

State of Florida

Department of Transportation



DISTRICT FOUR

APPENDIX 8
IT SERVICES STANDARD OPERATING
PROCEDURE (SOP)
Transportation Systems Management and
Operations (TSM&O) Device Maintenance
Contract, District Four

Financial Project Number(s): 406795-7-72-01 and various

Proposal/Contract Number: E4X61



7.01 Scope of Services & Policies

Table of Contents

IT DEPARTMENT OVERVIEW..... 4

SCOPE OF SERVICES..... 5

 Responsibilities.....5

 Security IT Resources5

INTRODUCTION – POLICIES 6

SECURITY AND USE OF INFORMATION TECHNOLOGY RESOURCES 7

 Access and Disclosure7

 Internet Use and Company Computer Network.....7

 Computer Network Use Limitations8

 Prohibited Activities8

 Illegal Copying8

 Communication Of Trade Secrets.....8

 Accessing Internet.....8

 Frivolous Use.....8

 Virus Detection.....9

 Privacy9

 No Expectation of Privacy9

 Waiver Of Privacy Rights.....9

 Monitoring Of Computer and Internet Usage9

 Blocking Sites with Inappropriate Content9

 Password Security9

 Inappropriate Use.....9

 FDOT Topic No. 325-060-020 - Document Update.....10

 Introduction11

 Physical Access Control11

 Internet Monitoring11

 Public Records Law.....12

 Password Complexity12

 Disaster Recovery Plans12

 Adherence To District IT Resource Usage Policy12

 FDOT Topic No. 325-000-002, Chapter 2 - Access to the Department's Information Technology Resources (Document Update).....13

 7.01.05 FDOT Topic No. 325-000-002, Chapter 11, Electronic Device and Media.....13

Document & Version History

Version #	Date	Author	Changes
1.0	12/13/2023	Yana Neishlos	Initial Draft
1.1	3/14/2024	Yana Neishlos	Combined 7.00 with 7.01 as one inclusive document under 7.01

IT DEPARTMENT OVERVIEW

These Standard Operating Procedures (SOPs) in Section 7 are followed by the Information Technology (IT) group at the Florida Department of Transportation (FDOT) District 4 building at 2300 W. Commercial Blvd, Fort Lauderdale, FL 33309. The SOP includes policies, processes, standards, plans, and procedures for managing IT resources, devices, software, and employee use of equipment.

The IT department, headquartered at the TSM&O RTMC, has a broad range of responsibilities for the District Four ITS program.

The IT department for District Four is responsible for all systems within the TSM&O RTMC building. Systems at the Vista Center have also been included in that description along with TIMSO within the Treasure Coast.

There are several annex FDOT buildings where equipment is located, ranging from Fort Lauderdale, as well as parts of Palm Beach.

The IT department is not officially responsible for anything physically located outside of these buildings. However, a partnership and a coordinated hand-off of responsibilities is required by the ITS program outside of these two buildings.

SCOPE OF SERVICES

There are many Cisco core switches physically located outside of the building at hub sites throughout District Four.

Responsibilities

To be closely defined, these would be the maintenance contractors' responsibility, as the current maintenance contractor for District Four. However, the IT department is fully responsible for all configuration of the Cisco core switches. The IT department also assists in troubleshooting of field-related problems. Into this mix of responsibilities also comes the software contractors, responsible for the SunGuide deployments within District Four.

Oftentimes the source of an apparent SunGuide problem can turn out to be SunGuide itself, the servers that SunGuide runs on, the network (either internal or external to the building), and finally the field devices. Due to the challenges to track down the root cause of such problems, the IT group assists with troubleshooting of problems of this type.

In addition, the IT department is involved in the planning and implementation of major ITS deployments. ITS deployments are largely field based in nature, with minimal systems installed in house. However, the network design (including the field network) must be in place in conjunction with the IT department. Hand-off and testing at the completion of major ITS deployments is the final step of that process, often involving many hours of work from the IT department.

Security IT Resources

Network Security falls under the IT department's responsibilities.

Due to the multitude of doorways leading to our network, one department must take responsibility for all. Security has a direct impact on all the IT department functions.

However, it includes things like:

- Establishing end-user policies for e-mail and Internet usage,
- Requirements for communicating to other districts and outside agencies,
- Policies on configuration of PCs,
- Laptops and Servers,
- Restrictions on network usage,
- Password requirements,
- Network designs.

In addition, included are things like recommending that door sensors be placed on file cabinets.

It is these policies and processes that keep the network operational and secure. Many of these processes are described in this IT SOP.

INTRODUCTION – POLICIES

You will find here the included policies for Florida Department of Transportation Policy that outline the network setup, access, remote access, and applications on the ITS system.

- Policies outlined:
- Section 7.01.01: Security and Use of IT Resources
 - Section 7.01.02: FDOT Topic No. 325-060-020 Security and Use of Information Technology Resources
 - Section 7.01.03: ITS TMC IT SOP
 - Section 7.01.04: FDOT Topic No. 325-000-002, Chapter 2, Access to the Department's Information Technology Resources
 - Section 7.01.05: FDOT Topic No. 325-000-002, Chapter 11, Electronic Device and Media Sanitization

- Features covered:
- Passwords
 - Using personal devices on the network.
 - Using the network only for RTMC-related activity, not personal Internet use.
 - Approved applications.
 - Change management checklists.

It is the responsibility of the IT Support Manager to guarantee that TSM&O RTMC policies meet or exceed those set out in this document.

SECURITY AND USE OF INFORMATION TECHNOLOGY RESOURCES

This policy outlines regulations regarding the security and use of Information Technology (IT) resources, including e-mail and internet by TSM&O RTMC personnel. Information technology resources include computer hardware and devices, software, networks, connections, applications and data.

Florida Department of Transportation policy, [Topic No. 325-060-020 Security and Use of Information Technology Resources](#) (SOP Section 7.01.02), with E-mail, Internet, and Anti-Virus Software is included with this policy. SMART SunGuide RTMC personnel are required to be familiar with this policy.

The RTMC IT Support Manager, the primary point of contact, replaces all references to the Chief Information Officer (CIO), Information Security Manager (ISM), and Office of Information Technology (OIT) in this policy.

The internet is a worldwide network of computers with vast amounts of information. Users are cautioned when reading articles with offensive, sexually explicit, and inappropriate material. In general, it is unavoidable. Even innocuous search requests may lead to sites with highly offensive content. Moreso, your e-mail address may lead to unsolicited e-mail with offensive content. We use the internet at our own their own risk. Florida Department of Transportation District Four TSM&O Regional Transportation Management Center, hereafter referred to as the RTMC, is not responsible for material viewed or downloaded from the internet.

Access and Disclosure

The RTMC reserves the right to access, review, download, print, copy, delete, modify, or disclose the contents of a user's electronic communications at its sole discretion.

Internet Use and Company Computer Network

The computer network is the property of the RTMC; to be used for business purposes.

Users are provided with network access when doing their jobs. Also, certain employees ("Users") may be provided with internet access through the computer network. Users have a responsibility to use the RTMC's computer resources and the internet in a professional, lawful, and ethical manner. Abuse of the computer network or the internet, may result in disciplinary action, including possible termination, and civil and/or criminal liability.

Computer Network Use Limitations

Factors	Details
Prohibited Activities	<p>Without prior written permission from the RTMC, the computer network may not be used to disseminate, view, or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horse programs, etc.) or any other unauthorized materials. Occasional personal use of the computer is permitted if such use does not a) interfere with the users or any other employee's job performance; b) have an undue effect on the computer or the RTMC network's performance; c) or violate any other policies, provisions, guidelines, or standards of this agreement or any other of the RTMC. Further, always, users are responsible for the professional, ethical, and lawful use of the computer system. Personal use of the computer is a privilege that may be revoked at any time.</p>
Illegal Copying	<p>Users may not copy material protected under copyright law or allow that material to be copied. You are responsible for complying with copyright law and applicable licenses that apply to software, files, graphics, documents, messages, and other material for download or use. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the RTMC.</p>
Communication Of Trade Secrets	<p>Unless authorized, Users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to the RTMC. Unauthorized dissemination of such material may result in severe disciplinary action and substantial civil and criminal penalties under state and federal Economic Espionage laws.</p>
Accessing Internet	<p>To ensure security and avoid the spread of viruses, users accessing the internet through a computer attached to the RTMC's network must do so through an approved internet firewall or other security device. Bypassing the RTMC's computer network security by accessing the internet directly by modem or other means is strictly prohibited unless the computer you are using is not connected to the RTMC's network.</p>
Frivolous Use	<p>Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits. Network Users have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the internet, playing games, engaging in online chat groups; uploading, or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the internet.</p>

Factors	Details
Virus Detection	Files obtained from sources outside the RTMC, including disks brought from home, files downloaded from the internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage the RTMC's computer network. Users should never download files from the internet, accept e-mail attachments from outsiders, or use disks from non RTMC sources, without first scanning the material with the RTMC-approved virus checking software. If you suspect that a virus has been introduced into the RTMC's network, notify the IT department immediately.

Privacy

Factors	Details
No Expectation of Privacy	Employees are provided with computers and internet access to do their jobs. There will be no privacy in any data employees manage, send, or receive using the RTMC's computer equipment. The computer network is the property of the RTMC and may be used only for company purposes.
Waiver Of Privacy Rights	An employee waives a right of privacy in any data managed, sent, or received using the company's software equipment. User consents to allow RTMC personnel access and review all materials managed, sent, or received by User through any RTMC network or internet connection.
Monitoring Of Computer and Internet Usage	The RTMC has the right to monitor and log all aspects of its computer system including, but not limited to internet visited, chat and newsgroups, file downloads, and all communications sent and received by users.
Blocking Sites with Inappropriate Content	The RTMC has the right to utilize software to identify and block access to internet sites containing sexually explicit or other material deemed inappropriate in the workplace.
Password Security	Individual access rights to the RTMC's communications systems and employees' passwords must be associated with an account issued in the name of an authorized user. The protection of an individual's password is a prime responsibility of a password owner. If something is authored from a password-protected system, it is presumed that an owner of the password is the author.
Inappropriate Use	Prohibited uses of the RTMC's communications systems include the following:

Factors	Details
	<ul style="list-style-type: none"> • Accessing, viewing, transmitting, or storing obscene or other inappropriate material such as pornography or email chain letters. • Engaging in unlawful or unethical communication including communication that is defamatory, obscene, harassing, or gambling. • Use of passwords to gain access to another user's information without proper authorization. • Knowingly introducing a computer virus or worm. • Developing or using programs which attempt to bypass system security mechanisms or to obtain unauthorized access to system resources or to interfere or disrupt system users or resources. • Excessive personal use of the RTMC communications systems. • Downloading files, listening to music, watching TV, and playing games. • Unauthorized screen savers or wallpapers.

Abuse is possible.

Hence, a good judgment and a commonsense approach must be used. It is inappropriate to use any resource which will interfere with the timely performance of normal work duties, cast disrespect or adverse reflection upon the RTMC or FDOT, reduce public confidence, support a personal business or outside employment, support political or religious activities, or detract from the RTMCs routine functions.

FDOT Topic No. 325-060-020 - Document Update

Section 7.01.01 References the FDOT Policy for Security and Use of Information Technology Resources.

This document is updated on a regular basis and can be found at the following link: [FDOT Topic No. 325-060-020, Security and Use of Information Technology Resources](#).

TMC INFORMATION TECHNOLOGY POLICIES

Introduction

The Florida Department of Transportation's (FDOT) traffic management centers (TMC) operate Florida's state roadways. Each TMC is equipped with mission critical assets that must be protected from unauthorized and inappropriate access, usage, and theft. The TMC's standard operating procedures (SOPs) are responsible for implementing ways to protect these assets. Several relevant policies and statutes are critical for explicit inclusion into the TMC SOPs statewide. They are listed in the following subsections along with implementation guidance for the TMC to comply with the relevant policies and statutes.

This policy guidance applies to: Intelligent Transportation System (ITS) facilities and ITS information technology resources. A TMC is a building housing at least one FDOT owned workstation permanently connected to the ITS Network for purposes of operating the Freeway Management System.

ITS Information Technology Resources are computer hardware, software, networks, devices, connections, applications, and data owned, operated, leased, or managed by the ITS operations.

Control Policy Statement	Implementation Controls Requirement
--------------------------	-------------------------------------

Physical Access Control

Rule Chapter 60GG-2, Information Technology Security, Florida Administrative Code (F.A.C.), requires that: information technology resources be protected by physical controls; agencies implement procedures to manage physical access to information technology facilities; and physical access to central information resource facilities be restricted to authorized personnel.

Also, [Topic No. 325-060-020, Security and Use of Information Technology Resources](#), requires that: information be created and maintained in a secure environment and safeguards be established to ensure the integrity and accuracy of Department information that supports critical functions of the department.

The TMC shall implement building and other access controls to protect the TMC and other assets.

Internet Monitoring

In accordance with Topic No. 325-060-020, Security and Use of Information Technology Resources, employees are prohibited from using IT resources for accessing, sending, storing, creating, or displaying inappropriate materials including, but not limited to gambling, illegal activity, sexually explicit materials, or materials

TMC shall implement controls for Internet access. Controls shall restrict access to inappropriate materials as defined above. A commercial web-filtering product

Control Policy Statement	Implementation Controls Requirement
that include profane, obscene, or inappropriate language, or discriminatory, racial, or ethnic content.	configured to deny access to these sites shall be in place as one of these controls.

Public Records Law

Chapter 119, Florida Statutes (F.S.) defines a public record as "all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

In addition, all state, county, and municipal records are open for personal inspection and copying by any person.

Providing access to public records is a duty of each agency." Topic No. 325-060-020, Security and Use of Information Technology Resources prohibits the use of non-departmental email systems (i.e., Gmail, AOL, Yahoo-mail) through the Department's network.

Password Complexity

Rule Chapter 60GG-2, F.A.C., defines a complex password as having at least 8 characters and being comprised of at least 3 of the following categories: uppercase English letters, lowercase English letters, numbers 0-9, and non-alphanumeric characters.

The rule also states that user accounts will be authenticated, at a minimum, by a complex password.

TMC shall implement controls requiring complex passwords to comply with the requirements in Rule Chapter 60GG-2 F.A.C at a minimum.

Disaster Recovery Plans

Rule Chapter 60GG-2, F.A.C., states that "each agency shall document disaster recovery plans that address protection of critical IT resources and provide for the continuation of critical agency functions in the event of disaster."

TMC shall have a Disaster Recovery Plan in place that defines the continual traffic operation if the primary TMC facility is no longer able to operate traffic.

Adherence To District IT Resource Usage Policy

Rule Chapter 60GG-2, F.A.C., states that "each agency is responsible for establishing an information security program that

[Topic No. 325-060-020, Security and Use of Information](#)

Control Policy Statement	Implementation Controls Requirement
<p>includes security policies, procedures, standards, and guidelines." The information security program ensures administrative, operational, and technical controls sufficiency to reduce to an acceptable level risks to the confidentiality, availability, and integrity of agency information and information technology resources. Topic No. 325-060-020, Security and Use of Information Technology Resources "applies to all Department information technology resources that access, process, or have custody of data.</p> <p>This includes all owned, leased, and contracted services involving mainframe, distributed processing, and networking environments. Department information technology resources are intended to be used for department business." Everyone with authorized access to the Department's IT resources must follow the policy, information security standards and procedures.</p>	<p>Technology Resources fulfills Rule Chapter 60GG-2, F.A.C.</p> <p>TMC staff shall be furnished with this policy and will sign and date a statement indicating they have read and will follow this policy. Completion of annual computer training addressing these computer security issues also meets the intent.</p>

FDOT Topic No. 325-000-002, Chapter 2 - Access to the Department's Information Technology Resources (Document Update)

Section 7.01.01 references the FDOT Policy for Accessing the Department's Information Technology Resources. This document is updated on a regular basis and can be found at the following link: [FDOT Topic No. 325-000-002, Chapter 2, Access to the Department's Information Technology Resources](#).

7.01.05 FDOT Topic No. 325-000-002, Chapter 11, Electronic Device and Media

Section 7.01.01 references the FDOT Policy for Accessing the Department's Information Technology Resources. This document is updated on a regular basis and can be found at the following link: [FDOT Topic No. 325-000-002, Chapter 11, Access to the Department's Information Technology Resources](#).



7.02 TSM&O NETWORK OVERVIEW

Table of Contents

- TSM&O NETWORK OVERVIEW.....4**
- FDOT.....5**
 - Consultant Offices5
 - SUNGUIDE.....5
 - IP Address Numbering Plan for IT5
 - VLANs.....5
- VIDEO6**
- COMPUTER NAMING STANDARDS7**

Document Version History

Version #	Date	Author	Changes
1.0	12/14/2023	Yana Neishlos	Initial Draft

TSM&O NETWORK OVERVIEW

There are currently two networks used in the RTMC.

One network is directly connected to the FDOT headquarters and is for the use of FDOT employees.

The other network carries the Office and SunGuide traffic. The office portions of the network permit e-Mail and Internet access, while the SunGuide portions of the network do not.

Office and SunGuide networks are separated from each other through their IP addressing schemes, by residing in separate Active Directory domains and using separate VLANs.

FDOT

Overview

PCs in use by FDOT employees in the RTMC connect directly to the FDOT District Four headquarters network at 3400 W. Commercial. The RTMC IT group does not support or manage these computers in any way. FDOT employees who use these computers to connect to the FDOT network must put in their own help desk tickets for any support to the FDOT.

The RTMC does have devices within 3400 W. Commercial that are supported directly by the RTMC personnel, however, these devices are located on a dedicated network connecting back to the RTMC controlled and managed by the IT Department.

Consultant Offices

The office portion of the network includes all VLANs used for internal corporate business applications. The distinguishing feature of this portion of the network is that its users may access e-Mail and the Internet. Computers on this network are almost universally on the Smartsunguide.com domain.

SUNGUIDE

The SunGuide portion of the network includes all VLANs used to support the SunGuide application. It is intended to be separated from the office network. However, for practicality there remain a very few controlled access points to the Office network. The distinguishing feature of this portion of the network is that its users may NOT access e-Mail and the Internet. Computers on this network are almost universally on the Field.net domain.

The SunGuide network also carries a great deal of video and other data traffic from the multitude of cameras, traffic detectors, electronic traffic notification display signs, image detection, and more sources installed in the ITS service area.

IP Address Numbering Plan for IT

The IP address numbering plan is in a document stored in the N: drive.

N:\System Documents\IP Addresses.

VLANs

All IP Address information is controlled through a secure IP Address database within the RTMC Monitoring system.

This system is located at: <https://solarwinds.smartsunguide.com>.

VIDEO

Currently, District Four has standardized on the use of MPEG2 multicast video, using VBrick encoders and decoders with a small exception of MPEG4 multicast video from Impath Encoders and IP cameras utilizing H.264.

The ITS also displays video from other networks, such as MPEG4 and Impath currently used by District Six.

District Four shares video with several other locations:

- District Six
- District Four main office at 3400 Commercial Blvd
- Broward County Sheriff's Office
- Trafficland
- 595 Express
- Florida's Turnpike

COMPUTER NAMING STANDARDS

Due to the sensitivity of the information in this document, it is only accessible by IT personnel at the following link: [DOCX File viewer | Microsoft Teams](#).

Place sensitive documents such as "Computer Naming Standards" in  [IT Documents](#) folder.



7.03 NETWORK ACCESS

Table of Contents

Version #	Date	Author	Changes
1.0	12/14/2023	Yana Neishlos	Initial Draft

Table of Contents

NETWORK AND ACCONT ACCESS – EMPLOYEE STATUS	4
Permanent Employees.....	4
Internal Contractors.....	4
External Contractors	4
Access Control.....	5
Identification and Authentication.....	5
NETWORK USER ACCOUNTS & PASSWORDS	6
Periodic Review of Accounts	6
Computer Passwords.....	6
Minimum Complex Password Requirements	6
Password Management Database.....	6
OKTA SELF-SERVICE FOR NEW USERS	7
Overview.....	7
Sign into Okta	7
Set Up Okta Verify.....	8
Set Up SMS Authentication.....	9
Set Up Voice Call Authentication.....	11
Enter a secondary email.....	13
OKTA SELF-SERVICE FOR EXISTING USERS	14
Sign Into Okta - Account Settings.....	14
Set Up Okta Verify.....	15
Set Up SMS Authentication	19
Set Up Voice Call Authentication	20
Select a Forgotten Password Question	21
Select a Security Image	23
OKTA: RESET YOUR PASSWORD OR UNLOCK YOUR ACCOUNT	24
Reset Your Password.....	24
Unlock Your Account	25
VPN CONNECTION	28
Request VPN Access	28
Okta Self-Service.....	28
Install And Open the Cisco ANYCONNECT Client	28
Enroll MFA Factors to log in to CISCO ANYCONNECT	30
Enroll in 1 – Call.....	30
Enroll in 2 - Push.....	32
Enroll in 3 - SMS.....	35
Log In to CISCO ANYCONNECT with MFA Factors Enrolled.....	36

NETWORK AND ACCOUNT ACCESS – EMPLOYEE STATUS

For the creation of a new user ID, the proper request form must be electronically signed and approved by the employee's manager a FDOT representative, and the RTMC IT Support Manager.

There are types of users who are given access to the RTMC network:

- Permanent employees.
- Internal contractors.
- External contractors.

Users requiring wireless access can connect to the FDOT On Ramp wireless network.

Permanent Employees

A permanent employee is a full-time employee who works at the RTMC usually every day of the week. These users are permitted access to the RTMC network in accordance to their respective scopes of work. For a new employee, use the following:

- New User Ticket Request, located at: https://support.smartsunguide.com/catalog_items/952373-new-hire-request.

The ITS Program Manager must OK this user access to the VPN, with a signed form to permit the user access to the VPN. New employees are also provided a 20-30-minute personal orientation to get familiar with the security implications of their access to the computers and network and. Also, they will get chance to answer questions about their responsibilities in this matter.

Internal Contractors

Internal contractors work onsite at the RTMC for the most work week. They are granted access to the RTMC network in accordance with their respective scopes of work.

For a new internal contractor, use the following:

- New User Ticket Request, at: https://support.smartsunguide.com/catalog_items/952373-new-hire-request.

The TSM&O Resource Manager must approve this user access to the VPN, with a signed form to permit the user access to the VPN. New internal contractors go for a 20 – 30-minute personal orientation to get familiar with the security implications of their access to the computers and network and, to allow them to answer questions and clarify their responsibilities in this matter.

These rules apply when a permanent employee (internal contractor) is granted network access:

1. Network ID and password are set to expire every 45 days.
2. When an ID is set to expire or the employee is no longer working for the DOT, the Office Manager must notify the IT group without delay.

External Contractors

An external contractor works at the RTMC only as needed for the scope of their tasks. These rules apply when an external contractor is given access to the network:

1. Network ID is set to expire every 30 days, for Active Directory.
2. For access approval to the VPN, a contractor must contact TSM&O IT Group to be granted access. The TSM&O Resource Manager must OK user access to the VPN.

Access Control

- FDOT TSM&O Resource Manager shall be responsible for authorizing access to information.
- IT Department shall review access rights periodically based on risk, access account change activity, and error rate.
- Workers shall be authorized access to agency information technology resources based on the principles of "least privilege" and "need to know."
- IT Department will assure access to information media is limited to authorized workers.
- Access authorization shall be promptly removed when the user's employment is terminated or access to the information resource is no longer required.
- Wireless access to an internal network shall require user-authentication.
- Only IT Support Manager approved wireless devices, services, and technologies may be connected to the internal network.
- Procedures for granting remote access shall be documented.
- Users may remotely connect computing devices to the internal network only through approved, secured remote access methods.
- Remote access client connections shall not be shared; used only by an authorized user.
- Only authorized information technology resources may connect to the internal network.
- Only IT Department approved managed mobile storage devices are authorized to store data.
- No privately-owned devices (e.g., MP3 players, thumb drives, printers) shall be connected to information technology resources without documented authorization from the IT Support Manager.
- Mobile computing devices shall be issued to and used only by authorized users.
- Mobile computing devices shall require user authentication.
- Workstations and mobile computing devices shall have enabled a screensaver secured with a complex password and with the automatic activation feature set at no more than 15 minutes.

The IT Department shall monitor for unauthorized information technology resources connected to the internal network.

Identification and Authentication

- ITS Unit computer users shall have unique user accounts.
- Where technology permits, user accounts shall be authenticated at a minimum by a complex password.
- The IT Support Manager shall ensure accounts with administrative rights are created, maintained, monitored, and removed in a manner that protects information technology resources.
- The ITS Unit shall not use vendor-supplied default passwords.
- Administrative account activities shall be traceable to an individual.

Upon leaving the Department or RTMC as a contractor a maximum of 30 days an account will be kept online, including email account access as well as profile and personal usage. All files required for continual operations must be taken over by the immediate supervisor of the said personnel leaving before 30 days is up.

NETWORK USER ACCOUNTS & PASSWORDS

Network user accounts are maintained in Active Directory within each of the domains (smartsunguide.com and field.net).

Periodic Review of Accounts

Every six months, IT group prints a list of active accounts. This list is reviewed by the RTMC Office Manager and the RTMC ITS Program Manager to verify active users for the following accounts:

- Active directory / iVEDS / SunGuide
- E-mail addresses / Telephone directory/voice mail / VPN access

Computer Passwords

Computer passwords at the RTMC are governed by the following rules. Passwords are needed for system security and are used to track user activity. Users are responsible for their passwords.

Minimum Complex Password Requirements

For all accounts within District Four TSM&O Unit these minimum complex password requirements are:

1. Must be a minimum of 14 characters in length.
2. Must be different from the last 24 passwords used.
3. Must contain at least one character from three of the following four categories:
 - a. Uppercase English characters (A-Z).
 - b. Lowercase English characters (a-z).
 - c. Numbers (0-9).
 - d. Non-alphanumeric special characters (~!@#\$%^&* _ - + = ` | \ () { } [] : ; " ' < > , . ? /).
4. Must not contain the User Account (User ID) or parts of the User's Full Name (First & Last Name) that exceed two consecutive characters.
5. Must be changed every 60 days.

Password Management Database

System Passwords are stored on a Password Management Database. The Password Management Database is configured in a high available active/passive configuration. All passwords are stored in real time on the primary database with a 1-minute delay for replication purposes to a disaster site in Fort Pierce. The database has 2-factor authentication, and full audit trail history of who, what, and when was a password resource active. The password manager has Federal Information Processing Standard (FIPS) 140-2 compliance capability. All passwords are encrypted with 256Bit Advanced Encryption Standard (AES) encryption both at the application and database level.

The password manager can verify that passwords within its database are in fact meeting the complexity requirements.

All workstations and laptops have been configured to automatically and lock after 15 minutes of non-use. Users are required to re-enter a username and password combination to unlock.

Users requiring wireless access can connect to the FDOT ONRAMP wireless network.

OKTA SELF-SERVICE FOR NEW USERS

Overview

This SOP Section outlines the steps for new users to register their Okta Self-Service account. The procedures provided below are → setting up the multifactor authentication (MFA) factors, entering a secondary email, choosing a forgot password question, and choosing a security image. The Okta Verify application on the user's mobile device is required for setting up the Okta Verify, SMS Authentication, and Voice Call Authentication MFA factors.

Steps / Screenshots

Sign into Okta

- 1.a Click the following link to access the Okta website: <https://smartsunguide.okta.com>.

Note.

The UserPrincipalName (UPN) format (i.e., username@domain.com) is required, when entering your username in the username field to sign into Okta.

- 1.b Using the UPN format,
- Enter your SMART SunGuide credentials.
 - Click **Sign in**.



Figure 1. Okta Sign-in Page

Steps / Screenshots

Set Up Okta Verify.

2.a On the **Set up multifactor authentication** screen,

- Click **Configure factor**.



Figure 2. Okta Verify Setup Screen

2.b Download the Okta Verify app onto your mobile device:

- **iPhone** - Download **Okta Verify** from the App Store.
- **Android** - Download **Okta Verify** from the Google Play Store.

2.c Once the **Okta Verify** app has been downloaded on your mobile device,

- Select **iPhone** or **Android** for your mobile device type.
- Click **Next**.

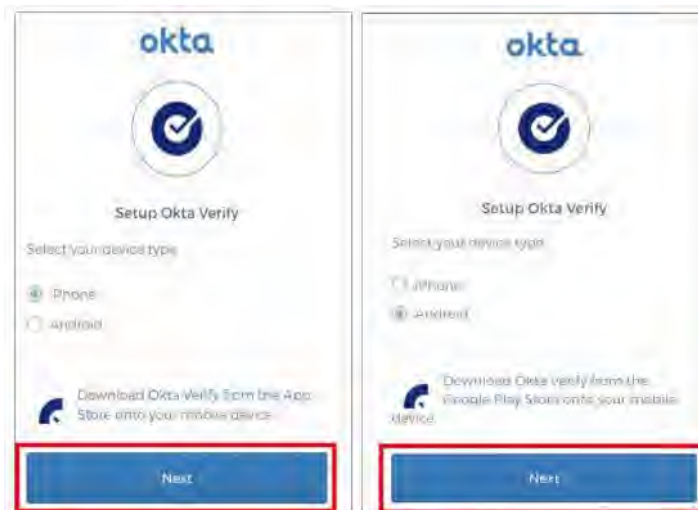


Figure 3. Okta Verify Setup - Mobile Device Type

2.d Open the Okta Verify app on your mobile device:

- Click **Add Account**.
- Select **Organization for account type**.

Steps / Screenshots

- Click **Scan a QR Code**.

- 2.e With your mobile device, scan the QR code on the **Setup Okta Verify** screen.



Figure 4. Scan the QR Code

- 2.f At the **Account Added** screen on your mobile device, → Click **done**.

Set Up SMS Authentication.

- 3.a Under Extra Verification,
- Click **Set up** next to SMS Authentication.

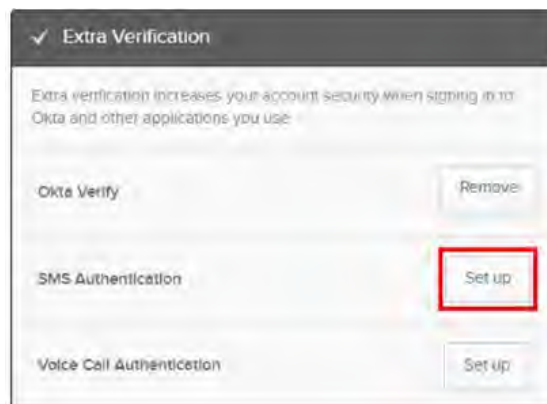


Figure 5. Set Up SMS Authentication

#	Steps / Screenshots
---	---------------------

- | | |
|-----|---|
| 3.b | <p>On the Set up multifactor authentication screen,</p> <ul style="list-style-type: none"> Click Setup. |
|-----|---|



Figure 6. SMS Authentication Set Up Screen

- | | |
|-----|--|
| 3.c | <p>On the Receive a code via SMS to authenticate screen,</p> <ul style="list-style-type: none"> Enter your phone number. Click Send code. |
|-----|--|



Figure 7. Receive a Code via SMS to Authenticate Screen

- | | |
|-----|--|
| 3.d | <ul style="list-style-type: none"> Enter the code from the text message that was sent to your mobile device. Click Verify. |
|-----|--|



Figure 8. SMS Authentication Code

Steps / Screenshots**Set Up Voice Call Authentication.**

- 4.a Under Extra Verification,
- Click **Set up** next to *Voice Call Authentication*.

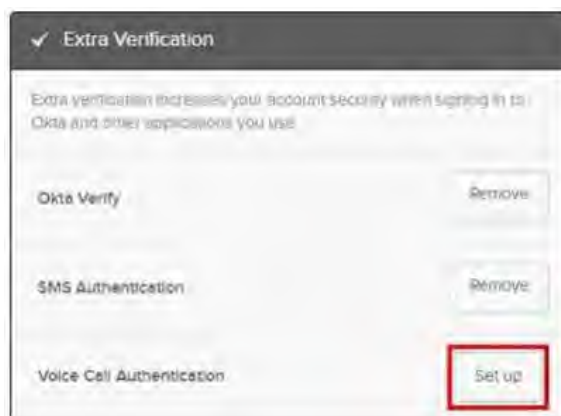


Figure 9. Set Up Voice Call Authentication

- 4.b On the Set up multifactor authentication screen,
- Click **Setup**.



Figure 10. Voice Call Authentication Set Up Screen

Steps / Screenshots

- 4.c – Enter your phone number.
- Click **Call**.

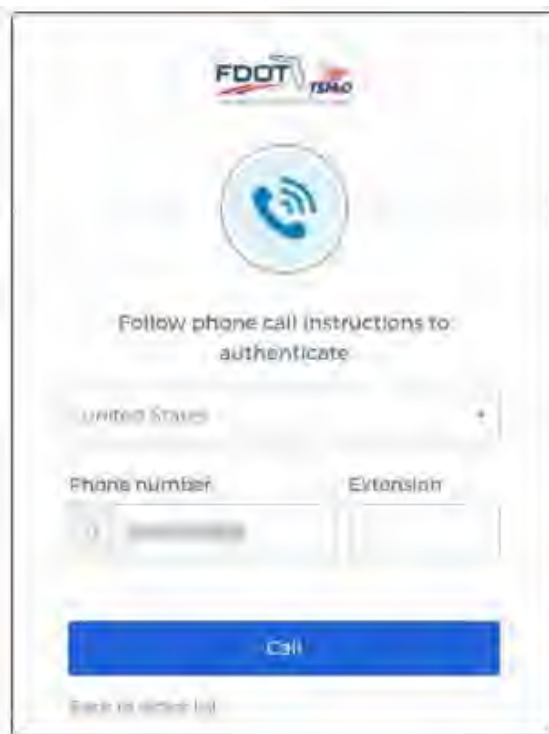


Figure 11. Follow Phone Call Instructions to Authenticate

- 4.d Answer the call from the Okta phone verification system,
- Enter the code provided.
- Click **Verify**.



Figure 12. Voice Call Authentication Code

Enter a secondary email

- 5.a
- Enter a secondary **email**.
 - Select a **forgot password question**.
 - Select a **security image**.

5.b Choose a **forgot password question**.

5.c Enter the **answer** to the forgot password question.

5.d Choose a **security image**.

5.e Click **Create My Account** to complete the additional security options.

The screenshot shows a web form titled "Secondary email" with five numbered steps indicated by red circles and boxes:

- Step 1:** A text input field for "Secondary email" is highlighted with a red box.
- Step 2:** A dropdown menu for "Choose a forgot password question" is highlighted with a red box. The selected question is "What is the food you eat (excluding a child?)".
- Step 3:** A text input field for the "Answer" to the question is highlighted with a red box.
- Step 4:** A grid of 12 security images is highlighted with a red box. The images include various landscapes, buildings, and nature scenes.
- Step 5:** A "Create My Account" button is highlighted with a red box.

Figure 13. Secondary Email, Forgot Password Question, and Security Image



OKTA SELF-SERVICE FOR EXISTING USERS

This SOP Section includes the procedures for existing users to edit their Okta Self-Service account:

- Setting up the multifactor authentication (MFA) factors,
- Entering a secondary email,
- Selecting a forgotten password question, and,
- Selecting a security image.

The Okta Verify application on the user's mobile device is required to set up the Okta Verify, SMS Authentication, and Voice Call Authentication MFA factors.

Sign Into Okta - Account Settings

#	Steps / Screenshots
1.	<p>Note. The UserPrincipalName (UPN) format (i.e., username@domain.com) is required when entering your username in the username field to sign into Okta.</p>
2.	<p>Using the UPN format, enter your SMART SunGuide credentials.</p> <ul style="list-style-type: none"> – Click Sign in.
	
	<p><i>Figure 14. Okta Sign In Page</i></p>
3.	<p>Once signed in,</p> <ul style="list-style-type: none"> – Click the down arrow next to your account name. – Click Settings.
	
	<p><i>Figure 15. Okta Account Settings</i></p>

Steps / Screenshots

- Click **Edit Profile** button in the upper right corner of the screen.



Figure 16. Edit Profile

- If prompted,
 - Enter your password.
 - Click **Verify**. Otherwise → Proceed to the next section.

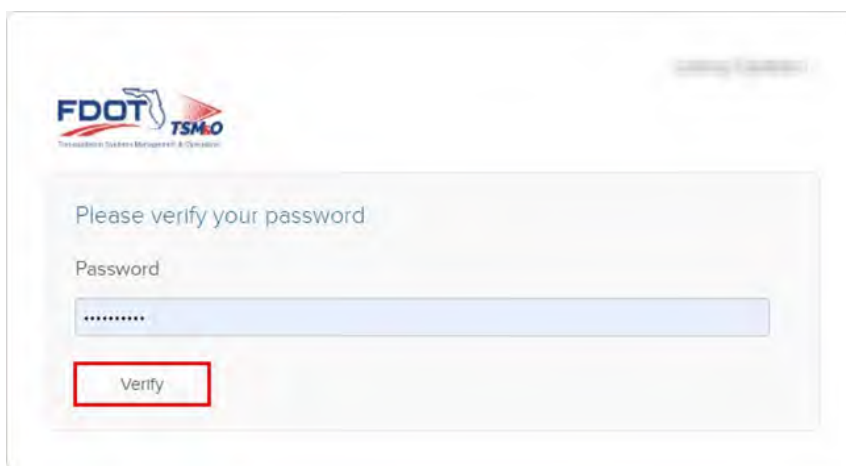


Figure 17. Verify Your Password

Set Up Okta Verify

Steps / Screenshots

- Under **Extra Verification**,
 - Click **Set up** next to **Okta Verify**.

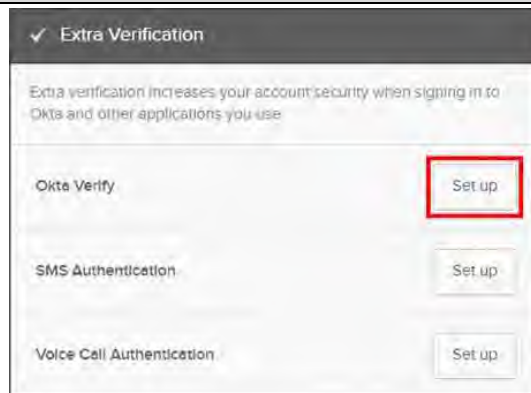


Figure 18. Set Up Okta Verify

Steps / Screenshots

2. If prompted,
 - Enter your password.
 - Click **Verify**. Otherwise → Proceed to step 3.

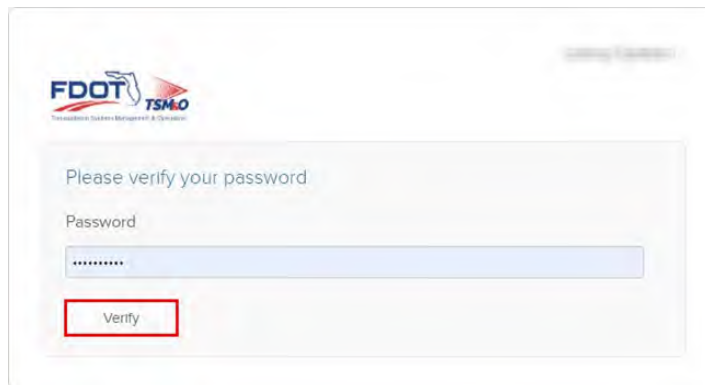


Figure 19. Verify Your Password

3. On the **Set up multifactor authentication** screen,
 - Click **Configure factor**.



Figure 20. Okta Verify Set Up Screen

4. Download the **Okta Verify app** onto your mobile device:
 - a. **iPhone** – Download Okta Verify from the App Store.
 - b. **Android** – Download Okta Verify from the Google Play Store.
5. Once the **Okta Verify** app has been downloaded on your mobile device,
 - Select iPhone or Android for your mobile device type,
 - Click **Next**.

Steps / Screenshots

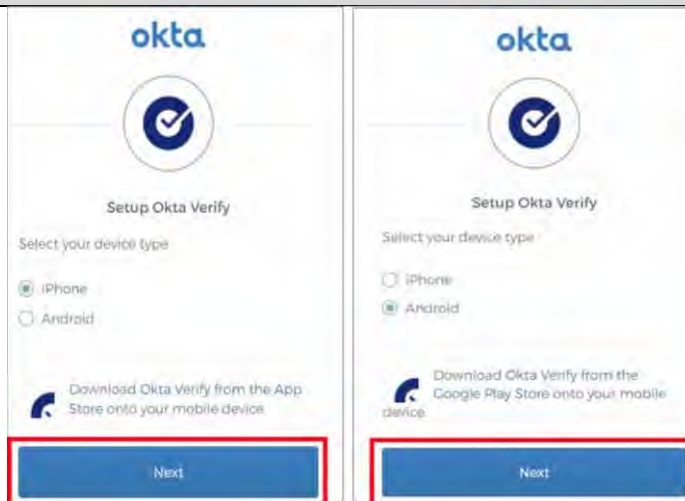


Figure 21. Okta Verify Setup - Mobile Device Type

6. Open the **Okta Verify** app on your phone:
 - a. Click **Add Account**.
 - b. Select **Organization** for account type.
 - c. On the **Do You Have Your QR Code?** screen,
 - Click **Yes, Ready to Scan**.



Figure 22. Yes, Ready to Scan

Steps / Screenshots

7. With your mobile device,
 - Scan the QR code on the Setup Okta Verify screen.



Figure 23. Scan the QR Code

8. At the **Account Added** screen on your mobile device,
 - Click **Done**.

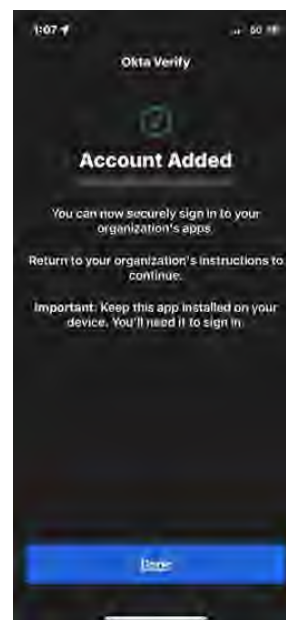


Figure 24. Okta Verify Account Added

Set Up SMS Authentication

Steps / Screenshots

- Under **Extra Verification**,
 - Click **Set up** button next to **SMS Authentication**



Figure 25. Set Up SMS Authentication

- On the **Set up multifactor authentication** screen,
 - Click **Setup**.



Figure 26. SMS Authentication Set Up Screen

- On the **Receive a code via SMS to authenticate** screen,
 - Enter your phone number.
 - Click **Send code**.



Figure 27. Receive a Code via SMS to Authenticate Screen

Steps / Screenshots

4. Enter the **code** from the text message sent to your mobile device.
 - Click **Verify**.



Figure 28. SMS Authentication Code

Set Up Voice Call Authentication

Steps / Screenshots

1. Under **Extra Verification**,
 - Click **Set up** next to *Voice Call Authentication*.

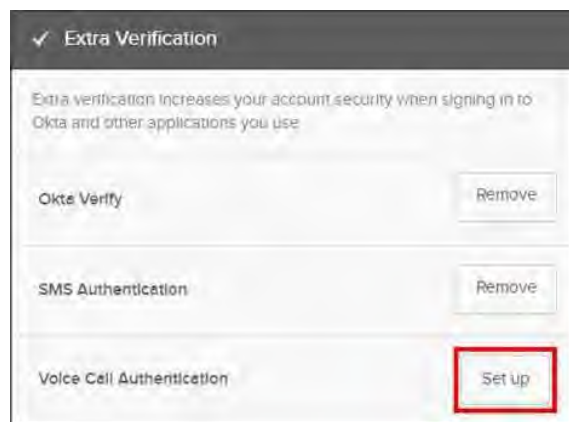


Figure 29. Set Up Voice Call Authentication

2. On the **Set up multifactor authentication** screen,
 - Click **Setup**.



#	Steps / Screenshots
---	---------------------

Figure 30. Voice Call Authentication Set Up Screen

3. Enter your **phone number**.
 - Click **Call**.

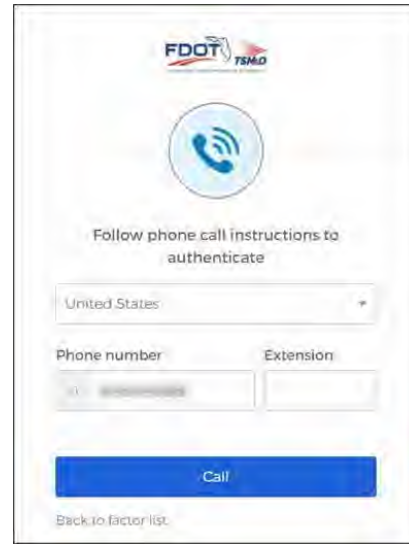


Figure 31. Follow Phone Call Instructions to Authenticate

4. Answer the call from the Okta phone verification system.
 - Enter the code provided.
 - Click **Verify**.

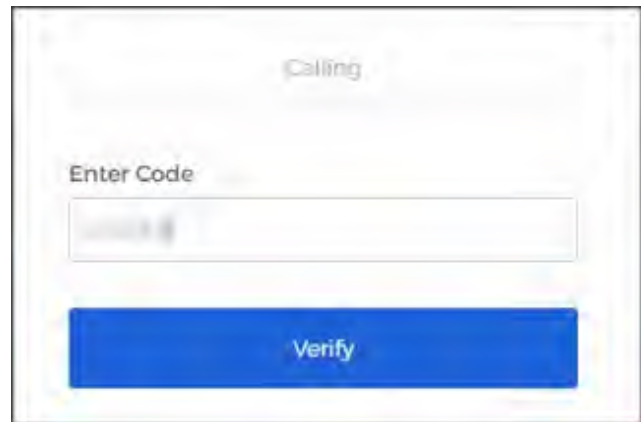


Figure 32. Voice Call Authentication Code

Select a Forgotten Password Question

#	Steps / Screenshots
---	---------------------

1.
 - Click **Edit** next to **Forgotten Password Question**.
 - Then, perform step a. or b. below.

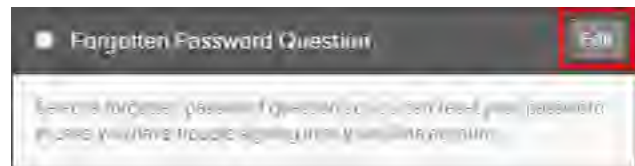


Figure 33. Edit Forgotten Password Question

Steps / Screenshots

- 2.a Select a **stock question**:
1. Click the **down arrow**.
 2. Select a **stock question**.
 3. Enter your **answer**.
 4. Click **Save**.



Figure 34. Forgotten Password Stock Question

- 2.b Select a **custom question**,
1. Click the **down arrow**.
 2. Select **Create your own security question**.
 3. Enter your **custom security question**.
 4. Enter your **answer**.
 5. Click **Save**.



Figure 35. Forgotten Password Custom Question

4. Your saved **forgotten password question** will appear in Okta Self-Service.

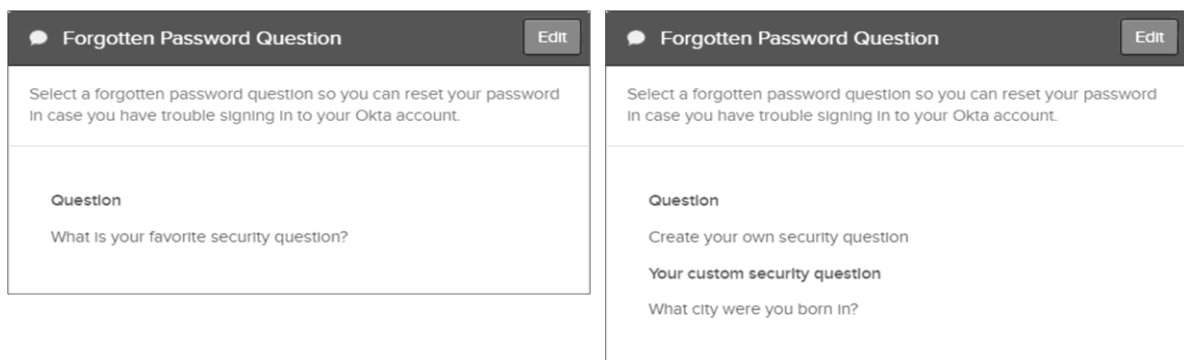


Figure 36. Examples of Saved Forgotten Password Questions

Select a Security Image

Steps / Screenshots

1. Click **Edit** next to **Security Image**.

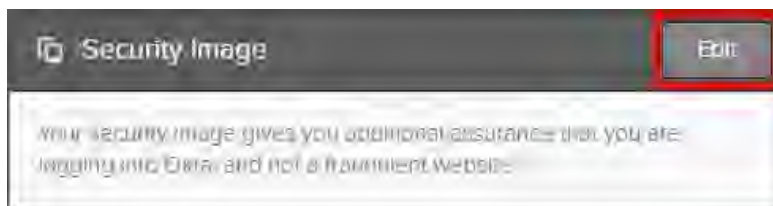


Figure 37. Edit Security Image

2.
 - Select a **security image**.
 - Click **Save**.



Figure 38. Select a Security Image

3. Your saved **security image** will appear in Okta Self-Service.



Figure 39. Example of Saved Security Image

OKTA: RESET YOUR PASSWORD OR UNLOCK YOUR ACCOUNT

Here is the process for resetting your Active Directory (AD) account password or unlocking your AD account with Okta Self-Service. The UserPrincipalName (UPN) format (i.e., username@domain.com) is required when entering your username in the username field to sign to Okta, reset your password, and unlock your account.

Reset Your Password

Steps / Screenshots

1. Click the following link to access the Okta website: <https://smartsunguide.okta.com>.
2. Click **Need help signing in?**

The screenshot shows the Okta sign-in interface for FDOT TSM.O. At the top, there is a logo for FDOT TSM.O. Below the logo is a circular image of a road leading to a horizon. Underneath the image is the text 'Sign In'. There are two input fields: 'Username' and 'Password'. Below the password field is a 'Remember me' checkbox. A large blue 'Sign In' button is positioned below the checkbox. At the bottom of the page, there are three links: 'Need help signing in?', 'Forgot password?', and 'Unlock account?'. The 'Need help signing in?' and 'Forgot password?' links are highlighted with red boxes and numbered 1 and 2 respectively.

Figure 40. Forgot Password?

3. Enter your **username** for the **smartsunguide.com** or **field.net** domains.

- a. **Smartsunguide.com** domain.
- Using the UPN format (i.e., username@domain.com), enter your username.
 - Click **Reset via SMS** or **Reset via Email**.

Figure 41. Reset Password for the Smartsunguide.com Domain

- b. **Field.net** domain.
- Using the UPN format (i.e., username@domain.com),
- Enter your **username**.
 - Click **Reset via SMS** or **Reset via Email**.

Figure 42. Reset Password for the Field.net Domain

4. Follow the instructions provided to change your password.

Unlock Your Account

Steps / Screenshots

1. Click the following link to access the Okta website: <https://smartsunguide.okta.com>.

2. Click **Need help signing in?**
Click **Unlock account?**

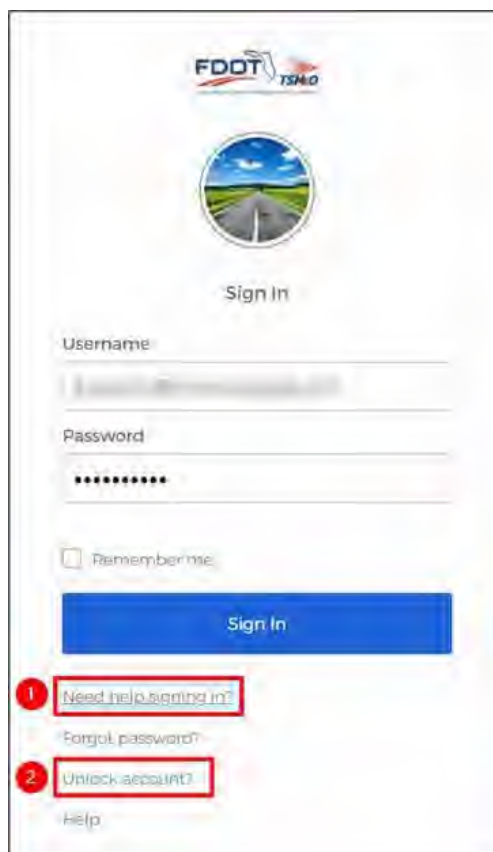


Figure 43. Unlock Account?

3. Enter your **username** for the **smartsunguide.com** or **field.net** domains.

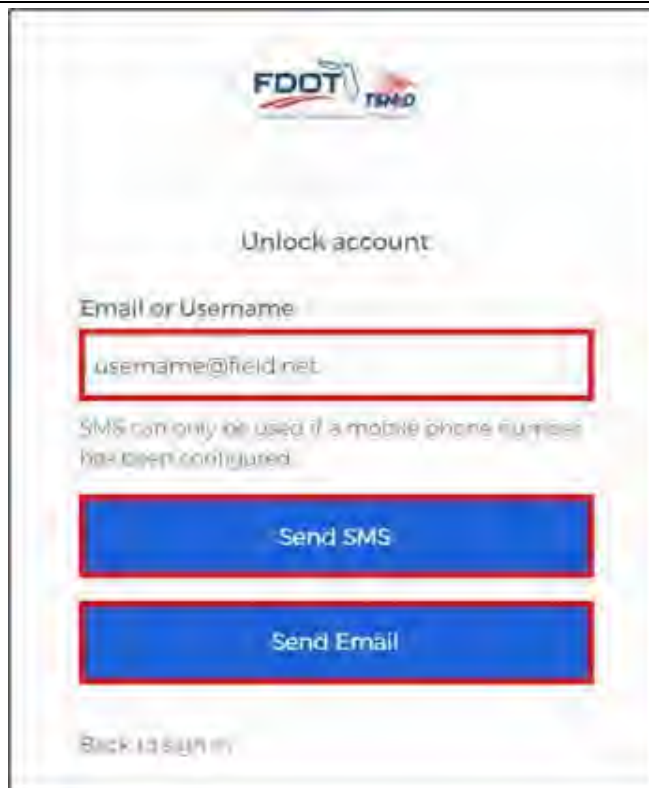
- a. **Smartsunguide.com** domain.

- Using the UPN format (i.e., username@domain.com), enter your **username**.
- Click **Send SMS** or **Send Email**.



Figure 44. Unlock Account for the Smartsunguide.com Domain

- b. Using the UPN format (i.e., username@domain.com),
- Enter your **username**.
 - Click **Send SMS**
- or
- **Send Email**.



FDOT TSMO

Unlock account

Email or Username

username@field.net

SMS can only be used if a mobile phone number has been configured.

Send SMS

Send Email

Back to sign in

Figure 45. Unlock Account for the Field.net Domain

VPN CONNECTION

The RTMC uses Cisco AnyConnect VPN software and Cisco ASA firewalls to permit access into the network. This SOP Section outlines the steps for users to connect to the D4 Network via VPN.

Request VPN Access

#	Steps / Screenshots
1.	To request VPN access, a helpdesk ticket needs to be created for new users or existing users and approved by the IT Support Manager.
1.a	The new user's Supervisor must submit the New-Hire Request to the RTMC Office Manager (currently, Erika Zen).
1.b	The existing user's Supervisor must submit the Access Change Request to the RTMC Office Manager.
2.	The IT department must add the user to the "Remote_User" AD security group to be permitted to use VPN.

Okta Self-Service

1. New users must register their Okta Self-Service account in accordance with SOP Section [7.03.05.01 Okta Self-Service for New Users](#).
2. Existing users must ensure that the MFA factors are set up in accordance with SOP Section [7.03.05.02 Okta Self-Service for Existing Users](#)

Install And Open the Cisco ANYCONNECT Client

Step #	Process / Screenshots
1.	The new or existing user must install the Cisco AnyConnect client on their PC by accessing the URL provided by the IT department.
2.	<p>Click Cisco AnyConnect icon located in your taskbar.</p> <p>Note. If the Cisco AnyConnect icon does not appear on your taskbar, perform step a. or b. below.</p> <p>Otherwise, proceed to step 3.</p>
2.a	<ul style="list-style-type: none"> – Click up/down arrow to scroll up/down on the taskbar. – Click Cisco AnyConnect icon.



Figure 46. Cisco AnyConnect Icon



Figure 47. Scroll Up/Down to Find the Cisco AnyConnect Icon

Step #	Process / Screenshots
--------	-----------------------

- | | |
|-----|--|
| 2.b | <ul style="list-style-type: none"> – Click up arrow to show hidden icons. – Click the Cisco AnyConnect icon. |
|-----|--|

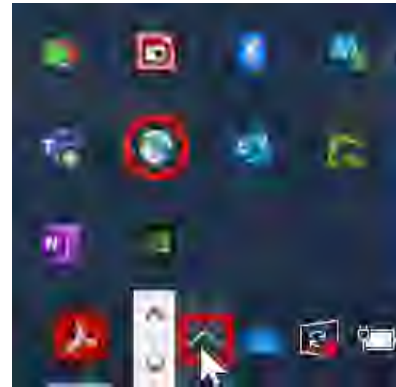


Figure 48. Hidden Icons to Find the Cisco AnyConnect Icon

- | | |
|----|--|
| 3. | <ul style="list-style-type: none"> – Enter the VPN tunnel information that you were provided by the IT department. – Click on Connect. |
|----|--|

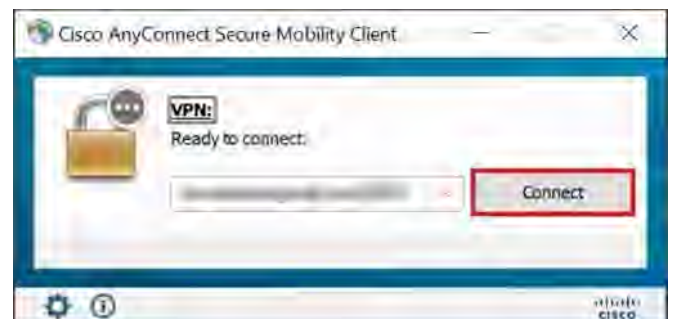


Figure 49. Cisco AnyConnect

- | | |
|----|--|
| 4. | Enter your username and password . |
|----|--|



Figure 50. Sign Into Cisco AnyConnect

- | | |
|-----|--|
| 4.a | Username: First initial followed by last name (e.g., jdoe). |
| 4.b | Password: Same password that you currently use to log in to your Windows account. |
| 5. | Click OK . |

Step # Process / Screenshots

Note. Users not previously set up one or more of the MFA factors will be prompted to select a factor to enroll in.

If necessary,

Perform the procedures in the **ENROLL MFA FACTORS TO LOG IN TO CISCO ANYCONNECT** section below.

Otherwise,

- skip the **ENROLL MFA FACTORS TO LOG IN TO CISCO ANYCONNECT** section below and
- proceed to the **LOG IN TO CISCO ANYCONNECT WITH MFA FACTORS ENROLLED** section.

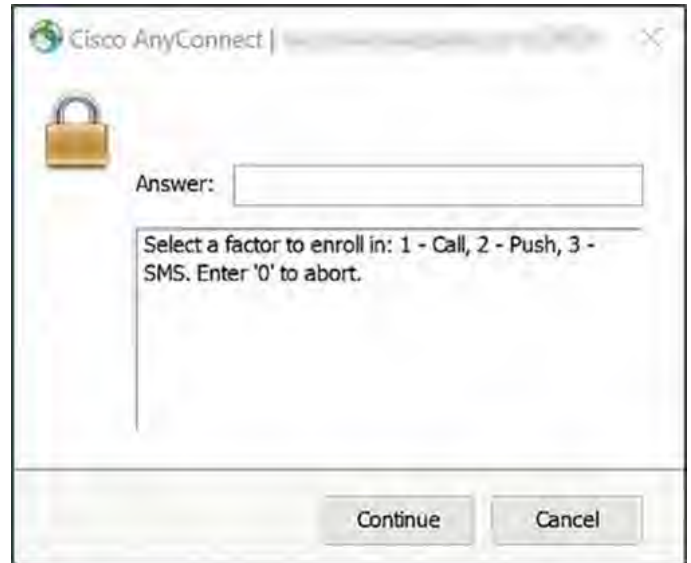


Figure 51. Select a Factor to Enroll In

Enroll MFA Factors to log in to CISCO ANYCONNECT

Process / Screenshots

1. Enroll in 1 – Call

- 1.a
- Enter.
 - Click **Continue**.

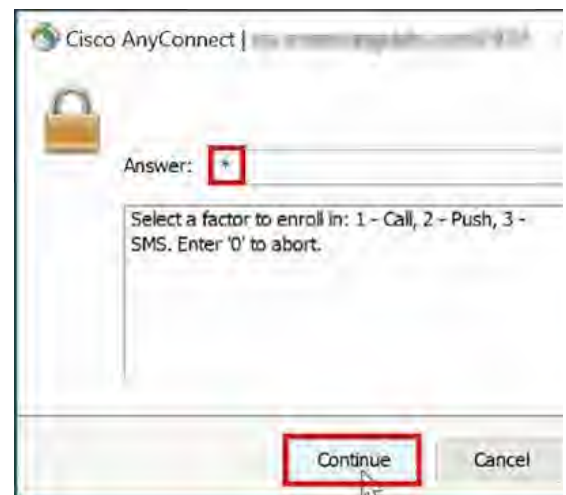


Figure 52. Enroll in 1 - Call

#	Process / Screenshots
---	-----------------------

- | | |
|-----|---|
| 1.b | <ul style="list-style-type: none"> – Enter your phone number and, – Click Continue. |
|-----|---|

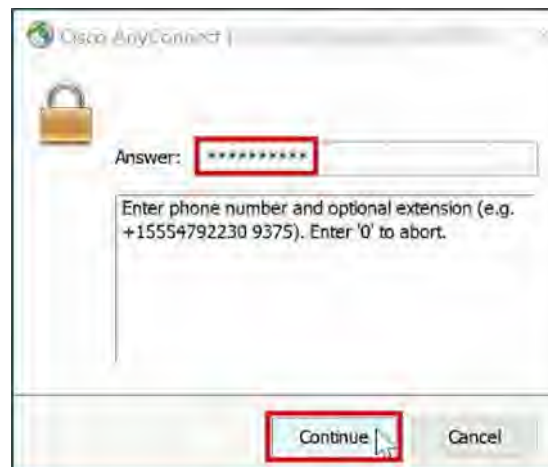


Figure 53. Enter Your Phone Number

- | | |
|-----|--|
| 1.c | <ul style="list-style-type: none"> – Answer the call from the Okta phone verification system, – Enter verification code provided, – Click Continue. |
|-----|--|



Figure 54. Enter the Verification Code

- | | |
|-----|---|
| 1.d | <ul style="list-style-type: none"> – Enter 0 – Click Continue to enroll in another authentication factor. |
|-----|---|



Figure 55. Call Enrollment Successful

#	Process / Screenshots
---	-----------------------

2.	Enroll in 2 - Push
----	--------------------

- | | |
|-----|---|
| 2.a | <ul style="list-style-type: none"> - Enter 1. - Click Continue. |
|-----|---|

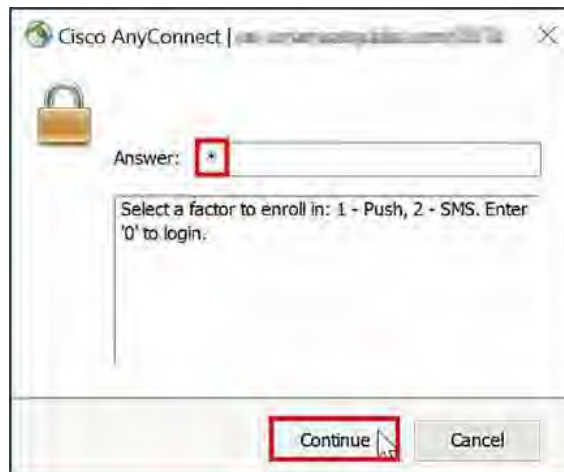


Figure 56. Enroll in 2 - Push

- | | |
|-----|---|
| 2.b | <ul style="list-style-type: none"> - Enter your mobile device number. - Click Continue. |
|-----|---|



Figure 57. Enter Your Mobile Device Number

- | | |
|-----|---|
| 2.c | <p>When you arrive at the screen,</p> <p>Follow the instructions sent to your mobile device via text message.</p> |
|-----|---|



Figure 58. Instructions sent to your mobile device via text message

Process / Screenshots

1. On your mobile device,
 - Click the *link* provided.

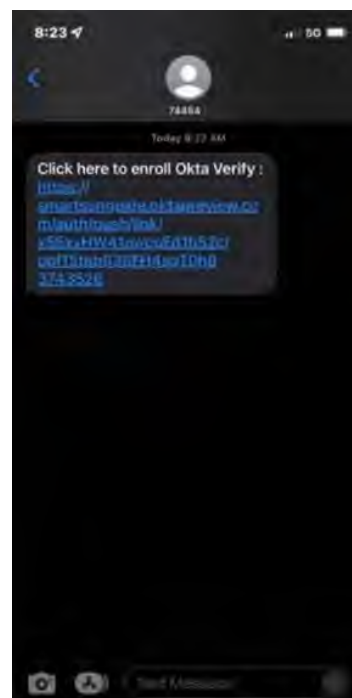


Figure 59. Enroll Okta Verify

2. On your mobile device,
 - Click **Get Started**.

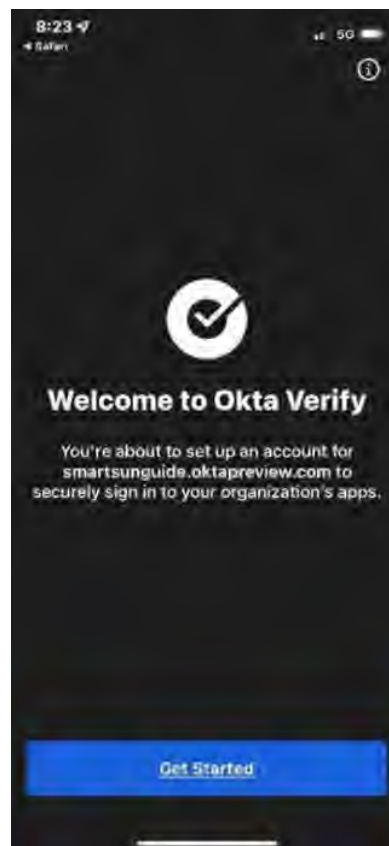


Figure 60. Welcome to Okta Verify

Process / Screenshots

3. On your mobile device → Click **Done**.

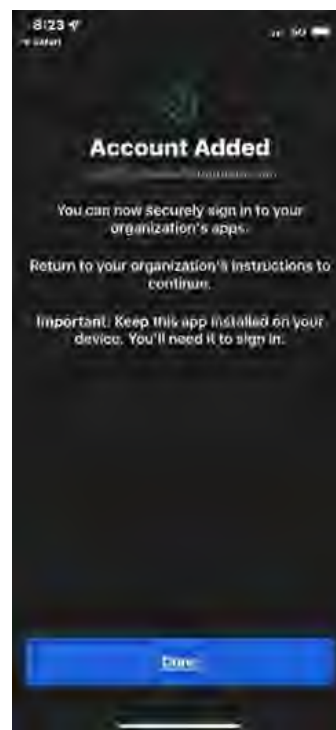


Figure 61. Account Added

4. Enter **0**.

- Click **Continue** to enroll in another authentication factor.



Figure 62. Push Enrollment Successful

#	Process / Screenshots
---	-----------------------

3.	Enroll in 3 - SMS
----	-------------------

- | | |
|-----|--|
| 3.a | <ul style="list-style-type: none"> – Enter 1 in the <i>Answer</i> box. – Click Continue. |
|-----|--|



Figure 63. Enroll in 3 - SMS

- | | |
|-----|---|
| 3.b | <ul style="list-style-type: none"> – Enter your mobile device number. – Click Continue. |
|-----|---|



Figure 64. Enter Your Mobile Device Number

- | | |
|-----|--|
| 3.c | <ul style="list-style-type: none"> – Enter the verification code from the text message sent to your mobile device. – Click Continue. |
|-----|--|



Figure 65. Enter the Verification Code

#	Process / Screenshots
---	-----------------------

- | | |
|-----|---|
| 3.d | <ul style="list-style-type: none"> – Enter 0 – Click Continue to log in. |
|-----|---|

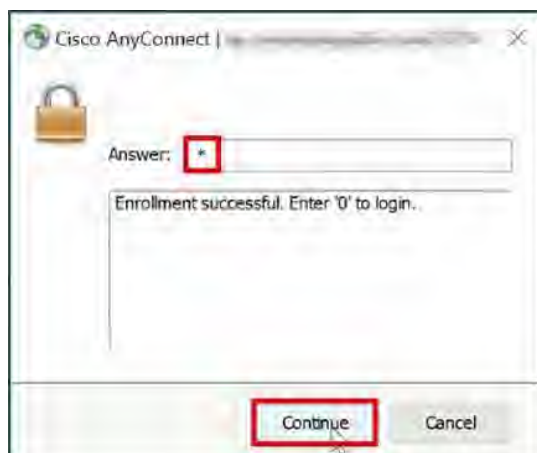


Figure 66. SMS Enrollment Successful

- | | |
|----|--|
| 4. | <ul style="list-style-type: none"> – In the acknowledgement and consent screen – Click Accept. |
|----|--|

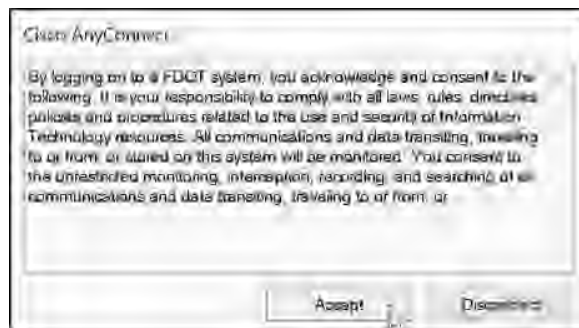


Figure 67. Cisco AnyConnect Acknowledgement and Consent Screen

Log In to CISCO ANYCONNECT with MFA Factors Enrolled

#	Steps / Screenshots
---	---------------------

- | | |
|----|---|
| 1. | <p>Select an authentication factor from the options provided.</p> <ul style="list-style-type: none"> a. Enter 1 to receive a phone call from the Okta phone verification system. b. Enter 2 to receive a push notification via the Okta Verify app. c. Enter 3 to receive a code via SMS. |
|----|---|

Steps / Screenshots

2. Click **Continue**.



Figure 68. Select an Authentication Factor

3. Perform step a., b., or c. below, based on your **authentication factor** selection above:

3.a 1 – Call

1. Answer the call from the Okta phone verification system.
2. Enter the **code** provided.
3. Click **Continue**.



Figure 69. Voice Call Authentication

3.b 2 – Push

1. On your mobile device, open the **push notification** from the Okta Verify app.

Steps / Screenshots

2. Click **Yes, it's me.**

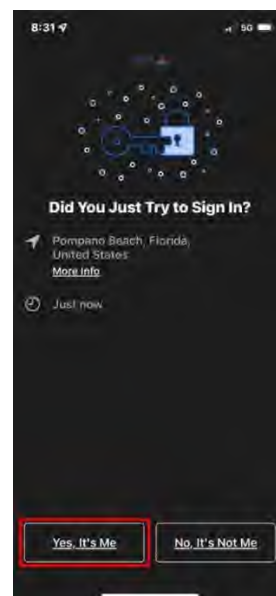


Figure 70. Okta Verify - Mobile Device Push Notification

3.c 3 – SMS

1. Enter the **code** from the text message that was sent to your mobile device.

2. Click **Continue.**



Figure 71. SMS Authentication

4. In the acknowledgement and consent screen,

- Click **Accept.**

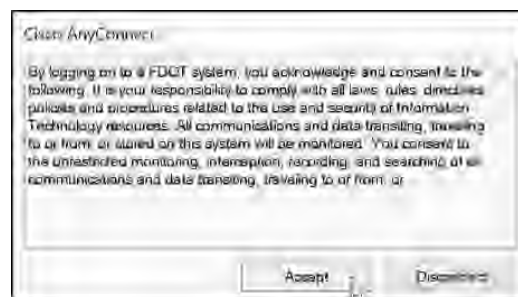


Figure 72. Cisco AnyConnect Acknowledgement and Consent Screen



7.04 Network Security

Table of Contents

Version #	Date	Author	Changes
1.0	12/19/2023	Yana Neishlos	Initial Draft

Table of Contents

SECURITY MEASURES	5
Important Factors.....	5
Personal Electronic Devices on the Network / Internet Use	6
Prohibited Use of Personal Electronic Devices.....	6
Computer Viruses	6
SYSTEM CONSIDERATIONS	7
WEB FILTERING.....	8
RTMC	8
VPN	8
INFORMATION SYSTEM MONITORING	9
Scope	9
Facilities and Data Centers	9
Monitoring Controls.....	9
Confidentiality-Integrity-Availability (CIA) Triad of Information Security.....	9
Policies	10
Network.....	10
Operating Systems.....	10
Applications	11
Procedures	11
VULNERABILITY PROJECT MANAGEMENT	12
Security Team	12
Stakeholders.....	13
Vulnerability Project Manager.....	14
SECURITY	15
Domain Administrator Account	15
Personal Electronic Devices on the Network / Internet Use	15
WEB FILTERING / VPN	15
INFORMATION SYSTEM MONITORING	16
Overview.....	16
Scope	16
Facilities and Data Centers	16
Monitoring Controls.....	16
Confidentiality-Integrity-Availability (CIA) Triad of Information Security.....	16
Policies	17
Network.....	17
Operating Systems.....	17
Applications	17
Procedures	17
VULNERABILITY PROJECT MANAGEMENT	19
Overview.....	19

Procedures19

 Security Team19

 Stakeholders.....20

 Vulnerability Project Manager.....21

TENABLE REMEDIATION SCAN GUIDE22

 Overview.....22

 Start a Remediation Scan23

 Start the Process.....23

 Create, Save, Launch a Scan.....24

 Complete a Remediation Scan.....28

SECURITY MEASURES

There are various security measures in place including:

- Password Manager Database / SolarWinds Orion Monitor / Trend Micro Apex One
- Trend Micro Deep Security / Cisco UTM / Umbrella DNS Web Filter.

