ack=10389 Win=6157 Len=0 TSval=1420679837 TSecr=2951723631
147	18.804505	172.20.4.63	172.20.4.62	TLSv1.2	5961 Application Data
148	18.804830	172.20.4.62	172.20.4.63	TCP	68 29999 → 38030 [ACK] Seq=10389 Ack=30862 Win=8133 Len=0 TSval=2951723632 TSecr=1420679838
149	20.011406	172.20.4.62	172.20.4.63	TLSv1.2	121 Application Data
150	20.054458	172.20.4.63	172.20.4.62	TCP	68 38030 → 29999 [ACK] Seq=30862 Ack=10442 Win=6157 Len=0 TSval=1420681088 TSecr=2951724838
151	20.055057	172.20.4.62	172.20.4.63	TLSv1.2	439 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
152	20.055076	172.20.4.63	172.20.4.62	TCP	68 38030 → 29999 [ACK] Seq=30862 Ack=10813 Win=6157 Len=0 TSval=1420681088 TSecr=2951724882
153	20.055200	172.20.4.63	172.20.4.62	TLSv1.2	729 Application Data
154	20.055460	172.20.4.62	172.20.4.63	TCP	68 29999 → 38030 [ACK] Seq=10813 Ack=31523 Win=8163 Len=0 TSval=2951724882 TSecr=1420681088
155	23.073145	172.20.4.62	172.20.4.63	TLSv1.2	121 Application Data
156	23.073187	172.20.4.63	172.20.4.62	TCP	68 38030 → 29999 [ACK] Seq=31523 Ack=10866 Win=6157 Len=0 TSval=1420684106 TSecr=2951727900

Figure 54. Example of PCAP with TLS protocol

Authentication

Authenticate users and services to verify their identity when authenticating to Command Center. This ensures that the authenticating entity is who they claim to be. Various authentication techniques like passwords can be used to validate the identity of the authenticating entity. After authentication, user authorization is checked to ensure that users can access only the resources that have been assigned. Users are not able to access additional resources beyond what they have been authorized for. This helps maintain security and control over sensitive information and functionalities.

User creation

Create user accounts or profiles with the appropriate roles to ensure only the authorized personnel have access to the system .

Command Center allows creating user accounts with strong passwords, and other security considerations enhance the protection of sensitive data and systems. Properly implementing authentication also improves user experience and maintains security compliance.

Federated users (LDAP)

Authenticate user accounts using LDAP protocol from Command Center to facilitate federated identity and access control in a centralized manner. LDAP is commonly used for tasks that are related to identity and access management, user authentication, and directory services.

LDAP allows for centralized management of user accounts, attributes, and access rights across all connected services, reducing discrepancies and errors.

SSO

Authenticate users to Command Center and allow users to log in with a single set of credentials to gain access to multiple applications and services at multiple locations. This eliminates the need to repeatedly enter login credentials and enhances user experience and security.

SSO allows secure remote access and provides a seamless login experience. Users only need to remember one credential to access multiple applications. Moreover, it provides logs and audit trails of user activities.

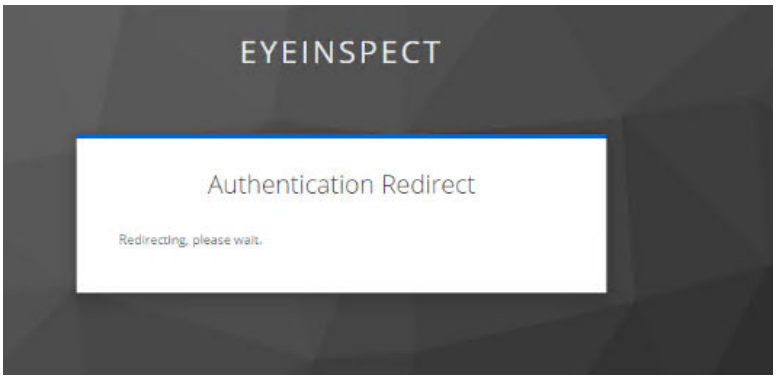


Figure 55. SSO redirect

Password policy

Command Center allows administrators to set rules and guidelines that establish how passwords are managed with enforcement policies. When a user creates their password, it must meet the defined requirements (for example, minimum length, special characters, complexity, uniqueness, and so on).

A strong password policy can reduce the risk of compromise, enhance security, and adopt best practices and meet compliance requirements. Forescout allows administrators to modify password policies, as shown in the following figure.

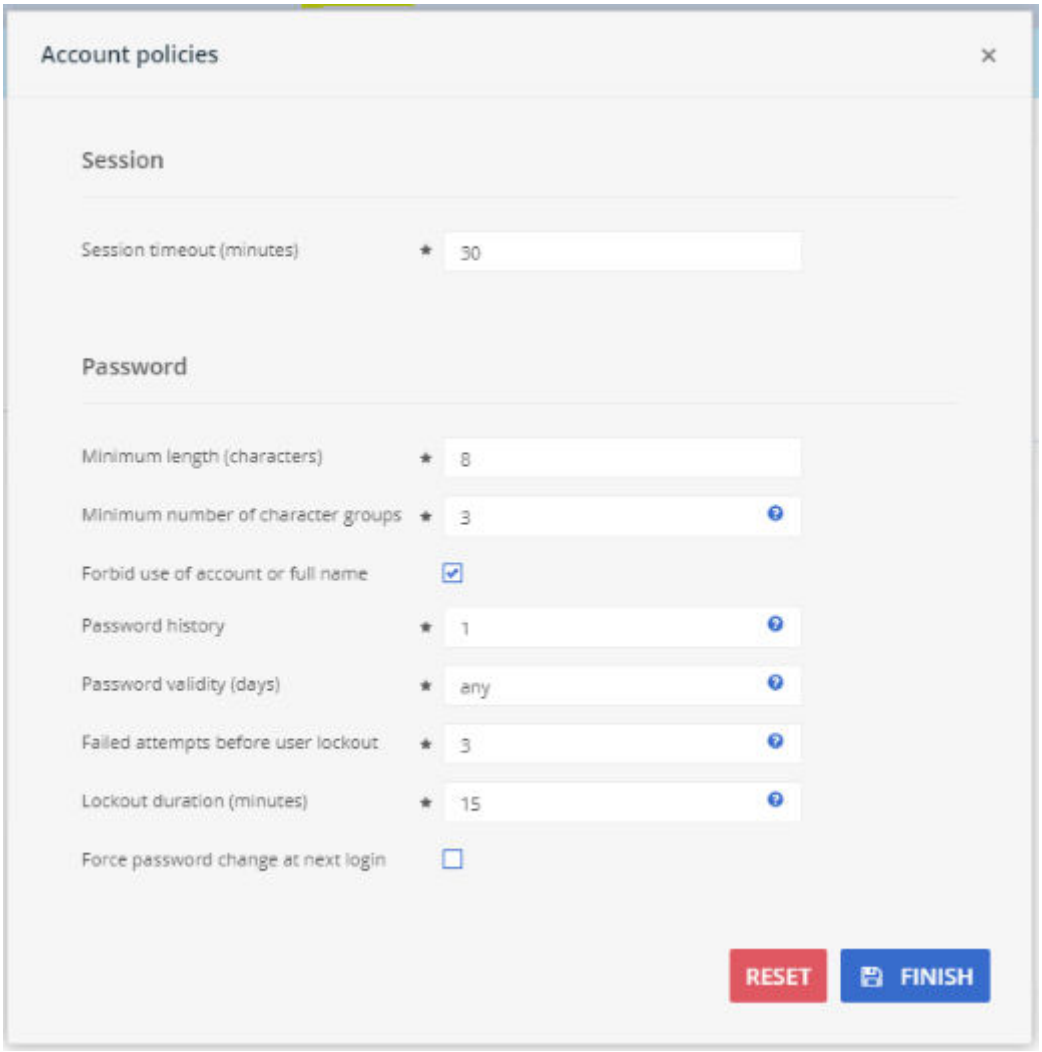


Figure 56. Account policies

Authentication feedback

This feature responds to users during the authentication process to inform them that their login attempt is unauthorized and provides guidance for how to proceed.

This informs the user of the potential errors before they attempt to log in again. Forescout is validated to provide the appropriate authentication feedback without exposing too much information.

