Base Load Power Hub (BLPH)

CYBER SECURITY SETTINGS

Document Number: 1724000594-IN-RE-00043
Supplier Document Number: E366772C00-CSS
Document Class: 2

01	21/02/2025	Accepted for Construction (AFC)	Bhoomika K R	S. Rao/ A.Berra	Sonia Corradi
00	24/09/2024	Issue for Review (IFR)	Bhoomika K R	S. Rao/ A.Berra	Sonia Corradi
Rev.	Date	Description	Prepared	Reviewed	Approved

This document undergoes an issuance cycle within EDMS Fusionlive. Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Revision / Change Log

Rev.	Description
00	Issue for Review (IFR)
01	Accepted for Construction (AFC)

This document undergoes an issuance cycle within EDMS Fusionlive. Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Table of contents

1 DEFINITIONS AND ABBREVIATIONS ---- 11
1.1 DEFINITIONS ---- 11
1.2 ABBREVIATIONS ---- 11
2 INTRODUCTION ---- 13
2.1 PROJECT OVERVIEW ---- 13
2.1.1 Project Location ---- 13
2.1.2 Project Concept ---- 14
3 NETWORK AND SECURITY SOLUTIONS (NSS) ---- 16
3.1 OVERVIEW OF SECURITY SOLUTIONS ---- 17
4 WINDOWS DOMAIN AND ACCOUNT MANAGEMENT ---- 18
4.1 BACKGROUND ---- 18
4.2 ACTIVE DIRECTORY FUNDAMENTALS ---- 18
4.3 DESIGN ARCHITECTURE: OVERVIEW ---- 19
4.4 DETAIL DESIGN ---- 19
4.4.1 Active Directory volumes ---- 19
4.4.2 Forest and Domain Functional Level ---- 19
4.4.3 Flexible Single-Master Operational (FSMO) Roles ---- 20
4.4.3.1 Global Catalog (GC) ---- 20
4.4.4 Active Directory Sites ---- 21
4.4.5 DNS Structure ---- 21
4.4.5.1 DNS redundancy ---- 21
4.4.5.2 Dynamic updating for hosts ---- 21
4.4.5.3 Forward & Reverse Lookup Zones ---- 22
4.4.5.4 DNS zones replications ---- 23
4.4.5.5 DNS suffixes configuration for computers ---- 23
4.5 TIME SYNCHRONIZATION ---- 24
4.6 ACTIVE DIRECTORY STRUCTURE ---- 24
4.6.1 Organizational Unit (OU) ---- 24
4.6.1.1 Design Considerations ---- 25
4.6.2 Users and Groups ---- 26
4.6.2.1 Users ---- 26
4.6.2.2 Groups ---- 26
4.6.2.3 Role based Access Control Security Groups. ---- 28
4.6.2.3.1 CENTUM Security Groups ---- 28
4.6.2.3.2 PROSAFE Security Groups ---- 28
4.6.2.3.3 PRM Security Groups ---- 28
4.6.2.3.4 CI Server Security Groups ---- 28
4.6.2.3.5 Veeam Backup and Recovery Security Groups ---- 29
4.6.2.3.6 WSUS Security Groups ---- 29
4.6.2.3.7 Trellix Security Groups ---- 29
4.6.2.3.8 NMS Security Groups ---- 29
4.7 GROUP POLICY OBJECTS ---- 30
4.7.1 Group Policy Assignment ---- 42
5 YOKOGAWA ENDPOINT SECURITY SOLUTION ---- 43
5.1 DESIGN ARCHITECTURE: OVERVIEW ---- 43
5.2 ANTI-VIRUS COMPONENTS ---- 43
5.2.1 Trellix ePolicy Orchestrator Server ---- 43
5.2.2 Trellix Agent ---- 44
5.2.3 Yokogawa Standard Antivirus Software (ENS) Software ---- 44
5.3 REPOSITORY ---- 45

5.3.1 Updates ---- 46
5.3.2 System Tree Groups ---- 46
5.3.3 Antivirus Policies ---- 47
5.3.3.1 Yokogawa Standard Antivirus Software (ENS) Policy ---- 48
5.3.3.2 Yokogawa Standard Antivirus Software (ENS) Task ---- 48
5.3.4 Yokogawa Standard Antivirus Software (ENS) Scan Types ---- 48
5.3.5 On-Demand Scan ---- 48
5.3.5.1 On-Access Scan ---- 49
5.3.6 Yokogawa Standard Antivirus Software (ENS) File Exclusions ---- 49
5.3.7 Yokogawa Standard Antivirus Software (ENS) Definition and Product Updates ---- 49
5.3.8 Host Name Resolution ---- 49
5.3.8.1 Queries ---- 49
5.3.8.2 Reports ---- 50
5.3.8.3 Logs ---- 50
5.3.8.4 Log Files for Troubleshooting ---- 50

6 OS PATCH MANAGEMENT ---- 51

6.1 DESIGN ARCHITECTURE OVERVIEW ---- 51
6.2 WSUS COMPONENTS ---- 51
6.2.1 WSUS Server ---- 51
6.2.2 WSUS Client Computers and their Automatic Updates ---- 52
6.3 WSUS FIREWALL PORT REQUIREMENT ---- 53
6.3.1 Firewall Port Requirement of the WSUS Server ---- 53
6.3.2 Firewall Port Requirement of the WSUS Client ---- 53
6.4 WSUS CLIENTS POLICY ---- 53
6.5 WSUS CLIENTS POLICY ---- 53
6.6 GROUPS ---- 53
6.7 SCHEDULING ---- 54
6.8 WSUS REPORTING ---- 54
6.9 OS PATCH UPDATES SERVICES ---- 55

7 BACKUP & RECOVERY SYSTEM ---- 56

7.1 BACKUP AND RECOVERY SYSTEM ---- 56
7.2 VEEAM BACKUP & REPLICATION (VBR) COMPONENTS ---- 56
BRS Server ---- 56
7.2.1 Physical Infrastructure ---- 56
7.2.2 Backup Repository ---- 57
7.3 VEEAM BACKUP & REPLICATION (VBR) BACKUP FILES ---- 57
7.4 RPO ---- 57
7.5 RTO ---- 57
7.6 DESIGN ARCHITECTURE OF BRS ---- 57
7.7 USED PORTS ---- 58
7.7.1 Physical Machines ---- 58
7.8 BACKUP JOB ---- 59
7.9 BACKUP SCHEDULE ---- 60
7.10 BACKUP SIZING DETAILS ---- 61
7.11 USER ACCOUNT CONFIGURATION ---- 63
7.12 AUDIT LOGS ---- 64
7.13 RECOVERY STRATEGY ---- 64
7.14 VERIFICATION ---- 64
7.15 REPORTING ---- 64

8 NETWORK MANAGEMENT SYSTEM ---- 65

8.1 NETWORK MANAGEMENT SYSTEM ARCHITECTURE COMPONENTS ---- 65
8.1.1 NMS Server ---- 65

8.1.2 Monitored Devices ---- 65
8.1.3 Monitoring Protocol ---- 66
8.2 Design ARCHitecture of NMS ---- 66
8.3 Network Management System Functionalities ---- 67
8.3.1 Fault Management ---- 67
8.3.2 Performance Management ---- 67
8.3.3 Reporting ---- 67
8.4 Types of Device Components to Monitor ---- 67
8.5 Steps to configure the monitoring of VNET/IP Devices. ---- 68
8.5.1 Active Monitoring ---- 69
8.5.2 Passive Monitoring ---- 69
8.5.3 System Alert Monitoring and Notification ---- 69
8.6 SNMP Community Name ---- 69
8.6.1 SNMP Configuration for Microsoft Windows ---- 69
8.6.2 SNMP Configuration for L2 / L3 Switches and Firewall ---- 70
8.7 WUG Visualizations ---- 70
8.7.1 Map View ---- 70
8.7.2 Device View ---- 70

9 APPLICATION WHITELISTING ---- 72

9.1 Design Architecture ---- 72
9.2 Application Whitelisting Components ---- 73
9.2.1 ePO Management Console ---- 73
9.2.2 Trellix Agent ---- 73
9.2.3 Trellix Application Control ---- 73
9.3 Application Whitelisting for Yokogawa Systems ---- 73
9.4 Application Whitelisting Mode ---- 74
9.4.1 Enabled Mode ---- 74
9.4.2 Update Mode ---- 74
9.5 Event and Response ---- 74
9.6 Trellix ePolicy Orchestrator (ePO) Server ---- 74
9.6.1 Trellix ePolicy Orchestrator (ePO) Server Configuration ---- 74
9.6.2 Yokogawa System Tree Groups ---- 74
9.6.3 Yokogawa System Tree Groups Members ---- 75
9.7 Application Whitelisting Policy ---- 75
9.8 Application Whitelisting Task ---- 76
9.9 Report and Logs ---- 76
9.10 Security Configuration ---- .....
9.11 User Account ---- .....
9.11.1 User Account Authentication (Windows Authentication) ---- .....
9.11.2 User Account Management ---- .....
9.11.3 User Account Integration with Windows Active Directory ---- .....
9.11.3.1 Windows Active Directory User Login ---- .....
9.11.3.2 Windows Active Directory Group Permission Set ---- .....
9.11.3.3 User Account Password Management ---- .....
9.11.3.4 Authenticator Feedback ---- .....
9.11.3.5 Permission Set ---- .....
9.11.3.6 Client to server account authentication ---- .....
9.11.3.7 System Notification ---- .....
9.11.3.8 Confidentiality of information ---- .....
9.11.3.9 Automated Server Backup ---- .....

10 FIREWALL ---- 77

10.1 Design Architecture: Overview ---- 77
10.2 Firewall Function ---- 77

10.2.1 Packet Filtering ---- 78
10.2.2 Firewall Operation Mode ---- 78
10.2.3 Network Object ---- 78
10.2.4 Access Rules ---- ....
10.2.5 DMZ Firewall Service Object ---- ....
10.3 FIREWALL HARDENING ---- 78
10.3.1 Security Banner ---- 79
10.4 FIREWALL MANAGEMENT ---- 79
10.4.1 Firewall Reporting ---- ....
10.5 FIREWALL PORT EXCEPTIONS ---- ....
11 SWITCHES ---- 80
11.1 SWITCH ROLE ---- 80
11.1.1 PIN Switch ---- 80
11.1.2 Vnet/IP Switch ---- 80
11.1.3 Switch Functions ---- 80
11.1.4 Redundant Switch Configurations ---- 80
12 REMOTE ACCESS CONNECTION ---- 82
13 IP ADDRESS ASSIGNMENT ---- ....
14 NETWORK FLOW DIAGRAM ---- 83

List of Figures

Figure 1- HOLLANDSE KUST NOORD WIND PARK Location Map ---- 13
Figure 1 - Wind Park Details ---- 14
Figure 2 – BLPH Concept ---- 14
Figure 3 – Windows Domain and Account Management Design Architecture ---- 19
Figure 5 – FSMO Configuration. ---- 20
Figure 4 – Dynamic Updating Setting for the default Forward lookup Zone ---- 22
Figure 5 – Dynamic Updates Setting for the Reverse lookup Zone ---- 22
Figure 6 – Time synchronization Flow Diagram ---- 24
Figure 7 – OU Structure ---- 27
Figure 9 – Group Policy Assignment ---- 42
Figure 10 – Antivirus Design ---- 43
Figure 11 – ePolicy Console ---- 44
Figure 12 – Trellix Agent Interface ---- 44
Figure 13 – Yokogawa Standard Antivirus Software (ENS) Console ---- 45
Figure 14 – Yokogawa Standard Antivirus Software (ENS) Master Repository ---- 45
Figure 15 –Group Structure ---- 46
Figure 16 – OS Patch Management System Logical Architecture Overview ---- 51
Figure 17 – WSUS Administrative Console ---- 52
Figure 18 – WSUS update Report ---- 54
Figure 19 – VBR Login Window ---- 56
Figure 20 – Physical Infrastructure ---- 56
Figure 21 – Disk-Based Storage ---- 57
Figure 22 – Example of Backup Files (Physical Machine) ---- 57
Figure 23 – Centralized Backup Management Architecture Overview ---- 58
Figure 24 - Agent Backup Job – System Backup ---- 59
Figure 25 - Agent Backup Job – Data Backup ---- 60
Figure 26 – Veeam Login ---- 63
Figure 27 – Active Directory Users and Groups ---- 63
Figure 28 – Audit Log and Timestamps ---- 64
Figure 29 - Web Console Dashboard ---- 65
Figure 30 - WhatsUp Gold Monitored Device List Interface ---- 66
Figure 31 – NMS Architecture. ---- 66
Figure 32 –Configurations to monitor Vnet/IP through NMS. ---- 69
Figure 33 – WhatsUp Gold Map View ---- 70

This document undergoes an issuance cycle within EDMS Fusionlive. Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Figure 34 – WhatsUp Gold Device View ---- 71
Figure 35 – Application Whitelisting Architecture ---- 72
Figure 36 – Overall Firewall Design ---- 77
Figure 37 – Redundant Switch Configuration ---- 80
Figure 38 – Network Flow Diagram ---- 83

This document undergoes an issuance cycle within EDMS Fusionlive. Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

List of tables

Table 1 – Domain Names ---- 18
Table 2 – Active Directory Volume Details ---- 19
Table 3 – Forest & Domain Functional Levels ---- 20
Table 4 – Global Catalog Configurations ---- 20
Table 5 – Forward & Reverse Lookup Zones ---- 23
Table 6 – Organizational Unit ---- 26
Table 7 – Centum Security Groups ---- 28
Table 8 – Prosafe Security Groups ---- 28
Table 9 – PRM Security Groups ---- 28
Table 10 – CI Server Security Groups ---- 29
Table 11– Veeam Backup and Recovery Security Groups ---- 29
Table 12 – WSUS Security Groups ---- 29
Table 13 – Trellix Security Groups ---- 29
Table 14 – NMS Security Groups ---- 29
Table 15 – Basic Group Policy Object (GPO) ---- 30
Table 16 – CC_Password Policy ---- 31
Table 17–CC_Account Lockout Policy ---- 31
Table 18- CC_USB_CD_Block Policy ---- 32
Table 19 – CCUC_Domain Policy ---- 33
Table 20 – CIX_Security Policy ---- 34
Table 21 – CC_Audit EventLog Policy ---- 35
Table 22 – CC_OS Patch Policy ---- 36
Table 23 – CC_Administrative Templates ---- 39
Table 24 – CC_AD Time Sync Policy ---- 39
Table 25 – CC_Domain Controller Policy ---- 39
Table 26 – CC_SNMP and SSL Policy ---- 39
Table 27 – CC_Windows Firewall Policy ---- 40
Table 28 – CC_Remote Desktop Common Policy ---- 40
Table 29 – UC_Hardening ---- 41
Table 30 – Policy Product and Categories ---- 47
Table 31 – Yokogawa Standard Antivirus Software (ENS) Policy ---- 48
Table 32 – Yokogawa Standard Antivirus Software (ENS) Task ---- 48
Table 33 – On-Demand Scan ---- 49
Table 34 – Scanning Schedule ---- 49
Table 35 – Trellix ePO Log Category ---- 50

This document undergoes an issuance cycle within EDMS Fusionlive. Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

Table 36 – Troubleshooting Log File Category ---- 50
Table 38 – WSUS Server Firewall Ports ---- 53
Table 39 – WSUS Client Firewall Ports ---- 53
Table 40 – WSUS Client Policy ---- 53
Table 41 – Child Groups Created on the WSUS Management Server ---- 54
Table 42 – Schedule of WSUS Automated Tasks ---- 54
Table 43 – Schedule of WSUS automated tasks. ---- 55
Table 44 - Used Ports for Physical Machines ---- 59
Table 37 – BRS Backup Schedule ---- 61
Table 38 – BRS Client Backup Size Estimation ---- 62
Table 45 - User Assignment ---- 64
Table 46 – SNMP Settings for Windows ---- 70
Table 47 – SNMP Settings for Hirschman Switches ---- 70
Table 48 – ePO Policy Templates ---- 75
Table 49 - Solidcore Rules Import ---- 75
Table 49- System Tags Import ---- 76
Table 50 - Querying and Logging ---- 76

1 DEFINITIONS AND ABBREVIATIONS

1.1 DEFINITIONS

COMPANY or Client (CPY):	Crosswind
CONTRACTOR (CTR):	ROSETTI MARINO S.p.A.
PROJECT:	HOLLANDSE KUST NOORD WIND PARK Project

1.2 ABBREVIATIONS

• COTS	Commercial off-the-shelf
• HKN	Hollandse Kust Noord Wind Park Project
• BLPH	Base Load power Hub
• VooW	Van Oord Offshore Wind
• BESS	Base Load Power Hub
• ICS	Industrial Control System
• IACS	Industrial Automation & Control System
• AD DS	Active Directory Domain Services
• DC	Domain Controller
• DNS	Domain Name System
• GPO	Group Policy object
• FSMO	Flexible Single-Master Operational
• RID	Relative Identifier
• PDC	Primary Domain Controller
• FQDN	Fully Qualified Domain Name
• PTR	Pointer Record
• NTP	Network Time Protocol
• GPS	Global Positioning System
• IAMS	Instrument Asset Management System
• EWS	Engineering Workstation
• PIN	Plant Information Network
• OU	Organizational Unit
• HIS	Human Interface System
• ePO	ePolicy Orchestrator
• DMZ	Demilitarized Zone
• ENS	End Point Network Security
• FTP	File Transfer Protocol
• OER	Onshore Equipment Room
• SSL	Secure Socket Layer

• HTTPS	Hyper Text Transfer Protocol Secured
• VBR	Veeam Backup & Replication
• WUG	WhatsUp Gold
• TCP	Transmission Control Protocol
• UDP	User Datagram Protocol
• MIB	Management Information Base
• OID	Object Identifier
• SNMP	Simple Network Management Protocol
• ACL	Access Control List
• NMSSVR	Network Management Server
• DCSVR01	Domain Controller Server 1
• DCSVR02	Domain Controller Server 2
• AVSVR	Antivirus Server
• WSUS	Windows Server Update Service
• CISVR01 & CISVR02	CI Server
• EWS0164	Engineering Workstation
• RPO	Recovery Point Objective
• RTO	Recovery Time Objective

This document undergoes an issuance cycle within EDMS Fusionlive. Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

2 INTRODUCTION

2.1 PROJECT OVERVIEW

Crosswind, a Shell and Eneco joint venture, was awarded the tender to develop the offshore Hollandse Kust Noord (HKN) wind farm, located 18.5km off the coast of the Netherlands near the town of Egmond aan Zee. The consortium plans to have HKN operational in 2023 with an installed capacity of 759MW generating at least 3.3TWh per year. This is sufficient renewable power to supply more than 1 million Dutch households with green electricity.

Offshore wind farms produce intermittent electricity and balancing these dips and peaks and integrating this electricity into the national energy system requires new technologies. For this reason, the offshore wind farm will include several new technologies that could be implemented at full-scale in the future. The new technologies being explored include a floating solar park, a short-duration battery storage as well as long-term storage via green hydrogen produced by water electrolysis and subsequently consumed in a fuel cell. The combination of these individual measures, herein referred to as the Base Load Power Hub (BLPH) will ensure a continuous power supply regardless of the wind situation.

2.1.1 Project Location

The Hollandse Kust Noord (HKN) wind farm is located 18.5km off the coast of the Netherlands near the town of Egmond aan Zee.

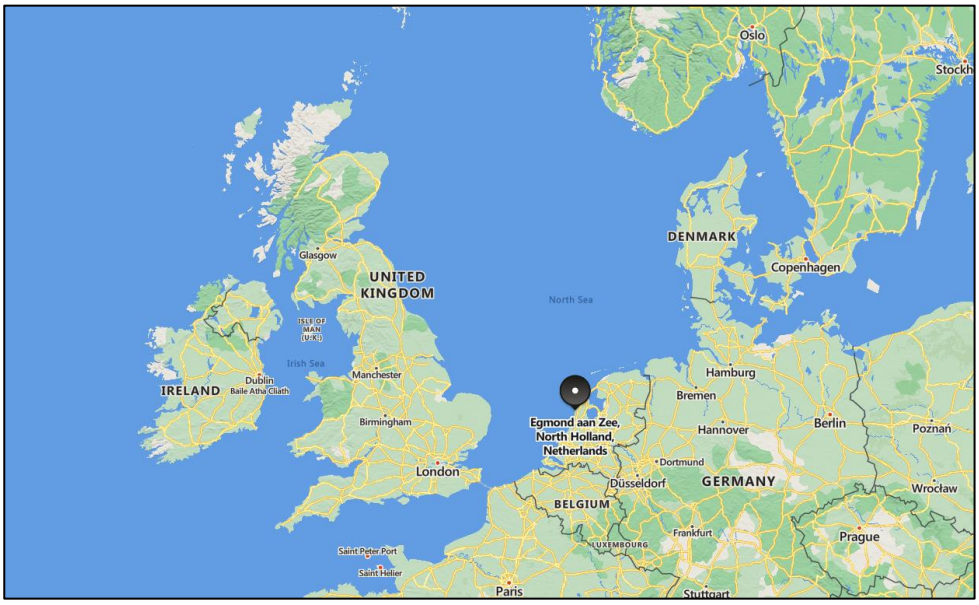


Figure 1- HOLLANDSE KUST NOORD WIND PARK Location Map

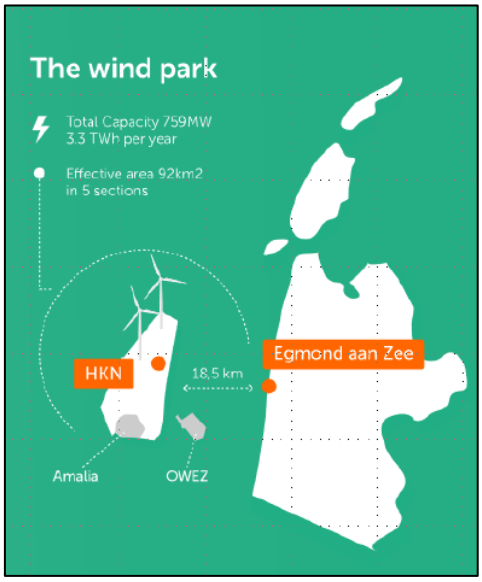


Figure 1 - Wind Park Details

The wind farm will consist of No. 69 x 11.5MW wind turbine generators each to be installed on a dedicated monopile structure. A 70th monopile located on coordinates E 590719.1, N 5841602.3 is reserved for installing the platform accommodating the BLPH. The monopile structure was designed and installed by Van Oord Offshore Wind (VooW) and therefore not part of the BLPH scope.

2.1.2 Project Concept

All components included in the BLPH will be integrated onshore on a topsides and installed in an offshore location within the boundaries of the HKN wind farm. At its simplest, the BLPH will store energy during periods of high electricity generation from renewable sources (a wind turbine generator and the floating solar PV farm) and release it during periods of low generation. In practice. It is expected that the energy stored will supplement generation from renewable sources to ensure that at least 1.0MW of power is exported to the electrical grid regardless of wind/solar availability.

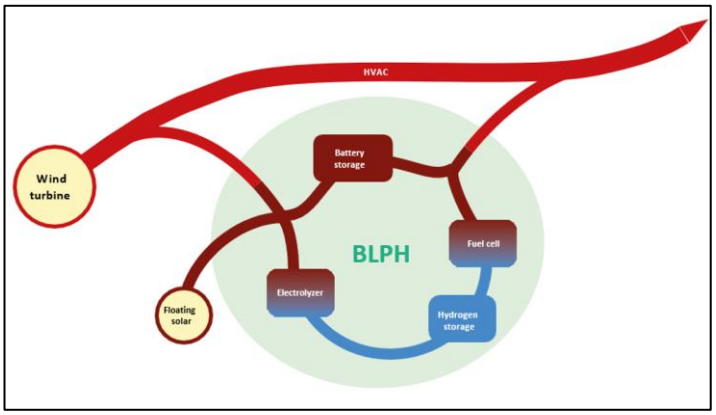


Figure 2 – BLPH Concept

Electricity in the BLPH will be stored in the form of electrons in a battery energy storage system (BESS) as well as converted into green hydrogen via water electrolysis. When the power output from the connecting wind turbine drops to below 1 MWe, the BLPH will return its stored energy to supplement the remaining power output. This will be by discharging the BESS, while stored hydrogen will be converted back into electricity using a fuel cell to extend the discharge duration.

The purpose of the BLPH is to function as a testbed for the integration of energy storage technologies with renewable generation. It is expected that equipment installed on the BLPH will operate as Normally Unmanned Installation for at

least two (2) years with no or minimal maintenance and it will have its own independent control room with the ability to communicate with Crosswind's control room.

3 NETWORK AND SECURITY SOLUTIONS (NSS)

Process automation systems have evolved from individual isolated computers with proprietary operating systems and networks to interconnected systems and applications employing commercial off-the-shelf (COTS) technology (i.e., operating systems and protocols). These systems are now being integrated with enterprise systems and other business applications through various communication networks. This increased level of integration provides significant business benefits, including:

- Increased visibility of process automation system activities (work in process, equipment status, production schedules) and integrated processing systems from the business level, which contributes to the improved ability to analyze to drive down production costs and improve productivity.
- Integrated manufacturing and production systems that have more direct access to business-level information, enabling a more responsive enterprise.
- Common interfaces that reduce overall support costs and permit remote support of production processes.
- Remote monitoring of the process automation system reduces support costs and allows problems to be resolved more quickly.

It is possible to define standards for models, terms, and information exchanges that allow the process automation system community to share information consistently. However, this ability to exchange information increases vulnerability to misuse and attack by individuals with malicious intent and introduces potential risks to the enterprise using a process automation system.