Important Factors

The following factors are significant.

Security Considerations	Details
Windows Update	Security patches and windows updates: applied automatically at each workstation and server by the Patch Management Team. There is no set schedule determined. Patches and updates are applied to small control environment first. Then – to the greater PC population after no ill affect takes place. Updates are downloaded from Windows Software Update Services Repositories.
Domain Administrator Account	The domain administrator account is granted to three users. Individuals who need the permissions equivalent to a domain administrator will be granted; these permissions are essential for that person's job duties and, approved at the discretion of the IT Support Manager.
Local Accounts	Workstations are configured with the built-in administration account disabled, and a custom administration user configured on each workstation. Multiple groups are added via GPO to grant users the administration access. These rights are documented in active directory.
Windows Domain Controllers – Domain Controller (DC) Servers	<ul style="list-style-type: none"> • Smartsunguide.com servers RODC's for its internet facing proxy servers. DCs are formatted as per naming standards within SharePoint. • Field.net holds identical number of DC's as smartsunguide.com with exception of 2 RODC's.
Backup And File Restoral	Backups are using Unitrends Enterprise Backup software.
Legal Banner	<p>These are the banner that users see when log-on is applied through group policy. The popup, FDOT Computer Usage Policy displays the following message, and a clickable button for the user to acknowledge the policy:</p> <p><i>By logging on to a FDOT computer, you acknowledge your responsibility to comply with all laws, rules, directives, policies, and procedures related to the use and security of information technology resources.</i></p> <p><i>Unauthorized use is strictly prohibited. You are hereby on notice that you should have no expectation of privacy as to your use of Department information technology resources as all data is potentially subject to Florida's public records law.</i></p>

Personal Electronic Devices on the Network / Internet Use

No personal electronic devices are permitted to be plugged into or otherwise connected to the RTMC ITS network. The RTMC does not allow operators in the control room any personal use of the Internet, and other users may only use the Internet for their job needs and a very limited personal use.

Prohibited Use of Personal Electronic Devices

To keep the TMC Intelligent Transportation Systems network free of viruses, adware, spyware, or malware, no employee is allowed to connect any personal electronic device to TMC owned PCs or laptops.

1	Do not plug any electronic device into a USB drive on any desktop or laptop –	Cell phones and other devices with internal and memory cards may contain dormant viruses that can enter and damage the ITS network. To charge a cell phone or other device, use a wall outlet. Using a USB connection to charge a personal electronic device is not permitted.
2.	Do not →	Copy any music, photograph, or video files to any TMC desktop, laptop, or network location unless directly applicable for work usage.
3.	Only the use of company-provided USB drives is allowed for TMC PCs or laptops.	Do not use company-provided USB drives in non-company provided PCs or laptops. One should not take your USB drive to your home computer (where there could be a virus) and then bring it back to the TMC.

Examples of personal electronic devices that may not be plugged into a TMC USB drive:

- iPods and other audio or video players.
- Cell phones with USB connections.
- Digital cameras.
- Thumb drives, or other portable memory sticks or hard drives.
- Any other removable memory storage.

Computer Viruses

- Do not send or receive personal e-mail through the Smart SunGuide e-mail.
- Use the computer in the break room for personal use of the Internet.
- Never plug a personal electronic device into a TMC desktop or laptop.

SYSTEM CONSIDERATIONS

System Uptime	The most critical system is SunGuide, and its uptime is the best effort at 99.9%. System monitoring is done by SolarWinds Orion, which sends immediate notices if downtime is detected.
Assigning IP Addresses	<p>IP addresses for network devices are documented in a spreadsheet kept in the IP Address Management Database. It an important database containing the IP addresses of all devices and machines on the ITS system. It contains current IP addresses, and addresses assigned to contractors working on new projects. It is a confidential database; should only be viewed by the IT network manager and network administrators.</p> <p>For contracts, opened for bidding, FDOT may assign a contractor IP addresses to be provided. When a project is under way, the contractor will request FDOT to provide specific IP addresses.</p> <p>Warning. IP addresses assignments (especially to contractors) must be documented immediately. This task is mandated (cannot be delegated) by the TMC IT Support Manager or IT Network Manager.</p>
Installing Or Updating Software	Windows updates with the WSUS server, and antivirus definitions to an already existing antivirus installation. VMWare uses Update Manager. All other updates are installed manually or through central management consoles depending on the software.
Intra-SMART	<p>Intra-SMART is the internal website. Any updates to the website are made by an IT department. The request for updates will be made by the operations management department through the helpdesk ticket system on an as needed basis.</p> <p>Requests made by anyone other than operations management should be sent to and approved by the operations management department.</p>
SMART SUNGUIDE.COM	<p>SMARTSunGuide.com is the public website. Updates are made by the SunGuide Administrator. Updates' requests are done by the marketing department monthly via email.</p> <p>Requests made by anyone other than the marketing department should be first sent to the marketing department.</p>
Antivirus Software	The RTMC uses Trend Micro Apex One as the endpoint protection solution for workstations and Trend Micro Deep Security as the enterprise protection solution for servers within the District 4 ITS network.
Network Monitoring Server	Reserved for future use.

WEB FILTERING

RTMC

RTMC has a highly secure web filtering solution. It utilizes a cluster of proxy servers to maintain web filtering within the RTMC network, along with secure DNS transactions to protect against DNS poisoning using hardened DNS forwarders.

The Cisco ASA firewall used for the control point of all Internet traffic prevents private DNS requests from being utilized.

DHCP polices route traffic for guest and contractor accounts through specific network locations to ensure all devices within the RTMC are controlled.

VPN

The RTMC uses Cisco AnyConnect VPN software and Cisco ASA firewalls to permit access into the network.

To request access, a helpdesk ticket needs to be created and approved by the IT Support Manager.

The user must be added to "Remote_User" AD security group for the use of VPN.

The user must have the VPN Anyconnect client installed on the machine and the link to connect will be given by the IT department.

INFORMATION SYSTEM MONITORING

This SOP Section provides the Florida Department of Transportation (FDOT) District Four (D4) Intelligent Transportation Systems (ITS) Information System Monitoring policies, information on Security Definitions Updates for monitoring applications, and the procedures for alerts received from the Cybersecurity & Infrastructure Security Agency (CISA) and the FDOT Office of Information Security Management (ISM) for a priority 1 notification of a security issue.

The FDOT D4 ITS environment incorporates different platforms and tools to monitor the network infrastructure. Assets are monitored at discrete intervals to identify potential cybersecurity events.

Scope

All information systems and assets are monitored to identify potential cybersecurity events on the District 4 ITS network.

Facilities and Data Centers

- Broward Regional Transportation Management Center (RTMC)
- Palm Beach Satellite Transportation Management Center (STMC)
- Treasure Coast STMC

Data Centers have restricted physical access. Door access control systems are installed at each facility. Device cabinets and buildings are controlled by CyberLock key-centric access control system.

Monitoring Controls

- SolarWinds Network Performance Monitor
- SolarWinds Event Manager
- Cisco Identity Services Engine
- Trend Micro Workload Security & ApexOne-as-a-Service
- Okta Adaptive Multifactor Authentication
- Okta Lifecycle Management
- Tenable IO
- CyberAudit-Web Enterprise
- Cisco Adaptive Security Appliance with FirePower
- Cisco Umbrella
- Milestone XProtect Video Monitoring System

Confidentiality-Integrity-Availability (CIA) Triad of Information Security

The CIA triad represents these three key principles of information security below. Source: Rule 74-2.001, Florida Administrative Code (F.A.C.).

- | | |
|------------------------|---|
| Confidentiality | <ul style="list-style-type: none"> • Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. |
|------------------------|---|

- Integrity**
- The principle that assures information remains intact, correct, authentic, accurate and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information.
- Availability**
- Ensuring timely and reliable access to and use of information.



Figure 1. CIA Triad of Information Security

Policies

Network

1.	The SolarWinds Network Performance Monitor	It assesses the availability of network devices and components. Resources are manually configured with required information for each node to be monitored. Alert policies are set in place to notify all stakeholders of performance degradation.
2.	The SolarWinds Event Manager	It aggregates logs from various devices and platforms. Rule sets are configured for a continuous analysis and detection of anomalies across the network infrastructure. Changes to rules are manually performed based on recommendations received from the US Department of Homeland Security, Florida Department of Law Enforcement Office of Statewide Intelligence, and the CISA.
3.	The Cisco Identity Services Engine	It facilitates identity and access control for network devices. Enterprise policies are enabled to enforced compliance and streamline service operations. Compliance policies are manually updated based on Microsoft Security update releases and recommendations received from the CISA.

Operating Systems

1.	The SolarWinds Network Performance Monitor	It detects performance issues and performs multiple validations against servers and workstations. Resources are manually configured with the required information for each node to be monitored. Alert policies are set in place to notify all stakeholders if a performance degradation occurs.
2.	Trend Micro Workload Security and ApexOne-as-a-Service	It monitors, maintains the security posture of endpoint devices, including threat defense, machine behavioral analysis, vulnerability intelligence. Threat pattern and intrusion prevention rules are automatically updated on connected agents directly from Trend Micromanagement engine. It is configured to perform real-time and scheduled scans, malicious codes and unauthorized mobile codes that are blocked, quarantined, or removed upon detection.

- 3. Tenable IO It scans the entire infrastructure and identifies security risks at scheduled intervals. Identified vulnerabilities are remediated in accordance with the FDOT D4 Vulnerability Management Plan.

Applications

- 1. Application Control policies Set, monitored using Trend Micro Workload Security and ApexOne-as-a-Service. Trend Micro manages and automatically updates security definition libraries. Security definitions are scheduled to automatically download; applied immediately to agents. Anti-malware and anti-spyware signatures are automatically updated and stored in the Trend Micro cloud libraries. They are configured to perform real-time and scheduled scans, malicious codes and unauthorized mobile codes that are blocked, quarantined, or removed upon detection.

- 2. Web applications Scanned at discrete intervals by Tenable IO to identify security risks. Identified vulnerabilities are remediated by the application developer, per the FDOT D4 Vulnerability Management Plan guidelines.

Procedures

- 1. Alerts concerning confirmed malicious cyber activity and exploits shared from the FDOT ISM and the CISA are reviewed by the ITS Information Security Team.
- 2. Once reviewed, all necessary stakeholders are notified and are provided with the recommended actions to minimize security risk.
- 3. Remediations are performed according to the given risk of impact and likelihood of occurrence.
 - a. Critical
 - (1) Vendor provided updates that clearly remediates cybersecurity vulnerabilities are tested within 7 days of release, and then applied.
 - (2) Monitoring and detection controls that require manual configuration are updated immediately after notification.
 - b. High
 - (1) Vendor provided updates that clearly remediates cybersecurity vulnerabilities are tested within 14 days of release, and then applied.
 - (2) Monitoring and detection controls that require manual configuration are updated immediately after notification.



Figure 2. Cybersecurity Risk Matrix

VULNERABILITY PROJECT MANAGEMENT

A vulnerability that requires actions from multiple stakeholders to resolve it, becomes a vulnerability project, which should be tracked for remediation by the Vulnerability Project Manager through coordination with stakeholders. The procedures for resolving vulnerability projects are provided below.

Security Team

1. The Security Team identifies vulnerabilities in the environment within Tenable.IO and performs research to determine what it takes to fix them.
2. If an identified vulnerability requires actions from multiple stakeholders to remediate it, the Security Team creates a SolarWinds Service Desk Security Vulnerability incident and assigns it to the Vulnerability Project Manager.

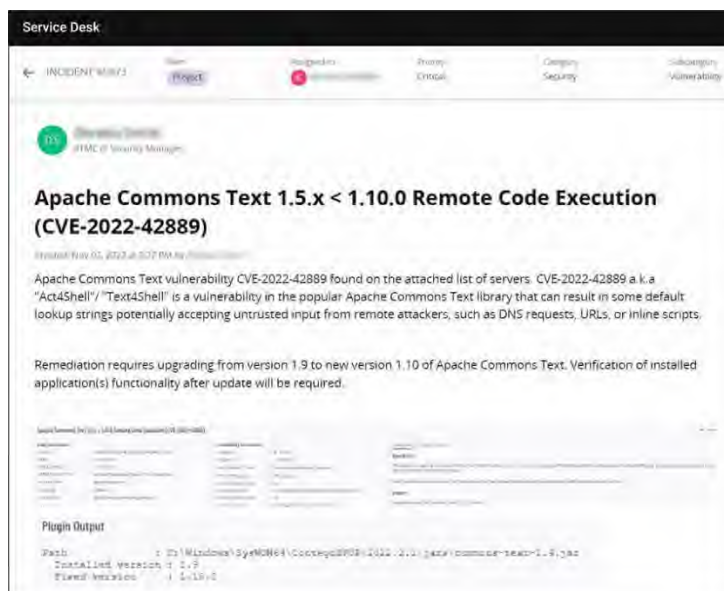


Figure 3. A SolarWinds Service Desk Security Vulnerability Incident

3. The SolarWinds Service Desk Security Vulnerability incident includes the following information:
 - a. Description of the vulnerability.
 - b. Solution for the vulnerability.
 - c. List of machines affected by the vulnerability.
 - d. Any other supporting information.

Stakeholders

1. Each stakeholder creates a change order or incident, as applicable, within the SolarWinds Service Desk and attaches the Security Vulnerability incident in the related tab.

Service Desk

← CHANGE #152 State: **Approved** Assigned to: MH Priority: Medium

MH
IT Desktop Analyst 1

Commons-Text Shell Remediation - Servers

Created: Nov 03, 2022 at 11:33 AM by Michelle Hazen

In an effort to secure our environment, security application servers with CVE-2022-42889 shall be patched with a version 1.10.0 of Commons Jar.

https://commons.apache.org/proper/commons-text/download_text.cgi

<https://community.tenable.com/feed/ID53a00008pSKXG7?fromEmail=1&s1oid=000300000000pZp&s1nid=0DBfZ000000TNC&s1uid=0053a00000kk2Oo&s1ext=08&kind=c&headerGroupDigest&emtm=1666499820056>

Machines to be worked on:

View more

Change Plan

- 1) Create snapshot of servers
- 2) Stop processes using java on server

View more

Rollback Plan

In case of issues with functionality, revert to taken snapshot.

Test Plan

Log in to servers and verify functionality of all applications.

COMMENTS DETAILS PROCESS (1) **RELATED (1)** TASKS (0) AUDIT

Related Items

1 item

INCIDENTS (1)

Apache Commons Text 1.5.x < 1.10.0 Remote Code Execution (CVE-2022-42889)
5875 - Resolved - Critical - Security - Vulnerability - Nov 14, 2022

Figure 4. Change Order Related to the Vulnerability Project Incident

2. Change order(s)/incident(s) include the following information, as applicable:
 - a. Requester's name or email address.
 - b. Descriptive title.
 - c. Justification for the need of the change order.
 - d. Tags and/or attachments.
 - e. Change plan.
 - f. Rollback plan.
 - g. Test plan.
 - h. Details.
 - i. Related items.

Vulnerability Project Manager

1. The Vulnerability Project Manager coordinates with all stakeholders responsible for applying the necessary solution for remediation to the machines affected by the vulnerability and tracks the project progress from the time it is created until it is resolved.
2. Upon verification of the vulnerability been remediated on all affected machines, the Vulnerability Project Manager changes the SolarWinds Service Desk Security Vulnerability incident from Project to Resolved, as shown.

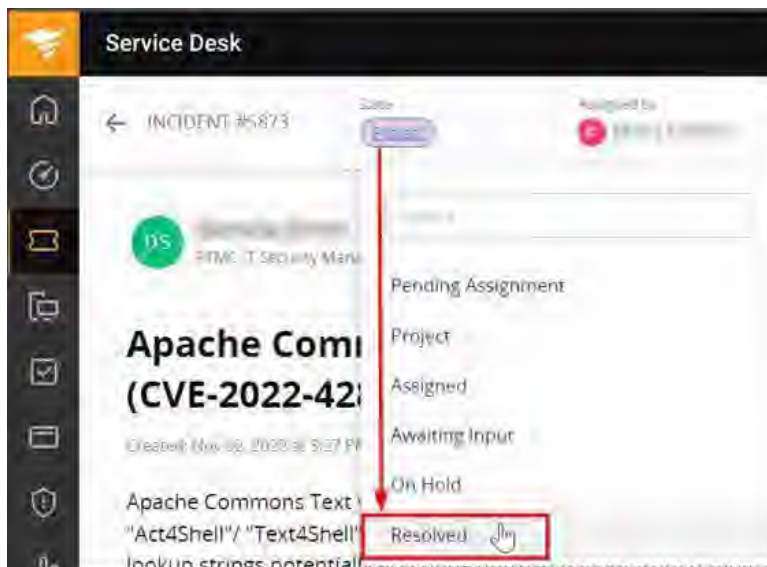


Figure 5. Vulnerability Project Resolved

SECURITY

Domain Administrator Account

A domain administrator account access is granted to three users. Individuals requiring permissions equivalent to a domain administrator will be granted it provided permissions are necessary to execute that person's job duties and, at the discretion of the IT Support Manager.

Personal Electronic Devices on the Network / Internet Use

No personal electronic devices are permitted to be plugged into or otherwise connected to the RTMC ITS network. The RTMC does not allow operators in the control room any personal use of the Internet, and other users may only use the Internet for their job needs and a very limited personal use.

Web Filtering / VPN

RTMC has a highly secure web filtering solution. It utilizes a cluster of proxy servers to maintain web filtering within the RTMC network, along with secure DNS transactions to protect against DNS poisoning using hardened DNS forwarders.

The Cisco ASA firewall used for the control point of all Internet traffic prevents private DNS requests from being utilized. DHCP polices route traffic for guest and contractor accounts through specific network locations to ensure all devices within the RTMC are controlled.

The RTMC uses Cisco AnyConnect VPN software and Cisco ASA firewalls to permit access into the network.

To request access, a helpdesk ticket needs to be created and approved by the IT Support Manager. The user must be added to "Remote_User" AD security group to be permitted to use VPN.

The user must have the VPN Anyconnect client installed on the machine and the link to connect will be given by the IT department.

INFORMATION SYSTEM MONITORING

Overview

This SOP Section provides the Florida Department of Transportation (FDOT) District Four (D4) Intelligent Transportation Systems (ITS) Information System Monitoring policies, information on how the security definitions for the monitoring applications are updated, and the procedures for alerts received from the Cybersecurity & Infrastructure Security Agency (CISA) and the FDOT Office of Information Security Management (ISM) for a priority 1 notification of a security issue.

The FDOT D4 ITS environment incorporates different platforms and tools to and monitor the network infrastructure. Assets are monitored at discrete intervals to identify potential cybersecurity events.

Scope

Information systems, assets are identified for potential cybersecurity events on the District 4 ITS network.

Facilities and Data Centers

- Broward Regional Transportation Management Center (RTMC)
- Palm Beach Satellite Transportation Management Center (STMC) / Treasure Coast STMC

Data Centers have restricted physical access. Door access control systems are installed at each facility. Device cabinets and buildings are controlled by CyberLock key-centric access control system.

Monitoring Controls

- SolarWinds Network Performance Monitor / SolarWinds Event Manager
- Cisco Identity Services Engine / Trend Micro Workload Security & ApexOne-as-a-Service
- Okta Adaptive Multifactor Authentication / Okta Lifecycle Management / Tenable IO
- CyberAudit-Web Enterprise / Cisco Adaptive Security Appliance with FirePower
- Cisco Umbrella / Milestone XProtect Video Monitoring System

Confidentiality-Integrity-Availability (CIA) Triad of Information Security

The CIA triad represents the following three key principles of information security:

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including a protection of personal privacy and proprietary information. (Source: Rule 74-2.001, F.A.C.)
- **Integrity:** The principle that assures information remains intact, correct, authentic, accurate and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information. (Source: Rule 74-2001, F.A.C.)
- **Availability:** Ensure timely reliable access and use of information. (Source: Rule 74-2.001, F.A.C.)



Figure 6. CIA Triad of Information Security

Policies Implemented

Network

SolarWinds Network Performance Monitor: assesses the availability of network devices and components. Resources are manually configured with required information for each node to be monitored. Alert policies will notify stakeholders of performance degradation.

SolarWinds Event Manager: aggregates logs from various devices and platforms. Rule sets are configured to continuously analyze and detect anomalies across the network infrastructure. Changes to rules are manually performed based on recommendations received from the US Department of Homeland Security, Florida Department of Law Enforcement Office of Statewide Intelligence, and the CISA.

Cisco Identity Services Engine: facilitates identity and access control for network devices. Enterprise policies enforce compliance and streamline service operations. Compliance policies are manually updated based on Microsoft Security update releases and recommendations received from the CISA.

Operating Systems

SolarWinds Network Performance Monitor: detects performance issues and performs multiple condition checks against servers and workstations. Resources are manually configured with required information for each node to be monitored. Alert policies are set in place to notify all stakeholders of performance degradation.

Trend Micro Workload Security and ApexOne-as-a-Service: monitor and maintain the security posture of endpoint devices, including threat defense, machine behavioral analysis, and vulnerability intelligence. Threat pattern and intrusion prevention rules are automatically updated on connected agents directly from Trend Micromanagement engine. Configured to perform real-time and scheduled scans, malicious codes and unauthorized mobile codes are blocked, quarantined, or removed upon detection.

Tenable IO: scans the infrastructure and identifies security risks at scheduled intervals. Vulnerabilities are remediated as in the FDOT D4 Vulnerability Management Plan.

Applications

Application Control policies: set and monitored using Trend Micro Workload Security and ApexOne-as-a-Service. Trend micromanages and automatically updates security definition libraries. These definitions are scheduled to download at once; immediately applied to agents. Anti-malware and anti-spyware signatures are updated and stored in the Trend Micro cloud libraries. Configured to perform real-time and scheduled scans. Malicious and unauthorized mobile are blocked, quarantined, or removed upon detection.

Web applications: scanned at isolated intervals by Tenable IO to identify security risks. Vulnerabilities are remediated by the application developer, per FDOT D4 Vulnerability Management Plan guidelines.

Procedures

1. Alerts concerning confirmed malicious cyber activity and exploits shared from the FDOT ISM and the CISA are reviewed by the ITS Information Security Team.
2. Once reviewed, all necessary stakeholders are notified and are provided with the recommended actions to minimize security risk.
3. Remediations are performed according to the given risk of impact and likelihood of occurrence.

- | | |
|-----------------|--|
| Critical | <ul style="list-style-type: none"> • Vendor provided updates that remediates cybersecurity vulnerabilities are tested within 7 days of release, and then applied. • Monitoring and detection controls requiring manual configuration are updated immediately after notification. |
|-----------------|--|

High

- Vendor provided updates that clearly remediates cybersecurity vulnerabilities are tested within 14 days of release, and then applied.
- Monitoring and detection controls that require manual configuration are updated immediately after notification.

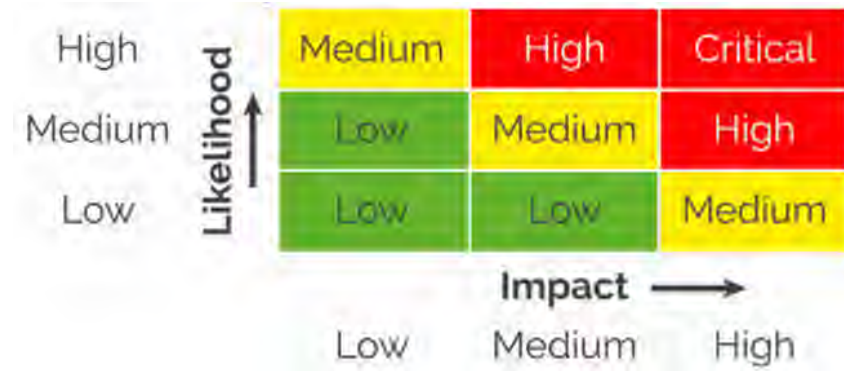


Figure 7. Cybersecurity Risk Matrix

VULNERABILITY PROJECT MANAGEMENT

Overview

A vulnerability requiring resolution from multiple stakeholders, becomes a vulnerability project, which will be tracked for remediation by the Vulnerability Project Manager by coordination with stakeholders. The procedures to resolve vulnerability projects are provided below.

Procedures

Security Team

Steps / Screenshots

1. The Security Team identifies vulnerabilities in the environment within Tenable IO and conducts the research for the fixes.
2. If an identified vulnerability requires remediation from multiple stakeholders, a Security Team creates a SolarWinds Service Desk Security Vulnerability incident and assigns it to the Vulnerability Project Manager, as shown in the example in Figure 3.

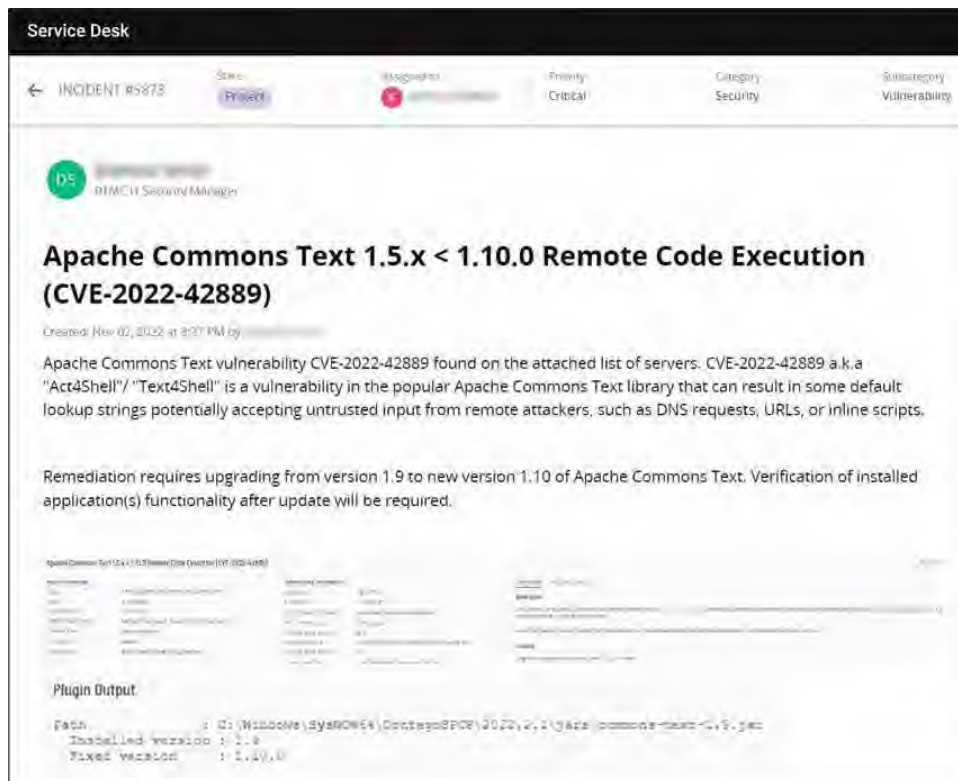


Figure 8. Example of a SolarWinds Service Desk Security Vulnerability Incident

3. The SolarWinds Service Desk Security Vulnerability incident includes the following information:

Steps / Screenshots

- Description of the vulnerability.
- Solution for the vulnerability.
- List of machines affected by the vulnerability.
- Any other supporting information.

Stakeholders

Steps / Screenshots

- Each stakeholder creates a change order or incident, as applicable, within the SolarWinds Service Desk and attaches the Security Vulnerability incident in the related tab

Service Desk

← CHANGE #152 Approved Assigned to: MH Priority: Medium

MH 13 Desktop Analyst

Commons-Text Shell Remediation - Servers

Created: Nov 03, 2022 at 11:31 AM by Mjake@Hill

In an effort to secure our environment, security application servers with CVE-2022-42889 shall be patched with a version 1.10.0 of Commons jar.

https://commons.apache.org/proper/commons-text/download_text.cgi

<https://community.tenable.com/s/thread/0D53a00002p5KXG?fromEmail=1&stoid=00D300000000pZp&stmid=00Bf2000000TNCI&stuid=0053a00000kzQo&stext=0&emkind=chatterGroupDigest&emtm=16065499820056>

Machines to be worked on:

View more:

Change Plan

- 1) Create snapshot of servers
- 2) Stop processes using Java on server

View more:

Rollback Plan

In case of issues with functionality, revert to taken snapshot.

Test Plan

Log in to servers and verify functionality of all applications.

COMMUNITY | DETAILS | PROCESS (1) | **RELATED (1)** | TASKS (4) | AUDIT

Related Items

INCIDENTS (1)

Apache Commons Text 1.5.x < 1.10.0 Remote Code Execution (CVE-2022-42889)

0873 • Resolved • Critical • Security • Vulnerability • May 14, 2022

Figure 9. Change Order Related to the Vulnerability Project Incident

Steps / Screenshots

2. Change order(s)/incident(s) include the following information, as applicable:
 - a. Requester's name or email address.
 - b. Descriptive title.
 - c. Justification for the need of the change order.
 - d. Tags and/or attachments.
 - e. Change plan.
 - f. Rollback plan.
 - g. Test plan.
 - h. Details.
 - i. Related items

Vulnerability Project Manager

Steps / Screenshots

1. A Vulnerability Project Manager coordinates with all stakeholders responsible for a solution for remediation to the machines affected by the vulnerability and tracks the project progress from the time it is created until it is resolved.

2. After verifying that a vulnerability is remediated on affected machines, a Vulnerability Project Manager changes the SolarWinds Service Desk Security Vulnerability incident from

Project to Resolved

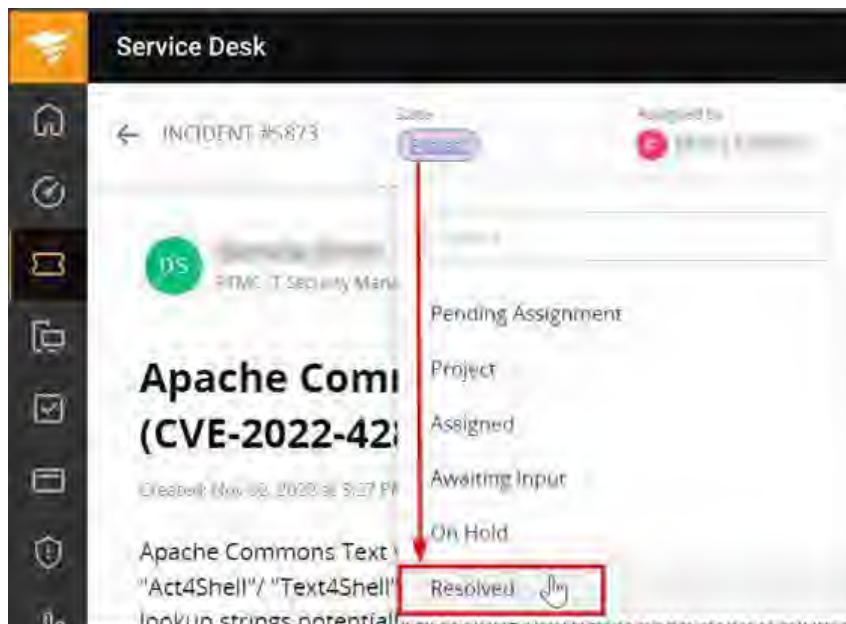


Figure 10. Vulnerability Project Resolved

TENABLE REMEDIATION SCAN GUIDE

Click [here](#) for detailed steps and screenshots

Overview

This document serves as a guide for starting, creating, saving, launching, and completing a remediation scan in Tenable.io. Assets affected by a vulnerability appear in the Active state in Tenable. Once the necessary steps are performed by the stakeholder(s) to remove the vulnerability from the affected asset, a remediation scan must be performed on the previously affected asset within Tenable for the vulnerability to be removed and for the state to change from Active to Fixed. The remediation steps are similar for servers and workstations. Plugin ID 168877 (vulnerability from an outdated version of Microsoft Edge) and asset VISWKS07 will be used as an example throughout this guide.

A remediation scan can be started after the necessary steps are performed by the stakeholder(s) to remove the vulnerability from the affected asset.



Figure 11. Microsoft Edge Vulnerability Removed from Asset VISWKS07

A remediation scan can easily be started from a vulnerability page. Or,



Figure 12. Start a Remediation Scan from the Vulnerability Page

from an asset page



Figure 13. Start a Remediation Scan from the Asset Page

Here, asset VISWKS07 is affected by Plugin ID 168877.



Figure 14. Asset VISWKS07 Affected by Plugin ID 16887

Start a Remediation Scan

Perform step 1. or 2. below to start a remediation scan.

Then, proceed to the Create, Save, And Launch a Scan section. 1.

Start the Process

Steps / Screenshots

1. To start a remediation scan from the **asset page**:

- Click **Actions**
- Select **Launch Remediation Scan**.



Figure 15. Asset Page > Actions

Steps / Screenshots



Figure 16. Asset Page > Actions > Launch Remediation Scan

To start a remediation scan from the **vulnerability page**,

2.
 - Click on **Actions**.
 - Select Launch Remediation Scan.

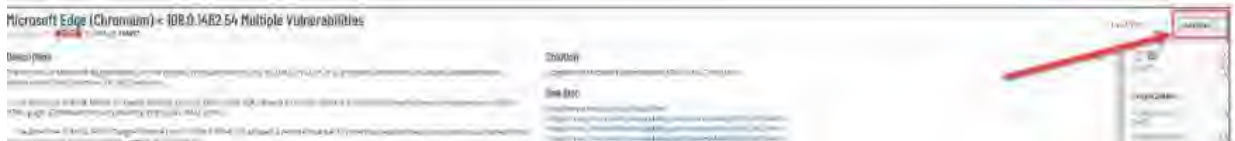


Figure 17. Vulnerability Page > Actions

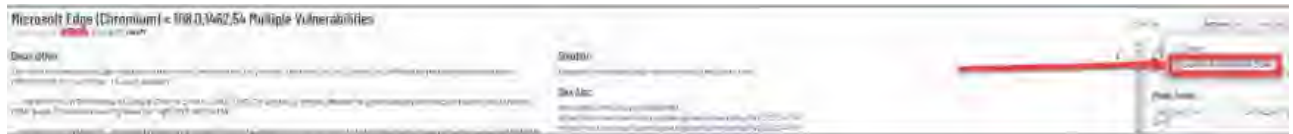


Figure 18. Vulnerability Page > Actions > Launch Remediation Scan

Create, Save, Launch a Scan

Perform steps 1. – 5. below to create a scan.

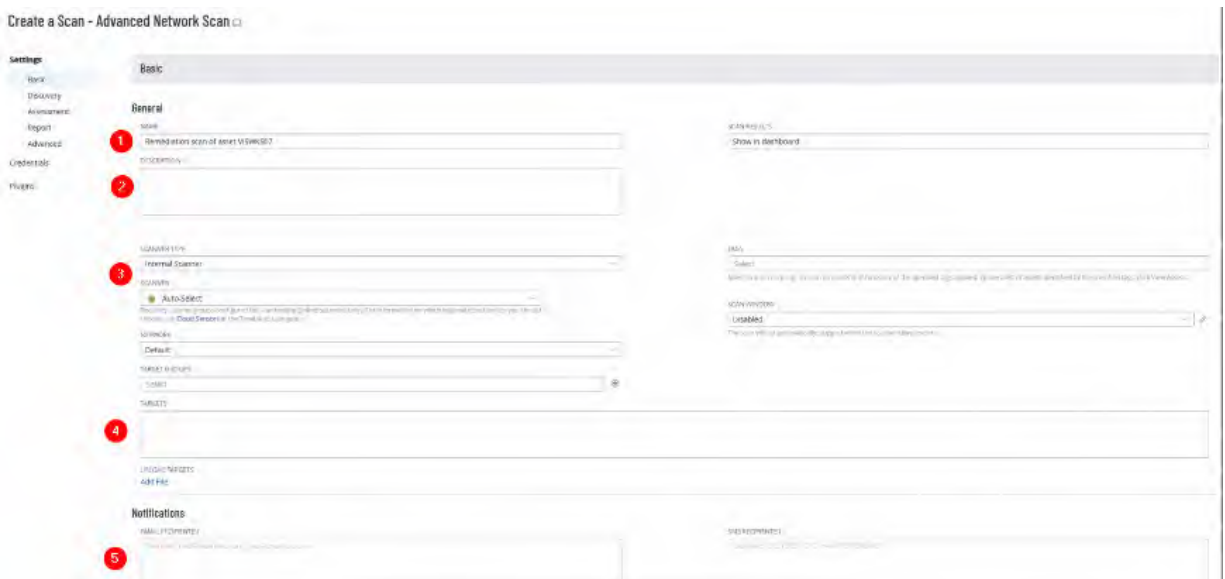


Figure 19. Create a Scan

Then, perform step 6. to launch it.

Steps / Screenshots

1. Name. This field will automatically be filled.
 - a. If the remediation scan is started from the asset page, it will **read Remediation scan of asset VISWKS07**.



Figure 20. Remediation Scan Started from the Asset Page

- b. If the remediation scan is started from the vulnerability page, it will **read Remediation scan of plugin 168877**.



Figure 21. Remediation Scan Started from the Vulnerability Page

2. **DESCRIPTION.** You can write a description of what you are doing in this field. It is helpful when different scans are performed.

Figure 22. Description

3. SCANNER TYPE.

- Click the drop-down menu for **SCANNER**.
- Select Internal Scanners.



Figure 23. Scanner

Steps / Screenshots

- a. **Credentials.** It is done for the scanner to have appropriate access to assets.
- On the left-hand side of the screen,
- Click **Credentials**.

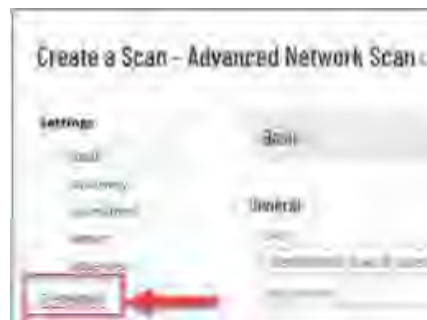


Figure 24. Credentials

- Click the + button next to **Add Credentials**.



Figure 25. Add Credentials

- b. On the right-hand side of the screen,
- Click the down arrow next to **MANAGED CREDENTIALS** to expand the menu options.
- When you scan an asset on the **smartsunguide** domain,
 - Select **SmartSunGuide LDAPAccount**.

When you scan an asset on the field domain,

- Select **Field LDAP Account**.

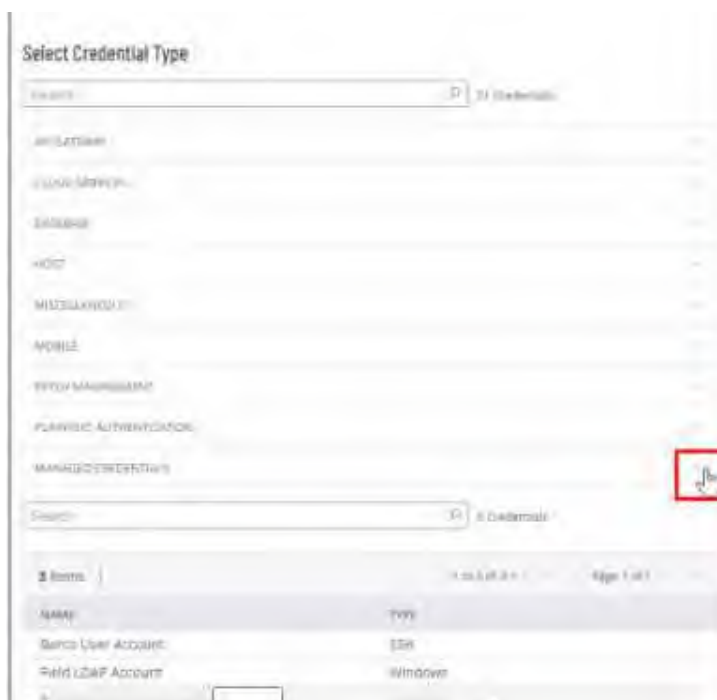


Figure 26. Managed Credentials

Steps / Screenshots

- c. Here, **SmartSunGuide LDAP Account** is selected.

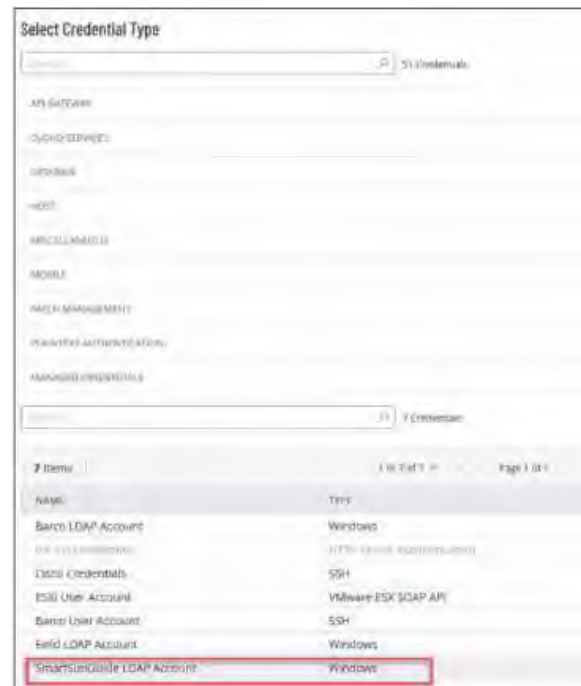


Figure 27. SmartSunGuide LDAP Account

4. **Targets.** These are the assets that will be covered in the scan.



Figure 28. Targets

- If launching a remediation scan from the asset page, its IP address will be auto-filled in this field.
- If launching a remediation scan from the vulnerability page, this field will be filled with the IP addresses of all assets listed in the vulnerability page.
- You can add or remove IP addresses here as you choose.

5. **Notifications.** In this field, you can enter your email address or that of others, to receive a notification.



Figure 29. Notifications

- The email will have the scan results and other information pertaining to what the scan found.

Steps / Screenshots

- b. You must return to Tenable for full details, when verifying if a certain vulnerability is eliminated from a particular asset.

6. At the bottom right-hand side of the page, Click **Save & Launch**. You will navigate back to your **Remediation Scans** page.

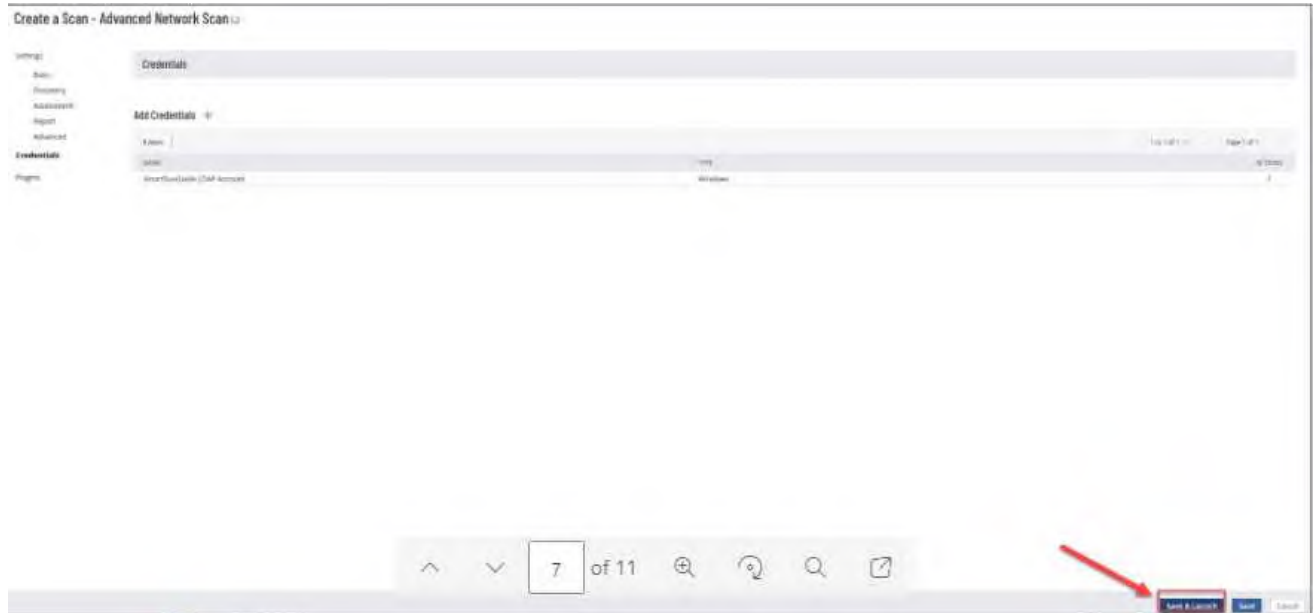


Figure 30. Save & Launch

Complete a Remediation Scan

Allow some time for the scan to complete. Completion time varies depending on how many machines are scanned as well as whether other scans are performed at the same time.

Steps / Screenshots

1. In the Remediation Scans page, you'll see the launched scan with a **Pending** status.

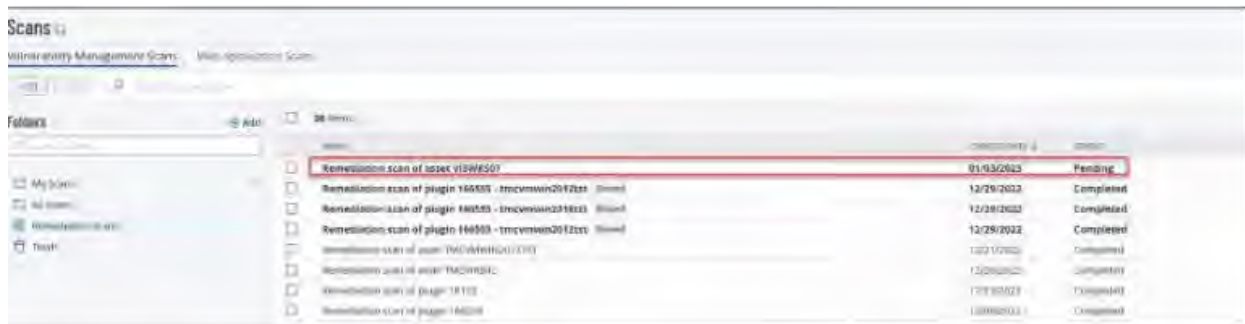


Figure 31. Remediation Scans Page – Status: Pending

2. Once the scan status is changed to **Completed**, Click it to view the details (e.g., scan duration and number of vulnerabilities).

Steps / Screenshots



Figure 32. Remediation Scans Page – Status: Completed

- a. Click **See All Details** to open a new page, where you can see more information about the asset.

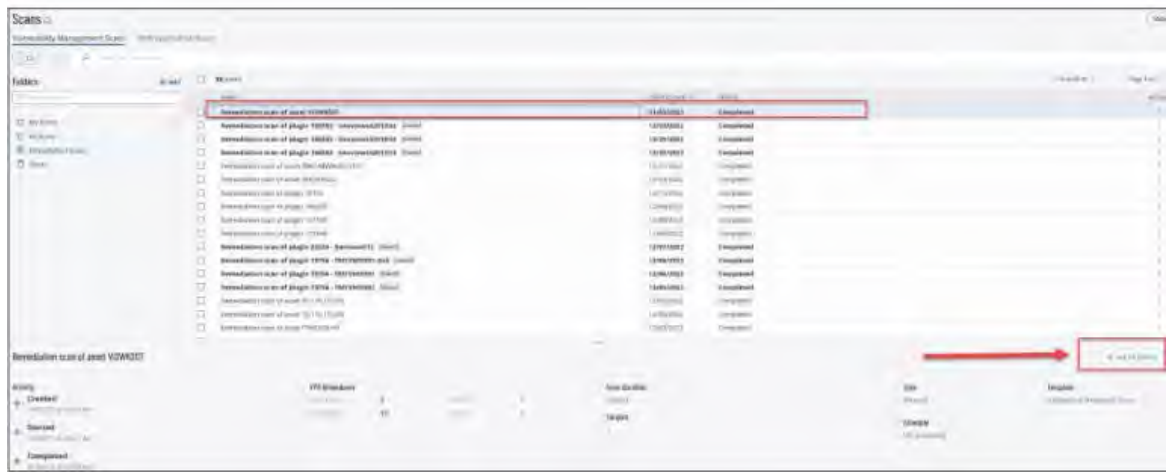


Figure 33. Remediation Scans Page – Status: Completed > See All Details



Figure 34. Remediation Scan Results

- b. Verify that the vulnerability has been removed from the affected asset.

Steps / Screenshots

(1) Compare the following screenshots, depicting the Microsoft Edge vulnerability before the remediation scan was performed.

The screenshot shows a list of vulnerabilities for asset VISWKS07. The Microsoft Edge vulnerability is highlighted in red. The table below represents the data shown in the screenshot.

Severity	Name	Impact	State	Count	CVSS
Critical	Microsoft Internet Explorer Unsupported Version Detection	Windows	Active	1	
Critical	Apache Log4j 1.x Multiple Vulnerabilities	Misc.	Resolved	1	
High	SSL Medium Strength Cipher Suites Supported (CVE-2015-4002)	Service	Active	2	
High	Microsoft Windows Update Reboot Required	Windows	Resolved	1	
High	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2017-1498)	Misc.	Resolved	1	
High	VeriSign Digital Signature Validation CVE-2013-3803 Mitigation (EnableCertificateCheck)	Windows / Microsoft Bulletins	Active	1	
High	KB901253: Windows 10 Version 20H2 / 21H1 / 21H2 / 22H2 Security Update (December 2022)	Windows / Microsoft Bulletins	Active	1	
High	Security updates for Microsoft .NET Framework (December 2022)	Windows / Microsoft Bulletins	Active	1	
High	Microsoft Edge (Chromium) < 108.0.1462.54 Multiple Vulnerabilities	Windows	Active	1	
Medium	SSL Certificate Cannot Be Trusted	Service	Active	2	
Medium	TLS Version 1.0 Protocol Detection	Service Detection	Active	2	
Medium	TLS Version 1.1 Protocol Detection	Service Detection	Active	2	
Medium	SSL Certificate with Wrong Issuance	Service	Active	1	
Medium	SSL Self-Signed Certificate	General	Active	1	
Medium	SSL Signing not required	Misc.	Active	1	
Low	Security updates for Microsoft .NET Framework (November 2022)	Windows / Microsoft Bulletins	Active	1	

Figure 35. Vulnerabilities List Before Remediation Scan

(2) Return to the asset page, away from the Scan section of Tenable, for the list of pending vulnerabilities on the asset in question, after the remediation scan was performed.

(3) The Microsoft Edge vulnerability no longer appears in the vulnerabilities list.

The screenshot shows the same list of vulnerabilities for asset VISWKS07 after a remediation scan. The Microsoft Edge vulnerability is no longer present. The table below represents the data shown in the screenshot.

Severity	Name	Impact	State	Count	CVSS
Critical	Microsoft Internet Explorer Unsupported Version Detection	Windows	Active	1	
Critical	Apache Log4j 1.x Multiple Vulnerabilities	Misc.	Resolved	1	8.4
High	SSL Medium Strength Cipher Suites Supported (CVE-2015-4002)	Service	Active	2	5.1
High	Microsoft Windows Update Reboot Required	Windows	Resolved	1	
High	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2017-1498)	Misc.	Resolved	1	7.8
High	VeriSign Digital Signature Validation CVE-2013-3803 Mitigation (EnableCertificateCheck)	Windows / Microsoft Bulletins	Active	1	7.8
High	KB901253: Windows 10 Version 20H2 / 21H1 / 21H2 / 22H2 Security Update (December 2022)	Windows / Microsoft Bulletins	Active	1	7.8
High	Security updates for Microsoft .NET Framework (December 2022)	Windows / Microsoft Bulletins	Active	1	7.4
Medium	SSL Certificate Cannot Be Trusted	General	Active	2	
Medium	TLS Version 1.0 Protocol Detection	Service Detection	Active	2	
Medium	TLS Version 1.1 Protocol Detection	Service Detection	Active	2	
Medium	SSL Certificate with Wrong Issuance	General	Active	1	
Medium	SSL Self-Signed Certificate	General	Active	1	
Medium	SSL Signing not required	Misc.	Active	1	

Figure 36. Vulnerabilities List After Remediation Scan

(4) Perform a search for Fixed vulnerabilities and see that the Microsoft Edge vulnerability appears in the list of fixed vulnerabilities.

Steps / Screenshots



Figure 37. Search for Fixed Vulnerabilities

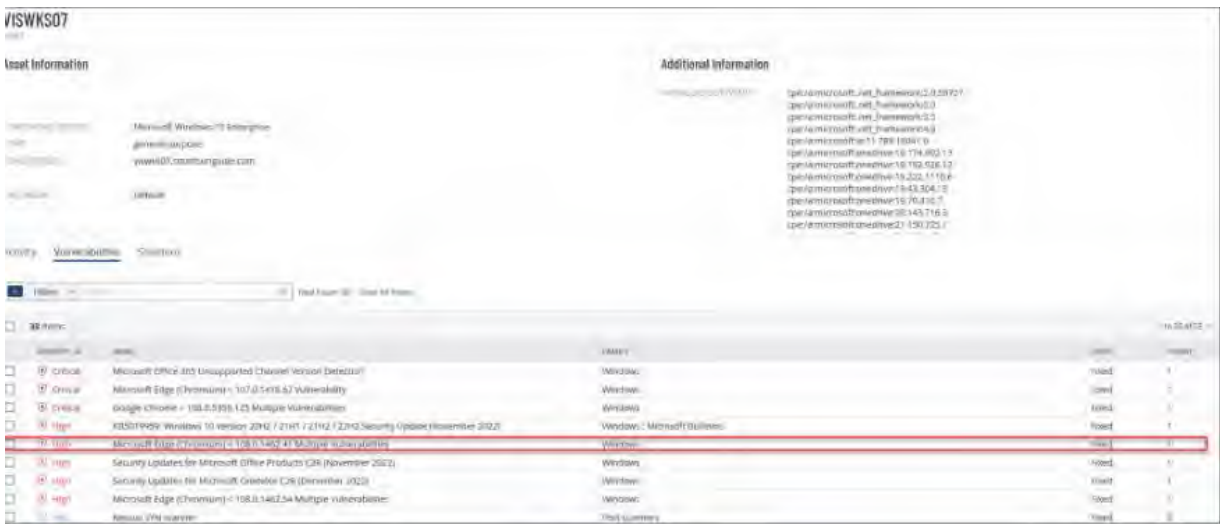


Figure 38. Fixed Vulnerabilities List



7.05 Network Backup and Recovery

Table of Contents

BACKUP	4
Four Levels of Backups.....	4
Email:.....	4
Configurations, database files:.....	4
File Share:.....	4
Physical and Virtual Servers:.....	4
Backups Scenarios.....	4
BACKUP DATA RULES AND REQUIREMENTS	5
Purpose.....	5
Practice.....	5
Method.....	5
Data Categories.....	5
Minimum Data Backup Requirements (Frequency).....	6
User Data.....	6
System and Infrastructure Data.....	6
Static Data.....	6
Exceptional Data.....	6
Technical Support: Roles & Responsibilities.....	6
Exceptions.....	7
APPENDIX: BACKUP DOCUMENTATION	8
Backup Software.....	8
Backup Locations.....	8
Backup Testing Procedures.....	9
DISASTER RECOVERY PLAN MANUAL	10
Introduction.....	10
Plan Objectives.....	10
Plan Scope.....	10
Service Recovery Point Objective (RPO) And Recovery Time Objective (RTO) Targets.....	10
Backup Strategy.....	11
Testing Schedule.....	11
Plan Review.....	11
Revision History.....	11
Roles and Responsibilities.....	11
Internal Contacts.....	11
External Contacts.....	12
Incident Response.....	12
DR Procedures.....	12
DR Plan for Damage to Servers.....	12
DR Plan for Damage to SAN.....	13
Failover Capabilities.....	13
Appendices	14
Alternate Work Locations.....	14
Notification Procedures.....	14
DR ACTIVITIES RECORDS	15

Document History

Version #	Date	Author	Changes
1.0	12/19/2023	Yana Neishlos	Initial Draft

BACKUP

Four Levels of Backups

1. **Email:** The Exchange system managing all e-mails is setup in a database availability group. Three separate copies of the Exchange database are stored on three separate systems. Two are located within the TMC, and the one – within TIMSO. The TIMSO Database is stored within the Enterprise Backup System. A Journaling rule is enabled to keep e-mails for seven years per Florida State Statue standards. E-mails used for public record are stored on a database, isolated from other user databases to prevent data corruption.
2. **Configurations, database files:** Configurations, database files for an application running a preset configuration that can back up the configuration via FTP, SFTP, or SSH, is automatically saved to the SFTP server running in the TMC. This server replicates configuration files to a remote site within TIMSO. Both the TMC SFTP and TIMSO SFTP Server are backed up via separate backup appliances that store the information long term to tape.
3. **File Share:** District Four utilizes a DFS cluster to house multiple copies of the same file across geographic locations housed on different servers. Each server tracks changes through a native Microsoft Volume Shadow service to provide self-service recovery by individual users within the Windows subsystem. But, servers, housing the same file, are saved independently, and backed up to disk archive through our backup server.
4. **Physical and Virtual Servers:** Physical and virtual servers are backed up twice through the backup appliance in the TMC and TIMSO for redundancy and fast recovery time for files. Cold Archive Storage is used for long-term backups more than a year old.

Backups Scenarios

1. **Lost / corrupted file(s) on a file server** District Four IT Department to perform a file level recovery through Microsoft Shadow Copy Service. If unavailable, → refer to file level backups on one of three file servers and restore from tape backup.
2. **Corrupted application and / or Operating System located on a server(s) providing services.** District Four: restore virtual machine(s) configuration(s) to its previous state from a virtual machine recovery point. If it is a physical server, District 4 will perform a recovery through restoring at a previous point in time through a recovery point within its backup appliance subsystem from the TMC or TIMSO that holds a copy of its system state.
3. **Complete destruction or failure of the TMC** District Four has developed a limited functionality hot site to provide baseline services of email, file, print, and SunGuide access through its Fort Pierce disaster recovery site. Services are live; replicated in real time to enable users' functions in case of a complete TMC failure. Based on the TMC damage, then a decision to be made to start with recovery from District Four ITS backup systems to new hardware. If a new hardware is not available, recovery to existing hardware a case-by-case scenario will be decided based upon immediate and long-term needs of the Department for data access.

BACKUP DATA RULES AND REQUIREMENTS

Purpose

This document establishes the baseline rules and requirements for the backup of data and servers throughout the FDOT District Four TSM&O environment unless otherwise noted in the Exceptions table. Moreso, the document establishes roles and responsibilities for FDOT District Four TSM&O staff as it relates to data backup.

Practice

[FDOT Topic No. 325-060-020](#), Section 7, Protection Against Loss, states all data and software essential to the continued operation of critical agency functions shall be mirrored to an off-site location or backed up regularly with a current copy stored at an offsite location. TSM&O has developed a standard process for backing up and retention of data and systems at the datacenters.

In addition, this document establishes roles and responsibilities for TSM&O staff for:

- Local backups
- Replicated data
- Data Restoration
- Troubleshooting
- Problem resolution
- Communication

As infrastructure or operational requires changes, it is common to reassess the provisions of this document. Reviews and updates shall occur bi-annually and in accordance with the Method and Practice Process.

Exceptions must be approved by District Four TSM&O managers or above and documented in the Exceptions Table located at the end of this document.

Method

Data Categories

Data is classified into five (5) data categories:

Category	Details	Examples
System Data	Consists of the server operating system and its extensions. Data is typically restored by restoring the entire virtual machine or rebuilding the machine from original installation media.	Operating systems, applications used to manage the servers.
Infrastructure Data	Supports the Local Area Network (LAN) and its users. If loss occurs, data will have special requirements for backup and recovery.	The installation and configuration files (not databases) for DNS, Active Directory, SQL Server.
Static Data	Static data does not change. It is copied from original media, e.g., CD, DVD, or original electronic source to LAN file server storage.	Usage: providing access to application installation files, service packs, and software updates not accessible via the Internet. Data is never modified.

Category	Details	Examples
User Data1	Staff requires this data to support operations and processes of the Department. User data is required to complete specific tasks and staff's daily work. Data type is modified regularly; essential to the operation of the Department.	It exists in various file formats. It is stored in shared folders, within other programs or databases such as security logs, SharePoint or stored on LAN file servers.
Exceptional Data1	Exceptional Data is data identified by the data owner as requiring special attention for the purpose of backup or recovery.	Data are CADD final plans requiring longer retention; it is sensitive; requires isolation and explicit permissions; email/messaging data subject to public record retention regulations.

User Data1

1 It is not the responsibility of the TSM&O to differentiate between User and Exceptional data. It is the responsibility of the data owner to notify TSM&O IT of data classified as Exceptional and to document a backup/recovery plan.

Exceptional Data1

Minimum Data Backup Requirements (Frequency)

User Data

Backup of user data is required daily to include databases containing user data or are necessary for data restoration. Backups of user data combined with system and infrastructure data shall ensure complete recovery of user data and a recovery of individual files. At the least, full backups must be performed weekly. Incremental backups must be performed between full backups for the user data to be restored from a daily point-in-time between full backups. User data backups are stored offsite.

System and Infrastructure Data

Incremental backups of all system and infrastructure data shall occur daily, and as necessary for changes to the environment. A full backup (or image) of all system and infrastructure data shall occur once a week or as changes are made to the infrastructure. System and infrastructure backups shall be stored offsite.

Static Data

No backup is required; however, a backup may be created for the purpose of faster recovery.

Exceptional Data

Data owners are responsible for creating a plan for backup and recovery.

Technical Support: Roles & Responsibilities

Local/ Replication Backup Site Responsibilities and Support

- At least two staffers shall be designated as primary and secondary technical support to ensure that all backups adhere to standard requirements. The designees shall be trained to perform data backup functions for each location.
- TSM&O IT staff are responsible for:

- configuring local backup, copy jobs, daily monitoring and resolving backup/copy failures. TSM&O IT staff will contact the backup software vendor to troubleshoot software related issues.
- monitoring all backup server hardware, operating systems, and backup software including the required system support software, i.e., antivirus.
- all restoration requests for their district staff.

Backup Scheduling

Backup administrators shall schedule backups according to manufacturer specifications of load and efficiency. Not all backups can run at once. Backups should be run in “non-peak” hours, from 7pm until 7am, or unless otherwise appropriate to schedule during the day, due to low usage on an asset.

Performance & Maintenance Requirements

Technical support staff for server backups shall adhere to the following requirements pertaining to onsite and offsite storage, retention, verification and logging, documentation, media, and software.

Onsite & Offsite Storage

The full backup (any classification of data) shall be digitally replicated to the replication backup site.

Retention

Backup data (any classification of data) shall be retained offsite for a minimum period of six months. This is a minimum requirement, and any further retention requirements is a decision made at the discretion of the D4 TSM&O management.

Verification & Logging

Backup integrity shall be verified. Designated D4 TSM&O IT technical support shall perform a test restore to a temporary directory of their choosing.

Documentation

Information concerning file server backups shall be thoroughly documented: “The IT Support Manager is responsible and accountable for ensuring the documentation includes sufficient information and details to enable competent staff to perform the same duties using that documentation.”

Documentation shall include the following items:

- Technical staff members responsible for backups (primary and backup).
- Instructions for performing the backup and restoration.
- Monitoring, testing, and verification procedures.
- Method for scheduling and recording the server backups.
- Backup method (Local Area Network or Wide Area Network).

Software Standards

The standard software for backup, retention, and software used for any specific backup purpose not defined in this document shall be limited.

Exceptions

Requestor	Approver	Approved	Date	Description Exception	Expiration

APPENDIX: BACKUP DOCUMENTATION

Backup Software

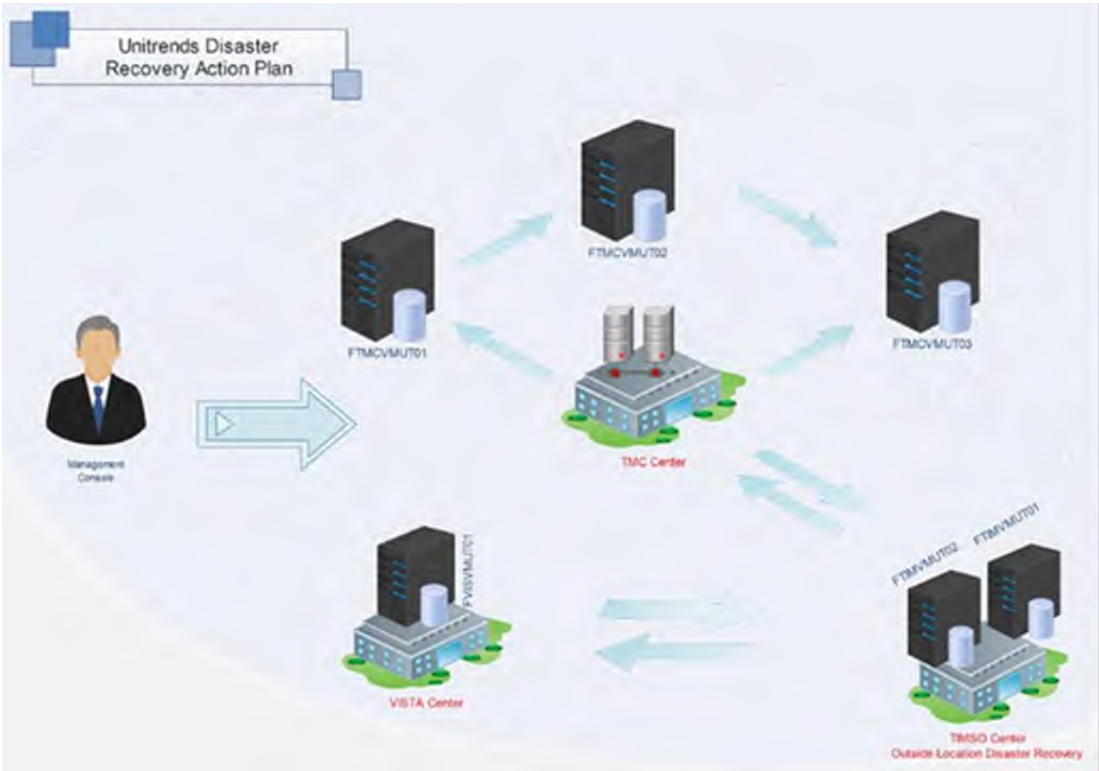
The current software being used is "Unitrends" backup. This runs on a virtual appliance in the D4 TSM&O VMware environment.

FTMCVMUT04 – Test Environment	
FTMCVMUT01 – Backup Target	Broward TMC
FTMCVMUT02 – Backup Target	
FTMCVMUT03 – Backup Target	
<hr/>	
FTIMVMUT01 – Backup Target	TIMSO Treasure Coast
FTIMVMUT02 – Backup Target	
<hr/>	
FVISVMUT01 – Backup Target	Palm Beach Ops Center

Backup Locations

The following locations are used for backups, with subsequent replication site info.

1. *Broward TMC* 2300 W. Commercial Blvd, Fort Lauderdale, FL 33309 Replication Site – TIMSO Treasure Coast
2. *TIMSO Treasure Coast* 3601 Oleander Ave, Fort Pierce, FL 34982 Replication Site – Broward TMC
3. *Palm Beach Operations Center* 7900 Forest Hill Blvd, West Palm Beach, Florida 33413 Replication Site – TIMSO Treasure Coast



Backup Testing Procedures

1. Backup testing will be conducted by the following designated personnel.
 - IT Server Manager
 - IT Server Administrator
2. Backup Verification will be conducted by the following designated personnel: IT Support Manager
3. Backup testing will happen every 6 months, and will contain the following items:
 - A file restore from the Share Drive (N: Drive), to be documented on the “Backup Test After-Action.”
 - A bare-metal restore, of a System and Infrastructure Data node, of non-significant value (i.e. no Domain Controllers or databases), to be documented on the “Backup Test After-Action.”
 - Backups, from both above types, will occur using both the primary and replication locations.
 - The “Backup Test After-Action will be submitted to the Verification designee within 24 hours of the completion of the test.
 - The verifier will test the “restores” for all aspects.
 - Functionality
 - Integrity
 - Performance
 - Accessibility
 - Accuracy
4. Any testing issues will be documented in the “After-Action Report” and a ServiceDesk ticket will be created for resolution. The ticket number will also be documented with all related Change Orders for resolution.

DISASTER RECOVERY PLAN MANUAL

Introduction

This document details the policies and procedures of FDOT District 4 TSM&O IT in the event of a disruption to critical IT services or damage to IT equipment or data. These processes will ensure that those assets are recoverable to the right level and within the right timeframe to deliver a return to normal operations, with minimal impact on the business.

Plan Objectives

- Reduce overall risk.
- Create a rapid response to outages.
- Provide contact details to key personnel.
- Provide example scenarios.
- Define communication to users and managers.

Plan Scope

This plan will incorporate all aspects of the D4 TSM&O IT environment and their disaster recovery capabilities and procedures. The contact information within this document will remain updated on a regular basis for any scenario where it will be used.

Service Recovery Point Objective (RPO) And Recovery Time Objective (RTO) Targets

RPO designates the variable amount of data lost or will have to be re-entered during network downtime. Commonly designated as the frequency of backups performed (i.e., daily backups = 24 hours, database backups = 1 hour).

RTO designates the amount of real time that can pass before the disruption begins to impact the flow of normal business operations. It is commonly designated as the amount of time the application or system can be down before causing interruption in business operations.

IT Service	Scenario	RPO	RTO	Priority
SunGuide	Server Failure	24 hours	15 minutes	Medium
Production Network	Fibre Cut/Equipment Failure	Indefinite	Instant	High
VMWare Virtual Environment	Server Failure/Location Disaster	24 hours	15 minutes	High
Internet Circuit	Cut/Loss of Service	Indefinite	Instant	High
Databases	Server Failure/Data Integrity	1 Hour	Instant	Medium
Cisco ASA	Equipment Failure/Loss of Power	Indefinite	Instant	High

IT Service	Scenario	RPO	RTO	Priority
SAN	Equipment Failure	24 hours	4 Hours	Medium

Backup Strategy

Refer to the "Backup Data Rules and Requirements" document for details.

Testing Schedule

The DR plan will be tested in its entirety once every 6 months.

Recovery process for IT service will be tested once every 6 months.

Plan Review

The DR plan itself will be formally reviewed once every 12 months and in response to regular testing.

Revision History

Version	Date	Revision details
1.0	02/24/2020	Initial Revision
2.0	02/10/2021	Updated the "Service RPO and RTO targets" and "Failover Capabilities" sections.
3.0	09/8/2021	Updated the "Internal Contacts" section and key contacts in the "DR Plan for Damage to Servers" and "DR plan for Damage to SAN" sections.