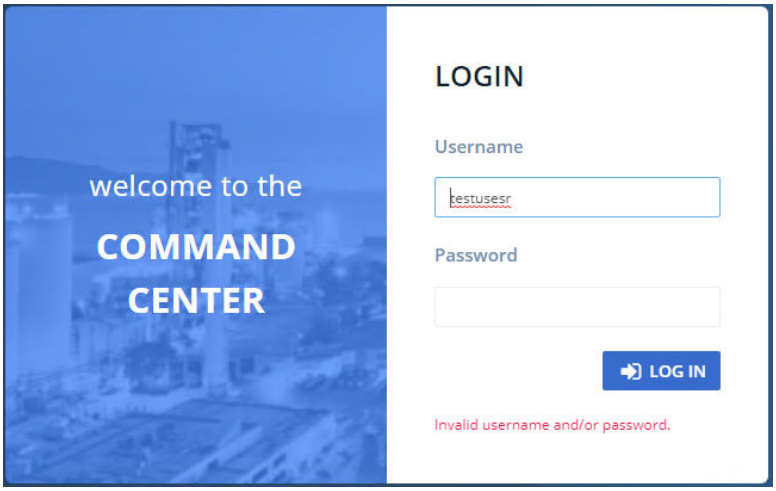


Figure 57. Example of incorrect credentials feedback

Authorization

Authorization is the process of granting or denying access rights to the systems based on the user/service credential. This ensures that only the relevant access is allowed based on defined roles.

User roles and privileges

Create roles and assign privileges for access control. This defines and manages the level of access and actions that users can perform. This helps to maintain security and manage the data integrity of the system.

With user roles and privileges, Forescout administrators can customize access to the individual to prevent unauthorized access to sensitive data.

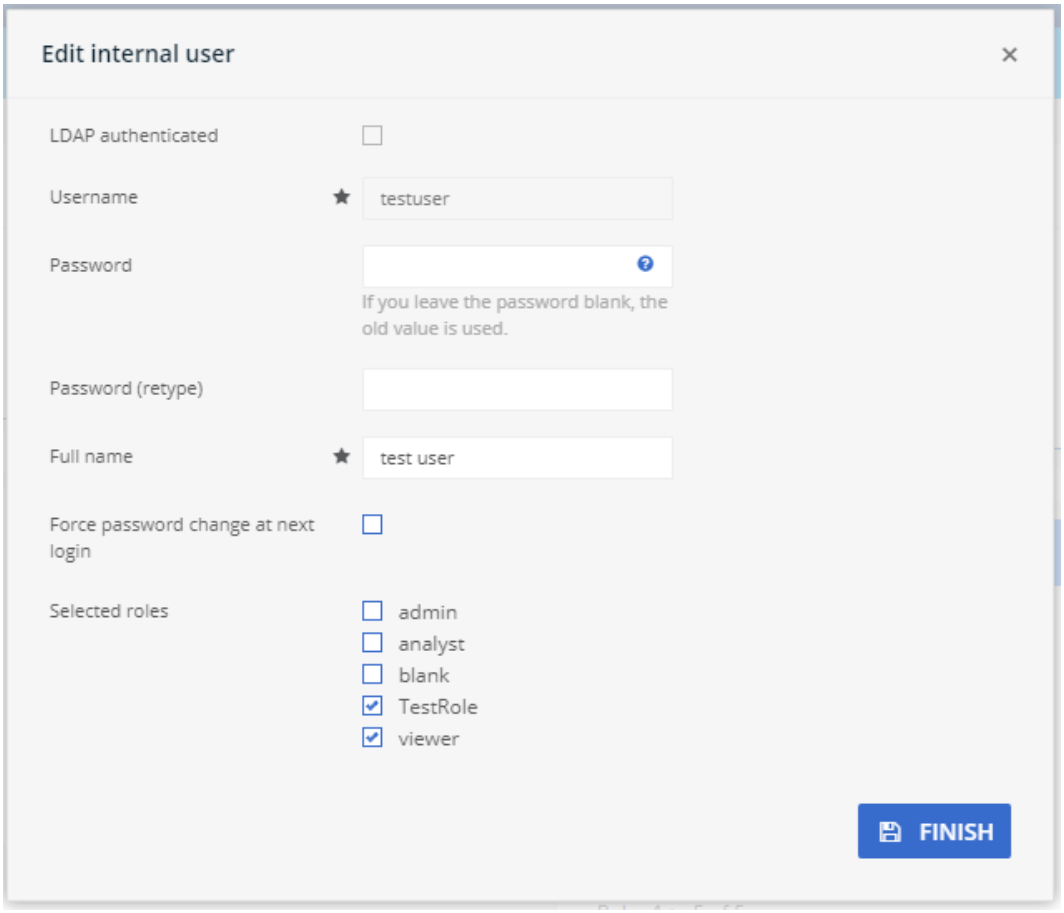


Figure 58. Assign roles

Session timeouts

The system automatically logs users out of Command Center who have been idle for a specific period of time. It is designed to enhance security by reducing the risk of unauthorized access when users forget to lock their computer or leave it unattended.

Timeouts help to prevent unauthorized access when the user is inactive and protects sensitive data if the device is lost.

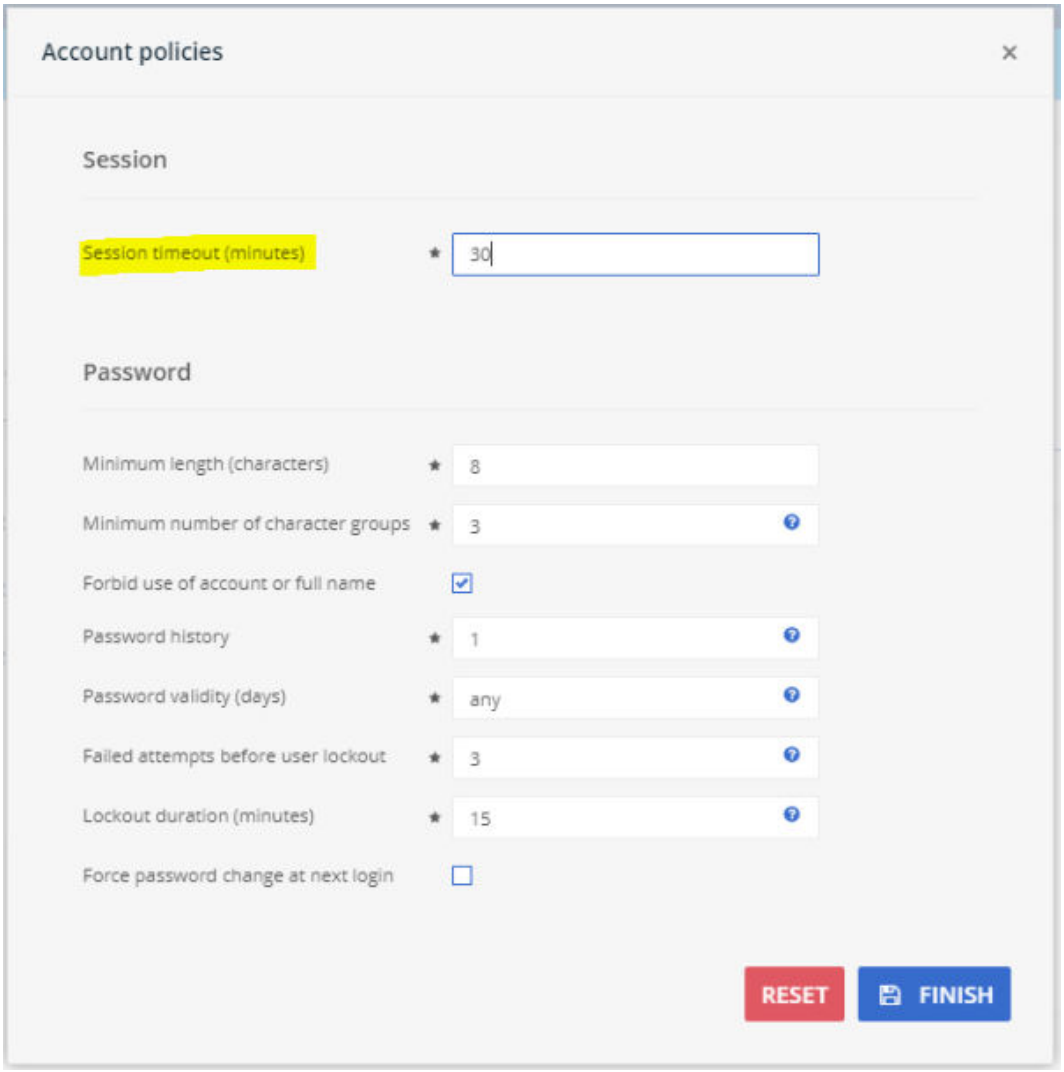


Figure 59. Session timeout

Accountability

Accountability is crucial in maintaining robust and effective cybersecurity. The individual is held responsible for their actions on the system.

User activity log

Forescout keeps track of all user activities on Command Center and on servers. It captures information about user interactions, changes made to data, system activities, and other events.

These logs help to monitor for suspicious activities, provide insights into what caused a problem, and helps with problem solving, auditing, and accountability.