Process automation system operates within a complex environment. Organizations are increasingly sharing information between business and process automation systems, and partners in one business venture can be competitors in another. However, because process automation system equipment connects directly to a process, loss of trade secrets and interruption in the flow of information are not the only consequences of a security breach. The potential loss of life or production, environmental damage, regulatory violation, and compromise to operational safety are far more serious consequences. These have ramifications beyond the targeted organization; they can grievously damage the infrastructure of the host region or nation.

External threats are not the only concern; knowledgeable insiders with malicious intent or even an innocent unintended act can pose a serious security risk. Since process automation systems are often integrated with other business systems, modifying or testing operational systems has led to unintended electronic effects on system operations.

Although technology changes are good for business, they increase the potential risk of compromising security. As the threats to business increase, so does the need for security.

3.1 OVERVIEW OF SECURITY SOLUTIONS

The CROSSWIND-BLPH project comprises the following Network & Security Solutions.

- Windows Domain and Account management
- Anti-virus Software Management
- OS-Patch Management
- Backup and Recovery Management
- Network Management System
- Application Whitelisting
- Firewall
- Switches

4 WINDOWS DOMAIN AND ACCOUNT MANAGEMENT

As network threats and attacks become more prevalent even in ICS environments, the need for securing networks has also been on the rise. Authenticating user login sessions, centrally managing computer policies, and imposing user-based restrictions are just a few ways to reduce the attack surface.

Having a centralized user account and computer setting management solution will address this need. The deployment of Domain Controllers, via Microsoft Active Directory Domain Services, in a network will also ease the administrative overhead of managing computers and user accounts.

In CROSSWIND-BLPH Windows Domain and Account Management will be implemented through Microsoft Active Directory Services(AD DS) using Windows Server 2022.

4.1 Background

AD DS is a server role in Microsoft Windows Server that enables an administrator to create a scalable, secure, and manageable infrastructure for user and resource management and provide support for directory-enabled applications. AD DS provides a distributed database that stores and manages information about network resources and application-specific data from directory-enabled applications.

4.2 Active Directory Fundamentals

In a Microsoft Active Directory logical structure, the core units are forests, trees & domains. A Domain is the boundary of the scope of an Active Directory implementation. In its simplest form, a forest is a single domain. A forest can contain multiple domains, and each new domain created with its unique namespace establishes a new tree within the forest. Grouping objects into one or multiple domains allows the Active Directory to reflect the organization. All network objects exist within a domain, and each domain stores only the information about the objects that it contains.

A Domain is an administrative boundary for the directory database. Each domain has its own unique accounts database. Thus, authentication is on a domain basis. Once a user account is authenticated to a domain, that user account has access to resources within that domain.

A Domain controller (DC) is a server that manages the Active Directory database to respond to security authentication requests (logging in, checking permissions, etc.) within the domain. At least one domain controller is necessary for installing an Active Directory domain. A redundant or secondary domain controller is recommended for fault tolerance and load balancing.

A Forest is a grouping or hierarchical arrangement of one or more transitive, trust-linked trees. It is the top functional level of an Active Directory structure.

A Tree is a transitive, trust-linked grouping, or hierarchical arrangement of one or more Windows domains. Domains are identified by their DNS name structure, the namespace.

A Organizational Units(OU) is a container used to organize and manage objects such as users, groups, computers, and other resources within a domain.

The Microsoft Active Directory Domain Services (AD DS) can organize resources in a logical structure. Grouping resources logically enables finding a resource by its name rather than by its physical location. The logical structure is composed of objects, organizational units, domains, trees, and forests.

It is vital to have control and management over all the objects to control the number of repositories in use, reduce administrative overheads, enhance operational efficiency, and have tighter control over the security of user information. It can carry out single sign-on to network resources; lockdown desktop configurations prevent access to specific operations such as software installation or registry editing, and set access control privileges on directory objects. AD DS centralizes identity management and supports role-based security.

Host Name	Domain Name	Site
DCSVR01 (Primary DC)	BLPH.OT.CROSSWINDHKN.NL	Default site
DCSVR02 (Secondary DC)	BLPH.OT.CROSSWINDHKN.NL	Default site

Table 1 – Domain Names

4.3 Design Architecture: Overview

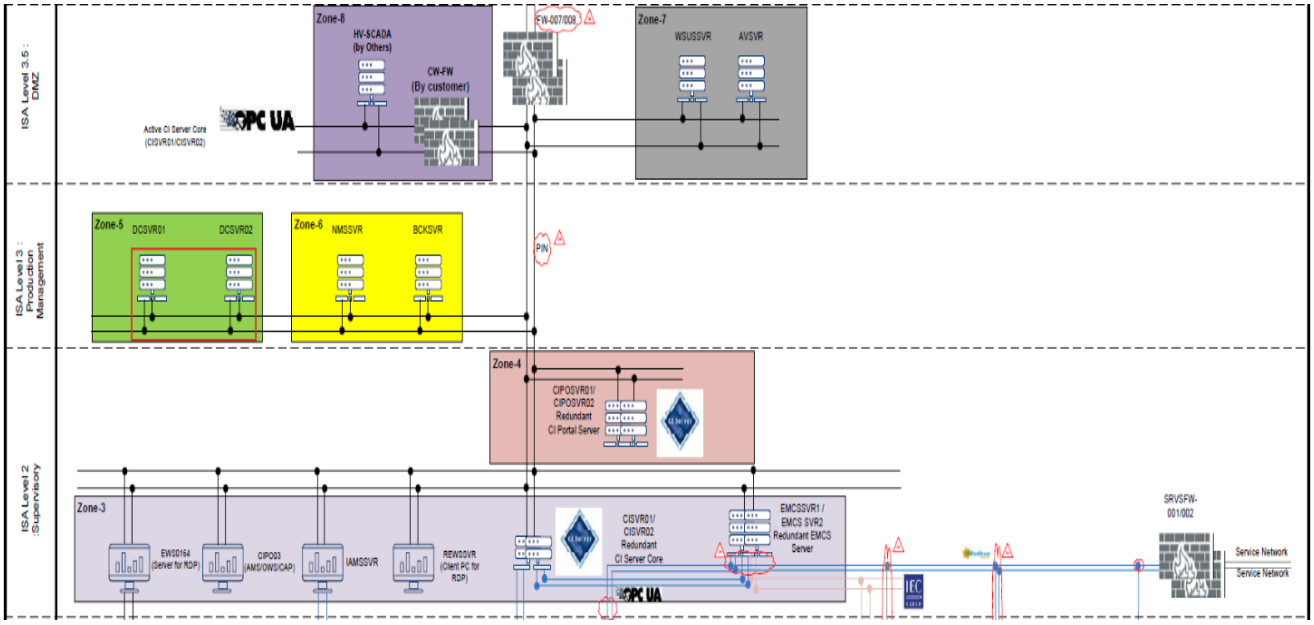


Figure 3 – Windows Domain and Account Management Design Architecture

In the Crosswind-BLPH project, DCSVR01 is considered as primary DC, and DCSVR02 as the secondary DC. The Domain Controllers shall facilitate:

- Centralized management of domain objects
- Authentication and authorization
- Users and devices provisioning
- Least privilege principle and segregation of permissions
- Physical and technical security controls using GPOs
- Time synchronization

4.4 Detail Design

4.4.1 Active Directory volumes

The Active Directory database, containing the OS volume (SYSVOL), the database information volume, and the Active Directory log files volume shall be deployed on three separate volumes as per Microsoft best practices in the locations detailed in the table below. In this project, the installation volumes will be located as follows on both domain controllers (DCSVR01 & DCSVR02).

Items	Location
The Operating system volume	C:\WINDOWS\SYSVOL
The Active Directory database information volume	C:\WINDOWS\NTDS
The Active Directory log files volume	C:\WINDOWS\NTDS

Table 2 – Active Directory Volume Details

4.4.2 Forest and Domain Functional Level

Functional levels determine the available AD DS domain or forest capabilities. They also determine which Windows operating systems will be able to run on the domain controller in the domain or forest. As per Microsoft best practices, the domain functional level and the forest functional level shall be implemented to the latest available version. Following the best practices from Microsoft, Yokogawa shall ensure the IACS Windows Environment Active Directory

is implemented with up-to-date features to perform optimal management of the OT domain. Though we are using Windows Server 2022 the latest available domain and forest functional level is Windows Server 2016.

Domain Controller	Domain Functional Level	Forest Functional Level
DCSVR01 (Primary DC)	Windows Server 2016	Windows Server 2016
DCSVR02 (Backup DC)	Windows Server 2016	Windows Server 2016

Table 3 – Forest & Domain Functional Levels

4.4.3 Flexible Single-Master Operational (FSMO) Roles

Microsoft Active Directory can consist of multiple domain controllers and can utilize multi-master replication among its domain controllers. This means every domain controller is capable of handling both read and write operations. At any time, more than one source can receive changes to the same database; hence conflicts can occur. If a conflict does occur, the Windows server system does have built-in mechanisms for resolution. These built-in mechanisms are called FSMO (Flexible Single Master Operation) roles. These operations are handled by only one domain controller either per domain or per forest depending on the operation.

The five FSMO roles are:

- Schema Master - Only one server can perform write operations to the directory schema.
- Domain Naming Master - Only one server can add/remove domains in the forest and add/remove cross-referenced objects to external directories.
- RID (Relative Identifier) Master - Controls the pools of security IDs available for the creation of objects.
- PDC (Primary Domain Controller) Emulator - Responsible for keeping the time Synchronized on all the DCs within a domain. Password changes performed by other DCs in the domain are replicated preferentially to the PDC emulator
- Infrastructure Master - Responsible for updating an object's SID and distinguished name in a cross-domain object reference

These five FSMO roles shall be hosted on the primary domain controller for CROSSWIND-BLPH.

4.4.3.1 Global Catalog (GC)

Another important role for Windows server 2022 is the global catalog server. The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain. It is stored on domain controllers(DCSVR01 & DCSVR02) that have been designated as global catalog servers.

The global catalog is built and updated automatically by the Active Directory multi-master replication system. Configuration will be done as per below table for CROSSWIND-BLPH Project.

Name of DC	Global Catalog	FSMO Roles					Active Directory Integrated DNS Server
		Schema Master	Domain Naming Master	RID Master	PDC Emulator	Infrastructure Master	
DCSVR01 (Primary)	✓	✓	✓	✓	✓	✓	✓
DCSVR02 (Backup)	✓	×	×	×	×	×	✓

Table 4 – Global Catalog Configurations

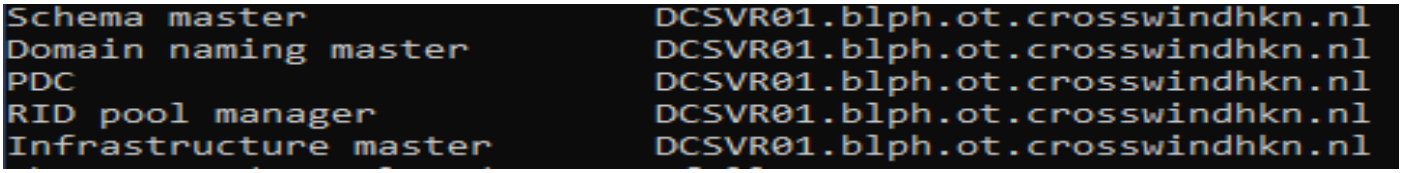


Figure 5 – FSMO Configuration.

4.4.4 Active Directory Sites

Sites in Microsoft Active Directory represent the physical structure, or topology, of a network. The Active Directory shall be deployed with a single default site to map the physical structure of a network. This deployment model shall ensure whether replication and authentication functionality are performing correctly. At the initial deployment stage, the Active Directory site name is "Default-First Site-Name".

Sites help facilitate several activities within Active Directory:

- Replication: Active Directory balances the need for up-to-date directory information with the need for "bandwidth optimization" (useful for remote locations with low bandwidth) by replicating information within a site more frequently than between sites.
- Authentication: Site information helps make authentication faster and more efficient. When a client logs on to a domain, it first searches its local site for a domain controller to authenticate against.

Active Directory, sites map the physical structure of a network, while domains map the logical or administrative structure of an organization.

4.4.5 DNS Structure

DNS is a very important aspect of the Windows system and is the prerequisite for Active Directory to function. DNS provides the resolution of computer names to their corresponding IP addresses and vice versa for various network and application communications. Active Directory domains are named with DNS names. This is because Active Directory uses DNS as its service location protocol. Windows Domain members requesting to log on to the network will query DNS to locate domain controllers.

For designing an Active Directory DNS structure, the following are five important factors:

- DNS redundancy.
- Dynamic updating for hosts.
- Forward & Reverse lookup zones.
- DNS zone replications.
- DNS suffixes configuration for computers

4.4.5.1 DNS redundancy

In CROSSWIND-BLPH, the DNS role shall be configured on both the domain controller servers(DCSVR01 & DCSVR02). The DNS servers are responsible for resolving hostnames employing FQDN that has "BLPH.OT.CROSSWINDHKN.NL" as a suffix.

4.4.5.2 Dynamic updating for hosts

Dynamic updating allows computers to dynamically update their host records if there is a change in hostname or IP address. Both forward and reverse lookup zones support two types of dynamic updating:

- Secure Only: Allows only authorized hosts to update themselves to the DNS server.
- Non-Secure and Secure: Allows unauthorized hosts to update themselves to the DNS server.

The CROSSWIND-BLPH shall be configured with Secure Dynamic Update.

4.4.5.3 Forward & Reverse Lookup Zones

- **Forward Lookup Zone:** Forward lookup zones map computer names to IP addresses.

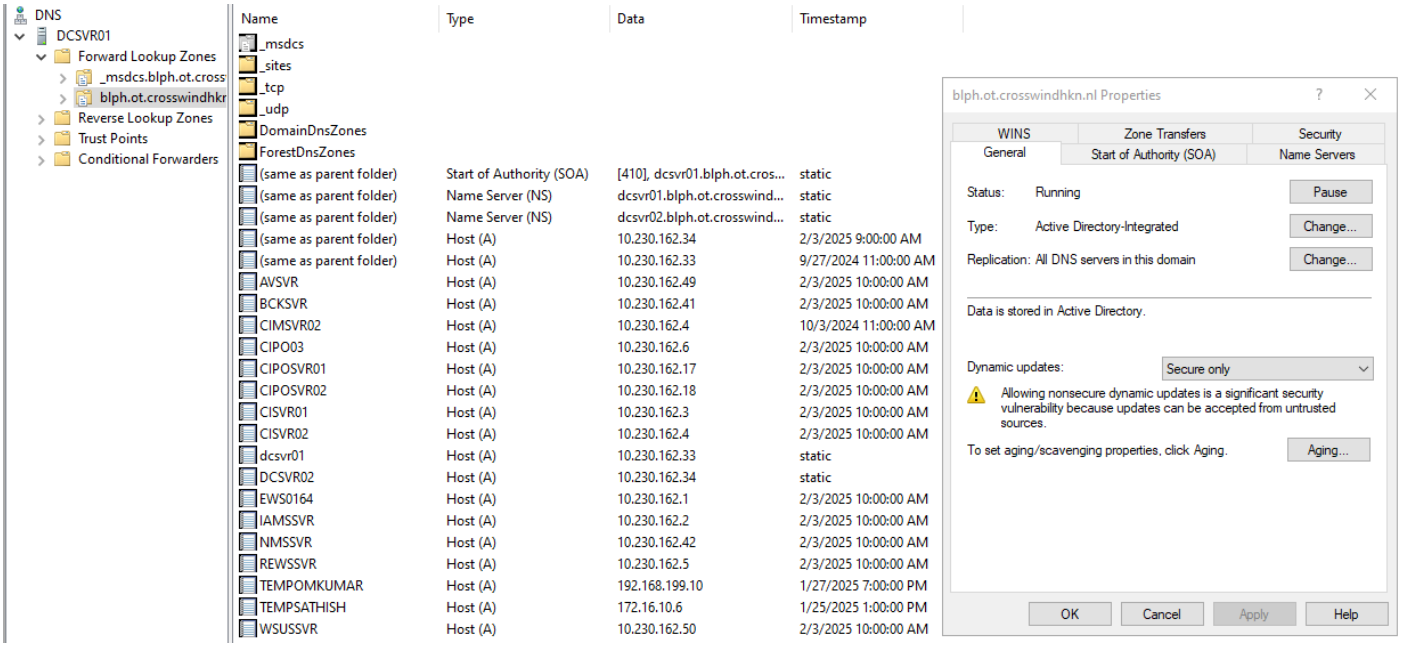


Figure 4 – Dynamic Updating Setting for the default Forward lookup Zone

- **Reverse Lookup Zones:** Reverse lookup zones do the opposite of the forward lookup zone. It resolves a computer's IP address to its corresponding name. The reverse lookup zone does not differentiate between a workgroup or domain computers. Instead, it uses a reversal of the IP address subnet (called in-addr.arpa domain) which creates a PTR record that maps to the correct corresponding host record in the forward lookup zones. It is to be noted that Reverse Lookup Zone(s) should be created manually.

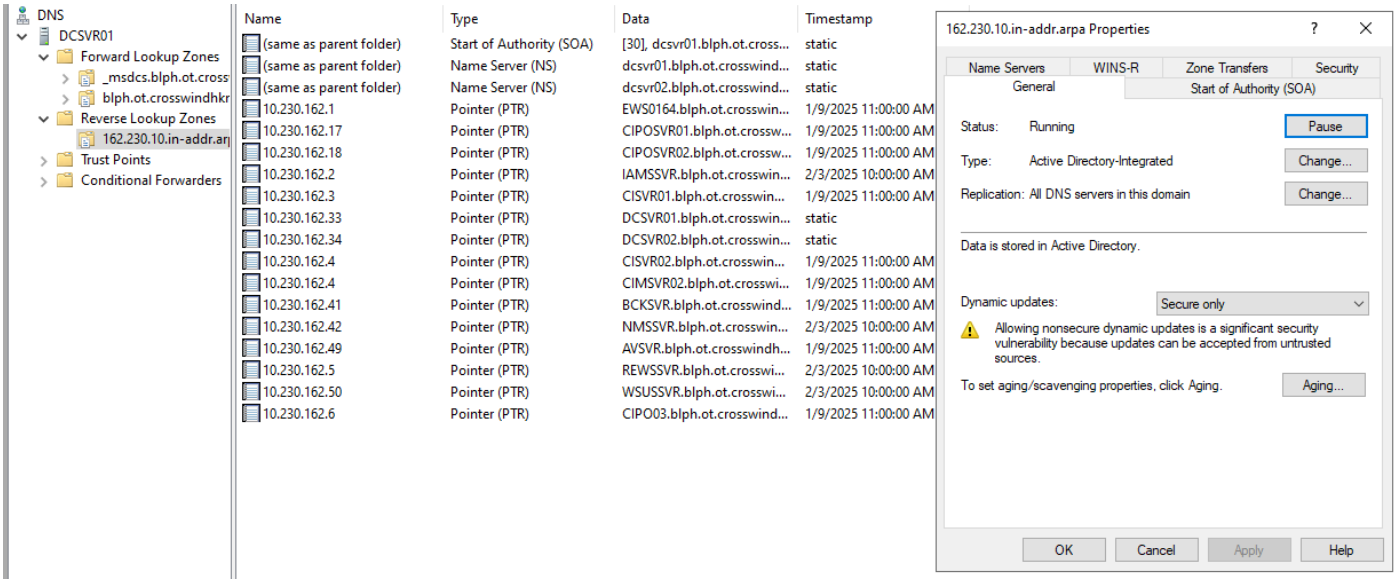


Figure 5 – Dynamic Updates Setting for the Reverse lookup Zone

4.4.5.4 DNS zones replications

The databases in the DNS server shall be replicated among each other to maintain database consistency through the IACS Windows Domain Environment. The replication mechanism designed by Microsoft is multi-master, thus any change performed into any domain controller shall automatically be replicated to the other domain controllers. In this way, if DNS is integrated into the Active Directory service, the replication engine will always synchronize the DNS zone information.

In CROSSWIND-BLPH DNS zone replication shall be configured as AD Integrated.

Lookup Zone Type	Zone Names	Zone Type	Dynamic Update Type	Replication
Forward Lookup	BLPH.OT. CROSSWINDHKN.NL	Active Directory Integrated	Secure only	All DNS servers in the Active Directory domain
Reverse Lookup	162.230.10in-addr.arpa	Active Directory Integrated	Secure only	All DNS servers in the Active Directory domain

Table 5 – Forward & Reverse Lookup Zones

4.4.5.5 DNS suffixes configuration for computers

In CROSSWIND-BLPH, DCSVR01 is preferred as the primary DNS server, and DCSVR02 is the Backup DNS Server. The DNS suffix will be added in the NIC settings as "BLPH.OT.CROSSWINDHKN.NL".

4.5 Time synchronization

The Windows Domain Environment components that are not equipped with a Vnet/IP card shall synchronize their time using GPO-enforced settings in combination with an NTP. An NTP time source shall be available for the domain controller to read and distribute using time server settings for the rest of the clients.

In the Crosswind-BLPH project, the NTP Server will receive its time from the GPS clock. Figure 4 shows how Workstations and Server are connected to the NTP Server for Time Synchronization.

- Domain Controllers and Time Master (Vnet/IP), will sync with an external Reliable Time provider (e.g. GPS Network Time Server).
- All Vnet/IP Devices such as EWS, and IAMS receive their time from Time Master.
- All Non-Vnet/IP Devices such as NMS, AV, and WSUS Servers receive their time from Domain Controller.

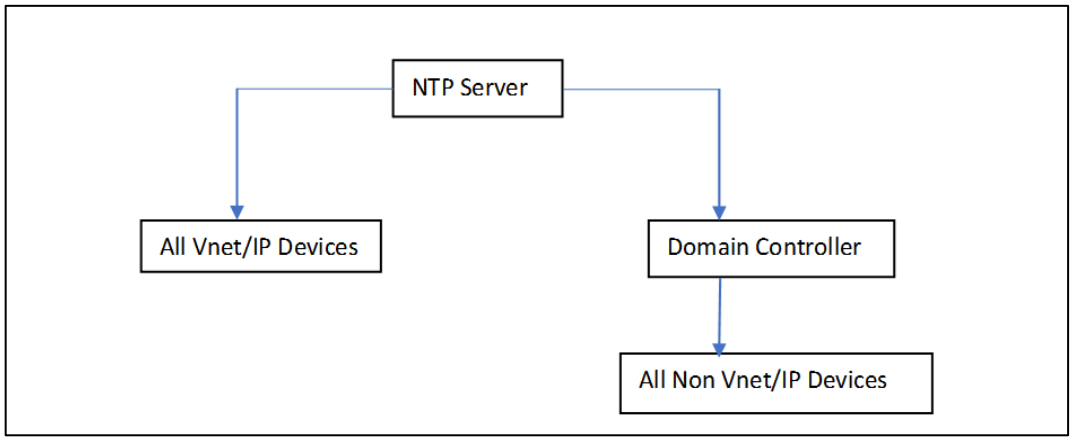


Figure 6 – Time synchronization Flow Diagram

Kerberos is the network authentication protocol that Active Directory domain members use when logging on to the domain. To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in sync as much as possible. In other words, both computers need to be set to the same time and date.

By default, the tolerated time difference is set at 5 minutes. If the difference between a domain member's clock and the domain controller's clock is more than this maximum time difference, any timestamp used in a session between the two computers will be not authenticated and will result in logon failure.

4.6 Active Directory Structure

Microsoft Active Directory Domain Services provides many features, mostly essential for the distributed computing environment that exists today. Some of them are

- Flexibility in grouping similar users logically.
- Access & permissions control through nesting of domain groups into local groups.
- Customization of available features & permissions through application Group Policy Objects (GPO).

4.6.1 Organizational Unit (OU)

Organizational units are Active Directory containers into which you can place users, groups, computers, and other organizational units. The objects held within a domain can be grouped into organizational units (OUs).

The main functions of OUs inside the IACS domain shall be to support the visual organization of objects, to group objects to manage the assignment of group policies, and to group objects to facilitate the delegation of permission for users and computers. The OUs in the Windows Domain environment shall be used to delegate administrative authorization and apply GPOs. The OUs structure shall be available only for Domain Admins and Enterprise Admins. Important points to consider about the use of OU are as follows:

- OU can be nested
- OU can be used to delegate administration
- OU are not security principals
- Group policy can be applied to an OU
- OU naming conventions and tree structures are flexible and relatively simple to change
- Users will not typically navigate the OU structure

OUs are organized to provide a hierarchy that eases applying group policies & thereby better control and can resemble the organization's structure. Different systems with similar properties are grouped to have better control and maintenance.

4.6.1.1 Design Considerations

The creation of OUs shall be done for the delegation of administration and the application of group policy objects as much as possible. The below OUs are identified for the CROSSWIND-BLPH project:

OU Name	SUB OU	Nested OU	Remarks
Builtin	-	-	Default OU
Computers	-	-	Default OU
Users	-	-	Default OU
Foreign Security Principals	-	-	Default OU
Managed Services Accounts	-	-	Default OU
Domain Controllers	-	-	Default OU
Crosswind	CIX	CIX_Security Groups	OU for the CI Server Security Group
		CIX_Servers&Workstations	OU For the CI Server, Portal and View
	VNET	VNET_Secuirty Groups	OU For the VNET Security Group
		VNET_Server&Workstations\CTM&PSF_Servers	OU for the Centum and Prosafe Application Servers
		VNET_Server&Workstations\IAMS&PRM_Servers	OU for the IAMS and PRM Servers
	NSS	NSS_Security Groups\AV_Groups	OU for the AV Application RBAC
		NSS_Security Groups\NMS_Groups	

OU Name	SUB OU	Nested OU	Remarks
			OU for the NMS Application RBAC
		NSS_Security Groups\WSUS Groups	OU for the WSUS Application RBAC
		NSS_Security Groups\VEEAM Groups	OU for the VEEAM Application RBAC
		NSS_Servers&Worksations	OU for the Cyber security Servers and Workstations
	CW_Domain Users	CW_Engineer Group	
		CW_Maintenance Group	
		CW_Operator Group	
	CW_Service Account		

Table 6 – Organizational Unit

4.6.2 Users and Groups

4.6.2.1 Users

In Active Directory, Users OU contains the Domain Administrator along with some default groups of the domain. Generally, a user can be created in the domain in any OU by simply right-clicking on the OU and selecting a new user. All users that shall operate, maintain, supervise, or administrate the IACS workstations, servers, or software platform that require authentication, shall be defined inside Active Directory. Only users that shall be authenticated against the Active Directory shall be granted access to devices. Local administrators shall be disabled on all devices.