Roles and Responsibilities

The following individuals are to assume responsibility for restoring IT services when the DR plan is activated:

Internal Contacts

Name	Job role	Contact details	DR process owned
Aaron Rapp recovery	IT Support Manager	RTMC, (954) 789-3478	Backup and data
Derron Ungolo recovery	IT Server Manager	RTMC, (954) 294-9448	Backup and data
Kuanming Li	IT Network Manager	RTMC, (954) 654-8407	Network Redundancy

External Contacts

Name	Organization	Contact details	DR process owned
Crown Castle Fiber Support	Crown Castle – Circuit ID VDP-0000138662 (FTLDFLFMH13)	(855) 93-FIBER	Network Circuit (Backup) RTMC
Comcast Business Support	Comcast – Account # 963195163	(800) 391-3000	Network Circuit (Primary) TIMSO
AT&T Support	AT&T – Account # 831-000-6324 541 / Router ID: 902744286	(855) 971-6681	Network Circuit (Primary) RTMC

Incident Response

The DR plan is to be activated when one or more of the following criteria are met:

- Activated by IT Support Manager.
- Activated by TSM&O Management.
- Activated by FDOT District Management.

The person discovering the incident must notify the following DR stakeholders, who collectively assume responsibility for deciding which - if any - aspects of the DR plan should be implemented, and for establishing communication with employees, management, partners, and customers.

- Theodore Burdusi, (954) 847-2797
- Nicole Forest, (954) 847-2631
- Dee McTague, (954) 691-5340

DR Procedures

Depending on the incident, and on the number and nature of the IT services affected, one or more of the following DR procedures may be activated by the DR team:

DR Plan for Damage to Servers

Scenario	Damage to servers at RTMC office
Possible causes	Fire, flooding, wind damage
IT services and data at risk	Email Systems, SunGuide, Databases, SAN, VMWare Virtual Environment
Impact	Internal/external communications lost; incident response affected
Plan of action	<ul style="list-style-type: none"> • Identify issue, coordinate initial response. • Remove damaged servers from data center.

- Evaluate damage.
- Establish data recovery targets and timeframes.
- Send courier for damaged servers.
- Share images after data recovery

Key Contacts Aaron Rapp
Derron Ungolo
Theodore Burdusi

DR Plan for Damage to SAN

Scenario	Damage to SAN at RTMC office
Possible causes	Fire, flooding, wind damage
IT services and data at risk	Email Systems, SunGuide, Databases, SAN, VMWare Virtual Environment
Impact	Internal and external services lost; incident response affected
Plan of action	<ul style="list-style-type: none"> • Identify issue, coordinate initial response. • Contact Dell Support for response. • Remove damaged drives/module. • Evaluate damage/failure. • Establish data recovery targets and timeframes
Key contacts	<ul style="list-style-type: none"> • Aaron Rapp • Derron Ungolo • Theodore Burdusi

Failover Capabilities

<u>IT Service</u>	<u>Primary</u>	<u>Secondary</u>
SunGuide	RTMC	TIMSO
Production Network	Layer 3 Failover / Multiple Routes	Layer 3 Failover / Multiple Routes
VMWare Virtual Environment	RTMC	TIMSO

Appendices

Alternate Work Locations

Site	Address	Contact details	Facilities available
Broward RTMC	2300 W. Commercial Blvd. Fort Lauderdale, FL 33309	(954) 847-2785	Server Room, Offices, Network connection, Servers
Treasure Coast TIMSO	3601 Oleander Ave. Fort Pierce, FL 33411		Server Room, One Office, Control Room, Network connection, Servers
Palm Beach Operations Center	7900 Forest Hill Blvd. West Palm Beach, FL 33413	(954) 593-8788	Server Room, Office, Control Room, Network Connection

Notification Procedures

In the event of a DR activation, an email will be sent out to the following distribution list:

Everybody-All-DL@smartsunguide.com. The email will include the following information, at a minimum:

- The location of the disaster.
- The services impacted.
- Restoration plan details and failover status.
- Estimated time of restoration.

Updates will be sent out at regular intervals until the completion of the DR plan.

DR ACTIVITIES RECORDS

Date	Activity	Outcome	Actions



7.06 Remove Outlook Mailbox From PC

Table of Contents

REMOVE OUTLOOK MAILBOX FROM PC	4
FDOT OUTLOOK SETUP INSTRUCTIONS	7
RESET YOUR FDOT EMAIL PASSWORD.....	10
SELF-PASSWORD RESET FOR OUTLOOK EMAIL	12
OUTLOOK MOBILE SETUP	18
EMAIL BACK-UP AND RECOVERY	20
REMOVE DOT EMAIL FROM SIRV PHONES	21
VIEW MEETINGS IN THE LARGE CONFERENCE ROOM	29

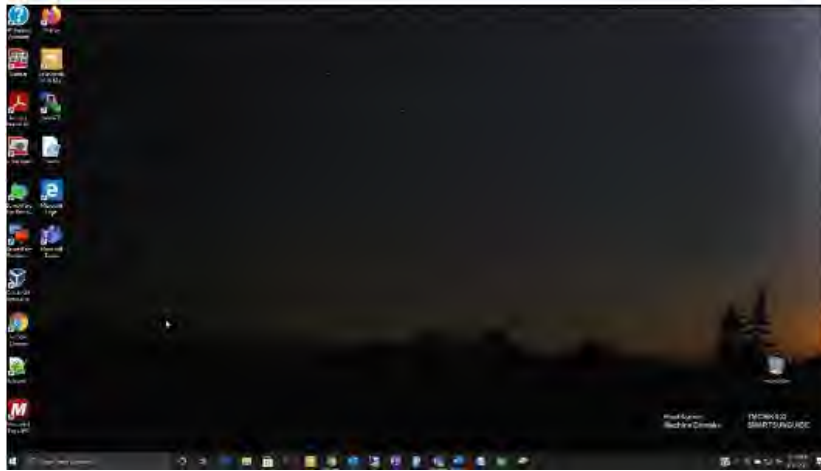
Document Version History

Version #	Date	Author	Changes
1.0	2/20/2023	Yana Neishlos	Initial Draft

REMOVE OUTLOOK MAILBOX FROM PC

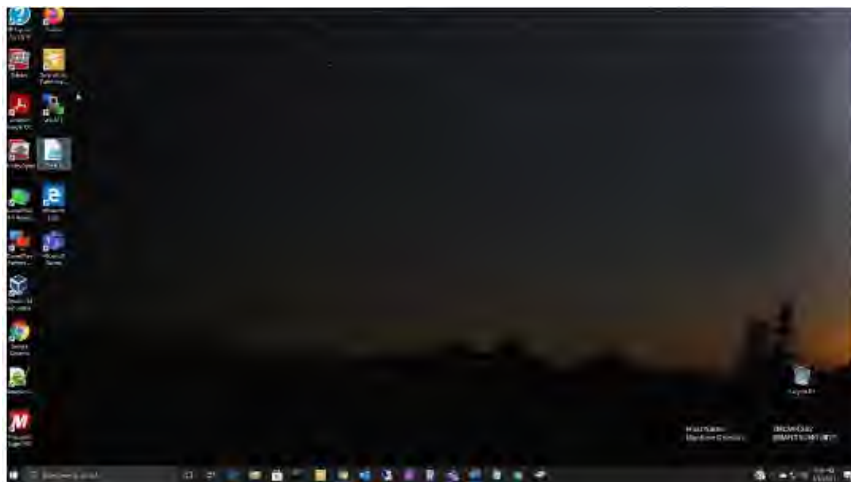
#	Steps / Screenshots
---	---------------------

1. Close the Outlook Application.



2. Contact the IT Office at the D4 RTMC to obtain the script.

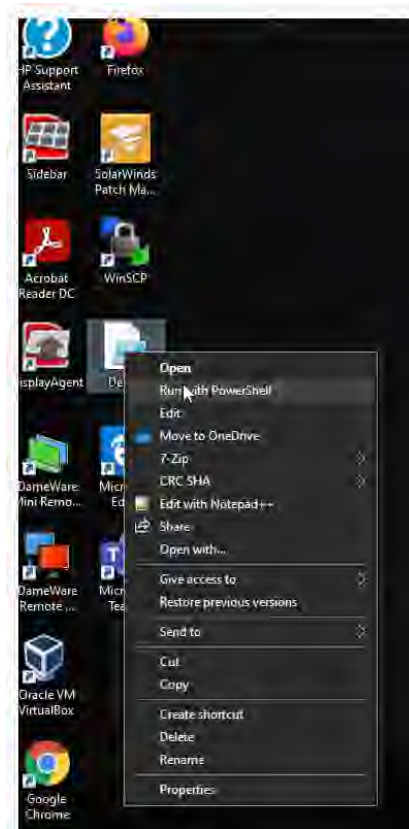
You must delete script.



3. After closing Outlook, → Go to the **Delete script** → Right-click on it.

Steps / Screenshots

- Right-click to delete script.
Select the option **Run with PowerShell**.



- After selecting the option, two things will happen. The script will run and give you a PowerShell prompt or it will simply run, and nothing will open on your screen. If you get the prompt it should look like below.

```

Windows PowerShell
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"):
  
```

- If you are prompted via PowerShell, you must type in the letter "A" for the option that says.
- After typing in option "A" and pressing enter. The script will run and close itself out.

```

Windows PowerShell
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"):
  
```

Steps / Screenshots

8. Right-click the script.

Run as PowerShell again. This time it should not ask you to enter in anything and should briefly run, and disappear.

9. Click **Start the Outlook application**.

10. The mailbox should be cleared.

You should be prompted to sign in now.



Sign in

Email or phone

[Can't access your account?](#)



FDOT OUTLOOK SETUP INSTRUCTIONS

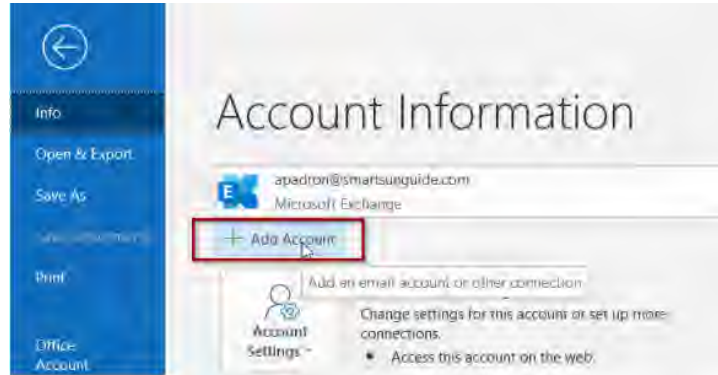
Here, you can find the instructions on how to add your Office 365 FDOT email account to your Outlook application. If you have any further questions, please submit a support ticket.

This document will cover the steps to login within Outlook on Workstation using your FDOT account.

Steps / Screenshots

1. Within Outlook,

- Click **File**.
- Click **Add Account**.



2. Fill in your FDOT email address and password into the provided fields.



3. Once you have successfully filled in your login information, you will see this prompt.

- Ensure you completely close Outlook.
- Then, re-open.



4. Your default web browser will automatically open a link to assist you with your mobile account access.

Steps / Screenshots



When you re-launch outlook, it could take a minute or two to load your new profile into Outlook.



Steps / Screenshots

5. Once outlook is done opening, locate your new mailbox by scrolling down on the left side of the application as shown below:



If you need any further assistance, please email support@floridadot.samanage.com and we will be able to assist you as soon as possible.

You can also still access your email while waiting for support. To do so, login using your FDOT email account on www.Outlook.com in order to access the web version of your outlook profile.

RESET YOUR FDOT EMAIL PASSWORD

Steps / Screenshots

1. On Intrasmart,

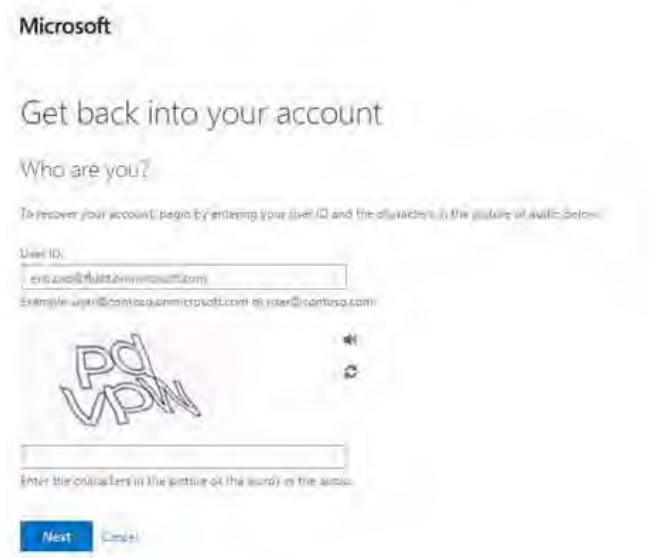
Go to Broward Resources
→ Click **FDOT Outlook Web**.



2. Select "Forgot my password".



3. Enter in your email in the "User ID" box and the characters in the text box below.



Steps / Screenshots

4. Enter your phone number and wait for the text message.

Microsoft

Get back into your account

verification step 1 > Choose a new password

Please choose the contact method we should use for verification:

Text my mobile phone

Call my mobile phone

In order to protect your account, we need you to enter your complete mobile phone number (*****14) below. You will then receive a text message with a verification code which can be used to reset your password.

Enter your phone number

Next

Cancel

5. Enter the verification code from the received text message.

verification step 1 > choose a new password

Please choose the contact method we should use for verification:

Text my mobile phone

Call my mobile phone

We've sent you a text message containing a verification code to your phone.

Enter your verification code

Next Try again Contact your administrator

Cancel

6. Enter your new password and type it again in the bottom text box to confirm your new password.

Get back into your account

verification step 1 ✓ > **choose a new password**

* Enter new password:

Password strength

* Confirm new password:

Finish Cancel

SELF-PASSWORD RESET FOR OUTLOOK EMAIL



Steps / Screenshots

1.
 - Open your browser.
 - Go to the intrasmart website at <https://intrasmart.smartsunguide.com>.
 - Click the **Broward Resources** Tab on the Intrasmart website.



2.
 - Click down the options under **Broward Resources** until you see **FDOT Outlook Email** → Click it.

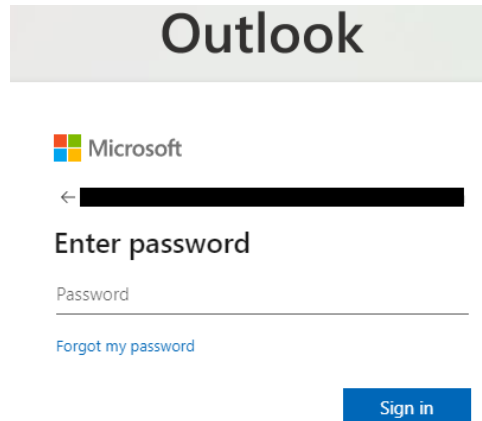
It should take you this site on your right.

- Enter in your FDOT email (Where it says **Email or phone**).
- Click **Next**.



Steps / Screenshots

3.
 - Enter your FDOT email's password.
 - Click **Sign in**.



4. To approve the sign in request on your mobile device,

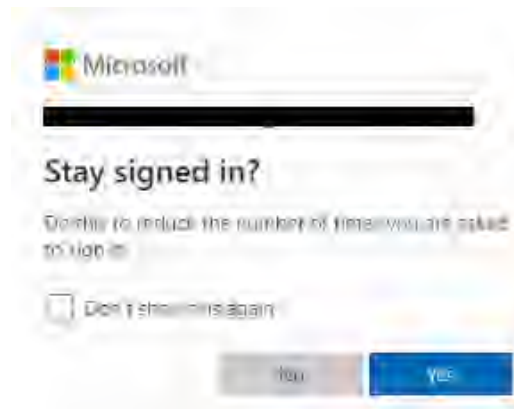
You would have had to set up your email account on the Microsoft Authenticator App already.



5. After successfully approving, it should take you to a page to **Stay Signed In**.

It does not matter which option you choose.

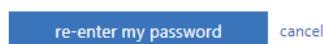
Click **Yes**.



6. It will take you to a new page that will request you to re-confirm your password.
 - Click **re-enter my password**.
 - Type in your password.

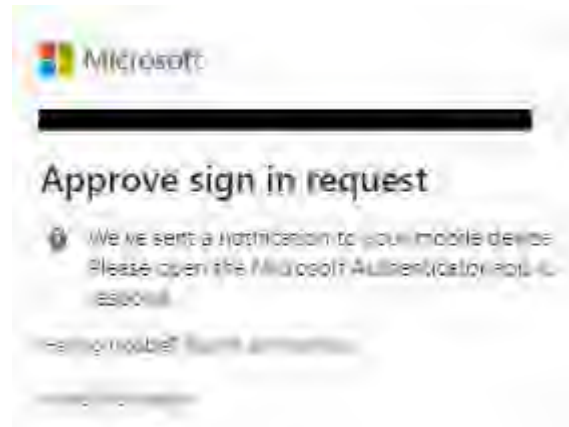
confirm your current password

In order to keep your security information private, we need you to re-enter your current password on the next page.



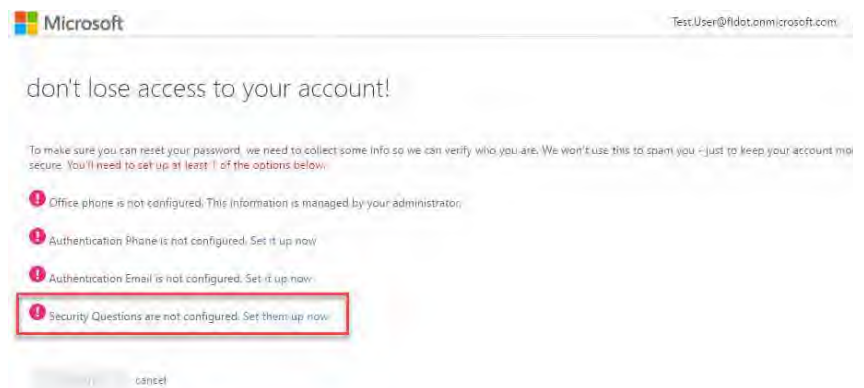
Steps / Screenshots

7. It will ask you to approve on the Microsoft Authenticator App once more.



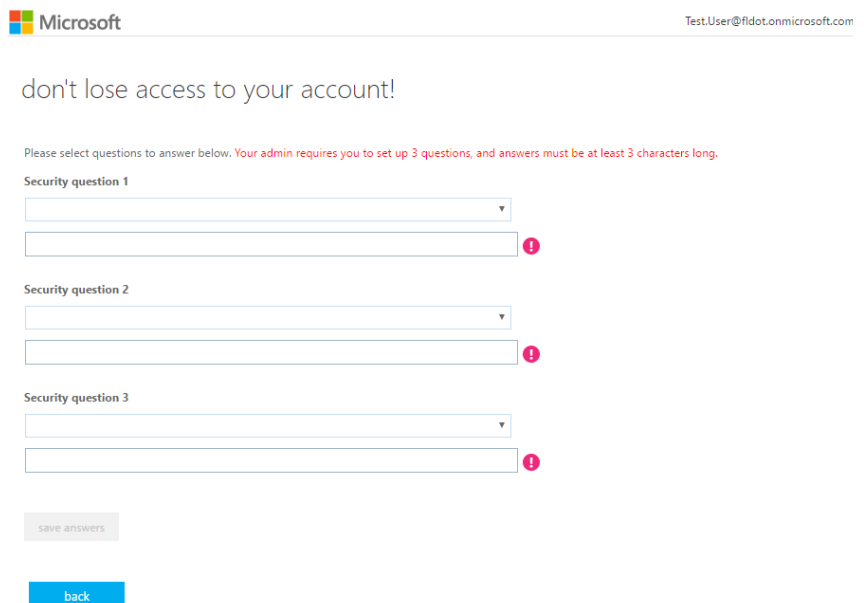
8. It will take you to this page on your right and to verify the recovery options.

- Confirm that the information already listed on the page is correct, i.e., your phone #.
- Preferably, → configure and use **Security Questions**, as shown.



9. – Click **Set them up now**. The Security Question Configuration screen will appear on your right.
- Pick at least three security questions from the pre-defined security questions box as shown below.

In what city was your father born?
 In what city was your first job?
 What city were you in on New Year's 2000?
 What is your father's middle name?
 What is your favorite food?
 What is your mother's middle name?
 What school did you attend for sixth grade?
 What was the make and model of your first car or motorcycle?
 What was the name of the first school you attended?
 What was the name of the hospital in which you were born?
 What was the name of your childhood hero?
 What was the name of your favorite stuffed animal?
 What was the name of your first pet?
 What was your childhood nickname?
 What was your first job?
 When you were young, what did you want to be when you grew up?



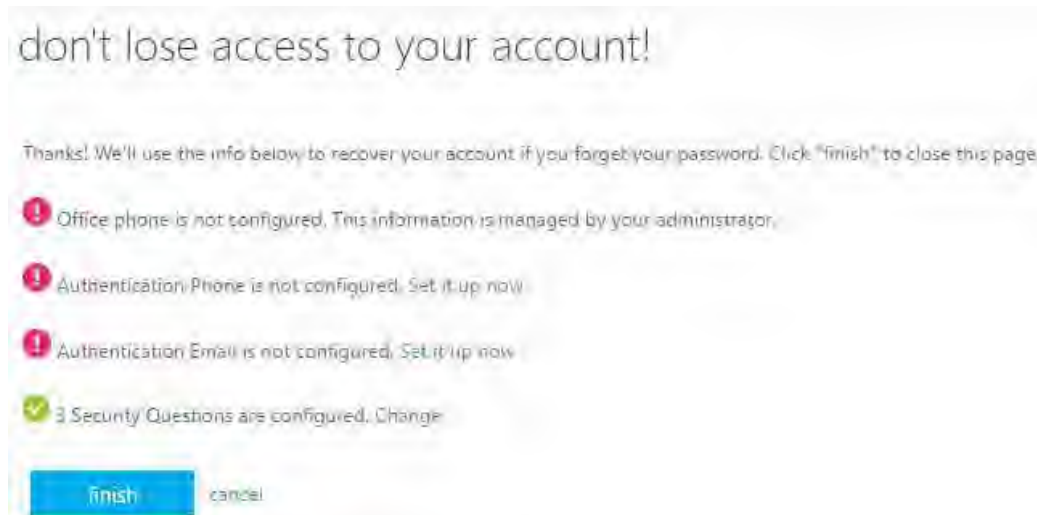
10. Once you have setup your questions,
- Click **Save Answers**.

Steps / Screenshots

It will take you back to the main account information screen.

There should be a green check mark next to the method you verified.

- Click **Finish**.



11. It should log you into to your Outlook email.

You can view your mailbox.

If that is not the option you see, you may see this page on your right instead.

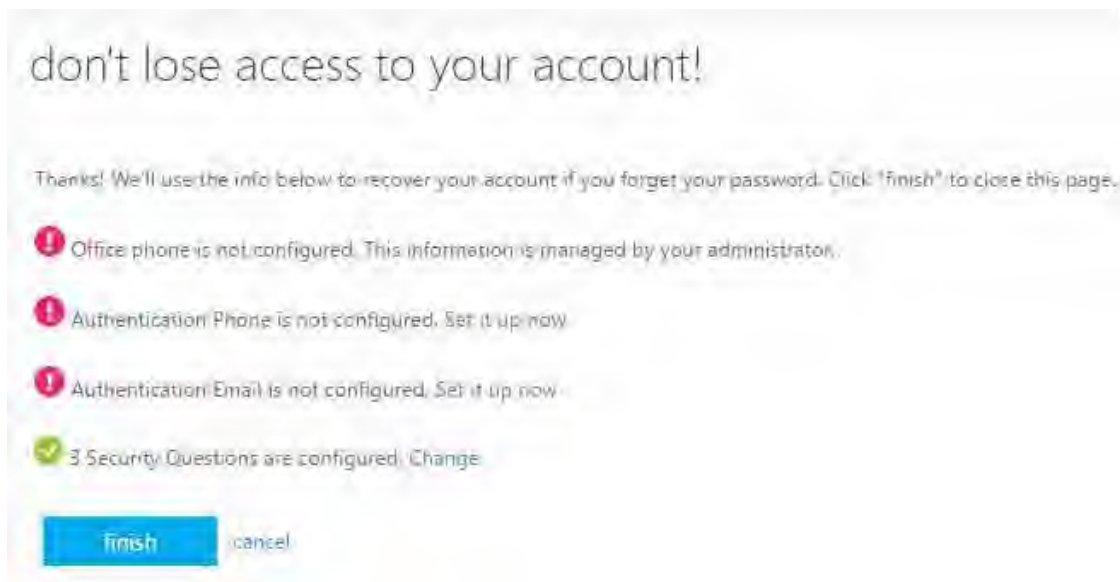
If you do → Select an option.

It will log you into your Outlook email.



Steps / Screenshots

12. This screen below will appear every 180 days to verify that the information you put in is still current.



13. If you wish to change these questions or answers → access the link below to go directly to the webpage to change them.

<https://go.microsoft.com/fwlink/?LinkId=309629&tenantIdentifier=db21de5d-bc9c-420c-8f3f-8f08f85b5ada>

14. With this in place, you now have two ways to reset your password.

A) On the main login screen, if you input your password wrong, you will see an error item with the ability for you to hit the “Forgot your password?” link.

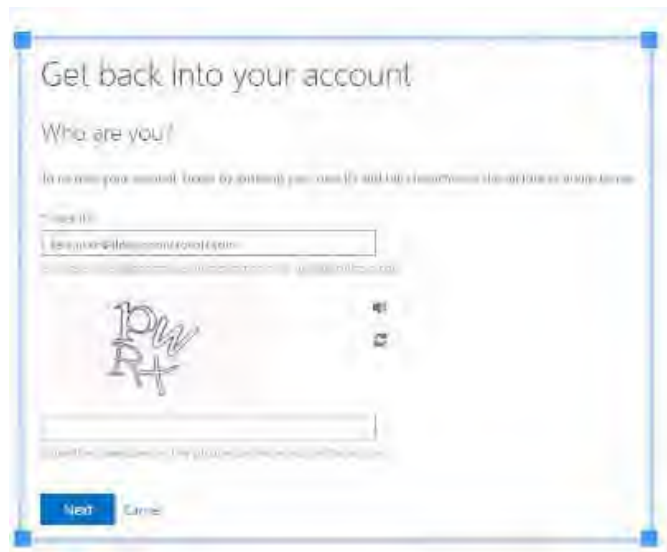


B) Go directly to the link for password resets which is located below:

<https://passwordreset.microsoftonline.com/>

Steps / Screenshots

15. Once you are on the password reset screen,
- Enter your User ID (login) and the text box captcha code.

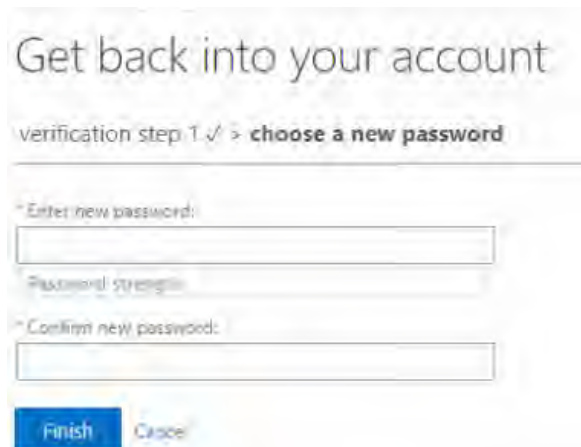


16. After entering a valid User ID and Captcha code,
- You will be taken to the account verification screen.

Input the security identifier that you have chosen (In this case security questions).



17. You will then be taken to the choose new password screen.
- Enter a new password which you will use to login:



OUTLOOK MOBILE SETUP

Steps / Screenshots

1. Locate the Outlook Mail app within the Google Play Store or the Apple App Store.

- Download and install the app.
- Click Get Started once you have launched the app.



2. Click **Add Account**.



3. Fill in your FDOT email account.

Click **Continue**.



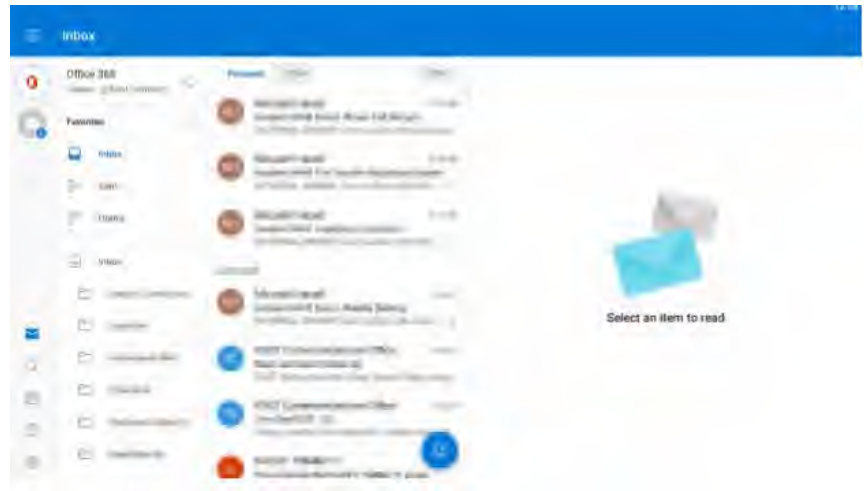
4. Fill in your account password.



Steps / Screenshots

5. Once your password has been entered, you will be redirected over to your mailbox as the messages start loading onto your device.

If you need additional support, you should open a support ticket.



EMAIL BACK-UP AND RECOVERY

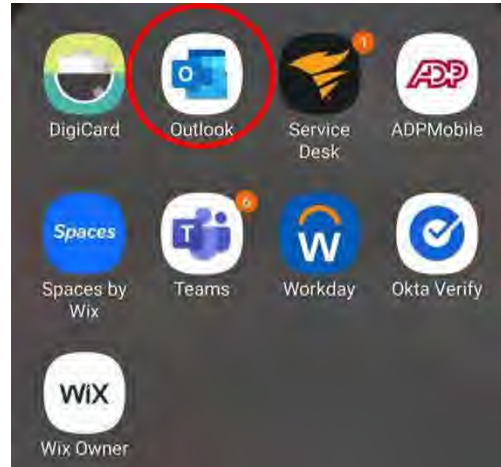
All email functionality and backup and recovery options reside with FDOT Central Office OIT.

REMOVE DOT EMAIL FROM SIRV PHONES

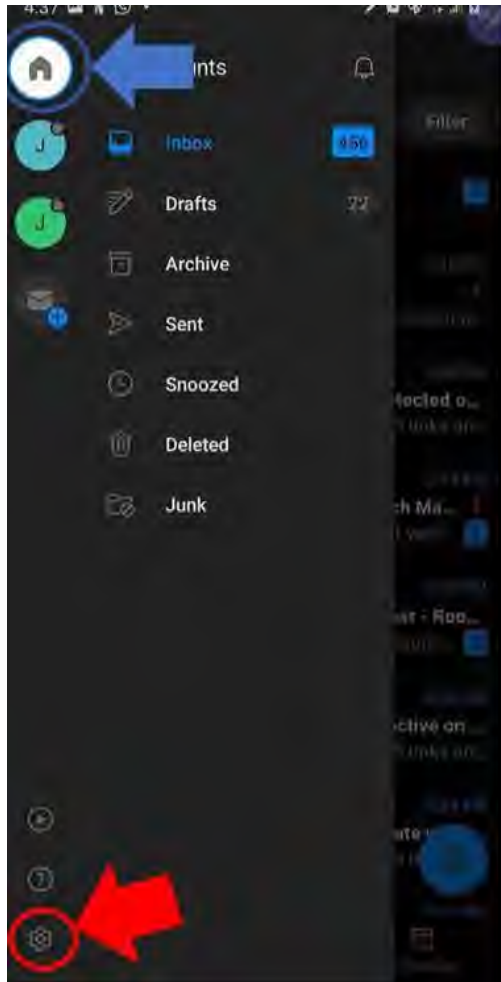
Remove DOT Email from XP8 Phones as following:

Steps / Screenshots

1. Open Outlook on your device.

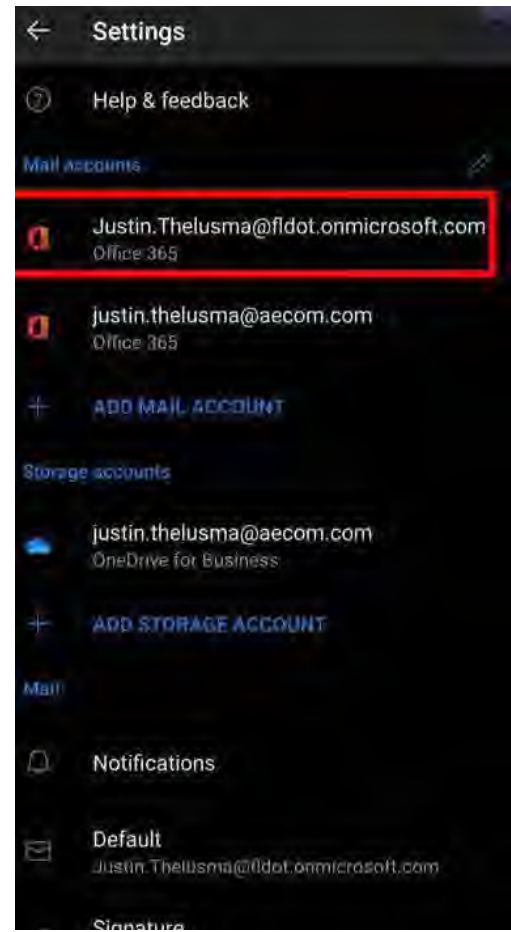


2. Select the Home Icon in the top left corner and press the settings button in the bottom left corner



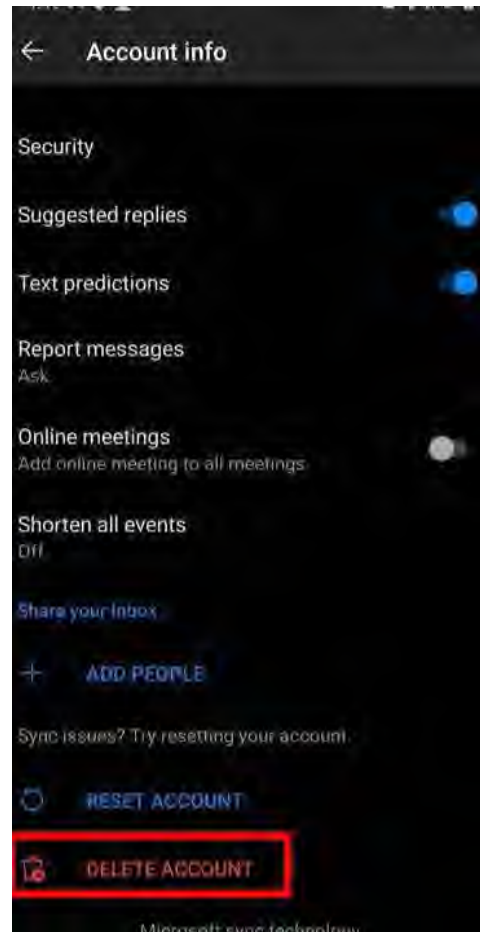
Steps / Screenshots

3. Select the account that needs to be deleted.



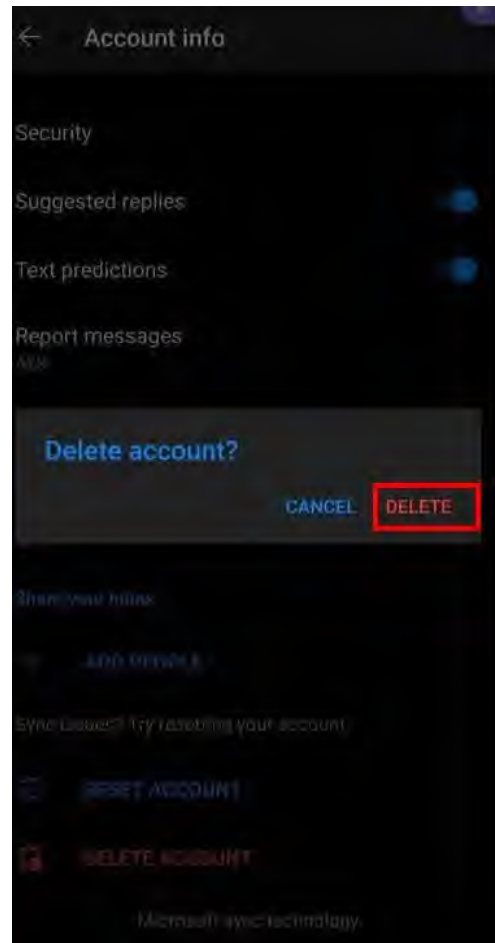
Steps / Screenshots

4. Scroll down to the bottom of this page and press the delete button.



Steps / Screenshots

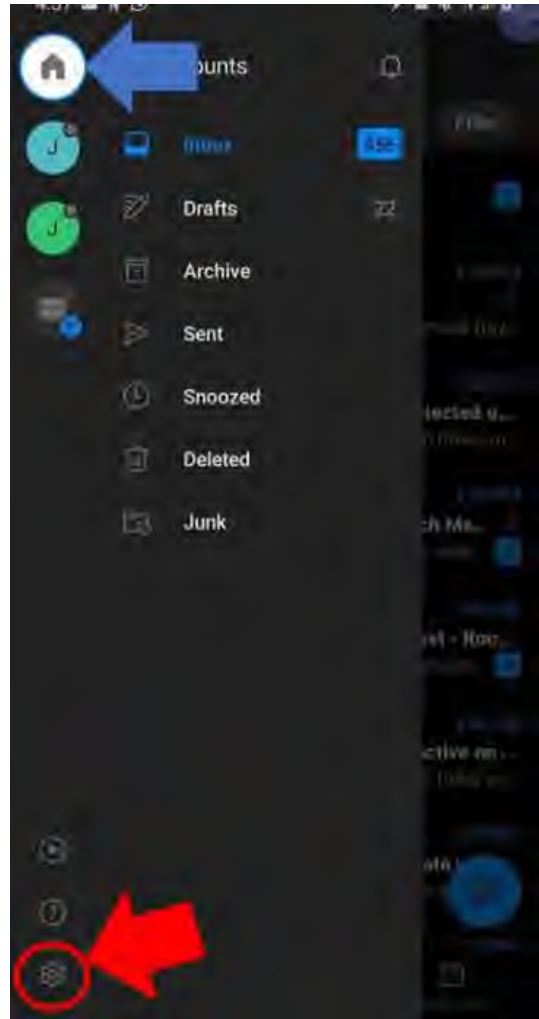
5. Press the delete button a second time when prompted.



Now the account has been removed, RESTART THE DEVICE then add the email back to outlook.

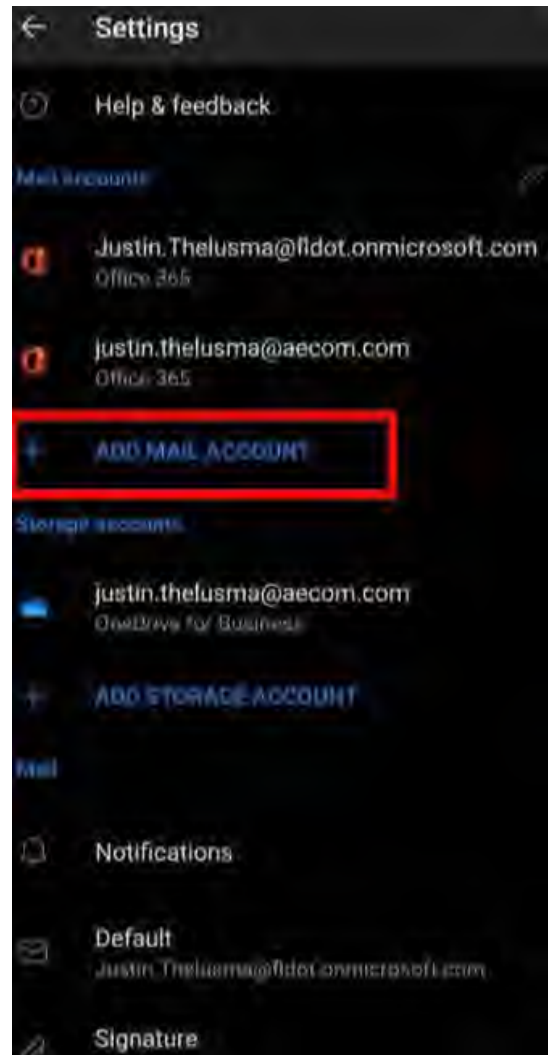
Steps / Screenshots

6. Add the email back to Outlook by returning to the settings



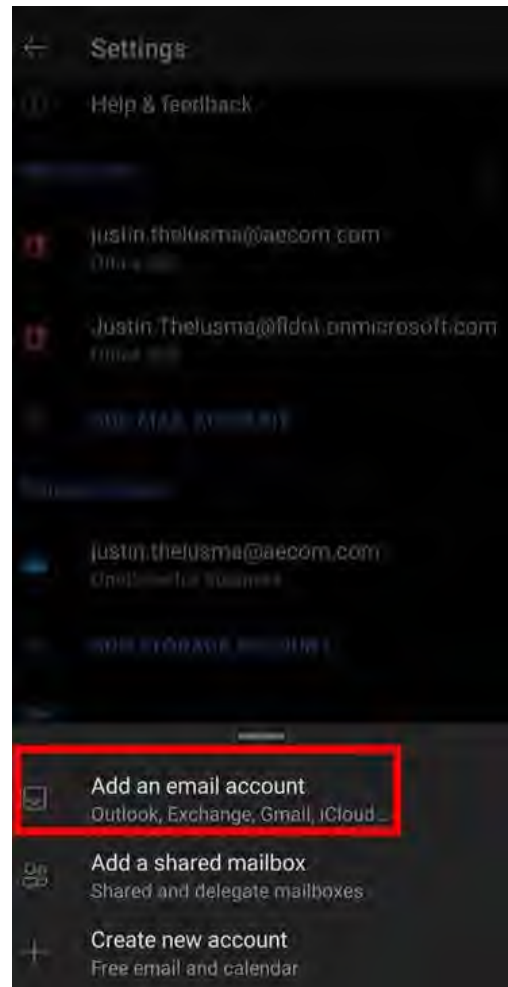
Steps / Screenshots

7. Press the add email button



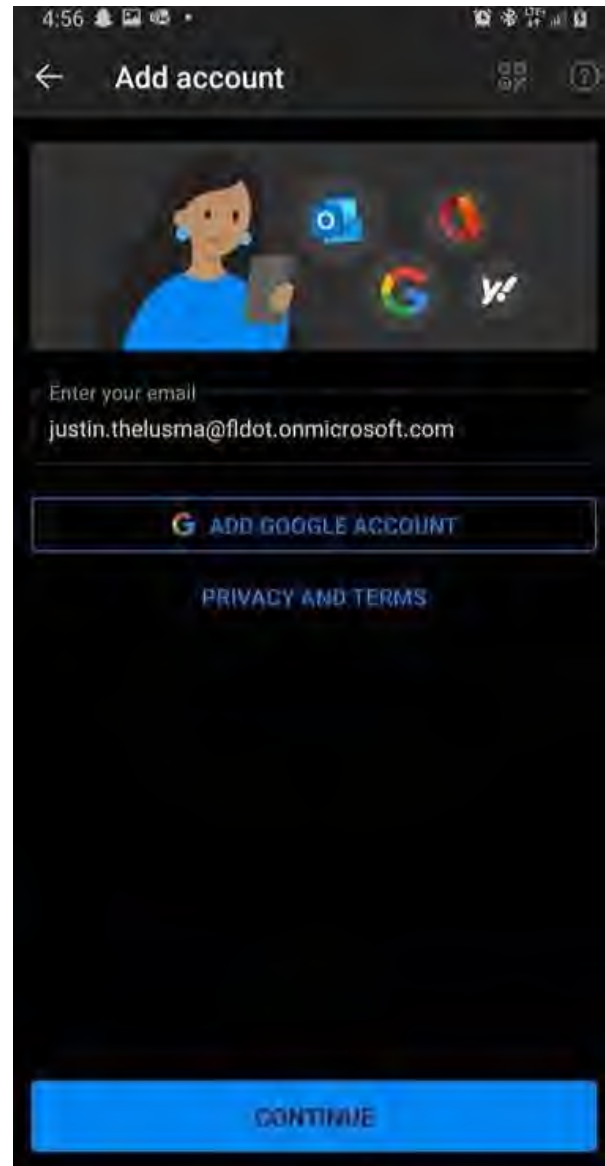
Steps / Screenshots

8. Select **Add an email account**



Steps / Screenshots

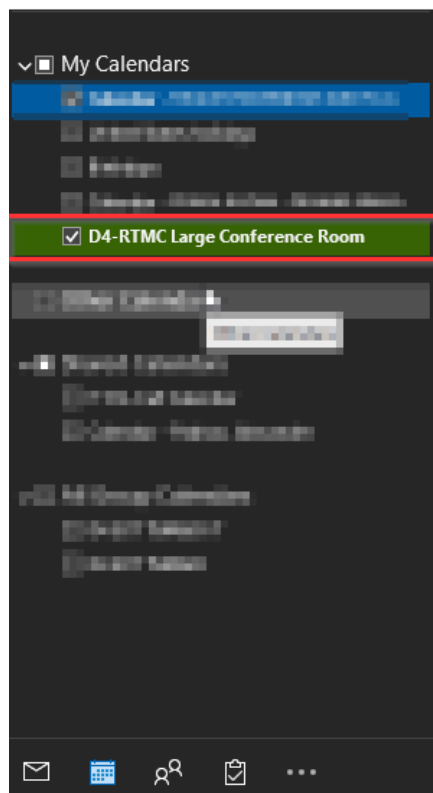
9. Input your DOT email address. The format is Firstname.Lastname@fldot.onmicrosoft.com



After inputting your password, the process is complete, and your email should be back on your phone. If you have any questions or concerns during this process, please call the IT help desk at 954-847-2733.

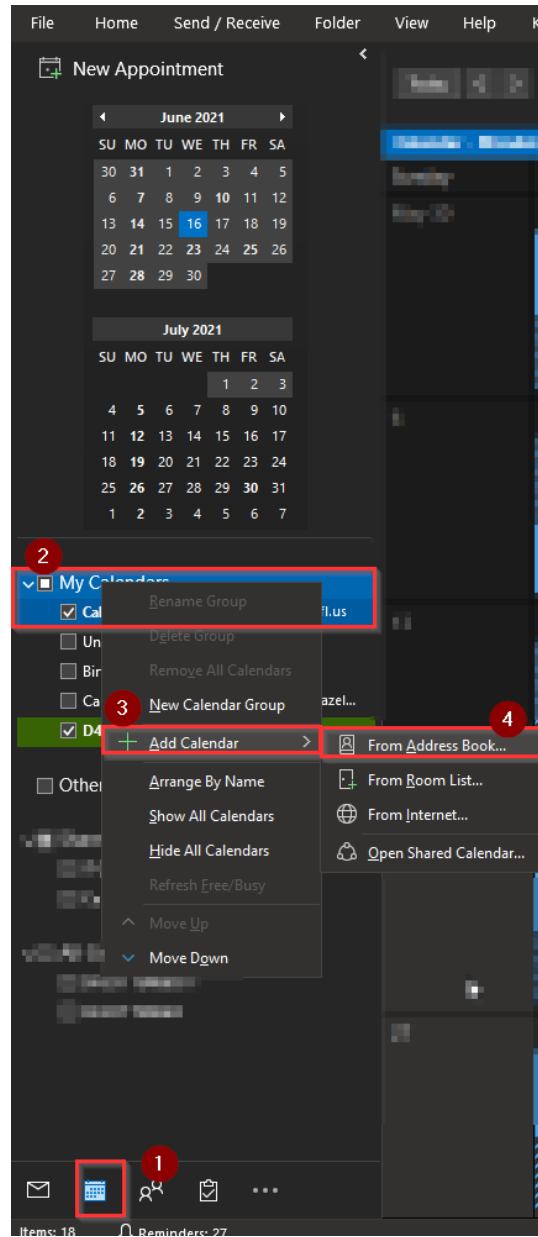
VIEW MEETINGS IN THE LARGE CONFERENCE ROOM

You should now see **"D4-RTMC Large Conference Room"**



1. First navigate to outlook and select the calendar icon lower left-hand corner of the application
2. Right click **My Calendars**.
3. Select **Add Calendar**.

4. Select "From Address Book"





7.08 Physical Security

Table of Contents

OVERVIEW	4
Physical Security Devices	4
Physical Security Applications	4
PHYSICAL SECURITY DEVICES & VMWARE INVENTORY	5
MAINTENANCE OF SYSTEMS	6

Document History

Version #	Date	Author	Changes
1.0	02/28/2024	Yana Neishlos	Initial Draft
1.1	5/23/2024	William Murray	Document Revision

OVERVIEW

In District 4, several solutions exist to manage the physical security of buildings and structures that contain ITS infrastructure. These solutions can be found in the RTMC, TIMSO, Roadside Hubs, ITS Cabinets, Eland Office, and Lake Worth FHP. This SOP will outline the existing solutions managed by the RTMC IT Department and the relevant workflows involving third parties such as ITS Maintenance.

Physical Security Devices

Axis Camera	Network video dome cameras are used for surveillance of assets at all locations.
Room Alert Device	IT and facilities environment monitoring hardware.
ARXYS Server	Physical server (host) that contains virtual servers.
CyberKey Vault	Cabinet, which programs and dispenses electronic keys with customized access privileges based on time, date, and authority level.
Web Authorizer	Communication devices that serve as the interface between CyberLock hardware and CyberAudit management software.

Physical Security Applications

Boring Lab	The Boring Toolbox is an extension of Milestone XProtect Management client to perform bulk operational maintenance support service.
CyberLock	An electronic access control system that manages lock access permissions with auditing capability.
Milestone	Milestone XProtect video management software manages IP cameras and digital video recordings.
Room Alert Manager	Management solution to discover and monitor Room Alert devices.

PHYSICAL SECURITY DEVICES & VMWARE INVENTORY

Due to the sensitivity of the information in this document, it is only accessible by IT personnel at the following link: [7.08 Physical Security_SD.pdf](#)

Sensitive documents, such as 7.08 Physical Security are placed in

[District 4 TSM&O Collaboration Portal \(Partner Site\) - PDF - IT Documents - ListView \(sharepoint.com\)](#)

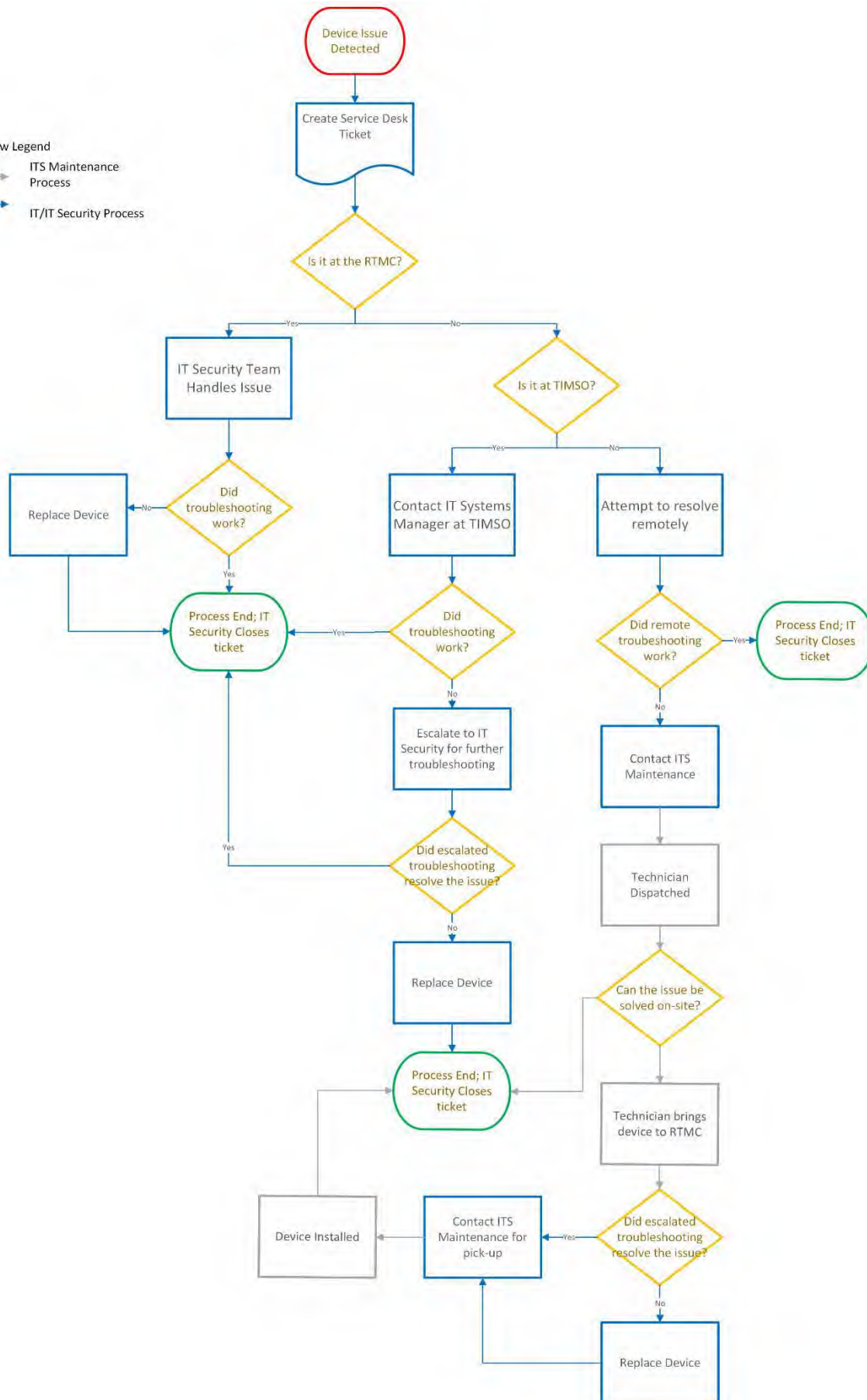
folder.

MAINTENANCE OF SYSTEMS

Due to the various locations of these systems, the RTMC IT Department relies heavily on ITS Maintenance personnel to troubleshoot, install, and remove Room Alert devices, CyberLock Web Authorizers, CyberLocks, and Security Cameras.

An example scenario for a maintenance request is like the following:

1. The IT Security Team notices a Room Alert device is no longer reporting environment data.
2. The IT Security Team contacts ITS Maintenance while simultaneously creating a Service Desk ticket.
3. ITS maintenance responds and dispatches a technician to troubleshoot.
4. If the technician can rectify the issue, no further action will be taken.
5. If the issue is not resolved on-site, the device will be brought to the RTMC to be further troubleshot by the IT Security Team.
6. Upon successfully completing further troubleshooting, IT Security contacts ITS maintenance again for retrieval.
7. A technician picks up the device and installs it in its original location.
8. Functionality is verified, and the ticket is then closed.





7.09 Broward RTMC

Table of Contents

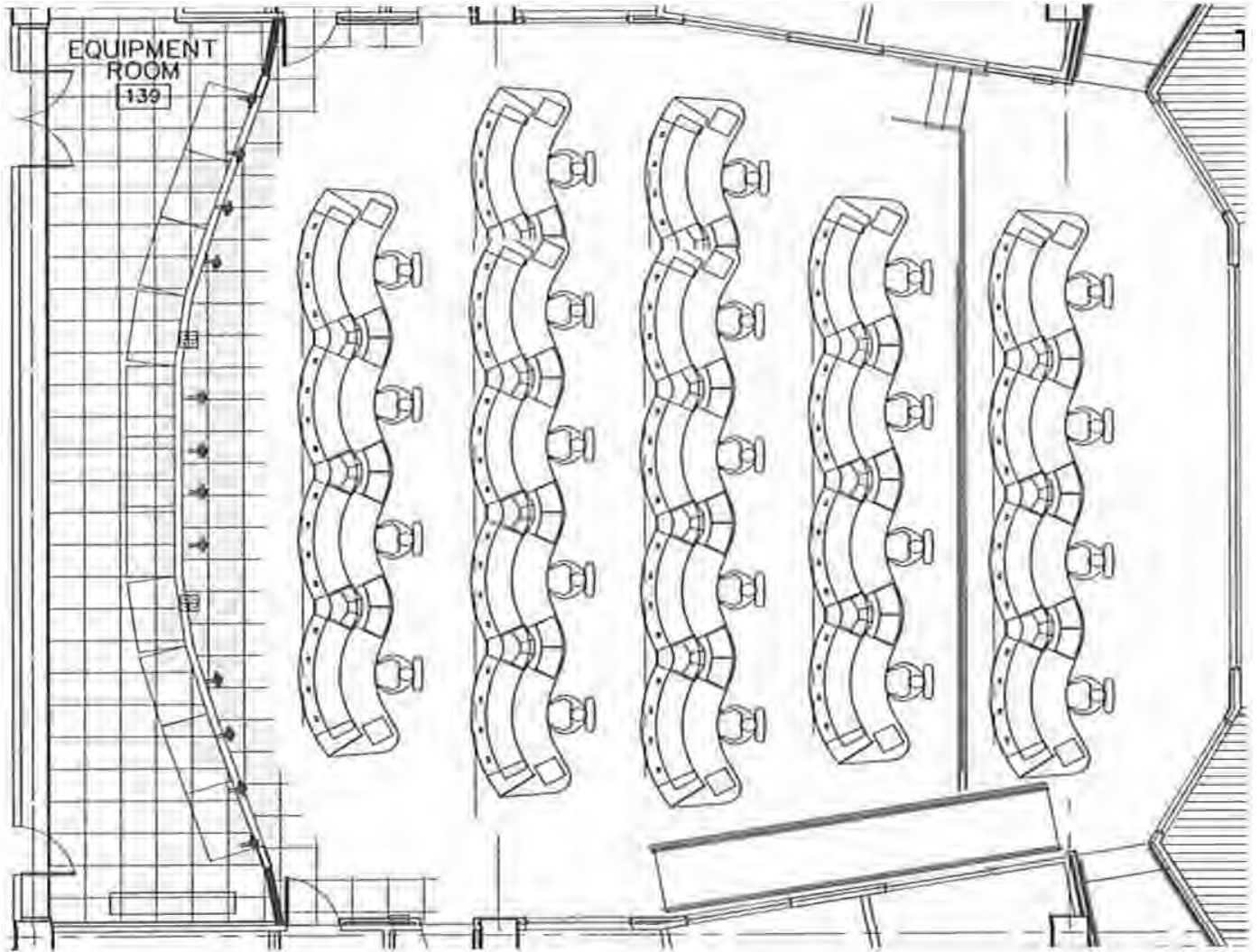
Version #	Date	Author	Changes
1.0	12/20/2023	Yana Neishlos	Initial Draft

Table of Contents

CONTROL ROOM	4
CONTROL ROOM CNNECTIONS	5
SHARING SPACE AT THE RTMC	15
Access.....	15
Housekeeping for Shared Spaces.....	15
Organization.....	15
Behind the video wall.....	15

CONTROL ROOM

The Control Room, FDOT section is divided into twenty-two (22) consoles total. Sixteen (16) of which having access to both SunGuide and Office network.



CONTROL ROOM CNNECTIONS

le	Device Connected	Console Port #	Closet Patch Panel # / Port #	4507 Blade # / Port #	3750 Port #
#001	SG PC	217	Patch 2 / Port 1	B6/P1	
#001	C2	218	Patch 2 / Port 2	B6/P2	
#001	C3	219	Patch 2 / Port 3	B6/P3	
#001	Vbrick	220	Patch 2 / Port 4	B6/P4	
#001	NONE	221	Patch 2 / Port 5	B6/P5	
#001	Joystick / MOXA	222	Patch 2 / Port 6	B6/6	
#001	NONE	223	Patch 2 / Port 25	N/A	
#001	NONE	224	Patch 2 / Port 26	N/A	
#001	NONE	225	Patch 2 / Port 27	N/A	
#001	NONE	226	Patch 2 / Port 28	N/A	
#001	NONE	227	Patch 2 / Port 29	N/A	
#001	Office PC	228	Patch 2 / Port 30	N/A	G1/0/1
#002	Joystick / MOXA	229	Patch 2 / Port 7	B6/P13	
#002	Smart Extender	230	Patch 2 / Port 8	B6/P14	
#002	Clear	231	Patch 2 / Port 9	B6/P15	
#002	C3	232	Patch 2 / Port 10	B6/P16	
#002	C2	233	Patch 2 / Port 11	B6/P17	

le	Device Connected	Console Port #	Closet Patch Panel # / Port #	4507 Blade # / Port #	3750 Port #
#002	SG	234	Patch 2 / Port 12	B6/P18	
#002	NONE	235	Patch 2 / Port 31		
#002	NONE	236	Patch 2 / Port 32		
#002	BARCO TEST	237	Patch 2 / Port 33	N/A	G1/0/8
#002	IT300002P	238	Patch 2 / Port 34	N/A	G1/0/7
#002	IT300003P	239	Patch 2 / Port 35	N/A	G1/0/6
#002	Office PC	240	Patch 2 / Port 36	N/A	G1/0/2
#003	BC	BC	BC	BC	BC
#004	BC	BC	BC	BC	BC
#005	SG	157	Patch 1 / Port 25	B7/P13	
#005	C2	158	Patch 1 / Port 26	B7/P14	
#005	C3	159	Patch 1 / Port 27	B7/P15	
#005	Vbrick	160	Patch 1 / Port 28	B7/P16	
#005	NONE	161	Patch 1 / Port 29	B7/P17	
#005	JoyStick / MOXA	162	Patch 1 / Port 30	B7/P18	
#005	NONE	163	Patch 1 / Port 31	N/A	
#005	NONE	164	Patch 1 / Port 32	N/A	
#005	NONE	165	Patch 1 / Port 33	N/A	

le	Device Connected	Console Port #	Closet Patch Panel # / Port #	4507 Blade # / Port #	3750 Port #
#005	NONE	166	Patch 1 / Port 34	N/A	
#005	Office PC	167	Patch 1 / Port 35	N/A	G1/0/11
#005	HPLaserJet 400	168	Patch 1 / Port 36	N/A	G1/0/10
#006	NONE	169	Patch 1 / Port 1	B7/P1	
#006	SG	170	Patch 1 / Port 2	B7/P2	
#006	C3	171	Patch 1 / Port 3	B7/P3	
#006	C2	172	Patch 1 / Port 4	B7/P4	
#006	Vbrick	173	Patch 1 / Port 5	B7/P5	
#006	MOXAM	174	Patch 1 / Port 6	B7/P6	
#006	NONE	175	Patch 1 / Port 7	N/A	
#006	NONE	176	Patch 1 / Port 8	N/A	
#006	NONE	177	Patch 1 / Port 9	N/A	
#006	NONE	178	Patch 1 / Port 10	N/A	
#006	NONE	179	Patch 1 / Port 11	N/A	
#006	Office PC	180	Patch 1 / Port 12	N/A	G1/0/9
#007	NONE	181	Patch 1 / Port 13	B7/P25	
#007	SG	182	Patch 1 / Port 14	B7/P26	
#007	C2	183	Patch 1 / Port 15	B7/P27	

le	Device Connected	Console Port #	Closet Patch Panel # / Port #	4507 Blade # / Port #	3750 Port #
#007	C3	184	Patch 1 / Port 16	B7/P28	
#007	Vbrick	185	Patch 1 / Port 17	B7/P29	
#007	MOXAM	186	Patch 1 / Port 18	B7/P30	
#007	NONE	187	Patch 1 / Port 19	N/A	
#007	NONE	188	Patch 1 / Port 20	N/A	
#007	NONE	189	Patch 1 / Port 21	N/A	
#007	NONE	190	Patch 1 / Port 22	N/A	
#007	NONE	191	Patch 1 / Port 23	N/A	
#007	Office PC	192	Patch 1 / Port 23	N/A	G1/0/17
#008	BC	BC	BC	BC	BC
#009	BC	BC	BC	BC	BC
#010	NONE	97	Patch 2 / Port 13	B6/P25	
#010	JoyStick / MOXA	98	Patch 2 / Port 14	B6/P26	
#010	Vbrick	99	Patch 2 / Port 15	B6/P27	
#010	C3	100	Patch 2 / Port 16	B6/P28	
#010	SG	101	Patch 2 / Port 17	B6/P29	
#010	C2	102	Patch 2 / Port 18	B6/P30	
#010	NONE	103	Patch 2 / Port 19	N/A	

le	Device Connected	Console Port #	Closet Patch Panel # / Port #	4507 Blade # / Port #	3750 Port #
#010	NONE	104	Patch 2 / Port 20	N/A	
#010	NONE	105	Patch 2 / Port 21	N/A	
#010	NONE	106	Patch 2 / Port 22	N/A	
#010	NONE	107	Patch 2 / Port 23	N/A	
#010	Office PC	108	Patch 2 / Port 24	N/A	G1/0/19
#011	C2	109	Patch 4 / Port 19	B3/P37	
#011	SG	110	Patch 4 / Port 20	B3/P38	
#011	C3	111	Patch 4 / Port 21	B3/P39	
#011	NONE	112	Patch 4 / Port 22	B3/P40	
#011	Vbrick	113	Patch 4 / Port 23	B3/P41	
#011	JoyStick / MOXA	114	Patch 4 / Port 24	B3/P42	
#011	NONE	115	Patch 4 / Port 43	N/A	
#011	NONE	116	Patch 4 / Port 44	N/A	
#011	NONE	117	Patch 4 / Port 45	N/A	
#011	NONE	118	Patch 4 / Port 46	N/A	
#011	NONE	119	Patch 4 / Port 47	N/A	
#011	Office PC	120	Patch 4 / Port 48	N/A	G1/0/20
#012	C2	121	Patch 4 / Port 13	B3/P25	

le	Device Connected	Console Port #	Closet Patch Panel # / Port #	4507 Blade # / Port #	3750 Port #
#012	C3	122	Patch 4 / Port 14	B3/P26	
#012	SG	123	Patch 4 / Port 15	B3/P27	
#012	Vbrick	124	Patch 4 / Port 16	B3/P28	
#012	NONE	125	Patch 4 / Port 17	B3/P29	
#012	JoyStick / MOXA	126	Patch 4 / Port 18	B3/P30	
#012	NONE	127	Patch 4 / Port 37	N/A	
#012	NONE	128	Patch 4 / Port 38	N/A	
#012	NONE	129	Patch 4 / Port 39	N/A	
#012	NONE	130	Patch 4 / Port 40	N/A	
#012	NONE	131	Patch 4 / Port 41	N/A	
#012	Office PC	132	Patch 4 / Port 42	N/A	G1/0/18
#013	BC	BC	BC	BC	BC
#014	BC	BC	BC	BC	BC
#015	SG	49	Patch 4 / Port 1	B3/P1	
#015	C1	50	Patch 4 / Port 2	B3/P2	
#015	C2	51	Patch 4 / Port 3	B3/P3	
#015	NONE	52	Patch 4 / Port 4	B3/P4	
#015	NONE	53	Patch 4 / Port 5	B3/P5	

le	Device Connected	Console Port #	Closet Patch Panel # / Port #	4507 Blade # / Port #	3750 Port #
#015	JoyStick / MOXA	54	Patch 4 / Port 6	B3/P6	
#015	NONE	25	Patch 4 / Port 25	N/A	
#015	NONE	26	Patch 4 / Port 26	N/A	
#015	NONE	27	Patch 4 / Port 27	N/A	
#015	NONE	28	Patch 4 / Port 28	N/A	
#015	NONE	29	Patch 4 / Port 29	N/A	
#015	Office PC	30	Patch 4 / Port 30	N/A	G1/0/3
#016	C2	61	Patch 3 / Port 7	B4/P13	
#016	SG	62	Patch 3 / Port 8	B4/P14	
#016	C1	63	Patch 3 / Port 9	B4/P15	
#016	Vbrick	64	Patch 3 / Port 10	B4/P16	
#016	NONE	65	Patch 3 / Port 11	B4/P17	
#016	JoyStick / MOXA	66	Patch 3 / Port 12	B4/P18	
#016	NONE	67	Patch 3 / Port 31	N/A	
#016	NONE	68	Patch 3 / Port 32	N/A	
#016	NONE	69	Patch 3 / Port 33	N/A	
#016	NONE	70	Patch 3 / Port 34	N/A	
#016	NONE	71	Patch 3 / Port 35	N/A	
#016	Office PC	72	Patch 3 / Port 36	N/A	G1/0/22

le	Device Connected	Console Port #	Closet Patch Panel # / Port #	4507 Blade # / Port #	3750 Port #
#017	JoyStick / MOXA	73	Patch 1 / Port 37	B7/P37	
#017	SG	74	Patch 1 / Port 38	B7/P38	
#017	Vbrick	75	Patch 1 / Port 39	B7/P39	
#017	NONE	76	Patch 1 / Port 40	B7/P40	
#017	NONE	77	Patch 1 / Port 41	B7/P41	
#017	NONE	78	Patch 1 / Port 42	B7/P42	
#017	NONE	79	Patch 1 / Port 43	N/A	
#017	NONE	80	Patch 1 / Port 44	N/A	
#017	NONE	81	Patch 1 / Port 45	N/A	
#017	NONE	82	Patch 1 / Port 46	N/A	
#017		83	Patch 1 / Port 47	N/A	G1/0/15
#017	Office PC	84	Patch 1 / Port 48	N/A	G1/0/16
#018	595	595	595	595	595
#019	C3	1	Patch 3 / Port 1	B4/P1	
#019	SG	2	Patch 3 / Port 1	B4/P2	
#019	C2	3	Patch 3 / Port 1	B4/P3	
#019	NONE	4	Patch 3 / Port 1	B4/P4	

le	Device Connected	Console Port #	Closet Patch Panel # / Port #	4507 Blade # / Port #	3750 Port #
#019	NONE	5	Patch 3 / Port 1	B4/P5	
#019	JoyStick / MOXA	6	Patch 3 / Port 1	B4/P6	
#019	NONE	7	Patch 3 / Port 25	N/A	
#019	NONE	8	Patch 3 / Port 26	N/A	
#019	NONE	9	Patch 3 / Port 27	N/A	
#019	NONE	10	Patch 3 / Port 28	N/A	
#019	Printer HP1600	11	Patch 3 / Port 29	N/A	G1/0/5
#019	Office PC	12	Patch 3 / Port 30	N/A	G1/0/4
#020	C2	13	Patch 3 / Port 13	B4/P25	
#020	SG	14	Patch 3 / Port 14	B4/P26	
#020	C3	15	Patch 3 / Port 15	B4/P27	
#020	Vbrick	16	Patch 3 / Port 16	B4/P28	
#020	NONE	17	Patch 3 / Port 17	B4/P29	
#020	JoyStick / MOXA	18	Patch 3 / Port 18	B4/P30	
#020	NONE	19	Patch 3 / Port 37	N/A	
#020	NONE	20	Patch 3 / Port 38	N/A	
#020	NONE	21	Patch 3 / Port 39	N/A	
#020	NONE	22	Patch 3 / Port 40	N/A	

le	Device Connected	Console Port #	Closet Patch Panel # / Port #	4507 Blade # / Port #	3750 Port #
#020	NONE	23	Patch 3 / Port 41	N/A	G1/0/23
Closet	Office PC	24	Patch 3 / Port 42	N/A	G1/0/24
#021	595	595	595	595	595
#022	595	595	595	595	595

SHARING SPACE AT THE RTMC

Access

We share space at the RTMC with Broward County and other groups. Therefore, IT staff members require workspaces and shared areas free of clutter, and never use equipment (such as tables and carts) that don't belong to us.

There are three shared spaces that affect IT:

- Server room (room 166).
- Behind the video wall (room 139).
- Telephone room (room 159/160).

The telephone equipment in room 159 is the demarcation for ISP's. This room is not to be used by the IT staff, except in the case of connecting to any of the equipment there. Any connection to the AT&T or CrownCastle equipment may only be done through the access hole in wall. A telephone contractor who needs access to the room must be always accompanied by an IT employee. Equipment in room 160 belongs to the IT group, but the room is also shared with Broward County.

In the large server room (166), only the four rows of server racks on the north side belong to the RTMC, including tables along the northwest corner. Except for the electrical panel in the room, the IT group should never enter the space that belongs to Broward County.

Beyond the main server room is the radio room, which contains a shared rack of radios. Equipment is stored in the cabinets along the east wall, which belongs exclusively to the IT group.

The following staff members have key card access to these rooms:

- FDOT Staff.
- AECOM IT and Maintenance Staff.
- Broward County Traffic Engineering Staff.
- 595 Express IT Staff.

If an outside contractor needs access to a server or telephone room, follow FDOT policy regarding visitors. Approved guests must be always accompanied by a member of the IT staff.