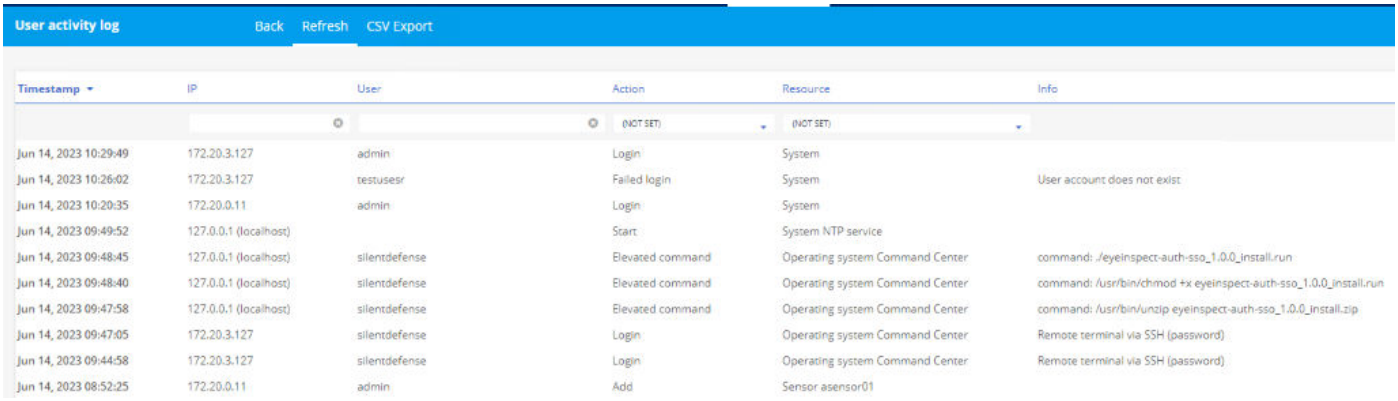


Figure 60. Example of activity logs

System event logs

The system event log keeps a record of various events and activities that occur within the system, captures important data about the system operations, errors, and warnings, and allows users to view logs in the Forescout Command Center diagnostic feature.

Value: System events help diagnose technical issues and errors, and help to identify trends or patterns within the system. Additionally, system events allow administrators to track changes and to detect, and respond to, potential security breaches.

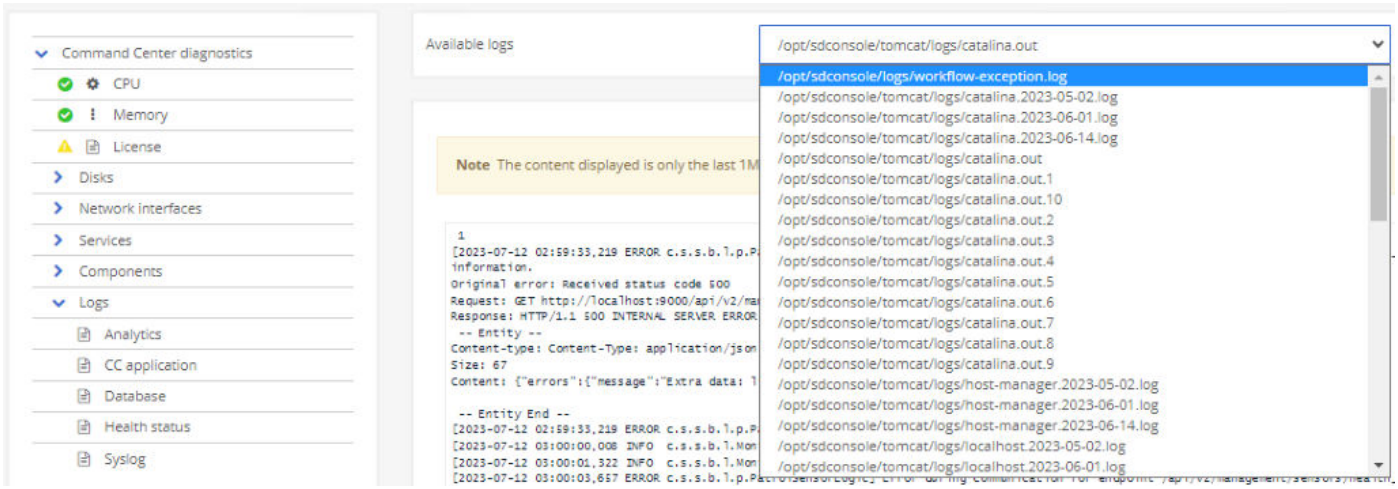


Figure 61. Syslog details in Command Center

Forwarding health status logs

Forescout provides the capability to notify users when the health status changes to above or below a critical level. These notifications can be forwarded to a remote syslog server or SIEM (for example, Splunk) to warn the user of any issues while they are not actively using the eyeInspect Command Center.

This results in faster response time to crucial events, helps avoid losses, ensures that sensitive data remains secure, and helps to maintain the trust of customers.

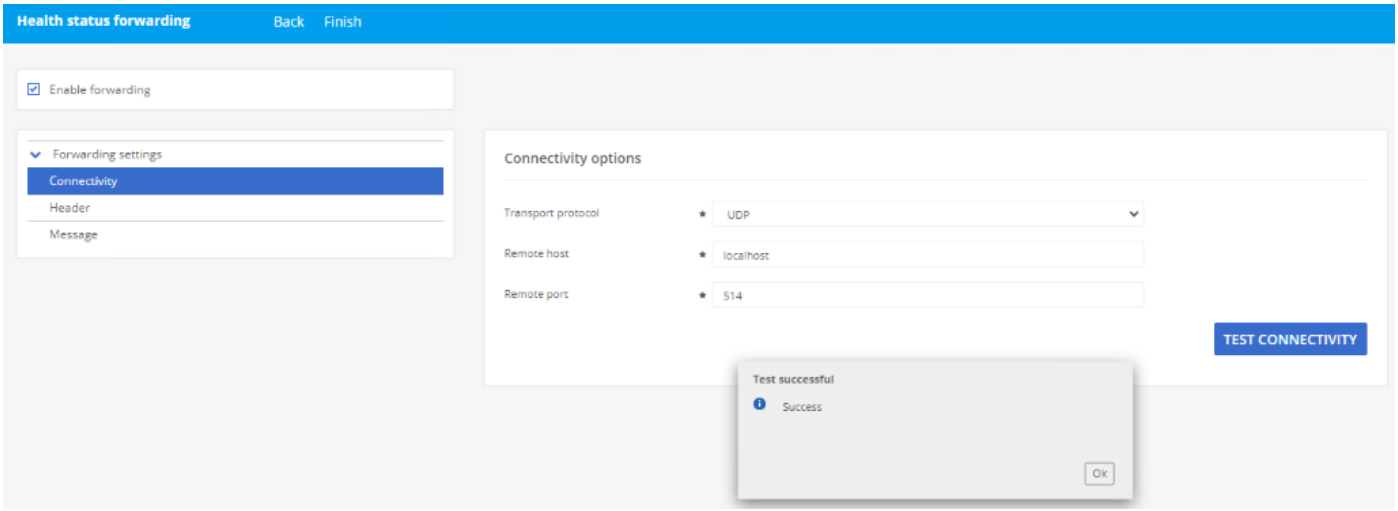


Figure 62. Health status forwarding

Clock

Time skew can impact the accuracy of logs, making them difficult to troubleshoot. To mitigate time skew, the Command Center date and time can be manually set, modified, or synced with NTP servers.

This helps with troubleshooting when using logs.