4.6.2.2 Groups

A group is a collection of user and computer accounts. Users and computers that belong to a group are referred to as group members. Groups can be used to simplify administration by assigning a common set of permissions and rights to many accounts at once, rather than assigning permissions and rights to each account individually. Groups in Active Directory are directory objects that reside within a domain and organizational unit container objects. Active Directory provides a set of default groups upon installation and allows the option to create groups.

Default Grouping: Whenever a system is migrated from a workgroup to a domain, by default

- The "Domain Admins" group of domain controllers shall become a member of the administrators' group of the system
- The "Domain Users" group of the domain controller shall become a member of the user's group of the system.

User Security Grouping: Along with other process control requirements within a plant, all users within a plant Active Directory are created and assigned appropriate rights using the user security groups. Windows Server 2022 supports three types of user security groups:

1) Domain Local Groups

    - Only available in native mode domains,

- Can contain members from anywhere in the forest, in trusted forests, or a trusted pre-Windows 2000 domain,
- Can only grant permissions to resources within the domain in which they exist,
- Typically used to gather security principals from across the forest to control access to resources within the domain.

2) Global Groups

- Are effectively the same as Windows NT global groups,
- Can only contain members from within the domain in which they exist,
- Can be granted permission to resources in any domain in the forest or trusted forests.

3) Universal Groups

- Can contain members from any Windows 2016 domain in the forest,
- Can be granted permission in any domain in the forest or trusted forests.

Though it is possible to add users to a universal group, it is recommended to restrict membership to global groups. In Crosswind-BLPH project Global Groups is considered for User Security Groups.

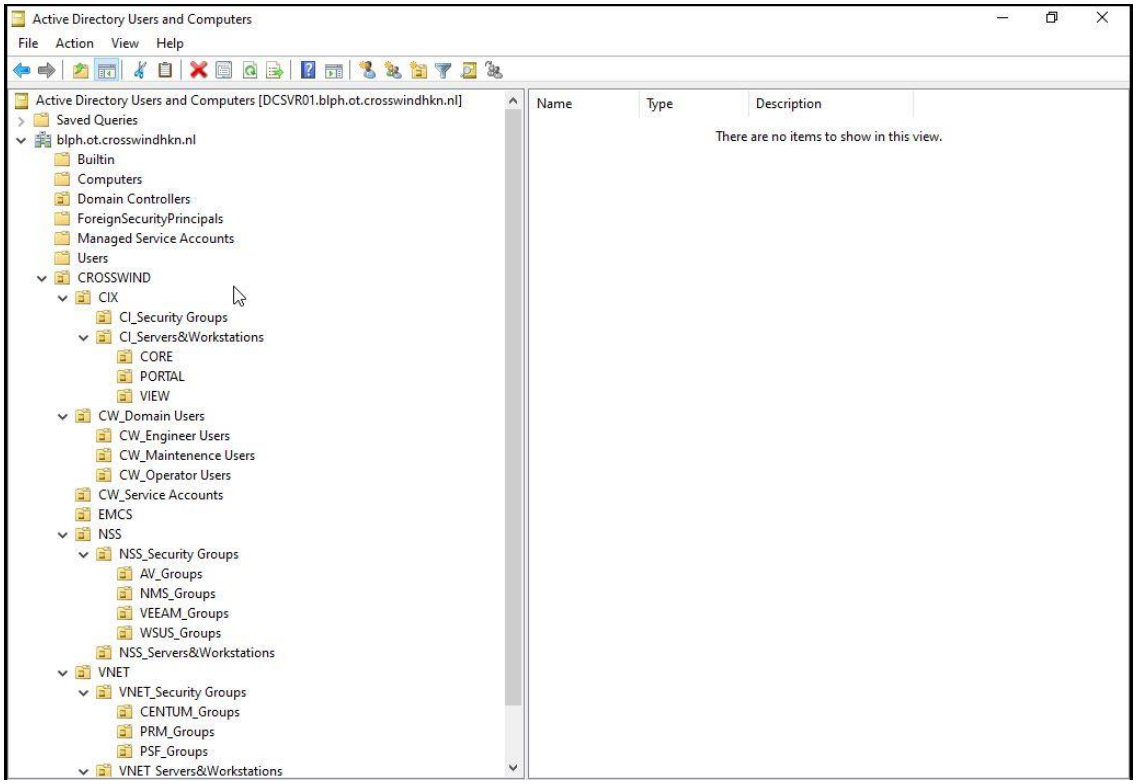


Figure 7 – OU Structure

4.6.2.3 Role based Access Control Security Groups.

RBAC is based on the concept of roles and privileges. Access is based on factors such as authority, competency, and responsibility. Network Object access and other resources - such as access to specific files or programs can be limited to each role, these roles will have different sets of authorization that shall be defined from the active directory to the member machine, administrator, or specialist user. These roles can also overlap or give different permission levels to specific roles

The following defines the users/group account and access requirement for Yokogawa IA System products (Centum VP, PROSAFE, PRM, CI-Server) and Network solutions (Backup & Replication, WSUS, AV, NMS) for the Crosswind-BLPH project.

4.6.2.3.1 CENTUM Security Groups

This is the critical security groups that control the authorization for the Centum (DCS) Applications.

SN. No	Groups	Domain Group	Descriptions
1.	CTM_MAINTENANCE	Domain Admins	Permission for CENTUM maintenance right
2.	CTM_ENGINEER_ADM	Domain Users	Permission for CENTUM system view, and so on. With privileges superior to the CTM_ENGINEER
3.	CTM_ENGINEER	Domain Users	Permission for CENTUM system view, and so on.
4.	CTM_OPERATOR	Domain Users	Permission for Operator access
5.	CTM_OPC	Domain Users	Permission for OPC communication with Centum

Table 7 – Centum Security Groups

4.6.2.3.2 PROSAFE Security Groups

This is the most critical security groups that control the authorization for the PROSAFE (Safety Control Systems) Applications

SN. No	Groups	Domain Group	Descriptions
1.	PSF_MAINTENANCE	Domain Admins	Permission for ProSafe-RS maintenance by SE (at the time of system construction)
2.	PSF_UTL	Domain Users	Permission for entry of the user who analyze data
3.	PSF_ENGINEER	Domain Users	Permission for ProSafe-RS Engineering.
4.	PSF_OPERATOR	Domain Users	Permission for Operator access
5.	PSF_OPC	Domain Users	Permission for OPC communication with ProSafe

Table 8 – Prosafe Security Groups

4.6.2.3.3 PRM Security Groups

This is the critical security groups that control the authorization for the PRM Applications.

SN. No	Groups	Domain Group	Descriptions
1.	PRM_MAINTENANCE	Domain Admins	Permission for PRM maintenance by SE (at the time of system construction)
2.	PRM_ENGINEER	Domain Users	Permission for PRM engineering such as using the PRM Setup Tool and the Integration Wizard
3.	PRM_USER	Domain Users	Permission for running the PRM system
4.	PRM_OPC	Domain Users	Permission for OPC Communication with PRM

Table 9 – PRM Security Groups

4.6.2.3.4 CI Server Security Groups

This is security groups that control the authorization for the CI Server Applications.

SN. No	Groups	Domain Group	Descriptions
1.	CIX_MAINTENANCE	Domain Admins	Group of users who perform CI Server installation and maintenance.
2.	CIX_ENGINEER	Domain Users	Group of users who perform CI Server system engineering by using the Engineering Module, Edit Module. and so on.
3.	CIX_OPERATOR	Domain Users	Group of users who use CI Server for operation.

SN. No	Groups	Domain Group	Descriptions
4.	CIX_OPC	Domain Users	Group of users who configure and manage OPC communication between CI Server and other systems.

Table 10 – CI Server Security Groups

4.6.2.3.5 Veeam Backup and Recovery Security Groups

This is security groups that control the authorization for the Veeam Backup and Recovery application and operation.

SN. No	Groups	Domain Group	Descriptions
1.	VEEAM_ MAINTENANCE	Domain Admins	Permission to user to have administrative right to local machine
2.	VEEAM_OPERATOR	Domain Users	Permission to user to have operation and monitoring right to Backup Recovery

Table 11– Veeam Backup and Recovery Security Groups

4.6.2.3.6 WSUS Security Groups

This is the security groups that control the authorization for the WSUS Server.

SN. No	Groups	Domain Group	Descriptions
1.	WSUS APPROVER	Domain Admins	Permission to user to have approval right to Patch Management Server
2.	WSUS_OPERATOR	Domain Users	Permission to user to have generation report right to Patch Management Server

Table 12 – WSUS Security Groups

4.6.2.3.7 Trellix Security Groups

This is the security groups that control the Trellix application and operation of the Antivirus.

SN. No	Groups	Domain Group	Descriptions
1.	AV_ADMIN	Domain Admins	Group of users with administrative permission on the le. Users within this group can edit settings and approve Polices on the Trellix ePO
2.	AV_ENGINEER	Domain Users	Group of users who can engineer the Polices on the Trellix ePO
3.	AV_OPERATOR	Domain Users	Group of users who has the Read only assess to the Operator Dashboards
4.	AV_SUPERVISOR	Domain Users	

Table 13 – Trellix Security Groups

4.6.2.3.8 NMS Security Groups

This is the security groups that controls the WhatsappGold application and operations.

SN. No	Groups	Domain Group	Descriptions
1.	NMS_ MAINTENANCE	Domain Admins	Group of users with administrative permission on the WUG Console. Users within this group can edit settings and make configurations on the WUG Console
2.	NMS_OPERATOR	Domain Users	Group of users with read-only permission on the WUG Console. Users within this group can view client status and reports generated by WUG

Table 14 – NMS Security Groups

4.7 Group Policy Objects

Group Policy Object (GPO) is a virtual collection of policy settings that will be applied to an OU, an active directory object, or to a user to unify security settings amongst domain members and control the behaviour of applications and network resources.

A GPO object is the combination of two types of configurations, a computer configuration and a user configuration.

1) **Computer Configurations(CC):** Settings that are under this configuration affect the computer as a whole and apply to any users who log on to this computer. Changes to settings under this configuration typically required a computer restart to bring about the changes.

2) **User Configurations(UC)**: Settings that are under this configuration affect only those users and apply to the user regardless of any domain computer that the user logs on. Changes to settings under this configuration typically required a user's logoff/logon from a computer to bring about the changes.

During the deployment stage of the Domain Controllers, the Yokogawa IT Security tool shall be on it, for each Yokogawa project-specific software. In doing so, the hardening of the Domain Controller shall be at a similar level as the Yokogawa workstations and servers. By default, two policies are created upon the installation of Active directory

1) Default Domain Policy

2) Default Domain Controller Policy

These policies contain the pre-defined settings at both the domain and the domain controllers. As per Microsoft's best practice, the above two default policies should not be used or modified. Instead, a copy of these policies should be made, and any modifications should be made only on the copies of these policies.

The following GPO shall be used for CROSSWIND-BLPH.

Sno.	Policy Name
1	- CC_**Password Policy**
2	17-CC_**Account Lockout Policy**
3	18- CC_USB_CD_**Block Policy**
4	- CCUC_**Domain Policy**
5	- CIX_**Security Policy**
6	- CC_Audit **EventLog Policy**
7	- CC_OS **Patch Policy**
8	- CC_**Administrative Templates**
9	- CC_AD Time **Sync Policy**
10	- CC_Domain **Controller Policy**
11	- CC_SNMP and **SSL Policy**
12	- CC_Windows **Firewall Policy**
13	CC_Remote_Desktop_Policy
14	UC_Operator_Hardeing Policy

Table 15 – Basic Group Policy Object (GPO)

Sub-category	Definition	Setting
Minimum password length	Set the password to meet the password length requirement	(8 characters)
Password must meet complexity requirements.	Set the password to meet the password complexity requirement	(Enabled)
		Consisting of a combination of at least three of the following four-character sets:
		Lowercase letters
		Uppercase letters
		Numeric digits
		Special characters
Password Age	Set the maximum and minimum length of the password age.	(Maximum of 90 days)
		(Minimum of 1 day)
Enforce password history	Set the number of times previously used passwords can be reused.	(24 passwords remembered)

Table 16 – CC_Password Policy

Sub-category	Definition	Setting
Account lockout threshold	Set the number of consecutive failed authentication login attempts before an account is lockout	(10 invalid logon attempts)
Account lockout duration	Set the time to wait for subsequent automatic unlock of the account	(15 Minutes)
Reset account lockout counter after	Set the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts.	(10 Minutes)

Table 17–CC_Account Lockout Policy

Sub-Category	Policy	Setting
Device Installation Restrictions	Allow administrators to override Device Installation Restriction policies	(Enabled)
	Display a custom message when installation is prevented by a policy setting	(Enabled <"Device Installation is prevented by Crosswind">
	Display a custom message title when device installation is prevented by a policy setting	(Enabled: <" Unauthorized Access.">
Administrative Templates > System/Removable Storage Access		
	CD and DVD: Deny execute access	(Enabled)
	CD and DVD: Deny read access	(Enabled)
	CD and DVD: Deny write access	(Enabled)
	Floppy Drives: Deny execute access	(Enabled)
	Floppy Drives: Deny read access	(Enabled)
	Floppy Drives: Deny write access	(Enabled)
	Removable Disks: Deny execute access	(Enabled)
	Removable Disks: Deny read access	(Enabled)
	Removable Disks: Deny write access	(Enabled)
	WPD Devices: Deny read access	(Enabled)

This document undergoes an issuance cycle within EDMS Fusionlive. Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

	WPD Devices: Deny write access	(Enabled)
Preferences > Registry	Start Order: 1 Key Path	SYSTEM\ControlSet001\Services\cdrom
	Start Order: 1 Value data	0x4 (4)
Preferences > Registry	Start Order: 2 Key Path	SYSTEM\ControlSet001\Services\USBSTOR
	Start Order: 2 Value data	0x4 (4)
Preferences > Registry	Start Order: 3 Key Path	SYSTEM\ControlSet001\Services\flpydisk
	Start Order: 3 Value data	0x4 (4)
Preferences > Registry	Start Order: 4 Key Path	SYSTEM\ControlSet001\Services\sfloppy
	Start Order: 4 Value data	0x4 (4)

Table 18- CC_USB_CD_Block Policy

Sub-category	Definition	Setting
Enforce user logon restrictions	Determines whether the Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the user account.	(Enabled)
Maximum lifetime for a service ticket	Determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service.	(600 minutes)
Maximum lifetime for user ticket	Determines the maximum amount of time (in hours) of a user's TGT (ticket-granting ticket).	(10 hours)
Maximum lifetime for user ticket renewal	Determines the period (in days) during which a user's TGT can be renewed.	(15 days)
Maximum tolerance for computer clock synchronization	Determines the maximum time difference (in minutes) that the Kerberos protocol allows between the time on the client computer's clock and the time on the domain controller that provides Kerberos authentication.	(5 minutes)
Deny log on locally		BLPH\CIX001
Deny log on through Terminal Services		BLPH\CIX001
Log on as a batch job		BLPH\CIX001,BLPH\AV_Service Account
Log on as a service		BLPH\CIX001,BLPH\AV_Service Account
Accounts: Guest account status		(Disabled)

Accounts: Rename administrator account		
Network access:Allow anonymous SID/Name translation		(Disabled)
Interactive logon: Prompt user to change password before expiration		10 days
Network security:Do not store LAN Manager hash value on next password change		(Enabled)
Network security:Force logoff when logon hours expire		(Disabled)
Shutdown:Allow system to be shut down without having to log on		(Disabled)
User Account Control:Admin Approval Mode for the built-in administrator account		(Enabled)
User Account Control:Behaviour of the elevation prompt for the administrators in admin approval mode		Prompt for consent
User Account Control:Behaviour of the elevation prompt for the standard users		Prompt for credentials
Audit:Force audit policy subcategory settings(Windows Vista or later) to override auidt policy category settings		(Enabled)

Table 19 – CCUC_Domain Policy

Services	Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	(Disabled)
Store passwords using reversible encryption	(Disabled)
Account lockout threshold	0 invalid logon attempts
Accounts: Guest account status	(Disabled)
Devices: Prevent users from installing printer drivers	(Enabled)
Devices: Restrict CD-ROM access to locally logged-on user only	(Enabled)
Devices: Restrict floppy access to locally logged-on user only	(Enabled)
Domain member: Require strong (Windows 2000 or later) session key	(Enabled)
Interactive logon: Do not require CTRL+ALT+DEL	(Disabled)
Interactive logon: Don't display last signed-in	(Enabled)
Interactive logon: Prompt user to change password before expiration	14 days
Microsoft network server: Digitally sign communications	(Enabled)
Network access: Don't allow anonymous enumeration of SAM accounts	(Enabled)
Network access: Do not allow storage of passwords and credentials for network authentication.	(Enabled)
Network access: Do not allow anonymous enumeration of SAM accounts and shares	(Enabled)

Network security: LAN Manager authentication level	Send NTLMv2 response only
Network security: Minimum session security for NTLM SSP-based (including secure RPC) clients	(Enabled)
Require NTLMv2 session security	(Enabled)
Require 128-bit encryption	(Enabled)
Network security: Minimum session security for NTLM SSP-based (including secure RPC) servers	(Enabled)
Require NTLMv2 session security	(Enabled)
Require 128-bit encryption	(Enabled)
Shutdown: Allow system to be shut down without having to log on	(Disabled)
User Account Control: Admin Approval Mode for Built-in Administrator account	(Enabled)
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent on the secure desktop
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	(Enabled)
Interactive logon: Display user information when the session is locked	User display name, domain and usernames.
Microsoft network server: Server SPN target name validation level	Accept if provided by client
Network security: Allow Local System to use computer identity for NTLM	(Enabled)
Network security: Allow LocalSystem NULL session fallback	(Disabled)
Audit Credential Validation	Success, Failure
Audit Computer Account Management	Success
Audit Other Account Management Events	Success, Failure
Audit Security Group Management	Success, Failure
Audit User Account Management	Success, Failure
Audit Process Creation	Success
Audit RPC Events	No Auditing
Audit Account Lockout	Success
Audit Logoff	Success
Audit Logon	Success, Failure
Audit Other Logon/Logoff Events	Success, Failure
Audit Special Logon	Success
Audit Application Generated	No Auditing
Audit Removable Storage	Success, Failure
Audit Policy Change	Success, Failure
Audit Authentication Policy Change	Success, Failure
Audit Filtering Platform Policy Change	Success, Failure
Audit MPSSVC Rule-Level Policy Change	Success, Failure
Audit Other Policy Change Events	Success, Failure
Audit Sensitive Privilege Use	Success, Failure
Audit Other System Events	Success, Failure
Audit Security State Change	Success, Failure
Audit Security System Extension	Success, Failure
Audit System Integrity	Success, Failure

Table 20 – CIX_Security Policy

Sub-Category	Definition	Setting
Audit account logon events	Determines whether the OS audits each time this computer validates an account's credential.	Success, failure
Audit account management	Determines whether to audit each event of account management on a computer (e.g., creation of user account, group account, etc.)	Success, Failure
Audit directory service access	Determines whether the OS audits user attempts to access Active Directory objects. Audit is only generated for objects that have system access control lists (SACL) specified and only if the type of access requested (such as write, read, and modify) and the account making the request match the settings in the SACL.	Success, Failure
Audit logon events	This security setting determines whether to audit each instance of a user logging on to or logging off from a computer.	Success, Failure
Audit object access	Determines whether the OS audits user attempts to access non-Active Directory Objects. Audit is only generated for objects that have system access control lists (SACL) specified.	Failure
Audit policy change	Determines whether to audit every incident of a change to user rights assignment policies, audit policies, or trust policies.	Success, Failure
Audit privilege use	Determines whether to audit each instance of a user exercising a user right.	Success, Failure
Audit process tracking	Determines whether the OS audits process-related events such as process creation, process termination, handle duplication and indirect object access.	Success
Audit system events	This option audits user attempts to shut down or restart the computer as well as events that affect system security or the security log	Success, Failure
Maximum application, security and system log size	Event viewers should be allocated adequate disk space to store all audit logs. The disk space needed should be based on the size of the server and review and backup intervals of the audit logs.	• Security (81,920 KB) • System (32768 KB) • Application (32768 KB)
Prevent local guest groups from accessing application, security, and system logs	Protect auditing info from guest accounts accessing application, system, and security logs.	(Enabled)

Table 21 – CC_Audit EventLog Policy

Sub-Category	Definition	Setting
Administrative Templates > Windows Components/ Windows Update	Allow Automatic Updates immediate installation	(Disabled)
	Allow non-administrators to receive update notifications	(Enabled)
	Automatic Updates detection frequency	(Enabled), Every 22 hours
	Allow signed updates from an intranet Microsoft update service location	(Disabled)
	Configure Automatic Updates	(Enabled
	Configure Automatic Updating	3 - Auto download and notify for installation
	Install during automatic maintenance	(Disabled)
	Scheduled install day:	0 - Every Sunday
	Scheduled install time:	03:00
	Every week	(Enabled)
	First week of the month	(Disabled)
	Second week of the month	(Disabled)
	Third week of the month	(Disabled)
	Fourth week of the month	(Disabled)
	Install updates for other Microsoft products	(Disabled)
	Do not display the 'Install Updates and Shut Down' option in Shut Down Windows dialog box	(Enabled)
	Do not include drivers with Windows Updates	(Disabled)
	No auto-restart with logged-on users for scheduled automatic updates installations	(Enabled)
	Specify intranet Microsoft update service location	(Enabled)
	Set the intranet update service for detecting updates	http://10.230.162.50:8530
	Set the intranet statistics server:	http://10.230.162.50:8530
	Set the alternate download server: (example: http://IntranetUpd01)	
	Download files with no URL in the metadata if an alternate download server is set.	(Disabled)
	Do not enforce TLS certificate pinning for windows update client for detecting updates	(Disabled)
	Select the proxy behaviour for windows update client for detecting updates	Only use system proxy for detecting updates (default)
	Turn off auto-restart for updates during active hours	(Enabled)
	Active Hours (Start):	5:00 AM
	Active Hours (End):	11:00 PM
	Turn on recommended updates via Automatic Updates	(Disabled)

Table 22 – CC_OS Patch Policy

Sub-category	Definition	Setting
Control Panel> Personalization	Prevent enabling lock screen camera	(Enabled)
Control Panel> Personalization	Prevent enabling lock slide show	(Enabled)
System/Audit Process Creation	Include command line in process creation events	(Disabled)
System/Group Policy	Configure registry policy processing	(Disabled)
System/Internet Communication Management	Turn off access to the Store	(Enabled)
	Turn off downloading of print drivers over HTTP	(Enabled)
	Turn off Event Viewer "Events.asp" links	(Enabled)
	Turn off internet download for web publishing and online ordering wizards	(Enabled)
	Turn off printing over HTTP	(Enabled)
	Turn off Search Companion content file updates	(Enabled)
	Turn off the "Publish to web" task for files and folders	(Enabled)
	Turn off Windows Messenger Customer Experience Improvement Program	(Enabled)
	Turn off Windows Customer Experience Improvement Program	(Enabled)
	Turn off windows update device driver searching	(Enabled)
System/Mitigation Options	Untrusted Font blocking	(Enabled)
	Mitigation Options	Block untrusted fonts and log events
System/Logon	Do not display network selection UI	(Enabled)
	Do not enumerate connected users on domain-joined computers	(Enabled)
	Do not Process the legacy run list	(Enabled)
	Do not Process the run once list	(Enabled)
	Turn off app notifications on the lock screen	(Enabled)
System/Power Management	Turn of the display (on battery)	(Enabled)
	Turn Off the Display (seconds):	0
	Turn off the display (plugged in)	(Enabled)
	Turn Off the Display (seconds):	0
System/Remote Procedure Call	Enable RPC Endpoint Mapper Client Authentication	(Enabled)
System/User Profiles	Turn off the advertising ID	(Enabled)
Windows Components/App Privacy	Let windows apps access account information	(Enabled), Force Deny
	Let windows apps access call history	(Enabled), Force Deny
	Let windows apps access contacts	(Enabled), Force Deny
	Let windows apps access email	(Enabled), Force Deny
	Let windows apps access location	(Enabled), Force Deny
	Let windows apps access messaging	(Enabled), Force Deny