Housekeeping for Shared Spaces

Organization

Keeping shared spaces organized is important for the safety of employees and security of equipment; respect for those who share the space; and professional appearance.

These are the expectations set forth by the FDOT. These areas will be inspected on a regular basis with a report going to the IT Manager and ITS Operations Manager.

Behind the video wall

Keep the floor and carts always clear in this room. All loose equipment must be stored in the cabinet where it belongs.

Server Room

- Area must be kept clean and organized.
- Food is not allowed.

- Boxes and trash cannot be stored. Full trash containers will be placed outside the server room for county maintenance staff to empty.
- Equipment must be stored in cabinets behind video wall, not left in the server room.
- At all times, the corridor space along the wall along the east side must remain completely open, to give access to Broward users.
- No equipment should ever be left on the open shelves across from the cabinets in the radio room.



7.10 Vista Center

Table of Contents

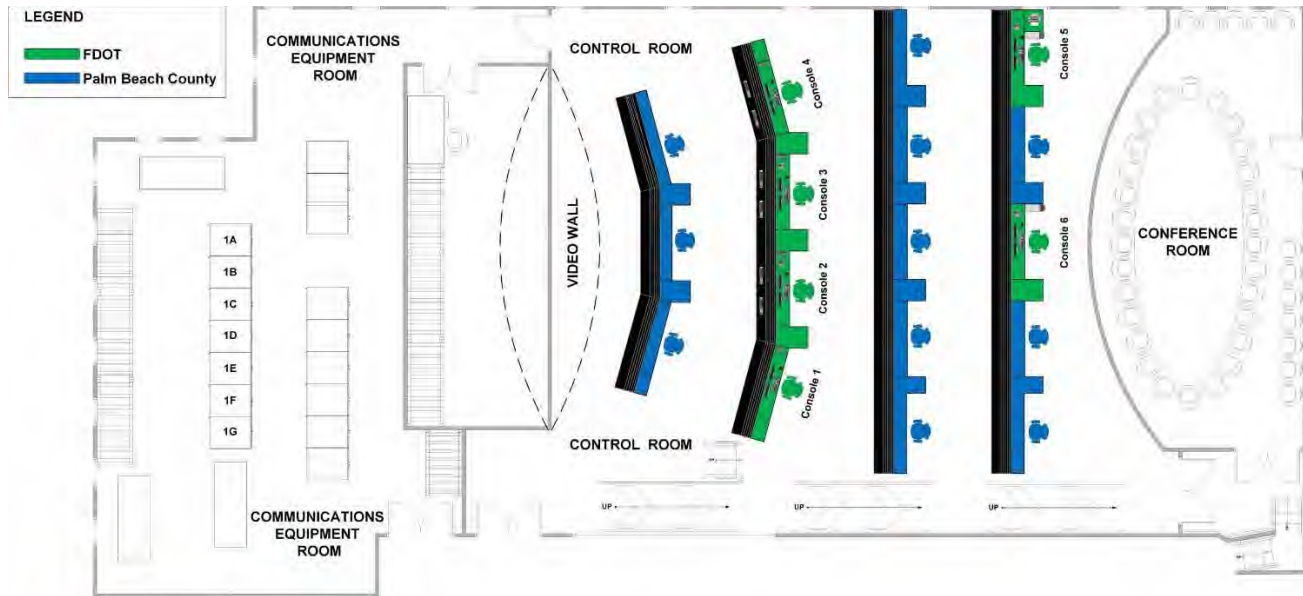
Version #	Date	Author	Changes
1.0	12/20/2023	Yana Neishlos	Initial Draft

Table of Contents

CONTROL ROOM.....	4
ITS CENTER.....	5

CONTROL ROOM

The Vista Center Control Room is used as a work area for the Palm Beach Maintenance and IT Department. The second row from the main screen contains equipment directly attached to the RTMC and two of the workstations in the fourth row are used by RTMC Operations. All other items within the control room are not used by FDOT.



ITS CENTER

Click on the link below to view the Floor Plan.

[7.10.01 ITS Center \(sharepoint.com\)](#)



7.11 Treasure Coast TMC

Document History

Version #	Date	Author	Changes
1.0	12/20/2023	Yana Neishlos	Initial Draft

Table of Contents

TREASURE COAST TMC	4
TSM&O BUILDING AND OPERATIONS CENTER BUILDING CABLE CONNECTIONS.....	5

TREASURE COAST TMC

FDOT D4 TSM&O utilizes the Traffic Incident Management Support Office (TIMSO) facility located at 3601 Oleander Avenue, Fort Pierce, FL, 34982 as a backup TMC to the Broward RTMC, which is approximately 100 miles away.

TIMSO is designed for limited FDOT D4 TSM&O ITS Operations in case of a catastrophic event, containing a Data Center equipped with a High Availability (HA) duplicate system and networking equipment. The critical computer system and network equipment at TIMSO are connected to the building UPS and generator for redundant power. IT Staff is responsible for bringing TIMSO to a state of readiness, as instructed by the Crisis Assessment Team (CAT).

The CAT members list is maintained by the RTMC Operations Manager. Upon determination by the CAT that the Broward RTMC is closed due to a major emergency, staff will report to TIMSO. RTMC operations will be run from the TIMSO control room with redundant SunGuide software that will support CCTV, DMS, and HAR. Operators will be assigned a console and monitors for CCTV control. TIMSO workstations will duplicate many functions and abilities of the Broward RTMC.

Click on the link below to view the floor plan:

[7.11.00 Treasure Coast TMC \(sharepoint.com\)](#)

TSM&O BUILDING AND OPERATIONS CENTER BUILDING CABLE CONNECTIONS

Due to the sensitivity of the information included in this document, it is only accessible by IT personnel at the following link: [DOCX File viewer | Microsoft Teams](#).



7.14 Server Room Physical Devices

Document History

Version #	Date	Author	Changes
1.0	2/27/2024	Yana Neishlos	Initial Draft

Table of Contents

RTMC PHYSICAL SERVERS4

OTHER RTMC SERVER ROOM PHYSICAL DEVICES6

VISTA CENTER PHYSICAL SERVERS7

TIMSO PHYSICAL SERVERS8

OTHER TIMSO SERVER ROOM PHYSICAL DEVICES10

Server Name	Serial #	Asset Tag	Make	Model	Rack #	Purpose	Operating System	Apps	SAN or Internal Storage	Warranty Exp.
TMCVHOSTDMZ01	2M291606N0	HW329768	HP	DL380 G10	3C	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
TMCVHOSTDMZ02	2M291606N8	HW329772	HP	DL380 G10	3C	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
TMCVHOSTDMZ03	2M290902QX	HW334616	HP	DL380 G10	3C	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
TMCVHOSTDMZ04	2M290902QN	HW334615	HP	DL380 G10	3C	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
LABHOST01	MXQ5290136	HW333350	HP	DL380 G9	3C	VMware Host (Lab)	VMware ESXi, 8.0.1	N/A	Internal	EXPIRED
LABHOST02	MXQ54906CW	HW333354	HP	DL380 G9	3C	VMware Host (Lab)	VMware ESXi, 8.0.1	N/A	Internal	EXPIRED
TMCVHOSTSGAPP01	MXQ24407Y6	HW406536	HP	DL380 G10	3D	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	12/4/2025
TMCVHOSTSGAPP02	MXQ24407Y7	HW406537	HP	DL380 G10	3D	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	12/4/2025
TMCVHOSTSGAPP03	MXQ24407Y8	HW406535	HP	DL380 G10	3D	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	12/4/2025
TMCVHOST01	2M291301ZL	HW329769	HP	DL380 G10	3E	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
TMCVHOST02	2M291606N9	HW329764	HP	DL380 G10	3E	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
TMCVHOST03	2M2920034G	HW329770	HP	DL380 G10	3E	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
TMCVHOST04	2M291606N6	HW329765	HP	DL380 G10	3E	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
TMCVHOST05	2M291606N4	HW329766	HP	DL380 G10	3E	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
TMCVHOST06	2M291606N3	HW329767	HP	DL380 G10	3E	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
TMCVHOST07	2M291606N5	HW329771	HP	DL380 G10	3E	VMware Host	VMware ESXi, 7.0.3	N/A	SAN	5/23/2024
D4SG09	USE121N93T	HW340196	HP	DL380 G7	3H	SELS	Windows Server 2012	SunGuide	Internal	EXPIRED
D4SG10	USE121N94Z	HW340197	HP	DL380 G7	3H	SELS	Windows Server 2012	SunGuide	Internal	EXPIRED

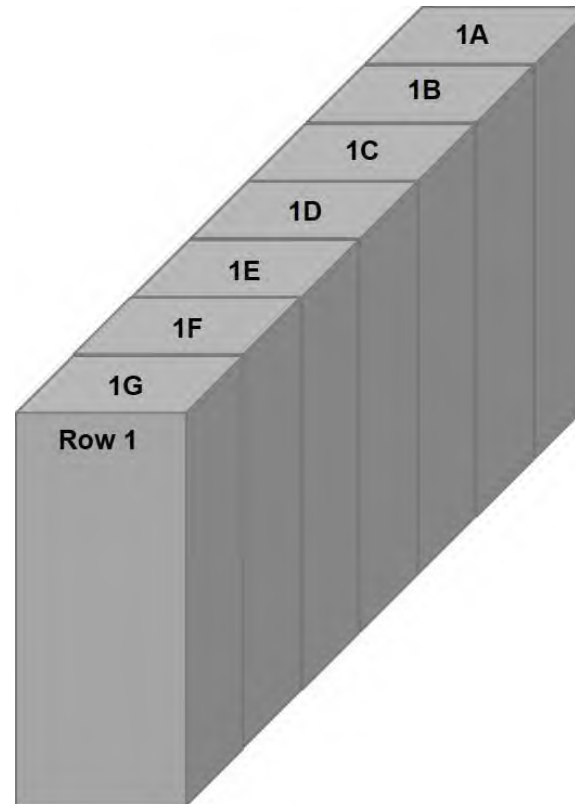
OTHER RTMC SERVER ROOM PHYSICAL DEVICES

Device	Device Name	Serial #	Asset Tag	Make	Model	# of Ports	Transfer Speed	Rack #	Storage	Warranty Exp.
SAN	XIOTMC02	FNM00180201292	HW306574	DELL EMC	EXTREM IO SAN	N/A	N/A	3G	N/A	1/10/2025
SAN	RTMC-PowerStoreSAN	1BB0BD3	HW399861	DELL EMC	PowerStore 1000T	N/A	N/A	3G	N/A	5/13/2024
SAN	TMC-EXAGRID	AVTA223106392	HW406488	Exagrid	084TSN22	N/A	N/A	3G	N/A	10/4/2025

VISTA CENTER PHYSICAL SERVERS

The figure on the right provides a visual representation of the Vista Center server room racks.

There is one row with seven racks, labeled A-G. All Vista Center physical servers are in rack 1B.

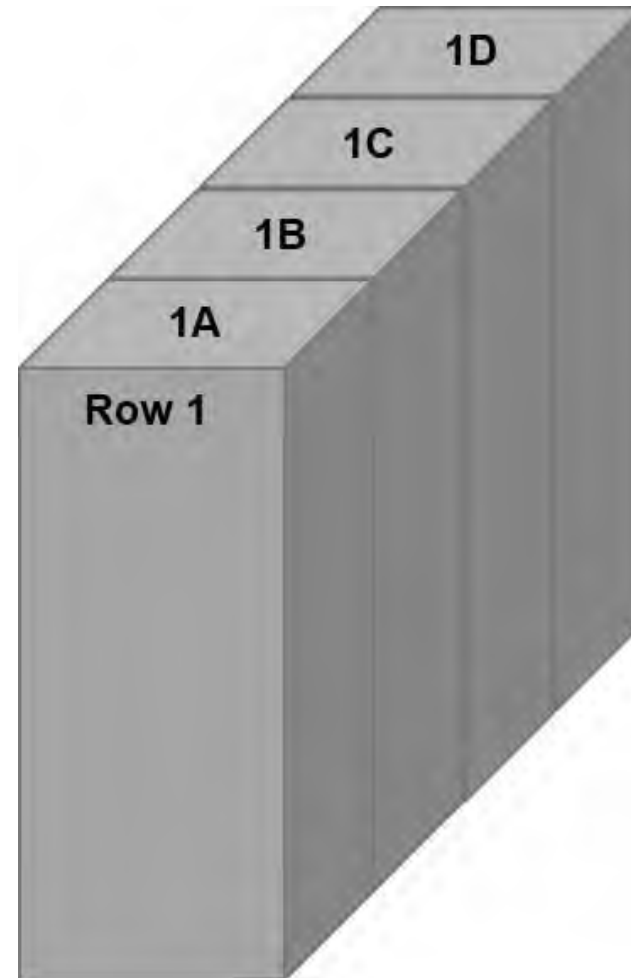


Server Name	Serial #	Asset Tag	Make	Model	Rack #	Purpose	Operating System	Apps	SAN or Internal Storage	Warranty Exp.
VISVHOST01	MXQ11713SW	HW399585	HP	DL360 G10	1B	Host	VMware ESXi, 7.0.3	N/A	Internal	8/1/2024
VISVHOST02	MXQ11713SV	HW399589	HP	DL360 G10	1B	Host	VMware ESXi, 7.0.3	N/A	Internal	8/1/2024
VISVHOST03	MXQ11713ST	HW399857	HP	DL360 G10	1B	Host	VMware ESXi, 7.0.3	N/A	Internal	8/1/2024
FVISVHUT01	2M293501Z9	HW334145	HP	DL360 G10	1B	Backup	VMware ESXi, 7.0.3	N/A	Internal	EXPIRED

TIMSO PHYSICAL SERVERS

The figure below provides a visual representation of the TIMSO server room racks. There is one row with four racks, labeled A-D.

All TIMSO physical servers are in rack # 1D.



Server Name	Serial #	Asset Tag	Make	Model	Rack #	Purpose	Operating System	Apps	SAN or Internal Storage	Warranty Exp.
TIMVHOST01	MXQ11712T9	HW399868	HP	DL360 G10	1C	Host	VMware ESXi, 7.0.3	N/A	Internal	7/31/2024
TIMVHOST02	MXQ11712T6	HW399866	HP	DL360 G10	1C	Host	VMware ESXi, 7.0.3	N/A	Internal	7/31/2024
TIMVHOST03	MXQ11712T7	HW399869	HP	DL360 G10	1C	Host	VMware ESXi, 7.0.3	N/A	Internal	7/31/2024
TIMVHOST04	MXQ11712T4	HW399865	HP	DL360 G10	1C	Host	VMware ESXi, 7.0.3	N/A	Internal	7/31/2024
TIMVHOST05	MXQ11712T5	HW399867	HP	DL360 G10	1C	Host	VMware ESXi, 7.0.3	N/A	Internal	7/31/2024
TIMVHOST06	MXQ11712T8	HW399870	HP	DL360 G10	1C	Host	VMware ESXi, 7.0.3	N/A	Internal	7/31/2024
FTIMPHDB02	2M29090319	HW334421	HP	DL380 G10	1D	SQL	Windows 2016	SQL	Internal	6/10/2022
FTIMVHUT02	MXQ63002V5	HW306336	HP	DL380 G9	1D	Backup	VMware ESXi, 7.0.3	Unitrends	Internal	9/30/2022

OTHER TIMSO SERVER ROOM PHYSICAL DEVICES

Device	Device Name	Serial #	Asset Tag	Make	Model	# of Ports	Transfer Speed	Rack #	Storage	Warranty Exp.
SAN	TIMSO-PowerStoreSAN	1BBZ9D3	HW399862	DELL	PowerStore 1000T	N/A	N/A	1C	N/A	5/13/2024
SAN	TIMSO-EXAGRID	AVTA223106389	HW406489	EXAGRID	084TSN22	N/A	N/A	1C	N/A	10/4/2025



7.15 Networks

Document History

Version #	Date	Author	Changes
1.0	2/28/2024	Yana Neishlos	Initial Draft

Table of Contents

NETWORKS4

- Overview4
- Network Devices4
- Network Devices Application4

NETWORKS – PHYSICAL DEVICES and VMWARE.....5

- RTMC Network Devices5
- RTMC Network VMs10
- Vista Center Network Devices10
- TIMSO Network Devices11
- HUB Buildings Network Devices12
- Network Devices at D4 HQ, Lake Worth, Powerline, Palm Beach Operations, and ELAND13
- AMS Hub Devices14

NETWORKS – CRITICAL SYSTEMS.....16

- Critical Network Devices16
- Critical Physical Servers16
- Critical VMs17

NETWORKS

Note. Due to the sensitivity of the information in this document, it is only accessible by IT personnel at the following link: [7.15 Networks SD.pdf](#).

Sensitive documents, such as “Networks” are placed in

[District 4 TSM&O Collaboration Portal \(Partner Site\) - IT Documents - ListView \(sharepoint.com\)](#).

Overview

There are network devices in place at the RTMC, TIMSO, Vista Center, HUB buildings, D4 HQ, Lake Worth, Powerline, and ELAND. A list of all network devices and application used in each location is provided in this SOP Section.

Network Devices

Cisco Adaptive Security Appliance (ASA)	Security device that combines firewall, antivirus, intrusion prevention, and VPN capabilities.
Cisco Router	Provides intent-based networking for the WAN, LAN, and cloud. Guides and directs network data, using packets that contain various data types.
Cisco Switch	Facilitates the sharing of resources by connecting all computers, wireless access points, printers, and servers on the network.
Wireless LAN Controllers	Manages wireless network access points for wireless devices connecting to the network.

Network Devices Application

Cisco Unified Communications Manager (CUCM)	Private Branch Exchange (PBX) application that provides call control and session management.
---	--

NETWORKS – PHYSICAL DEVICES and VMWARE

RTMC Network Devices

Device	Serial #	Model #	Asset Tag	Location	Rack #	Warranty Exp.
Cisco Switch	FGE21502Z7F	Cisco C6807-XL	HW378519	Server Room	2B	9/1/2020
Cisco Switch	FGE21492Y95	Cisco C6807-XL	HW378520	Server Room	2D	9/1/2022
Cisco Switch	FXS2422Q2JU	Cisco C9407R (X86)	HW329972	Server Room	1E	12/2/2030
Cisco Switch	JAE242625EB	C9200L-48P-4X	HW329775	Server Room	1F	10/7/2030
Cisco Switch	JAE242625DJ	C9200L-48P-4X	HW329776	Server Room	1F	10/7/2030
Cisco Switch	JAE242625NT	C9200L-48P-4X	HW329773	Server Room	1F	10/7/2030
Cisco Switch	JAE242625EN	C9200L-48P-4X	HW329774	Server Room	1F	10/7/2030
Cisco Switch	JAE242608WV	C9200L-48T-4X	HW329805	Server Room	1F	10/6/2030
Cisco Switch	JAE242608LR	C9200L-48T-4X	HW329850	Server Room	1F	10/5/2030

Device	Serial #	Model #	Asset Tag	Location	Rack #	Warranty Exp.
Cisco Switch	FOC2426L8J3	C9500-40X	HW329870	Control Room	N/A	10/25/2030
Cisco Switch	FOC2428L0N8	C9500-40X	HW329871	Control Room	N/A	10/25/2030
Cisco Switch	JAE242622BP	C9200L-48T-4X	HW329804	Server Room	3E	10/6/2030
Cisco Switch	JAE242608MS	C9200L-48T-4X	HW329802	Server Room	3F	10/6/2030
Cisco Switch	JAE24252KAU	C9200L-48T-4X	HW329848	Server Room	3G	10/5/2030
Cisco Switch	FOC2422R1C3	N3K-C3172TQ-10GT	HW329854	Server Room	3E	10/16/2021
Cisco Switch	FOC2422R1AB	N3K-C3172TQ-10GT	HW329856	Server Room	3E	10/16/2021
Cisco Switch	FOC2422R18L	N3K-C3172TQ-10GT	HW329852	Server Room	3E	10/16/2021
Cisco Switch	FOC2422R197	N3K-C3172TQ-10GT	HW329853	Server Room	3E	10/16/2021
Cisco Switch	FOC2422R0JH	N3K-C3172TQ-10GT	HW329865	Server Room	3E	9/26/2021

Device	Serial #	Model #	Asset Tag	Location	Rack #	Warranty Exp.
Cisco Switch	FOC2422R0KU	N3K-C3172TQ-10GT	HW329866	Server Room	3E	9/26/2021
Cisco ASA	FCH21477EJU (FTX2201W0Y B)	ASA5545	HW315970	IT Phone Room	1B	12/28/2022
Cisco ASA	FCH21477ELG (FTX2201W0Y D)	ASA5545	HW315969	TIMSO	1A	12/28/2022
Cisco Wireless Controller	FCH2419L0DW	AIR-CT5520-K9	HW329806	Server Room	3G	10/14/2023
Cisco BE7K	WMP242200NS	BE7M-M5-K9	HW329867	Server Room	3D	10/27/2023
Cisco BE7K	WMP242200NN	BE7M-M5-K9	HW329868	Server Room	3D	10/27/2023
Cisco Switch	JAE24252K7X	C9200L-48T-4X	HW329849	Server Room	1H	10/5/2030
Cisco Switch	JAE24252K4W	C9200L-48T-4X	HW329847	Server Room	1H	10/5/2030

Device	Serial #	Model #	Asset Tag	Location	Rack #	Warranty Exp.
Cisco Secure Network Server	WZP24180KM7	SNS-3615-K9	HW329885	Server Room	3E	TBD
Cisco Router	FLM242611RV	ISR4461/K9		Server Room	2B	1/1/2021
Cisco Switch	FOC2421L928	WS-C3560CX-12PD-S	HW329831	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L97L	WS-C3560CX-12PD-S	HW329832	Control Room	N/A	9/25/2030
Cisco Switch	FOC2506L2DZ	WS-C3560CX-12PD-S	IT300440	Control Room	N/A	
Cisco Switch	FOC2421L95H	WS-C3560CX-12PD-S	HW329833	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L936	WS-C3560CX-12PD-S	HW329830	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L91Y	WS-C3560CX-12PD-S		Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L921	WS-C3560CX-12PD-S	HW329839	Control Room	N/A	9/25/2030

Device	Serial #	Model #	Asset Tag	Location	Rack #	Warranty Exp.
Cisco Switch	FOC2421L90K	WS-C3560CX-12PD-S	HW329836	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L92K	WS-C3560CX-12PD-S	HW329844	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L930	WS-C3560CX-12PD-S	HW329827	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L94Q	WS-C3560CX-12PD-S	HW329841	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L91U	WS-C3560CX-12PD-S	HW329840	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L942	WS-C3560CX-12PD-S	HW329829	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L92W	WS-C3560CX-12PD-S	HW329843	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L8YP	WS-C3560CX-12PD-S	HW329828	Control Room	N/A	9/25/2030
Cisco Switch	FOC2421L92C	WS-C3560CX-12PD-S	HW329835	Control Room	N/A	9/25/2030
Cisco Switch	JAE242628HV	C9200L-48T-4X	HW329803	Server Room	1D	10/6/2030

Device	Serial #	Model #	Asset Tag	Location	Rack #	Warranty Exp.
Cisco Switch	JAE24221ZVT	C9200L-24T-4X	HW329810	Server Room	3C	10/7/2030
Cisco Router	FLM242611S0	ISR4461/K9		Server Room	3C	1/1/2021

RTMC Network VMs

Note. The VMs below are sitting on physical machines (RTMC-BE7K1 and RTMC-BE7K2).

Virtual Server Description	Application
CUCM Publisher	CUCM
CUCM Subscriber	CUCM
CUCM Subscriber	CUCM

Vista Center Network Devices

Device	Serial #	Model #	Asset Tag	Location	Rack #	Warranty Exp.
Cisco Switch	FXS2422Q2DB	C9407R	HW329971	Vista Center	1A	12/2/2030

TIMSO Network Devices

Device	Serial #	Model #	Asset Tag	Location	Rack #	Warranty Exp.
Cisco Switch	FXS2422Q2D9	C9407R	HW329970	TIMSO	1A	12/2/2030
Cisco Router	FJC2428D10H	ISR4451-X/K9	HW329874	TIMSO	1A	1/14/2021
Cisco Wireless Controller	FCH2419L08X	AIR-CT5520-K9	HW329845	TIMSO	1A	10/14/2023
Cisco Secure Network Server	WZP24180KLW	SNS-3615-K9	HW329886	TIMSO	1A	
Cisco BE7K	WMP242200NW	BE7M-M5-K9	HW329869	TIMSO	1A	10/27/2023
Cisco Switch	FOC2422R18N	N3K-C3172TQ-10GT	HW329851	TIMSO	1C	10/16/2021
Cisco Switch	FOC2422R18M	N3K-C3172TQ-10GT	HW329855	TIMSO	1C	10/16/2021
Cisco Switch	FOC2413U09P	C9300-24UB-E		TIMSO	1C	9/30/2030
Cisco Switch	FOC2511R0F5	N3K-C3172TQ-10GT	HW399879	TIMSO	1C	5/27/2022
Cisco Switch	FOC2527R2DE	N3K-C3172TQ-10GT	HW399916	TIMSO	1C	10/23/2022

HUB Buildings Network Devices

Device	Serial #	Model #	Location	Warranty Exp.
Cisco Switch	FXS2435Q0VG	C9606R	Airport/I-95/ I-595 Hub	1/30/2031
Cisco Switch	FXS2431Q159	C9606R	Turnpike/I-595 Hub	12/12/2030
Cisco Switch	FXS2431Q156	C9606R	I-75 Hub	12/12/2030
Cisco Switch	FXS2440Q006	C9606R	Turnpike/Hillsboro Hub	4/2/2031
Cisco Switch	FXS2431Q14V	C9606R	Miramar Hub	12/12/2030
Cisco Switch	FXS2431Q158	C9606R	I-95/Hollywood Hub	12/12/2030
Cisco Switch	FXS2431Q15D	C9606R	I-95/Commercial Hub	12/12/2030
Cisco Switch	FXS2435Q0VP	C9606R	PGA BLVD	1/27/2031
Cisco Switch	FXS2435Q0VN	C9606R	Atlantic Avenue	1/27/2031
Cisco Switch	FXS2431Q15N	C9606R	N3C Hub 3 / Fellsmere Road	12/12/2030
Cisco Switch	FXS2431Q157	C9606R	N3C Hub 2 / Okeechobee Road	12/12/2030
Cisco Switch	FXS2431Q14T	C9606R	N3C Hub 1 / Kanner Highway	12/12/2030

Device	Serial #	Model #	Location	Warranty Exp.
Cisco Switch	FGE224856YF	C6807-XL	I-95/Palmetto Hub	

Network Devices at D4 HQ, Lake Worth, Powerline, Palm Beach Operations, and ELAND

Device	Serial #	Model #	Asset Tag	Location	Warranty Exp.
Cisco Router	FLM242611RX	ISR4461/K9		ELAND	1/1/2021
Cisco Switch	FOC2413U096	C9300-24UB-E		ELAND	9/30/2030
Cisco Switch	FOC2426W00S	C9300-48UB-E		ELAND	10/6/2030
Cisco Switch	FOC2413U09Y	C9300-24UB		Powerline FDOT	9/30/2030
Cisco Switch	FOC2114Z28R	WS-C2960CX	IT300424	Powerline FDOT	
Cisco Switch	FOC2413U09U	C9300-24UB	IT300435	Palm Beach Operations	9/30/2030
Cisco Router	FLM242611RY	ISR4461/K9		Lake Worth	1/1/2021

Device	Serial #	Model #	Asset Tag	Location	Warranty Exp.
Cisco Switch	JAE24410SNS	C9200L-24T-4X		Lake Worth	TBD
Cisco Router	FLM242611RZ	ISR4461/K9		D4 HQ	1/1/2021
Cisco Switch	FCW2412D0E0	C9300-24UB-E		D4 HQ	9/30/2030
Cisco Switch	JAE24221G6T	C9200L-24T-4X	HW32981 1	D4 HQ	10/7/2030
Cisco Switch	FOC26357W3 5	C9200L-24P-4X	HW4064 92	D4 HQ	
Cisco Switch	FOC2635807T	C9200L-24P-4X	HW4064 91	D4 HQ	
Cisco Switch	FOC2638BJ6G	C9200L-48P-4X	HW4064 71	D4 HQ	

AMS Hub Devices

Device	Serial #	Model #	Location	Warranty Exp.
Cisco Switch	FXS2443Q2BE	C9606R	Oakland Park Blvd/441	1/20/2022
Cisco Switch	FXS2440Q049	C9606R	US1/Oakland Park Blvd	1/21/2022

Device	Serial #	Model #	Location	Warranty Exp.
Cisco Switch	FXS2443Q2F3	C9606R	University Drive/Broward	1/20/2022
Cisco Switch	FXS2443Q2DZ	C9606R	Sunrise/441	1/20/2022
Cisco Switch	FXS2440Q00K	C9606R	Sunrise/US1	1/21/2022
Cisco Switch	FXS2441Q0L9	C9606R	Griffin Rd/441	3/17/2031
Cisco Switch	FXS2444Q0Y3	C9606R	University Drive/Pines Blvd	4/8/2031
Cisco Switch	FXS2431Q16G	C9606R	Hollywood/US1	12/12/2030
Cisco Switch	FXS2431Q14S	C9606R	Hallandale/441	12/12/2030

NETWORKS – CRITICAL SYSTEMS

This SOP Section describes what happens if failure occurs on the network devices listed below, which include switches, physical servers, and VMs that are essential to the operations of D4 TSM&O.

Critical Network Devices

Network Device Name	If the RTMC Network Device Fails
RTMC	The in-house field core network consists of two Cisco 6807-XL switches with Virtual Switching Systems (VSS) setup. The Control Room, SunGuide, and the field side connect to these two core switches. If they go down, the RTMC network goes down and becomes isolated.
OfficeCore	All office PCs connect to this switch, which cross connects to the two switches above. If it goes down, internet and email access will be lost.
ASA5545	ASA5545 (backup ASA firewall) takes over.
WLC5520	WLC5520 backup wireless controller WLC5520 takes over.
ITSWAN-4661	D4 will be isolated. The other Districts/Central Office will not see us.

Critical Physical Servers

The RTMC manages an Enterprise Phone System utilizing a Cisco Call Manager Multi-Site. The phone system consists of three Cisco BE7K servers (two in the RTMC and one in TIMSO), which provide the phone calls for the Operators and office users at TIMSO, Vista, Lake Worth, Powerline, Palm Beach Operations, and Eland.

The phone system also includes two Primary Rate Interface (PRI) circuits (one AT&T at the RTMC and one Comcast at TIMSO) for redundancy. The RTMC utilizes a dedicated PRI line strictly for voice, along with over 100 DID numbers for the primary circuit at the RTMC, with a secondary PRI line with 20 DID numbers at TIMSO.

Critical VMs

Note. The VMs below are sitting on physical servers.

VM Name / Description	IF VM Fails
CUCM Publisher	In case of a potential crash, the Publisher on the CUCM must be manually shut down. With the two CUCM Subscribers up and running, the CUCM will keep working, but no changes can be made.

Florida Department of Transportation
DISTRICT FOUR TSM&O REGIONAL TRANSPORTATION MANAGEMENT CENTER
STANDARD OPERATING PROCEDURES

IT

Software Whitelists

Software Request Form for Desktops

7.16.01

OVERVIEW

A list of all whitelisted software, including the version number and vendor for FDOT D4 TSM&O desktops is provided at the end of this form. Personnel that require any other software not whitelisted to do their job, must complete a software request form and submit it for approval.

SOFTWARE REQUEST DETAILS

1. **Employee Printed Name:**
- a. **Title:**
- b. **Email:**
- c. **Department:**
- d. **Supervisor:**
2. **Software Name:**
- a. **Expected Software Use:**
- b. **Software Vendor/Developer:**
- c. **Operating System Compatibility:**
- d. **Third Party Plugin/Software Requirement:**
- e. **Third Party Plugin/Software Vendor:**
- f. **Software Support Maintenance Partner:**

Employee Signature: _____

Date: _____

Florida Department of Transportation
DISTRICT FOUR TSM&O REGIONAL TRANSPORTATION MANAGEMENT CENTER
STANDARD OPERATING PROCEDURES

IT

Software Whitelists

Software Request Form for Desktops

7.16.01

SOFTWARE REQUEST FORM APPROVAL PROCESS

1. The requester completes and submits the software request form to the RTMC IT Support Manager via email for review and to approve or deny the request.
 - a. If the software request is denied, the RTMC IT Support Manager notifies the requester via email.
 - b. If approved, the RTMC IT Support Manager submits the software request form to the TSM&O IT Manager for review and to approve or deny the request.
 - (1) If the software request is denied, the TSM&O IT Manager notifies the requester via email.
 - (2) If approved, the TSM&O IT Manager submits the software request form to the TSM&O Resource Manager for final review and to approve or deny the request.
 - (a) If the software request is denied, the TSM&O Resource Manager notifies the requester via email.
 - (b) If approved, the TSM&O Resource Manager notifies the group (requester, RTMC IT Support Manager, and the TSM&O IT Manager) via email of the final status of the software request.
2. The requestor submits the approved software request form to the IT Department via email.
3. The IT Department contacts the requestor to schedule the software installation.

Florida Department of Transportation
DISTRICT FOUR TSM&O REGIONAL TRANSPORTATION MANAGEMENT CENTER
STANDARD OPERATING PROCEDURES

IT

Software Whitelists

Software Request Form for Desktops

7.16.01

SOFTWARE WHITELIST FOR DESKTOPS

Software	Version	Vendor
7-Zip	22.01 and later	7-Zip
Access Rights Manager	21.4.1.3	SolarWinds
Acrobat Reader	22.002.20191 and later	Adobe
AMD Software	22.8.2	Advanced Micro Devices, Inc.
AVTECH Device Discover Utility	4.3.2 and later	AVTECH Software
Barco DisplayAgent		Barco
Barco ProServer		Barco
Barco Sidebar	3.10.0.0117 and later	Barco
Cisco AnyConnect Secure Mobility Client	4.10.05111	Cisco Systems
Cisco ASDM-IDM	1.9.02	Cisco Systems
Cisco Webex Meetings	42.8.4 and later	Cisco Systems
CyberLink	2.21.3	Videx Inc.
Dameware Mini Remote Control	12.2.3 and later	SolarWinds
daVinci Resolve	18.0.10003	Blackmagic Design
DYMO ID	1.4.658.45027 and later	Sanford, L.P.
Folder Sizes	9.5 and later	Key Metric Software
Google Chrome	105.0.5195.54 and later	Google LLC
Greenshot Image Editor	1.2.10.6	Greenshot
Heyna	14.4 and later	System Tools Software
Kofax Power PDF Standard	3.10.6687	Kofax Inc.
Microsoft Edge	104.0.1293.70 and later	Microsoft
Microsoft Office 365	16.0.14701.20262 and later	Microsoft
Microsoft Office Professional Plus 2016		Microsoft
Microsoft Teams	1.5.00.21668	Microsoft Corporation
Microsoft Visio	16.0.15601.20088	Microsoft Corporation
Milestone xProtect Management Client	20.2.1 and later	Milestone Systems
Milestone xProtect Smart Client	20.2.2352.1 and later	Milestone Systems
Mozilla Firefox	104.0.2 and later	Mozilla
Mutualink Edge	7.2.3.2800	Mutualink
Nessus Agent	10.1.4.20122 and later	Tenable Inc.

Version: 1.0

Click or tap to enter a date.

Page 3 of 4

Florida Department of Transportation
DISTRICT FOUR TSM&O REGIONAL TRANSPORTATION MANAGEMENT CENTER
STANDARD OPERATING PROCEDURES

IT

Software Whitelists

Software Request Form for Desktops

7.16.01

Software	Version	Vendor
Notepad++	7.8.8 and later	Notepad++ Team
OBS Studio	27.0.0	OBS Project
PowerShell	7.1.5.0	Microsoft
PuTTY	0.73.0.0	Simon Tatham
SmartDeploy Client		SmartDeploy
SmartSensor Manager HD	21.2.505.255	Wavetronix LLC
SolarWind Patch Manager Console	120.2.50032.6 and later	SolarWinds
SolarWinds Agent	2020.2.50025.6 and later	SolarWinds
SolarWinds Orion Network Atlas	1.23.50016.0	Solarwinds Worldwide, LLC.
SolarWinds SEM Agent		SolarWinds
SunGuide Operator Map	8.0.0.7464 and later	SunGuide
The Boringlab Toolbox	5.22.0720 and later	The Boring Lab
TightVNC	2.8.59.0 and later	GlavSoft LLC.
Trend Micro Apex One Security Agent	14.0.11676 and later	Trend Micro
VLC media player	3.0.16 and later	VLC media player
Vmware Remote Console	12.0.2	Vmware, Inc.
WinSCP	5.17.1 and later	Martin Prikryl
Zebra Printing	1.1.9.1290 and later	Zebra Technologies Corporation
Zoom	5.11.3 and later	Zoom Video Communications

Florida Department of Transportation
DISTRICT FOUR TSM&O REGIONAL TRANSPORTATION MANAGEMENT CENTER
STANDARD OPERATING PROCEDURES

IT

Software Whitelists

Software Request Form for Servers

7.16.01

OVERVIEW

A list of all whitelisted software, including the version number and vendor for FDOT D4 TSM&O servers is provided at the end of this form. Personnel that require any other software not whitelisted to do their job, must complete a software request form and submit it for approval.

SOFTWARE REQUEST DETAILS

1. **Employee Printed Name:**
- a. **Title:**
- b. **Email:**
- c. **Department:**
- d. **Supervisor:**
2. **Software Name:**
- a. **Expected Software Use:**
- b. **Software Vendor/Developer:**
- c. **Operating System Compatibility:**
- d. **Third Party Plugin/Software Requirement:**
- e. **Third Party Plugin/Software Vendor:**
- f. **Software Support Maintenance Partner:**

Employee Signature: _____

Date: _____

Florida Department of Transportation
DISTRICT FOUR TSM&O REGIONAL TRANSPORTATION MANAGEMENT CENTER
STANDARD OPERATING PROCEDURES

IT

Software Whitelists

Software Request Form for Servers

7.16.01

SOFTWARE REQUEST FORM APPROVAL PROCESS

1. The requester completes and submits the software request form to the RTMC IT Support Manager via email for review and to approve or deny the request.
 - a. If the software request is denied, the RTMC IT Support Manager notifies the requester via email.
 - b. If approved, the RTMC IT Support Manager submits the software request form to the TSM&O IT Manager for review and to approve or deny the request.
 - (1) If the software request is denied, the TSM&O IT Manager notifies the requester via email.
 - (2) If approved, the TSM&O IT Manager submits the software request form to the TSM&O Resource Manager for final review and to approve or deny the request.
 - (a) If the software request is denied, the TSM&O Resource Manager notifies the requester via email.
 - (b) If approved, the TSM&O Resource Manager notifies the group (requester, RTMC IT Support Manager, and the TSM&O IT Manager) via email of the final status of the software request.
2. The requestor submits the approved software request form to the IT Department via email.
3. The IT Department contacts the requestor to schedule the software installation.

Florida Department of Transportation
DISTRICT FOUR TSM&O REGIONAL TRANSPORTATION MANAGEMENT CENTER
STANDARD OPERATING PROCEDURES

IT

Software Whitelists

Software Request Form for Servers

7.16.01

SOFTWARE WHITELIST FOR SERVERS

Software	Version	Vendor
Boring Server Complete	5.21.0322	The Boring Lab
Ecava IntegraXor	9.2.1001.19	Ecava
IP Video Transcoding	5.12.4.1 or later	IP Video Trans
MaxView Server	1.9.0.755	Intelight
Microsoft Edge	104.0.1293.70 and later	Microsoft
Microsoft SQL Server 2014		Microsoft
Milestone xProtect	20.21.4122 and later	Milestone Systems
Nessus Agent	10.1.4.20122 and later	Tenable Inc
NetTime		
Okta AD Agent	3.8.0 and later	Okta
Okta RADIUS Agent	2.17.2 and later	Okta
Password Manager Pro	12.1.0 and later	Manage Engine
PowerShell	7.1.5.0	Microsoft
RoomAlert Manager	2.3 and later	AVTECH Software
SolarWinds Access Rights Manager	21.4.1.3 and later	SolarWinds
SolarWinds Agent	2020.2.50025.6 and later	SolarWinds
SolarWinds Log Forwarder for Windows	1.1.19	SolarWinds
SolarWinds Orion		SolarWinds
SolarWinds Patch Manager	120.2.50032.6 and later	SolarWinds
SunGuide Operator Map	8.0.0.7464 and later	Sunguide
Tableau Server 2021.4	20221.22.0616.1738 and later	Tableau Software
TimeTrax Sync	3.0.18.6	Pyramid Technologies, LLC
Trend Micro Workload Security Agent	20.0.5394 and later	Trend Micro
Umbrella Connector		Cisco Systems Inc.
Unitrends Agent	10.5.8.1.6848 and later	Unitrends
VMware Tools	12.1 and later	Vmware
WinGate Proxy	9.4 and later	WinGate
WOWZA		WOWZA
Microsoft SQL Server 2016	15.0.18410.0 and later	Microsoft
Cyberlock	9.5.18 or later	Videx

Version: 1.0

Click or tap to enter a date.

Page 3 of 3



7.17 SunGuide and RTMC Software

Table of Content

- SETUP SUNGUIDE ON A COMPUTER OVERVIEW4
- Configure A Computer to Access SunGuide4
- Access SunGuide.....4
- SMART SUNGUIDE IDS.....5

Document History

Version #	Date	Author	Changes
1.0	12/20/2023	Yana Neishlos	Initial Draft

SETUP SUNGUIDE ON A COMPUTEROVERVIEW

Configure A Computer to Access SunGuide

1. The computer should be on a SunGuide network segment. To confirm get the IP Address of the computer and compare to the IP Numbering Plan document for reference.
2. Login using an account which includes the permissions to install and configure software.
3. Navigate to <https://intrasmart.smartsunguide.com> and go to the APPS section of the page and click on SunGuide. Follow onscreen prompts to install.

Access SunGuide

1. Click on Start and type in SunGuide and click on the on-screen search result.
2. Click Operator Map when loaded.
3. Login using your assigned username and password.

SMART SUNGUIDE IDS

The Software Contractor creates and manages SunGuide network IDs.

The Supervisor of the user submits requests for new employees or to change the status for current employees who already have an ID located within the helpdesk application.

This request is then approved by the managers and sent to the IT Department and Software Contractor for creation.



7.19 VMware Virtual Environment

Table of Content

VMware VIRTUAL ENVIRONMENT.....	5
RTMC VMware Virtual Environment – ftmcmva03.field.net	5
TIMSO VMware Virtual Environment – FTIMVMVA05.field.net	19
VMware VIRTUAL ENVIRONMENT – CRITICAL SYSTEMS	24
NIC TEAMING in VMware – TMC	26
Create Link Aggregation Group (LAG) Group for TMC-Field-DS.....	26
Configure tmcvhost01	28
Configure tmcvhost01 – vmnic2	28
Configure tmcvhost01 – vmnic3	33
Configure tmcvhost02.....	38
Configure tmcvhost03.....	39
Configure tmcvhost03 – vmnic2	39
Configure tmcvhost03 – vmnic3	44
Configure tmcvhost04 – tmcvhost08	50
Edit Distributed Port Groups for TMC-Field-DS	50
Create Link Aggregation Group (LAG) Group for TMC-Internet-DS	52
Configure tmcvhost01 – tmcvhost08	53
Assign Uplinks to the Hosts.....	57
Assign uplinks for tmcvhost01	57
Assign uplinks for tmcvhost02	58
Assign uplinks for tmcvhost03	59
Assign uplinks for tmcvhost04	60
Assign uplinks for tmcvhost05	61
Assign uplinks for tmcvhost06	62
Assign uplinks for tmcvhost07	63
Assign uplinks for tmcvhost08	64
Complete following Links Assigning	65
Edit Distributed Port Groups for TMC-Internet-DS.....	66
NIC TEAMING in VMware – TIMSO	68
Create Link Aggregation Group (LAG) for TIMSO-DS	68
Configure timvhost01	70
Configure timvhost01 – vmnic5	70
Configure timvhost01 – vmnic4	75
Configure timvhost01 – vmnic3	81
Configure timvhost01 – vmnic2	88
Configure timvhost04.....	94
Configure timvhost04 – vmnic2	94
Configure timvhost04 – vmnic3	100
Configure timvhost04 – vmnic4	106
Configure timvhost04 – vmnic5	112
Configure timvhost02, timvhost03, timvhost05,timvhost06.....	117
Edit Distributed Port Groups for TIMSO-DS.....	118
ADD an iSCSI ADAPTER to a HOST	120

ESXi Configuration: Disk.DiskMaxIOSize = 1024 120

CREATE a NEW DISTRIBUTED SWITCH 122

ENABLE JUMBO FRAMES 125

 Enable Jumbo Frames on the New Distributed Switch 125

 Enable Jumbo Frames on the Cluster 126

HOST GROUPS 127

 Add Hosts to A Distributed Switch 127

 Create A Host Group 129

ADD VMKernel ADAPTERS 130

 Add VMkernel Adapters to the Hosts – TMC_SAN_41_iSCSI1 130

 Add VMkernel Adapters to the Hosts – TMC_SAN_41_iSCSI2 134

 Add Storage Adapters to the Hosts 138

CREATE NEW STORAGE VOLUMES, CONTENT LIBRARIES, DATASTORE 148

 Create a New Storage Volume – ContentLibraryTMC 148

 Add a New Host 150

 Enter Host Details 150

 Create a New Storage Volume – VMDatastore_TMC 152

 Create a New Storage Volume Group 156

 Create a New Storage Folder 157

 Create a New Datastore - DatastoreContentLibrary_TMC 158

 Create a New Content Library – TMC 162

 Create a New Content Library – TIMSO 165

 Create a New Datastore – DatastoreVM_TMC 167

MIGRATE VMs to a NEW DATASTORE with vMOTION 172

 Migrate (Compute Only) Virtual Machines (VMs) 172

 Migrate Storage Only 173

Document History

Version #	Date	Author	Changes
1.0	2/28/2024	Yana Neishlos	Initial Draft

VMware VIRTUAL ENVIRONMENT

Due to the sensitivity of the information in this document, it is only accessible by IT personnel at the following link:

[7.19 VMWare Virtual Environment - Virtual Server Lists_SD.pdf](#).

Sensitive documents, such as “VMware Virtual Environment” are placed in

[District 4 TSM&O Collaboration Portal \(Partner Site\) - IT Documents - ListView \(sharepoint.com\)](#).

A separate list for all RTMC, Vista Center, TIMSO virtual servers to include the backup frequency and most recent restoration test date for each virtual server / machine is provided in this SOP Section.

RTMC VMware Virtual Environment – ftmcmva03.field.net

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
BarcoWall01_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
BarcoWall02_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
BarcoWall03_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
BarcoWall04_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
BarcoWall05_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
BarcoWall06_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
BarcoWall07_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
BarcoWall08_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
BarcoWall09_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
BarcoWall10_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
BarcoWall11_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
BarcoWall12_Smartsunguide.com	TMC	TMC BARCO Wall	Desktop Support	Desktop Team	On	2	Daily
FTMCVMAP01_OTM	TMC	OTM Website Connection for District 6. Jump server to District 6 SELS Application. Used by Alana & Dee.	Server Team	Server Team	On	2	Daily
FTMCVMAP02_Okta	TMC	Okta Application Server	Security Team	Security Team	On	2	Daily
FTMCVMAP04_WWD	TMC	Wrong Way Detection	IBI Team	IBI Team	On	8	Daily
FTMCVMAP05_SIRVAPP	TMC	SIRV Application Server	IBI Team	IBI Team	On	8	Daily
FTMCVMAP07_US27VSL	TMC	Variable Speed Limit application on US 27	Server Team / David Needham	Server Team	On	4	Daily
FTMCVMAP08_SunGuideTestEnvironment	TMC	Sunguide Application Test Environment Server	IBI Team	IBI Team	On	8	Daily
FTMCVMAP09_SunGuideTestEnvironment	TMC	Sunguide Application Test Environment Server	IBI Team	IBI Team	On	8	Daily
FTMCVMAP10_WebProxy	TMC	Web Proxy Server	IBI Team	IBI Team	On	8	Daily
FTMCVMAP11_TOQC	TMC	TOQC Application Server	IBI Team	IBI Team	On	2	Daily
FTMCVMAP12_RampSignaling	TMC	Ramp Signaling Application Server	IBI Team	IBI Team	On	6	Daily
FTMCVMAP13_US27VSL	TMC	Variable Speed Limit application on US 27	Server Team / David Needham	Server Team	On	4	Daily
FTMCVMAP14_MIMS	TMC	MIMS Application Server	IBI Team	IBI Team	On	8	Daily
FTMCVMAP15_RAMP-API	TMC	Ramp API Server	IBI Team	IBI Team	On	2	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
FTMCVMAP16_US27	TMC	US27 Snapshots Server	IBI Team	IBI Team	On	8	Daily
FTMCVMAP17_AMSSnapshots	TMC	AMS Snapshots Server	IBI Team	IBI Team	On	10	Daily
FTMCVMAP18_RoadRangerApplication	TMC	Road Ranger Application Server	IBI Team	IBI Team	On	6	Daily
FTMCVMAP19_IBITestEnvironment	TMC	IBI Application Test Environment Server	IBI Team	IBI Team	On	8	Daily
FTMCVMAP20_ELSTestEnvironment	TMC	ELS Pricing System Test Environment Server	IBI Team	IBI Team	On	4	Daily
FTMCVMAP21_SELSTestEnvironment	TMC	SELS Test Environment Server	IBI Team	IBI Team	On	4	Daily
FTMCVMAP22_595Report	TMC	595 Reporting System Server	IBI Team	IBI Team	On	4	Daily
FTMCVMAP23_SELSI75	TMC	SELS I75 Cluster Node 1	IBI Team	IBI Team	On	4	Daily
FTMCVMAP24_ELSI95	TMC	ELS Pricing System Server	IBI Team	IBI Team	On	8	Daily
FTMCVMAP25_Snapshots	TMC		IBI Team	IBI Team	On	10	Daily
FTMCVMAP26_SELSI75	TMC	SELS I75 Cluster Node 2	IBI Team	IBI Team	On	4	Daily
FTMCVMAP27_TimeControl	TMC	TimeControl- Controls the wall clocks in the TMC used by Desktop Support	Server Team	Server Team	On	4	Daily
FTMCVMAP29_Generators	TMC	Generators Web Server	Server Team	Server Team	On	4	Daily
FTMCVMAP30_AMSTestEnvironment	TMC	AMS Test Environment Application Server	IBI Team	IBI Team	On	4	Daily
FTMCVMAP31_SNAPS	TMC		IBI Team		On	4	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
FTMCVMAP32_SICE	TMC	SICE Server	Server Team	Server Team	On	2	Daily
FTMCVMAP33_HAR	TMC		IBI Team	IBI Team	On	8	Daily
FTMCVMAP34_DisplayControl	TMC	Display Control	Desktop Support	Desktop Team	On	4	Daily
FTMCVMAP35_KOHLER	TMC		Desktop Support	Server Team	On	2	Daily
FTMCVMARM01_ARMCollector	TMC		Security Team	Security Team	On	2	Daily
FTMCVMDB01_MYSQL	TMC	IT Database	IT Team	IT Team	On	8	Daily
FTMCVMDB02_MYSQL	TMC	IT Database	IT Team	IT Team	On	8	Daily
FTMCVMDC01_DC	TMC	Domain Controller	Server Team	Server Team	On	4	Daily
FTMCVMDC02_DC	TMC	Domain Controller	Server Team	Server Team	On	4	Daily
FTMCVMDC03_DC	TMC	Domain Controller	Server Team	Server Team	On	4	Daily
FTMCVMDC04_DC	TMC	Domain Controller	Server Team	Server Team	On	4	Daily
FTMCVMSQL01_SunGuide	IBI	SELS I75 MySQL cluster node 2	IBI Team	IBI Team	On	32	Daily
FTMCVMSQL02_SunGuide	IBI	Sunguide Application SQL Server	IBI Team	IBI Team	On	32	Daily
FTMCVMUT01_UEB	Backup	Unitrends Backup Application Server	Server Team	Server Team	On	12	Daily
FTMCVMUT02_UEB	Backup	Unitrends Backup Application Server	Server Team	Server Team	On	12	Daily
FTMCVMUT03_UEB	Backup	Unitrends Backup Application Server	Server Team	Server Team	On	12	Daily
FTMCVMUT04_UEB	Backup	Unitrends Backup Application Server	Server Team	Server Team	On	4	Daily
FTMCVMVA03_vCenter	TMC	VMware vCenter Server Appliance	Server Team	Server Team	On	2	Daily
FTMCVMVA04_Cyberlock	TMC	Cyberlock Application Host	Security Team	Security Team	On	2	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
FTMCVMVW01_CMSServer	TMC	CMS Image for virtual box and VMware	Desktop Support	Desktop Support	On	8	Daily
FTMCVMVW02_CMSServer	TMC	CMS Image for virtual box and VMware	Desktop Support	Desktop Support	On	8	Daily
TMCVASEM01_SecurityEventMgr	TMC	Security Event Manager	Security Team	Security Team	On	6	Daily
TMCVMAP04_Intrasmart	TMC	Intrasmart Application Server (TIMSO) internal web server	IBI Team	Server Team	On	4	Daily
TMCVMAP08_BaslerElectric	TMC		Server Team	Server Team	On	2	Daily
TMCVMAP09_KMS	TMC	Key Management Server	Server Team	Server Team	On	4	Daily
TMCVMAP12_Intrasmart	TMC	Intrasmart NLB node 2. internal web server	Server Team	Server Team	On	4	Daily
TMCVMAP14_Website	TMC	Proxy Server between Sunguide Applications and Smartsunguide.com Website	IBI Team	IBI Team	On	12	Daily
TMCVMAP15_BSO	TMC		Server Team	Server Team	On	8	Daily
TMCVMAP18_BSO	TMC		Server Team	Server Team	On	8	Daily
TMCVMAP19_Solarwinds NTM	TMC	Solarwinds Network Topology Manager	Server Team	Server Team	On	2	Daily
TMCVMAP20_DMZWifi DHCP Server	TMC	DHCP server for the guest network (DMZ)	Server Team	Server Team	On	2	Daily
TMCVMAP22_SmartDeploy	TMC	SmartDeploy	Server Team	Server Team	On	4	Daily
TMCVMAP25_NessusSensor	TMC	Tenable Vulnerability Scanner	Security Team		On	2	Daily
TMCVMAP26_D4Snapshots	TMC	D4 Snapshots	IBI Team	IBI Team	On	32	Daily
TMCVMAP29_Okta	TMC	Okta Application Server	Security Team	Security Team	On	2	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
TMCVMAP30_SolarWindsService Desk	TMC	SolarWinds Service Desk	Desktop Team	Server Team	On	4	Daily
TMCVMAPPTST01_Software Team Test Environment	TMC	Software Team Test Environment	Software Team	Software Team	On	4	Daily
TMCVMAR01_AccessRightsMgr	TMC	Solarwinds Access Rights Manager	Security Team	Security Team	On	2	Daily
TMCVMBDS01_BeaconDashboard	TMC		Server Team	Server Team	On	8	Daily
TMCVMCA01_CertificateAuthority	TMC	Certificate Authority Server (Subordinate CA)	Server Team	Server Team	On	2	Daily
TMCVMCA02_CertificateAuthority	TMC	Certificate Authority Server	Server Team	Server Team	On	2	Daily
TMCVMD4SG07_Web Server	DMZ	Web Server	Software Team	Software Team	On	4	Daily
TMCVMD4SG08_Web Server	DMZ	Web Server	Software Team	Software Team	On	4	Daily
TMCVMDAMEWARE01_Dameware Application	TMC	Dameware Application	Desktop Team	Desktop Team	On	2	Daily
TMCVMDB01_ITSQL	TMC	IT SQL Database (Part of AlwaysOn Cluster)	Server Team	Server Team	On	4	Daily
TMCVMDB02_ITSQL	TMC	IT SQL Database (Part of AlwaysOn Cluster)	Server Team	Server Team	On	4	Daily
TMCVMDC01_DC	TMC	Domain Controller (Smartsunguide Domain)	Server Team	Server Team	On	6	Daily
TMCVMDC02_DC	TMC	Domain Controller (Smartsunguide Domain)	Server Team	Server Team	On	8	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
TMCVMDC03_DC	TMC	Domain Controller (Smartsunguide Domain)	Server Team	Server Team	On	2	Daily
TMCVMDFS01	TMC	Distributed File Server	Server Team	Server Team	On	4	Daily
TMCVMDHCP01	TMC	DHCP Server	Server Team	Server Team	On	2	Daily
TMCVMELS59501_ELS595	Sunguide Applications		Software Team	Software Team	On	2	Daily
TMCVMELS59502_ELS595	Sunguide Applications		Software Team	Software Team	On	2	Daily
TMCVMELSI9501_ELSI95 Application	Sunguide Applications		Software Team	Software Team	On	2	Daily
TMCVMELSTST01_ELSTestEnvironment	Sunguide Applications		Software Team	Software Team	On	4	Daily
TMCVMEVIS01_EdgeVisTestServer	TMC				On	4	Daily
TMCVMFP01_PrinterServer	TMC	Print Server	Server Team	Server Team	On	4	Daily
TMCVMFP02_SFTP	Backup	SFTP NLB Node 2	Server Team	Server Team	On	8	Daily
TMCVMFSG01_Freeway Sunguide	Sunguide Applications	Sunguide Application	Software Team	Software Team	On	2	Daily
TMCVMFSG02_Freeway Sunguide	Sunguide Applications	Sunguide Application	Software Team	Software Team	On	2	Daily
TMCVMFSG03_Freeway Sunguide	Sunguide Applications	Sunguide Application	Software Team	Software Team	On	2	Daily
TMCVMIM01_HPDesktopManagement	TMC	HP Desktop Management	Desktop Team	Desktop Team	On	2	Daily
TMCVMNAVISET01_Display Control	TMC	Naviset Monitor Display Application	Desktop Team	Desktop Team	On	2	Daily
TMCVMNVR01	TMC	Milestone Application ARXYS NVR	Security Team	Security Team	On	2	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
TMCVMNVR02_SmartWall	TMC		Security Team	Security Team	On	2	Daily
TMCVMNVR03_RecordingServer	TMC		Security Team	Security Team	On	2	Daily
TMCVMOTM01_OTM Application	TMC		Server Team	Server Team	On	2	Daily
TMCVMRMALERT01_Room Alert	TMC	Room Alert Application	Security Team	Security Team	On	6	Daily
TMCVMSD01_SolarwindsDB	TMC	Solarwinds Database Server	Server Team	Server Team	On	12	Daily
TMCVMSD02_SolarwindsDB	TMC	Solarwinds Database Server	Server Team	Server Team	On	12	Daily
TMCVMSDSCAN01_Solarwinds Service Desk Scanner	TMC	Solarwinds Service Desk Scanner	IT Team				Daily
TMCVMSELSI7501_SELSI75 Application	Sunguide Applications		Software Team				
TMCVMSELSI7502_SELSI75 Application	Sunguide Applications		Software Team				
TMCVMSELSTST01_SELSTestEnvironment	Sunguide Applications		Software Team				
TMCVMSEM01_SecurityEventManager	TMC	Security Event Manager	Security Team	Security Team	On	2	Daily
TMCVMMSG01_SunGuideAMS	TMC	Sunguide AMS Application Server	Software Team	Software Team	On	8	Daily
TMCVMMSG02_SunGuideAMS	TMC	Sunguide AMS Application Server	Software Team	Software Team	On	8	Daily
TMCVMMSG03_SunGuideAMS	TMC	Sunguide AMS Application Server	Software Team	Software Team	On	8	Daily
TMCVMMSGIDS01_Bling Bling	DMZ	SunGuide Incident Detection System Module	Server Team	IBI Team	On	4	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
TMCVMSM01_PasswordManager	TMC	Password Manager Application Server	Security Team	Security Team	On	1	Daily
TMCVMSM02_PasswordManager	TMC	Password Manager Application Server	Security Team	Security Team	On	4	Daily
TMCVMSMTP01_SMTP	TMC	SMTP Relay Server	Server Team	Server Team	On	2	Daily
TMCVMSNAPS01_SNAPS	TMC		Software Team	Software Team	On	2	Daily
TMCVMSO01_SolarwindsOrionPoller	TMC	Solarwinds Poller	Server Team	Server Team	On	24	Daily
TMCVMSO02_SolarwindsOrionPoller	TMC	Solarwinds Poller	Server Team	Server Team	On	8	Daily
TMCVMSO03_SolarwindsAdditionalWebServer	TMC	Solarwinds Web Server	Server Team	Server Team	On	8	Daily
TMCVMSP01_SolarwindsPatchManagement	TMC	SolarWinds Patch Management	Desktop Support	Server Team/Desktop Team	On	6	Daily
TMCVMSP02_SolarwindsWsus	TMC	SolarWinds WSUS server	Desktop Support	Server Team/Desktop Team	On	6	Daily
TMCVMCRM_Site Recovery Manager	TMC	VMware Site Recovery Manager	Server Team	Server Team	On	4	Daily
TMCVMSVRTST_Security Team Test Server	TMC	Security Team Test Server	Security Team	Security Team	On	2	Daily
TMCVMTAB01_Tableau	TMC		Software Team	Software Team	On	2	Daily
TMCVMTE01_IT	TMC	Terminal Server	Desktop Team	Desktop Team	On	2	Daily
TMCVMTS02_3400	TMC	3400 Terminal Server	Server Team	Server Team	On	4	Daily
TMCVMTS03_MaintenanceRDS	TMC	Maintenance Terminal Server	Server Team	Server Team	On	8	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
TMCVMTS04_MaintenanceRDS	TMC	Maintenance Terminal Server	Server Team	Server Team	On	8	Daily
TMCVMTS05_SirvRDS	TMC	SIRV Terminal Server	Server Team	Server Team	On	8	Daily
TMCVMTS06_SirvRDS	TMC	SIRV Terminal Server	Server Team	Server Team	On	8	Daily
TMCVMTVIS01_TrafficVision	TMC		IT Team	IT Team	On	2	Daily
TMCVMUA01_OpenDNS	TMC	Open DNS	Server Team	Server Team	On	1	Daily
TMCVMUA02_OpenDNS	TMC	Open DNS	Server Team	Server Team	On	1	Daily
TMCVMUA03_OpenDNS	TMC	Open DNS	Server Team	Server Team	On	1	Daily
TMCVMUA04_OpenDNS	TMC	Open DNS	Server Team	Server Team	On	1	Daily
TMCVMUA05_OpenDNS	TMC	Open DNS	Server Team	Server Team	On	1	Daily
TMCVMUA06_OpenDNS	TMC	Open DNS	Server Team	Server Team	On	1	Daily
TMCVMUA07_OpenDNS	TMC	Open DNS	Server Team	Server Team	On	1	Daily
TMCVMUA08_OpenDNS	TMC	Open DNS	Server Team	Server Team	On	1	Daily
TMCVMUA09_OpenDNS	TMC	Open DNS	Server Team	Server Team	On	1	Daily
TMCVMUA10_OpenDNS	TMC	Open DNS	Server Team	Server Team	On	1	Daily
TMCVMUC01_UmbrellaConnector	TMC	Cisco Umbrella Connector Server	Server Team	Server Team	On	2	Daily
TMCVMUC02_UmbrellaConnector	TMC	Cisco Umbrella Connector Server	Server Team	Server Team	On	2	Daily
TMCVMVA16_ESRS	TMC	ESRS Server	Server Team	Server Team	On	1	Daily
TMCVMVA17_NTPServer	TMC	NTP Server	Server Team	Server Team	On	2	Daily
TMCVMVA29_NessusWebApp	TMC	Tenable Web Application Scanner	Security Team	Security Team	On	4	Daily
TMCVMVA30_Nessus Scanner	TMC	Tenable Core	Security Team	Security Team	On	4	Daily
TMCVMVEEAM01_Veeam Backup & Recovery Server	TMC	Veeam Backup & Recovery Console	Server Team	Server Team	On	4	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
TMCVMVEEAMONE01_Veeam One	TMC	Veam One Application	Server Team	Server Team	On	8	Daily
TMCVMVG04_IPVideoTranscoder	TMC	IP Video Camera Transcoder Software Application Host	Security Team	Security Team	On	25	Daily
TMCVMVG05_IPVideoTranscoder	TMC	IP Video Camera Transcoder Software Application Host	Security Team	Security Team	On	16	Daily
TMCVMVG06_IPVideoTranscoder	TMC	IP Video Camera Transcoder Software Application Host	Security Team	Security Team	On	16	Daily
TMCVMVG07_IPVideoTranscoder	TMC	IP Video Camera Transcoder Software Application Host	Security Team	Security Team	On	16	Daily
TMCVMVG08_IPVideoTranscoder	TMC	IP Video Camera Transcoder Software Application Host	Security Team	Security Team	On	16	Daily
TMCVMVG09_IPVideoTranscoder	TMC	IP Video Camera Transcoder Software Application Host	Security Team	Security Team	On	16	Daily
TMCVMVG10_IPVideoTranscoder	TMC	IP Video Camera Transcoder Software Application Host	Security Team	Security Team	On	8	Daily
TMCVMVG11_IPVideoTranscoder	TMC	IP Video Camera Transcoder Software Application Host	Security Team	Security Team	On	4	Daily
TMCVMVMS01_VMSGateway	TMC	VMSGateway	IT Team	IT Team	On	2	Daily
TMCVMVMS02_VMSGateway	TMC	VMSGateway	IT Team	IT Team	On	2	Daily
TMCVMVPXYDMZ01_Veeam Proxy Server	DMZ	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	2	Daily
TMCVMVPXYDMZ02_Veeam Proxy Server	DMZ	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	2	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
TMCVMPXYHOST01_ Veeam Proxy Server	TMC	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TMCVMPXYHOST02_ Veeam Proxy Server	TMC	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TMCVMPXYHOST03_ Veeam Proxy Server	TMC	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TMCVMPXYHOST04_ Veeam Proxy Server	TMC	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TMCVMPXYHOST05_ Veeam Proxy Server	TMC	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TMCVMPXYHOST06_ Veeam Proxy Server	TMC	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TMCVMPXYHOST07_ Veeam Proxy Server	TMC	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TMCVMPXYSGAP01_ Veeam Proxy Server	Sunguide Applications	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TMCVMPXYSGAP02_ Veeam Proxy Server	Sunguide Applications	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TMCVMPXYSGAP03_ Veeam Proxy Server	Sunguide Applications	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TMCVMPSPHEREREP_vCenter Replication Appliance	TMC	vCenter Replication Appliance	Server Team	Server Team	On	4	Daily
TMCVMVW01	TMC	CMS Server	Desktop Team	Desktop Team	Off	8	Daily
TMCVMVW02	TMC	CMS Server	Desktop Team	Desktop Team	Off	8	Daily
TMCVMWINPXY01_Wingate Proxy	TMC	Wingate Application Proxy Server	Server Team	Server Team	On	2	Daily
Windows 10 Enterprise Image – BASE (SmartDeploy)	TMC	Windows 10 Enterprise Image - BASE (SmartDeploy)	Desktop Team	Desktop Team	Off	4	Daily

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
Windows 10 Enterprise Image - Control Room Internet	TMC	Windows 10 Enterprise Image - Control Room Internet	Desktop Team	Desktop Team	Off	4	Daily
Windows 10 Enterprise Image - IT (SmartDeploy)	TMC	Windows 10 Enterprise Image - IT (SmartDeploy)	Desktop Team	Desktop Team	Off	4	Daily
Windows 10 Enterprise Image - Maintenance (SmartDeploy)	TMC	Windows 10 Enterprise Image - Maintenance (SmartDeploy)	Desktop Team	Desktop Team	Off	4	Daily
Windows 10 Enterprise Image - Office (SmartDeploy)	TMC	Windows 10 Enterprise Image - Office (SmartDeploy)	Desktop Team	Desktop Team	Off	4	Daily
Windows 10 Enterprise Image - SIRV Laptop	TMC	Windows 10 Enterprise Image - SIRV Laptop	Desktop Team	Desktop Team	Off	4	Daily
Windows 10 Enterprise Image - VDU	TMC	Windows 10 Enterprise Image - VDU	Desktop Team	Desktop Team	Off	4	Daily
Wowza	DMZ		Software Team	Software Team	On	2	Daily
Wowza01	DMZ		Software Team	Software Team	On	8	Daily
Wowza02	DMZ		Software Team	Software Team	On	8	Daily
Wowza03	DMZ		Software Team	Software Team	On	8	Daily
Wowza04	DMZ		Software Team	Software Team	On	8	Daily
WSUS Test Environment - IT Department	TMC						

Server Name	Cluster	Server Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
WSUS Test Environment - Office (Windows 10)	TMC						

TIMSO VMware Virtual Environment – FTIMVMVA05.field.net

Virtual Server / Machine Name	Cluster	Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
FTIMVMAP01_SunGuide	TIMSO	Sunguide Application Server	IBI Team	IBI Team	On	4	Daily
FTIMVMAP02_SunGuide	TIMSO	Sunguide Application Server	IBI Team	IBI Team	On	4	Daily
FTIMVMAP03_SunGuide	TIMSO	Sunguide Application Server	IBI Team	IBI Team	On	4	Daily
FTIMVMAP04_SunGuide	TIMSO	Sunguide Application Server	IBI Team	IBI Team	On	4	Daily
FTIMVMAP05_Okta	TIMSO	Okta Application Server	Security Team	Security Team	On	2	Daily
FTIMVMAP06_SolarWinds	TIMSO	Solarwinds Application Server	Server Team	Server Team	On	4	Daily
FTIMVMAP07_MIMS	TIMSO	MIMS Application Server	IBI Team	IBI Team	On	4	Daily
FTIMVMAP12_SELSI75	TIMSO	SELS I75	IBI Team	IBI Team	On	4	Daily
FTIMVMDB01_i75MYSQL	TIMSO	i75MYSQL	IBI Team	IBI Team	On	8	Daily
FTIMVMDC01_DC	TIMSO	Domain Controller (Field Domain)	Server Team	Server Team	On	4	Daily
FTIMVMDC02_DC	TIMSO	Domain Controller (Field Domain)	Server Team	Server Team	On	2	Daily
FTIMVMUT01_UEB	Backup	Unitrends Backup Application Server (TIMSO)	Server Team	Server Team	On	16	Daily
FTIMVMUT02_UEB	Backup	Unitrends Backup Application Server (TIMSO)	Server Team	Server Team	On	12	Daily
FTIMVMVA05_VCenter	TIMSO	VMware vCenter Server	Server Team	Server Team	On	2	Daily

Virtual Server / Machine Name	Cluster	Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
FVISVMDC01_DC	VISTA	Domain Controller (Field Domain)	Server Team	Server Team	On	4	Daily
FVISVMDC02_DC	VISTA	Domain Controller (Field Domain)	Server Team	Server Team	On	4	Daily
FVISVMUT01_UEB	VISTA	Unitrends Backup Application Server	Server Team	Server Team	On	12	Daily
TIMVMAP03_TrendMicro	TIMSO	Trend Micro Application Server	Security Team	Security Team	On	8	Daily
TIMVMAP04_Okta	TIMSO	Okta Application Server	Security Team	Security Team	On	2	Daily
TIMVMAP08_Intrasmart	TIMSO	Intrasmart Application Server (TIMSO) internal web server	Server Team	Server Team	On	2	Daily
TIMVMDB01_ITSQL	TIMSO	IT SQL Database (Part of AlwaysOn Cluster)	Security Team	Security Team	On	4	Daily
TIMVMDBI7501_I75MYSQL	TIMSO	I75MYSQL	Software Team	Software Team	On	2	Daily
TIMVMDBSG01_Sunguide Database	TIMSO	Sunguide Database	Software Team	Software Team	On	2	Daily
TIMVMDC01_DC	TIMSO	Domain Controller (Field Domain)	Server Team	Server Team	On	2	Daily
TIMVMDC02_DC	TIMSO	Domain Controller (Field Domain)	Server Team	Server Team	On	2	Daily
TIMVMDFS01_DFS	TIMSO	DFS Server (smartsunguide)	Server Team	Server Team	On	4	Daily
TIMVMDHCP01_DHCP	TIMSO	DHCP Server	Server Team	Server Team	On	2	Daily
TIMVMFP01_PrintServer	TIMSO	Print Server (TIMSO)	Server Team	Server Team	On	4	Daily

Virtual Server / Machine Name	Cluster	Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
TIMVMFSG01_Sunguide Application	TIMSO	Sunguide Application	Software Team	Software Team	On	2	Daily
TIMVMFSG02_Sunguide Application	TIMSO	Sunguide Application	Software Team	Software Team	On	2	Daily
TIMVMHPESUM01_HPE SUM	TIMSO	HP Software Update Manager	Server Team	Server Team	On	4	Daily
TIMVMMMAINT01_Maintenance Team Applications	TIMSO	Maintenance Team Application Server	Desktop Team	Desktop Team	On	2	Daily
TIMVMMIMS01_MIMS Application	TIMSO	MIMS Application	Software Team	Software Team	On	2	Daily
TIMVMSELSI7501_SEL75 Application	TIMSO		Software Team	Software Team	On	2	Daily
TIMVMSKYHLTH01-VMware Skyline Health	TIMSO	VMware Skyline Application	Server Team	Server Team	On	4	Daily
TIMVMMSM01_PasswordManager	TIMSO	Password Manager Application Server	Security Team	Security Team	On	1	Daily
TIMVMMSM02_PasswordManager	TIMSO	Password Manager Application Server	Security Team	Security Team	On	8	Daily
TIMVMSRM_Site Recovery Manager	TIMSO	VMware Site Recovery Manager Application	Server Team	Server Team	On	4	Daily
TIMVMUA01_OpenDNS	TIMSO	Cisco Open DNS	Server Team	Server Team	On	1	Daily
TIMVMUA02_OpenDNS	TIMSO	Cisco Open DNS	Server Team	Server Team	On	1	Daily

Virtual Server / Machine Name	Cluster	Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
TIMVMUA03_OpenDNS	TIMSO	Cisco Open DNS	Server Team	Server Team	On	1	Daily
TIMVMUC01_UmbrellaConnector	TIMSO	Cisco Umbrella Connector Application Server	Server Team	Server Team	On	2	Daily
TIMVMVA04_Nessus	TIMSO	Nessus (Tenable) Application Server	Security Team	Security Team	On	4	Daily
TIMVMVA05_NTPServer	TIMSO	NTP Server	Server Team	Server Team	On	2	Daily
TIMVMVEEAM01_Veeam Backup & Recovery Server	TIMSO	Veeam Backup & Recovery Console	Server Team	Server Team	On	4	Daily
TIMVMVPXYHOST01_Veeam Proxy Server	TIMSO	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TIMVMVPXYHOST02_Veeam Proxy Server	TIMSO	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TIMVMVPXYHOST03_Veeam Proxy Server	TIMSO	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TIMVMVPXYHOST04_Veeam Proxy Server	TIMSO	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TIMVMVPXYHOST05_Veeam Proxy Server	TIMSO	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TIMVMVPXYHOST06_Veeam Proxy Server	TIMSO	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
TIMVMVSPHEREP_vCenter Replication Appliance	TIMSO	vSphere Replication Application	Server Team	Server Team	On	4	Daily

Virtual Server / Machine Name	Cluster	Role	Managed By	Patched By	Powered On / Off	CPUs	Backup Frequency
VISVMAP01_OktaPreview	VISTA	Okta Application Server	Server Team	Server Team	On	2	Daily
VISVMDC01_DC	VISTA	Domain Controller (Smartsunguide Domain)	Server Team	Server Team	On	4	Daily
VISVMDC02_DC	VISTA	Domain Controller (Smartsunguide Domain)	Server Team	Server Team	On	4	Daily
VISVMDHCP01_DHCP	VISTA		Server Team	Server Team	On	2	Daily
VISVMFP01_PrintServer	VISTA	Print Server (VISTA)	Server Team	Server Team	On	4	Daily
VISVMSM01_PasswordManager	VISTA	Password Manager Application Server	Server Team	Server Team	On	1	Daily
VISVMUA01_OpenDNS	VISTA	Cisco Open DNS	Server Team	Server Team	On	1	Daily
VISVMUA02_OpenDNS	VISTA	Cisco Open DNS	Server Team	Server Team	On	1	Daily
VISVMUA03_OpenDNS	VISTA	Cisco Open DNS	Server Team	Server Team	On	1	Daily
VISVMUC01_UmbrellaConnector	VISTA	Cisco Umbrella Connector Application Server	Server Team	Server Team	On	2	Daily
VISVMVPXYHOST01_VeeamProxy Server	VISTA	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
VISVMVPXYHOST02_VeeamProxy Server	VISTA	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily
VISVMVPXYHOST03_VeeamProxy Server	VISTA	Veeam Backup & Recovery Proxy	Server Team	Server Team	On	6	Daily

VMware VIRTUAL ENVIRONMENT – CRITICAL SYSTEMS

There are many applications that run on VMs, which are essential to the operations of D4 TSM&O. Provided below is a list of all critical VMs that are managed by the IT Department. If failure occurs on the VMs at the RTMC, the applications will continue to operate through VMs at the disaster recovery center (TIMSO).