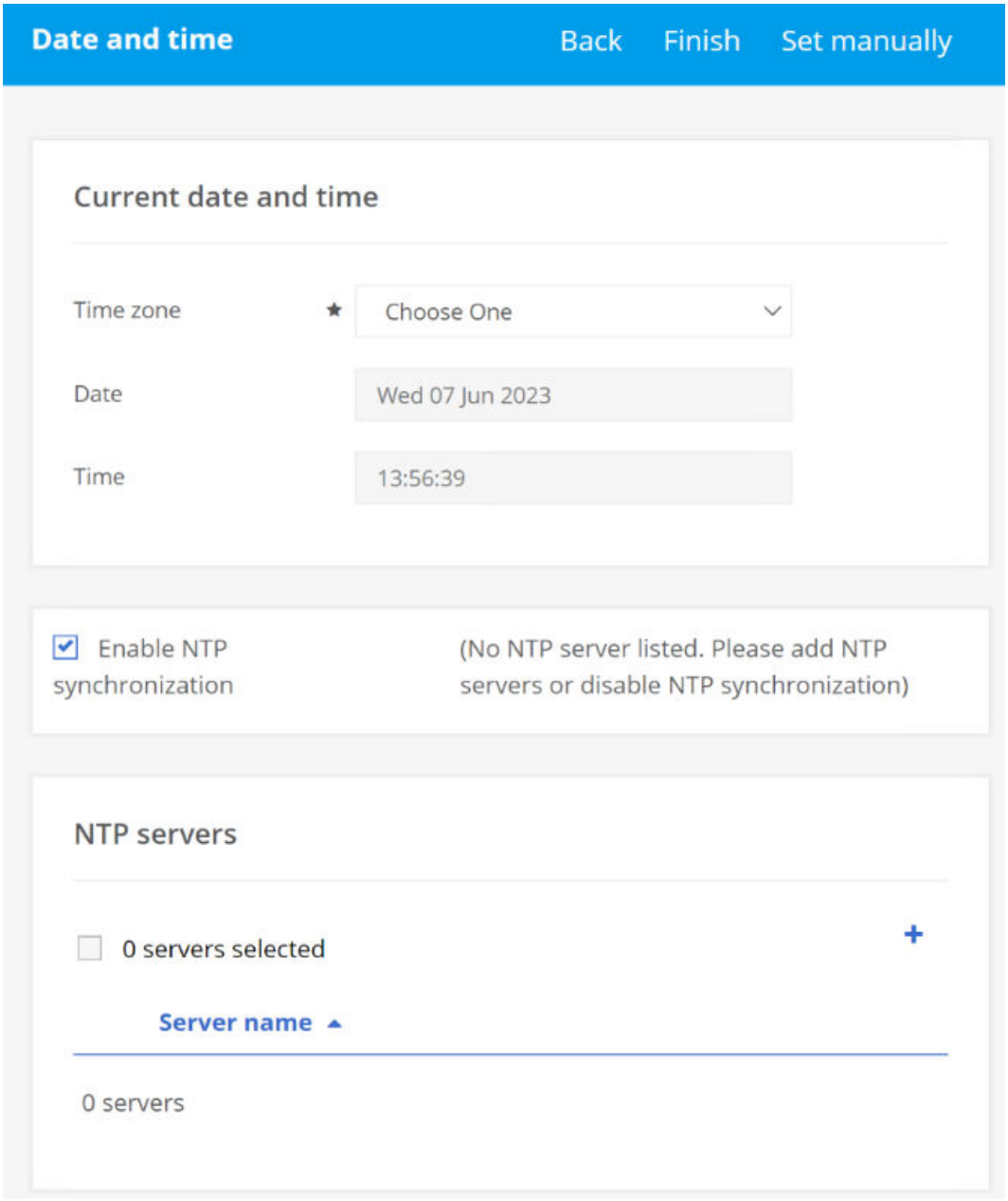


Figure 63. Date and time

Account lockout

This feature helps to avoid brute force attacks. Forescout user accounts are locked when a certain number of consecutive failed logins have been attempted within a given time period. The user is temporarily denied access until the administrator unlocks their account, or the user has to wait for a period of time until their account is automatically unlocked.

This feature prevents unauthorized access and cyberattacks.

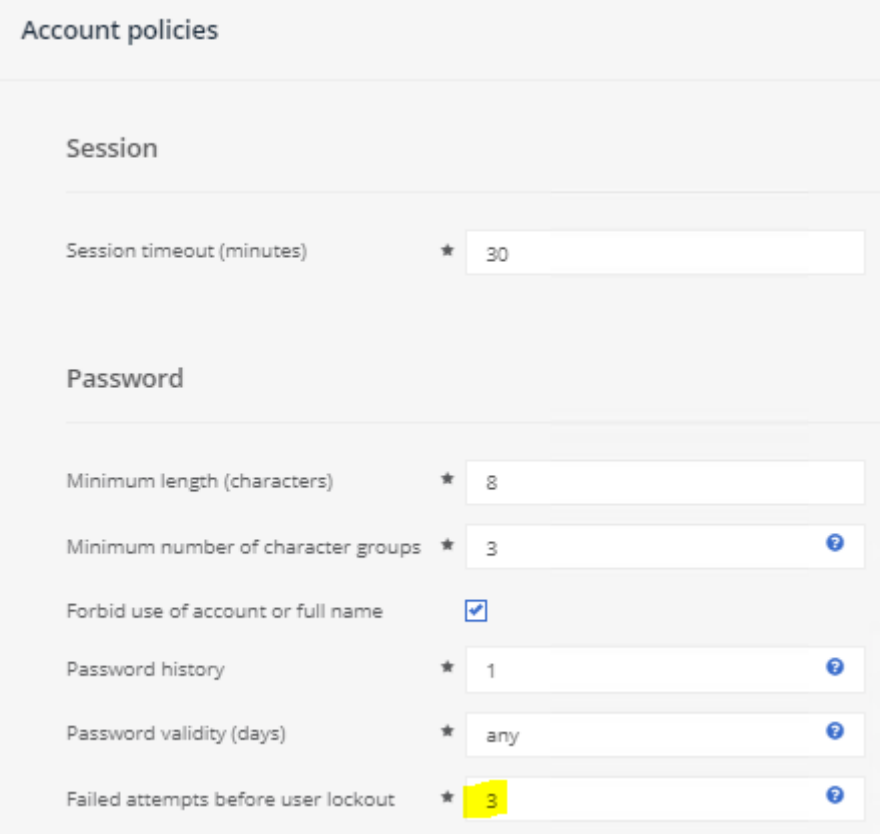


Figure 64. Failed attempts before user lockout

DMZ architecture and validation

A demilitarized zone is a vital buffer to insulate the substation from unwanted network intrusions. It is recommended to implement a firewall at this external interface to limit traffic to only expected and approved sources and protocols.

Architecture

The Security architecture figure shows the DVD architecture and its security components.

VPN tunnel

An important feature of this architecture is the VPN tunnel which is used to encrypt traffic between the substation and the control center. Even in the case where an OT protocol does not support its own secure connection, the VPN can provide the needed confidentiality.

DMZ firewall

Of particular importance is the firewall that is hosted on the substation DMZ. All traffic initiated externally is routed through this firewall, and it is the first line of defense against intrusion. It is important to configure this DMZ such that all necessary traffic, and only intended traffic, is permitted through.

In the following section, see a list of potential firewall rules to be implemented for Forescout software to function properly for Command Center with Passive Sensor or Active Sensor deployments. Consider that each deployment has its own required communications, and the list may not be representative of your use case.

For more information about eyeInspect firewall and networking considerations, see the **Prerequisites** chapter in the eyeInspect 5.2.0 Installation Guide.

DMZ firewall rules

NOTE: The firewall rules that are shown here are illustrative using default ports. Part of a defense-in-depth approach to security is to avoid using default ports.

Table 10. DMZ firewall rules for Forescout

Description	Source network	Source device	Destination network	Destination device	Port
Allow eyeInspect Command Center to connect with the Passive Sensor at the substation.	Station Bus	Passive Sensor	Control Center	Command Center	TCP 29999
Allow eyeInspect Passive Sensor data to reach Command Center.	Station Bus	Passive Sensor	Control Center	Command Center	TCP 9092
Allow eyeInspect Command Center to manage Active and Passive Sensor.	Control Center	Command Center	Station Bus	Active and Passive Sensor	TCP 22
Allow Active Sensor to send diagnostic logs to Command Center.	Station Bus	Active Sensor	Control Center	Command Center	TCP 24224
Allow Active Sensor to send data up to the Command Center.	Station Bus	Active Sensor	Control Center	Command Center	TCP 9001

NOTE: These firewall rules assume that the VPN endpoint in the substation does not use network address translation (NAT). If it does, the source is within the DMZ.

7

Gateways

Topics:

What is an industrial gateway?

An industrial gateway is a device that is typically deployed in an industrial environment, close to telemetry devices and industrial controllers at the edge. The primary goal of the industrial gateway at the substation is to offer a ruggedized, small form-factor device that can be used for auxiliary computing needs.

Introduction to Dell Edge Gateways

Dell Technologies has introduced several industrial gateways that come factory-configured with a specific operating system, or they allow customer-configurable OS environments to enable support for several different edge applications. Designed in a rugged, stackable, rack-mountable and fanless design, the Dell Edge Gateways are compact and robust enough to endure 24/7/365 operations. The modular designs of these gateways support multiple resources and configuration options.

This Dell Validated Design supports the following Dell Edge Gateways:

- Dell Edge Gateway 3200
  - The EGW-3200 is a compact, fanless, and ruggedized gateway with an Intel Atom processor. The EGW-3200 is built to withstand harsh environments, provide stable and efficient connections in different IoT scenarios, and can fulfill real-time computing demand with a lower entry point. It offers a multicore CPU with up to 32 GB of memory, and features WiFi, 4G or 5G, and traditional Ethernet connectivity.
  - The EGW-3200 comes factory configured with two OS options (Windows 10 IoT or Ubuntu). With Windows installed, it supports the deployment of the ABB ZEE600 Runtime client.
  - The EGW-3200 withstands temperatures ranging from –20°C to 60°C for 24/7 operations. See the EGW-3200/EGW-5200 Spec Sheet for additional information about the gateways' specifications.
  - For more details, refer to Dell EGW-3200 Support.
- Dell Edge Gateway 5200
  - The EGW-5200 is a compact, fanless, and ruggedized gateway with 9th Gen Intel Core processor and SSD drive compatibility. The EGW-5200 is built to withstand harsh environments to provide performance at the edge to support sizeable workloads. It offers a multicore CPU with up to 64 GB of memory, and features WiFi, 4G or 5G, and traditional Ethernet connectivity.
  - The EGW-5200 comes factory configured with two OS options (Windows 10 IoT or Ubuntu). With Windows installed, it supports the deployment of the ABB ZEE600 Runtime client.
  - The EGW-5200 withstands temperatures ranging from 0°C to 60°C for 24/7 operations. See the EGW-3200/EGW-5200 Spec Sheet for additional information about the gateways' specifications.
  - For more details refer to Dell EGW-5200 Support.