	Let windows apps access motion	(Enabled), Force Deny
	Let windows apps access calendar	(Enabled), Force Deny
	Let windows apps access the camera	(Enabled), Force Deny
	Let windows apps access the microphone	(Enabled), Force Deny
	Let windows apps access trusted devices	(Enabled), Force Deny
	Let windows apps control radios	(Enabled), Force Deny
Windows Components/App Runtime	Block launching Universal Windows apps with Windows Runtimes API Access from hosted content	(Enabled)
Windows Components/Camera	Allow use of camera	(Disabled)
Windows Components/Autoplay Policies	Disallow Autoplay for non-volume devices	(Enabled)
	Turn off Autoplay	(Enabled)
	Turn off Autoplay on:	CD-ROM and removable media drives
Windows Components/Cloud Content	Do not show Windows Tips	(Enabled)
	Turn off Microsoft consumer experiences	(Enabled)
Windows Components/Data Collection and Preview Builds	Do not show feedback notifications	(Enabled)
	Toggle user control over Insider builds	(Enabled)
Windows Components/Event Log Service/Application	Specify the maximum log file size (KB)	(Enabled)
	Maximum Log Size (KB)	32768
Windows Components/Event Log Service/Security	Specify the maximum log file size (KB)	(Enabled)
	Maximum Log Size (KB)	32768
Windows Components/Event Log Service/Setup	Specify the maximum log file size (KB)	(Enabled)
	Maximum Log Size (KB)	32768
Windows Components/Event Log Service/System	Specify the maximum log file size (KB)	(Enabled)
	Maximum Log Size (KB)	32768
Windows Components/File Explorer	Turn-off heap termination on corruption	(Disabled)
Windows Components/MDM	Disable MDM Enrollment	(Enabled)
Windows Components/Search	Allow Cortana	(Disabled)
	Don't Search the web or display web results in Search	(Enabled)
	Don't Search the web or display web results in Search over metered connections	(Enabled)
Windows Components/Software Protection Platform	Turn off KMS Client Online AVS Validation	(Enabled)
Windows Components/Store	Turn off Automatic Download and Install of updates	(Enabled)
	Disable all apps from Microsoft store	(Enabled)
	Turn off the Store application	(Enabled)
	Do not sync Apps	(Enabled)

Windows Components/Sync your settings	Allow users to turn "AppSync" syncing on.	(Disabled)
	Do not sync start settings	(Enabled)
	Allow users to turn "start layout" syncing on.	(Disabled)
Windows Components/Windows Defender Antivirus	Turn off Windows Defender Antivirus	(Enabled)
Windows Components/Windows Error Reporting	Automatically send memory dumps for OS-generated error reports	(Disabled)
Windows Components/Windows Logon Options	Sign in and lock the last interactive user automatically after a restart	(Disabled)

Table 23 – CC_Administrative Templates

Sub-category	Definition	Setting
Enable Windows NTP Client	Policy definitions (AMDX files) retrieved from the central files - Computer Configuration > Administrative Templates > System	(Enabled)
Enable Windows NTP Server		(Enabled)
NTPServer		192.168.123.254,0x8
Type		NTP
CrossSiteSyncFlags		2
ResolvePeerBackOffMaxTime		7
ResolvePeerBackOffMinutes		15
SpecialPollingInterval		1024
EventLogFlags		0
MaxAllowedPhaseOffset		300
MaxPosPhaseCorrection		172800
MaxNegPhaseCorrection		172800
AnnounceFlags		10

Table 24 – CC_AD Time Sync Policy

Sub-category	Definition	Setting
Domain controller	LDAP server signing requirements	None
Domain member	Digitally encrypt or sign secure channel data (always)	(Enabled)
Microsoft network server	Digitally sign communications (always)	(Enabled)
	Digitally sign communications (if the client agrees)	(Enabled)

Table 25 – CC_Domain Controller Policy

Services	Setting
Specify Communities	(Enabled), Communities – 2K25CWyok@!23
Specify Permitted Managers	(Enabled), Permitted Managers: 10.230.162.42
Specify Traps for Public Community	(Enabled), Trap Configuration: 10.230.162.42
ECC Curve Order	(Enabled), ECC Curve Order- curve25519, NistP256, NistP384
SSL Cipher Suite Order	Enabled

Table 26 – CC_SNMP and SSL Policy

Sub-category	Definition	Setting
Windows Settings > Security Settings > Windows Firewall with Advanced Security	Global Settings > Policy > Policy Version	2.31
	Domain Profile Settings > Firewall State	On
	Private Profile Settings > Firewall State	On
	Public Profile Settings > Firewall State	On
Administrative Templates	Network/Network Connections > Windows Defender Firewall: Protect all network connections	(Enabled)

Table 27 – CC_Windows Firewall Policy

Sub-category	Definition	Setting
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections	Allow users to connect remotely by using Remote Desktop Services	(Enabled)
	Automatic reconnection	(Enabled)
	Limit the number of connections	(Enabled)
	RD Maximum Connections allowed	4
	Select RDP transport protocols	(Enabled)
	Select Transport Type	Use both UDP and TCP
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Device and Resource Redirection	Do not allow Clipboard redirection	(Enabled)
	Do not allow drive redirection	(Enabled)
	Do not allow smart card device redirection	(Enabled)
	Do not allow supported Plug and Play device redirection	(Enabled)
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Remote Session Environment	Enable RemoteFX encoding for Remote FXclients designed for Windows Server 2008 R2 SP1	(Disabled)
	Enforce Removal of Remote Desktop Wallpaper	(Enabled)
	Remove the "Disconnect" option from the Shut Down dialog	(Enabled)
	Remove the Windows Security item from the Start Menu	(Enabled)
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Host Security	Require secure RPC communication	(Enabled)
	Require user authentication for remote connections by using Network level authentication	(Enabled)
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Session Time Limits	End session when time limits are reached	(Enabled)
	Set a time limit for active but idle RemoteDesktop Services sessions	(Enabled)
	Idle session limit:	1 hour
	Set a time limit for disconnected sessions	(Enabled)
	End a disconnected session	30 minutes

Table 28 – CC_Remote Desktop Common Policy

Sub-category	Definition	Setting
User Configuration> Policies> Administrative Templates	Control Panel/Display>Disable the display control panel	(Enabled)
	Control Panel/ Display>Hide Settings tab	(Enabled)
	Control Panel/Personalization>Enable Screen saver	(Disabled)
	Control Panel/Personalization>Prevent changing desktop background	(Enabled)
	Control Panel/Personalization>Prevent changing desktop icons	(Enabled)
	Control Panel/Programs>Hide"Get Programs" page	(Enabled)
	Control Panel/Programs>Hide"Installed Updates" page	(Enabled)
	Control Panel/Programs>Hide"Programs and features" page	(Enabled)
	Control Panel/Programs>Hide"Set Programs access and computer deafults" page	(Enabled)
	Control Panel/Programs>Hide"Windows features" page	(Enabled)
	Control Panel/Programs>Hide"Windows marketplace" page	(Enabled)
	Control Panel/Programs>Hide the programs control panel	(Enabled)
	Desktop>Hide internet explorer icon on desktop	(Enabled)
	Start Menu and Taskbar>Remove games link from start menu	(Enabled)
	Start Menu and Taskbar>Remove help menu from start menu	(Enabled)
	Start Menu and Taskbar/Notifications>Turn off toast notifications	(Enabled)

Table 29 – UC_Hardening

4.7.1 Group Policy Assignment

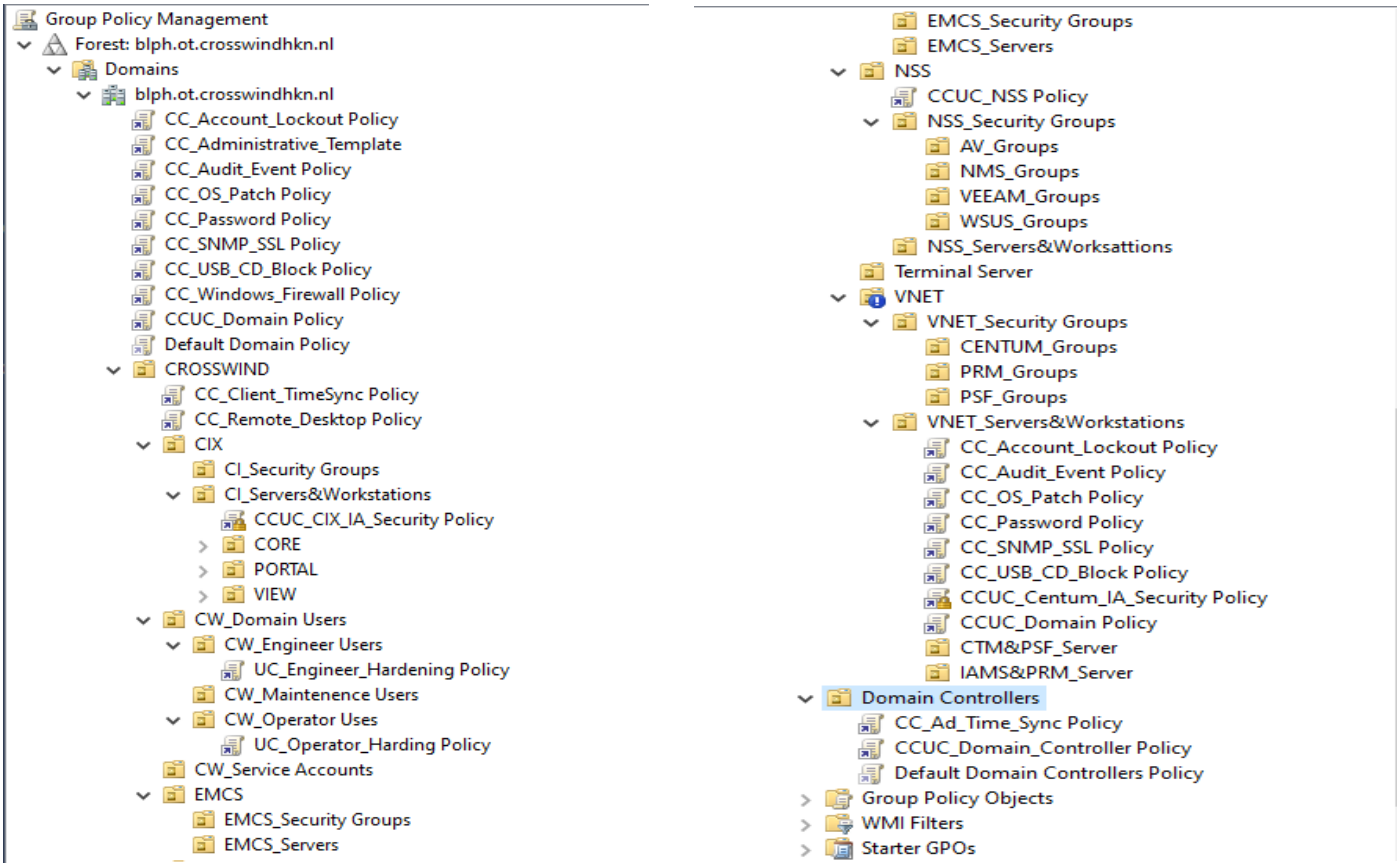


Figure 9 – Group Policy Assignment

5 YOKOGAWA ENDPOINT SECURITY SOLUTION

Significant risks of malware intrusion and infection are increasing every day, to reduce this risk, Yokogawa in collaboration with Trellix provides a Standard Antivirus software for the Yokogawa IA control system. Based on Trellix's antivirus technology, the antivirus software (Trellix Endpoint Security (ENS)) shall use the centralized management concept using the Trellix ePolicy Orchestrator and its features. The ePO is an integrated endpoint security platform that fully supports the Yokogawa IACS products.

5.1 Design Architecture: Overview

In the CROSSWIND-BLPH Project, Yokogawa Standard Antivirus shall be used for Yokogawa systems which shall be integrated with ePolicy Orchestrator. The ePolicy Orchestrator (ePO) provides the system security management console to centrally manage client systems, networks, data, and compliance solutions.

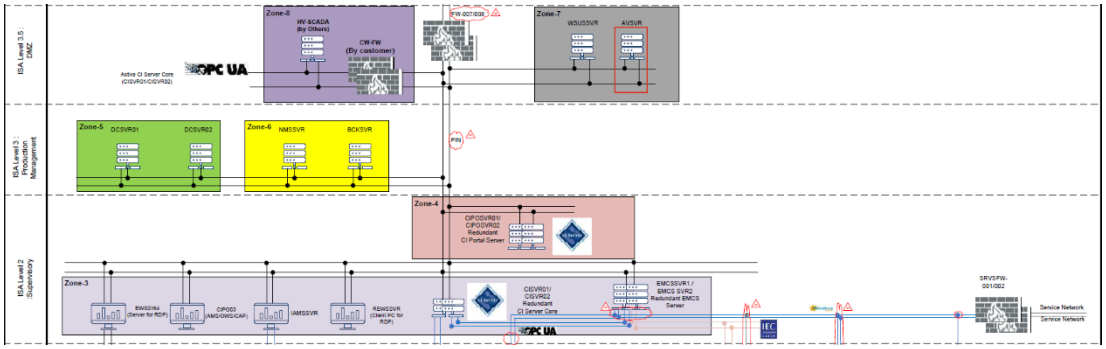


Figure 10 – Antivirus Design

- All Yokogawa-supplied computers in Level 2,3 are installed with an Antivirus agent to deliver services such as updating, logging, reporting events and properties, task scheduling, communication, and policy storage to/from the Antivirus Management server.
- An Anti-Virus Management server shall be deployed at the DMZ level and will be used to download updates from an upstream server located in the office domain on a scheduled basis. AVSVR(Downstream) manages all the clients in Level 2,3.
- The Antivirus Management server (DMZ) stores all the repositories needed for the implementation requirements including the extensions, product, and definition updates.

Note: In the Crosswind-BLPH project, the AV downstream Server is present at Level 3.5(DMZ).

5.2 Anti-Virus Components

5.2.1 Trellix ePolicy Orchestrator Server

The Trellix ePolicy Orchestrator (ePO) server provides a security management console to centrally manage and enforce a policy on the endpoint client. Trellix ePO monitors and manages all clients, detects threats, and protects against them. Easily accessible from any web browser, the Trellix ePO web console provides detailed information and reports through a customizable dashboard. Trellix ePO Server features:

- A robust database that collects information about the operations of the agent software on the client systems in the network.
- A querying system that lets the user monitor the security status and quickly act on the gathered data.
- A software repository that stores the Trellix products and their updates that are deployed through the network.
- A scheduling capability to distribute updated Yokogawa Standard Antivirus Software (ENS) security policies.

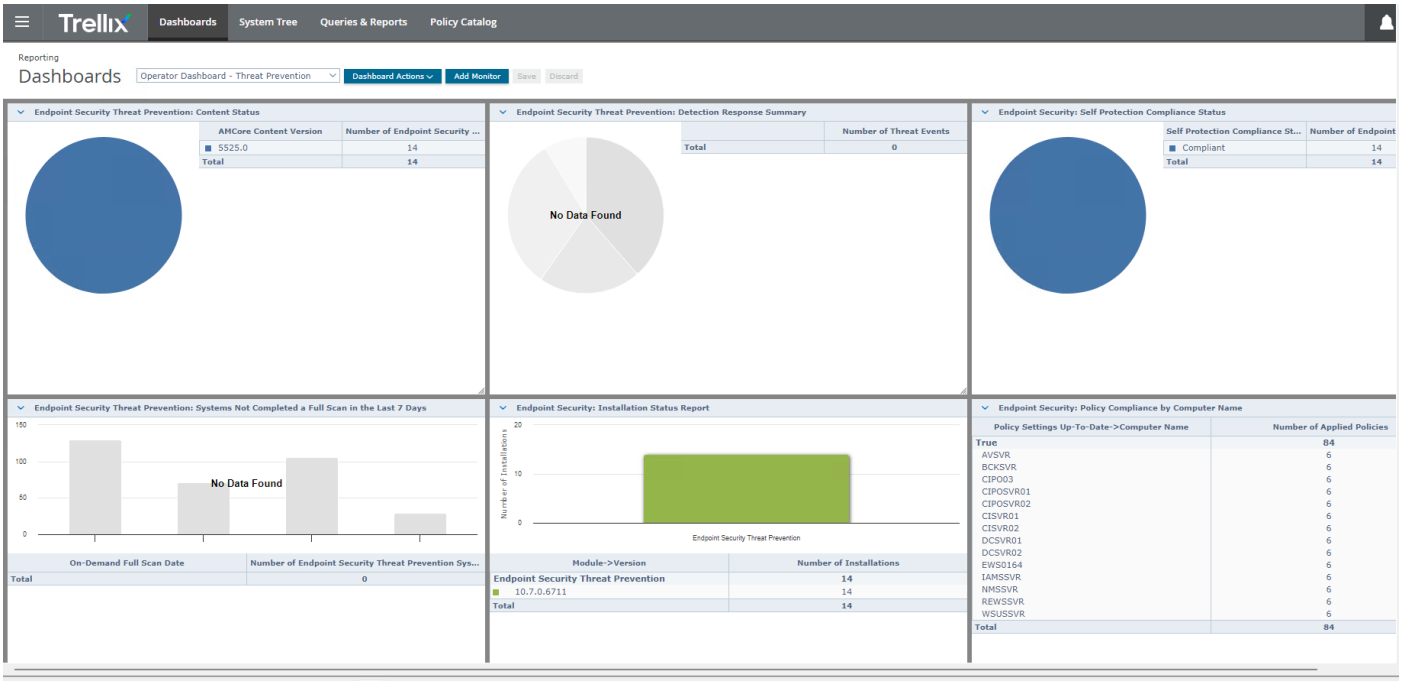


Figure 11 – ePolicy Console

5.2.2 Trellix Agent

The agent provides a communication channel from the managed client to the Trellix ePolicy Orchestrator server. It downloads and enforces policies and executes client-side tasks such as deployment and updating. The Trellix Agent is also responsible for uploading events and provides the system status to the Trellix ePO server. Client systems cannot be managed by the Trellix ePO server unless a Trellix Agent is installed.

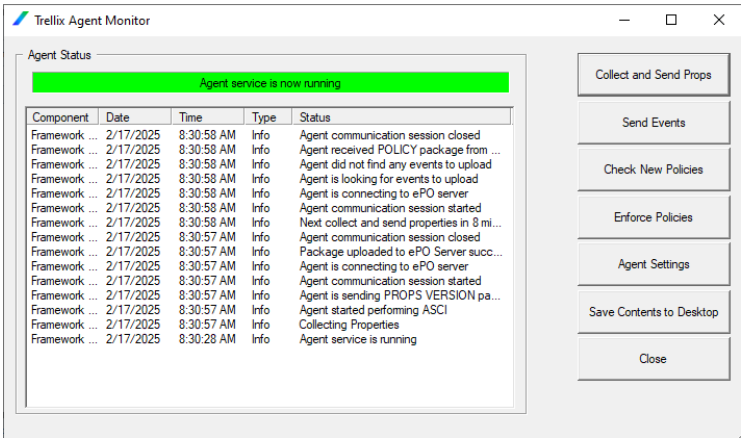


Figure 12 – Trellix Agent Interface

5.2.3 Yokogawa Standard Antivirus Software (ENS) Software

The Yokogawa Standard Antivirus Software (ENS) simplifies the antivirus environment by providing a single type of agent to deploy and manage the environment. This software ensures that the endpoint is protected by providing malware prevention, detection, and removal. The Yokogawa Standard Antivirus Software (ENS) console offers quick access to multiple functions like the System Scan, Definition file update and access to multiple event log information.

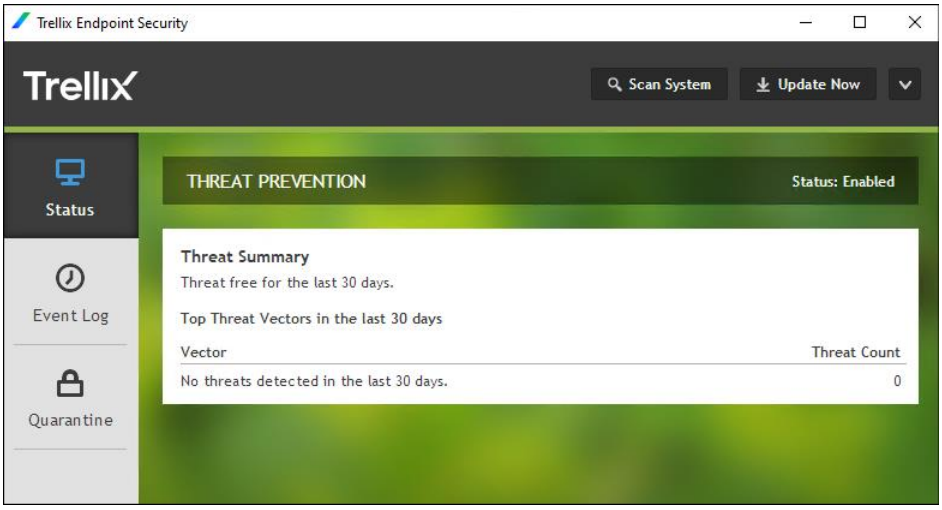


Figure 13 – Yokogawa Standard Antivirus Software (ENS) Console

5.3 Repository

The repository refers to the location where all the Trellix security software products and updates files are stored. The Trellix ePO repository architecture offers flexibility to ensure that deploying and updating software is as easy and automated as your environment allows.

The Repository content can include the following:

- Managed Software to Deploy to your clients
- Security Contents such as DATs and Signature
- Patches and other software needed for client tasks

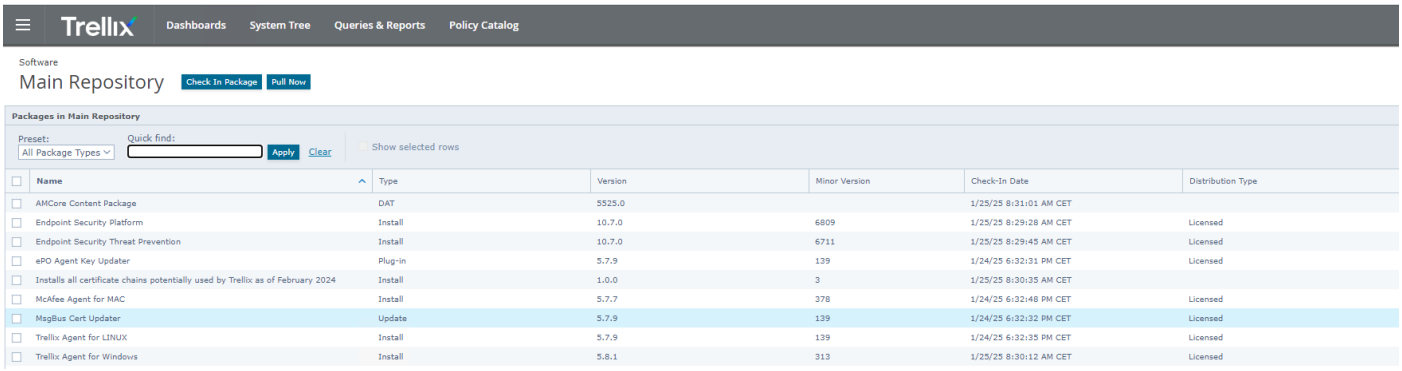


Figure 14 – Yokogawa Standard Antivirus Software (ENS) Master Repository

5.3.1 Updates

Updates are downloaded to ensure most up-to-date security solution in the anti-virus system.

For updating the definition files and product updates, customer can avail the Endpoint Security Service / Security Information Service that is catered by Yokogawa for continuous updating of this solution.

A monthly release of the latest and validated definition and products updates are provided by this service to the customers. Customers can either obtain the complete list of the validated definition and product updates for their implementation or have a Yokogawa Engineer to carry out the updates On- site on their behalf.

5.3.2 System Tree Groups

The System Tree groups refer to the location where all the managed systems are present. The managed system can be organized into logical subgroups based on their machine type, topological/ geographical locations or their functionality boundaries. Creating subgroups for systems with similar properties or requirements allows the administrator to manage policies and tasks for the system in one location.

The default System Trees structure contains My Organization and the Lost and Found Group.

- My organization – The root of the System Tree
- Lost and Found Group – The catch-all subgroup for any system that could not be added to any group

Note: System Tree Group Structure is in sync with the Active Directory OU Structure.