VM Description	If the RTMC VM Fails
TMCVMVEEAM01	TIMVMVEEAM01 takes over.
FTMCVMAP14_MIMS	MIMS will continue to run on FTIMVMAP07.
FTMCVMAP23_SELSI75	SELS runs on these two VMs for redundancy. If failure occurs on both VMs, FTIMVMAP12 takes over.
FTMCVMAP26_SELSI75	
FTMCVMDB01_MYSQL	SELS runs on MYSQL on these two VMs for redundancy. If failure occurs on both VMs, FTIMVMDB01 takes over.
FTMCVMDB02_MYSQL	
TMCVMAP07_TrendMicro Deep Security	It will re-route to the management virtual server in TIMSO (TIMVMAP03) to get definition updates.
TMCVMAP07_TrendMicro ApexOne	It will re-route to the appliance in TIMSO (TIMVMAP07) to get definition updates.
TMCVMFP01_PrinterServer	TIMVMFP01 takes over.
TMCVMAP04_Intrasmart	Intrasmart runs on these two VMs for redundancy. If failure occurs on both VMs, TIMVMAP08 takes over.
TMCVMAP12_Intrasmart	
FTMCVMAP02_Okta	FTIMVMAP05_Okta takes over. If AD Agents are not available, the integrated applications (field domain) will be inaccessible.
TMCVMAP29_Okta	TIMVMAP04_Okta takes over. If AD Agents are not available, the integrated applications (smartsunguide domain) will be inaccessible.
TMCVMAP25_NessusSensor	TIMVMVA04 takes over.
TMCVMNTP01_NTPServer	TIMVMNTP01_NTP Server takes over.
TMCVMSM01_PasswordManager	TIMVMSM01 takes over.
TMCVMSM02_PasswordManager	We can still access passwords on the read only version in TIMSO (TIMVMSM02). However, changes of any kind (e.g., grant new passwords or permissions) cannot be made.
TMCVMDFS01	This DFS server replicated to TIMVMDFS01
FTMCVMAP04	WWD (Wrong Way Driving Detection)
FTMCVMVA03_vCenter	FTIMVMVA05_VCenter takes over.
TMCVMUA01_OpenDNS	TIMVMUA01_OpenDNS takes over.
TMCVMUA02_OpenDNS	TIMVMUA02_OpenDNS takes over.
TMCVMUA03_OpenDNS	TIMVMUA03_OpenDNS takes over.
TMCVMUC01_UmbrellaConnector	TIMVMUC01_UmbrellaConnector takes over.
FTMCVMAP11_TOQC	The IT department takes a daily snapshot of it to recover the ADAPT, DART, TOQC, and WWD applications.
FTMCVMAP14_MIMS	MIMS will continue to run on FTIMVMAP07.

VM Description	If the RTMC VM Fails
FTMCVMAP33_HAR	The IT department takes a daily snapshot of it to recover the HAR software.
WOWZA01	The video stream from the Sidebar application, which is transcoded on the WOWZA website for public access, runs on these four VMs for redundancy. The IT department takes a daily snapshot of them for recovery, in case of failure.
WOWZA02	
WOWZA03	
WOWZA04	

NIC TEAMING in VMware – TMC

Create Link Aggregation Group (LAG) Group for TMC-Field-DS

Steps / Screenshots

1.

- Click `ftmcmvva03.field.net`.
- Click Networking.



Figure 1. `ftmcmvva03.field.net` > Networking

2. (1) Click the down arrow next to **ftmcmvva03.field.net**
- (2) Click the down arrow next to **TMC**

- (3) Click **TMC-Field-DS**
- (4) Click **Configure**
- (5) Click **LACP**
- (6) Click **NEW**.

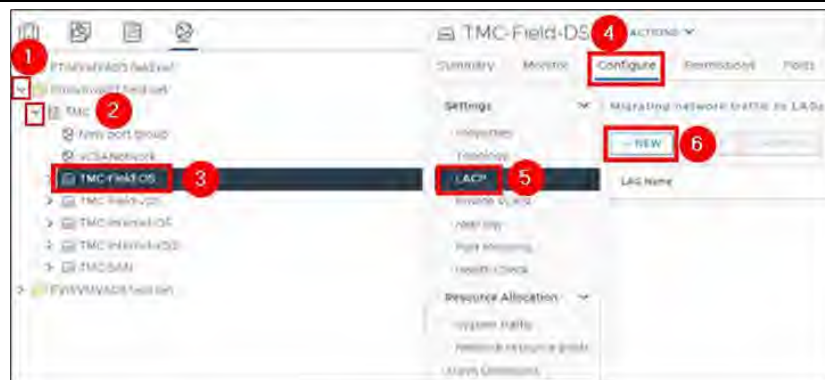


Figure 2. `TMC-Field-DS` > Configure > LACP > NEW

3. Enter the following information in the New LAG window, as shown in Figure 3:

- Name: `LAG_1`
- Number of ports: 2
- Mode: Active
- Load balancing mode: Source and destination Mac address
- Timeout mode: slow
- Click **OK**.



Number 3. New LAG – LAG_1

Steps / Screenshots

4. (1) Click the down arrow next to **TMC-FIELD-DS**
- (2) right Click **TMC_FIELD_MGMT_100**
- (3) Click **Edit Settings**

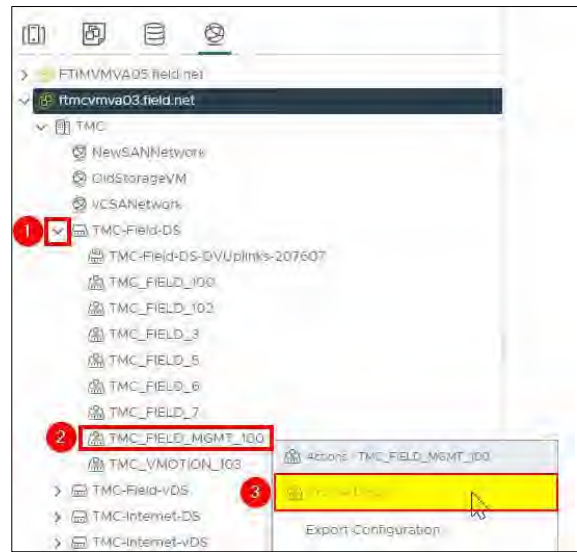


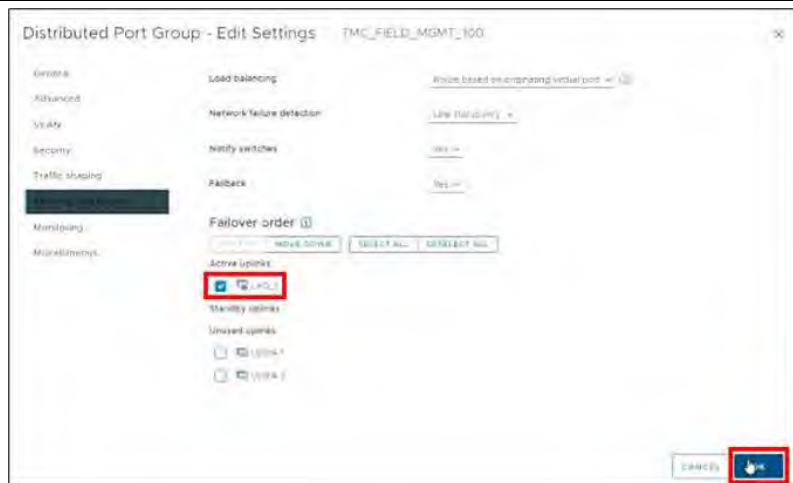
Figure 4. TMC-Field-DS > TMC_FIELD_MGMT_100 > Edit Settings

5.
 - Click Teaming and Failover
 - Move **Uplink 1** and **Uplink 2** to Unused uplinks.



Figure 5. Move Uplink 1 and Uplink 2 to Unused Uplinks.

- 6
 - Move **LAG_1** to Active uplinks.
 - Click **OK**.



Steps / Screenshots

Figure 6. Move LAG_1 to Active Uplinks

Configure tmcvhost01

Configure tmcvhost01 – vmnic2

Steps / Screenshots

1. (1) Click **host and clusters**,
- (2) Click the down arrow next to **TMC Cluster**,
- (3) Click **tmcvhost01.smartsunguide.com**,
- (4) Click **Configure**,
- (5) Click **Physical adapters**,
- (6) Click **vmnic2**



Figure 7. Configure tmcvhost01 - vmnic2

2. Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), which will be provided to the Network Manager.
 - Device ID: **Switch # 1**
 - Port ID: **Port # 1**

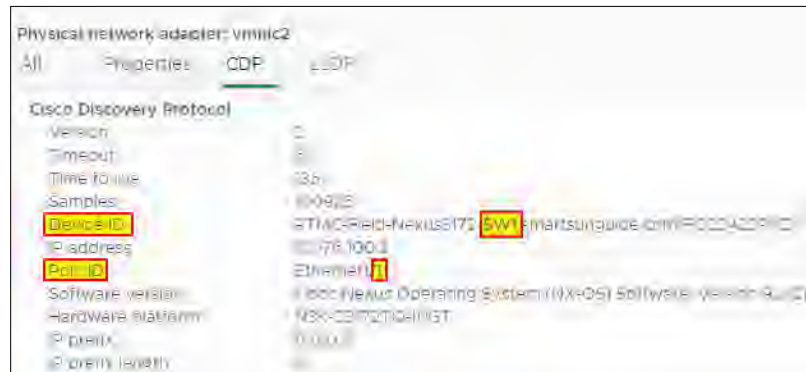


Figure 8. vmnic2 Device ID and Port ID.

3.
 - On the physical switch, the Network Manager will down the port connected to **vmnic2**.
 - Confirm that the port is down.

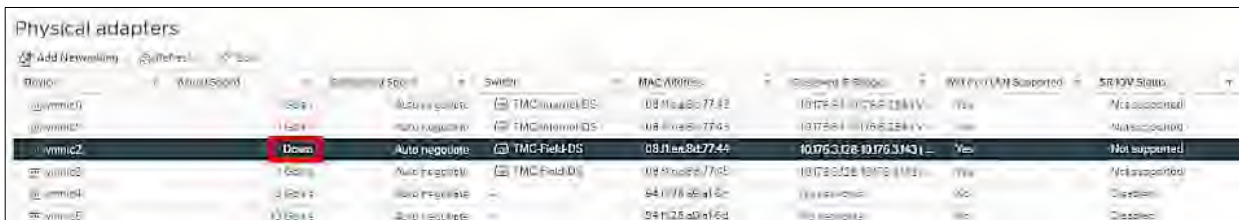


Figure 9. Confirm that the Port is Down.

Steps / Screenshots

On the physical switch, the Network Manager will place the port connected to **vmnic2** in the LACP/EtherChannel configuration.

4.
 - Click networking,
 - Right Click **TMC-Field-DS**,
 - Click Add and Manage Hosts

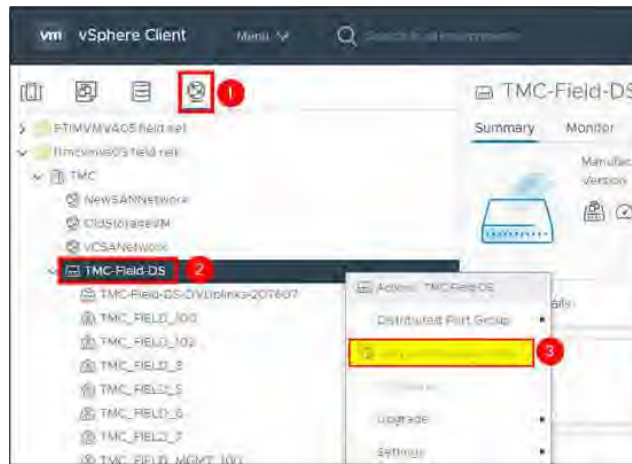


Figure 10. Add and Manage Hosts.

5.
 - Select Manage host networking and,
 - Click **NEXT**

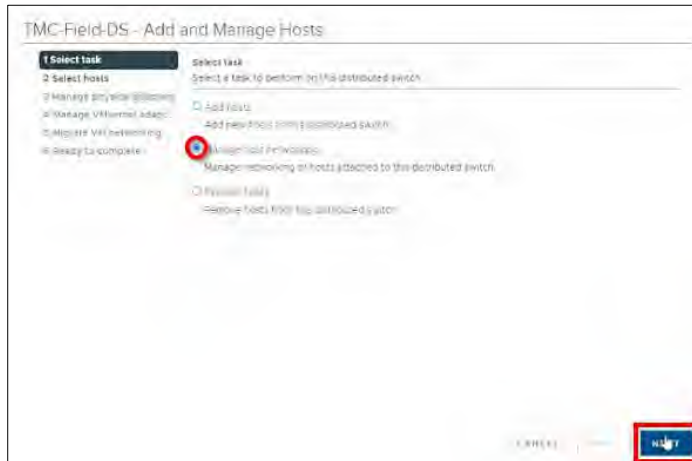


Figure 10. Select Task

6.
 - Click Attached hosts → check the box next to tmcvhost01.smarsunguide.com,
 - Click **OK**.

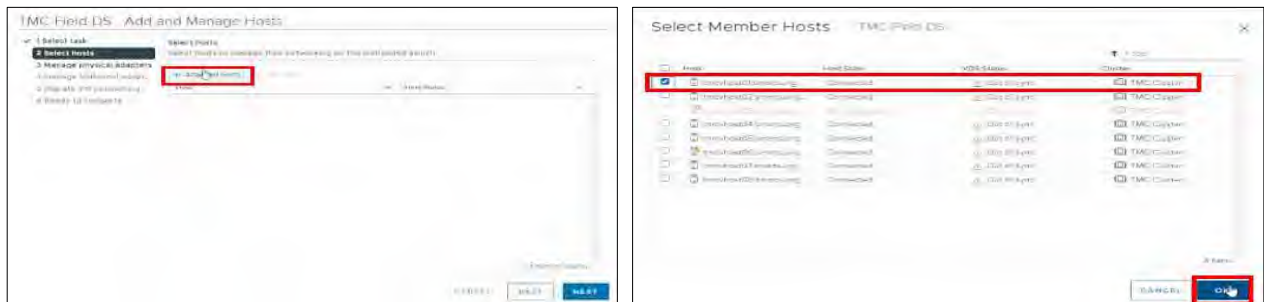


Figure 11. Select Member Host

Steps / Screenshots

7. Click **NEXT**

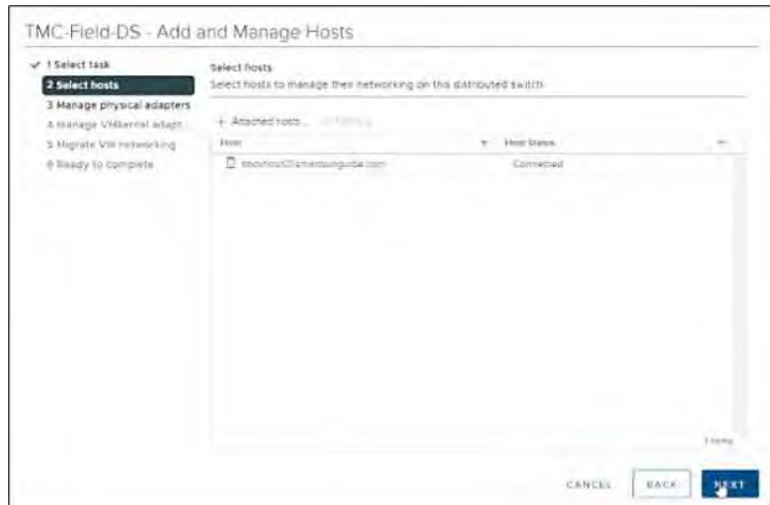


Figure 12. Select Host.

8. Add **vmnic2** to one of the LAG Uplinks as follows:

- Select **vmnic2**.
- Click Assign uplink.
- Select LAG_1-0.
- Click **OK**.

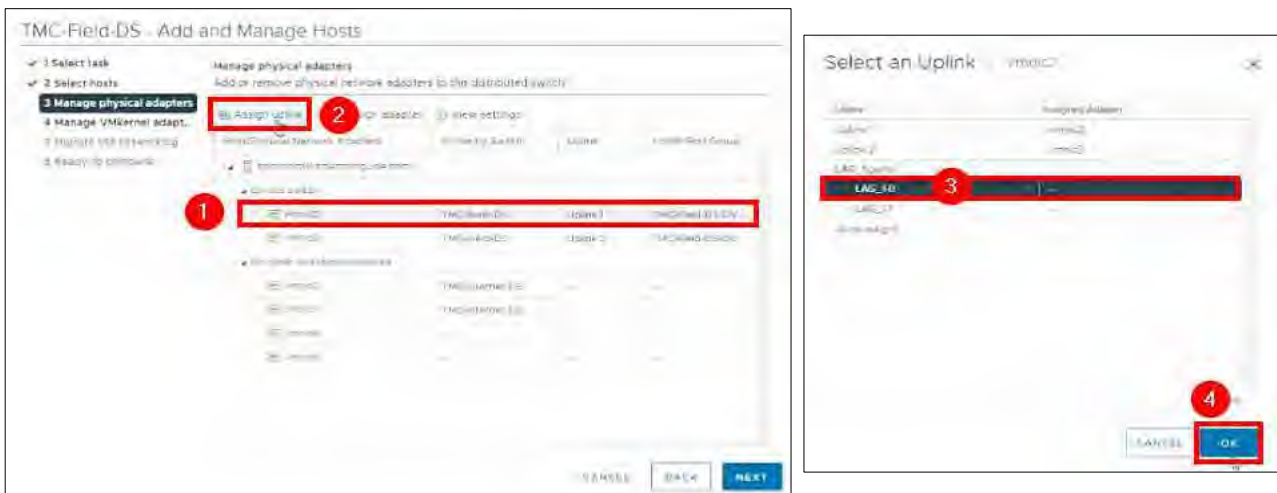


Figure 13. Manage Physical Adapters – Select an Uplink

Steps / Screenshots

9. Click **NEXT**.

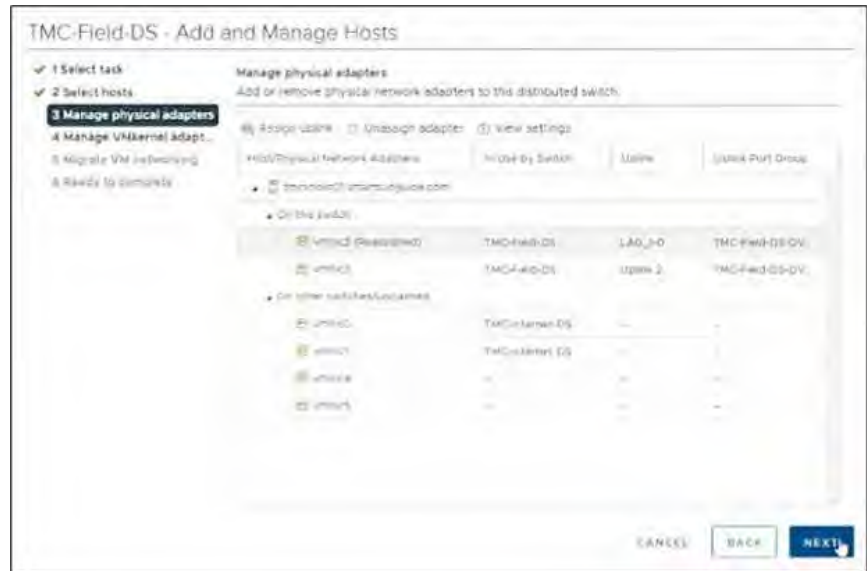


Figure 14. Manage Physical Adapters

10. Click **NEXT**.

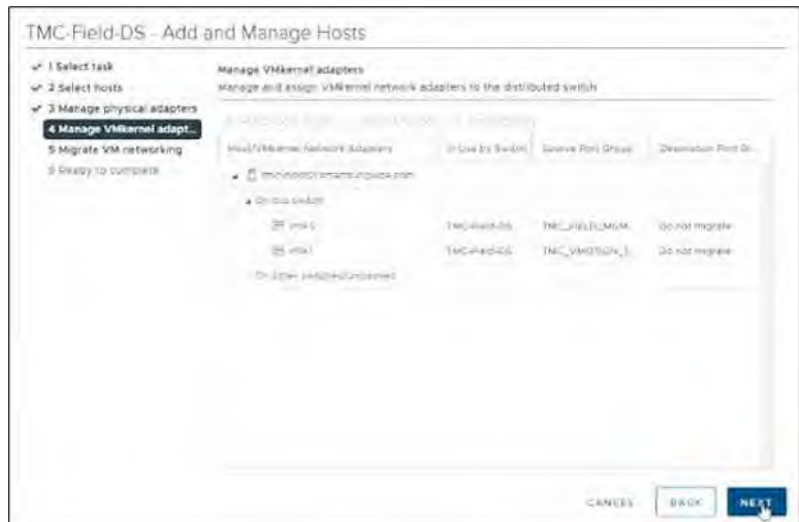


Figure 15. Manage VMkernel Adapters

Steps / Screenshots

11. Click **NEXT**.

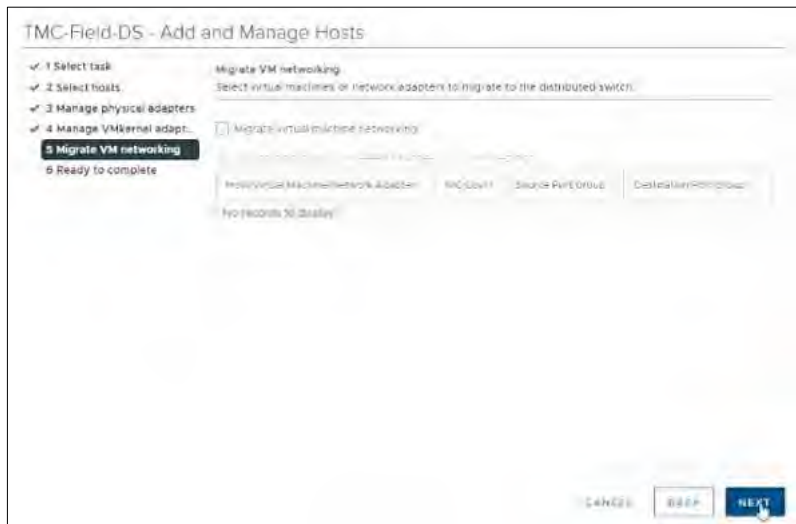


Figure 16. Migrate VM Networking

12. Click **FINISH**.

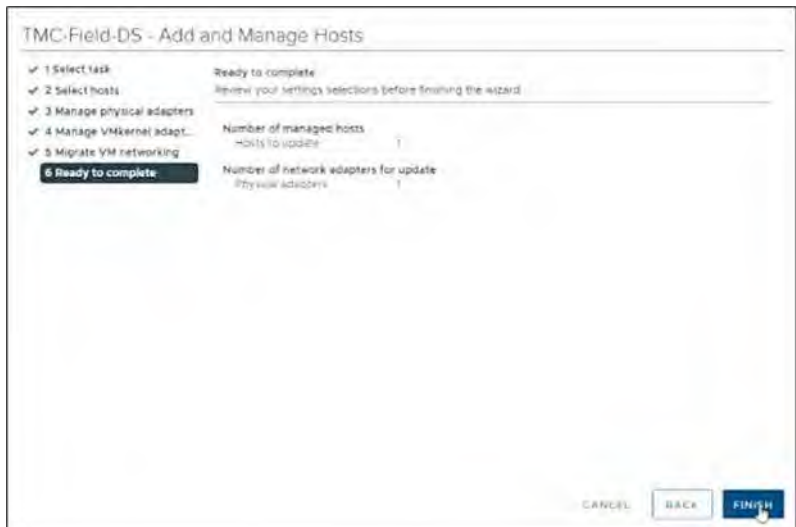


Figure 17. Ready to Complete

The Network Manager will bring the port back up.

1. Go back **Physical adapters** and wait for port to come back up.



Figure 18. Wait for Port to Come Back Up

- Click the **All** tab and wait for networks to appear.

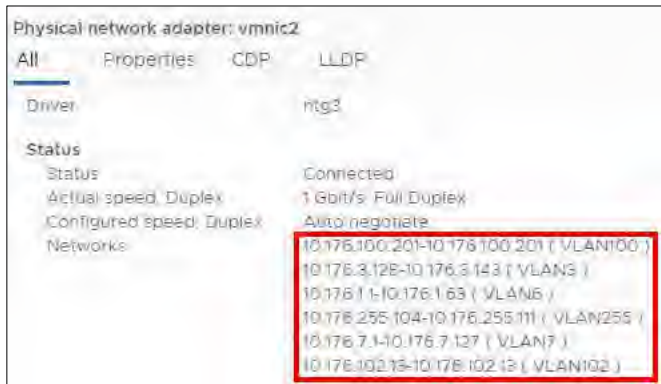


Figure 19. Wait for Networks to Appear

Configure tmcvhost01 – vmnic3

Steps / Screenshots

- (1) Click host and clusters,
 - (2) Click the down arrow next to **TMC Cluster**,
 - (3) Click tmcvhost01.smartsunguide.com,
 - (4) Click Configure,
 - (5) Click Physical adapters,
 - (6) Click **vmnic3**.



Figure 20. Configure tmcvhost01 - vmnic3

- Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), which will be provided to the Network Manager 22).
 - Device ID: **Switch # 2**
 - Port ID: **Port # 1**



Figure 21. vmnic3 Device ID and Port ID

On the physical switch → Network Manager will down the port connected to **vmnic3**.
Confirm that the port is down.

Steps / Screenshots

Device	Speed	Switch	MAC Address	Observed IP	Media on LAN	SR-IOV Status	
vmnic0	1 Gbps	Auto negotiate	TMC-Internal-DS	08:00:50:77:43	10.10.10.13/10.10.10.27/1 VL	Yes	Not supported
vmnic1	1 Gbps	Auto negotiate	TMC-Internal-DS	08:00:50:77:43	10.10.10.13/10.10.10.27/1 VL	Yes	Not supported
vmnic2	1 Gbps	Auto negotiate	TMC-Field-DS	08:00:50:77:44	10.10.100.10/10.100.10.25	Yes	Not supported
vmnic3	Down	Auto negotiate	TMC-Field-DS	08:00:50:77:45	10.10.100.64-10.10.100.7	Yes	Not supported
vmnic4	10 Gbps	Auto negotiate	-	84:0D:29:40:16:00	No networks	No	Disabled
vmnic5	10 Gbps	Auto negotiate	-	34:0D:29:40:16:00	No networks	No	Disabled

Figure 22. Confirm that the Port is Down

On the physical switch → Network Manager will place the port connected to **vmnic3** in the LACP/EtherChannel configuration.

- (1) Click **networking**,
 - (2) Right Click **TMC-Field-DS**,
 - (3) Click Add and Manage Hosts

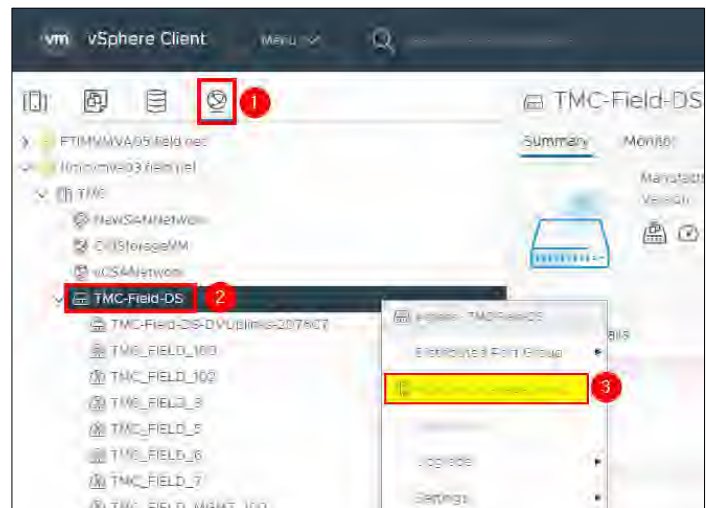


Figure 23. Add and Manage Hosts.

- Select Manage host networking.
 - Click **NEXT**

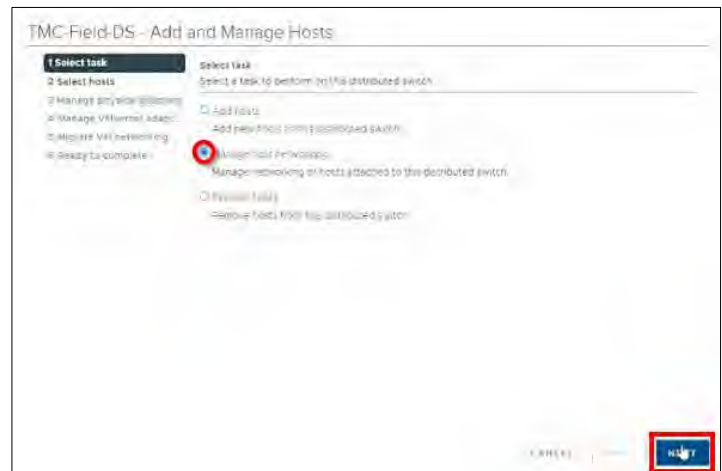


Figure 24. Select Task

- Click Attached hosts → check the box next to `tmcvhost01.smarsunguide.com`,

Steps / Screenshots

- Click **OK**.

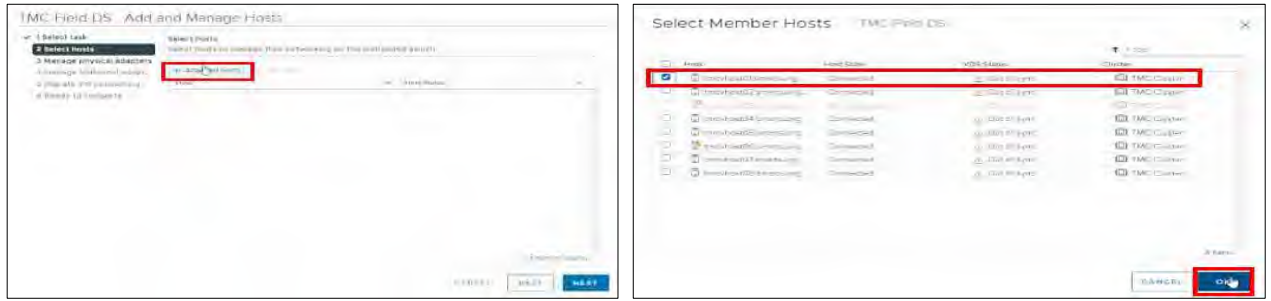


Figure 25. Select Member Host

- 6. Click **NEXT**

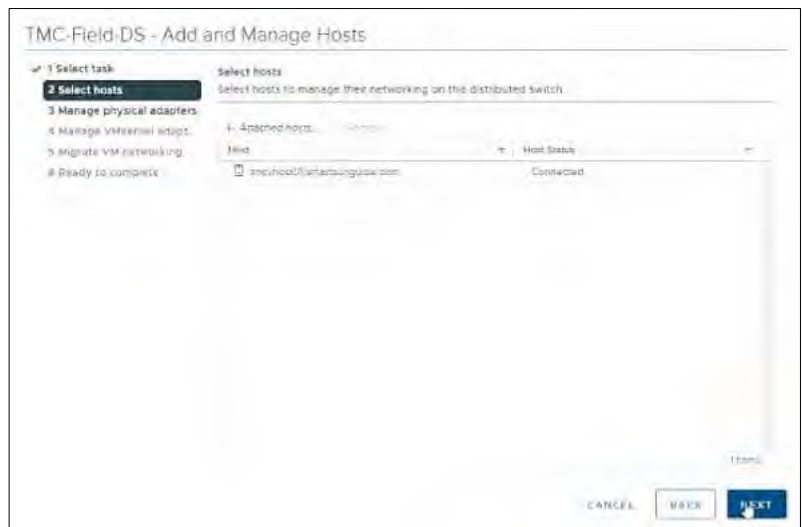


Figure 26. Select Host

- 7.
 - Add **vmnic3** to one of the LAG uplinks:
 - (1) Select **vmnic3**
 - (2) Click Assign uplink
 - (3) Select **LAG_1-1**
 - (4) Click **OK**.

Steps / Screenshots

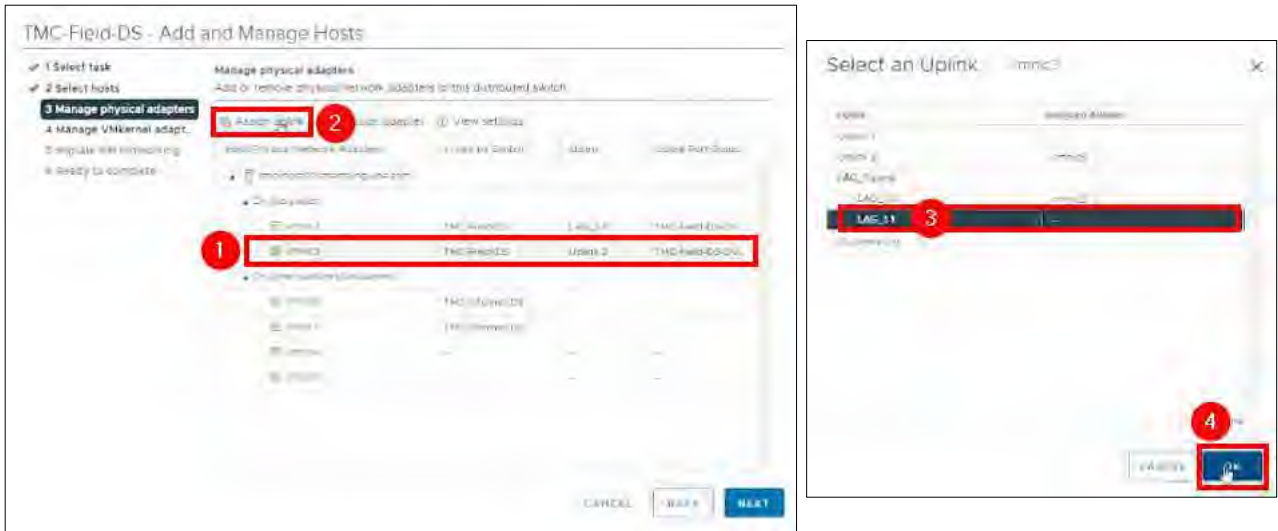


Figure 27. Manage Physical Adapters – Select an Uplink

8.
 - Click NEXT

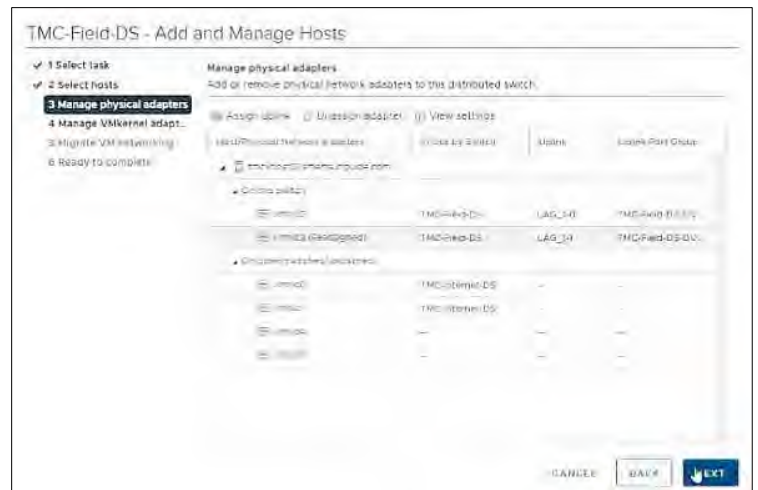


Figure 28. Manage Physical Adapters

Steps / Screenshots

- 9. -
- Click **NEXT**



Figure 29. Manage VMkernel Adapters

- 10. -
- Click **NEXT**

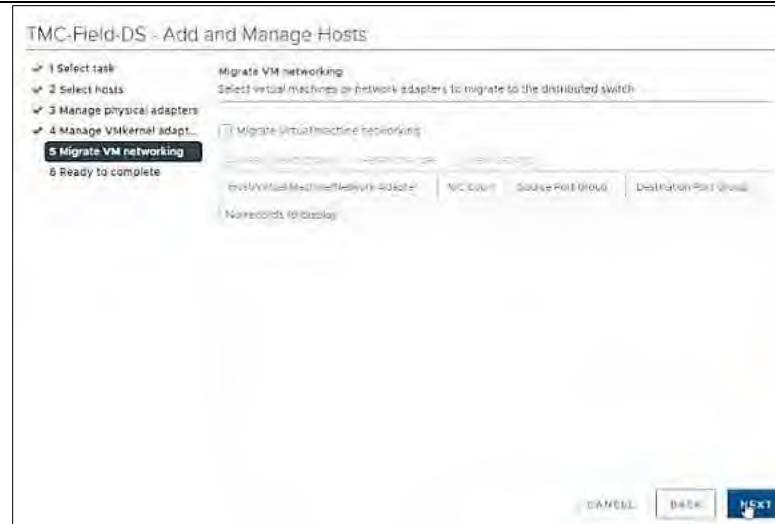


Figure 30. Migrate VM Networking

- 11. -
- Click **FINISH**



Figure 31. Ready to Complete

Steps / Screenshots

The Network Manager will bring the port back up. Go back **Physical adapters**; wait for port to come back up.

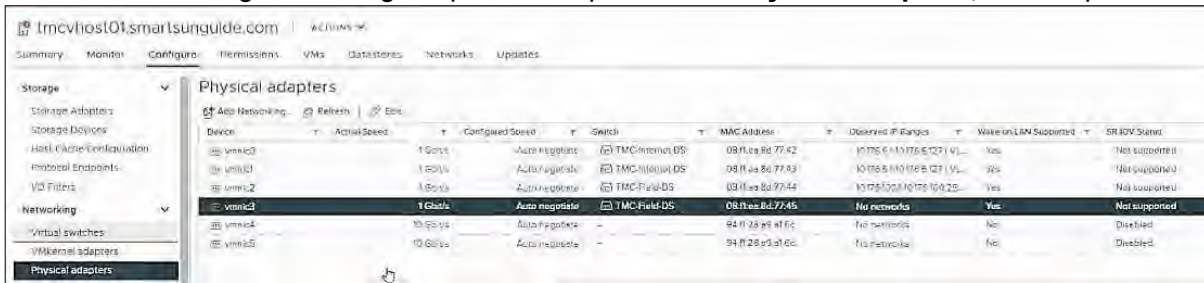


Figure 32. Wait for Port to Come Back Up

- Click **All** tab and wait for networks to appear.

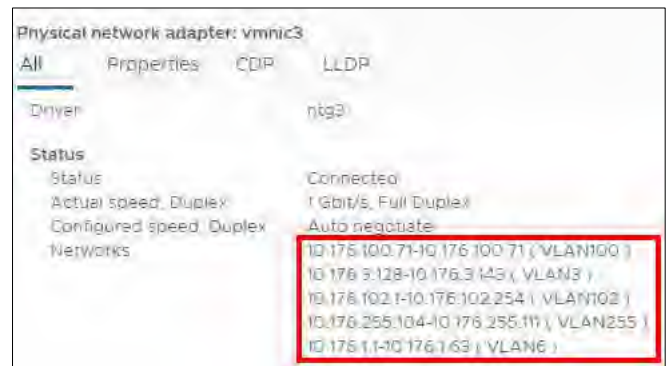


Figure 33. Wait for Networks to Appear

Configure tmcvhost02

- Refer to steps 1 and 2 in the **Configure tmcvhost01** procedures.
- Configure **vmnic2** and **vmnic3** on **tmcvhost02** in accordance with steps 1 and 2 of the **Configure tmcvhost01** procedures.

Configure tmcvhost03

Configure tmcvhost03 – vmnic2

#	Steps / Screenshots
---	---------------------

- Click host and clusters,
 - Click the down arrow next to **TMC Cluster**,
 - Click tmcvhost03.smartsunguide.com,
 - Click **Configure**,
 - Click Physical adapters, and,
 - Click **vmnic2**.

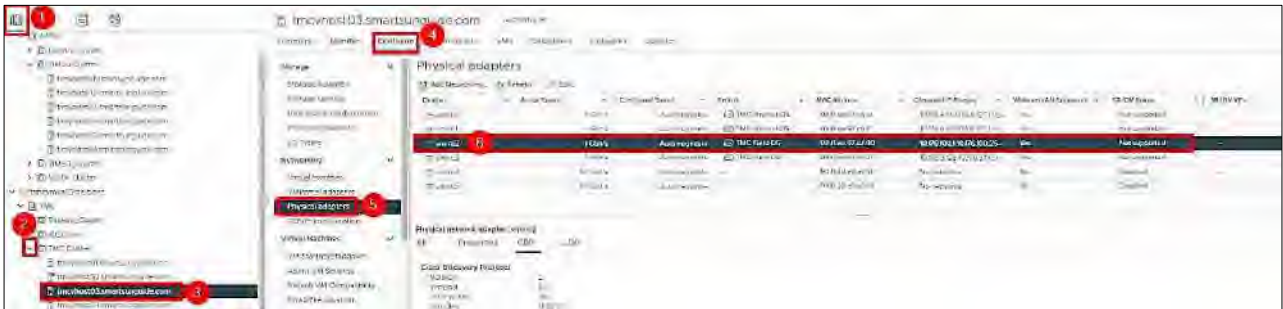


Figure 34. Configure tmcvhost03 - vmnic2.

- Click networking,
 - Right Click **TMC-Field-DS**,
 - Click Add and Manage Hosts.

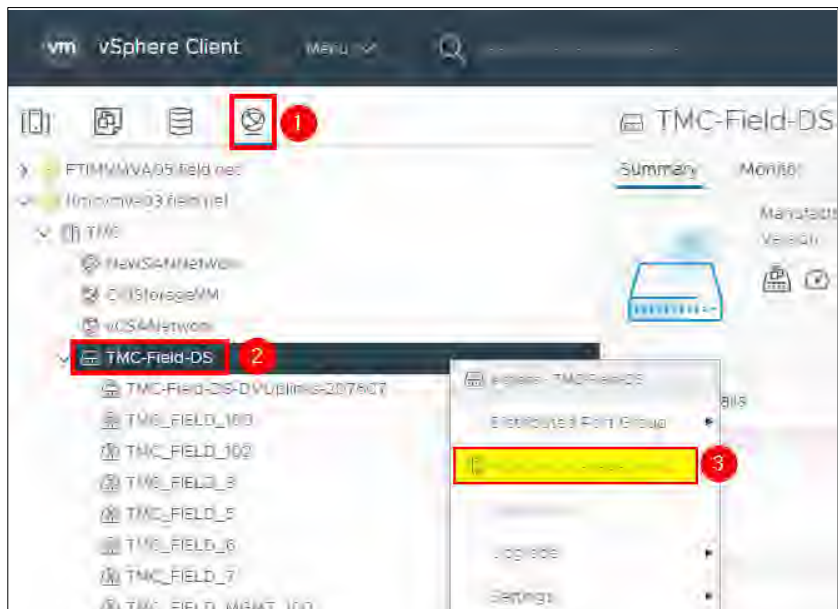


Figure 35. Add and Manage Hosts.

Steps / Screenshots

3.
 - Select Manage host networking.
 - Click **NEXT**.

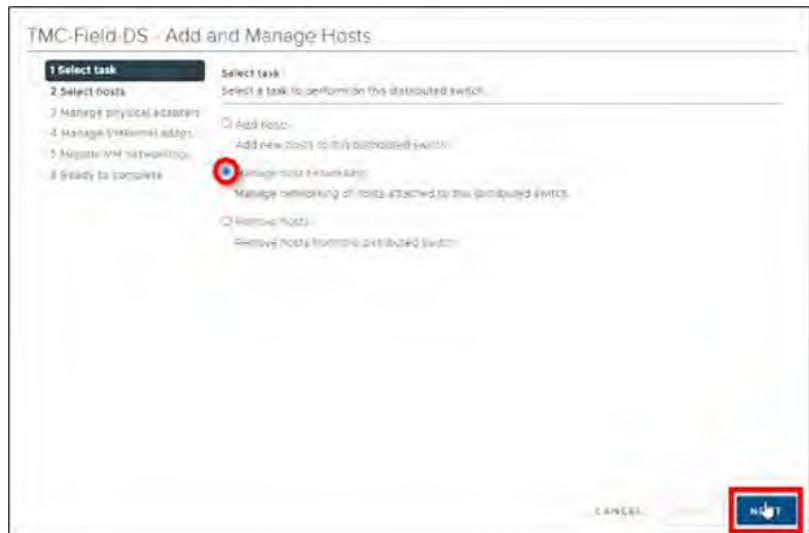


Figure 36. Select Task.

4.
 - Click Attached hosts.
 - Check the box next to tmcvhost03.smarsunguide.com, and,
 - Click **OK**.

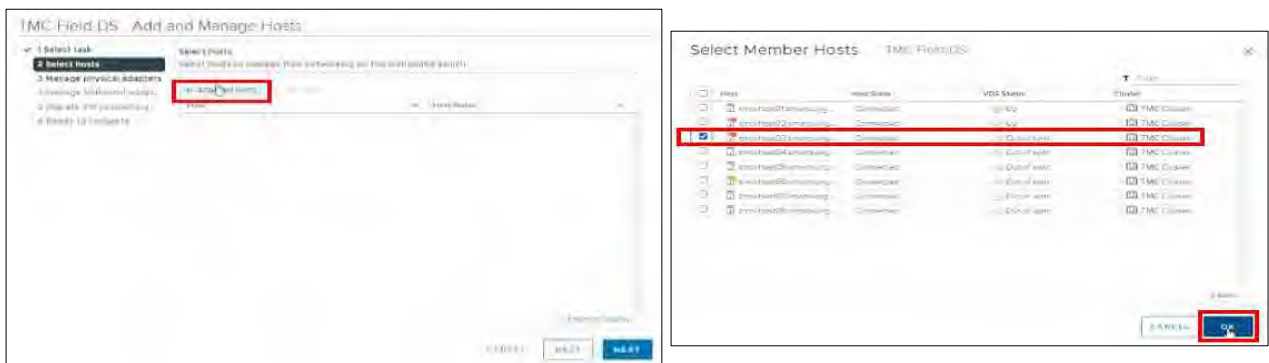


Figure 37. Select Member Host

5. Click **NEXT**.

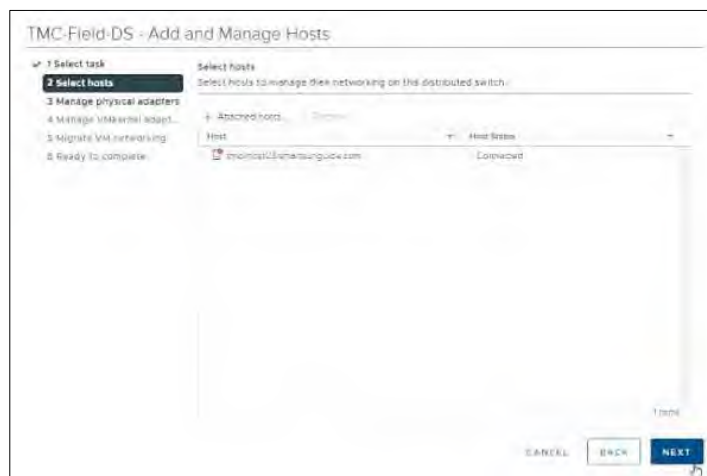


Figure 38. Select Host

Steps / Screenshots

6. (1) Select **vmnic3**
 (2) Click Assign **uplink**
 Add **vmnic3** to one of the LAG uplinks.
 (3) Select **LAG_1-1**
 (4) Click **OK**

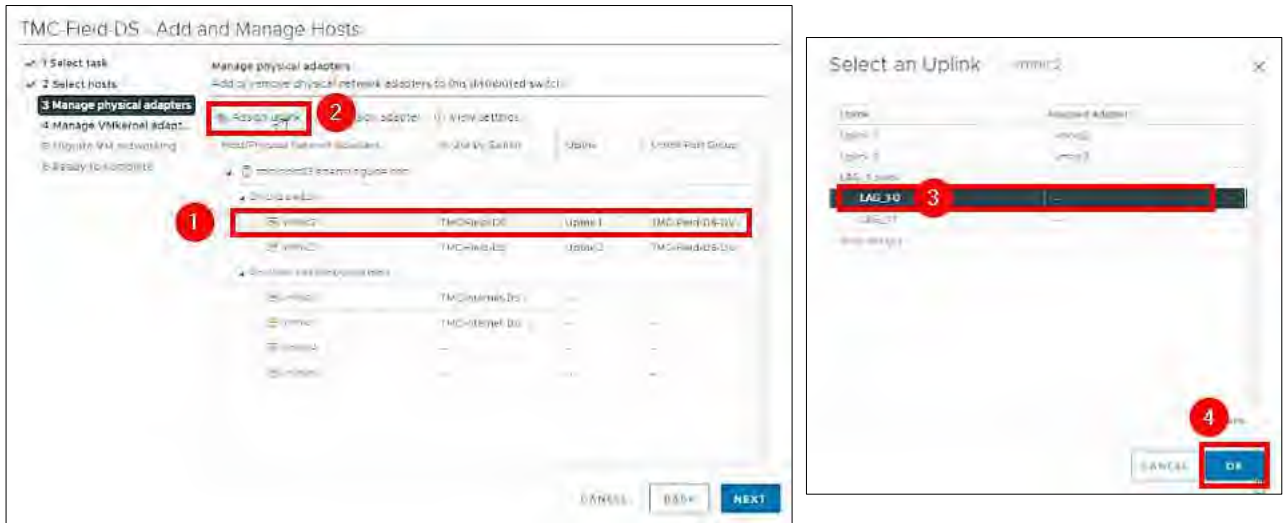


Figure 39. Manage Physical Adapters – Select an Uplink

7. Click **NEXT**.

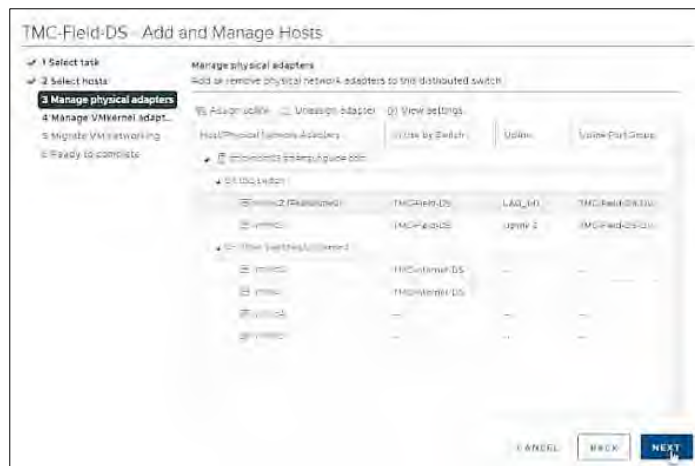


Figure 40. Manage Physical Adapters

Steps / Screenshots

8. Click **NEXT**.

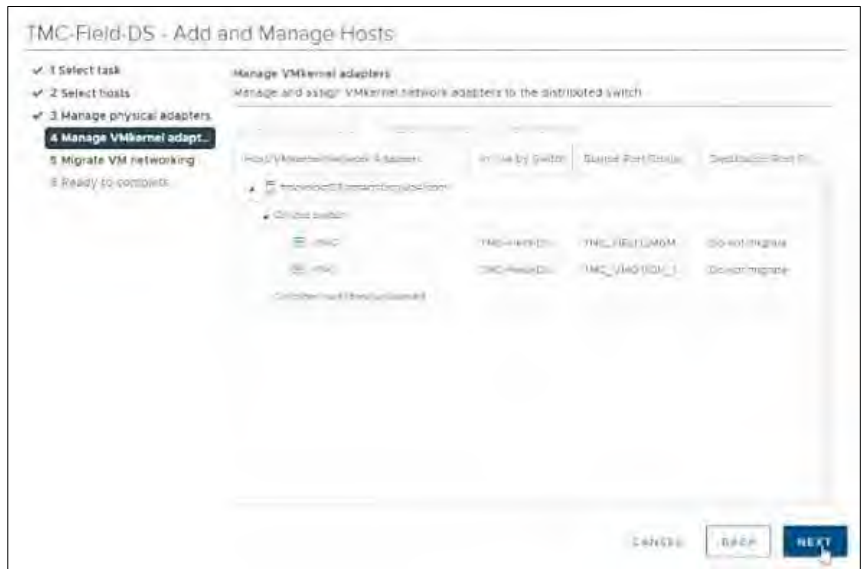


Figure 41. Manage VMkernel Adapters.

9. Click **NEXT**.

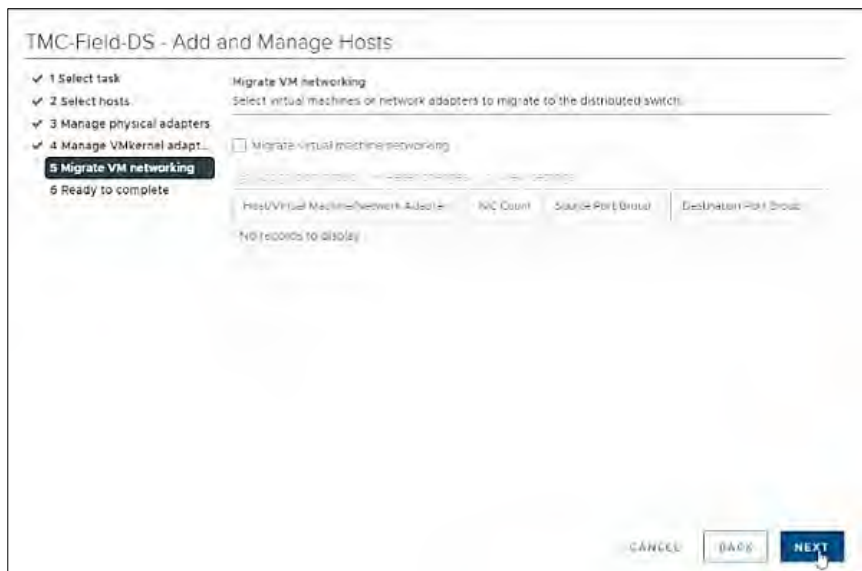


Figure 42. Migrate VM Networking

Steps / Screenshots

10. Click **FINISH**.

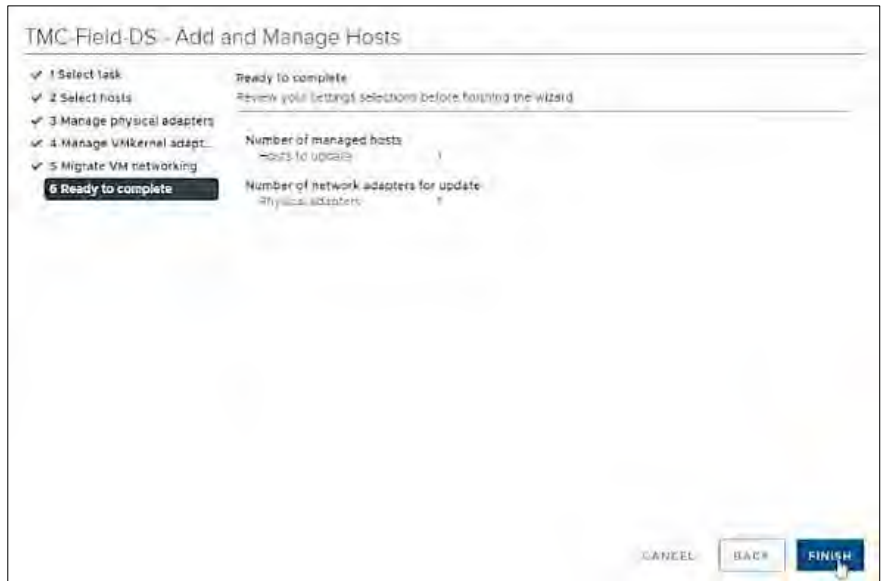


Figure 43. Ready to Complete.

11. Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), to be provided to the Network Manager.

- Device ID: **Switch # 1**
- Port ID: **Port # 3**

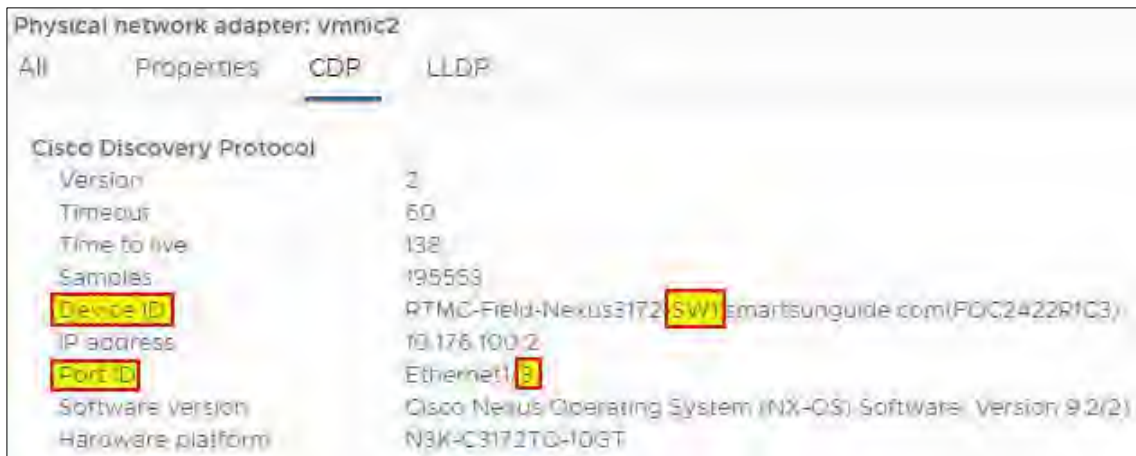


Figure 44. vmnic2 Device ID and Port ID

On the physical switch, the Network Manager will place the port connected to **vmnic2** in the LACP/EtherChannel configuration.

Configure tmcvhost03 – vmnic3

Steps / Screenshots

1.
 - (1)Click host and clusters,
 - (2)Click the down arrow next to TMC Cluster,
 - (3)Click tmcvhost03.smartsunguide.com,
 - (4)Click Configure,
 - (5)Click Physical adapters,
 - (6)Click vmnic3.
 - (7)Click the CDP tab to find the Device ID and Port ID (Switch # and Port #), to be provided to the Network Manager.

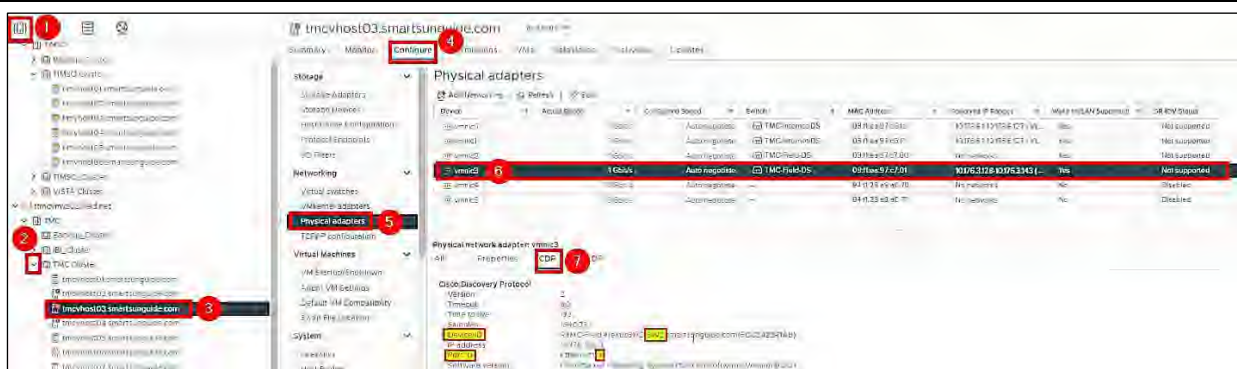
Device ID: **Switch # 2**Port ID: **Port # 3**

Figure 45. Configure tmcvhost03 – vmnic3.

2. On the physical switch, the Network Manager will down the port connected to **vmnic3**. Confirm that the port is down .

Name	Actual Speed	Connection Speed	Switch	MAC Address	Connected to Switch	Wake on LAN Supported	DRIV Status
vmnic0	Down	Auto negotiate	TMC-Internal-DS	08:00:27:00:00:00	1076.9128.1076.9127	No	Not supported
vmnic1	Down	Auto negotiate	TMC-Internal-DS	08:00:27:00:00:00	1076.9128.1076.9128	No	Not supported
vmnic2	Down	Auto negotiate	TMC-Field-BS	08:00:27:00:00:00	No connection	Yes	Not supported
vmnic3	Down	Auto negotiate	TMC-Field-BS	08:00:27:00:00:00	1076.9128.1076.9143	Yes	Not supported
vmnic4	Down	Auto negotiate	-	04:00:25:00:00:00	No connection	No	Disabled
vmnic5	Down	Auto negotiate	-	04:00:25:00:00:00	No connection	No	Disabled

Figure 46. Confirm that the Port is Down.

Steps / Screenshots

3. On the physical switch, the Network Manager will place the port connected to **vmnic3** in the LACP/EtherChannel configuration.

- Click networking,
- Right-click **TMC-Field-DS**,
- Click Add and Manage Hosts.

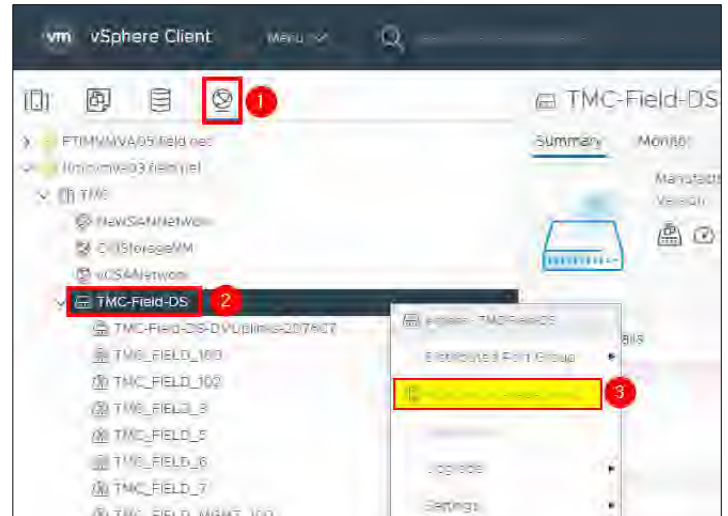


Figure 47. Add and Manage Hosts.

- 4.
- Select **Manage host networking**.
 - Click **NEXT**.

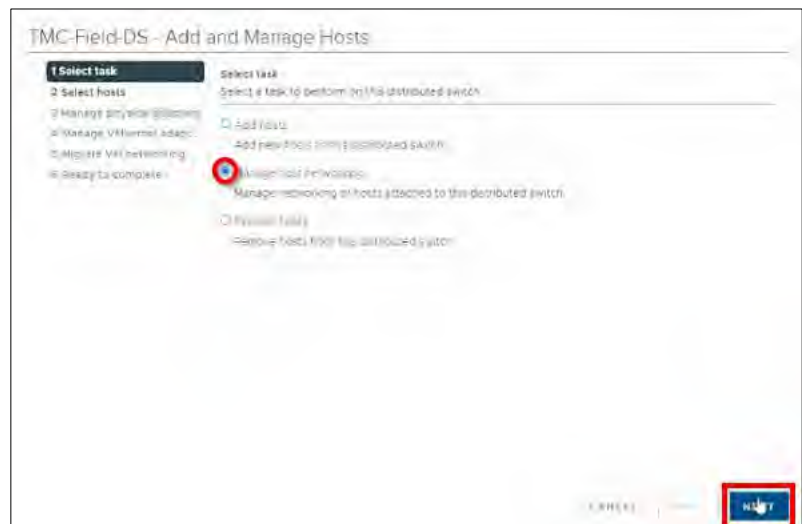


Figure 48. Select Task.

Steps / Screenshots

5.
 - Click Attached hosts,
 - Check the box next to tmcvhost03.smarsunguide.com,
 - Click **OK**.

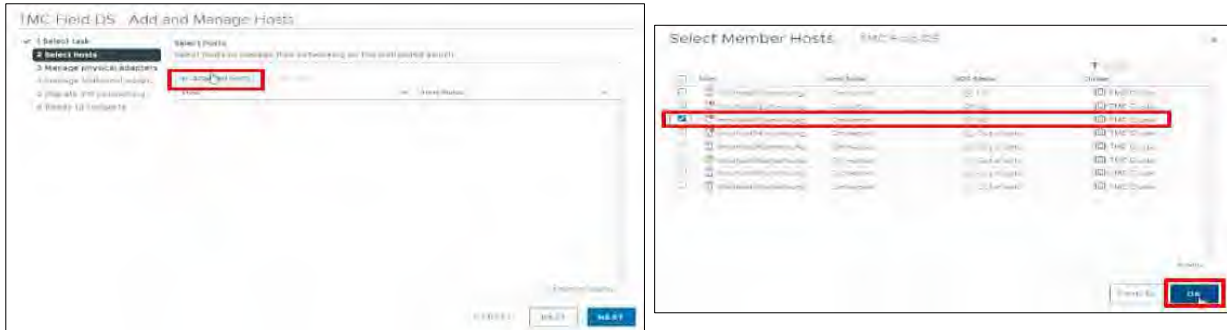


Figure 49. Select Member Host.

6. Click **NEXT**

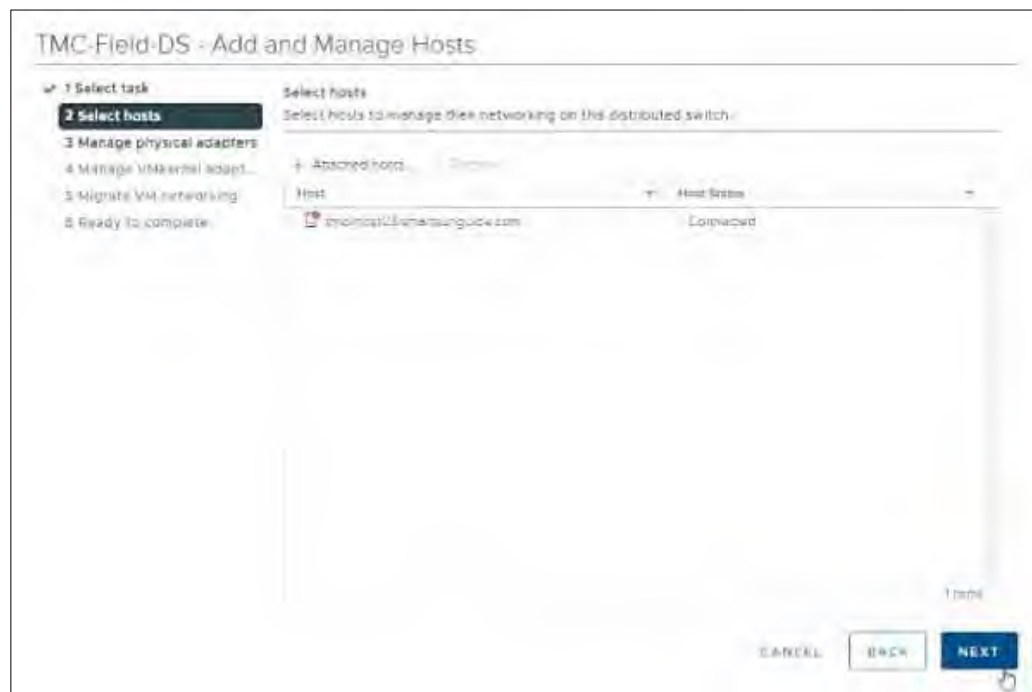


Figure 50. Select Host.

7.
 - Add vmnic3 to one of the LAG uplinks by selecting vmnic3 and clicking on Assign uplink.
 - Select **LAG_1-1** and
 - Click **OK**.