Gateway considerations

There are several design considerations to think about for industrial gateways:

1. Operating system
2. Industry standards and certifications
3. Security
4. Gateway hardware specifications

5. Network deployment and configuration

Operating system

When selecting an operating system to deploy on the industrial gateway, it is important to consider that software solutions can have different OS requirements. When an application supports both Windows and Linux Ubuntu operating systems, it is also important to choose an OS based on different factors, such as how lightweight it might need to be, what dependencies it might or might not support, and what other applications may be collocated on the machine.

The Dell Validated Design for Energy Edge leverages Dell Edge Gateways with Windows 10 LTSC 2019 to host the ABB ZEE600 Runtime client application. Refer to ISV-specific contents for details on supported operating systems and deployment options.

NOTE: All drivers are preloaded, and if there is a need for a driver update, download it from the Dell Technologies Support Site.

Industry certifications

Industry standards and certifications are an important factor to consider when deploying equipment in an industrial environment. One such industry standard is the Ingress Protection (IP) rating, also defined as IEC 60529. This standard classifies the different levels of protection provided by the casing around the device. It looks at the intrusion protection, such as solid objects followed by the moisture protection, such as shielding from water spray. Depending on your environment, you will need different values to stay compliant and for the gateway to stay operational.

Other than the IP rating, there are other standards and certifications to consider, depending on the environment and use case. For safety standards in the industrial space, consider IEC 61010 and the newer IEC 62368 standards.

Dell Edge Gateways are also tested and certified under MIL/NEBS standards environments to withstand most levels of shock, vibration, and extreme conditions found in remote locations.

More information about the certifications and ratings of the Dell Edge Gateways can be found in the EGW-3200/EGW-5200 Spec Sheet.

Security

Security is a crucial consideration, as it plays a role in protecting the safety of facility workers, protecting sensitive company data, and providing availability. When using Dell Edge Gateways in your deployments, consider utilizing or implementing the following:

- Ensure that only authorized users have access to the gateway, both physically and over the network. For example, consider access methods such as integrating with a central authentication server, such as Windows Active Directory, for more effective management of users. Any unused physical ports (for example, an unused RJ-45 port) should be sealed or disabled in the BIOS. Consider physically placing the gateway in an area that requires key-card access for authorized personnel only.
- Create user roles based on job function to follow the principal of least privilege—these roles can be applied to gateway access, and many ISV applications support the same role-based access control (RBAC). Review access and authorization periodically to ensure that both are up-to-date and accurate. It is also recommended to configure logging on the gateway (OS and any relevant applications) and to ideally forward those logs to a centralized logging server.
- Protect any data that exists within the gateway and any data going through it. Consider using up-to-date encryption algorithms to protect the confidentiality of the data. An example would be to encrypt any data at rest while leveraging the TPM module of the Dell Edge Gateway for secure encryption key management. Also, it may be appropriate to use hashing algorithms to protect the integrity of the data.
- Review segmenting of access as well. An example of this is to either designate a VLAN per function, or to physically segment management traffic from data traffic. Proper segmentation of data prevents someone without access from pivoting from one section of the network to another. This is important because process data is often considered intellectual property, and therefore it must be protected and separated from other data.

Gateway hardware specifications

Hardware specifications help define the amount of processing that the gateway can handle. Consider what functions and applications the hardware needs to support in order to choose the appropriate device.

Specific hardware specifications to consider include the CPU, memory, network ports and capabilities, and local storage, as well as other special capabilities such as multipathing capabilities. For example, if you require low power consumption, then require a gateway that runs the Intel Atom CPU. More information can be found on the Dell Technologies Support Site.

Consider the physical environment where the gateway is deployed. Review the form-factor of the gateway for constrained spaces. Environmental factors like operating temperature, humidity, and vibration are essential considerations as well.

Network deployment and configuration

It is important to pre-plan the network deployment of the gateway to ensure a successful outcome. Consider where and how the gateway will be connected. Ensure that the necessary IP addresses are reserved in your network for the gateway or gateways being deployed. If using VLANs, ensure that they are configured on the correct ports and that they are extended to the right devices. Test connectivity from the gateway to the services it requires, such as to DNS or NTP servers. This will verify that the Layer 2 and Layer 3 settings are configured correctly.

Review network redundancy for continued availability and minimal disruptions. Consider planning for network multipathing and fault tolerance by deploying redundant connections and switches. It is also important to plan for gateway failure scenarios. Ensure that there is a plan to restore gateway functionality with minimal downtime. For example, preconfigure a spare gateway on-site and nearby so that it is ready to be deployed with minimal configuration. For more detail, see High Availability and Disaster Recovery.

Another topic to consider is support for required network services. Common services and protocols to think about are NTP and DNS, as well as network monitoring (for example, SNMP) and logging. Also consider ISV applications that require a specific connection within the network or externally, and ensure that the local networking supports this. Lastly, think about network security considerations such as firewall rules. Are the necessary ports and protocols allowed for the gateway software to carry out all its functions? Are the necessary network services allowed through the network path? Successful network planning results in an easier and more successful deployment. See Cybersecurity for further details on validated firewall access-list rules between various ISV applications.

8

Sizing and Scaling Guidance

Topics:

Sizing and scaling overview

What does it do?

Sizing a system is a process to determine the pools of resources needed to satisfy workload demands and their service level objectives at an optimal cost. Sizing output depends highly on how accurately the requirements are defined and the intended use of the system. This DVD provides a predefined configuration for hardware platforms to enable customers to:

- Simplify the sizing process by providing a baseline for comparison.
- Make solution offerings simple.
- Ensure predictable and consistent performance.
- Remove cost ambiguity.

How does it work?

The Dell Edge Solutions Engineering team sizes workloads and scenarios in accordance with industry experience. These workloads are tested against various hardware configurations and optimal resource sizing information is gathered. Hardware systems are sized in three different sizes (small, medium, and large) for simplicity and shared in the Bill of Materials chapter of this document. These sizes reference the ISV applications and workload sizes they support, as shown in the following section.

Dell PowerEdge XR12 model servers are offered in this solution for substation automation and cybersecurity. Systems are sized based on workload parameters for the ISV applications. Scale and performance tests have been run and results are compiled to determine recommended configurations for system sizes.

A 3-node high-availability hardware platform is available as well, leveraging VMware vSAN and HA.

Platforms with PowerEdge

The Dell PowerEdge XR12 server is compact with a rugged design capable of supporting accelerators for remote private networks requiring artificial intelligence, machine learning, deep learning (AI/ML/DL) types of workloads. It offers reliable DC power in a hardened chassis to support, collect, and analyze edge gateway data.

Accuracy

The following figure details three common scenarios for sizing your workload. In existing environments, the workload is well defined. In a new or greenfield environment, this may not be known, and a reference workload is helpful. The sizing and scaling information detailed in this section provides guidance by referencing tested configurations of the software and hardware platforms.

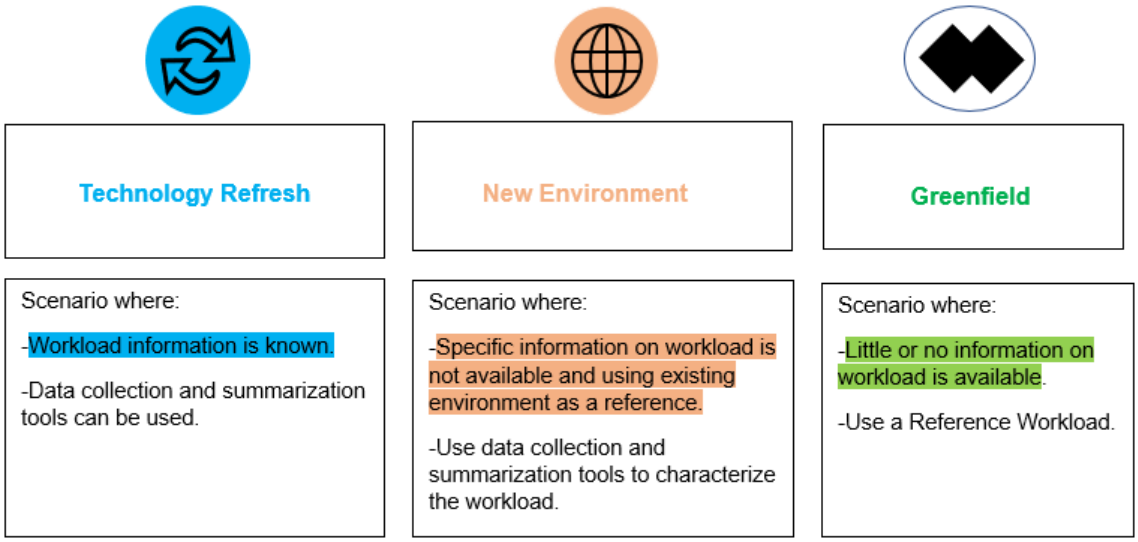


Figure 65. Factors affecting requirement accuracy

ABB sizing and scaling

Protocol considerations

The sizing process considers workloads originating from the following protocols:

- DNP3 TCP
- DNP3 Serial
- IEC 104
- IEC 61850
- Modbus TCP
- Modbus Serial

Design considerations

The following table outlines the considerations for workloads with predefined configurations.