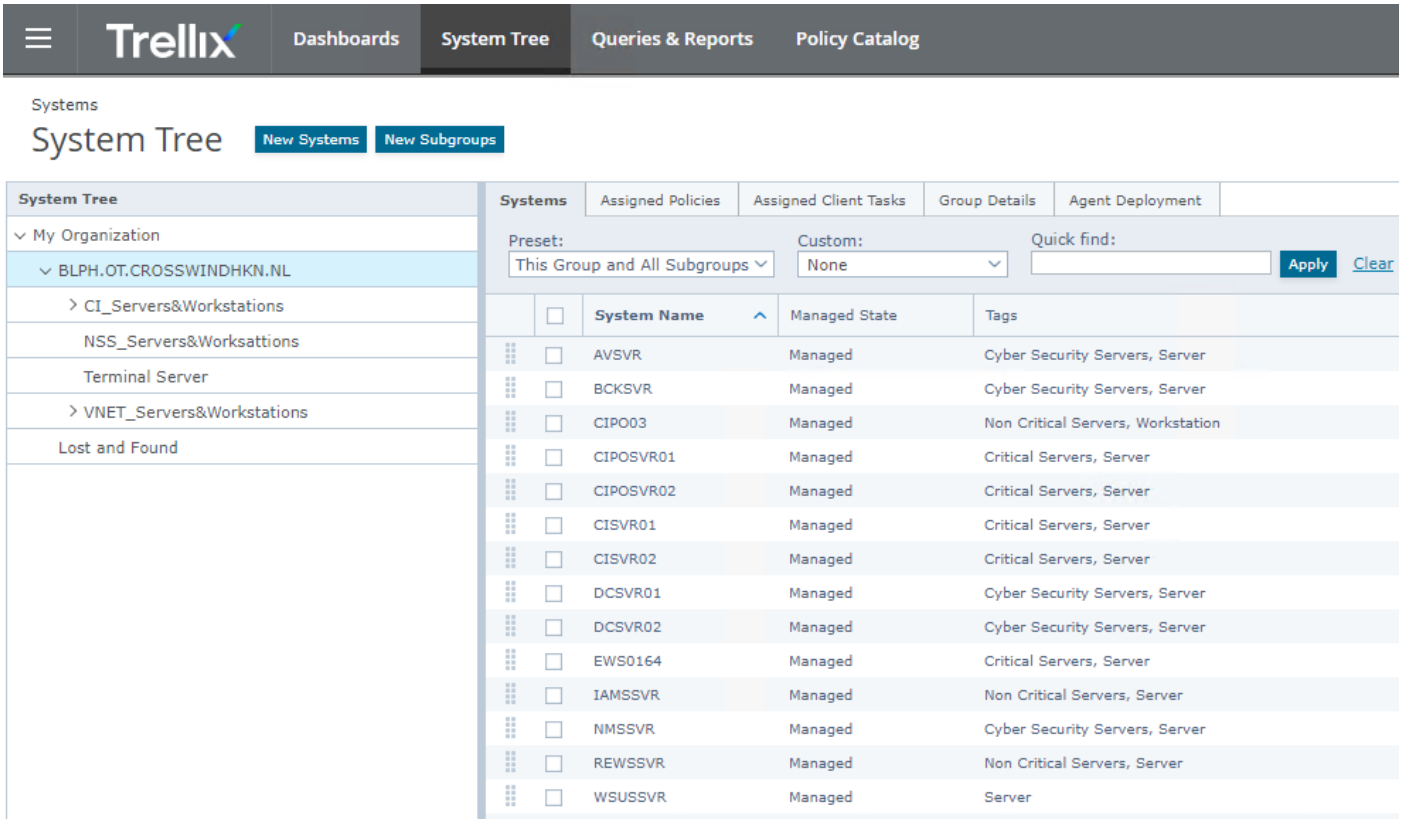


Figure 15 –Group Structure

5.3.3 Antivirus Policies

The policies are a collection of settings that are created in the Trellix ePO Server and then enforced on all the managed clients. Policies are organized by product and then subdivided into different categories. The Antivirus platform shall be implemented using the Yokogawa Standard Antivirus (ENS) Policy.

Product	Categories
Endpoint Security	Common-In Trellix Endpoint Security we have some common categories where you can configure the endpoint security settings.
Endpoint Security Threat Prevention	Option- The Options page is where you configure Common settings, including passwords, exclusions, and activity and debug logging. • Access Protection- It control and restrict access to sensitive data, applications, and systems by User Authentication, Role-Based Access Control, Application Control etc. • Exploit Prevention- It detects and block attempts to exploit vulnerabilities in software applications and operating systems by Monitoring application for suspicious behaviour. • On-Access Scan- A real-time scanning feature that actively monitors files and processes as they are accessed, created, or modified on endpoints. It detects and block malware and other threats before they can execute or spread by scanning files immediately when they are accessed, checking files, providing insights into potential threats and system health. • On-Demand Scan- It allows administrators to manually initiate scans on endpoints at any time. This can be useful for performing targeted security checks or ensuring that systems are free of malware after a suspected infection.
Trellix Agent	• Custom-These are the customizable settings or configurations that allow organizations to tailor the agent's behaviour and policies to meet specific security needs by Policy Customization, User permission • General- The default configurations and basic options that govern the overall behaviour and operation of the agent. Ex. Agent status, Version Information, Logging activities. • Product Improvement- It refers to enhancements and updates made to the agent software to enhance its functionality, security, and overall user experience. • Repository- It refers to a centralized storage location where security updates, threat definitions, and other data are kept for the agent to access. • Troubleshooting- It identifies and resolves issues that may arise during the agent's operation. This process ensures that the agent functions effectively and maintains endpoint security.

Table 30 – Policy Product and Categories

5.3.3.1 Yokogawa Standard Antivirus Software (ENS) Policy

Part of the Yokogawa Standard Antivirus Software (ENS) feature is an optimized policy configuration. This policy is tested to ensure the stable operation of the Yokogawa ICSS (Industrial Control &Safety System) products. Using the policy import method, the administrator can ensure that only tested policies are used and minimize human error in configuring the Trellix ePO Policy.

After the policy import, the policy will automatically be assigned to the Yokogawa Group. All the managed clients of the Yokogawa Group will then be able to download all the preconfigured policies.

Product	Category	Policy Name
Endpoint Security	• Common	• Yokogawa Advanced
Endpoint Security Threat Prevention	• On-Access Scan • On-Demand Scan • Option • Access Protection • Exploit Protection	• Yokogawa Advanced
Trellix Agent	• General • Repository • Troubleshooting • Custom Properties • Product Improvement	• Yokogawa Advanced

Table 31 – Yokogawa Standard Antivirus Software (ENS) Policy

5.3.3.2 Yokogawa Standard Antivirus Software (ENS) Task

Part of the Yokogawa Standard Antivirus Software (ENS) feature is an optimized task configuration. Create a scheduled task to automate multiple action items in the Trellix ePO environment.

After the task import, create a scheduled task and assign the task to the Yokogawa Group. All the managed clients of the Yokogawa Group will then be able to download and schedule the preconfigured task.

Product	Task Type	Task Name
Trellix Agent	Product Update	AMCore Update
Trellix Agent	Product Deployment	ENS_Yokogawa_Advanced
Trellix Agent	Product Deployment	MfeSysprep

Table 32 – Yokogawa Standard Antivirus Software (ENS) Task

5.3.4 Yokogawa Standard Antivirus Software (ENS) Scan Types

Scanning is the process of inspecting a file for threats. It is recommended to scan files for threats while the user accesses them as this provides intrusion when they occur. In addition to this, the periodical scanning area of your system most susceptible to infection ensures complete protection.

The Yokogawa Standard Antivirus Software (ENS) has two types of scans, **On-Demand Scan,** and **On-Access Scan**.

5.3.5 On-Demand Scan

The On-Demand Scan inspects all parts of the managed client for any potential threats. The On-Demand Scan complements the continuous protection of the On-Access Scan. This type of scan can be triggered manually or based on a predefined schedule.

Category	Description
Manual Scan	Run a predefined on-demand scan at any time from the **Endpoint Security Client** by clicking the Scan System button. On-Demand Scan Type: • **Quick Scan** runs a quick check of the areas of the system most susceptible to infection.

	• **Full Scan** performs a thorough check of all areas of the system.
Scheduled Scan	The administrator (or user, for self-managed systems) configures and schedules on-demand scans to run on computers. To configure and schedule on-demand scans, use these client task settings: • **Custom On-Demand Scan** – Configures and schedules custom on-demand scans, such as daily memory scans. • **Policy-Based On-Demand Scan** – Schedules the predefined **Quick Scan** and **Full Scan** on-demand scans.

Table 33 – On-Demand Scan

Note: In general, running a full system scan puts an additional load on the client and affects the machine's performance. To avoid this scenario, the full system scan shall be scheduled according to plant operation.

Scan Type	Frequency	Scheduled Time
On-demand Full scan	Once in a Week	As per Site requirements

Table 34 – Scanning Schedule

5.3.5.1 On-Access Scan

The On-Access Scanner examines files on the managed client as they are accessed to provide continuous, real-time detection of threats. Whenever files, folders, and programs are accessed by automated process (for databases) or by manually triggered processes like copying/accessing over the network or adding removable data volume, the on-access scanner intercepts the operation and scans the item, based on criteria defined in the settings for Yokogawa Automation products.

5.3.6 Yokogawa Standard Antivirus Software (ENS) File Exclusions

Trellix ePO allows an exception to its scheduled scan by applying folder or file exclusions. Applying an exclusion to a file means that it won't be monitored for malicious activity. The exclusion configuration for the Yokogawa products is already part of the provided pre-configured policies. There is no need to further exclude manually the Yokogawa products folder and files.

5.3.7 Yokogawa Standard Antivirus Software (ENS) Definition and Product Updates

To update the definition files and product updates, the end-user should be part of the Basic Endpoint Security Solution. As part of this service, a monthly release of the latest and validated virus definition files and product updates shall be provided to the end-user. Yokogawa releases the verified update files every second Tuesday of each month.

5.3.8 Host Name Resolution

In a Windows Domain environment, a Domain Name System (DNS) service will be available as part of the Active Directory Domain Services requirements. The DNS service will be responsible for translating the domain hostnames into their corresponding IP Addresses. The Trellix ePO can create its queries and reports. Part of the application is a Query Builder and a Report Builder, which creates and runs user-configured data queries and reports into user-configured charts and tables. In addition to the query and report features, logs can be used to gather information about activities that occur on the Trellix ePO server.

5.3.8.1 Queries

Queries are configurable objects that retrieve and display data from the database. The results of queries are displayed in charts and tables. Any query result can be exported to a variety of formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can be used as dashboard monitors.

Queries can be personal (private) or public. Private queries exist in the user's My Groups list and are available only to their creator. Public queries exist in the Shared Groups list and are available to everyone who has permission to use public queries. By default, all Trellix ePolicy Orchestrator default queries are public.

5.3.8.2 Reports

Reports display the query results in a PDF document, enabling offline analysis. It is a collection of information such as threat events and detected malware activity. The most recently run result is stored in the system and is readily available for viewing. You can restrict access to reports by using groups and permission sets in the same way you restrict access to queries. Reports and queries can use the same groups, and because reports primarily consist of queries, this configuration allows for consistent access control.

5.3.8.3 Logs

Logs are used to gather information about activities that occur on the Trellix ePO server. These Logs are available inside the Trellix ePO Server console.

Category	Details
Audit Log	The Audit Log records all Trellix ePO user actions.
Server Task Log	The Server Task Log provides the status of your server tasks and displays an error that might have occurred.
Threat Event Log	The Threat Event Log provides the threat status and information such as source, threat name, Threat Severity, etc.

Table 35 – Trellix ePO Log Category

5.3.8.4 Log Files for Troubleshooting

The Trellix ePO provides log files that can be used for maintenance and troubleshooting. These log files contain important information such as event history, policy enforcement, and others.

Category	Details
Installer Logs	Include details about the installation path, user credentials, the database used, and communication ports configured.
Server Logs	Include details about server functionality, client event history, and administrator services.
Agent Logs	Include details about agent installation, wake-up calls, updating, and policy enforcement.

Table 36 – Troubleshooting Log File Category

6 OS PATCH MANAGEMENT

The Windows Server Update Services (WSUS) is a Microsoft solution that provides a platform for managing and distributing the latest Microsoft product updates to computers on the network. Implementing this solution and following the recommended configuration gives the plant asset administrator the capability to control the patches that would be installed on the plant asset.

Patch management is the process of using a strategy and plan of what patches shall be applied to which systems at a specified time. In ICS, many considerations and careful planning is required for patch management to fulfil its intended function.

Applying updates for the OS is a critical task for the ICS environment. The considerations between system security and application stability must be properly met for a patch to be approved. The WSUS server provides a management console to centrally manage and enforce updates to the client. The WSUS stores all the applicable updates and ensures availability to the clients upon patch approval. The WSUS console provides detailed client update information and reports through the dashboard. In the Yokogawa OS Patch implementation, the WSUS server must be able to connect to the Microsoft Update to get the latest available update information. This server shall have a secure connection to the Microsoft website.

If an organization cannot determine and maintain a known level of trust within its operating systems and application software, it might have several security vulnerabilities, which if exploited could lead to a loss of revenue and intellectual property. The Downstream WSUS server (WSUSSVR) shall be in DMZ zone L3.5.

6.1 Design Architecture Overview

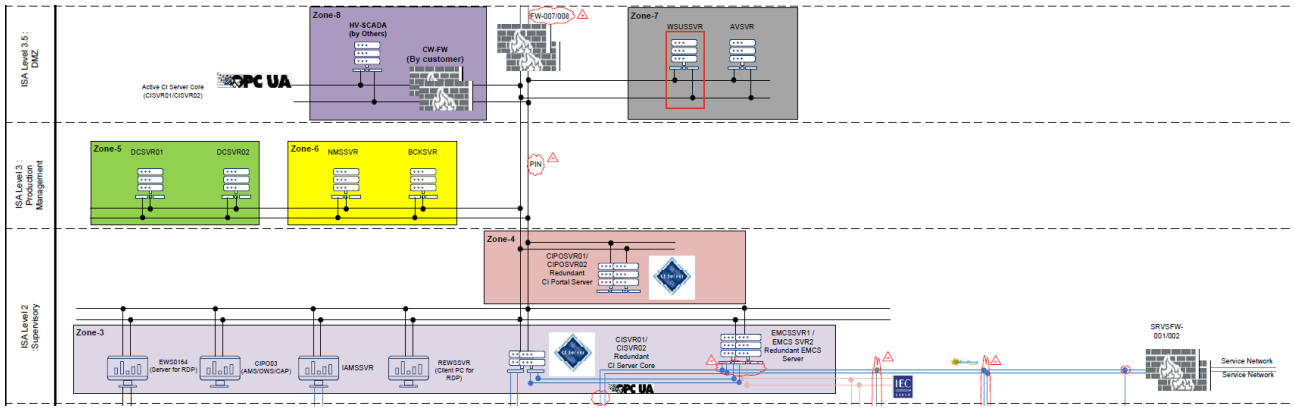


Figure 16 – OS Patch Management System Logical Architecture Overview

In CROSSWIND-BLPH project, WSUS Server is present at OER region. A Downstream WSUSSVR is present at L3.5(DMZ) and it will get the updates from the Crosswind OT WSUS Server.

6.2 WSUS Components

WSUS provides a management infrastructure consisting of the following:

1) WSUS Server (Administration Console)
2) WSUS Client Computers

6.2.1 WSUS Server

Server component of the WSUS server (v10.0.20348.1) is installed on a computer running a Windows server 2022 operating system. The WSUS server provides the features that administrators need to manage and distribute updates through the WSUS Administration Console.

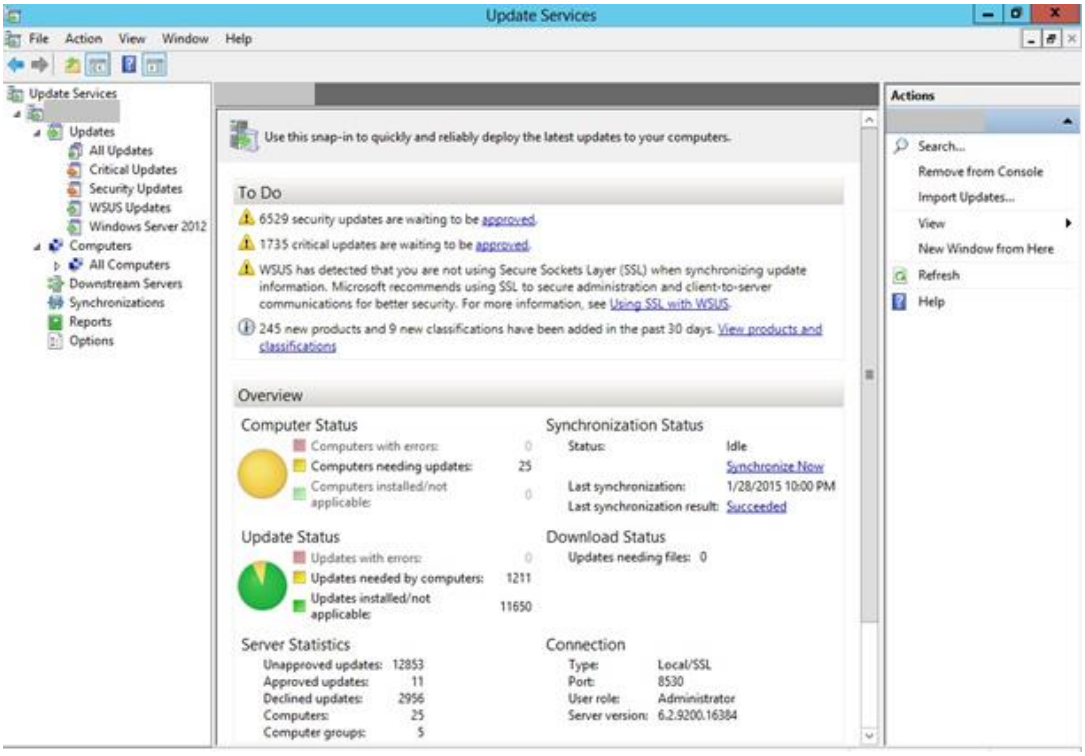


Figure 17 – WSUS Administrative Console

6.2.2 WSUS Client Computers and their Automatic Updates

Computers that are installed with Microsoft's OS are the main purpose of the implementation of the WSUS. OS running Server – (Windows server 2022), platforms are the components required for this implementation.

Each installation of Microsoft Windows OS is preconfigured with Windows Update, a built-in service provided by Microsoft for a routine check and installation of updates for the OS. By default, Windows Update is configured to connect to the Microsoft Update site via the Internet. However, this configuration can be changed to connect to WSUS server whenever WSUS is available. Administrators can configure the behaviour of Windows Update by using local group policy in a Workgroup environment or by Group Policy in an Active Directory environment. Windows Updates service works in the background so that it doesn't majorly impact the plant operation and network's functionality.

All Yokogawa-supplied computers will have their Windows Update service configured for the following:

1) Check for updates with the WSUS management server on a scheduled basis.
2) Approved updates will be downloaded and notified for installation.
3) Manual restart after updating only to avoid disruption to plant operations.

6.3 WSUS Firewall Port Requirement

The ports described in this section are used as a reference when configuring a firewall to allow the communication traffic that is needed by the WSUS environment.

6.3.1 Firewall Port Requirement of the WSUS Server

The ports described in this section are used as a reference when configuring a firewall to allow traffic to and from the WSUS server.

	Port	Protocol	Traffic Direction
Server-Client communication port	8531/8530	TCP	Outbound connection to the WSUS client

Table 38 – WSUS Server Firewall Ports

6.3.2 Firewall Port Requirement of the WSUS Client

The ports described in this section are used as a reference when configuring a firewall to allow traffic to and from the WSUS Client.

	Port	Protocol	Traffic Direction
Server-Client communication port	8531/8530	TCP	Outbound connection to the WSUS Server

Table 39 – WSUS Client Firewall Ports

6.4 WSUS Clients Policy

The Group Policy Object (GPO) settings for the WSUS client updates control how WSUS clients can interact with Windows Update to obtain updates. Installation of updates to a WSUS client may require the operating system to restart which can affect the plant operation. In the Yokogawa implementation, the WSUS clients are configured not to automatically download updates from the WSUS server.

Downloading of updates will only happen once an administrator manually triggers a Windows update during the target machine maintenance schedule. This configuration ensures that the WSUS server implementation does not create any adverse effect on the plant operation.

6.5 WSUS Clients Policy

The Group Policy Object (GPO) settings for the WSUS client updates control how WSUS clients can interact with Windows Update to obtain updates. Installation of updates to a WSUS client may require the operating system to restart which can affect the plant operation. In the Yokogawa implementation, the WSUS clients are configured not to automatically download updates from the WSUS server. Downloading of updates will only happen once an administrator manually triggers a Windows update during the target machine maintenance schedule. This configuration ensures that the WSUS server implementation does not create any adverse effect on the plant operation.

Group Policy	Settings
Configure Automatic Updates	Disabled
Automatic Update Detection Frequency	Disabled

Table 40 – WSUS Client Policy

6.6 Groups

The purpose of grouping is to segregate computers that require different approved updates. For example, if a critical update is incompatible with one application but compatible with another, the administrator can ensure that the patch is distributed to only computers with compatible applications.

Each WSUS client is assigned to a group inside the WSUS server. Groups in the WSUS server are arranged hierarchically. At the root of the hierarchical tree is a group called All Computers. This group is created by default upon the installation of the WSUS server and cannot be removed. All other child groups will be created under this group.

When the Automatic Update Services of the WSUS clients are configured to check for updates from the WSUS server, these clients are assigned automatically to the Unassigned Computers group. They are then manually housed into different child groups based on the categories of applications running on them.

Updates are approved based on the group segregation in the WSUS console, & group naming is based on the product group for the systems. E.g., CENTUM VP R6, Prosafe RS, PRM, etc. The table below lists the child groups that are created based on the categories of application. These child groups are created based on the application categories.

Child Groups	Description
YOK-CENTUM/Prosafe-RS	EWS/SENG
YOK-PRM	IAMS
YOK-CI Server	CI Server
GENERAL	Active Directory Server, Backup Server, AVOS Server, NMS server.
Unassigned Computers	Newly added systems.

Table 41 – Child Groups Created on the WSUS Management Server

6.7 Scheduling

The following table lists a schedule of the various automated tasks that will take place during daily operation.

Types	Automated Tasks	Frequency	Scheduled Time
WSUS upstream server	Synchronization schedule	Monthly	1:00 AM
WSUS clients	Automatic Updates detection frequency	22 hours (Default)	NA
	Auto download and notify for install	Daily	3:00 AM

Table 42 – Schedule of WSUS Automated Tasks

6.8 WSUS Reporting

The WSUS Server collects information about updated events in the network and presents them in various report formats as and when required. When a report is created, the report is displayed in a separate window. A copy of the report can be saved in web archive format or can be printed out.

There are no configurations required on the WSUS management server to generate a report. These reports are in the report section of the WSUS management server. They are generated manually from that section as and when the administrator needs to know about the status of a certain update event.

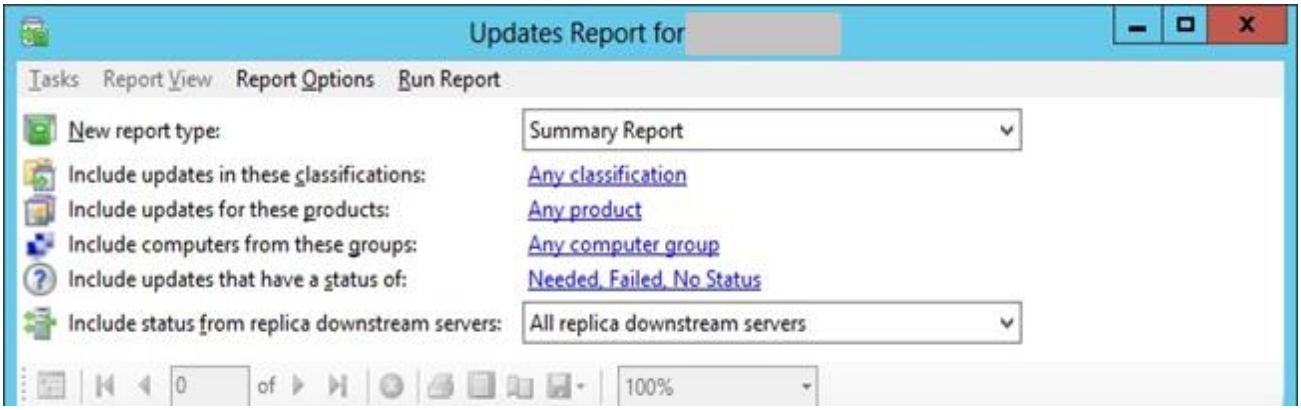


Figure 18 – WSUS update Report

The table below lists all the types of reports that can be generated by the administrator.

Report Category	Report	Description
Update Reports	Update Status Summary	Shows a summary of the update status, with one page per update.
	Update Detailed Status	Shows a summary of the update status, with the update status of all computers for each update. One update is shown per page.
	Update Tabular status	Shows a summary of the update status in a tabular view, suitable for exporting to a spreadsheet.
Computers Reports	Computer Status Summary	Shows a summary of the Computer status, with one page per computer.
	Computer Detailed Status	Shows details of each computer's status, with the update status for each update. One computer is shown per page.
	Computer Tabular Status	Shows a summary of computer status in a tabular view suitable for exporting to a spreadsheet.
Synchronization Reports	Synchronization Results	Shows the report of the last synchronization.

Table 43 – Schedule of WSUS automated tasks.

6.9 OS Patch Updates Services

Technologies for computing continuously evolve and innovate, yet information security threats and attacks are also increasing and evolving each day whenever a new technology emerges. Successful implementation of a secure network does not stop, but it is a baseline of the continuous and improving lifecycle of network security required for the customer's plant and operations.

'Sustainable Plant' is one of Yokogawa's initiatives to provide its customers a better if not the best solutions and services a Plant Automation and Integration company can offer. This initiative is the Life Cycle Agreement. Under this agreement, is a Defence-In-Depth strategy for securing a plant's network – Yokogawa Endpoint Security Services. Customers will benefit from monthly updates of security patches without having to bother with checking and testing the updates before rolling them out to their production network.

To ensure that every patch released by Microsoft does not cause any unwanted disruption to customers' plant operation and production, Yokogawa conducts a thorough test for each patch released against the operating systems and Yokogawa products and solutions before approval of an update. Yokogawa Engineers also specializes in implementation security requirements for customers and are more than eager to attend to the customer's help needed to secure the plant's control and operations network.

7 BACKUP & RECOVERY SYSTEM

7.1 Backup and Recovery System

It is important to have an effective backup management solution that can manage the plant-wide backup operation from a central location. The scope of this proposal will cover the backup & recovery management for only Yokogawa Windows-Based Control Systems.

7.2 Veeam Backup & Replication (VBR) Components

This section will discuss the Veeam Backup & Replication's different components and its functions.

BRS Server

The BRS Server is the assigned station for a centralized backup management system. This station houses the VBR console and performs all types of administrative activities:

- Coordinates backup, replication, recovery verification and restore tasks
- Controls job scheduling and resource allocation
- Is used to set up and manage backup infrastructure components as well as specify global settings for the backup infrastructure.