Steps / Screenshots

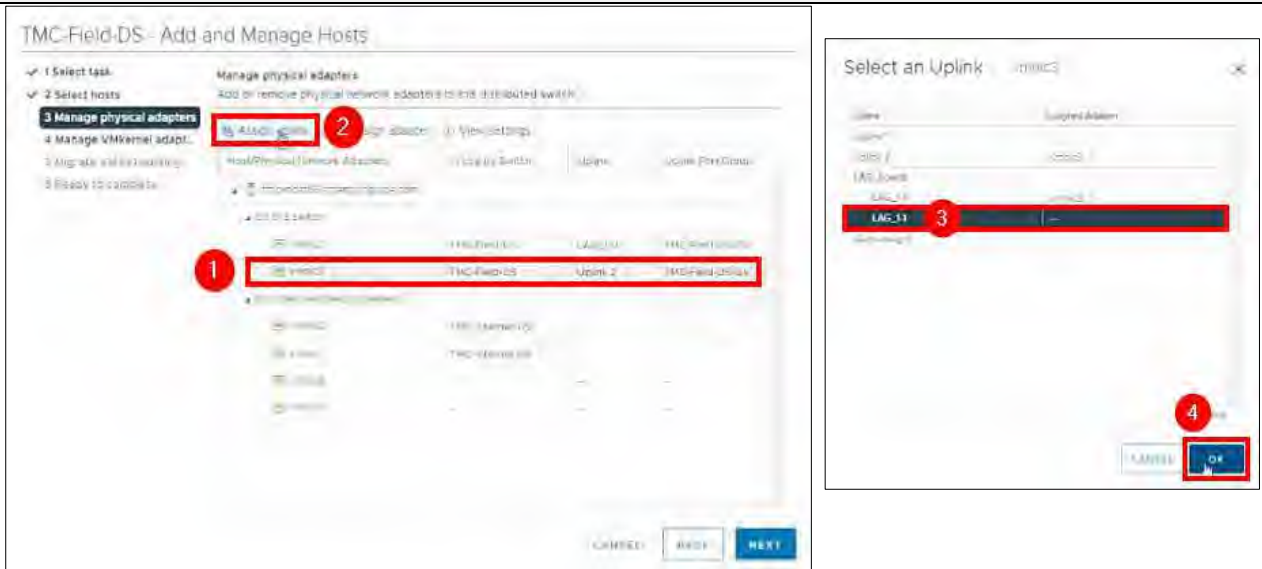


Figure 51. Manage Physical Adapters – Select an Uplink.

8. Click **NEXT** .

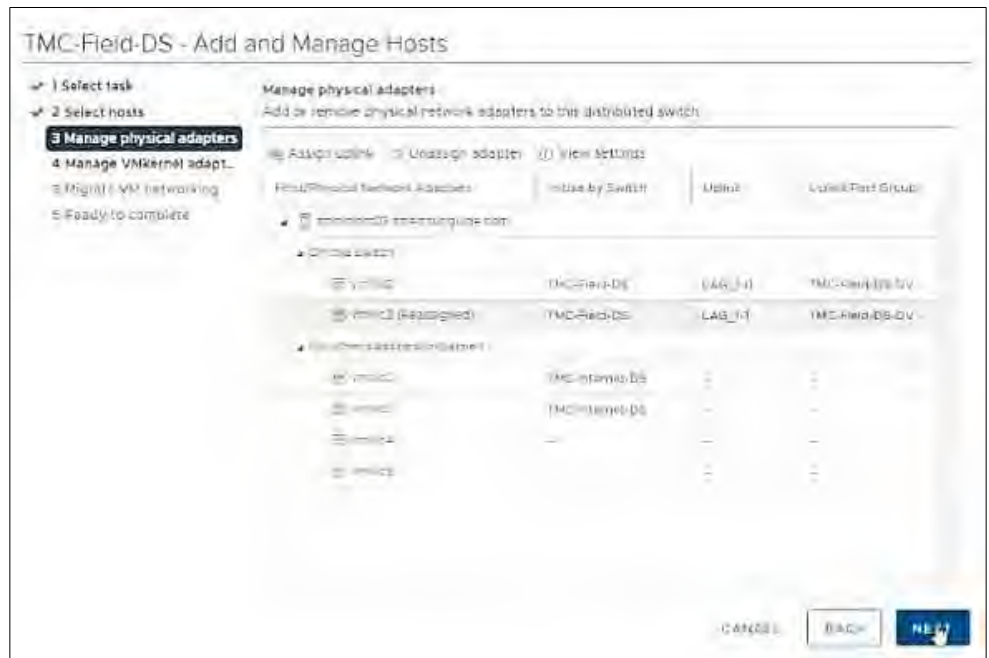


Figure 52. Manage Physical Adapters.

Steps / Screenshots

9. Click **NEXT**.



Figure 53. Manage VMkernel Adapters.

10. Click **NEXT**.

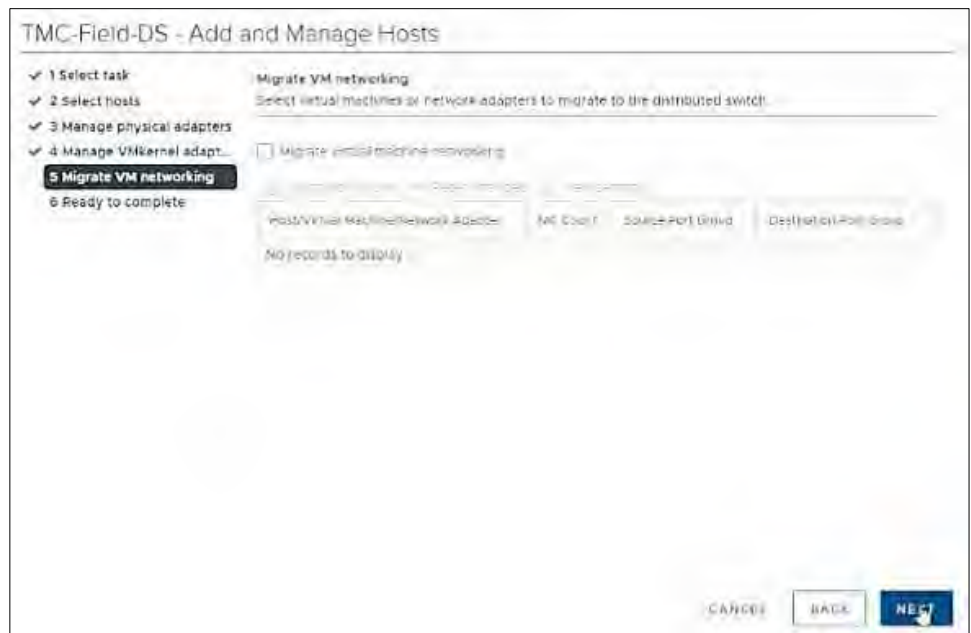


Figure 54. Migrate VM Networking.

Steps / Screenshots

11, Click **FINISH**.

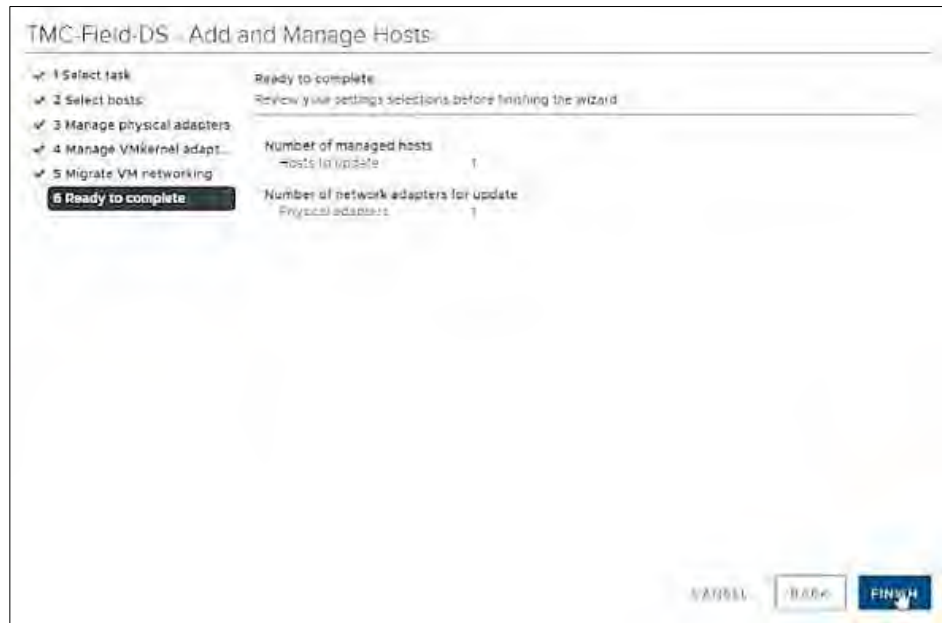


Figure 55. Ready to Complete.

12. The Network Manager will bring the port back up.

Go back **Physical adapters** and wait for port to come back up,

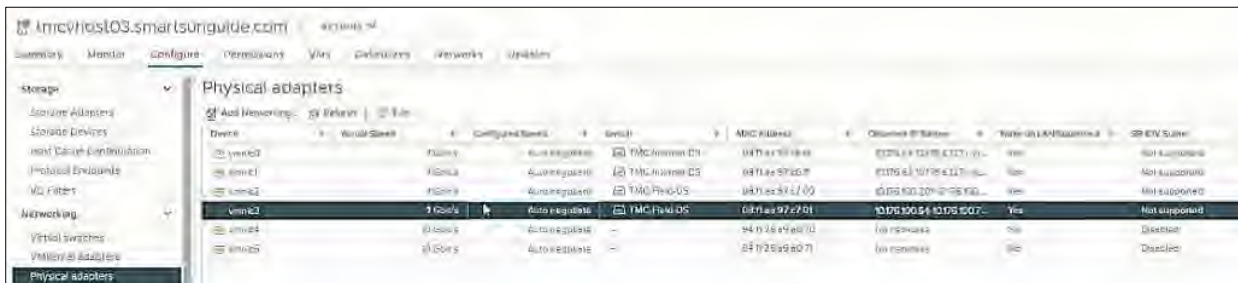


Figure 56. Wait for Port to Come Back Up.

13. Click the **All** tab and wait for networks to appear.

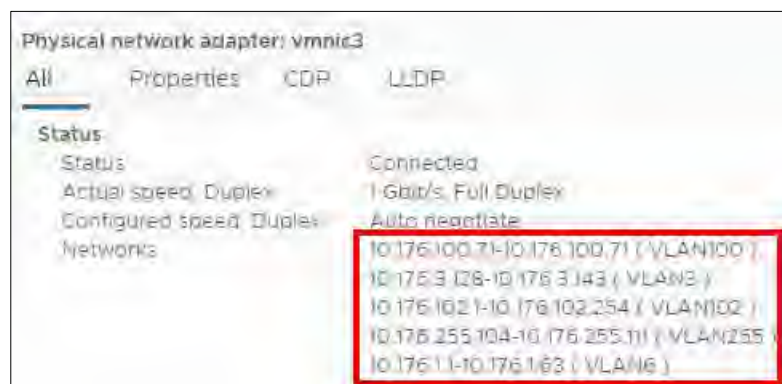


Figure 57. Wait for Networks to Appear.

Configure tmcvhost04 – tmcvhost08

1. Refer to steps 1 and 2 in the **Configure tmcvhost03** procedures.
2. Configure **vmnic2** and **vmnic3** on **tmcvhost04, tmcvhost05, tmcvhost06, tmcvhost07, tmcvhost08** in accordance with steps 1 and 2 of the **Configure tmcvhost03** procedures.

Edit Distributed Port Groups for TMC-Field-DS

Perform steps 1 to 3 below to change the Teaming and Failover for all distributed port groups to use the LAG instead of the uplinks.

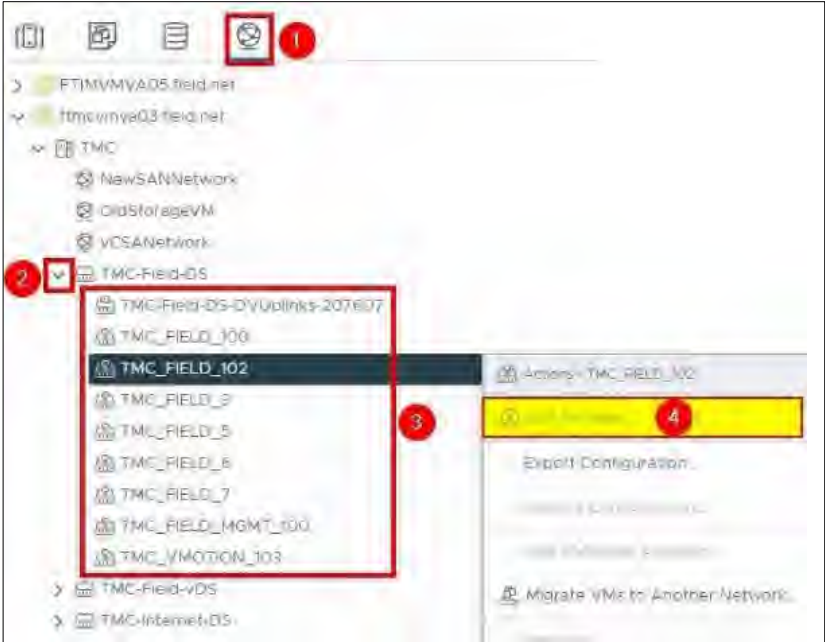
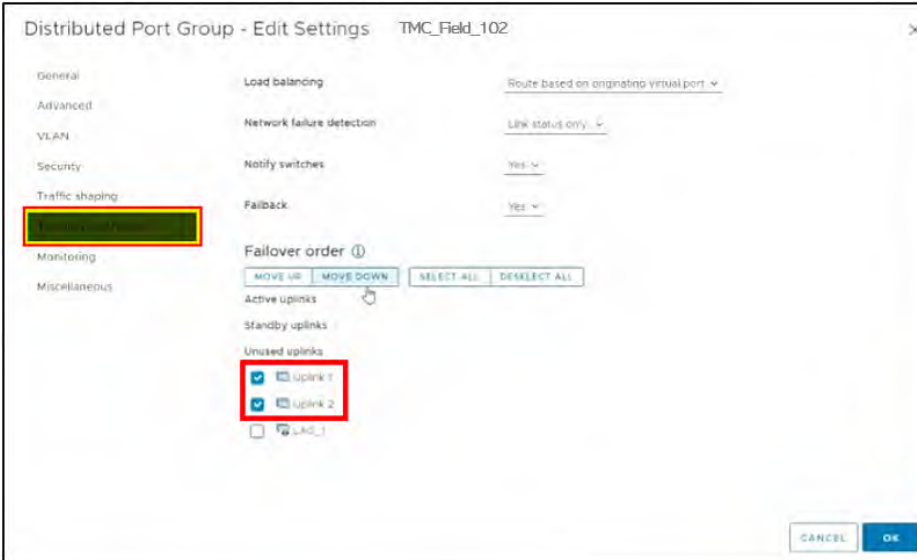
#	Steps / Screenshots	
1	<ul style="list-style-type: none"> – (1) Click Networking, – (2) Click the down arrow next to TMC-Field-DS, – (3) Right-click one of the distributed port groups, – (4) Click Edit Settings. 	
2	<ul style="list-style-type: none"> – Click Teaming and Failover, – Move Uplink 1 and Uplink 2 to Unused uplinks. 	

Figure 58. Edit Distributed Port Groups for TMC-Field-DS

Steps / Screenshots

Figure 59. Move Uplink 1 and Uplink 2 to Unused Uplinks.

- 3
- Move **LAG_1** to Active uplinks.
 - Click **OK**.

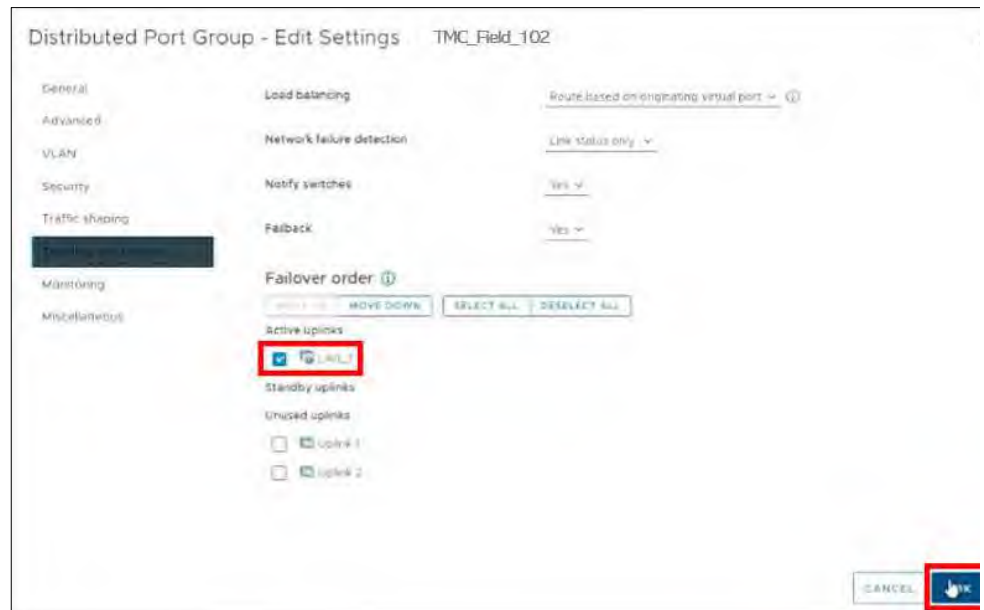


Figure 60. Move LAG_1 to Active Uplinks.

Repeat steps 1 to 3 above on all other distributed port groups under TMC-Field-DS.

Create Link Aggregation Group (LAG) Group for TMC-Internet-DS

Steps / Screenshots

1.
 - (1) Click `ftmcmvma03.field.net`
 -
 - (2) Click Networking.



Figure 61. `ftmcmvma03.field.net` > Networking.

2.
 - (1) Click the down arrow next to `ftmcmvma03.field.net` and
 - (2) Click the down arrow next to **TMC**.
 - (3) Click TMC-Internet-DS,
 - (4) Click Configure,
 - (5) Click **LACP**,
 - (6) Click **NEW** .

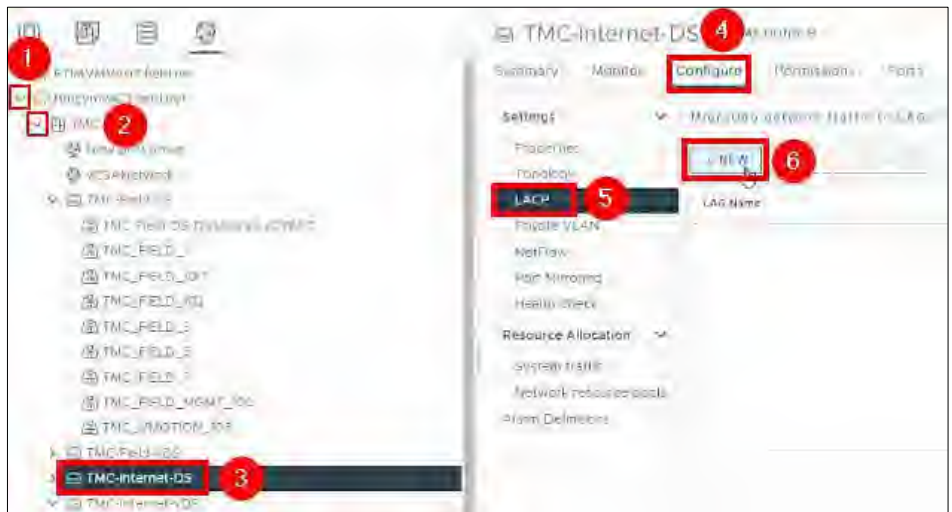


Figure 62. TMC-Internet-DS > Configure > LACP > NEW.

3.
 - Enter the following information in the **New LAG** window:
 Name: **LAG_1**
 Number of ports: **2**
 Mode: **Active**
 Load balancing mode: Source and destination Mac address
 Timeout mode: **slow**
 - Click **OK** .

Steps / Screenshots

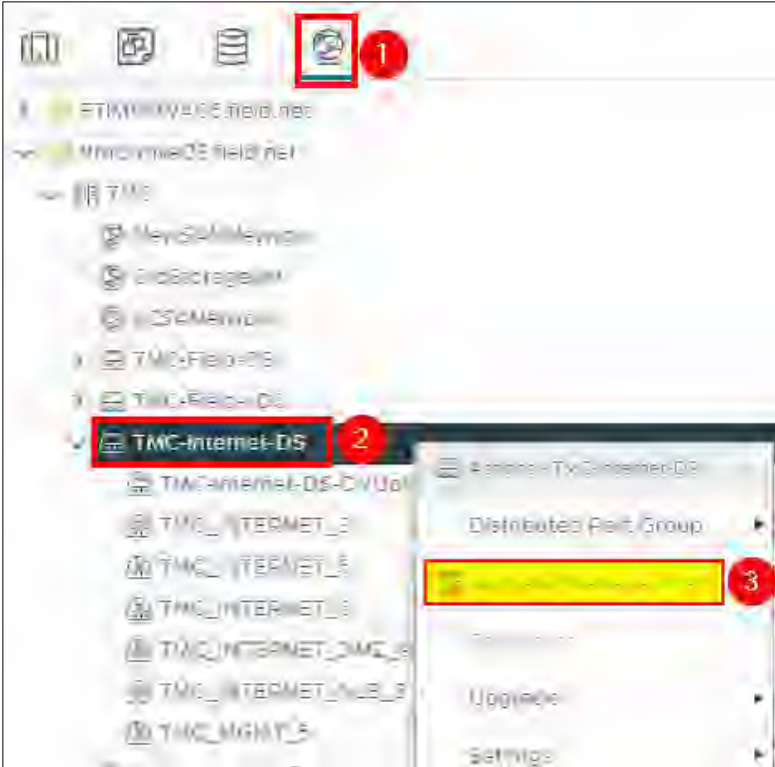
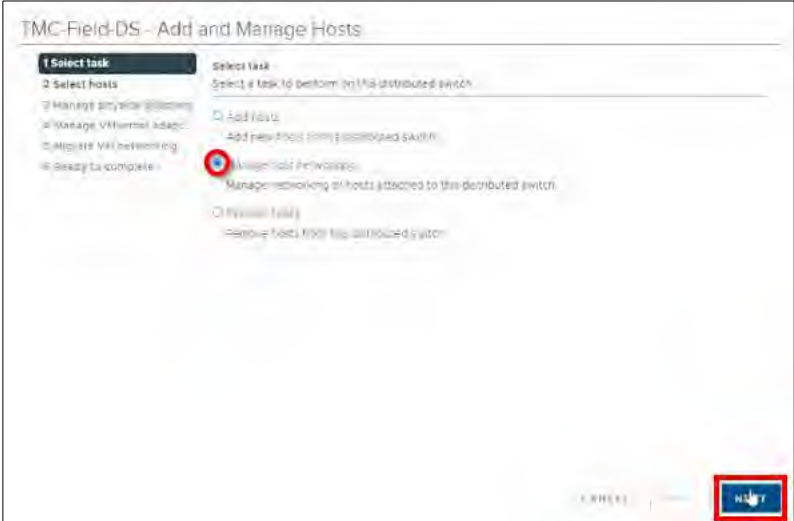



Figure 63. New LAG – LAG_1.


Configure tmcvhost01 – tmcvhost08

#	Steps / Screenshots
1.	– Configure vmnic0 and vmnic1 on all hosts (tmcvhost01 – tmcvhost08).

#	Steps / Screenshots																																																												
	<p>The Network Manager configures the ports for vmnic0 and vmnic1 on all TMC hosts .</p> <p><i>Table 1. TMC Hosts & Physical Adapters - Switch and Port Numbers.</i></p> <table border="1"> <thead> <tr> <th>Host</th> <th>Physical Adapters</th> <th>Switch #</th> <th>Port #</th> </tr> </thead> <tbody> <tr> <td rowspan="2">tmcvhost01</td> <td>vmnic0</td> <td>1</td> <td>1</td> </tr> <tr> <td>vmnic1</td> <td>2</td> <td>1</td> </tr> <tr> <td rowspan="2">tmcvhost02</td> <td>vmnic0</td> <td>1</td> <td>2</td> </tr> <tr> <td>vmnic1</td> <td>2</td> <td>2</td> </tr> <tr> <td rowspan="2">tmcvhost03</td> <td>vmnic0</td> <td>1</td> <td>3</td> </tr> <tr> <td>vmnic1</td> <td>2</td> <td>3</td> </tr> <tr> <td rowspan="2">tmcvhost04</td> <td>vmnic0</td> <td>1</td> <td>4</td> </tr> <tr> <td>vmnic1</td> <td>2</td> <td>4</td> </tr> <tr> <td rowspan="2">tmcvhost05</td> <td>vmnic0</td> <td>1</td> <td>5</td> </tr> <tr> <td>vmnic1</td> <td>2</td> <td>5</td> </tr> <tr> <td rowspan="2">tmcvhost06</td> <td>vmnic0</td> <td>1</td> <td>6</td> </tr> <tr> <td>vmnic1</td> <td>2</td> <td>6</td> </tr> <tr> <td rowspan="2">tmcvhost07</td> <td>vmnic0</td> <td>1</td> <td>7</td> </tr> <tr> <td>vmnic1</td> <td>2</td> <td>7</td> </tr> <tr> <td rowspan="2">tmcvhost08</td> <td>vmnic0</td> <td>1</td> <td>8</td> </tr> <tr> <td>vmnic1</td> <td>2</td> <td>8</td> </tr> </tbody> </table>	Host	Physical Adapters	Switch #	Port #	tmcvhost01	vmnic0	1	1	vmnic1	2	1	tmcvhost02	vmnic0	1	2	vmnic1	2	2	tmcvhost03	vmnic0	1	3	vmnic1	2	3	tmcvhost04	vmnic0	1	4	vmnic1	2	4	tmcvhost05	vmnic0	1	5	vmnic1	2	5	tmcvhost06	vmnic0	1	6	vmnic1	2	6	tmcvhost07	vmnic0	1	7	vmnic1	2	7	tmcvhost08	vmnic0	1	8	vmnic1	2	8
Host	Physical Adapters	Switch #	Port #																																																										
tmcvhost01	vmnic0	1	1																																																										
	vmnic1	2	1																																																										
tmcvhost02	vmnic0	1	2																																																										
	vmnic1	2	2																																																										
tmcvhost03	vmnic0	1	3																																																										
	vmnic1	2	3																																																										
tmcvhost04	vmnic0	1	4																																																										
	vmnic1	2	4																																																										
tmcvhost05	vmnic0	1	5																																																										
	vmnic1	2	5																																																										
tmcvhost06	vmnic0	1	6																																																										
	vmnic1	2	6																																																										
tmcvhost07	vmnic0	1	7																																																										
	vmnic1	2	7																																																										
tmcvhost08	vmnic0	1	8																																																										
	vmnic1	2	8																																																										

#	Steps / Screenshots	
2.	<ul style="list-style-type: none"> - (1) Click networking, - (2) Right-click TMC-Field-DS, - (3) Click Add and Manage Hosts. 	 <p style="text-align: center;">Figure 64. Add and Manage Hosts.</p>
3.	<ul style="list-style-type: none"> - Select Manage host networking. - Click NEXT. 	 <p style="text-align: center;">Figure 65. Select Task.</p>

#	Steps / Screenshots
4.	<ul style="list-style-type: none"> - Click Attached hosts, - Check the box next to all TMC hosts (tmcvhost01 – tmcvhost08), - Click OK. <div style="display: flex; justify-content: space-around; margin-top: 10px;">  </div> <p style="text-align: center; margin-top: 5px;"><i>Figure 66. Select Member Hosts.</i></p>

5.	<p>Click NEXT .</p> <div style="margin-top: 10px;">  </div> <p style="text-align: center; margin-top: 5px;"><i>Figure 67. Select Hosts</i></p>
----	--

Assign Uplinks to the Hosts

Assign uplinks for tmcvhost01

- (1) Click **vmnic0**
- (2) Click Assign uplink
- (3) Select **LAG_1-0**
- (4) Click **OK**
- (5) Click **vmnic1**
- (6) Click Assign uplink
- (7) Select **LAG_1-1**
- (8) Click **OK**.

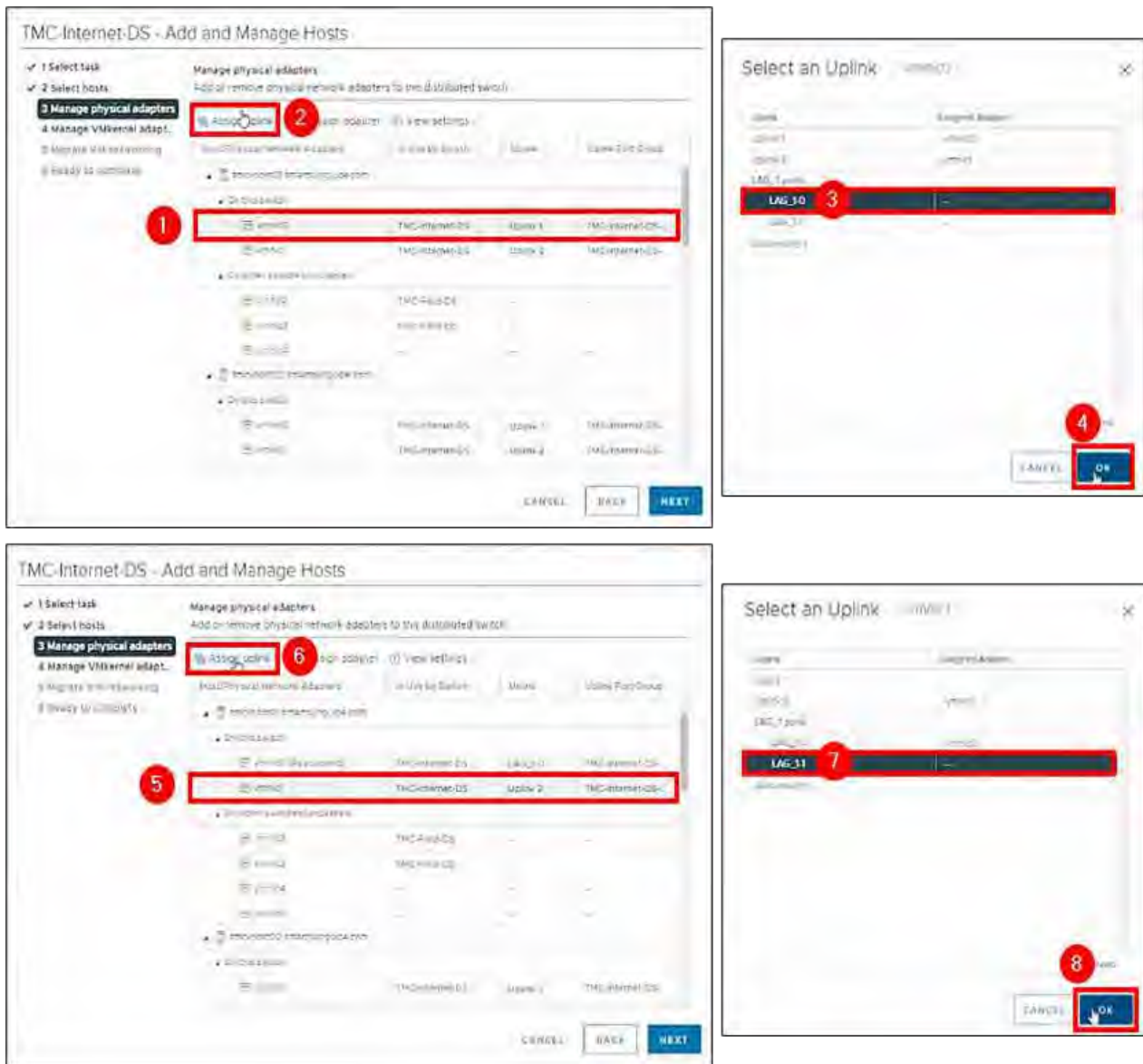


Figure 68. Manage Physical Adapters – Assign Uplinks for tmcvhost01.

Assign uplinks for tmcvhost02

Scroll down to **tmcvhost02**.

- (1) Click **vmnic0** and
- (2) Click Assign uplink
- (3) Select **LAG_1-0** and
- (4) Click **OK**.
- (5) Click **vmnic1** and
- (6) Click Assign uplink
- (7) Select **LAG_1-1** and
- (8) Click **OK**.

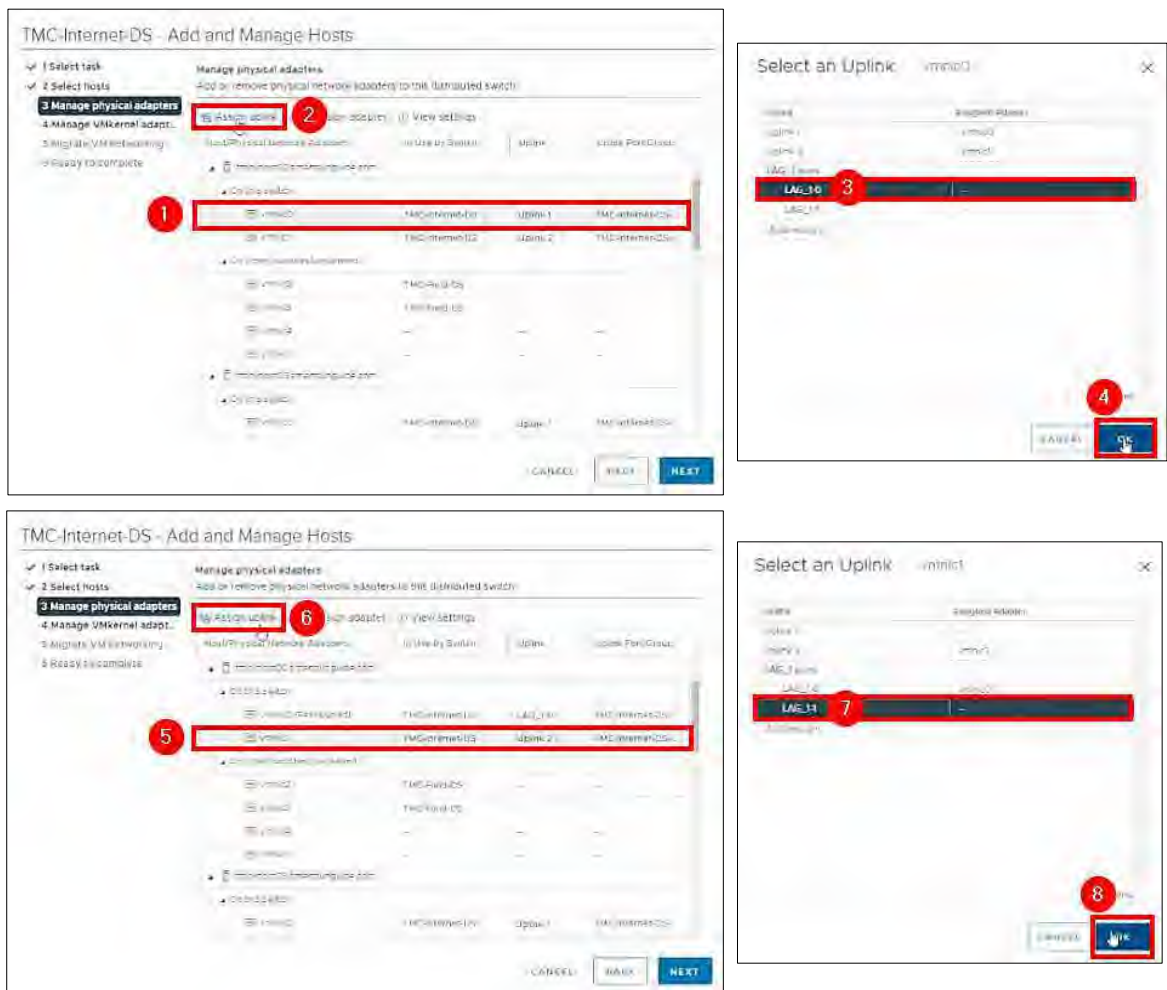


Figure 69. Manage Physical Adapters – Assign Uplinks for tmcvhost02

Assign uplinks for tmcvhost03

Scroll down to **tmcvhost03**.

- (1) Click **vmnic0**
- (2) Click Assign uplink .
- (3) Select **LAG_1-0**
- (4) Click **OK**.
- (5) Click **vmnic1**
- (6) Click Assign uplink
- (7) Select **LAG_1-1**
- (8) Click **OK**.

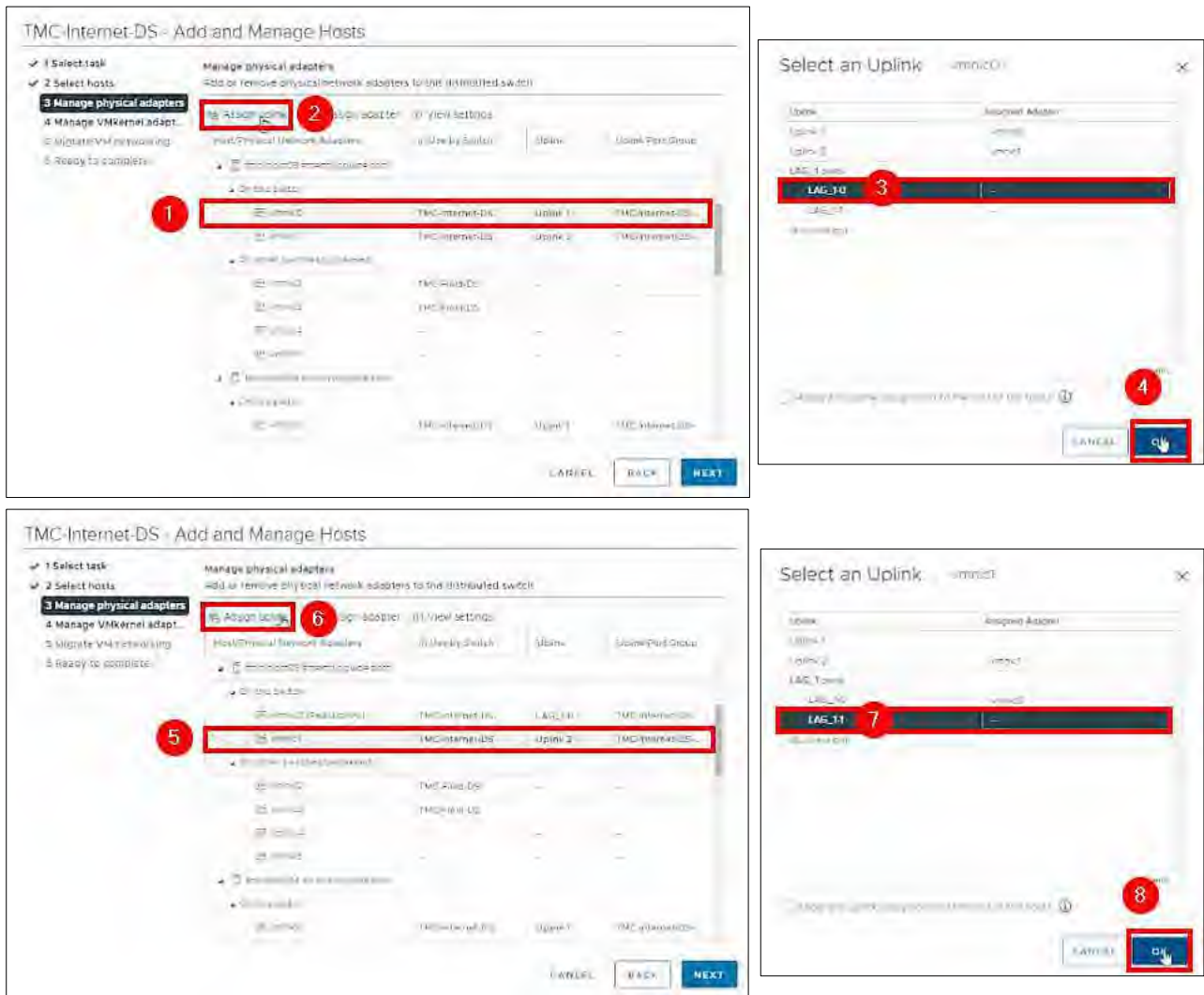


Figure 70. Manage Physical Adapters – Assign Uplinks for tmcvhost03.

Assign uplinks for tmcvhost04

Scroll down to **tmcvhost04**.

- (1) Click **vmnic0**
- (2) Click Assign uplink
- (3) Select **LAG_1-0**
- (4) Click **OK**
- 5) Click **vmnic1**
- 6) Click Assign uplink
- (7) Select **LAG_1-1**
- (8) Click **OK**.

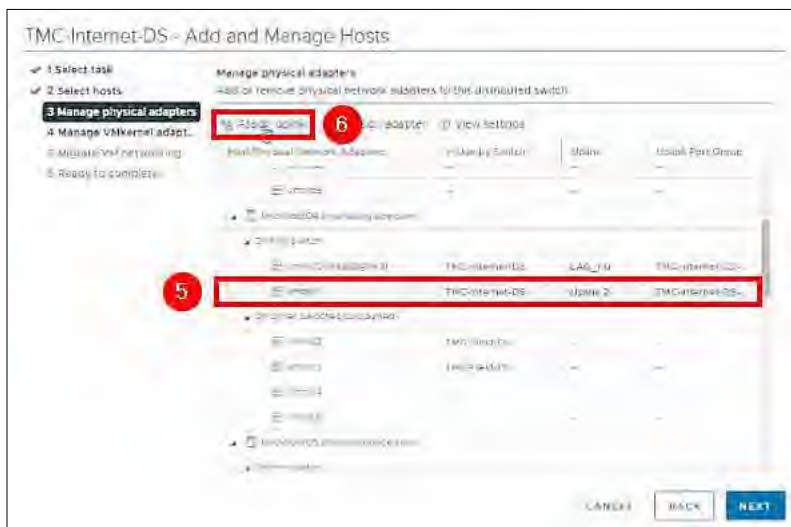
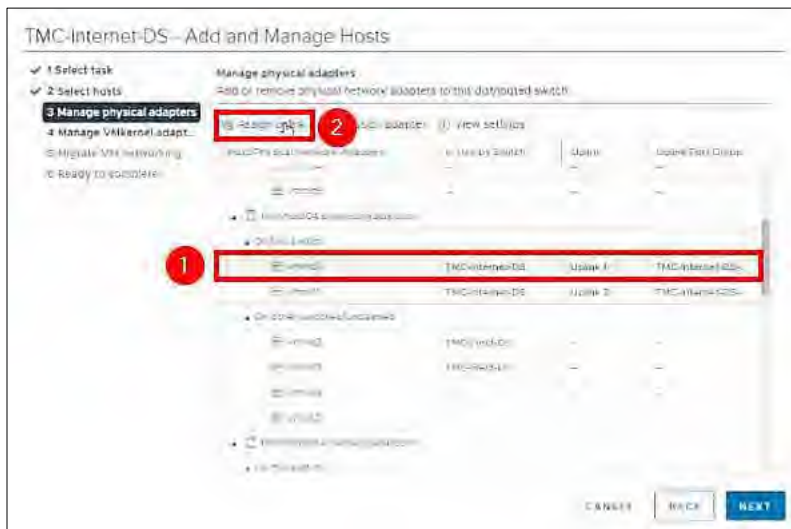


Figure 71. Manage Physical Adapters – Assign Uplinks for tmcvhost04.

Assign uplinks for tmcvhost05

Scroll down to **tmcvhost05**.

- (1) Click **vmnic0** and
- (2) Click **Assign uplink**.
- (3) Select **LAG_1-0**
- (4) Click **OK**.
- (5) Click **vmnic1**
- (6) Click **Assign uplink**
- (7) Select **LAG_1-1**
- (8) Click **OK**.

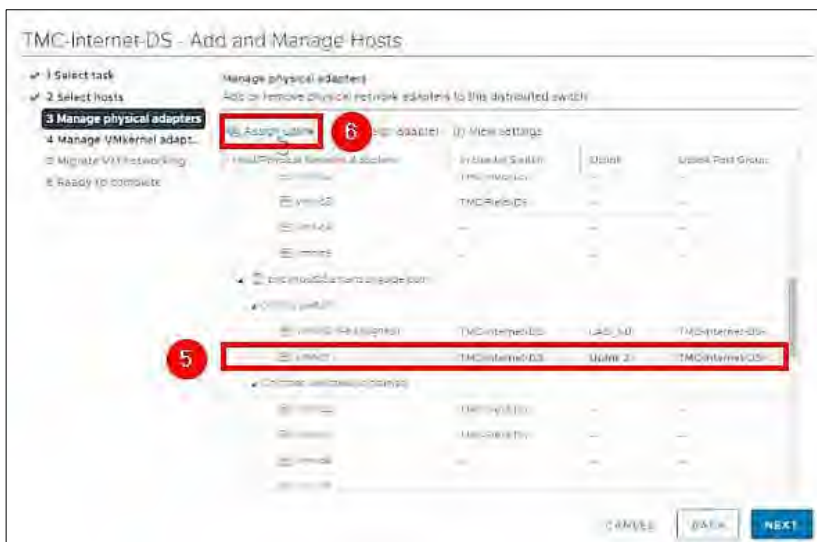
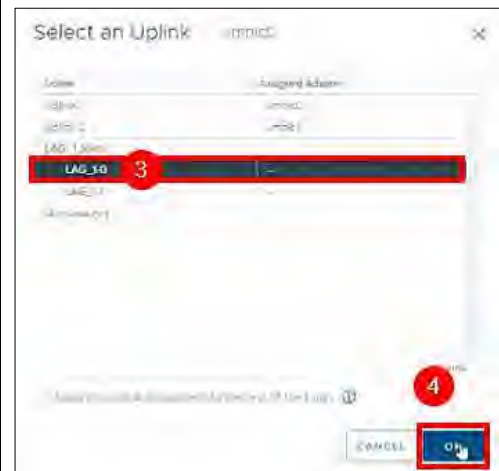
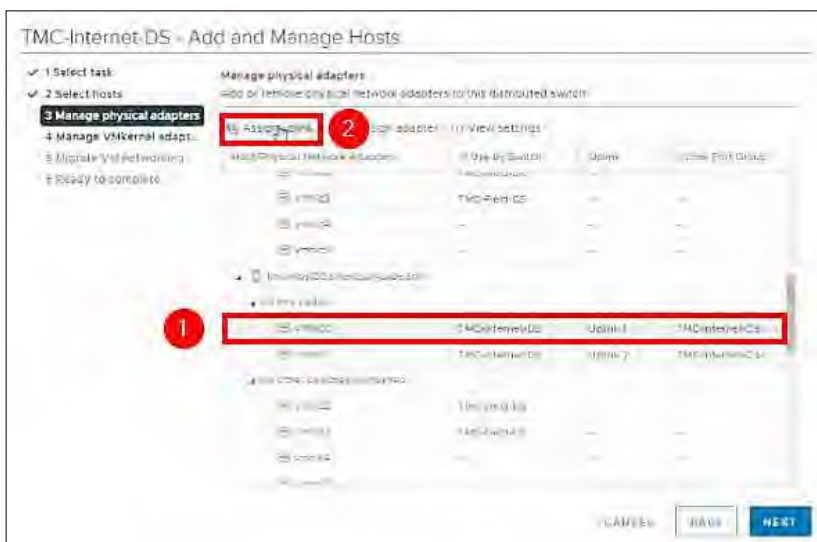


Figure 72. Manage Physical Adapters – Assign Uplinks for tmcvhost05.

Assign uplinks for tmcvhost06

Scroll down to **tmcvhost06**.

- (1) Click **vmnic0**
- (2) Click **Assign uplink**
- (3) Select **LAG_1-0**
- (4) Click **OK**
- (5) Click **vmnic1**
- (6) Click **Assign uplink**
- (7) Select **LAG_1-1**
- (8) Click **OK**.

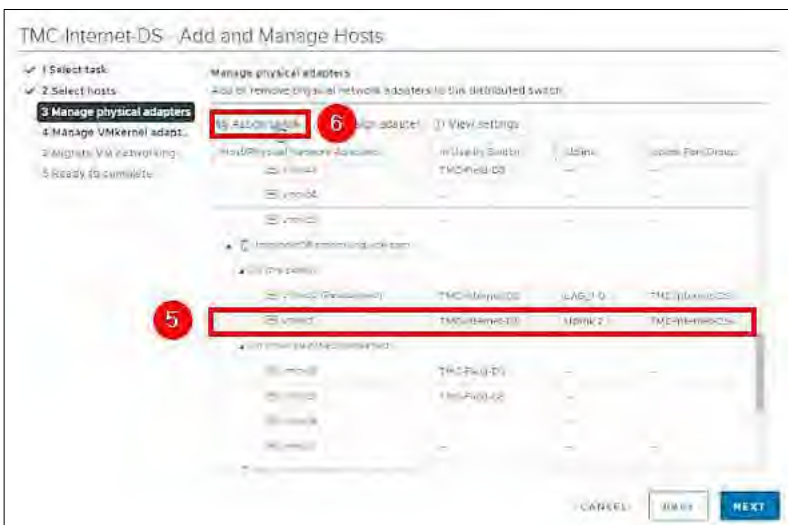
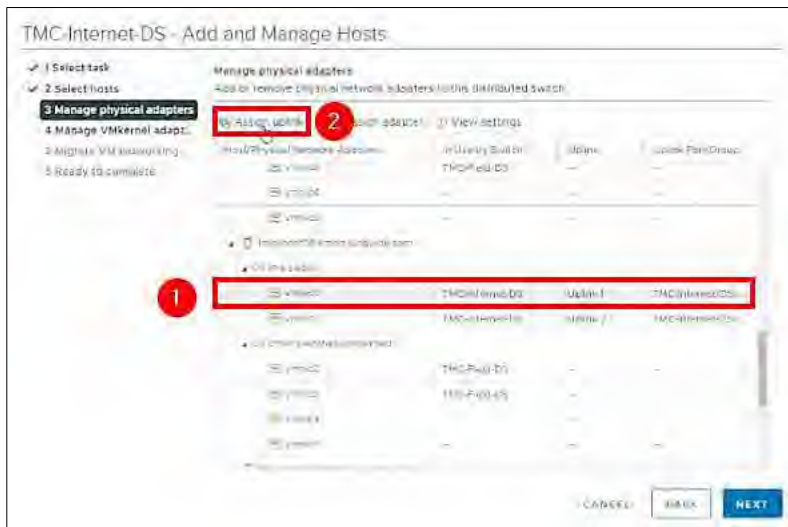


Figure 73. Manage Physical Adapters – Assign Uplinks for tmcvhost06.

Assign uplinks for tmcvhost07

Scroll down to **tmcvhost07**.

- Click **vmnic0**.
- Click Assign uplink.
- Select **LAG_1-0**.
- Click **OK**.
- Click **vmnic1**.
- Click Assign uplink.
- Select **LAG_1-1**.
- Click **OK**.

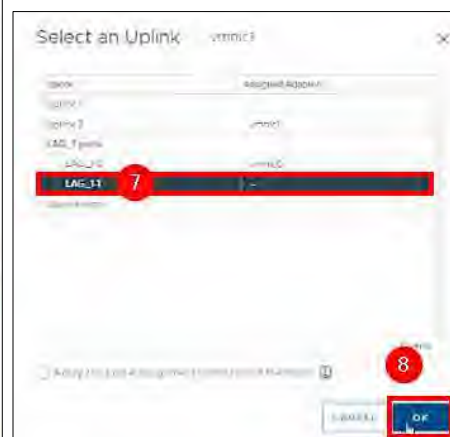
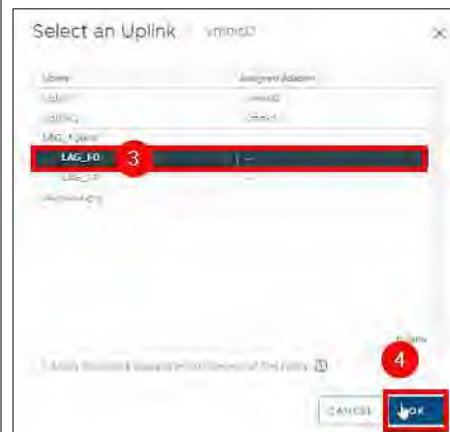
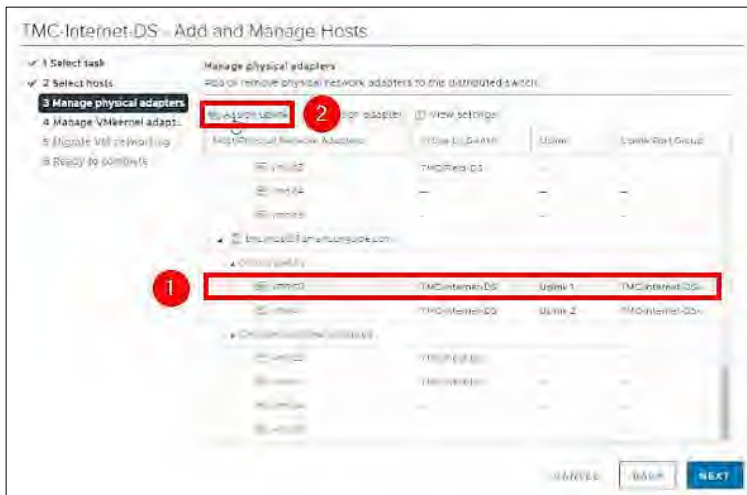


Figure 74. Manage Physical Adapters – Assign Uplinks for tmcvhost07.

Assign uplinks for tmcvhost08
 Scroll down to **tmcvhost08**.

- Click **vmnic0** and
- Click **Assign uplink**.
- select **LAG_1-0** and
- Click **OK**
- Click **vmnic1** and
- Click **Assign uplink**.
- Select **LAG_1-1**
- Click **OK**

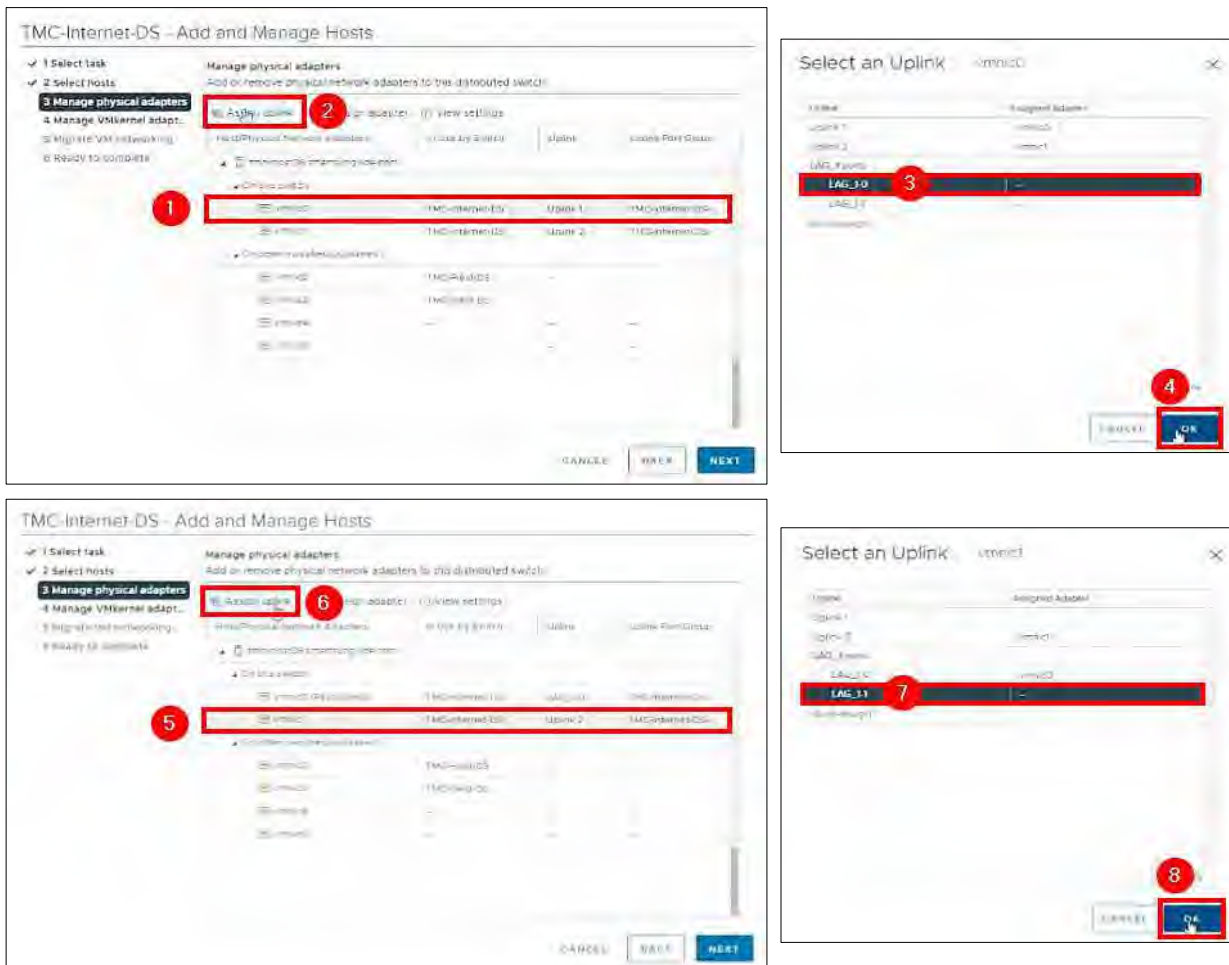


Figure 75. Manage Physical Adapters – Assign Uplinks for tmcvhost08.

Complete following Links Assigning

1. Click **NEXT**.



Figure 76. Manage VMkernel Adapters.

2. Click **NEXT**.



Figure 77. Migrate VM Networking.

3. Click **FINISH**.



Figure 78. Ready to Complete.

Edit Distributed Port Groups for TMC-Internet-DS

Perform steps a – c below, to change the **Teaming and Failover** for all distributed port groups to use the LAG instead of the uplinks.

1.
 - Click Networking
 - Click the down arrow next to **TMC-Internet-DS**
 - Right-click one of the distributed port groups
 - Click Edit Settings.

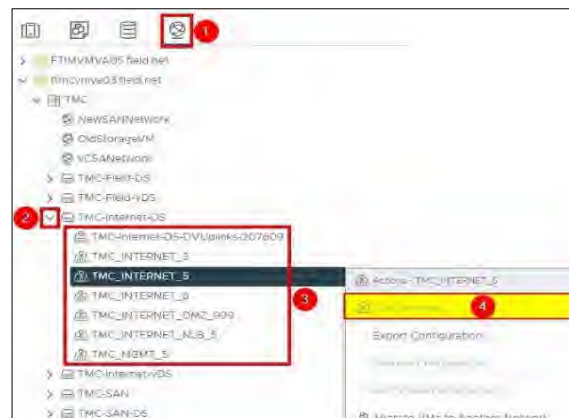


Figure 79. Edit Distributed Port Groups for TMC-Internet-DS.

2.
 - Click Teaming and Failover
 - Move **Uplink 1** and **Uplink 2** to Unused uplinks.



Figure 80. Move Uplink 1 and Uplink 2 to Unused Uplinks.

3.
 - Move **LAG_1** to Active uplinks
 - Click **OK**.

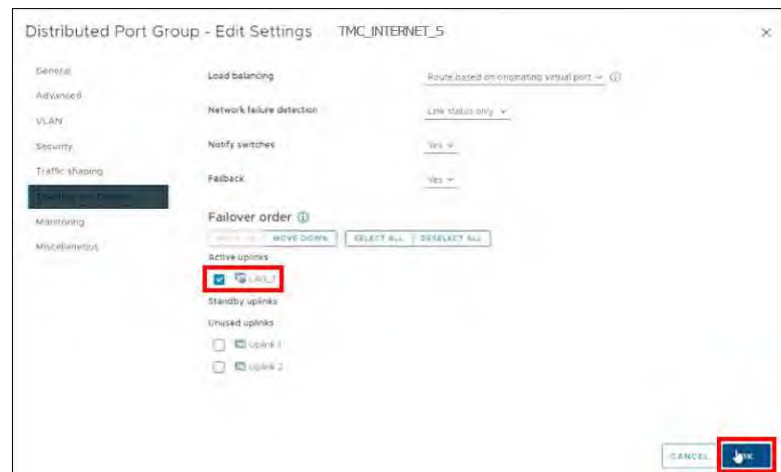


Figure 81. Move LAG_1 to Active Uplinks.

Repeat steps 1-3 above on all other distributed port groups under TMC-Internet-DS.

NIC TEAMING in VMware – TIMSO

Create Link Aggregation Group (LAG) for TIMSO-DS

Note. Only one LAG is needed for the distributed switch. Each host at TIMSO will have four ports.

Steps / Screenshots

1.
 - (1) Click FTIMVMVA05.field.net
 - (2) Click **Networking**



Figure 82. FTIMVMVA05.field.net > Networking

2.
 - (1) Click the down arrow next to **FTIMVMVA05.field.net**.
 - (2) Click the down arrow next to **TIMSO**.
 - (3) Click **TIMSO-DS**
 - (4) Click **Configure**
 - (5) Click **LACP**
 - (6) Click **NEW**.

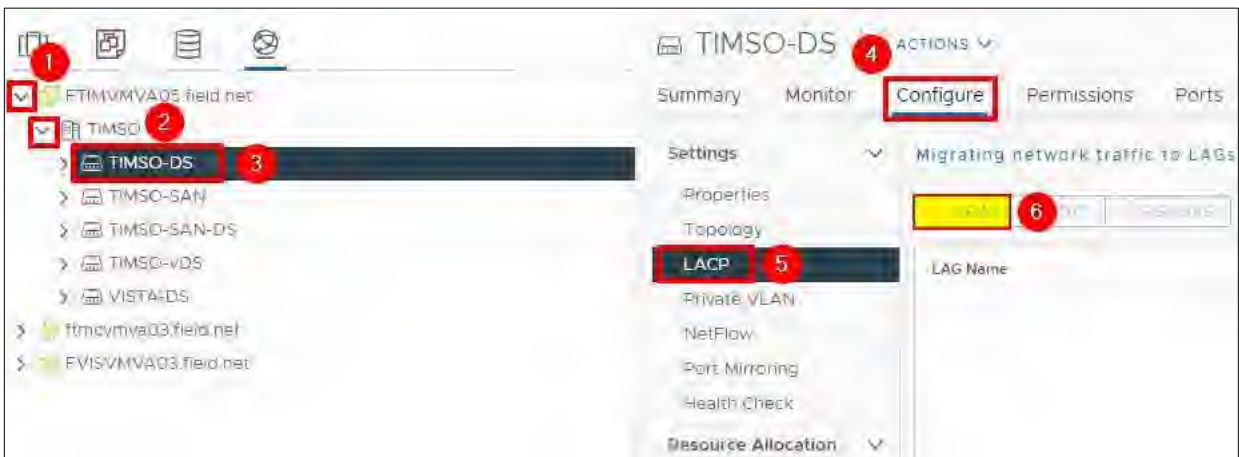


Figure 83. FTIMVMVA05.field.net > Networking > TIMSO-DS > Configure > LACP > NEW

3. Enter the following information in the **New LAG** window.
 - Name: LAG_1
 - Number of ports: 4
 - Mode: Active
 - Load balancing mode: Source and destination MAC address
 - Timeout mode: **slow**

Steps / Screenshots

Click **OK**.



Figure 84. New LAG – LAG_1

4.
 - Click the down arrow next to **TIMSO-DS**,
 - Right Click **TIMSO_MGMT_919**,
 - Click Edit Settings.



Figure 85. TIMSO-DS > TIMSO_MGMT_919 > Edit Settings

5.
 - Click Teaming and failover.
 - Move **Uplink 1** and **Uplink 2** to Unused uplinks.
 - Move **LAG_1** to Active uplinks.
 - Click **OK**.

Steps / Screenshots

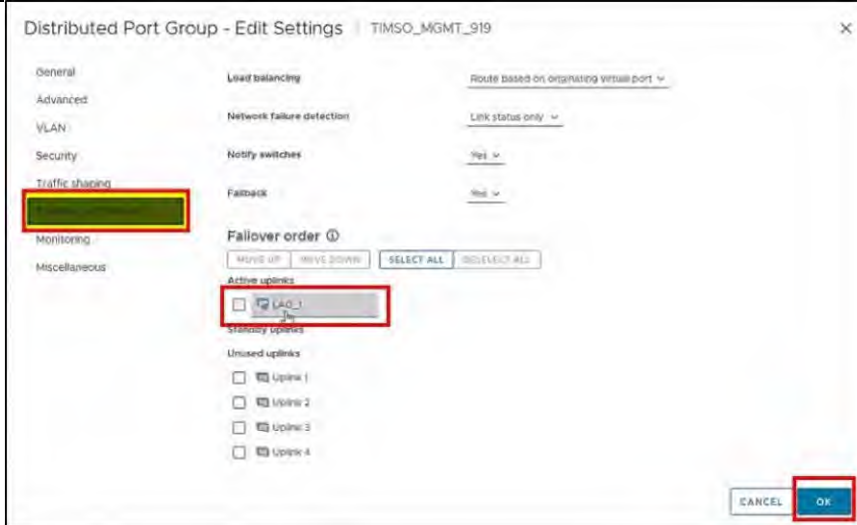


Figure 86. Move Uplink 1 and Uplink 2 to Unused Uplinks.

Configure timvhost01

This configuration differs from *timvhost02 – timvhost06*. It has a standard switch on it instead of a distributed switch.

Configure timvhost01 – vmnic5

Steps / Screenshots

1. Migrate **vmnic5** to the distributed switch while it is changed to the LAG group.
 - (1) Click host and clusters,
 - (2) Click the down arrow next to TIMSO Cluster,
 - (3) Click *timvhost01.smartsunguide.com*,
 - (4) Click Configure,
 - (5) Click Physical adapters,
 - (6) Click *vmnic5*.

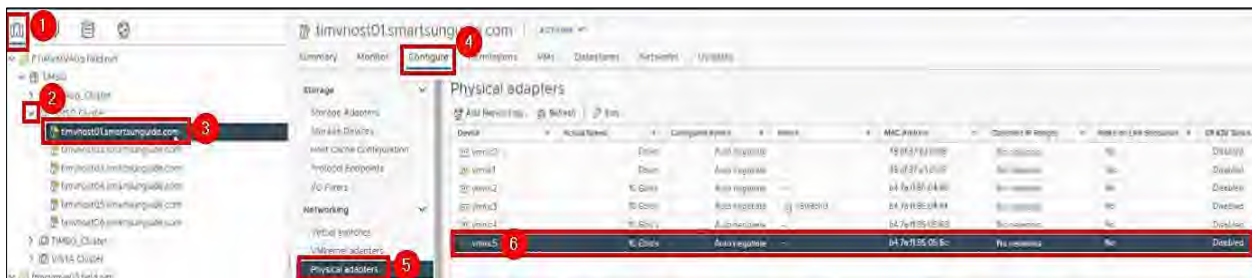


Figure 87. Configure timvhost01 - vmnic5

Steps / Screenshots

- Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), to be provided to the Network Manager:

Device ID: **Switch # 2**
 Port ID: **Port # 9**



Figure 88. vmnic5 Device ID and Port ID.

- On the physical switch, the Network Manager will down the port connected to **vmnic5**.

Confirm that the port is **Down**.

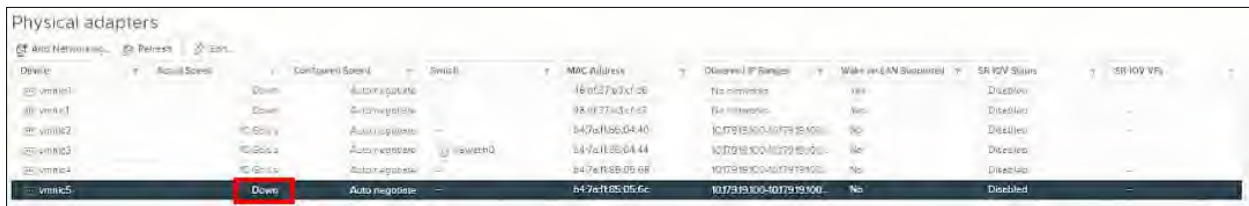


Figure 89. Confirm that the Port is Down

- On the physical switch, the Network Manager will place the port connected to **vmnic5** in the LACP/EtherChannel configuration.

- (1) Click Virtual switches,
- (2) Click the ellipses next to MANAGE PHYSICAL ADAPTERS,
- (3) Click Migrate Networking.



Figure 90. Migrate Networking

- (1) Select **vmnic5**
 - (2) Click Assign uplink.

Add **vmnic5** to one of the LAG uplinks.

- (3) Select **LAG_1-3**
- (4) Click **OK**.

Steps / Screenshots

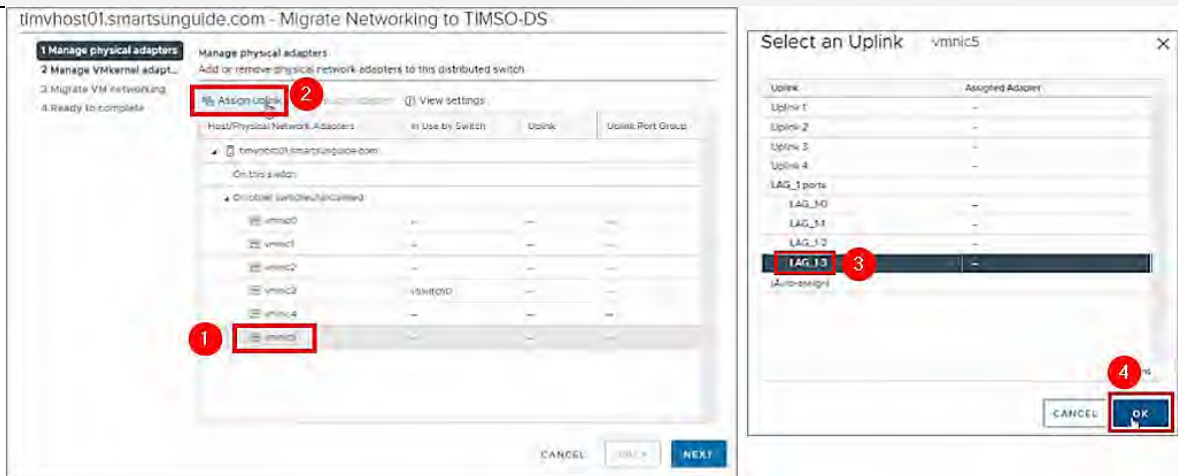


Figure 91. Manage Physical Adapters – Select an Uplink.

6. Click **NEXT**.

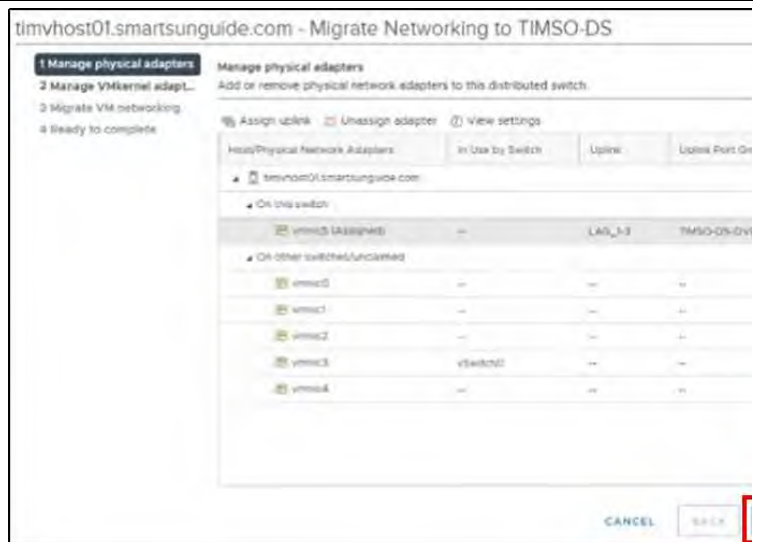


Figure 92. Manage Physical Adapters.

7.
 – Click **vmk0**
 – Click **Assign port group**.



Figure 93. Manage VMkernel Adapters - Assign Port Group.

Steps / Screenshots

- 8.
 - Click TIMSO_MGMT_919
 - Click **OK**.