Table 11. Sizing for ABB predefined configurations

Predefined configuration	Small	Medium	Large
Number of IEDs	10	20	30
Number of TAGs (total)	5,000	10,000	15,000
Number of master stations	1	2	3
Number of TAGs mapped to master stations	5%	5%	5%
Number of analog TAGs changes/sec	150	300	450
Binary input TAGs changes/sec	150	300	450
Number of IEDs per protocol	DNP3 TCP - 5 DNP3 Serial - 1 Modbus TCP - 1 Modbus Serial - 1	DNP3 TCP - 10 DNP3 Serial - 2 Modbus TCP - 2 Modbus Serial - 2	DNP3 TCP - 15 DNP3 Serial - 3 Modbus TCP - 3 Modbus Serial - 3

Table 11. Sizing for ABB predefined configurations (continued)

Predefined configuration	Small	Medium	Large
	IEC 104 - 1 IEC 61850 - 1	IEC 104 - 2 IEC 61850 - 2	IEC 104 - 3 IEC 61850 - 3
Process gateway protocols	DNP3 TCP	DNP3 TCP IEC104	DNP3 TCP IEC104 OPCUA
CPU (ZEE600)	4 cores	4 cores	4 cores
Memory (ZEE600)	4 GB minimum[a] 8 GB recommended	4 GB[a] 8 GB recommended	4 GB[a] 8 GB recommended
Network usage (ZEE600)	<1 Mbps	<1.5 Mbps	<1.5 Mbps
Storage usage (ZEE600)	<1.5 GB write/day	<1.5 GB write/day	<1.5 GB write/day

a. 4 GB of RAM was enough for ZEE600, however in testing some OS tasks occasionally pushed the memory usage over 5 GB. Recommend 8 GB to leave headroom for OS- related operations.

Forescout sizing and scaling

Sizing considerations

The sizing process considers the following factors:

- Number of IEDs (processed by ABB ZEE600)
- Number of TAGs (processed by ABB ZEE600)
- Bandwidth received from Forescout Passive Sensors
- Number of simultaneous active queries (Forescout Active Sensors)

This validation focused specifically on the components that are deployed at the substation, namely PowerEdge XR12 servers and Forescout sensors. Both passive and active Forescout sensors were tested for expected bandwidth and processing power per sensor. Scaling of the Forescout Command Center was not included as part of this validation effort, as it is already well defined by Forescout.

Design considerations

Forescout Passive Sensors

The following table outlines the considerations for workloads with predefined configurations.

Table 12. Sizing for Forescout Passive Sensors predefined configurations

Predefined configuration	Small	Medium	Large
Number of IEDs (ABB)	10	20	30
Number of TAGs (total)	5,000	10,000	15,000
Upper limit of bandwidth tested for Forescout	500 Mbps	800 Mbps	1 Gbps
CPU (passive)	4 cores	8 cores	12 cores
Memory	4–16 GB[a]	16–32 GB[a]	64–256 GB[a]
Storage (100 GB thin provisioned recommended)	<2.5 GB write/day[a]	<2.5 GB write/day[a]	<2.5 GB write/day[a]

Table 12. Sizing for Forescout Passive Sensors predefined configurations

a. These are the recommended memory levels per Forescout. These numbers can depend on factors such as throughput and number of devices monitored. However, in simulated testing, the lower end of the resource requirements was more than sufficient to process the limits displayed here.

Forescout Active Sensors

Active sensor testing was based on the recommended limit that is provided by Forescout of fifty active queries running simultaneously. Fifty simultaneous queries were run in various scenarios, including a mix of query types, entire /24 and /21 subnets, and single IPs. The following table shows the resources and results.

Table 13. Testing resources and results for Forescout Active Sensors

Predefined configuration	Max
CPU allocated	4 cores
CPU max/avg usage	6192/3284 MHz
Memory	4 GB
Network utilization	< 5 Mbps
Storage written	~241 MB/hr (at peak, during queries)
Storage recommendation	16 GB+ required (at least 50 GB thin provisioned recommended)

9

Bill of Materials

Topics:

Overview

The minimum hardware specifications per model for the Dell Validated Design for Energy Edge are noted in this section. There are several considerations when selecting the servers. The minimum configuration is provided for implementation planning; however, higher capacity components are available depending on the scaled needs of the environment.

Substations

This DVD supports Dell PowerEdge XR12 servers for software components deployed at substations. The software components include ABB ZEE600 Runtime Server and Forescout Sensor. Options are displayed for small, medium, and large server configurations, which scale Intel Xeon processors with additional cores along with greater storage and memory capacity

Control center

This DVD supports Dell PowerEdge R660 and R760 servers for the control center layer of the architecture. This is where Forescout Command Center (and other optional software) is deployed. The following tables are designed with Forescout Command Center in mind. However, a customer may want to deploy additional ISV software, such as Forescout EyeSight, here as well. Systems will need to be sized in-line with the ISV requirements for any additional software pieces.

ABB Runtime Client

Dell Edge Gateways, models EGW-3200 and EGW-5200, may be used for ABB Runtime Client. ABB Runtime Client is installed on Windows and thus some options for Windows-based Dell Edge Gateways are listed in the following tables.

The following diagram shows where each server option fits into the overall architecture.

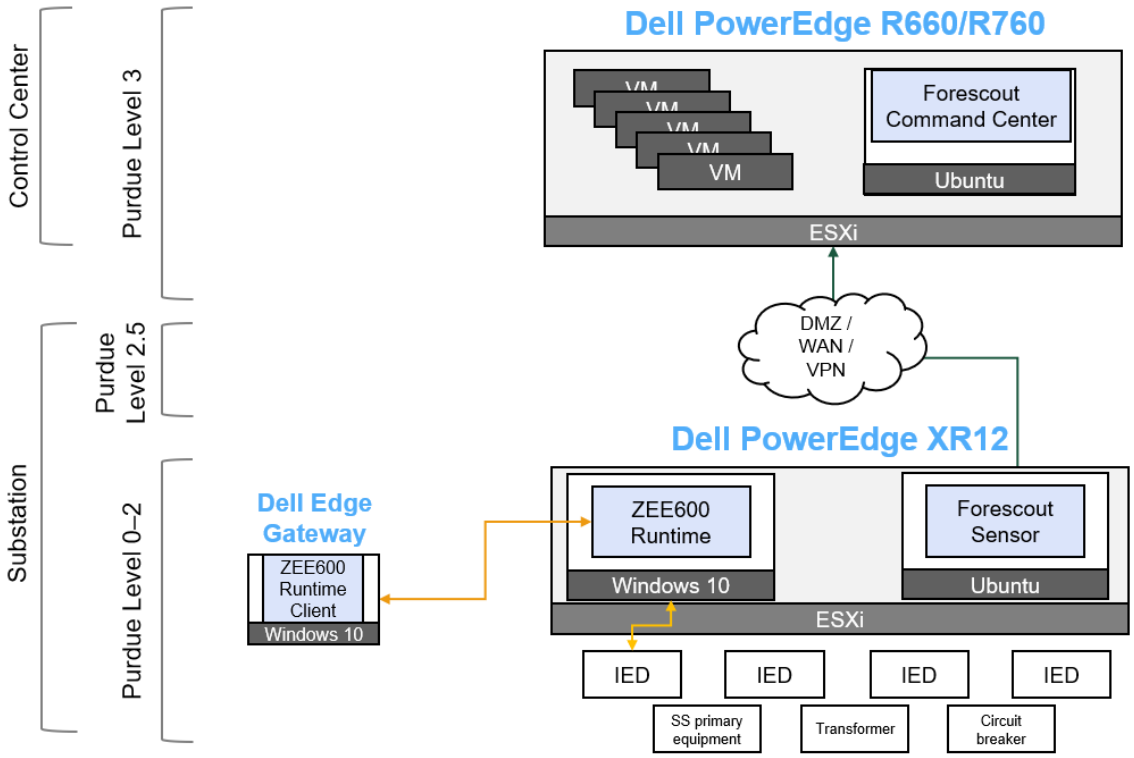


Figure 66. Device options within the architecture

Configurations

Table 14. PowerEdge XR12 configurations (at substation)