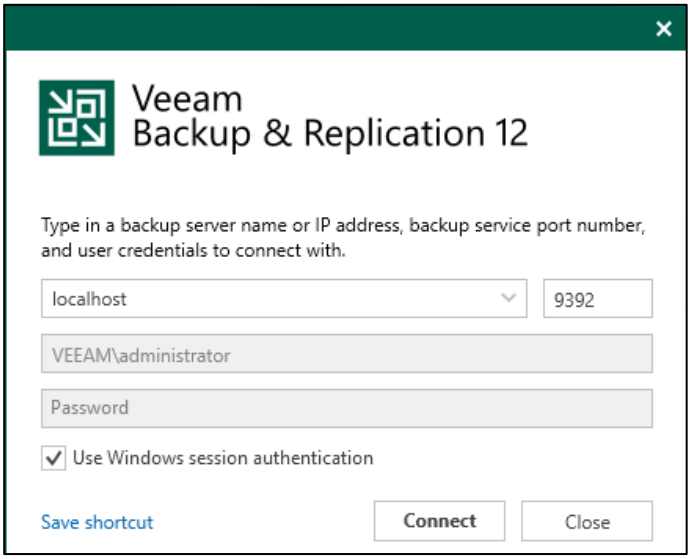


Figure 19 – VBR Login Window

7.2.1 Physical Infrastructure

This comprises the physical machines that need to be managed by the VBR server. In the Yokogawa environment, this corresponds to the physical machines that are a Yokogawa product, or a Yokogawa-provided security solutions.

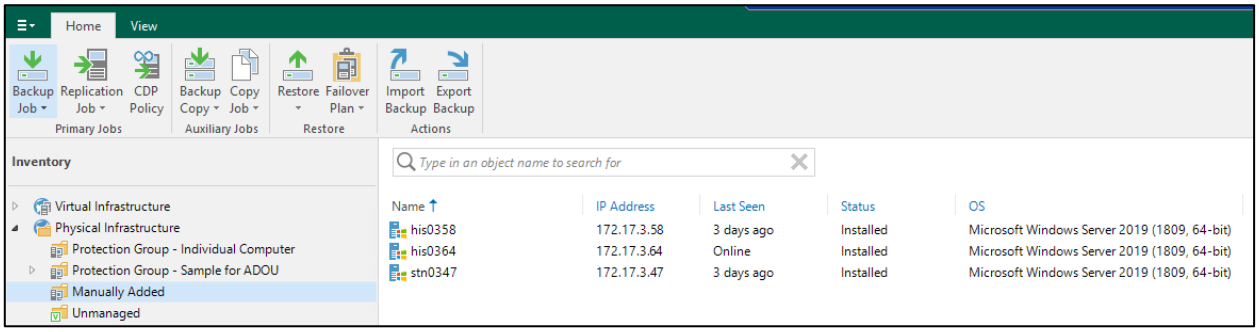


Figure 20 – Physical Infrastructure

7.2.2 Backup Repository

This refers to the storage location where Veeam keeps backup files and metadata. A disk-based storage device in the form of storage array will be used as the backup repository.

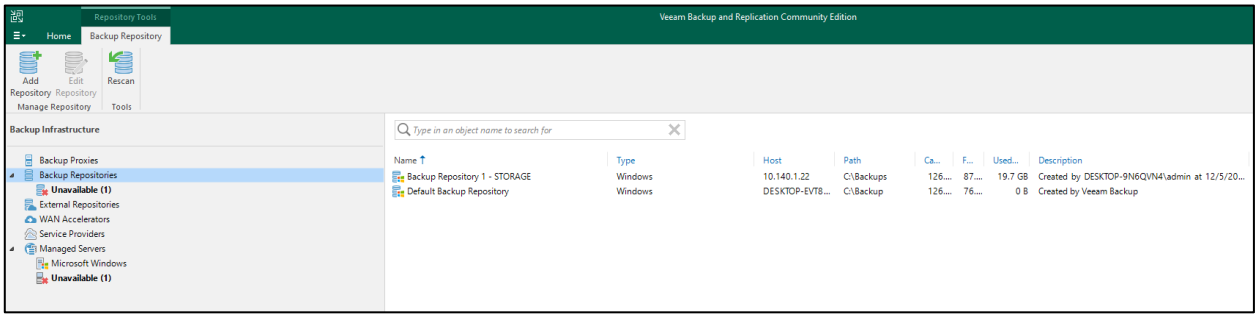


Figure 21 – Disk-Based Storage

7.3 Veeam Backup & Replication (VBR) Backup Files

VBR backup job creates different types of backup files. Backup files create a Backup Chain. Backup Chain consists of full backup file, incremental backup files and backup metadata files.

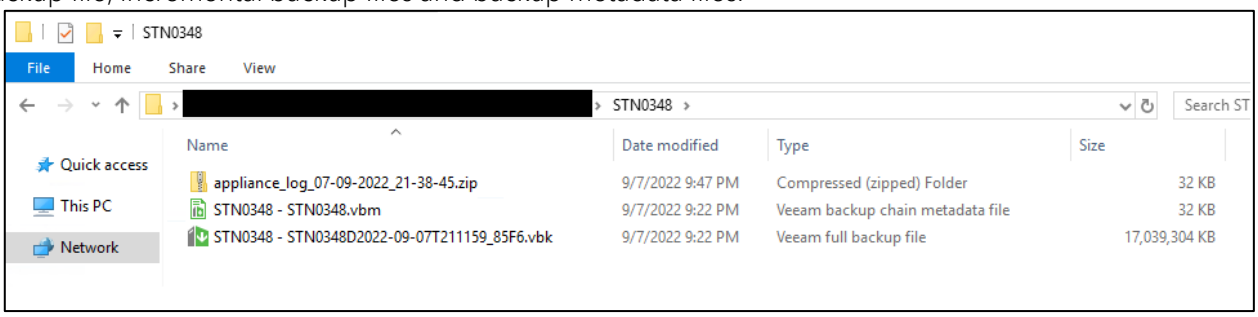


Figure 22 – Example of Backup Files (Physical Machine)

The following are the types of backup files:

a. VBK: Full backup files that store copies of full images.

b. VIB or VRB: Incremental backup files that store incremental changes of images.

7.4 RPO

Recovery point objective (RPO) The point in time that the restarted infrastructure will reflect. Essentially, this is the rollback that will be experienced because of the recovery. The most desirable RPO would be the point just before the data loss event. Making a more recent recovery point achievable requires increasing the frequency of synchronization between the source data and the backup repository.

7.5 RTO

Recovery time objective (RTO) The amount of time elapsed between disaster and restoration of business functions

7.6 Design Architecture OF BRS

The backup architecture enables centralized backup management of all critical data residing in the control systems database and is designed with a high-performance data protection strategy that integrates disk with an optimized backup application that can streamline back and recovery operations.
The key components of the architecture are as follows:

1) Backup Management Server and Storage

2) Backup Management Software Veeam backup and replication

The Backup Management Server will be connected to the PIN network at level 3. The diagram below shows the architecture of centralized backup management:

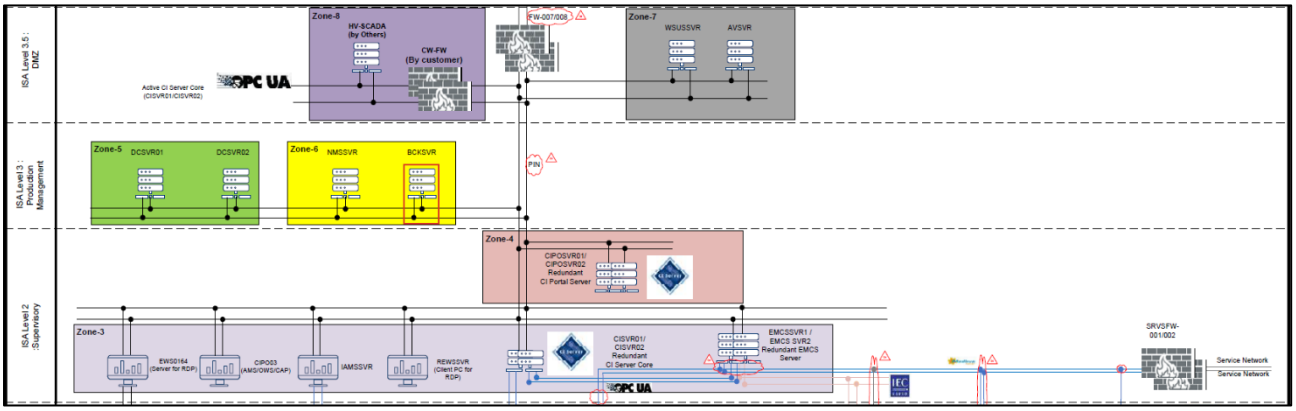


Figure 23 – Centralized Backup Management Architecture Overview

The Active Directory (AD) will be used for user authentication and authorization services. Authorized domain users will be used to log in to the BRS Server and the Veeam Environment. An organizational unit containing BRS user accounts and groups will be created. Same with the BRS Server, AD is located at Level 3 of the Purdue Model. Veeam Backup and Replication will deploy Veeam agents to the BRS clients using the PIN network. The Veeam agents will be used to establish communication with Veeam Backup and Replication. The Network Management System Server, located at Level 3 of the Purdue Model, will be utilized in the implementation. Veeam Backup and Replication will send Windows Event logs to What's Up Gold (WUG). The logs will be accessed and viewed using WUG's log management feature.

7.7 Used Ports

7.7.1 Physical Machines

From	To	Protocol	Port	Notes
Backup server	Veeam Agent Computer (Microsoft Windows)	TCP	6184	Default port used for communication with the Veeam Agent for Microsoft Windows Service.
		TCP UDP	135,137 to 139, 445,6160, 11731	Default ports used for communication with the Veeam Installer Service.
		TCP	2500 to 3300	[For Microsoft SQL logs shipping] Ports used to collect Microsoft SQL logs from the Veeam Agent computer.
		TCP	49152 to 65535	Dynamic RPC port range.
		TCP	9380	Default port used for communication with the Veeam Distribution Service.
Veeam Agent Computer (Microsoft Windows)	Backup server	TCP	10005	Default port used by Veeam Agent for Microsoft Windows operating in the managed mode for communication with the Veeam Backup server. Data between the Veeam Agent computer and backup repositories is transferred directly, bypassing Veeam backup servers.
	Veeam Agent Computer (Microsoft Windows)	TCP	9395 6183	Ports used locally on the Veeam Agent computer for communication between Veeam Agent components and Veeam Agent for Microsoft Windows Service.
Backup server	Microsoft SQL Server hosting the Veeam Backup & Replication configuration database	TCP	1433	Port used for communication with Microsoft SQL Server on which the Veeam Backup & Replication configuration database is deployed (if you use a Microsoft SQL Server default instance).

	DNS server with forward/reverse name resolution of all backup servers	UDP	53	Port used for communication with the DNS Server.
Backup server	Backup server	TCP	9501	Port used locally on the backup server for communication between Veeam Broker Service and Veeam services and components.

Table 44 - Used Ports for Physical Machines

7.8 Backup Job

A backup job refers to the process of creating copies of data to protect it from loss or corruption. These jobs ensure that critical information can be restored in case of hardware failures, data corruption, or other disasters.
There are two types of backup jobs:

1. System Backup: For Agent Backup Job, if it is required to create a backup of the entire computer image, this can be done by selecting the [Entire Computer].

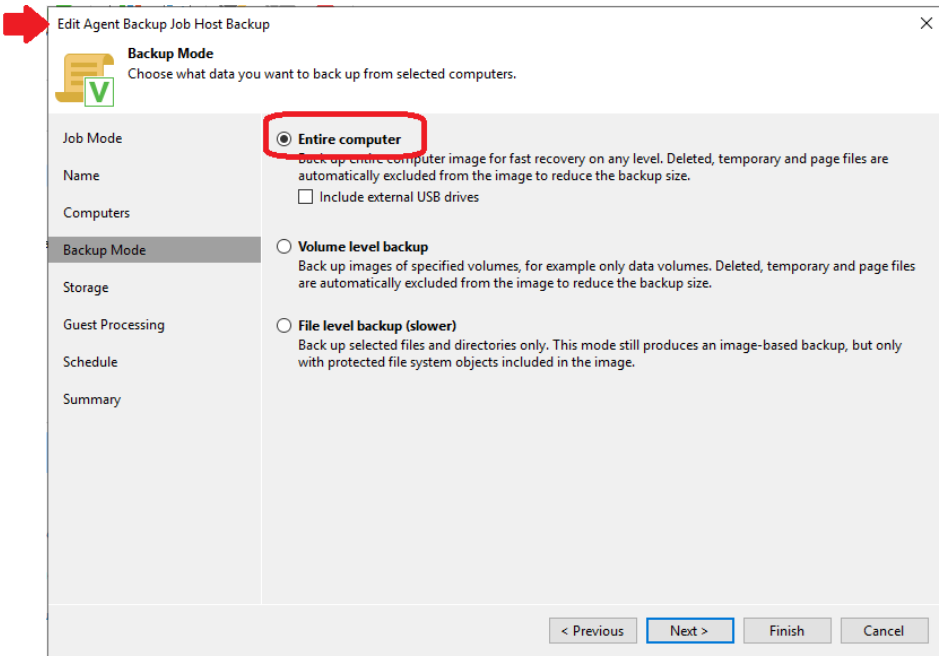


Figure 24 - Agent Backup Job – System Backup

2. Data Backup: For the Agent Backup Job, if it is required to create a backup on the data or file level only, this can be done by selecting the [File level backup (Slower)]. In Crosswind-BLPH project Data Backup will be taken.

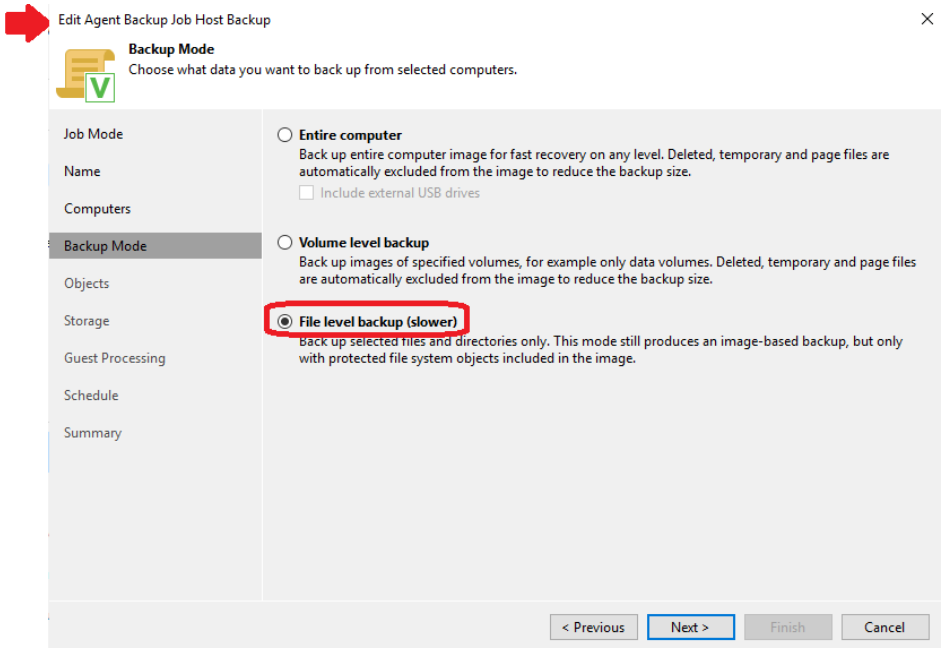


Figure 25 - Agent Backup Job – Data Backup

7.9 Backup Schedule

Efficient backup scheduling is the cornerstone of a robust data protection strategy. By defining a backup schedule job, we establish a routine that ensures the continuous availability and recoverability of our information. Regular backups not only safeguard against accidental file deletions or system failures but also provide a defense against data corruption, cyberattacks, and natural disasters. A well-planned backup schedule minimizes the risk of data loss and reduces the time and effort required for recovery. By automating this process, we can streamline backup operations and allocate resources more effectively, Backup schedules are carefully defined to not affect the plant operation during peak hours.

Host Names	Priority	Schedule for Backup (Full System Backup)	Weekly Incremental Backup
EWS0164	High	Once in a month Sunday @12:00 AM	Once in a week Sunday @1 AM
CISVR01	High	Once in a month Sunday @2:00 AM	Once in a week Sunday @2 AM
CISVR02	High	Once in a month Sunday @5:00 AM	Once in a week Sunday @3 AM
IAMSSVR	High	Once in a month Monday @12:00 AM	Once in a week Sunday @4 AM
EMCSSVR1	High	Once in a month Monday @2:00 AM	Once in a week Sunday @5 AM
EMCSSVR2	High	Once in a month Monday @5:00 AM	Once in a week Monday @1 AM
CIPO03	Low	Once in a month Tuesday @2:00 AM	Once in a week Monday @2 AM
REWSSVR	Low	Once in a month Tuesday @12:00 AM	Once in a week Monday @3 AM
CIPOSVR01	Low	Once in a month Tuesday @4:00 AM	Once in a week Monday @4 AM
CIPOSVR02	Low	Once in a month Tuesday @6:00 AM	Once in a week Monday @5 AM
CIPO04	Low	Once in a month Wednesday @12:00 AM	Once in a week Tuesday @1 AM
CIPO05	Low	Once in a month Wednesday @2:00 AM	Once in a week Tuesday @2 AM
IAMSCLT	Low	Once in a month Wednesday @4:00 AM	Once in a week Tuesday @3 AM
BCKSVR	Low	Once in a month Thursday @12:00 AM	Once in a week Tuesday @4 AM
NSMSVR	Low	Once in a month Thursday @2:00 AM	Once in a week Tuesday @5 AM
DCSVR01	Low	Once in a month Thursday @4:00 AM	Once in a week Wednesday @1 AM
DCSVR02	Low	Once in a month Friday @12:00 AM	Once in a week Wednesday @2 AM
AVSVR	Low	Once in a month Friday @2:00 AM	Once in a week Wednesday @3 AM
WSUSSVR	Low	Once in a month Friday @4:00 AM	Once in a week Wednesday @4 AM

Table 37 – BRS Backup Schedule

7.10 Backup Sizing Details

In CROSSWIND-BLPH, Backup sizing will be configured as per the below table.

SL No	Zones	Modified Names	PC Models	OS	Backup Method	Backup Target Source	Backup frequency and Schedule	Media	No of Images	Retention Period	Estimated System Image Size In GB (Monthly)	Backup Size after compression (in GB)	Full backup (2 Months retention)	Estimated Weekly incremental data (in GB)	Incremental 2 months retention (weekly * 8)	RPO (Days)	RTO (Days)
1	DCS Zone	EWS0164	GP4SY		Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	4	2 Months	600	480	1920	48	384	1	1
2	DCS Zone	REWSSVR	GP2SY		Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	600	480	960	48	384	1	1
3	DCS Zone	CISVR01	GP4SY		Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	4	2 Months	1000	800	3200	160	1280	1	1
4	DCS Zone	CISVR02	GP4SY		Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	4	2 Months	1000	800	3200	160	1280	1	1
5	DCS Zone	IAMSSVR	GP4SY		Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	600	480	960	48	384	1	1
6	DCS Zone	EMCSSVR1	GP4SY		Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	4	2 Months	600	480	1920	48	384	1	1
7	DCS Zone	EMCSSVR2	GP4SY		Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	4	2 Months	600	480	1920	48	384	1	1
8	DCS Zone	CIPO03	GP4SY		Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	600	480	960	48	384	1	1
9	Application Server facility Zone	CIPOSVR01	GP4SY		Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	600	480	960	48	384	1	1
10	Application Server facility Zone	CIPOSVR02	GP4SY		Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	600	480	960	48	384	1	1
11	Application Server facility Zone-OD	CIPO04			Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	300	240	480	24	192	1	1
12	Application Server facility Zone-OD	CIPO05			Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	300	240	480	24	192	1	1
13	Application Server facility Zone-OD	IAMSCLT			Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	300	240	480	24	192	1	1
14	Security Management Zone-2	BCKSVR			Full backup(Image), Catalog shall be added in backup	Entire disk C and D drive, Opt out SAN disk	Once per Month	SAN	1	2 Months	600	480	960	48	384	1	1
15	Security Management Zone-3	NSMSVR			Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	600	480	960	48	384	1	1
16	Security Management Zone-1	DCSVR01			Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	300	240	480	24	192	1	1
17	Security Management Zone-1	DCSVR02			Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	300	240	480	24	192	1	1
18	Demilitarized Zone	AVSVR			Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	300	240	480	24	192	1	1
19	Demilitarized Zone	WSUSSVR			Full backup(Image)	Entire disk C and D drive	Once per Month	SAN	1	2 Months	600	480	960	48	384	1	1
	Incremental backup for 8 weeks				8							8320	22720	992	7936		
	Full backup for 2 month retention				2						In GB	30656					
	Weekly incremental in %				0.1						In TB	30					
	backup size compression in %				0.8						Approx	40 TB min or 50 TB recommended			Raid failover 5 to 6 TB		

Table 38 – BRS Client Backup Size Estimation

7.11 User Account Configuration

The Windows Active Directory Domain Services will be linked to Veeam Backup and Replication, requiring users to input credentials using the **domain\username** format. Microsoft-level authorization will be configured in the Active Directory, and Veeam roles will be set in the Veeam environment.

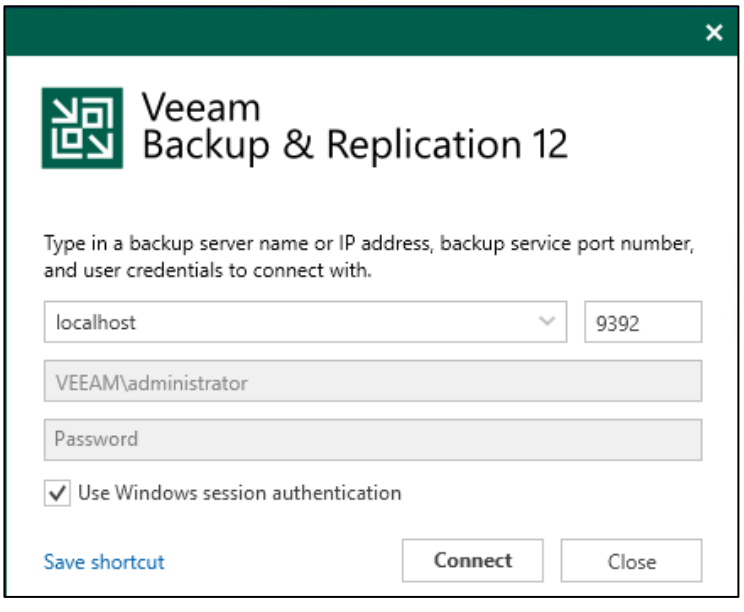


Figure 26 – Veeam Login

User account management will be handled by the Active Directory and Veeam's Security settings. The credentials used for logging in the BRS Server will be the same credentials that will be used for logging in the VBR Console. BRS Organizational Unit will be created in the Active Directory and the following is the default configuration of BRS user accounts and groups.

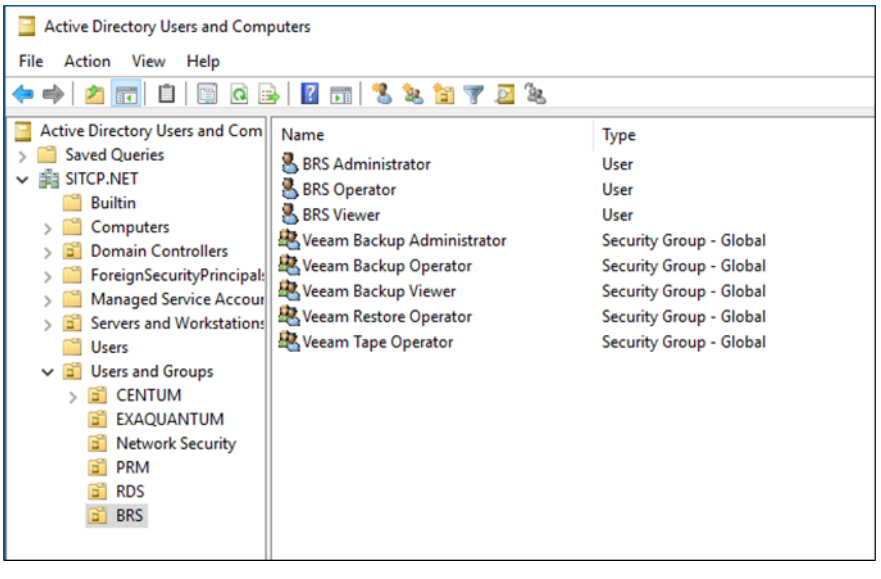


Figure 27 – Active Directory Users and Groups

User Account	AD Group
Domain\BRS Administrator	Veeam Backup Administrator
Domain\BRS Operator	Veeam Backup Operator Veeam Restore Operator Veeam Tape Operator
Domain\BRS Viewer	Veeam Backup Viewer

Table 45 - User Assignment

7.12 Audit Logs

Veeam Backup & Replication provides detailed logging of performed activities data protection and disaster recovery tasks. By default, the log files are stored in %ProgramData%\Veeam\Backup for the BRS Server, Microsoft Windows. Since Veeam follows the local system time of the BRS Server, timestamps of audit record are generated based on the server. The BRS Server's local system time is managed by the domain controller using a NTP Solution to ensure time synchronization for all servers and avoid unauthorized alteration.