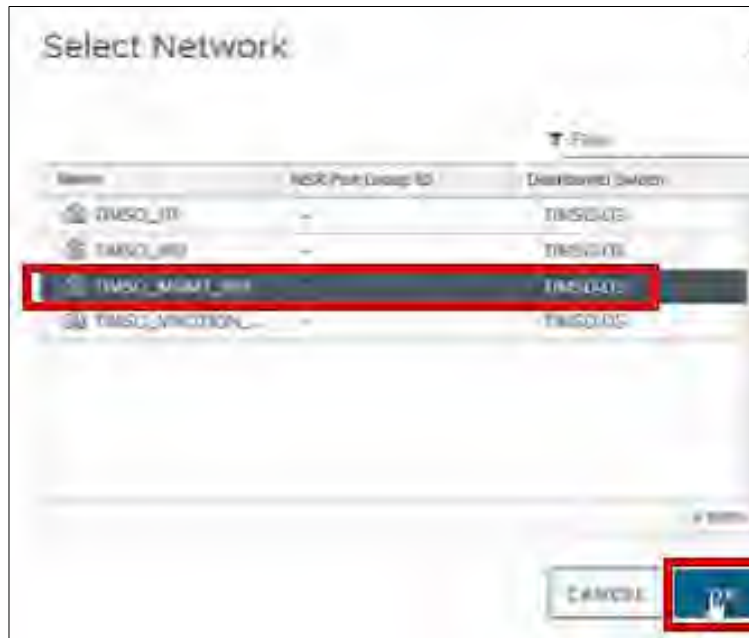


Figure 94. Select Network - TIMSO_MGMT_919

- 9. Click **NEXT**.



Figure 95. Manage VMkernel Adapters.

Steps / Screenshots

10. Click **NEXT**.



Figure 96. Migrate VM Networking

11. Click **FINISH**.



Figure 97. Ready to Complete

The Network Manager will bring the port back up.
Go back **Physical adapters**. Wait for the port to come back up.



Figure 98. Wait for Port to Come Back Up.

Steps / Screenshots

- 1 Click the **All** tab.
- 2 Wait for networks to appear.



Figure 99. Wait for Networks to Appear.

Configure timvhost01 – vmnic4

Steps / Screenshots

1.
 - (1) Click host and clusters,
 - (2) Click the down arrow next to TIMSO Cluster,
 - (3) Click timvhost01.smartsunguide.com,
 - (4) Click Configure,
 - (5) Click Physical adapters,
 - (6) Click vmnic4.



Figure 100. Configure timvhost01 – vmnic4

2. Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), to be provided to the Network Manager.

Device ID: **Switch # 1**

Port ID: **Port # 9**

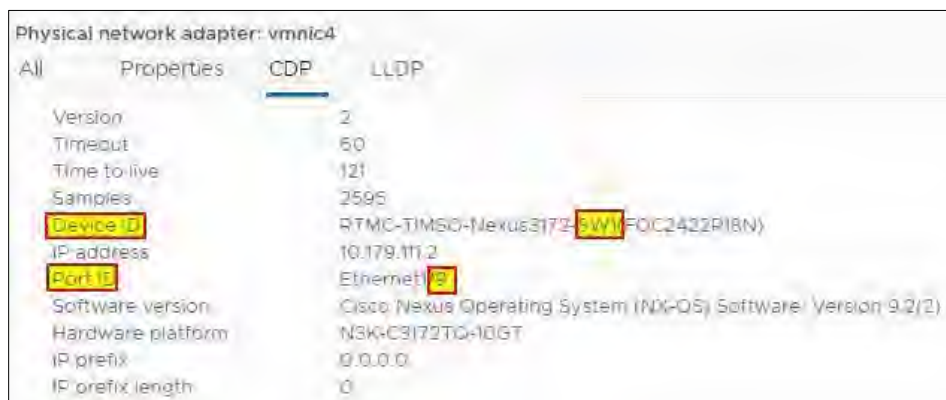


Figure 101. vmnic4 Device ID and Port ID

Steps / Screenshots

3. On the physical switch, the Network Manager will down the port connected to **vmnic4**. Confirm that the port is Down.

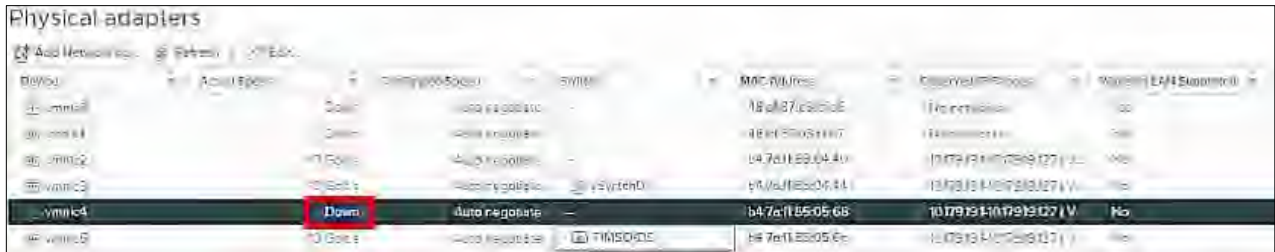


Figure 102. Confirm that the Port is Down.

On a physical switch, the Network Manager will place the port connected to **vmnic4** in the LACP/EtherChannel configuration.

4.
 - (1) Click networking,
 - (2) Right-click **TIMSO-DS**,
 - (3) Click Add and Manage Hosts.

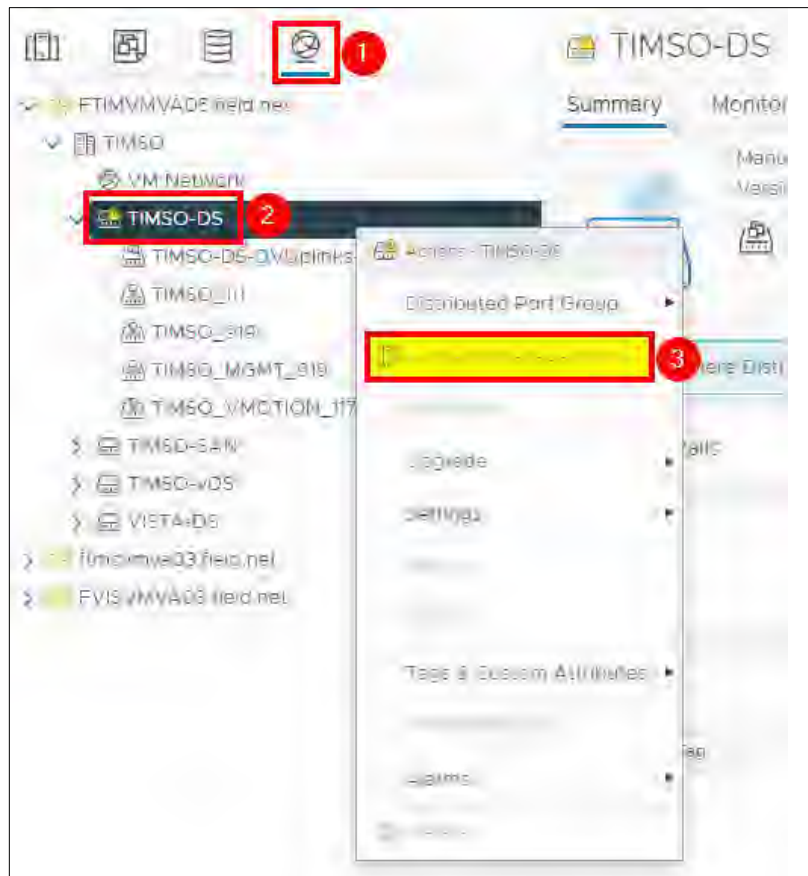


Figure 103. Add and Manage Hosts.

5.
 - Select Manage host networking
 - Click **NEXT**.

Steps / Screenshots

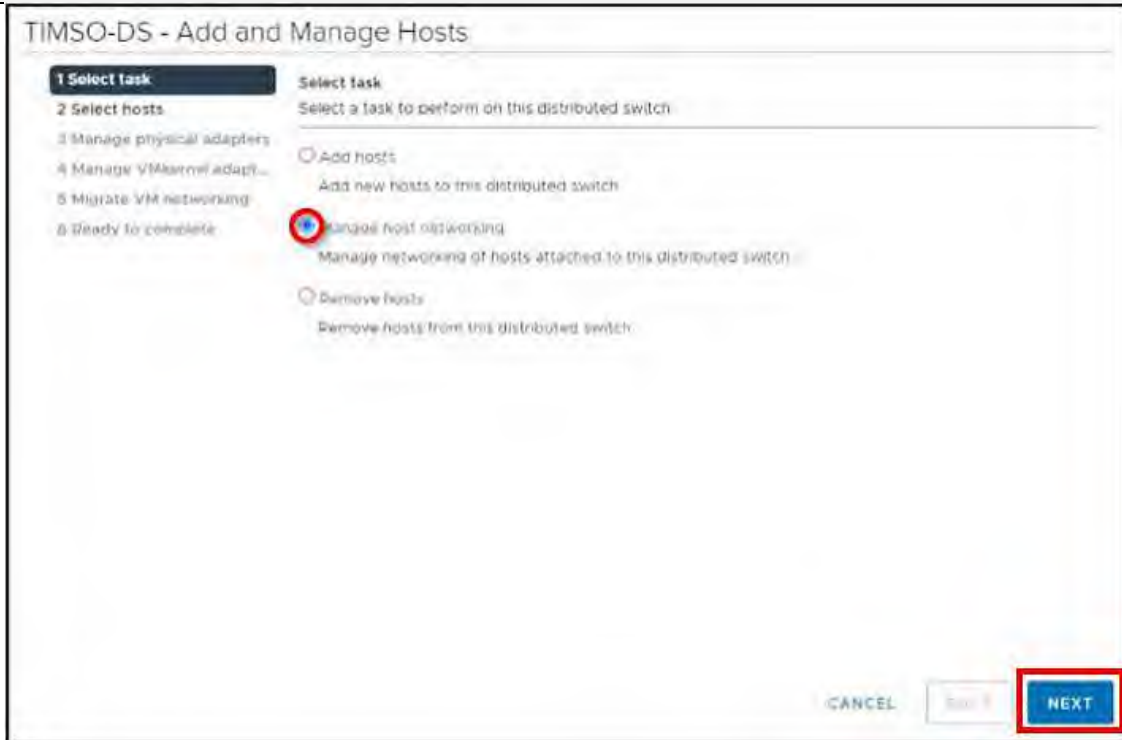


Figure 104. Select Task.

6.
 - Click Attached hosts,
 - Check the box next to timvhost01.smarsunguide.com,
 - Click **OK**.

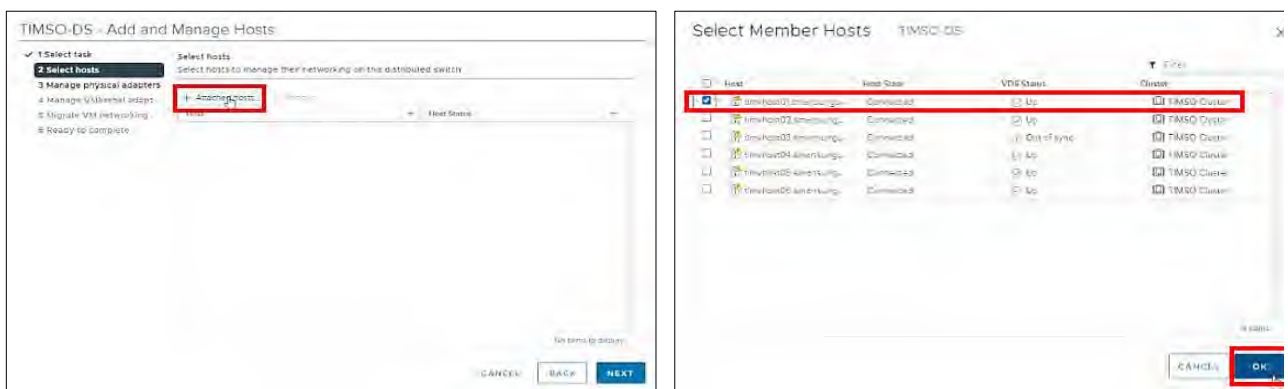


Figure 105. Select Member Host.

Steps / Screenshots

7. Click **NEXT**.

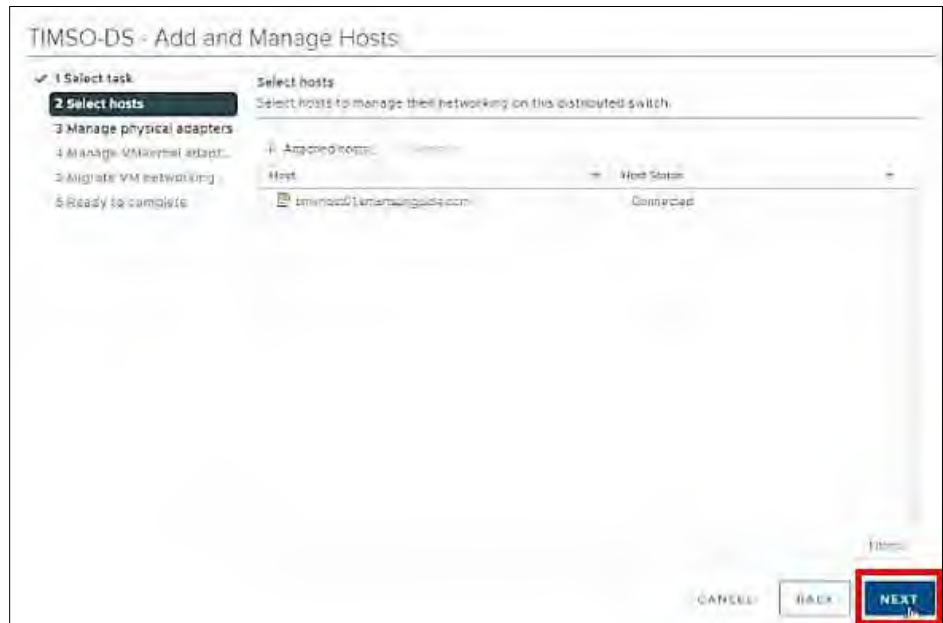


Figure 106. Select Host.

- 8.
- (1) Select **vmnic4** and
 - (2) Click Assign uplink

Add **vmnic4** to one of the LAG uplinks by.

- (3) Select **LAG_1-2**
- (4) Click **OK**.

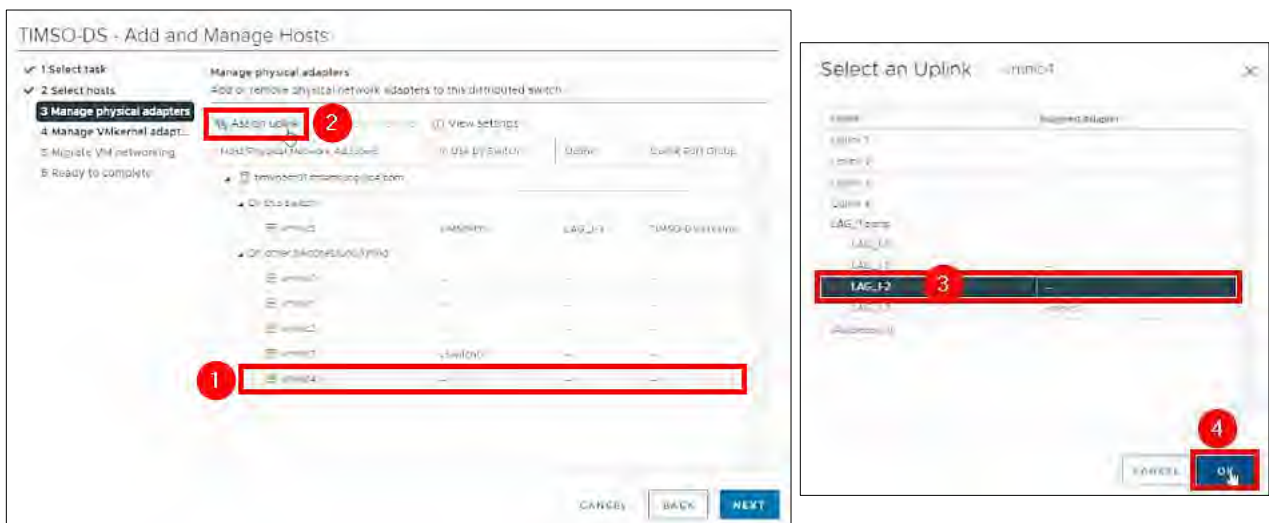


Figure 107. Manage Physical Adapters - Select an Uplink.

Steps / Screenshots

9. Click **NEXT**.



Figure 108. Manage Physical Adapters.

10. Click **NEXT**.

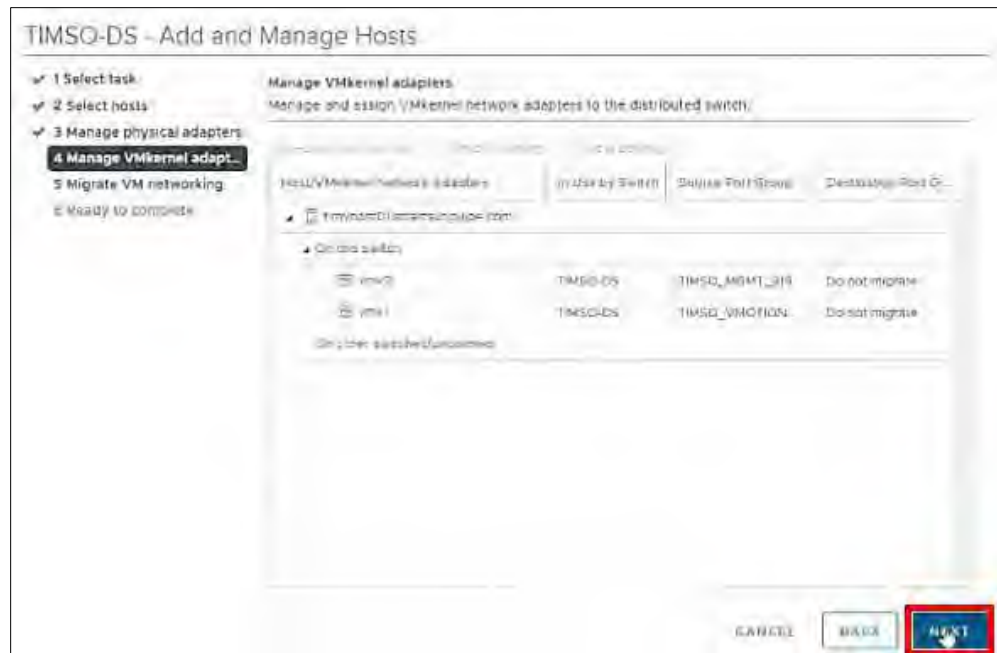


Figure 109. Manage VMkernel Adapters.

Steps / Screenshots

11. Click **NEXT**

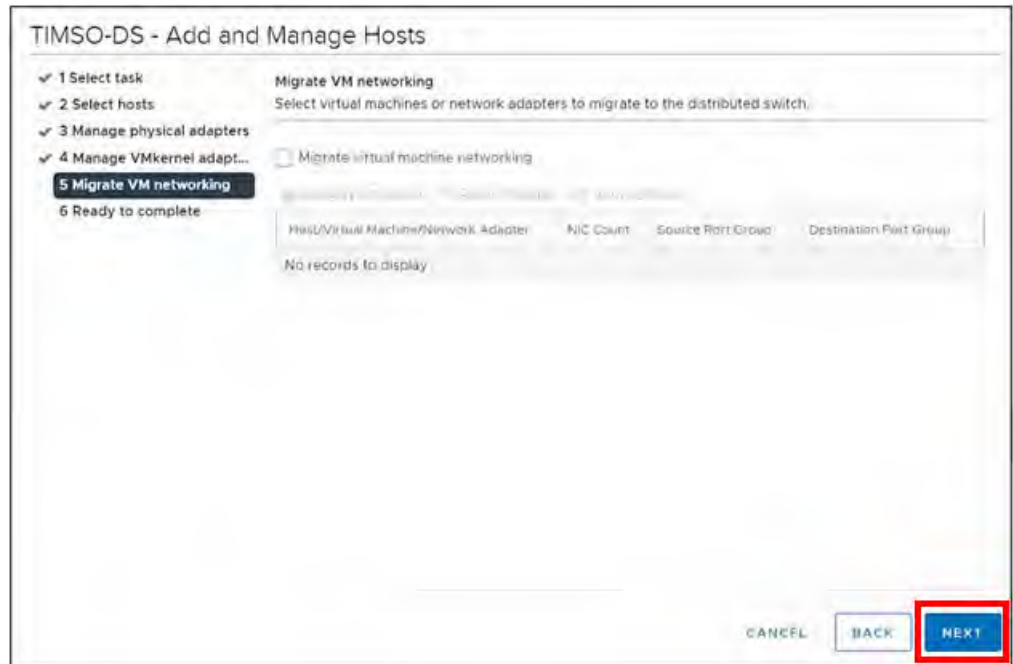


Figure 110. Migrate VM Networking.

12. Click **FINISH**.

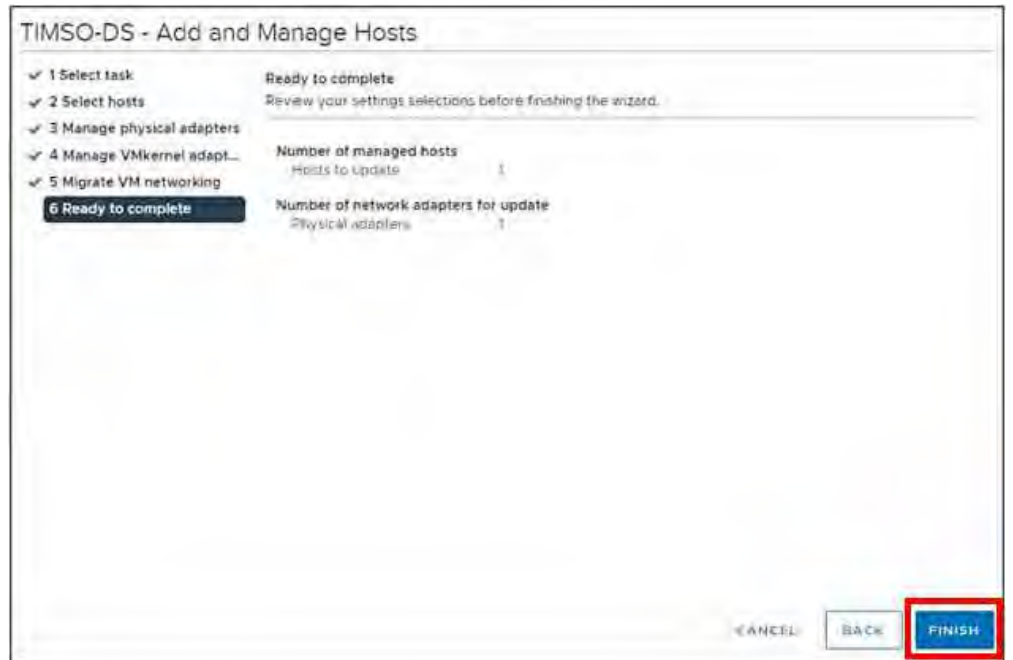


Figure 111. Ready to Complete.

The Network Manager will bring the port back up. Go back **Physical adapters**. Wait for port to come back up.

Steps / Screenshots



Figure 112. Wait for Port to Come Back Up.

13. Click the **All** tab and wait for networks to appear.



Figure 113. Wait for Networks to Appear.

Configure timvhost01 – vmnic3

Steps / Screenshots

1.
 - (1) Click host and clusters,
 - (2) Click the down arrow next to TIMSO Cluster,
 - (3) Click timvhost01.smartsunguide.com,
 - (4) Click Configure,
 - (5) Click Physical adapters,
 - (6) Click vmnic3.



Figure 114. Configure timvhost01 – vmnic3.

Steps / Screenshots

- Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), which will be provided to the Network Manager.

Device ID: **Switch # 1**

Port ID: **Port # 3**

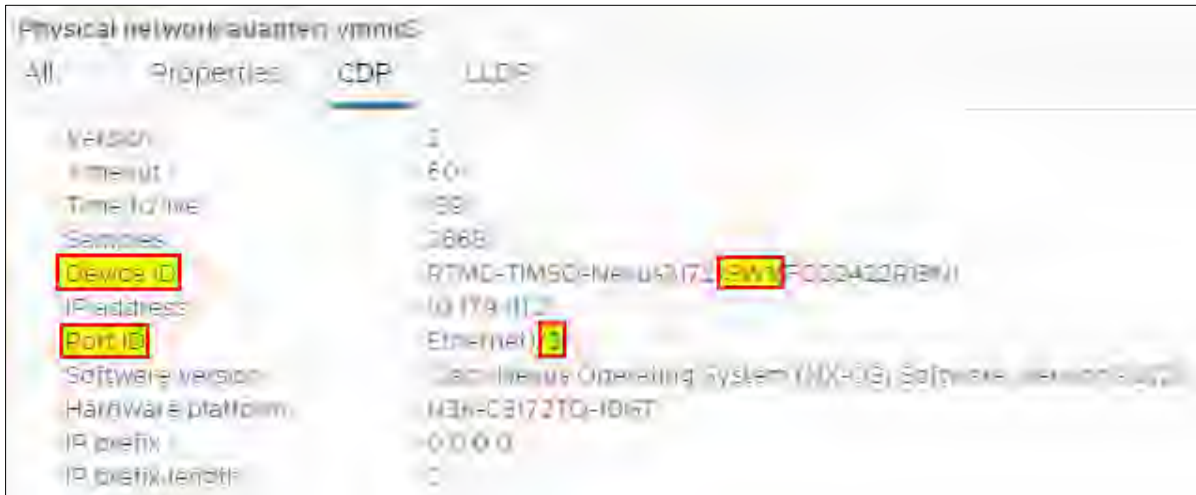


Figure 115. vmnic3 Device ID and Port ID.

On the physical switch, the Network Manager will down the port connected to **vmnic3**. Confirm that the port is **down**.

Device	Speed	Configured Speed	Switch	MAC Address	Observed P-Range	Wake on LAN Supported	VMCI/Port
vmnic0	Down	Auto Negotiate		18:07:43:2:06	10.179.11.0/24	Yes	Disabled
vmnic1	Down	Auto Negotiate		18:03:74:9:1:87	10.179.11.0/24	Yes	Disabled
vmnic2	Down	Auto Negotiate	Timsc05	04:00:11:85:04:40	10.179.11.0/24	Yes	Disabled
vmnic3	Down	Auto Negotiate	vSwch0	04:7c:11:25:04:44	10.179.11.0/24	No	Disabled
vmnic4	Down	Auto Negotiate	TIMSC05	18:7e:11:85:05:08	10.179.11.0/24	Yes	Disabled
vmnic5	Down	Auto Negotiate	TIMSC05	04:7c:11:85:05:6c	10.179.11.0/24	Yes	Disabled

Figure 116. Confirm that the Port is Down.

Steps / Screenshots

3. On the physical switch, the Network Manager will place the port connected to **vmnic3** in the LACP/EtherChannel configuration.

- (1) Click **networking**,
- (2) Right-Click **TIMSO-DS**,
- (3) Click Add and Manage Hosts.

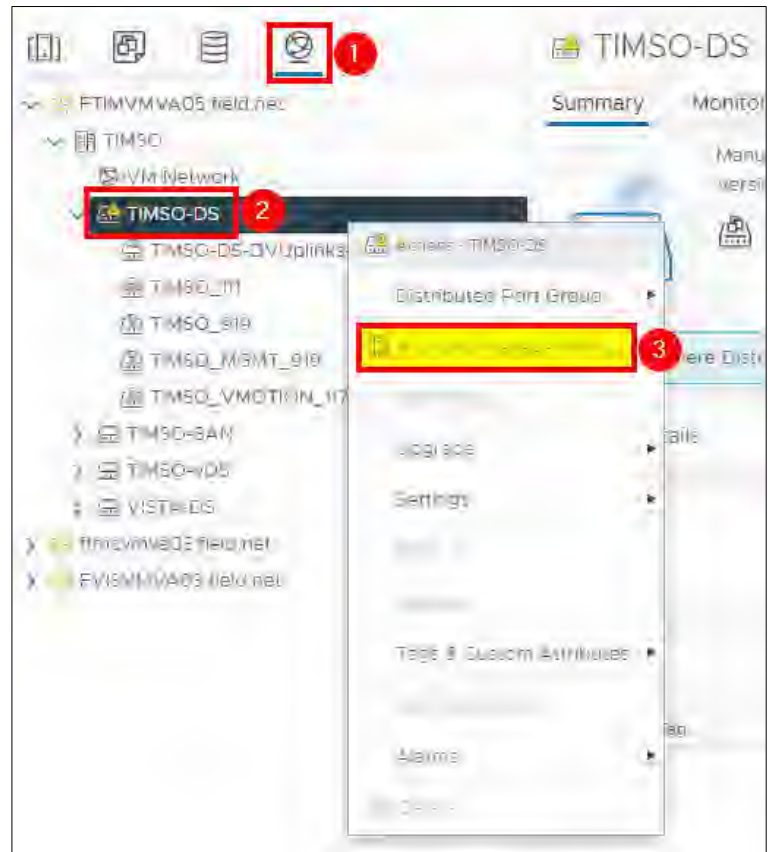


Figure 117. Add and Manage Hosts.

- 4.
- Select Manage host networking
 - Click **NEXT**.

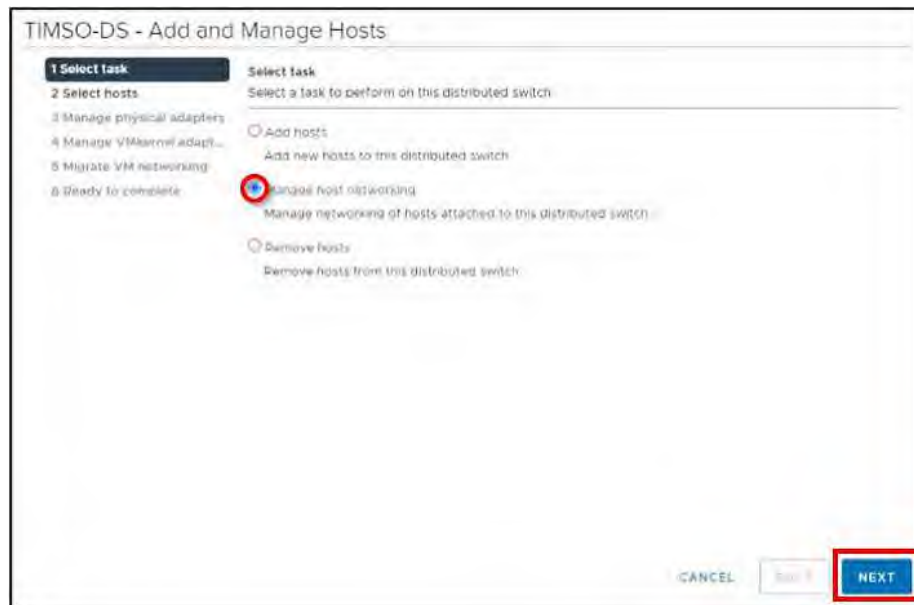


Figure 118. Select Task.

Steps / Screenshots

5.
 - Click Attached hosts,
 - Check the box next to timvhost01.smarsunguide.com,
 - Click **NEXT**.



Figure 119. Select Member Host.

6. Click **NEXT**.

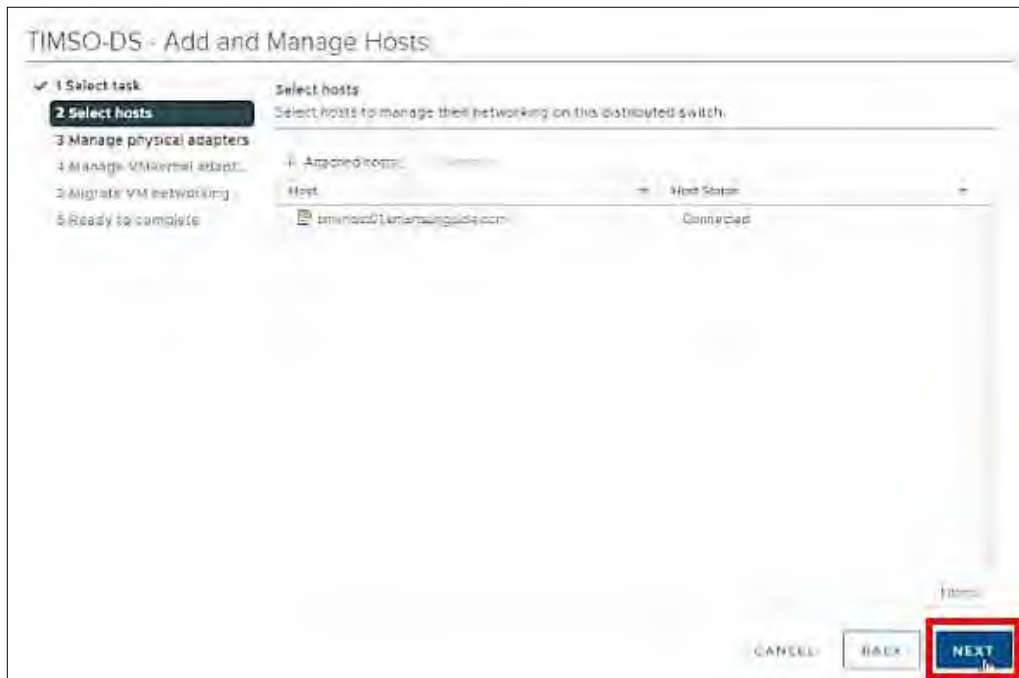


Figure 120. Select Host.

7.
 - Select **vmnic3**
 - Click Assign uplink.

Add **vmnic3** to one of the LAG uplinks.

- Select **LAG_1-1** and
- Click **OK**.

Steps / Screenshots

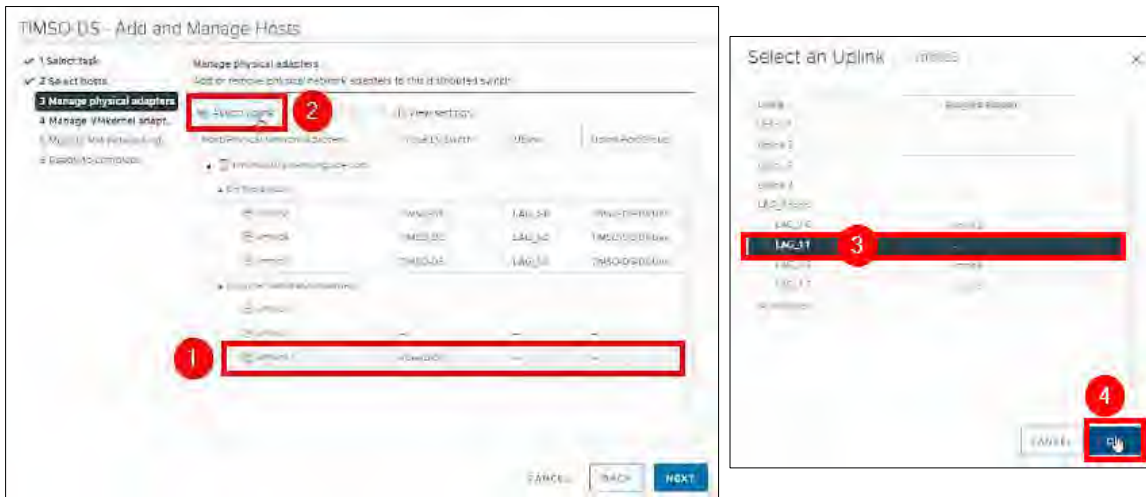


Figure 121. Manage Physical Adapters – Select an Uplink.

8. Click **NEXT**.

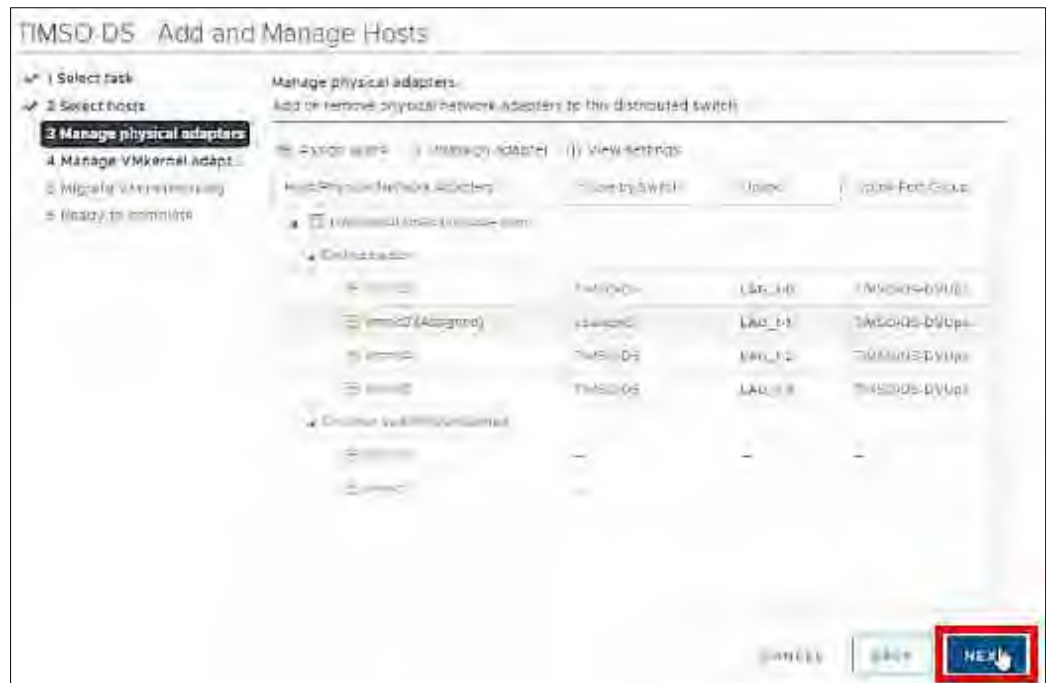


Figure 122. Manage Physical Adapters.

Steps / Screenshots

9. Click **NEXT**.

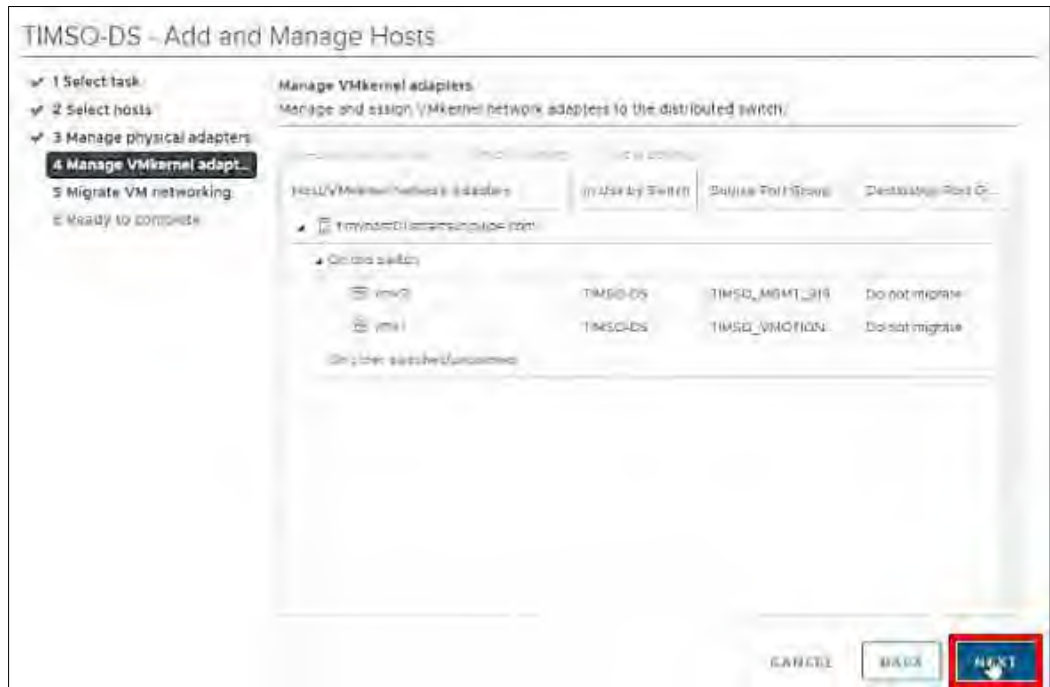


Figure 123. Manage VMkernel Adapters.

10. Click **NEXT**.

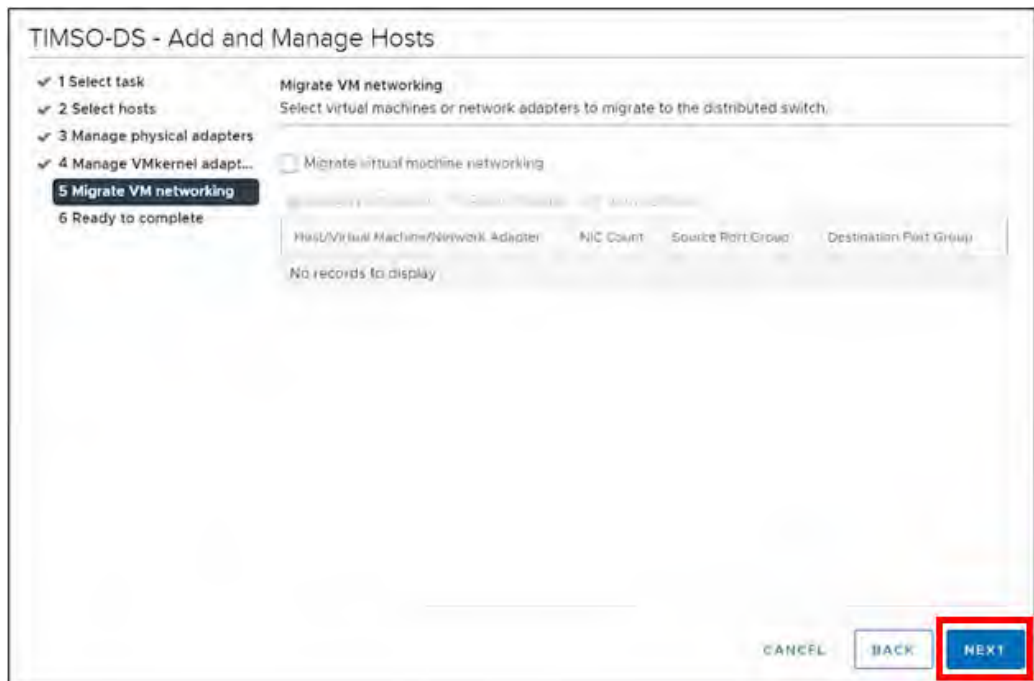


Figure 124. Migrate VM Networking.

Steps / Screenshots

11. Click **FINISH**.



Figure 125. Ready to Complete.

The Network Manager will bring the port back up. Go back **Physical adapters**. Wait for port to come back up,



Figure 126. Wait for Port to Come Back Up.

Click the **All** tab and wait for networks to appear.



Figure 127. Wait for Networks to Appear.

Configure timvhost01 – vmnic2

Steps / Screenshots

1.
 - (1) Click host and clusters,
 - (2) Click the down arrow next to TIMSO Cluster,
 - (3) Click timvhost01.smartsunguide.com,
 - (4) Click Configure,
 - (5) Click Physical adapters,
 - (6) Click vmnic2.

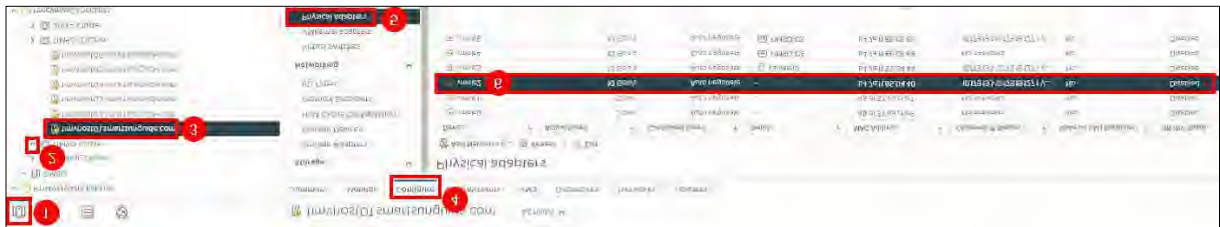


Figure 128. Configure timvhost01 – vmnic2.

2. Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), to be provided to the Network Manager.
 - Device ID: **Switch # 2**
 - Port ID: **Port # 3**



Figure 129. vmnic2 Device ID and Port ID.

3. On the physical switch, the Network Manager will down the port connected to **vmnic2**. Confirm that the port is **down**.

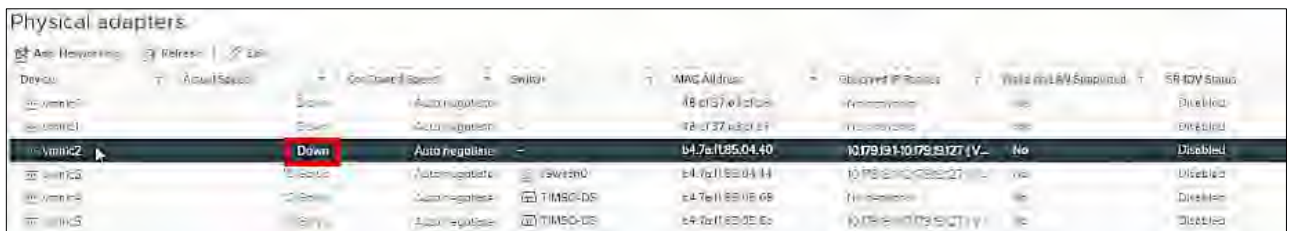


Figure 130. Confirm that the Port is Down.

Steps / Screenshots

4. On the physical switch, the Network Manager will place the port connected to **vmnic2** in the LACP/EtherChannel configuration.

(1) Click networking,

(2) Right-Click **TIMSO-DS**,

(3) Click Add and Manage Hosts.

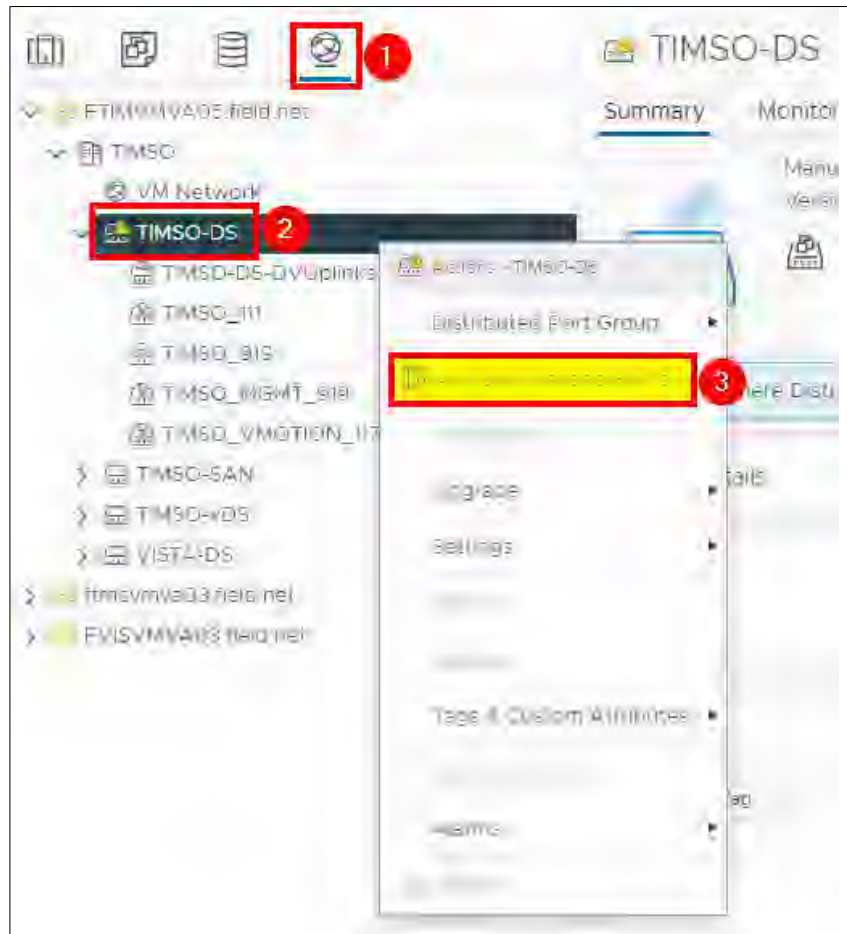


Figure 131. Add and Manage Hosts.

- 5.
- Select Manage host networking
 - Click **NEXT**.

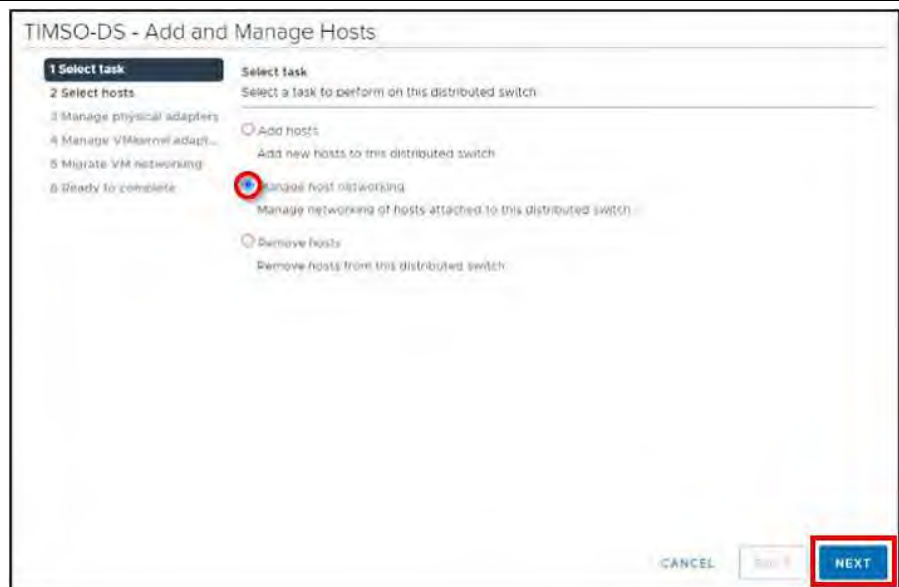


Figure 132. Select Task.

Steps / Screenshots

6.
 - Click Attached hosts,
 - Check the box next to timvhost01.smarsunguide.com,
 - Click **OK**.

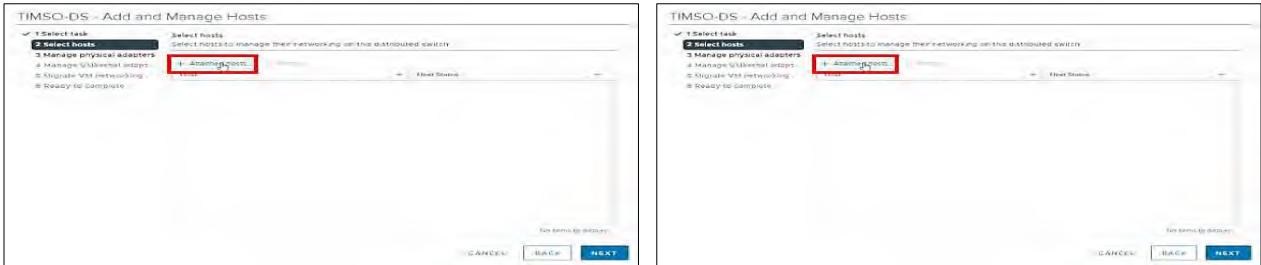


Figure 133. Select Member Host.

7. Click **NEXT**.

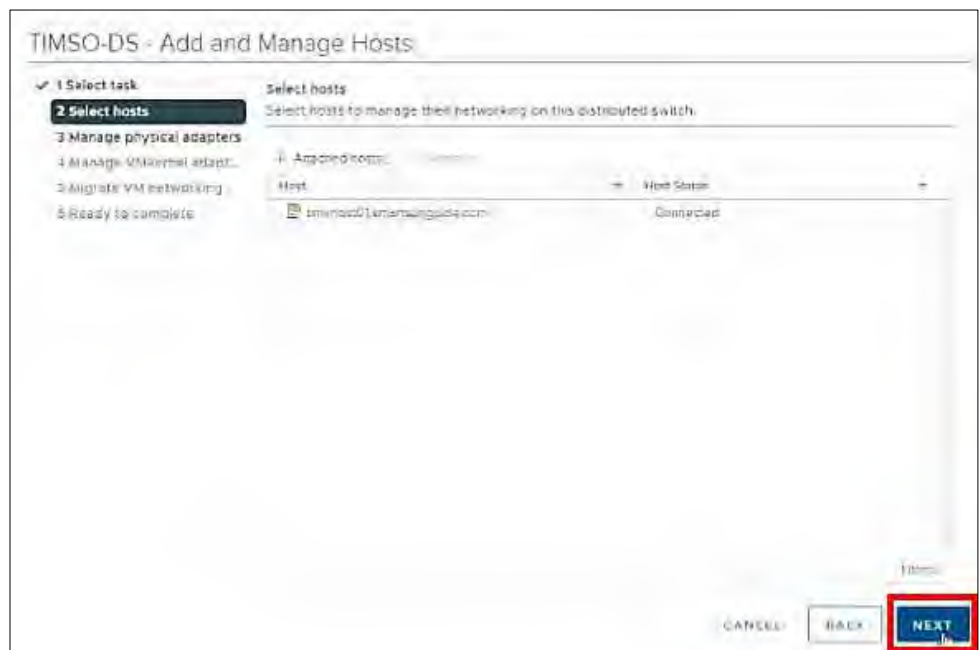


Figure 134. Select Host.

8.
 - (1) Select vmnic2.
 - (2) Click Assign uplink.

Add **vmnic2** to one of the LAG uplinks.

- (3) Select LAG_1-0
- (4) Click **OK**.

Steps / Screenshots

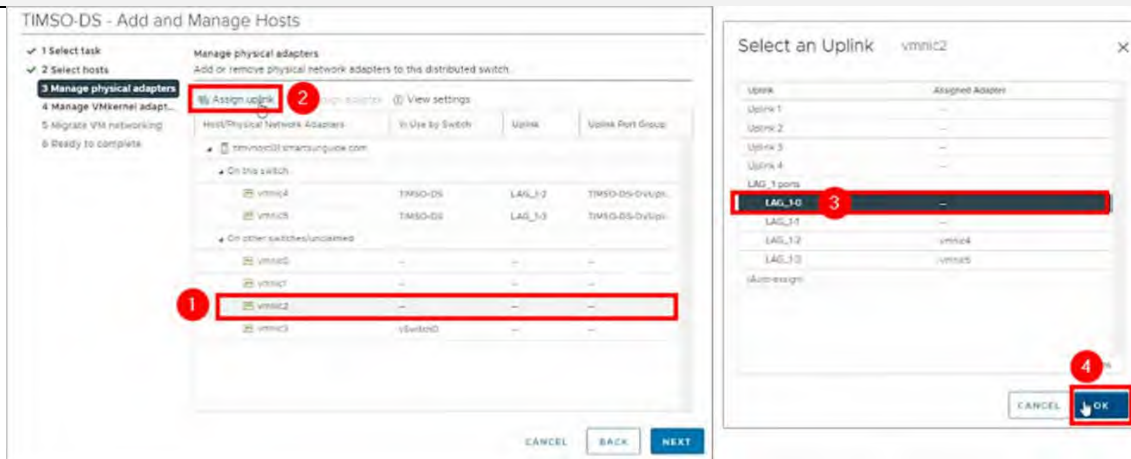


Figure 135. Manage Physical Adapters – Select an Uplink.

9. Click **NEXT**.

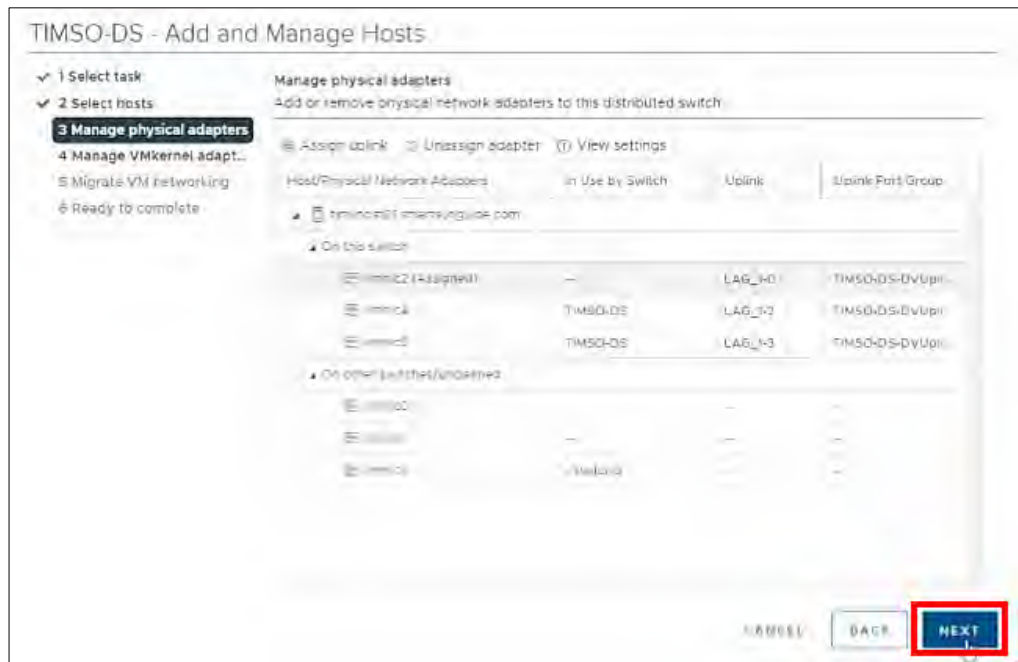


Figure 136. Manage Physical Adapters.

Steps / Screenshots

10. Click **NEXT**.

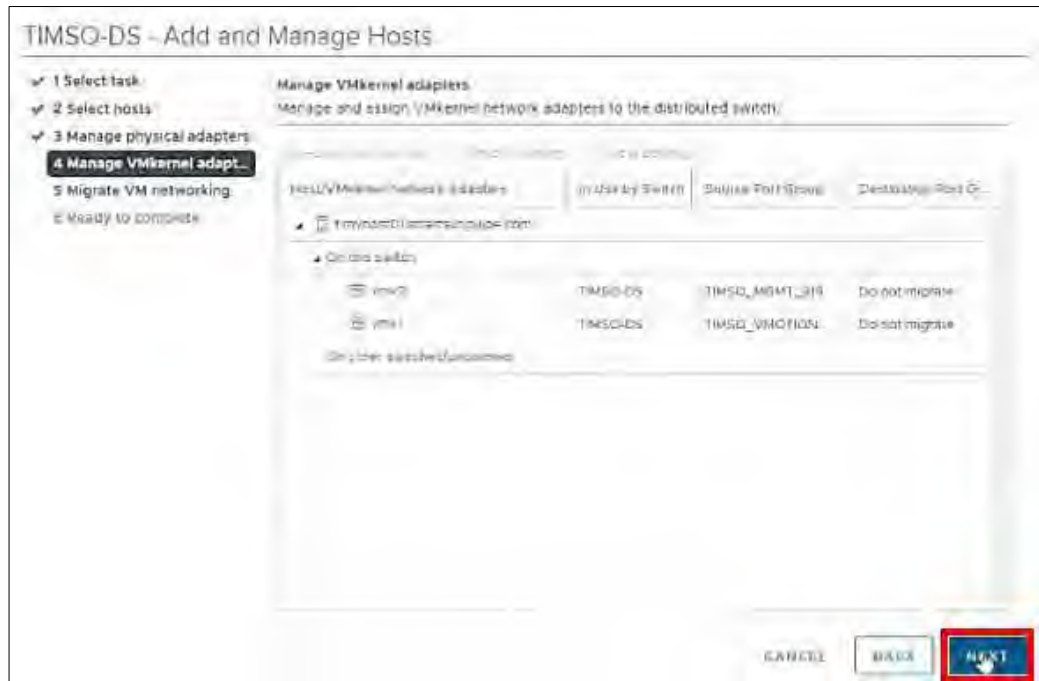


Figure 137. Manage VMkernel Adapters.

11. Click **NEXT**.

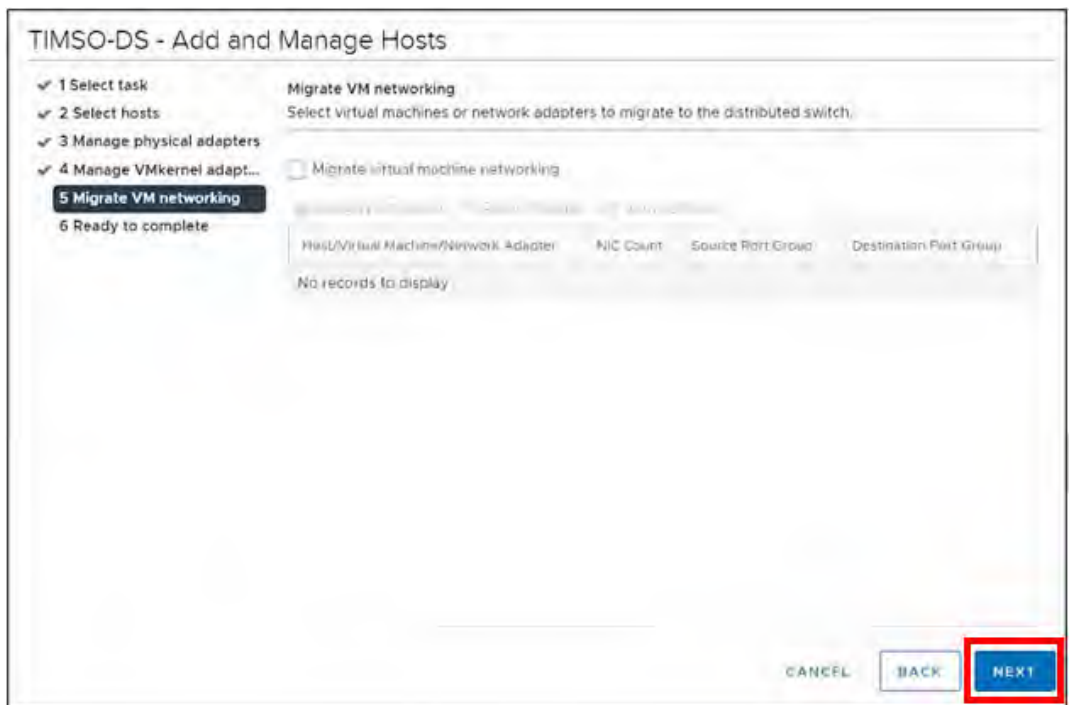


Figure 138. Migrate VM Networking.

Steps / Screenshots

12. Click **FINISH**.

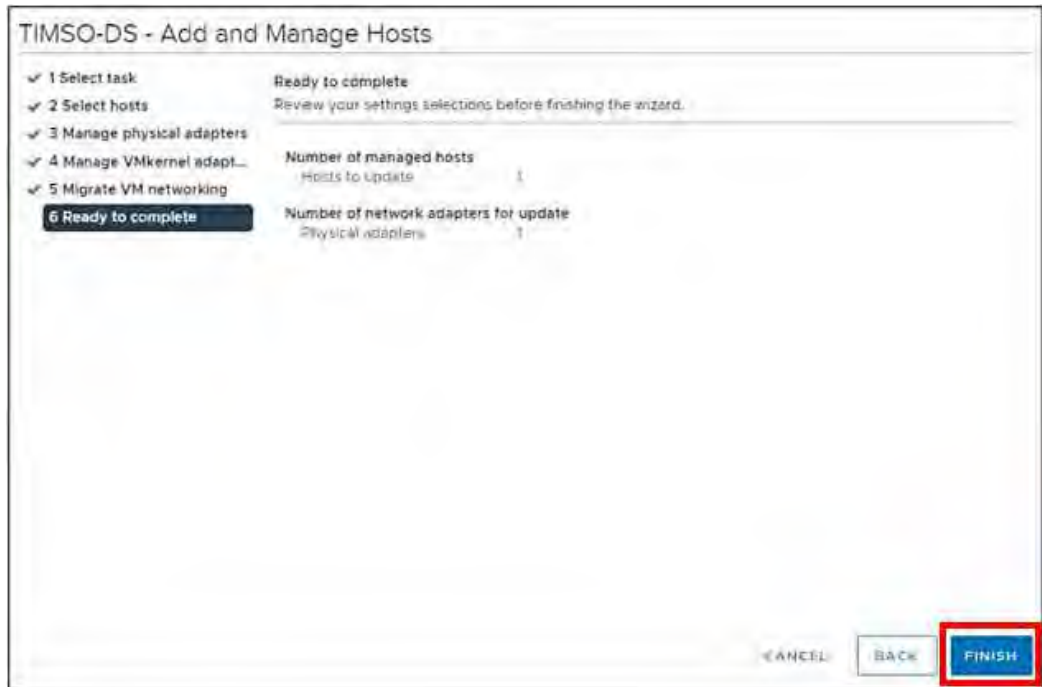


Figure 139. Ready to Complete.

The Network Manager will bring the port back up. Go back **Physical adapters**. Wait for port to come back up.



Figure 140. Wait for Port to Come Back Up.

Steps / Screenshots

13. Click the **All** tab and wait for networks to appear,



Figure 141. Wait for Networks to Appear.

Configure timvhost04

Configure timvhost04 – vmnic2

Steps / Screenshots

1.
 - (1) Click host and clusters,
 - (2) Click the down arrow next to TIMSO Cluster,
 - (3) Click timvhost04.smartsunguide.com,
 - (4) Click **Configure**,
 - (5) Click Physical adapters,
 - (6) Click **vmnic2**.



Figure 142. Configure timvhost04 - vmnic2

2. Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), to be provided to the Network Manager.

Device ID: **Switch # 2**

Port ID: **Port # 6**

Steps / Screenshots

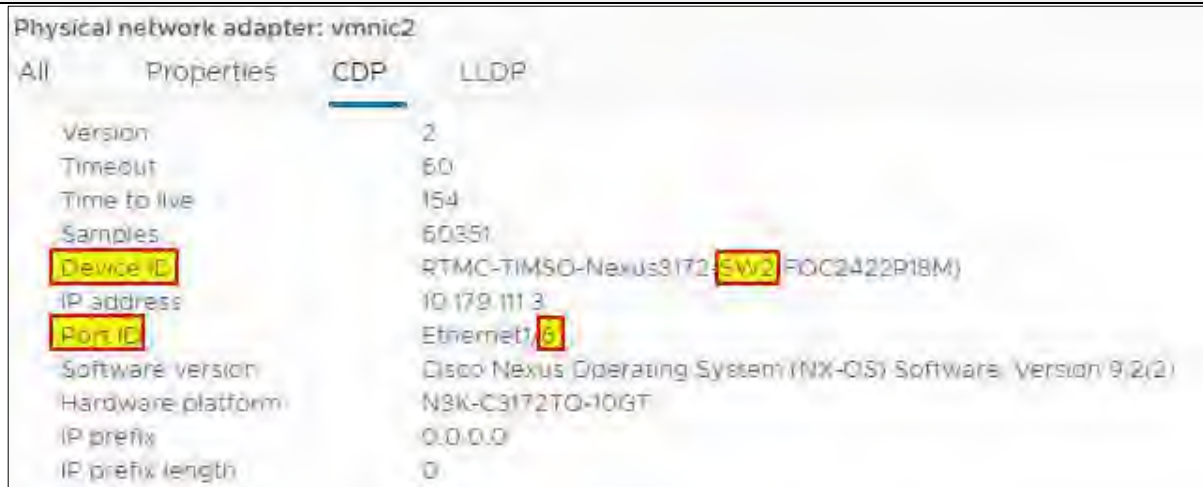


Figure 143. vmnic2 Device ID and Port ID

- On the physical switch, the Network Manager will down the port connected to vmnic2. Confirm that the port is **Down**.



Figure 144. Confirm that the Port is Down

- On the physical switch, the Network Manager will place the port connected to vmnic2 in the LACP/EtherChannel configuration.

- (1) Click **networking**,
- (2) Right-click **TIMSO-DS**,
- (3) Click Add and Manage Hosts.

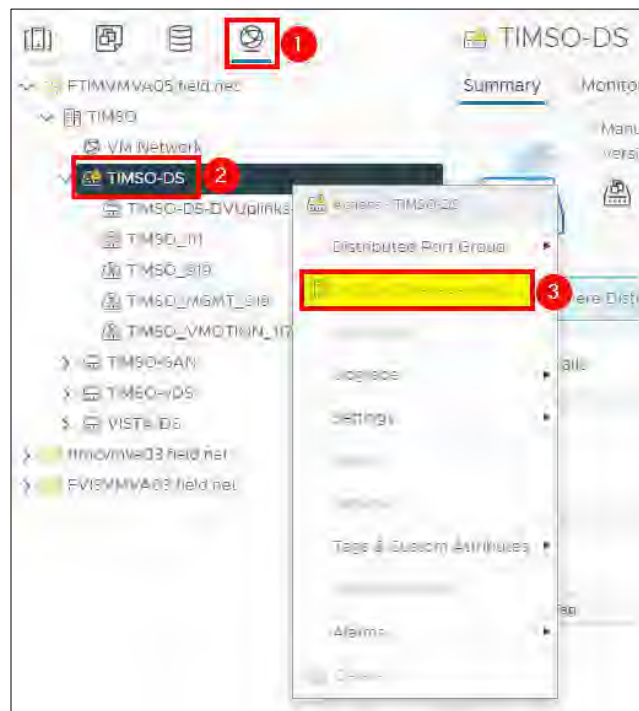


Figure 145. Add and Manage Hosts.

Steps / Screenshots

5.
 - Select Manage host networking
 - Click **NEXT**.



Figure 146. Select Task.

6.
 - Click Attached hosts,
 - Check the box next to timvhost04.smarsunguide.com,
 - Click **OK**.

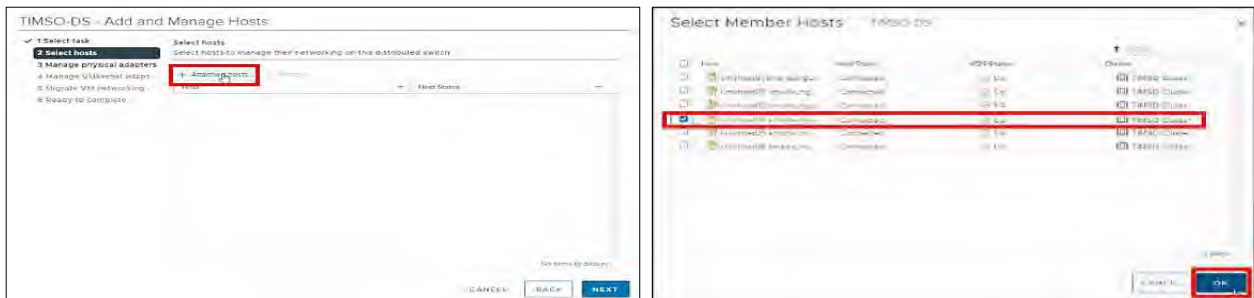


Figure 147. Select Member Host.

Steps / Screenshots

7. Click **NEXT**.

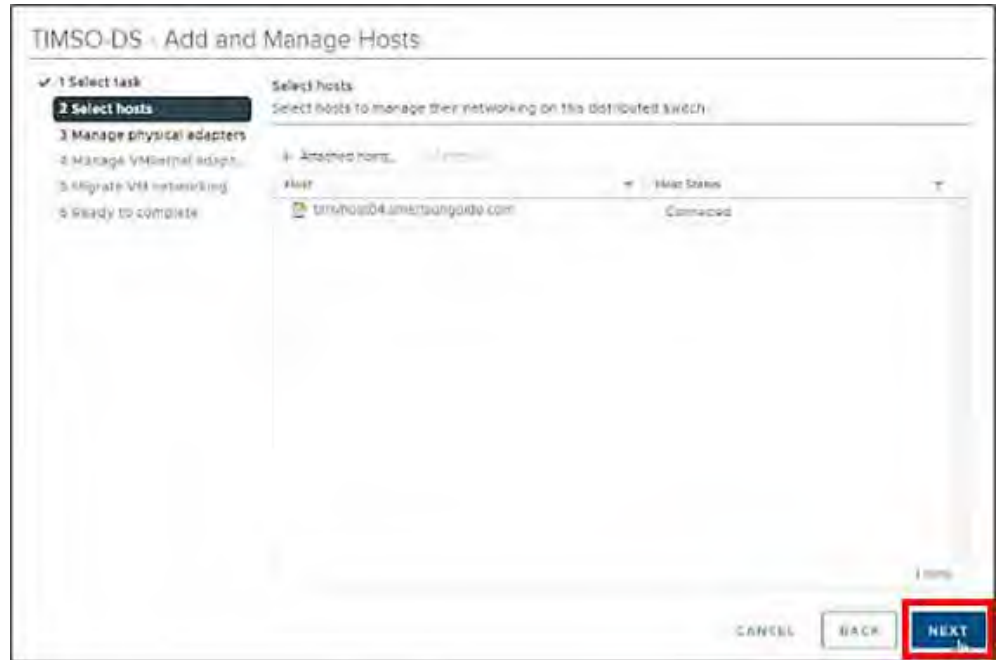


Figure 148. Select Host

- 8.
- (1) Select **vmnic2** and
 - (2) Click Assign uplink.