Specification	Small PowerEdge XR12	Medium PowerEdge XR12	Large PowerEdge XR12
Compute and memory			
CPU	Intel Xeon Silver 4310 2.1G, 12C/24T, 10.4GT/s, 18 M Cache, Turbo, HT (120 W) DDR4-2666	Intel Xeon Silver 4314 2.4G, 16C/32T, 10.4GT/s, 24 M Cache, Turbo, HT (135 W) DDR4-2666	Intel Xeon Gold 6312U 2.4G, 24C/48T, 11.2GT/s, 36 M Cache, Turbo, HT (185 W) DDR4-3200
Cores	12	16	24
Threads	24	32	48
Memory	64 GB	96 GB	256 GB
Storage			
Cache[a]	1x 480 GB SSD SAS (VSAN HA only)	1x 480 GB SSD SAS (VSAN HA only)	1x 480 GB SSD SAS (VSAN HA only)
Capacity drives	2x 480 GB SSD SAS (boot, RAID-1) 2x 960 GB SSD SAS (data)	2x 480 GB SSD SAS (boot, RAID-1) 2x 1.92 TB SSD SAS (data)	2x 480 GB SSD SAS (boot, RAID-1) 2x 3.84 TB SSD SAS (data)
Networking			
Integrated physical interface	4x 25 GbE SFP28	4x 25 GbE SFP28	4x 25 GbE SFP28
Additional network interface[b]	Intel X710-T2L Dual Port 10 GbE BASE-T Adapter, PCIe Low Profile	Intel X710-T2L Dual Port 10 GbE BASE-T Adapter, PCIe Low Profile	Intel X710-T2L Dual Port 10 GbE BASE-T Adapter, PCIe Low Profile
Power: AC PSU[c]	2x 1100 W 100–240 Vac	2x 1100 W 100–240 Vac	2x 1100 W 100–240 Vac
Dimensions	H: 86.8 mm (3.41 inches) W: 482.6 mm (19 inches) D: 400 mm (15.74 inches) Ear to rear wall 477 mm (18.77 inches) with bezel 463 mm (18.22 inches) without bezel	H: 86.8 mm (3.41 inches) W: 482.6 mm (19 inches) D: 400 mm (15.74 inches) Ear to rear wall 477 mm (18.77 inches) with bezel 463 mm (18.22 inches) without bezel	H: 86.8 mm (3.41 inches) W: 482.6 mm (19 inches) D: 400 mm (15.74 inches) Ear to rear wall 477 mm (18.77 inches) with bezel 463 mm (18.22 inches) without bezel
Weight	13.8 kg / 30.5 lb	13.8 kg / 30.5 lb	13.8 kg / 30.5 lb
Fans	6	6	6
Operating environment			
Ambient operating temperature	5–40°C / 41–104°F	5–40°C / 41–104°F	5–40°C / 41–104°F
Operating relative humidity	8–85% (non-condensing)	8–85% (non-condensing)	8–85% (non-condensing)
Operating altitude with no deratings	3048 m approx. 10,000 ft	3048 m approx. 10,000 ft	3048 m approx. 10,000 ft
Heat dissipation	1100 W 3753.4 btu/h	1100 W: 3753.4 btu/h	1100 W: 3753.4 btu/h
Licensing	VMware Edge Compute Stack iDRAC Enterprise OpenManage Base	VMware Edge Compute Stack iDRAC Enterprise OpenManage Base	VMware Edge Compute Stack iDRAC Enterprise OpenManage Base

Table 14. PowerEdge XR12 configurations (at substation) (continued)

Specification	Small PowerEdge XR12	Medium PowerEdge XR12	Large PowerEdge XR12
	OpenManage Advanced (optional)	OpenManage Advanced (optional)	OpenManage Advanced (optional)

a. Cache devices are only required in vSAN configurations. vSAN is a VMware offering for platform high availability.
b. Additional NIC to support 1/10 GbE connections as needed.
c. A 48 V DC power supply is also available as a supported option for the XR12 server.

Table 15. PowerEdge R660 configurations (at control center)

Specification	Small PowerEdge R660	Medium PowerEdge R660	Large PowerEdge R660
Compute and memory			
CPU	2x Intel Xeon Silver 4410Y 2G, 12C/24T, 16 GT/s, 30 M Cache, Turbo, HT (150 W) DDR5-4000	2x Intel Xeon Silver 4410Y 2G, 12C/24T, 16 GT/s, 30 M Cache, Turbo, HT (150 W) DDR5-4000	2x Intel Xeon Gold 6426Y 2.5G, 16C/32T, 16 GT/s, 38 M Cache, Turbo, HT (185 W) DDR5-4800
Cores	24	24	32
Threads	48	48	64
Memory	64 GB	128 GB	256 GB
Storage			
Capacity drives	2x 960 GB SSD SAS	2x 1.92 TB GB SSD SAS	2x 3.84 TB GB SSD SAS
BOSS card (RAID 1)	2x 480 GB M.2	2x 480 GB M.2	2x 480 GB M.2
Networking			
Integrated physical interface	4x 25 GbE SFP28	4x 25 GbE SFP28	4x 25 GbE SFP28
Power: AC PSU	2x 1100 W 100–240 Vac	2x 1100 W 100–240 Vac	2x 1100 W 100–240 Vac
Dimensions	H: 42.8 mm (1.68 inches) W: 482 mm (18.97 inches) D: 822.88 mm (32.39 inches) with bezel 809.04 mm (31.85 inches) without bezel	H: 42.8 mm (1.68 inches) W: 482 mm (18.97 inches) D: 822.88 mm (32.39 inches) with bezel 809.04 mm (31.85 inches) without bezel	H: 42.8 mm (1.68 inches) W: 482 mm (18.97 inches) D: 822.88 mm (32.39 inches) with bezel 809.04 mm (31.85 inches) without bezel
Weight	21.7 kg / 47.8 lb	21.7 kg / 47.8 lb	21.7 kg / 47.8 lb
Fans	4	4	4
Operating environment			
Ambient operating temperature	5–40°C / 41–104°F	5–40°C / 41–104°F	5–40°C / 41–104°F
Operating relative humidity	8–85% (non-condensing)	8–85% (non-condensing)	8–85% (non-condensing)
Operating altitude with no deratings	3048 m approx. 10,000 ft	3048 m approx. 10,000 ft	3048 m approx. 10,000 ft
Heat dissipation	1100 W 3753.4 btu/h	1100 W 3753.4 btu/h	1100 W 3753.4 btu/h
Licensing	VMware Edge Compute Stack iDRAC Enterprise OpenManage Base	VMware Edge Compute Stack iDRAC Enterprise OpenManage Base	VMware Edge Compute Stack iDRAC Enterprise OpenManage Base

Table 15. PowerEdge R660 configurations (at control center) (continued)

Specification	Small PowerEdge R660	Medium PowerEdge R660	Large PowerEdge R660
	OpenManage Advanced (optional)	OpenManage Advanced (optional)	OpenManage Advanced (optional)

Table 16. PowerEdge R760 configurations (at control center)

Specification	Small PowerEdge R760	Medium PowerEdge R760	Large PowerEdge R760
Compute and memory			
CPU	2x Intel Xeon Silver 4410Y 2G, 12C/24T, 16 GT/s, 30 M Cache, Turbo, HT (150 W) DDR5-4000	2x Intel Xeon Silver 4410Y 2G, 12C/24T, 16 GT/s, 30 M Cache, Turbo, HT (150 W) DDR5-4000	2x Intel Xeon Gold 6426Y 2.5G, 16C/32T, 16 GT/s, 38 M Cache, Turbo, HT (185 W) DDR5-4800
Cores	24	24	32
Threads	48	48	64
Memory	64 GB	128 GB	256 GB
Storage			
Capacity drives	2x 960 GB SSD SAS	2x 1.92 TB GB SSD SAS	2x 3.84 TB GB SSD SAS
BOSS card (RAID 1)	2x 480 GB M.2	2x 480 GB M.2	2x 480 GB M.2
Networking			
Integrated physical interface	4x 25 GbE SFP28	4x 25 GbE SFP28	4x 25 GbE SFP28
Power: AC PSU	2x 1400 W 100-240 Vac	2x 1400 W 100-240 Vac	2x 1400 W 100-240 Vac
Dimensions	H: 86.8 mm (3.41 inches) W: 482 mm (18.97 inches) D: 772.13 mm (30.39 inches) with bezel 758.29 mm (29.85 inches) without bezel	H: 86.8 mm (3.41 inches) W: 482 mm (18.97 inches) D: 772.13 mm (30.39 inches) with bezel 758.29 mm (29.85 inches) without bezel	H: 86.8 mm (3.41 inches) W: 482 mm (18.97 inches) D: 772.13 mm (30.39 inches) with bezel 758.29 mm (29.85 inches) without bezel
Weight	27.5 kg / 60.6 lb	27.5 kg / 60.6 lb	27.5 kg / 60.6 lb
Fans	6	6	6
Operating environment			
Ambient operating temperature	5–40°C / 41–104°F	5–40°C / 41–104°F	5–40°C / 41–104°F
Operating relative humidity	8–85% (non-condensing)	8–85% (non-condensing)	8–85% (non-condensing)
Operating altitude with no deratings	3048 m approx. 10,000 ft	3048 m approx. 10,000 ft	3048 m approx. 10,000 ft
Heat dissipation	1400 W: 4777 btu/h	1400 W: 4777 btu/h	1400 W: 4777 btu/h
Licensing	VMware Edge Compute Stack iDRAC Enterprise OpenManage Base OpenManage Advanced (optional)	VMware Edge Compute Stack iDRAC Enterprise OpenManage Base OpenManage Advanced (optional)	VMware Edge Compute Stack iDRAC Enterprise OpenManage Base OpenManage Advanced (optional)