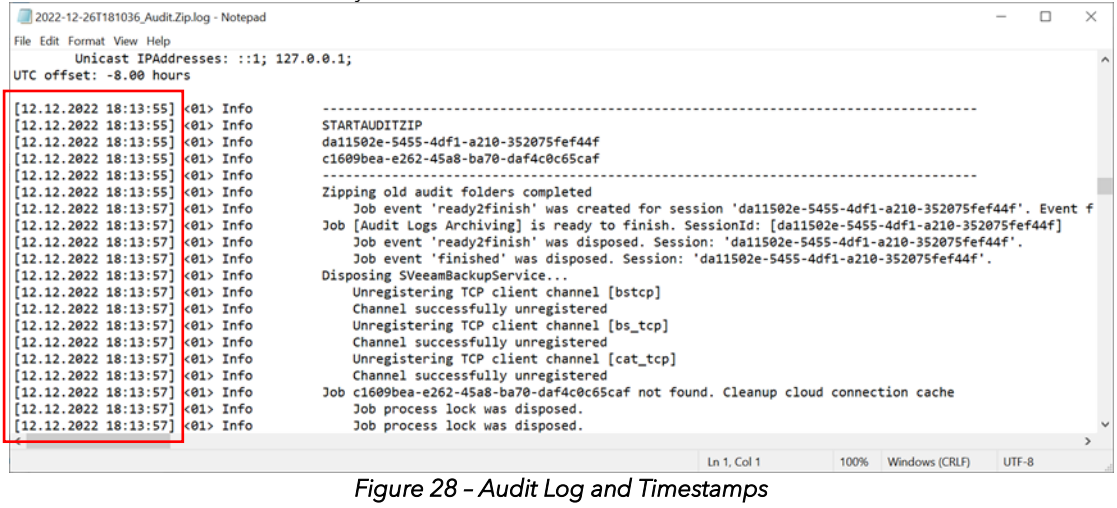


Figure 28 – Audit Log and Timestamps

7.13 Recovery Strategy

In the event of Operating System (OS) corruption which could cause control systems to malfunction or be unable to boot up, a total recovery of the system partition can be initiated by using Veeam Backup with the latest backup, even to dissimilar hardware. In the situation of data loss in control systems that may be caused by system crash, virus attack or other factors, data recovery can be performed using a similar procedure.

7.14 Verification

For file and folder restoration, Veeam Backup does not have the verification function in the restore job. However, Veeam Backup does check for corrupted files during backup. The corrupted files will not be backed up and this will be recorded in the Backup job history log. Hence, it is recommended to always check the history job log after backup and restoration jobs complete.

7.15 Reporting

Backup and Recovery Management solution includes standard reports showing detailed system information. We can view real-time statistics for rescan jobs, as well as Veeam Agent backup jobs and backup policies configured in Veeam Backup & Replication. We can also generate reports with statistical data for performed rescan jobs or backup job sessions.

8 NETWORK MANAGEMENT SYSTEM

The Network Management System (NMS) is Yokogawa's solution for providing visibility to all the monitored assets in the plant. Implementing this solution and following the recommended monitoring approach gives the plant asset administrator valuable information that could be used for asset administration, maintenance, and troubleshooting. The following commonly available functions are included in a standard management entity:

1) Network discovery
2) Topology mapping of managed device
3) Event handler
4) Performance data collector
5) Management data browser

The network management entity can be the main console for network operations. The ability to detect problems quickly in any network is critical for each plant. Network operation personnel can rely on NMS graphical network map to display the operational states of critical network devices such as routers, switches, servers, and other SNMP-based devices that NMS monitors.

8.1 Network Management System Architecture Components

8.1.1 NMS Server

The Network Management System uses the inbuilt polling capabilities to monitor the status of the devices in the network, which are then stored in its database. The NMS Server will be configured to trigger actions and generate reports based on the data it receives as per the project requirement.

WhatsUp Gold is the recommended software to be used for the Network Management System in the Yokogawa environment. Using the inbuilt polling capabilities, the application can monitor the devices by listening to MIB data, which are then stored in its database (Microsoft SQL). The WhatsUp Gold application can be configured to trigger actions and generate reports based on the data it receives. Easily accessible from any web browser, the WhatsUp Gold web console provides an effective way for engineers to view real-time and historical data.

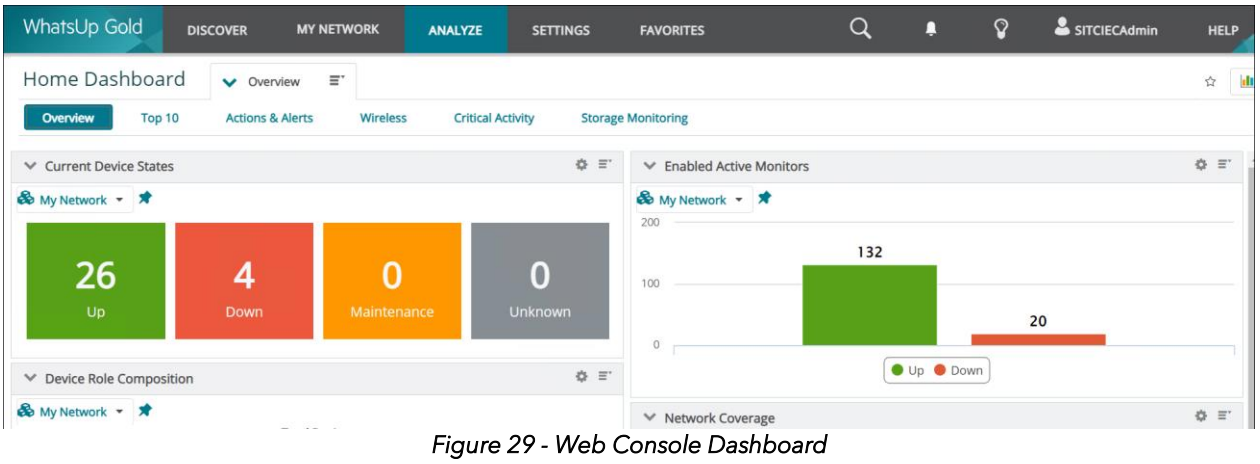


Figure 29 - Web Console Dashboard

8.1.2 Monitored Devices

The NMS Server acquires information about the devices connected to the network using multiple supported network management protocols. The gathered information is then processed by the NMS server and displayed on the console dashboard. Devices are contacted via requests, and they answer with details about their configuration and condition.

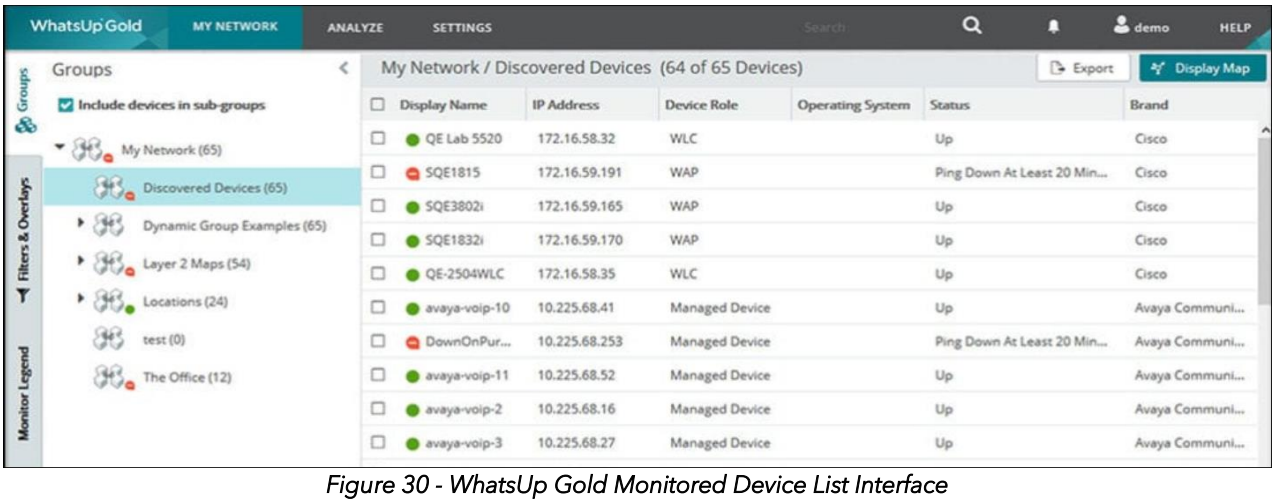


Figure 30 - WhatsUp Gold Monitored Device List Interface

WhatsUp Gold provides a visual mapping of all the monitored devices. Using this feature, the zoning shall be configured to monitor that all the devices are properly grouped according to their zone.

8.1.3 Monitoring Protocol

The NMS Server acquires information about the devices connected to the network using multiple supported network management protocols. The gathered information is then processed by the NMS server and displayed on the console dashboard.

8.2 Design ARCHitecture of NMS

The NMS server will be connected to the PIN network on Level 3. In the Crosswind-BLPH Project "WhatsUp Gold" from IP Switch software shall be used for Network Monitoring Activity.

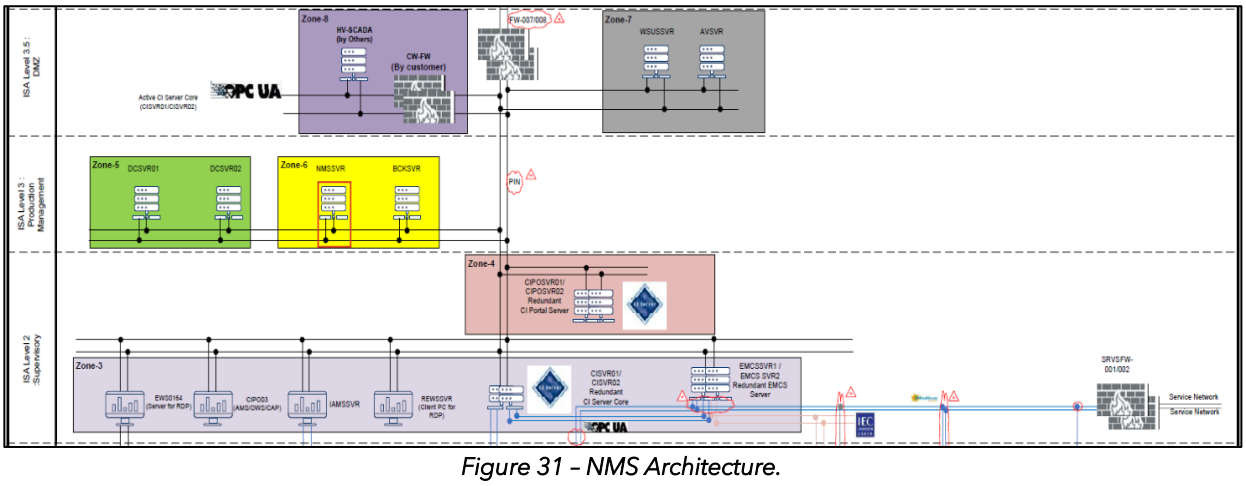


Figure 31 – NMS Architecture.

The NMS platform is integrated with Windows Domain Active Directory for user authentication in terms of WhatsUp Gold users for administration and monitoring, server-client secure communication, and domain authentication process.
Through NMS all Vnet/IP Switches and Firewalls will also be monitored. Equipment's needed to set up Vnet/IP switches and firewall monitoring are:

- Additional Ports will be required.
- Additional Configuration must be done in the Firewall.
- Additional Cables should also be laid for monitoring purpose.

WhatsUp Gold will import group information from a Microsoft Domain Controller into WhatsUp Gold. When an Active Directory group user logs into WhatsUp Gold with their Windows Domain credentials, they are automatically assigned to the WhatsUp Gold group that corresponds to that Active Directory group.

8.3 Network Management System Functionalities

8.3.1 Fault Management

The objective of fault management is to detect, log, and notify users of network problems to keep the network running effectively. Since a fault can cause network downtime or unacceptable network degradation, Fault Management is widely implemented across all industries. Fault detection is accomplished when the devices send trap messages, polling, remote monitoring thresholds, messages. Ideally, a fault management system should be able to correctly identify events and automatically act, either launching a program or script to take corrective action or activating notification software that allows a human to take proper intervention.
In an NMS management console, each network device is represented by a graphical element. Different colours on the graphical elements represent the current operational status of network devices. Upon receiving the notifications, the graphical element representing the network device changes to a different colour depending on the severity of the notification received. The notification, usually called an event, is placed in a log file.

8.3.2 Performance Management

Various interface statistics can be collected from network devices to measure the performance level. These statistics can be included as metrics in the SLA (Service Level Agreement). Statistics such as input queue drops, output queue drops, and ignored packets are useful for diagnosing performance-related problems.
At the device level, performance metrics can include CPU utilization, buffer allocation (big buffer, medium buffer, misses, hit ratio), and memory allocation. The performance of certain network protocols is directly related to buffer availability in network devices. Measuring device-level performance statistics are critical in optimizing the performance of higher-level protocols.

8.3.3 Reporting

Utilizing the Network Management System's comprehensive reporting capability, the users can quickly access pertinent information on the status of the network and all the monitored devices. You can monitor and manage your network infrastructure with the help of the several sorts of reports offered by WhatsUp Gold. WhatsUp Gold's report will include the following:

- Device inventory report: which lists all the devices on your network along with their IP addresses, hostnames, MAC addresses, and other information.
- Availability Report: This report offers details about the uptime and downtime metrics for your network's hardware and services.
- Performance Report: This report offers details about the functionality of your network's hardware and services, including CPU and memory usage and data on network traffic.
- Configuration Report: This report offers details on the hardware setup, software versions, and firmware versions of your network devices.
- User Activity Report: A report on user activity on your network, including login timings and activity logs, is provided in item number five.
- Security Report: The data in this report pertains to security-related activities on your network, such as intrusion attempts, firewall logs, and security policy violations.
- Topology Report: The network topology, including network devices and their connections, is shown graphically in this report.

8.4 Types of Device Components to Monitor

1) Network Devices: Here are the elements to be monitored for Network Devices such as Switches:
    - Ping

- Power supply
- Interfaces Status
- Temperature

2) Servers: Here are the elements to be monitored for servers:
   - Network interface port
   - CPU and memory
   - Hard disk
   - Power Supply
   - Ping
   - HDD utilization 80%

In the Crosswind BLPH project Network Monitoring System is used to monitor all the Non-Vnet/IP, Vnet/IP, and Service Switches and Firewalls.

8.5 Steps to configure the monitoring of Vnet/IP Devices.

Currently, the ports handling VNet traffic from the switches SNSW and CNSW are WAN1 and Port 1. In addition, to monitor the management traffic of Bus 1 switches (CNSW and SNSW), define two separate VLANs: 150 and 151.

- CNSW on Port 2 is assigned to VLAN 150 and is connected to the firewall on Port 2.
- SNSW on Port 3 is assigned to VLAN 151 and is connected to the firewall on Port 3.
- Ports 2 and 3 on the firewall are trunked.

Additionally, two VDOMs (Virtual Domains) have been created:

1. Transparent Mode VDOM: Dedicated for Vnet traffic. The ports assigned to this VDOM are Port 1, WAN1, and Port 5.
2. Routed Mode VDOM: Handles management traffic. The ports assigned to this VDOM are Port 2, Port 3, and Port 4.

For the firewall's management traffic, VLAN 153 is assigned to Port 4. This port is configured as a trunk link to carry the management traffic of both CNSW L2 and SNSW L2 to the Time Switch.
The Time Server is directly connected to Port 5 on the firewall. The same ports will be used for the Vnet Bus 2 firewall and switches.

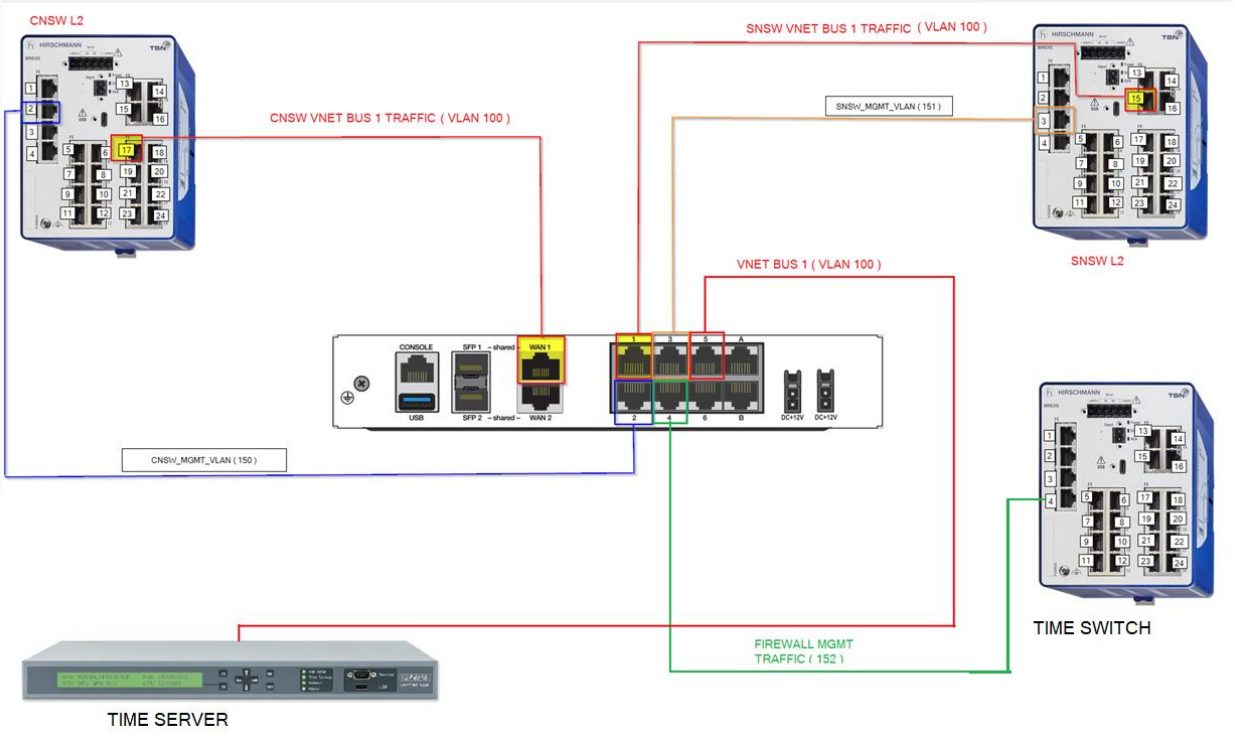


Figure 32 –Configurations to monitor Vnet/IP through NMS.

8.5.1 Active Monitoring

This monitoring normally uses standard protocol like SNMP which will be Enabled/Installed on Agents to determine its status. Active monitoring sometimes requires using MIB and OID to get more detailed and specific information about the monitored devices and some customized scripts for monitoring disk space utilization, disk space check, process checker, etc. Also, this monitoring works to pull the data from monitored devices and the NMS server will convert the collected data into an interpretable and readable format.

8.5.2 Passive Monitoring

This monitoring normally works behind the scenes approach wherein it just periodically gets information like CPU, memory, and hard disk utilization from monitored devices, this also uses standard protocols like SNMP, installed agents, MIB, and OID to get more detailed specific information. Like active monitoring this works to pull the data from monitored devices and the NMS server will convert and interpret it to readable format.

8.5.3 System Alert Monitoring and Notification

System alerts and the notifications system work together to help users stay informed about what is happening in the network and the devices connected to it. It is a cooperative relationship that can be configured to go beyond the default settings included. Using the system library functionality, notifications can be configured to Web Alarm – Console base notification.

8.6 SNMP Community Name

SNMP community name is used for authenticating communication between an NMS Server and an SNMP Agent. It needs to be configured on the NMS server and all managed devices running SNMP v1 and v2 to successfully establish communication.

8.6.1 SNMP Configuration for Microsoft Windows

The following are the SNMP settings for Windows server 2022-based machines:

S No.	Parameters	Input (Example)	Remarks and Explanation
1	Community Name	CROSSWIND-BLPH	Community Name for communication exchange between NMS Server and Managed Devices
2	SNMP access rights	READ-ONLY	SNMP access rights (Default)
3	Host	172.17.1.42	NMS Server's IP address
4	Trap destinations	172.17.1.42	NMS Server's IP address
5	SNMP Trap community name	CROSSWIND-BLPH	Community Name for Passive Monitor

Table 46 – SNMP Settings for Windows

8.6.2 SNMP Configuration for L2 / L3 Switches and Firewall

The SNMP username's password must meet the minimum complexity requirement. Password will be shared through KEEPASS.

Username	Password	User Access Mode	SNMP Version	Authentication	Encryption	SNMP Access Mode
*********	*******	READ ONLY	version 3	SHA/MD5	DES	READ ONLY

Table 47 – SNMP Settings for Hirschman Switches

8.7 WUG Visualizations

WhatsUp Gold provides two viewing modes and tools that help track down where a problematic device is located. Below are the views provided by WhatsUp Gold.

8.7.1 Map View

The Map view allows creation and viewing of a network's graphical representation. In this view, icons signify information such as device's relationship, status and type. Devices are added into the map either manually or through WUG discovery. Discovery is performed using the ICMP and SNMP protocol, it scans a specific IP address range for manageable devices. Map view can be accessed by any devices in the PIN Network.



Figure 33 – WhatsUp Gold Map View

Note: WUG does not display map with more than 256 devices.

8.7.2 Device View

The Device View gives you an in-depth look at the current status of your devices; it shows the current state of the devices and the monitored status associated with it. Below is the figure of device view.

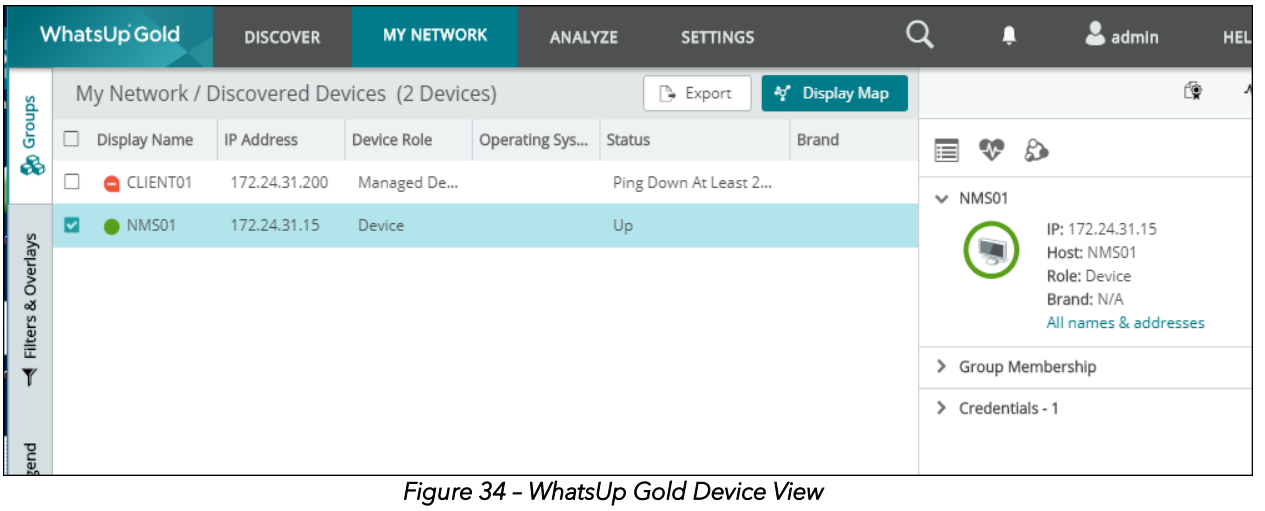


Figure 34 – WhatsUp Gold Device View

9 Application Whitelisting

Application whitelisting is a process that controls the behavior of the applications that are stored or installed in a computer system. It enables the administrator to manage these applications to be either authorized or not to run/execute whenever configured on the system.

Application whitelisting is designed to permit the execution and processes of known programs and software and block all others. This helps mitigate threats that any unauthorized application can trigger whenever it is invoked to run or executed.

As one of the leading vendors in the field of whitelisting software, Trellix Application Control software offers easily scalable protection, fast performance, and flexible design to protect system from viruses, worms, Trojan horses, as well as potentially unwanted code and programs. Trellix Application Control is the whitelisting software that ensures the endpoint servers and workstations remain malware execution free. It prevents the execution of unknown software including malicious software.

Apart from preventing an unauthorized application to run/execute on a host, application whitelisting can also provide the following features:

- Keeping track of the software applications that are authorized or not to run/execute.
- Monitors the integrity of an application whenever there is an attempt to change the file.
- Notifies the administrator of an attempt to run an unauthorized application file and to change an application file for a proper incident response from the organization.
- Memory protection or the technique to prevent zero-day attacks based on buffer overflow.
- Access control for portable storage devices.
- ePO integration.

9.1 Design Architecture

Application whitelisting main objective is to protect all servers and workstations supplied with and installed Yokogawa software products. Yokogawa systems and applications shall be configured on every station as an authorized application as well as a trusted updater to cater to the changes that are required daily for production and operations purposes. Pre-defined policies catered for Yokogawa software applications are configured on the managed clients to allow the set of applications defined as a whitelist.

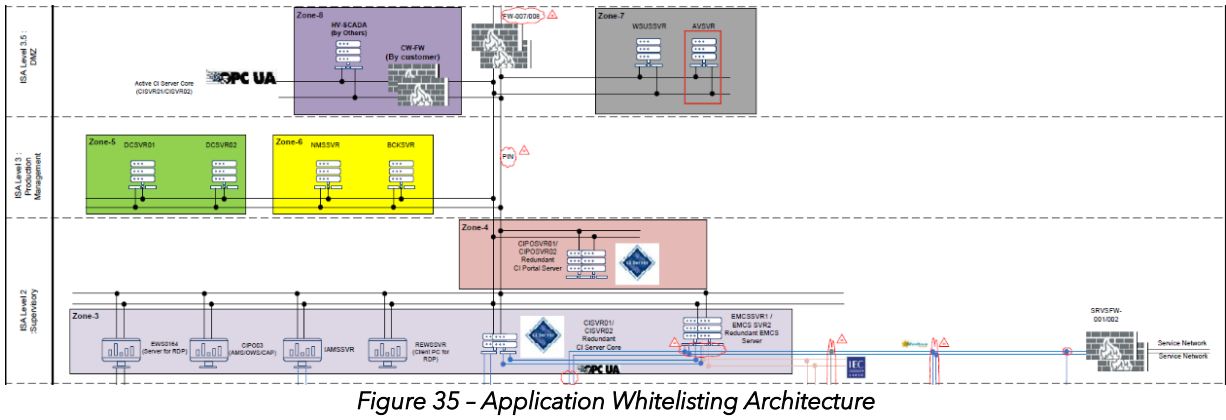


Figure 35 – Application Whitelisting Architecture

Application Whitelisting shall be deployed on target stations and servers (with supported Windows OS and Yokogawa software application installed) connected in PIN Level 2. A Central management server shall also be connected to the PIN Level 2 network, this server shall be installed with Trellix ePolicy Orchestrator (ePO) in the network to manage the Whitelisting software, and stations with the Whitelisting application.

ePO management server shall be joined to Active Directory Domain Services (ADDS) in place to enforce centralized authentication for administration and monitoring, server-client secure communication, and domain authentication process.

9.2 Application Whitelisting Components

This section describes the components that are required in Application Whitelisting. Application Whitelisting solution is composed of:

- ePO Management Console
- Trellix Agent
- Trellix Application Control

9.2.1 ePO Management Console

The management console is used with the server for easy management of the Application Whitelisting solution. The console can be accessed from the server that is hosting the Application Whitelisting solution or remotely through any web browser. All the configurations and management tasks can be configured through the console. The management console will be used for the following functions:

- Deploys, monitors, and manages agents to clients.
- Manages Solidcore (*1) software packages and extensions for rules and policies of the applications authorized to run and update the systems of the managed stations.
- Console display for status updates of managed stations and servers on communication and compliance with the current rules and policies configured on the ePO.
- Trellix logs files connection with Log Management Platform – Log files generated by Trellix ePO Console (activity, error, and debug logs) will be available for the Log Management Platform to extract and analyze.

Note: (*1) Solidcore is a software package and extensions that shall be installed on the ePO management server for the deployment of the Yokogawa Standard Application Whitelisting solution. Trellix incorporates Trellix Application and Change Control solutions in a single software package. The scope of this specification is solely for Application Control.

9.2.2 Trellix Agent

The agent provides a secure communication channel from the managed client to the ePO server. It downloads and enforces policies and executes client-side tasks such as deployment and updating. The agent is also responsible for uploading events and status to the ePO server.

9.2.3 Trellix Application Control

Application Control protects IACS-connected devices against malware attacks before they occur by proactively controlling the applications that run on managed devices. In turn, this also prevents zero-day attacks by blocking the execution of unauthorized applications. Key features of Application Control:

- Prevent malicious, untrusted, or unwanted software from being executed.
- Automatically identify trusted software and authorize it to run.
- Block users from introducing software that poses a risk to your company.

Note: Trellix Application Control is a Solidcore software package for ePO that will be used for the Yokogawa Standard Application Whitelisting solution.

9.3 Application Whitelisting for Yokogawa Systems

One of the basic functionalities of application control is to whitelist an application software with the following attributes: that include file path, filename, file size, digital signature, and even the checksum or the

cryptographic hash of an application file. This type of whitelisting requires the right balance of configurations in terms of the security, maintainability, and usability of application software.

Setting a simpler attribute such as file path, or file name may not be a powerful configuration given that it can still allow an unauthorized application software to run. The same applies to digital signatures and checksum or cryptographic hash. Setting a whitelisting configuration for these two attributes is more secure in blocking unauthorized application software but may cause problems or issues with usability and maintainability in case an authorized application is updated.

Application Whitelisting solution shall implement the file and folder attributes control for the related Yokogawa software applications.

9.4 Application Whitelisting Mode

Application whitelisting offers various operation runtime modes when implemented. This helps the administrator to either evaluate the behaviour of the host on the applied whitelist or completely allow or not the application to execute whether authorized or not.

9.4.1 Enabled Mode

Application Whitelisting enabled mode permits only whitelist items to be executed and blocks the execution of all others.

9.4.2 Update Mode

Application Whitelisting is active but allows changes to take place while providing and enforcing memory protection. This mode allows for product upgrades or removal to take place.

9.5 Event and Response

ePO management server provides a platform to manage clients and their corresponding status and events centrally. This information is stored locally in the ePO server database and is accessible from the ePO console dashboard.

9.6 Trellix ePolicy Orchestrator (ePO) Server

To deploy the Application whitelisting solution, an ePO server installation is required to be set up and configured.
The ePO server provides a platform for central management for the following:

- Application Control software package and its extensions required for the implementation.
- Trellix Agent software and deployment
- Rules and Policies configuration
- Web-based management console for administration and operation.

Before the ePO is set up, the server will be joined to the domain environment as defined in the table below. The domain user account must also have administrative privileges or be a member of the domain / local administrators' group.

9.6.1 Trellix ePolicy Orchestrator (ePO) Server Configuration

The Trellix ePolicy Orchestrator server will manage both the Application Whitelisting and the Yokogawa Standard Antivirus Software (ENS).

9.6.2 Yokogawa System Tree Groups

The System Tree groups refer to the location where all the managed systems are presented. The managed system can be organized into logical subgroups based on their machine type, topological/ geographical

locations, or their functionality boundaries. Creating subgroups for systems with similar properties or requirements allows the administrator to manage policies and tasks for the system in one location.

9.6.3 Yokogawa System Tree Groups Members

Target stations and servers for Application Whitelisting configuration shall follow the recommended member grouping to manage and distinguish all the client machines with ease.

9.7 Application Whitelisting Policy

A policy is a collection of settings that is created, configured, and then enforced. Policies make sure that the managed security software products are configured according to the required settings and perform correctly. Policies are grouped by product followed by category. Each policy category refers to a specific subset of policy settings.

Application whitelisting restricts or denies the execution of all other programs other than what is classified as a whitelist. This method protects the stations and servers from any malicious code execution. Predefined Yokogawa policies shall be imported to the ePO server for the implementation of required policies applicable to the systems included in the Yokogawa group.

Policy Name	Description
Yokogawa_Policy_MA.xml	The file defines the following policies of Trellix Agent for Yokogawa Standard Whitelisting Software: General Repository Troubleshooting Custom Properties Product Improvement Program
Yokogawa_Policy_Solidcore.xml	The file defines the following policies of Solidcore for Yokogawa Standard Whitelisting Software: Integrity Monitoring Rules (Windows) Application Control Rules (Windows) Application Control Options (Windows) Exception Rules (Windows) Configuration (Client)
Yokogawa_Policy_ Assignment_Rules.xml	The file defines the following assignment rules for Yokogawa Standard Whitelisting Software Yokogawa (KB91569) Yokogawa (Yokogawa Standard AV)

Table 48 – ePO Policy Templates

Import the Solidcore rules as defined in the table below.

Rule Name	Description
Yokogawa_Solidcore_Rules.xml	The file defines the following Solidcore rule groups for Yokogawa Standard Whitelisting Software: Windows Update (KB91569), Yokogawa

Table 49 - Solidcore Rules Import

Import the Tags policy as defined in the table below.

Tag File	Description
Yokogawa_Tags.xml	The file defines the following tags for Yokogawa Standard Whitelisting Software: Yokogawa Standard AV Windows 7 Windows 10 LTSB 2016

	Windows 10 LTSC 2019 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022

Table 49- System Tags Import

9.8 Application Whitelisting Task

Create and schedule client tasks to automate how the system is managed in the network. In this project, client tasks are used for Application Control commands and Product Deployment.

To fully establish the endpoint protection of every server and station in the IACS network, ePO is required to push install all the required software packages on each managed station. This can easily be done by setting a task for the managed stations. ePO shall be configured with the product deployment and Application Whitelisting tasks that shall be utilized for the installation of agents and tasks on each managed client.

9.9 Report and Logs

Create and schedule client tasks to automate how the system is managed in the network. In this project, client tasks are used for Application Control commands.

The ePO comes with Querying and Reporting capabilities which can create and run queries and reports that result in user-configured data in user-configured charts and tables. In addition to these capabilities, logs are available that gather information about activities that occur on the ePO server and throughout the network.

The table below lists the default queries, reports, and logs that can be generated and viewed on the ePO server.

Category	Item	Description
Query	Solidcore Health Monitoring	Compliance reports that include Application Control
Report	ePO Summary	A report showing a high-level summary of activity.
Log	Audit	Audit Log maintains and accesses records of all ePolicy Orchestrator user actions.
Log	Server Task	Server Tasks Log shows the detailed results of scheduled server tasks that are running or have been run on the server.
Log	Threat Event	Threat Event Log is used to quickly view and sort through events in the database.

Table 50 - Querying and Logging

10 FIREWALL

A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow. In most server infrastructures, firewalls provide an essential layer of security that, combined with other measures, prevents malicious attackers from accessing your servers. Combining firewalls with other network security solutions provides a higher level of security, thus it is highly recommended to adopt a multi-layered security approach. Firewalls are subdivided into two types:

- Hardware Firewall: Hardware firewalls are standalone devices with custom software and hardware, it is deployed directly onto a network and performs traffic filtering between trusted and untrusted zones.
- Software Firewall: Software firewalls perform almost the same function as hardware firewalls but in the form of a program installed on the host's operating system. Since a firewall is installed on the host itself, in a scenario where the host/workstation is not connected to the corporate network it will still be protected.

10.1 Design Architecture: Overview

Firewalls are one of the key features and factors in designing and implementing a network as these devices can help secure the network from threats that originate at every point of attack. Firewalls act as the first line of defense which are logically deployed between trusted and untrusted zones, as shown in the below figure.

Yokogawa is using a "defense in depth" approach that protects lower-layer assets even when defense at a higher layer is broken. To achieve the defense-in-depth, reduce risks, costs, and failures, and build a robust, secure, and cost-effective system, a proper network architecture that can serve as the basis for security countermeasures is essential. In Level 3.5 (DMZ), the Firewall serves as a buffer zone to cater to the security solutions (AV/OS) . The firewall provides another layer of security in the network to prevent the Office Domain (outside network) and Yokogawa/Process Control Network (inside network) from having a direct connection to each other domains.

In Level 2 (PCN), a Firewall is placed between the DCS and SIS system to segregate the network within the Control Network (Vnet/IP) to prevent attacks such as man-in-the-middle attacks and allow only the authorized stations and packets to communicate with each other.

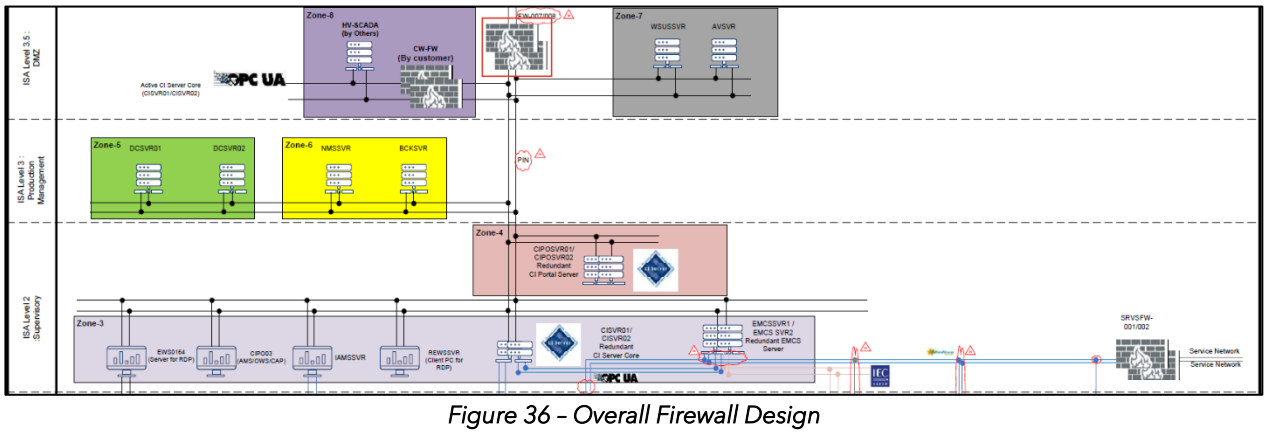


Figure 36 – Overall Firewall Design

10.2 Firewall Function

When choosing firewalls, it is important to pay attention to their capability and features. These make a huge difference in designing and securing the network. Infrastructure requirements differ from one customer to

another, depending on the situation a feature may be of greater importance compared to others. The most common required firewall functionalities are as follows:

10.2.1 Packet Filtering

- Stateful Firewall: A stateful firewall can hold in memory significant attributes of connections, from start to finish. The attributes, known as the state of the connection, include details such as source and destination IP addresses, communication ports, and sequence numbers of the packets traversing the firewall.

By keeping track of the connection state, stateful firewalls provide added efficiency in terms of packet inspection. This is because for existing connections the firewall needs only to check the state table, instead of checking the packet against the firewall's rule set.

- Stateless Firewall: A stateless firewall watches network traffic and restricts or allows packets based on source and destination IP addresses, and other static values. It is not 'aware' of traffic patterns and data flows. It simply uses rule sets that do not account for the possibility wherein a packet received by the firewall might be 'pretending' to be a legitimate packet or it is spoofed. Stateless firewalls are typically faster and perform better under heavier traffic loads.

In the CROSSWIND-BLPH project, Stateful Firewalls are provided at DMZ (L3.5).

10.2.2 Firewall Operation Mode

- Routed Firewall: A routed firewall from the name itself performs routing functions. An IP address is required to be configured on its interfaces. It acts as a router and can also act as a default gateway to connected networks. All Firewalls in this project are configured to function under Routed Mode. In the CROSSWIND BLPH project, all non-VNet/IP firewalls will be in routed mode.
- Transparent Firewall: A transparent firewall performs Layer 2 functionality; it allows communication and filtering between devices on the same network or IP subnet. It acts like a "bump in the wire" or a "stealth firewall", for it is not perceived as a router hop by the connected devices. Because of that, it can be easily introduced onto existing networks; without the necessity to readdress IPs.

In the CROSSWIND BLPH project, all Vnet/IP firewalls will be in Transparent mode.

10.2.3 Network Object

Object groups are a firewall component that enables the administrator to easily configure and implement policy rules in the network. It is very useful for streamlining subsequent configuration of policies such as access rules. Defined objects can be modified, and it will be inheriting all the modifications done by any rules linked to it instead of manual entry.

10.3 Firewall Hardening

The main purpose of a firewall is to secure the network. It is just as important to make sure that the firewall is secure or “hardened”. This will prevent it from being compromised. Hardening is the process of securing your device or hardware by reducing its surface vulnerability. To secure the firewall the following feature for the CROSSWIND-BLPH project will be implemented:

1) Login Strategy - Password complexity shall be enforced for this project
2) Security Banner - This is to give a warning to an intruder who wants to access the firewall.
3) Access Rules - Implementing a “deny all /permit none” rule at the end of the rule base.
4) Policies & Procedure - Policies and procedures need to be documented and put in practice. Such as change management.
5) Physical Security
6) Unused Ports are Disabled.

10.3.1 Security Banner

The following login banner will be set for the CROSSWIND-BLPH project on firewalls.

Firewall Login Banner
"***Unauthorized Access is prohibited *** This property belongs to 'CROSSWIND-BLPH' and any unauthorized access will be logged and investigated. Violators will be prosecuted in conformance with local state laws."

10.4 Firewall Management

Firewall Management is one of the key components for maintaining a secure and functional network. Monitoring the status, logs, and configuration changes of the firewall helps in the maintenance and troubleshooting. Network engineers should perform and document the following:

1) Changes to the firewall rule base
2) Changes to system and/or group definitions
3) Changes to the authentication configuration established at the user, client, and session levels
4) Changes to the network routing tables and ACLs
5) Changes and upgrades to firewall software, per licensing agreement(s).

11 Switches

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive, or forward data packets or data frames over the network.

A switch has many ports, to which multiple devices are plugged. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks, and sends the frame to the corresponding device(s). It supports unicast, multicast as well as broadcast communications.

11.1 Switch Role

11.1.1 PIN Switch

The level 3.0 PIN switch is connected to the level 3.0 Servers (NSS, AD, BCK server). This switch must be used for all traffic going from these servers to other networks and from those networks to these servers.

11.1.2 Vnet/IP Switch

The Vnet/IP Switches are special switches used only to connect the devices that are capable of communication in Vnet/IP Protocol. These devices are referred to as stations. The Station can be a Controller, Engineering Station, Human interface station, or other station.

11.1.3 Switch Functions

Only Layer 2-managed switches are envisaged for this project. The features supported are listed below.

1) It is an intelligent network device that can be conceived as a multiport network bridge.
2) It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
3) It supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
4) It supports creation and configuration of VLANs.

11.1.4 Redundant Switch Configurations

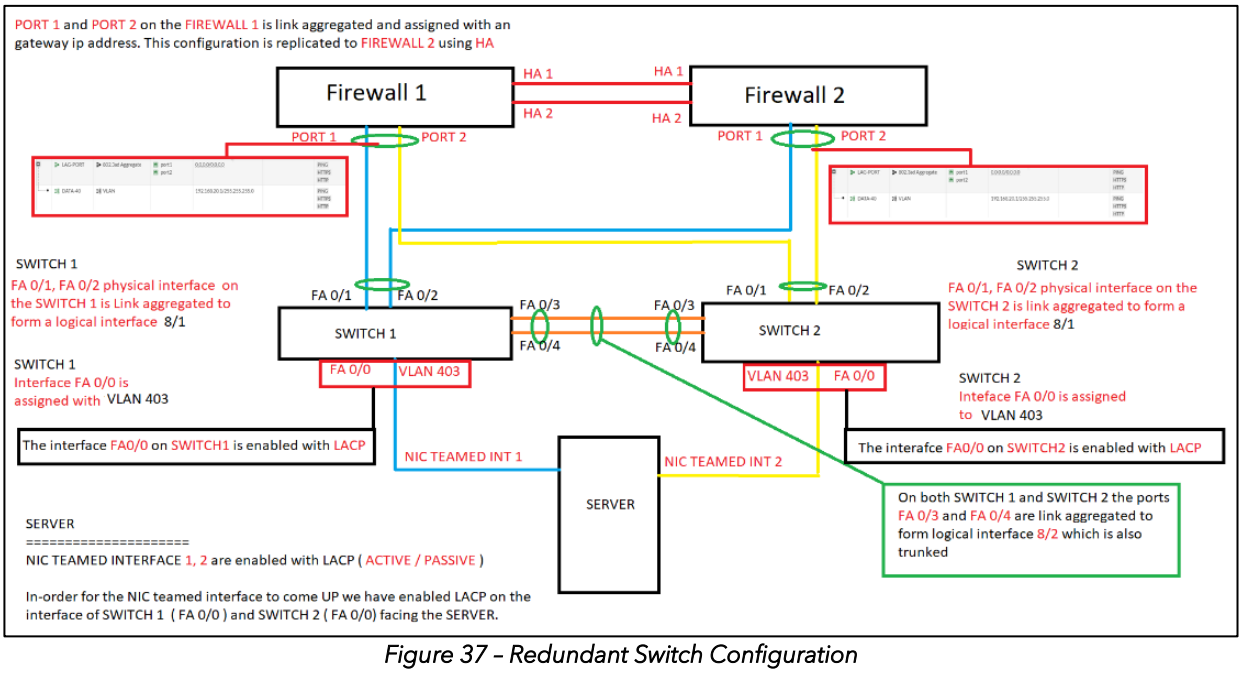


Figure 37 – Redundant Switch Configuration

As per above diagram server is connected to two switches (Switch 1 and Switch 2) via NIC teaming, and both switches are connected to two firewalls with link aggregation and trunking enabled. This ensures that in the event of a failure in one link or device, traffic can automatically reroute through the alternative paths, maintaining network continuity.

Additionally, with MSTP (Multiple Spanning Tree Protocol) configured on the switches, the failover process will be much faster, ensuring minimal downtime in case of any failure. This setup optimizes the network's resilience and performance.

In addition to the redundancy achieved through NIC teaming and link aggregation, the firewalls in this setup are configured in High Availability (HA) mode. This ensures that if one firewall fails, the secondary firewall will automatically take over without any disruption to the network traffic.

With the combination of HA on the firewalls and MSTP (Multiple Spanning Tree Protocol) on the switches, the entire network is highly resilient. Failover processes will be seamless and fast, providing continuous network uptime and reliability in case of any component failure.

This document undergoes an issuance cycle within EDMS Fusionlive. Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

12 Remote Access Connection

A remote access connection allows users to connect to a computer or network from a remote location, enabling them to access resources, applications, and data.

In Crosswind- BLPH Project Remote Access is taken by enabling the Remote Desktop Connection (RDP) in all the machines which are in level 2,3 and 3.5. A user can log into CIPO04, CIPO05, IAMSSCLT and can access the CIPO03, REWSSVR via RDP, wherein we get access to log into all the servers in ITER region. We can also take the remote of AD, AVSVR, and WSUS server by CIPO04, CIPO05, IAMSSCLT via RDP.

Remote Access Connection enables flexibility wherein a user can access and monitor all the devices wherever and whenever they need without moving to the physical Location.

This document undergoes an issuance cycle within EDMS Fusionlive. Its distribution is electronically controlled. Once printed shall be considered as "NOT CONTROLLED" copy

13 Network Flow Diagram

Below diagram shows the flow of network in Crosswind-BLPH Project.

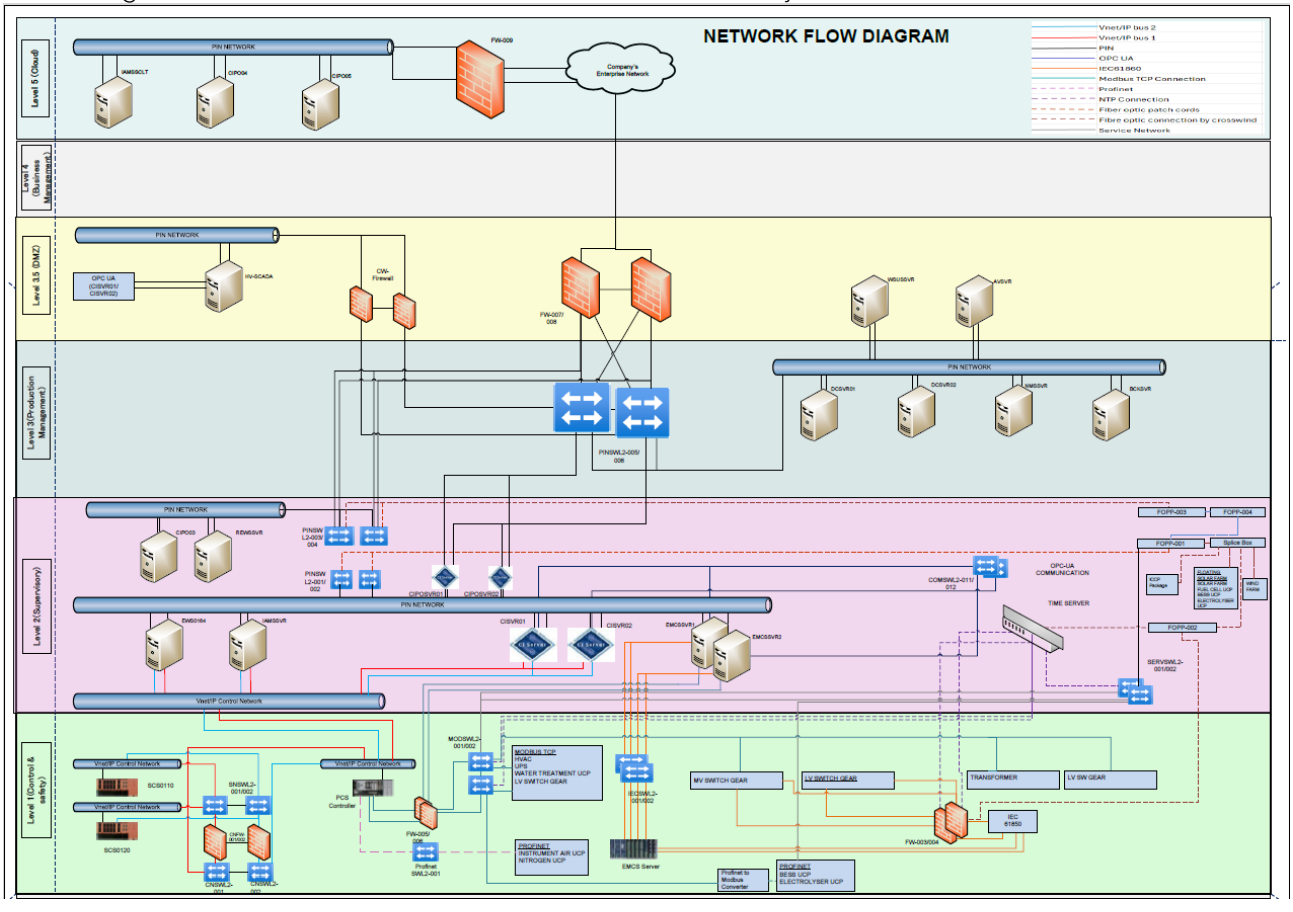


Figure 38 – Network Flow Diagram