Table 17. Dell Edge Gateway configurations (Windows, for ABB Runtime Client)

Specification	EGW-3200 (Win10)	EGW-5200 (Win10)
Compute and memory		
CPU	Intel Atom x6425RE 1.9 G	Intel Core i7-9700TE 1.8 G
Cores	4	8
Memory	16 GB	32 GB
Storage	512 GB	512 GB
Network interfaces	2x 1 GbE	3x 1 GbE
USB ports	4x USB 3.0 ports	3x USB 3.1 Type A 3x USB 2.0 Type A

10

Conclusion

The guidance provided in this document, validated in collaboration with ABB and Forescout, provides best practices for preparation and deployment of the ABB ZEE600 platform and the Forescout Platform's eyeInspect within an electrical substation. By leveraging a proven implementation, documented by industry leaders, the path to value is accelerated and the risks are reduced. A jointly produced reference architecture exemplifies critical implementation principles that yield a scalable and repeatable foundation for Industry 4.0 initiatives across an energy provider's grid infrastructure. As modern applications drive utility providers to move more compute resources to the enterprise edge or substation, the solution from Dell Technologies leverages the value of an enterprise-grade, industry-certified infrastructure to run applications closer to where the data is being created and where results are most valuable. This joint energy edge reference architecture, developed in collaboration between Dell Technologies, ABB, and Forescout, delivers unprecedented stability, security, scalability, and repeatability for every substation initiative.

A

Additional Information

Topics:

About Dell Validated Designs

The Dell Validated Design for Energy Edge enables customers to build energy edge data center and substation solutions with speed and confidence. Engineering-validated designs are built upon optimized architectures for your energy automation applications using industry-leading servers, software, networking, and storage.

Dell Validated Designs enable customers to deploy energy application-optimized edge data centers faster, reducing research and troubleshooting time through the Dell in-house design, build, and validation efforts. Validated workload-optimized architectures can reduce customer proof-of-concept time and eliminate months of design and testing time that is required to plan correct configurations prior to deployment. Customers can rely on architectures that are tested and validated by our world-class engineers in collaboration with our third-party software and hardware partners. To refine our architectures into a customer's more prescriptive needs, Dell Professional Services are available when and where you need them.

Ordering guidance

Configuration support and ordering of Dell PowerEdge servers and Dell Edge Gateways is available through your Technical Sales Representative (Commercial and Enterprise), Inside Sales Representative (Commercial and Enterprise), Account Executive (AE), System Consultant (SC), Global Client and Compute Sales Representative (GCCS), and Dell Technologies partner System Integrators (SI).

This guide may also be used by support and professional services teams to better understand the underlying hardware and software structure of the Dell PowerEdge and Dell Edge Gateway platforms. Pricing is not available in this document.

For ordering and license guidance, you must have a valid sales or partner seller Dell Technologies two-factor authentication account.

Acronyms and terminology

The following table provides definitions for some of the terms that are used in this document.

Table 18. Acronyms and terminology

Term	Definition
AC	(Voltage) Alternating Current
ADMS	Active Directory Migration Services
AE	Account Executive
AI	Artificial Intelligence
ANSI	American National Standards Institute
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BIOS	Basic Input Output System
BOSS	Boot-Optimized Storage System

Table 18. Acronyms and terminology (continued)

Term	Definition
BTU	British Thermal Unit
C	Centigrade
CapEx	Capital Expense
CAT	Category (Rating)
CC	Control Center
CIP	Critical Infrastructure Protection
CLI	Command Line Interface
CNSA	Commercial National Security Algorithm
CPU	Central Processing Unit
D	Depth (Measurement)
DAN	Doubly Attached Node
DER	Distributed Energy Resources
DL	Deep Learning
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol 3
DNS	Domain Name Service
DR	Disaster Recovery
DRS	Distributed Resources Scheduler
DVD	Dell Validated Design
ECS	Edge Compute Stack
EGW	(Dell Technologies) Edge Gateway
EMS	Energy Management Services
ESXi	ESX integrated
EV	Electric Vehicle
F	Fahrenheit
FIPS	Federal Information Processing Standards
FT	Fault Tolerance
GB	Giga-Byte
GbE	Gigabit Ethernet
GOOSE	Generic Object Oriented Substation Event
GPU	Graphics Processing Unit
GUI	Graphical User Interface
H	Height (Measurement)
HA	High Availability
HCI	Hyper-Converged Infrastructure
HDD	Hard Disk Drive
HMI	Human Machine Interface

Table 18. Acronyms and terminology (continued)

Term	Definition
HT	Hyper-Threading
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol Secure
IACS	Industrial Automation Control System
ICS	Industrial Control System
iDRAC	Integrated Dell Remote Access Controller
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IED	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
ISA	International Society of Automation
ISV	Independent Software Vendor
IT	Information Technology
KB	Kilo-Byte
KG	(Weight) Kilogram
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LB	(Weight) Pound
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over Transport Layer Security
LTSC	Long Term Servicing Channel
MB	Mega-Byte
MIL-STD	Military Standard
ML	Machine Learning
MM	(Distance) Millimeter
MMS	Manufacturing Message Specification
NAT	Network Address Translation
NEBS	Network Equipment-Building System
NERC	North American Electric Reliability Corporation
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NVMe	Non-Volatile Memory Express
OPC-UA	Open Library Environment Process Control Unified Architecture
OpEx	Operating Expense

Table 18. Acronyms and terminology (continued)

Term	Definition
OS	Operating System
OT	Operations Technology
OWASP	Open Worldwide Application Security Project
PCAP	Packet Capture
PCIe	Peripheral Component Interconnect Express
PLC	Programmable Logic Controller
PRP	Parallel Redundancy Protocol
PSU	Power Supply Unit
PTP	Precision Time Protocol
QA	Quality Assurance
RAID	Redundant Arrays of Inexpensive Disks Controller
RAM	Random Access Memory
RBAC	Role-Based Access Control
RJ	Registered Jack
RPO	Recovery Point Objective
RS	Recommended Standard
RSTP	Rapid Spanning Tree Protocol
RTO	Recovery Time Objective
RTU	Remote Terminal Unit
SAS	Serial Attached Small Computer System Interface
SAS	Shared Access Signature
SATA	Serial Advanced Technology Attachment
SC	System Consultant
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy
SCSI	Small Computer System Interchange
SCV	Secured Component Verification
SEKM	Secure Enterprise Key Management
SFP	Small Form-Factor Pluggable
SI	System Integrator
SIEM	Security Information and Event Management
SL	Service Level
SL-A	Security Level Achieved
SL-C	Security Level Compatibility
SL-T	Security Level Target
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol

Table 18. Acronyms and terminology (continued)

Term	Definition
SNMP	Simple Network Management Protocol
SS	Substation
SSH	Secure Shell
TCP/IP	Transmission Control Protocol Internet Protocol
ToR	Top of Rack
TPM	Trusted Platform Module
U	(Rack) Unit
UDP	User Datagram Protocol
URL	Universal Resource Locator
vDS	Virtual Distribution Switch
VLAN	Virtual Local Area Network
VLT	Virtual Link Trunking
VM	Virtual Machine
vSAN	Virtual Storage Area Network
VPN	Virtual Private Network
W	Width (Measurement)
WAN	Wide Area Network
XML	eXtensible Markup Language

B

References

Topics:

Dell Technologies documentation

The following Dell Technologies documentation provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

VxRail Network Planning Guide

Dell Validated Design Security Configurations for Edge Solutions using VMware vSphere v7.0 - Configuration Guide

Dell Validated Design Security Configurations for Edge Solutions using VMware vSphere v8.0 - Configuration Guide

PowerEdge XR12 Documentation

PowerEdge R660 Documentation

PowerEdge R760 Documentation

Dell Edge Gateway 3200 Documentation

Dell Edge Gateway 5200 Documentation

VMware documentation

The following VMware documentation provides additional and relevant information:

VMware vSphere documentation

VMware vSphere Security Configuration Guide 7

VMware vSphere Security Configuration Guide 8

VMware vSAN Product Page

Using Encryption in a vSAN Cluster

Support and feedback

For technical support, go to https://www.dell.com/support or call (USA) 1-800-945-3355.

Dell Technologies and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell Technologies Solutions team by email.