Add **vmnic2** in one of the LAG uplinks.

- (3) Select the **LAG_1-0**
- (4) Click **OK**.

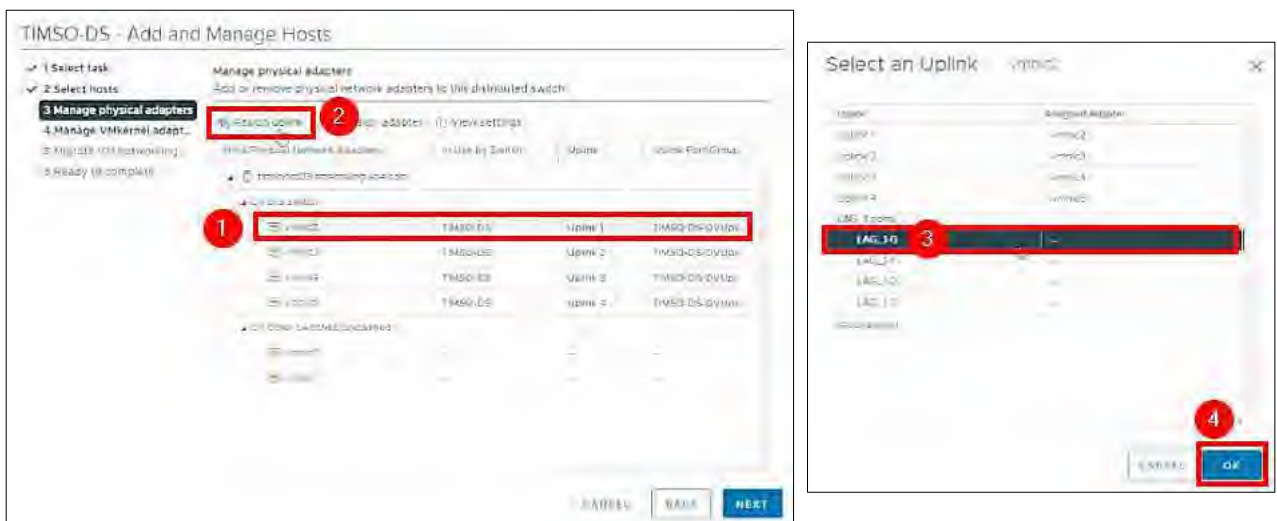


Figure 149. Manage Physical Adapters – Select an Uplink

Steps / Screenshots

9. Click **NEXT**.



Figure 150. Manage Physical Adapters

10. Click **NEXT**.

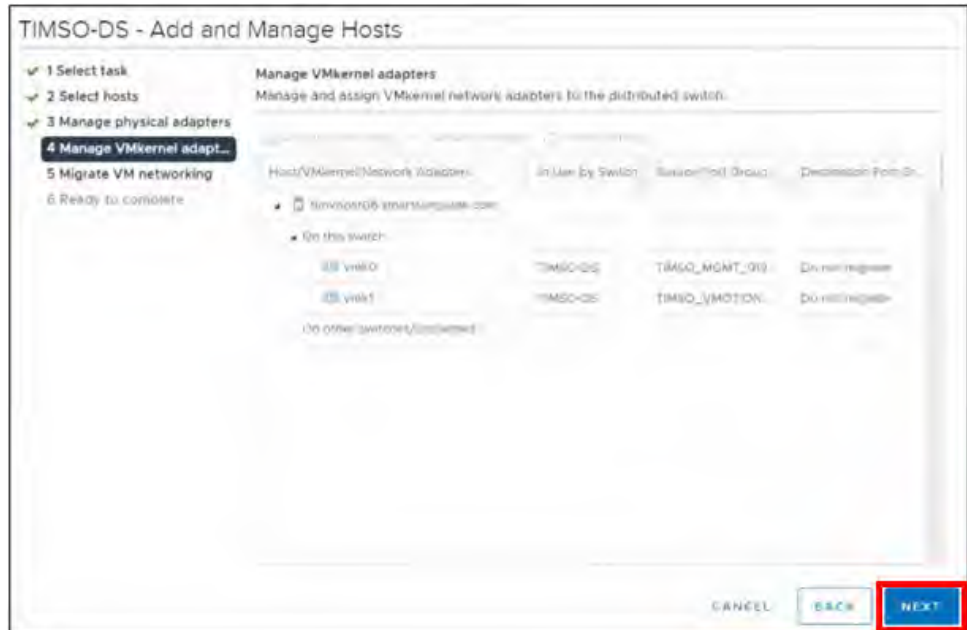


Figure 151. Manage VMkernel Adapters

Steps / Screenshots

11. Click **NEXT**.

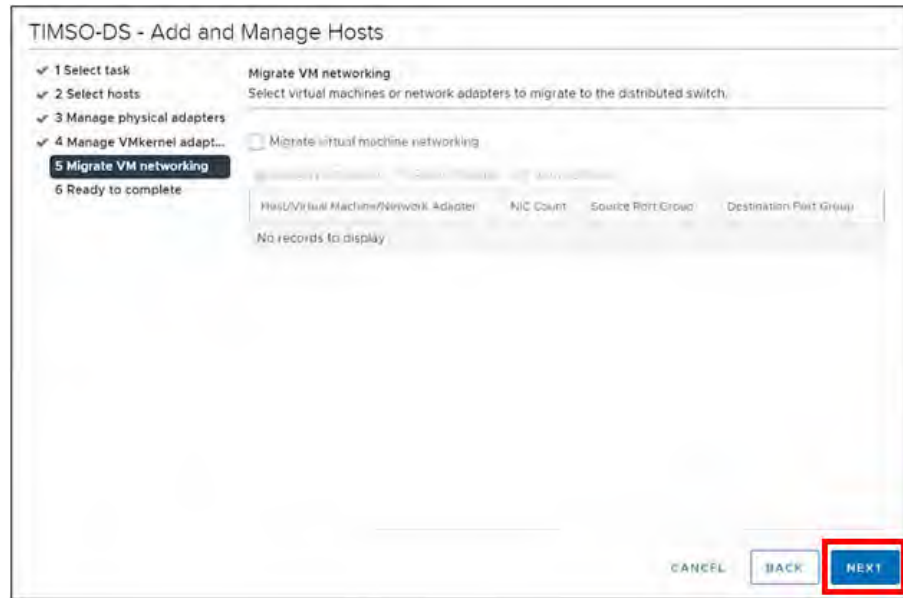


Figure 152. Migrate VM Networking

12. Click **FINISH**.



Figure 153. Ready to Complete

The Network Manager will bring the port back up. Go back **Physical adapters**. Wait for port to come back up.



Figure 154. Wait for Port to Come Back Up

Steps / Screenshots

13. Click the **All** tab and wait for networks to appear.

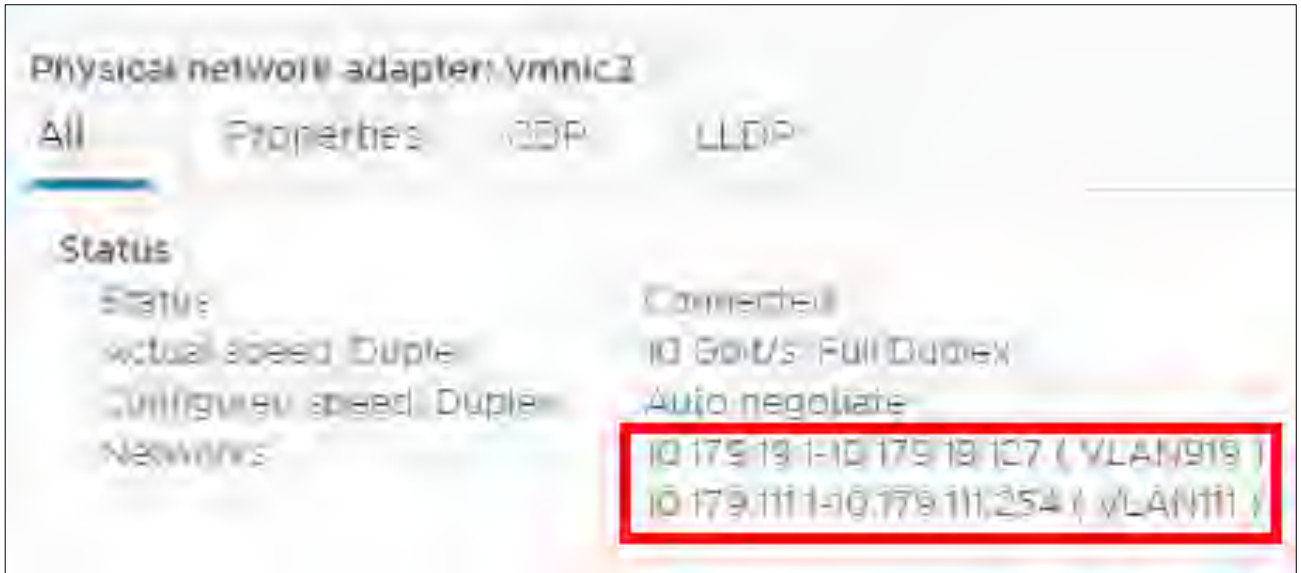


Figure 155. Wait for Networks to Appear

Configure timvhost04 – vmnic3

Steps / Screenshots

1.
 - (1) Click host and clusters,
 - (2) Click the down arrow next to TIMSO Cluster,
 - (3) Click timvhost04.smartsunguide.com,
 - (4) Click Configure,
 - (5) Click Physical adapters,
 - (6) Click vmnic3.

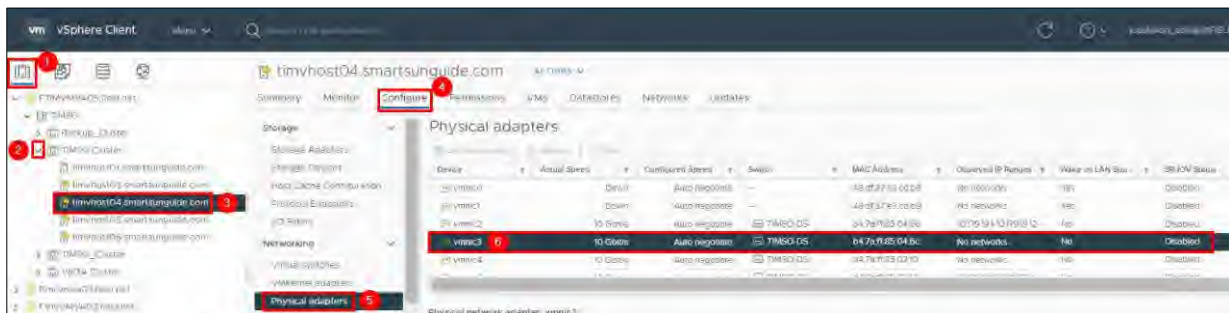


Figure 156. Configure timvhost04 – vmnic3

2. Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), to be provided to the Network Manager.
 - Device ID: **Switch # 1**
 - Port ID: **Port # 6**

Steps / Screenshots



Figure 157. vmnic3 Device ID and Port ID

- On the physical switch, the Network Manager will down the port connected to vmnic3. Confirm that the port is **Down**.



Figure 158. Confirm that the Port is Down

- On the physical switch, the Network Manager will place the port connected to vmnic3 in the LACP/EtherChannel configuration.
 - (1) Click networking,
 - (2) Right-click **TMSO-DS**,
 - (3) Click Add and Manage Hosts.

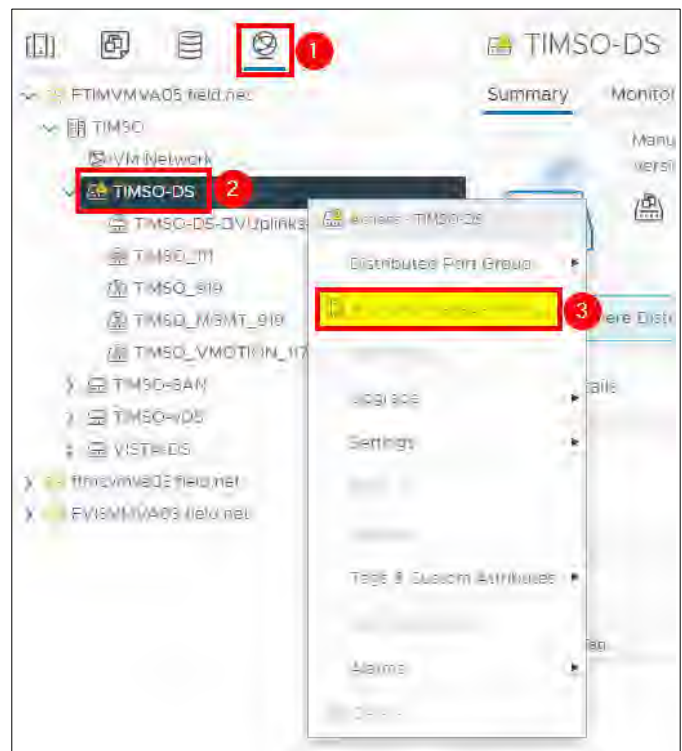


Figure 159. Add and Manage Hosts

Steps / Screenshots

5.
 - Select Manage host networking and
 - Click **NEXT**.

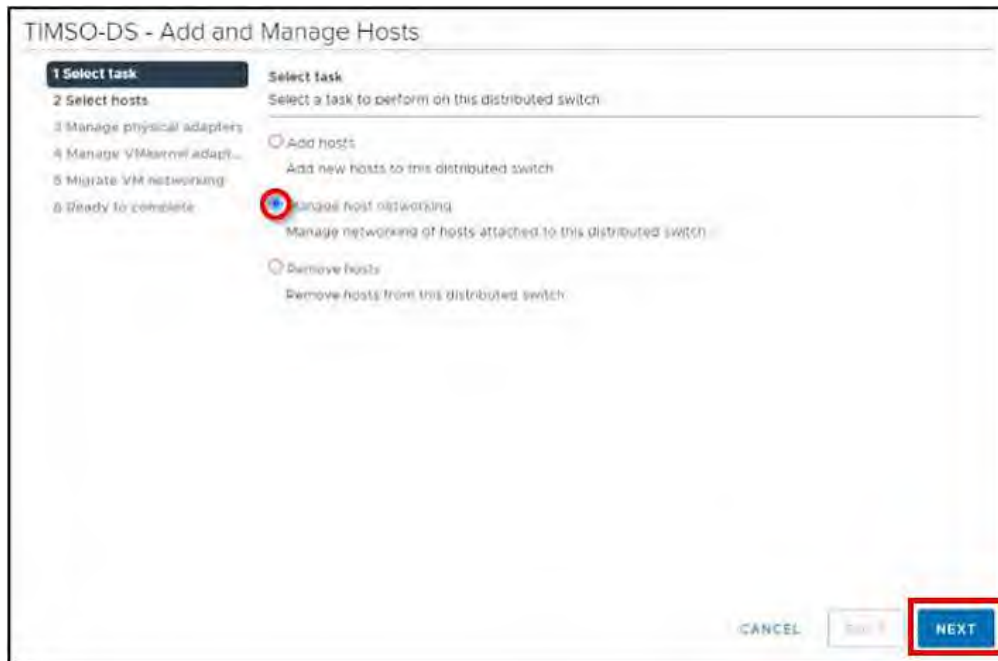


Figure 160. Select Task

6.
 - Click Attached hosts,
 - Check the box next to timvhost04.smarsunguide.com,
 - Click **OK**.

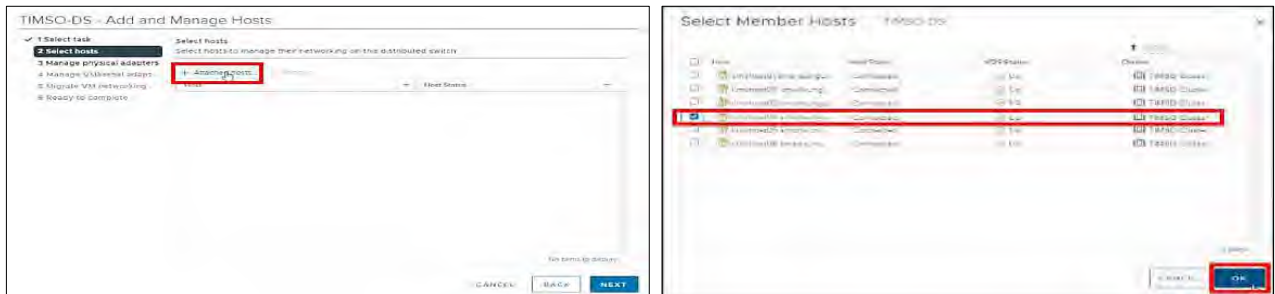


Figure 161. Select Member Host

Steps / Screenshots

7. Click **NEXT**.

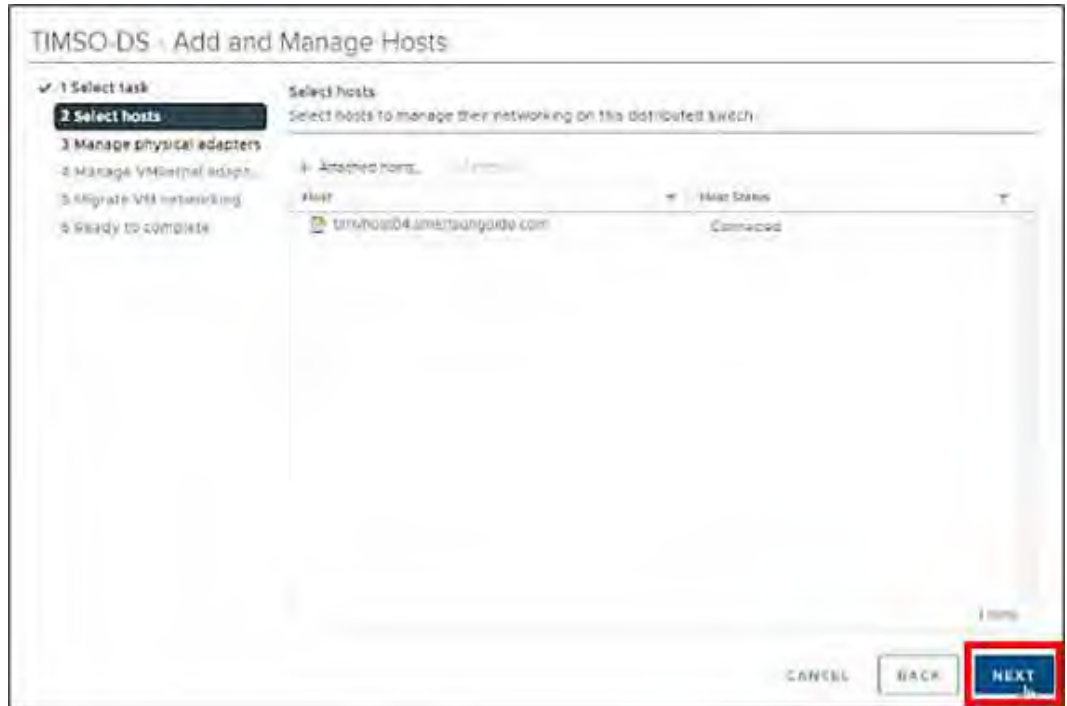


Figure 162. Select Host

- 8.
- (1) Select **vmnic3**
 - (2) Click Assign uplink

Add **vmnic3** in one of the LAG uplinks.

- (3) Select the **LAG_1-1**.
- (4) Click **OK**.

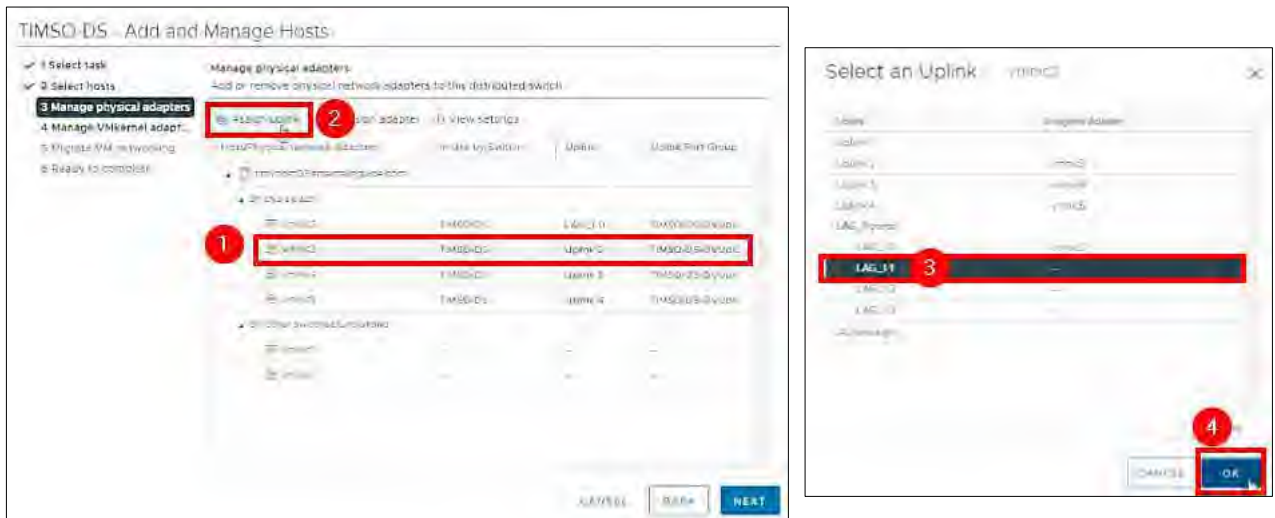


Figure 163. Manage Physical Adapters – Select an Uplink.

Steps / Screenshots

9. Click **NEXT**.

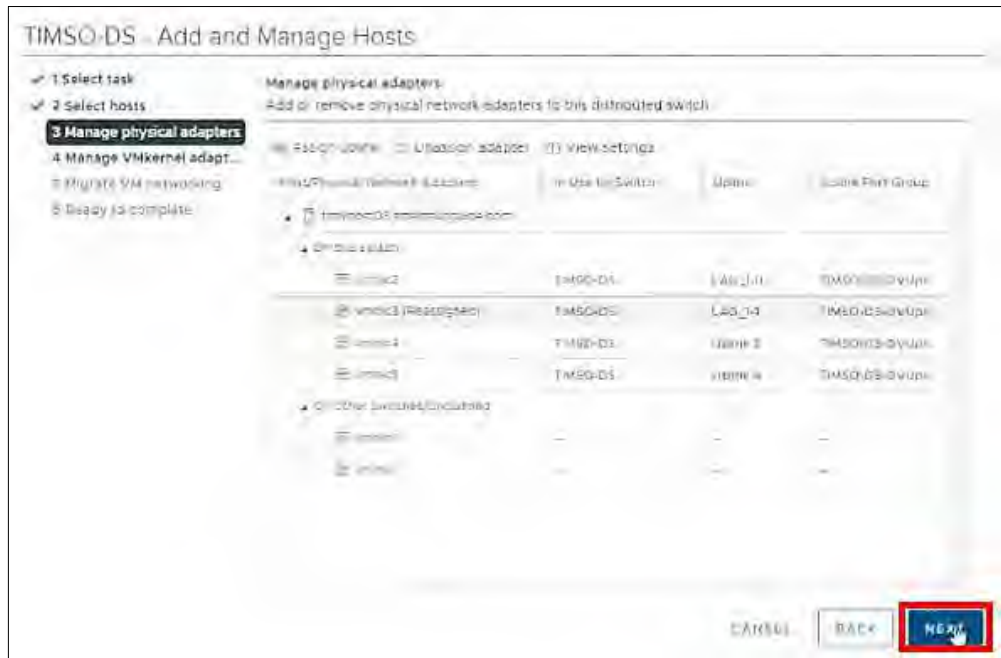


Figure 164. Manage Physical Adapters

10. Click **NEXT**.

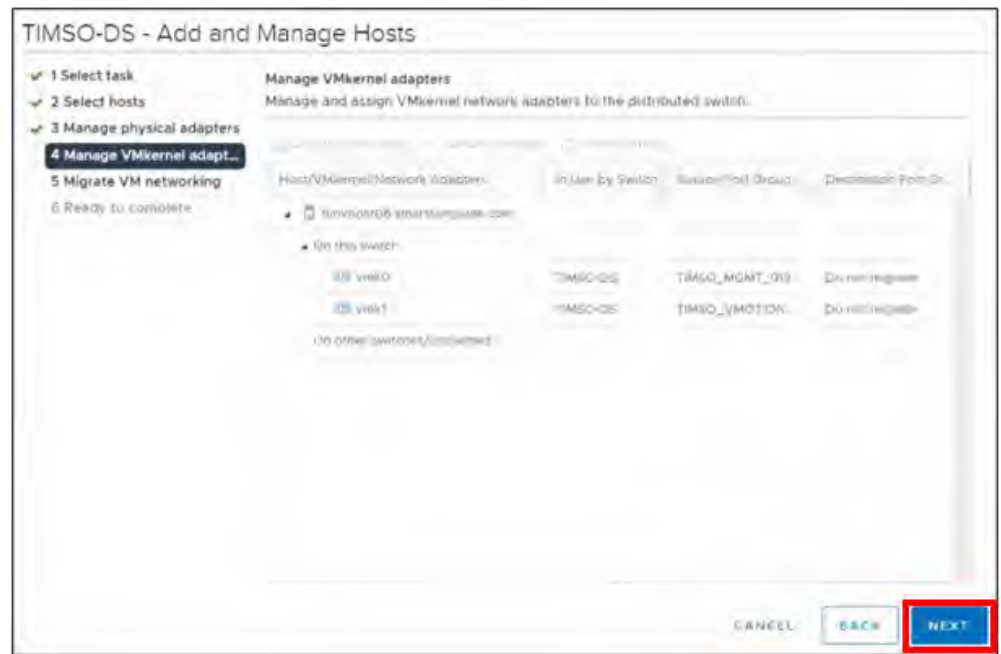


Figure 165. Manage VMkernel Adapters

Steps / Screenshots

11. Click **NEXT**

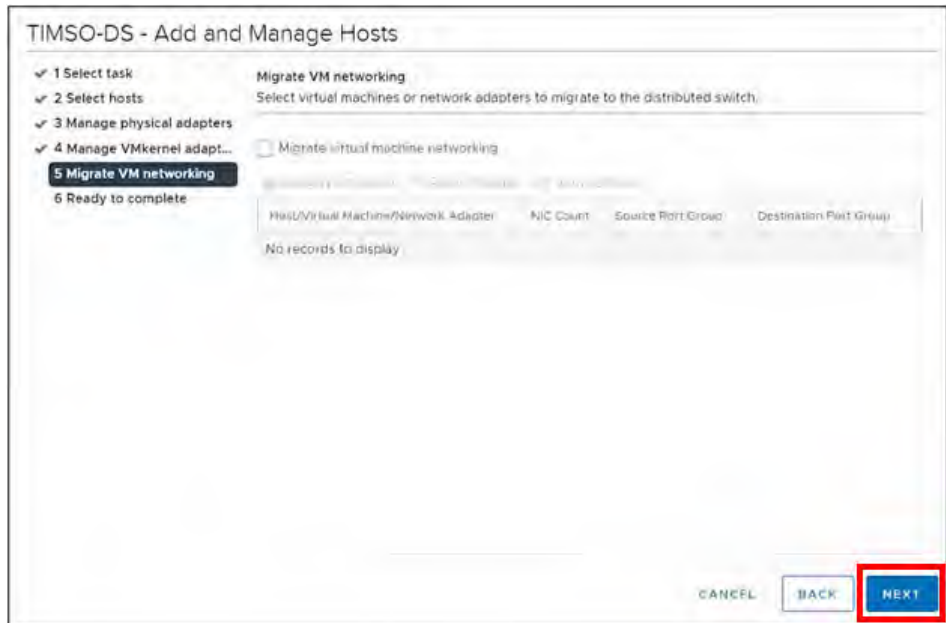


Figure 166. Migrate VM Networking

12. Click **FINISH**.



Figure 167. Ready to Complete

The Network Manager will bring the port back up. Go back **Physical adapters**. Wait for port to come back up.

Physical adapters								
Device	Actual Speed	Configured Speed	Switch	MAC Address	Observed IP Ranges	Wake on LAN Sup...	SR-IOV Status	
vmnic0	Down	Auto negotiate	--	48:df:37:e3:cd:b8	No networks	Yes	Disabled	
vmnic1	Down	Auto negotiate	--	48:df:37:e3:cd:b9	No networks	Yes	Disabled	
vmnic2	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ff:85:04:68	10.179.19.1-10.179.19.12...	No	Disabled	
vmnic3	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ff:85:04:6c	No networks	No	Disabled	
vmnic4	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ff:85:02:10	No networks	No	Disabled	

Figure 168. Wait for Port to Come Back Up.

Steps / Screenshots

13. Click the **All** tab and wait for networks to appear.

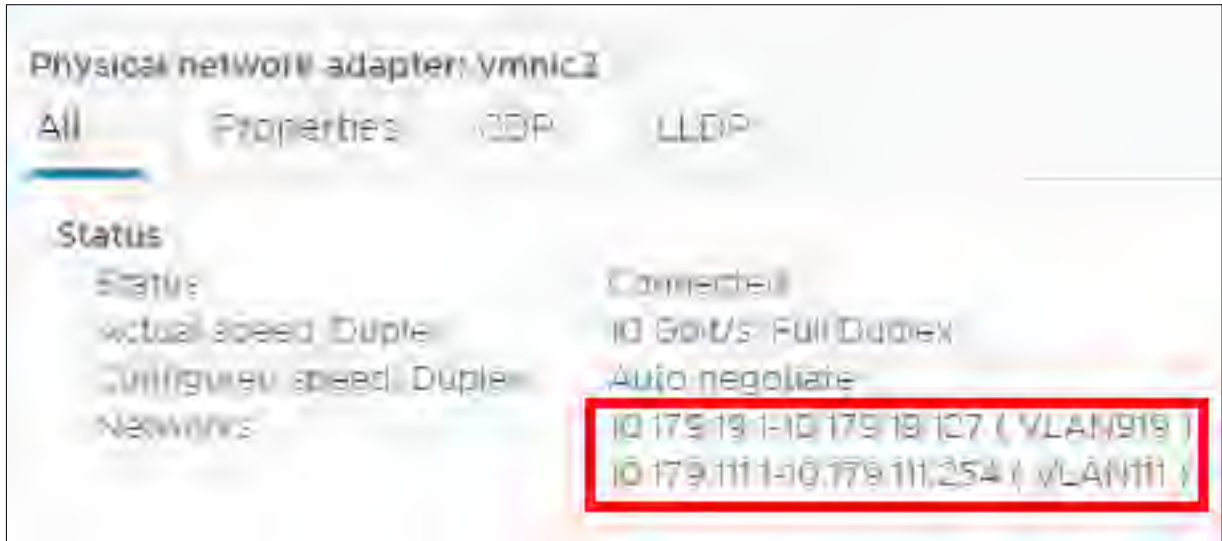


Figure 169. Wait for Networks to Appear

Configure timvhost04 – vmnic4

Steps / Screenshots

1.
 - (1) Click host and clusters,
 - (2) Click the down arrow next to TIMSO Cluster,
 - (3) Click timvhost04.smartsunguide.com,
 - (4) Click Configure,
 - (5) Click Physical adapters,
 - (6) Click vmnic4.

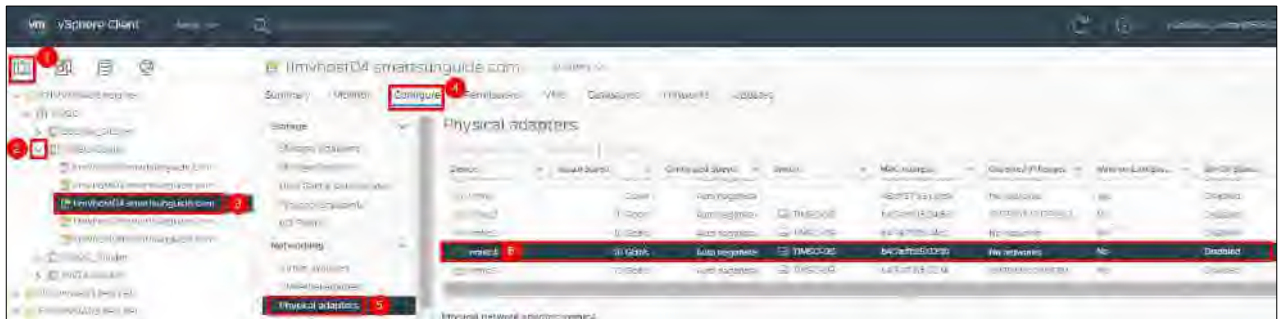


Figure 170. Configure timvhost04 – vmnic4

2. Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), to be provided to the Network Manager.
 - Device ID: **Switch # 1**
 - Port ID: **Port # 12**

Steps / Screenshots

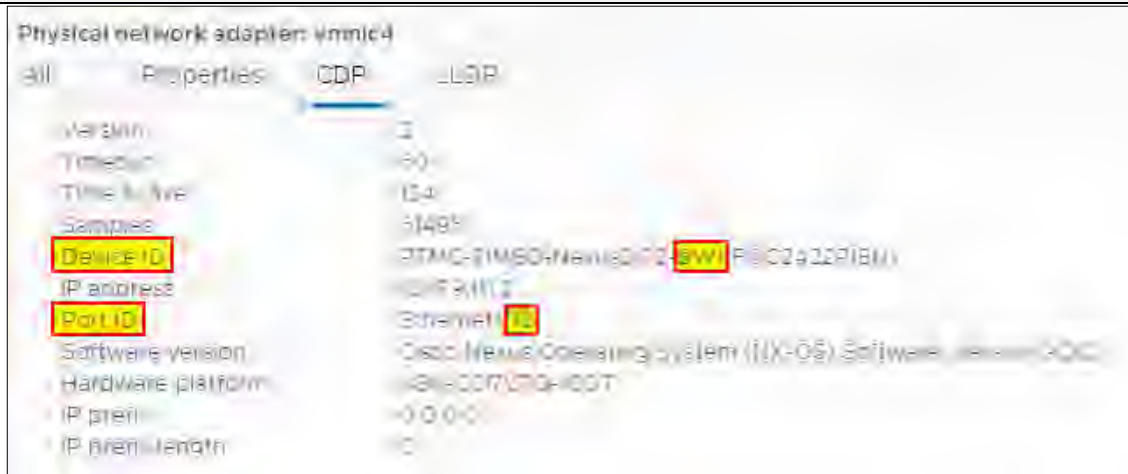


Figure 171. vmnic4 Device ID and Port ID

- On the physical switch, the Network Manager will down the port connected to vmnic4. Confirm that the port is **Down**.

Device	Status	Speed	MAC Address	Received IP Pkts	Error Rate
vmnic0	Down	Auto negotiate	18:0d:11:03:4d:01	0	0.00%
vmnic1	Down	Auto negotiate	a8:1d:11:03:4d:02	0	0.00%
vmnic2	Down	Auto negotiate	24:7a:11:03:4d:03	0	0.00%
vmnic3	Down	Auto negotiate	64:7a:11:03:4d:04	0	0.00%
vmnic4	Down	Auto negotiate	b4:7a:11:03:4d:05	0	0.00%
vmnic5	Down	Auto negotiate	24:7a:11:03:4d:06	0	0.00%

Figure 172. Confirm that the Port is Down

- On the physical switch, the Network Manager will place the port connected to vmnic4 in the LACP/EtherChannel configuration.

- (1) Click **networking**,
- (2) Right-click **TIMSO-DS**,
- (3) Click Add and Manage Hosts.

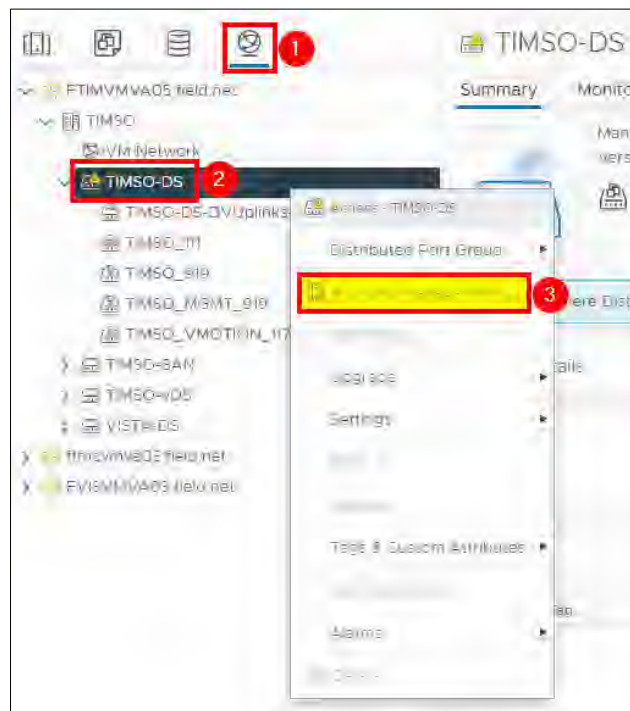


Figure 173. Add and Manage Hosts

Steps / Screenshots

5.
 - Select Manage host networking and
 - Click **NEXT**.

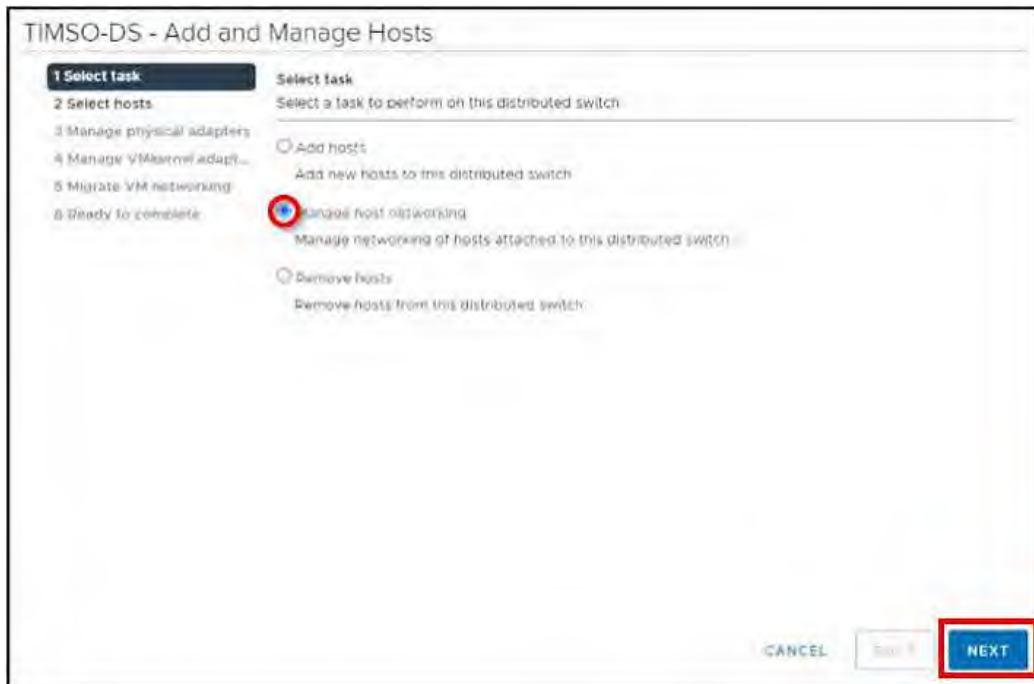


Figure 174. Select Task

6.
 - Click Attached hosts,
 - Check the box next to timvhost04.smarsunguide.com,
 - Click **OK**.

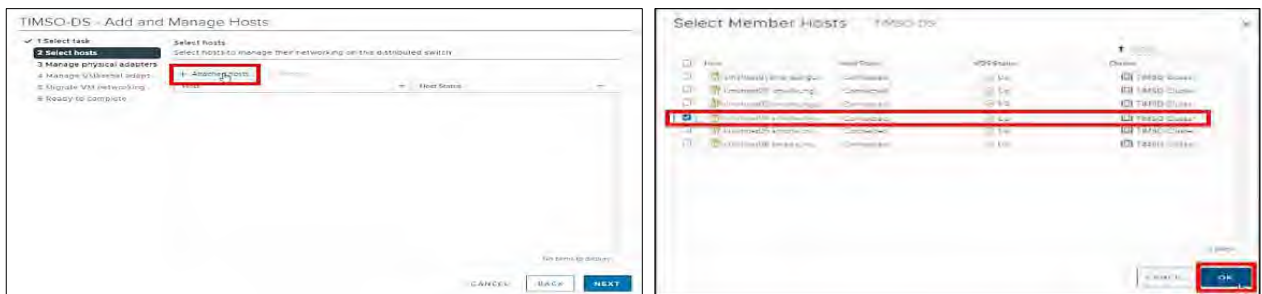


Figure 175. Select Member Host

Steps / Screenshots

7. Click **NEXT**.

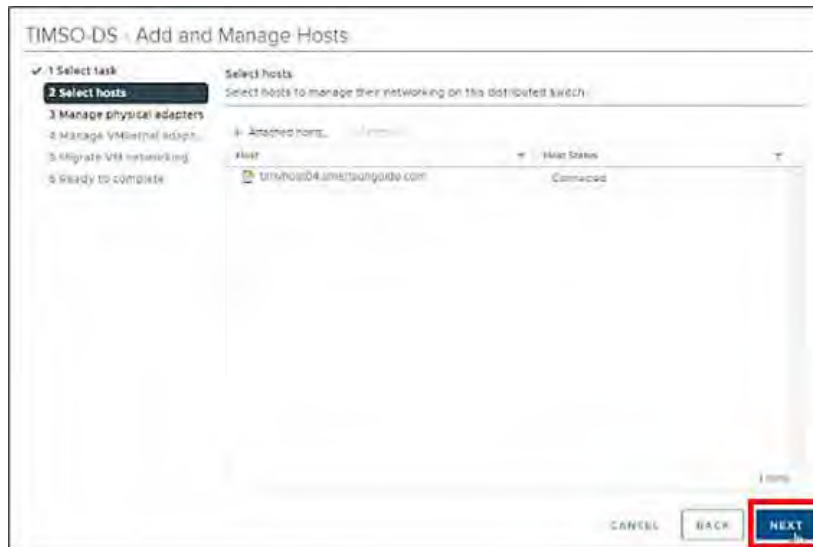


Figure 176. Select Host.

- 8.
 - Select **vmnic4** and
 - Click Assign uplink.

Add **vmnic4** in one of the LAG uplinks.

- (3) Select the **LAG_1-2** and
- (4) Click **OK**.

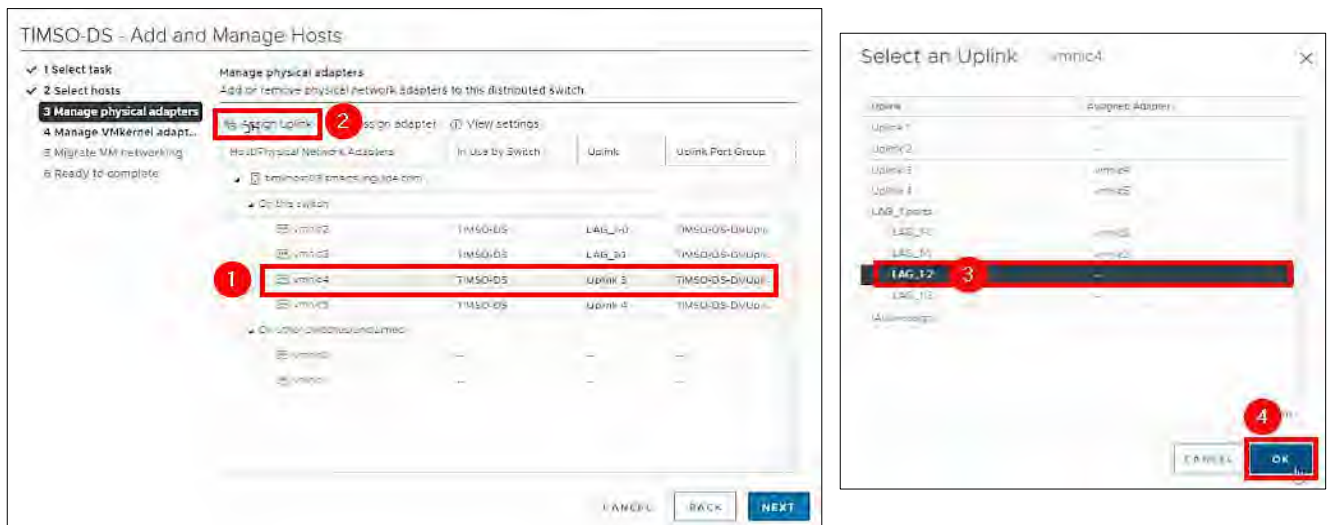


Figure 177. Manage Physical Adapters – Select an Uplink.

Steps / Screenshots

9. Click **NEXT**.

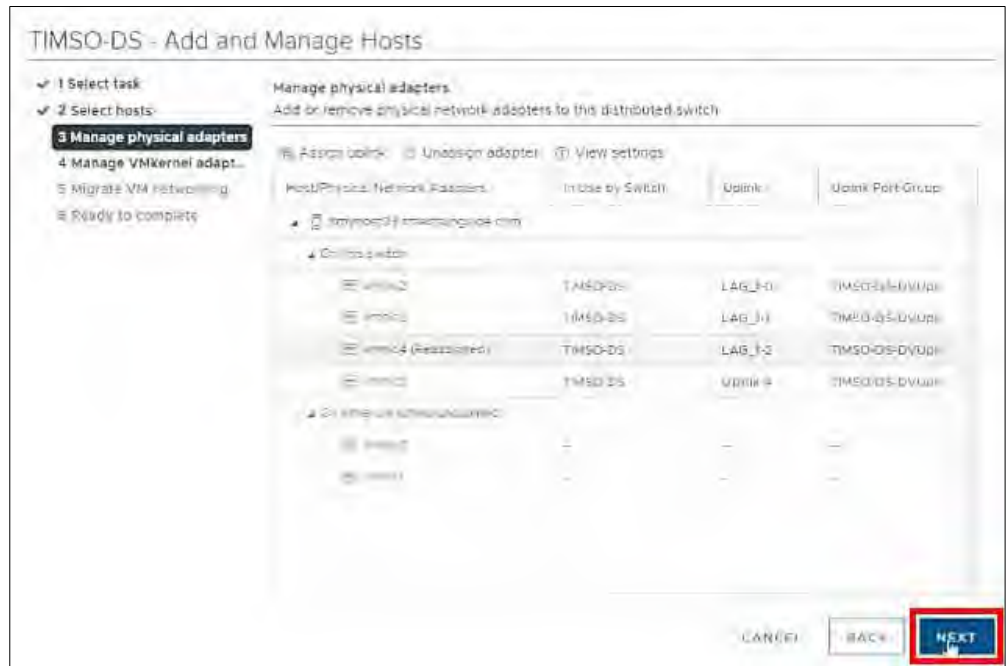


Figure 178. Manage Physical Adapters.

10. Click **NEXT**.

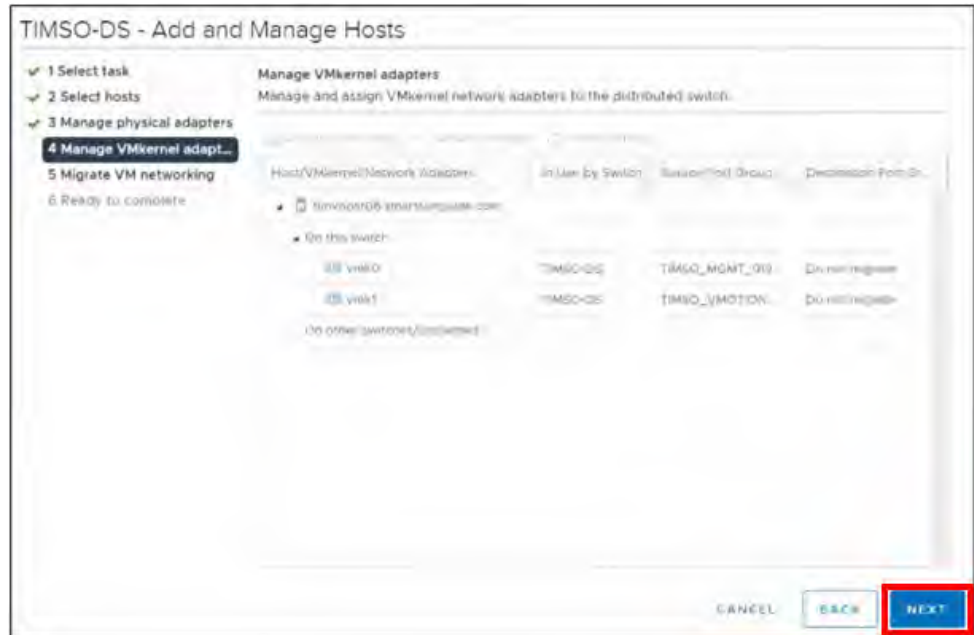


Figure 179. Manage VMkernel Adapters.

Steps / Screenshots

11. Click **NEXT**.

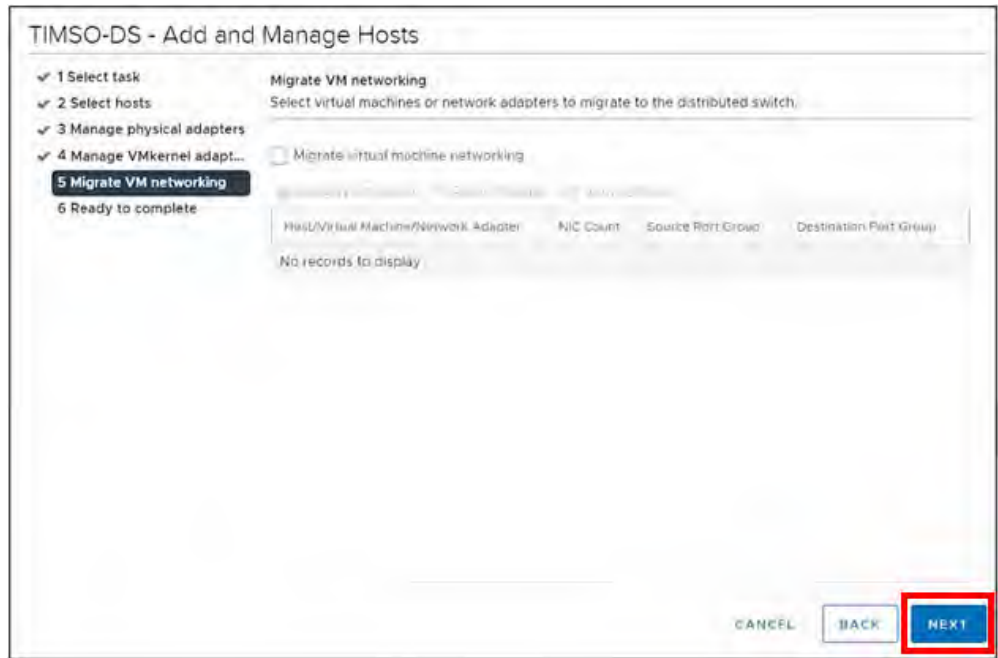


Figure 180. Migrate VM Networking.

12. Click **FINISH**.



Figure 181. Ready to Complete.

The Network Manager will bring the port back up. Go back **Physical adapters**. Wait for port to come back up,

Device	Actual Speed	Configured Speed	Switch	MAC Address	Observed IP Ranges	Wake on LAN Sup...	SR-IOV Status
vmnic0	Down	Auto negotiate	--	48:df:37:e3:cd:b9	No networks	Yes	Disabled
vmnic1	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ft:85:04:68	10.179.19.1-10.179.19.12...	No	Disabled
vmnic2	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ft:85:04:6c	No networks	No	Disabled
vmnic3	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ft:85:02:10	No networks	No	Disabled
vmnic4	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ft:85:02:14	10.179.19.100-10.179.1...	No	Disabled
vmnic5	10 Gbit/s	Auto negotiate	TIMSO-DS				

Figure 182. Wait for Port to Come Back Up.

Steps / Screenshots

13. Click the **All** tab and wait for networks to appear.

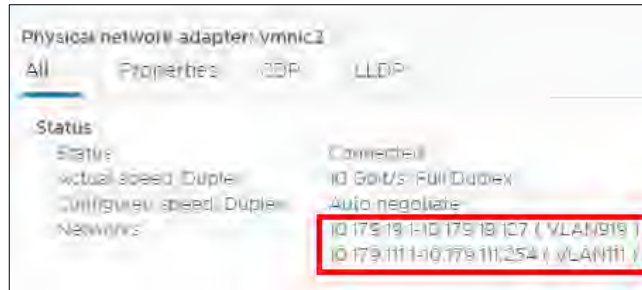


Figure 183. Wait for Networks to Appear

Configure timvhost04 – vmnic5

Steps / Screenshots

1.
 - (1) Click host and clusters,
 - (2) Click the down arrow next to **TIMSO Cluster**,
 - (3) Click timvhost04.smartsunguide.com,
 - (4) Click **Configure**,
 - (5) Click Physical adapters,
 - (6) Click **vmnic5**.

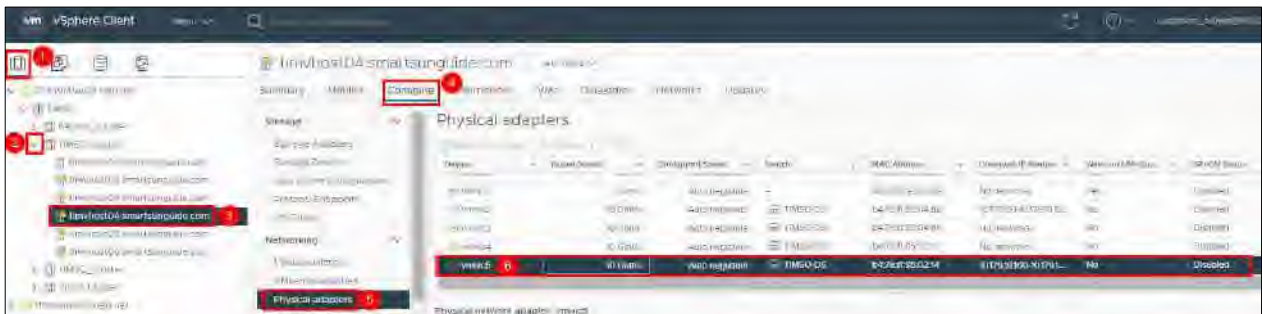


Figure 184. Configure timvhost04 – vmnic5.

2. Click the **CDP** tab to find the Device ID and Port ID (Switch # and Port #), to be provided to the Network Manager.

- Device ID: **Switch # 2**
- Port ID: **Port # 12**

Steps / Screenshots

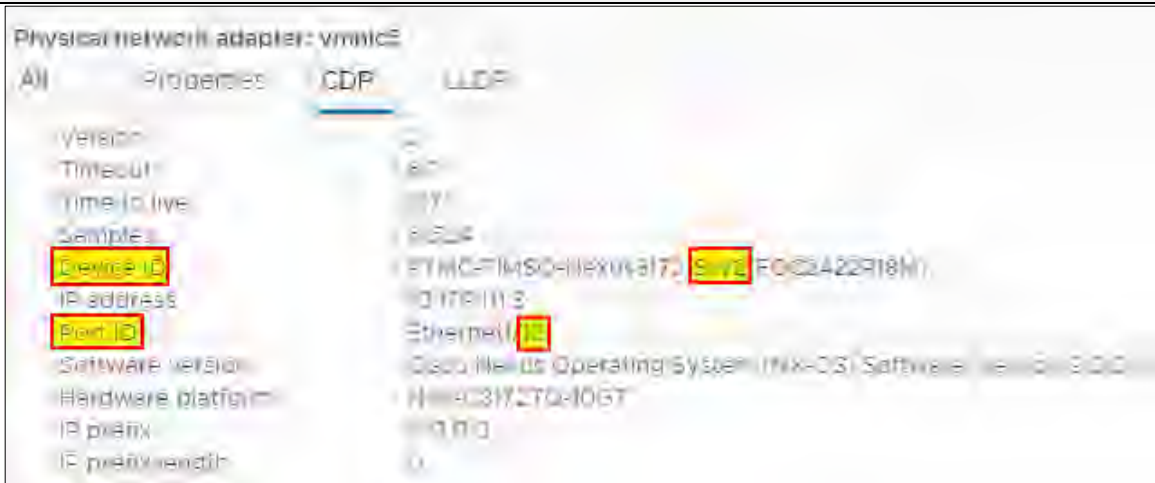


Figure 185. vmnic5 Device ID and Port ID.

- On the physical switch, the Network Manager will down the port connected to vmnic5. Confirm that the port is **Down**.

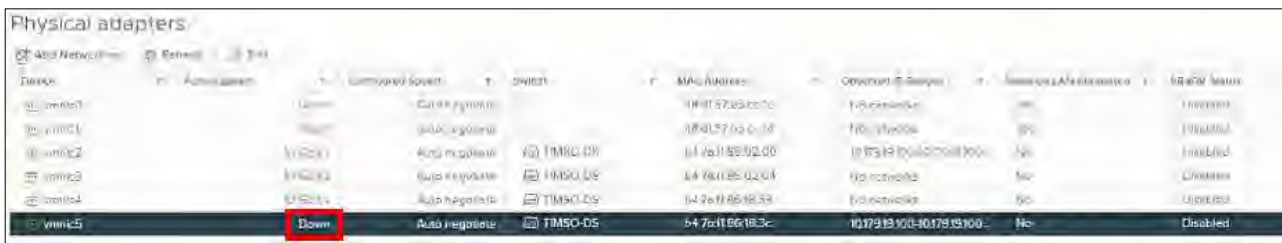


Figure 186. Confirm that the Port is Down

- On the physical switch, the Network Manager will place the port connected to vmnic4 in the LACP/EtherChannel configuration.
 - (1) Click **networking**,
 - (2) Right-Click **TIMSO-DS**,
 - (3) Click **Add and Manage Hosts**.

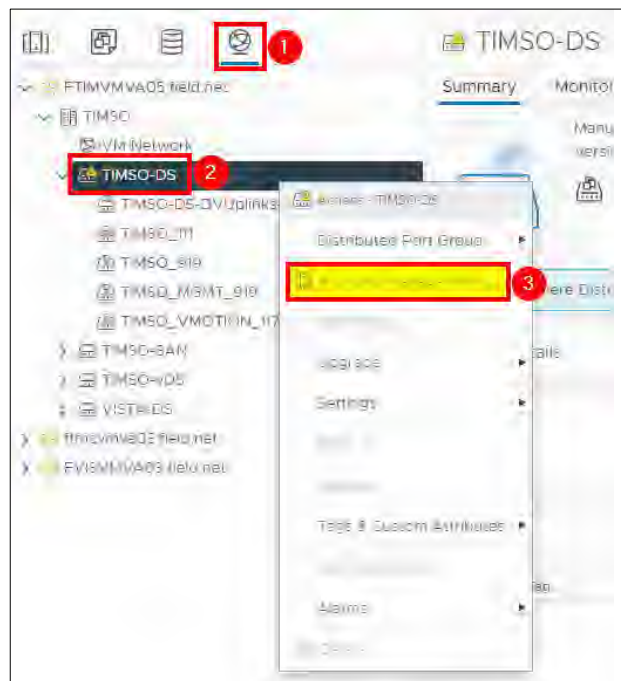


Figure 187. Add and Manage Hosts.

Steps / Screenshots

5.
 - Select Manage host networking
 - Click **NEXT**.

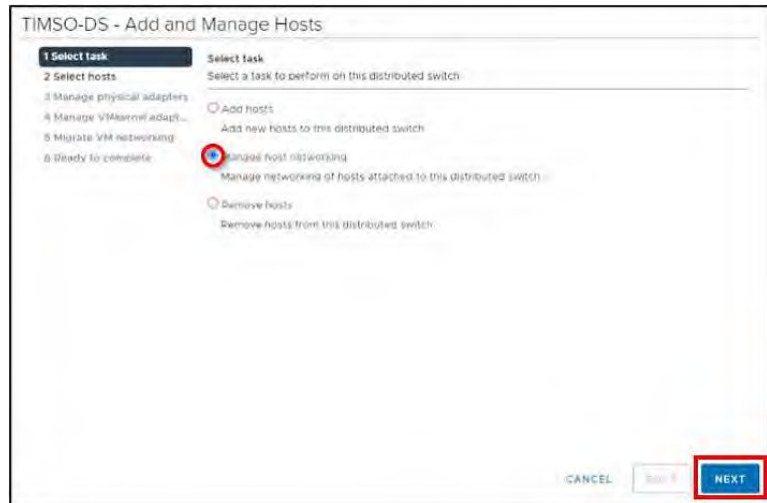


Figure 188. Select Task.

6.
 - Click Attached hosts,
 - Check the box next to timvhost04.smarsunguide.com,
 - Click **NEXT**.

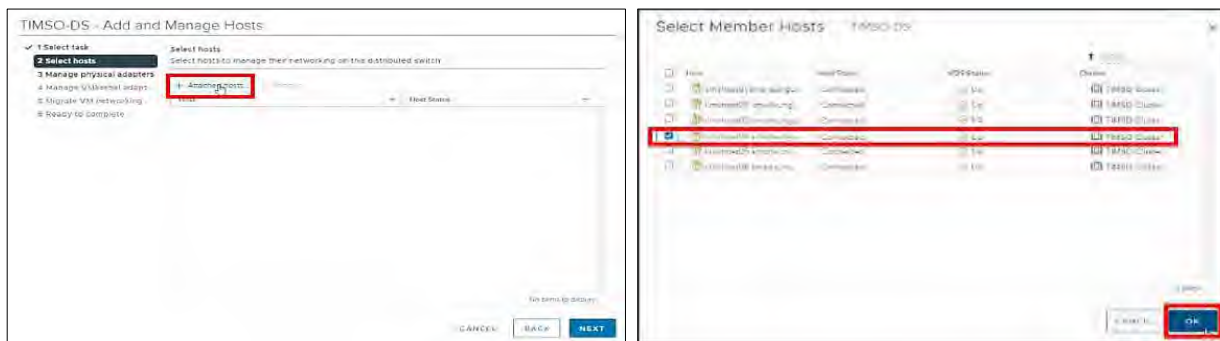


Figure 189. Select Member Host.

7. Click **NEXT**.

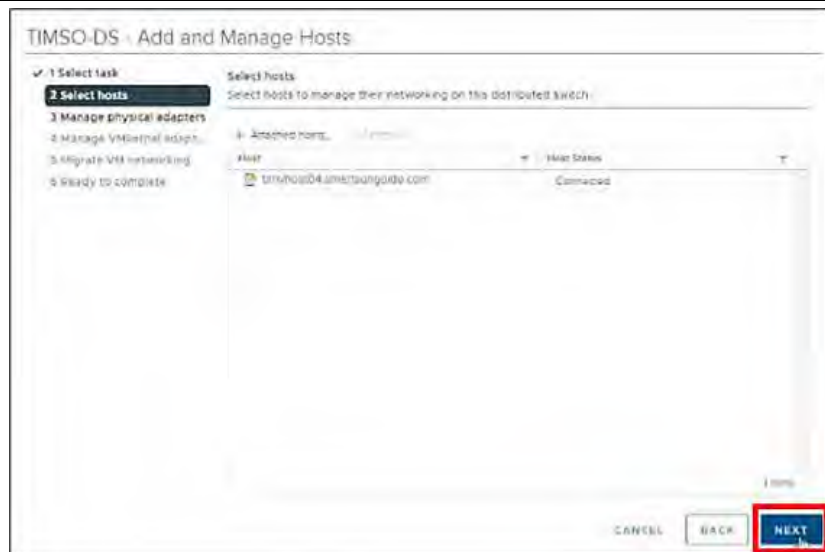


Figure 190. Select Host.

Steps / Screenshots

8.
 - Select **vmnic5** and
 - Clicking Assign uplink.

Add **vmnic5** in one of the LAG uplinks by.

- Select the **LAG_1-3**
- Click **OK**.

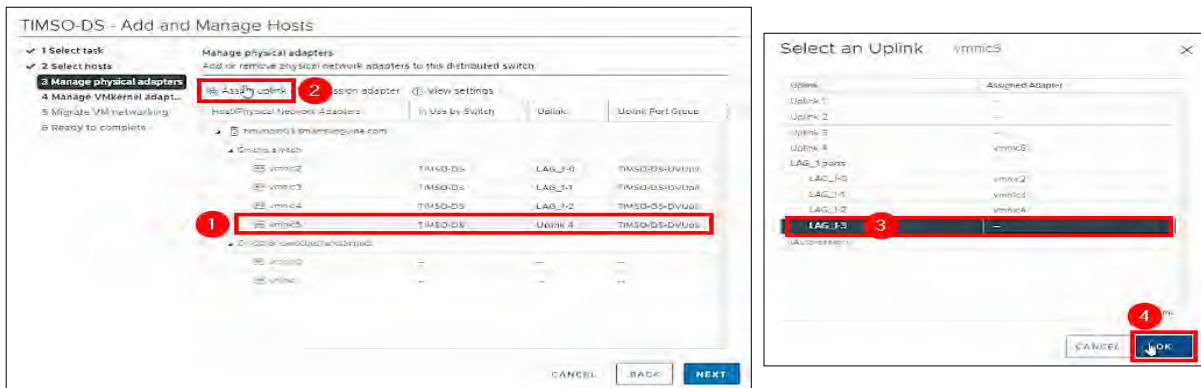


Figure 191. Manage Physical Adapters – Select an Uplink

9. Click **NEXT**.

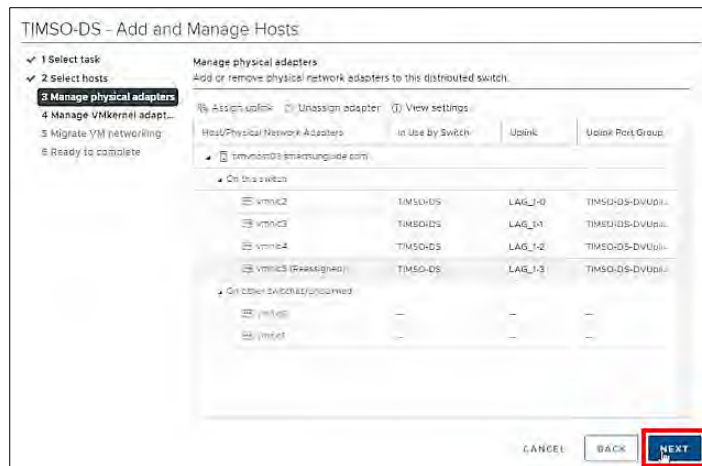


Figure 192. Manage Physical Adapters

Steps / Screenshots

10. Click **NEXT**.



Figure 193. Manage VMkernel Adapters.

11. Click **NEXT**.

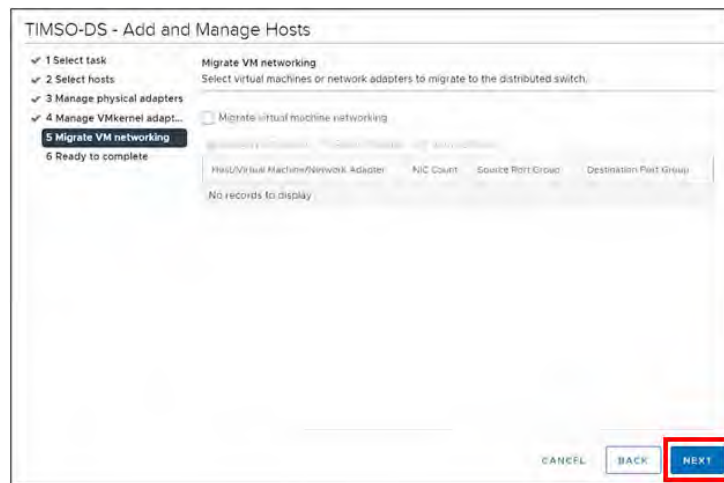


Figure 194. Migrate VM Networking.

12. Click **FINISH**.



Figure 195. Ready to Complete

The Network Manager will bring the port back up. Go back **Physical adapters**. Wait for port to come back up,

Steps / Screenshots

Physical adapters

Add Networking... Refresh Edit...

Device	Actual Speed	Configured Speed	Switch	MAC Address	Observed IP Ranges	Wake on LAN Sup...	SR-IOV Status
vmnic1	Down	Auto negotiate	--	48:df:37:e3:cd:b9	No networks	Yes	Disabled
vmnic2	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ff:85:04:68	10.179.19.1-10.179.19.12...	No	Disabled
vmnic3	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ff:85:04:6c	No networks	No	Disabled
vmnic4	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ff:85:02:10	No networks	No	Disabled
vmnic5	10 Gbit/s	Auto negotiate	TIMSO-DS	b4:7a:ff:85:02:14	10.179.19.100-10.179.1...	No	Disabled

Figure 196. Wait for Port to Come Back Up.

- Click the **All** tab and wait for networks to appear.

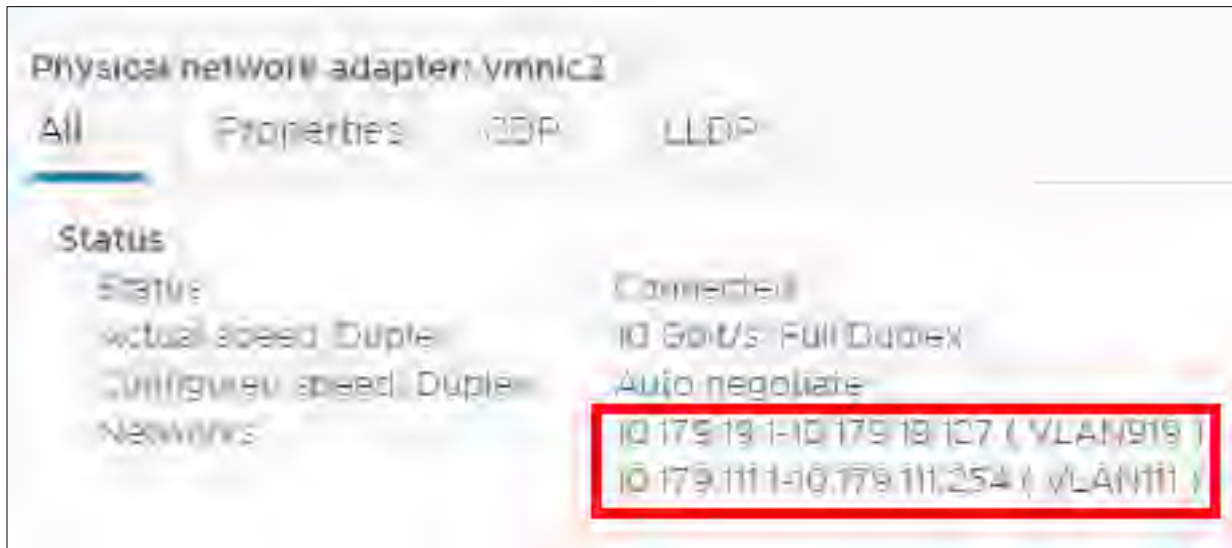


Figure 197. Wait for Networks to Appear

Configure timvhost02, timvhost03, timvhost05,timvhost06

- Refer to steps 1 – 4 in the **Configure timvhost04** procedures.
- Configure **vmnic2 – vmnic5** on **timvhost02, timvhost03, timvhost05,timvhost06** in accordance with all the steps (1 – 4) of the **Configure timvhost04** procedures.

Edit Distributed Port Groups for TIMSO-DS

Perform steps below, to change the **Teaming and Failover** on all distributed port groups to use the LAG instead of the uplinks.

1. (1) Click **Networking**,
- (2) Click the down arrow next to **TIMSO-DS**,
- (3) Right-click one of the distributed port groups,
- (4) Click Edit Settings.

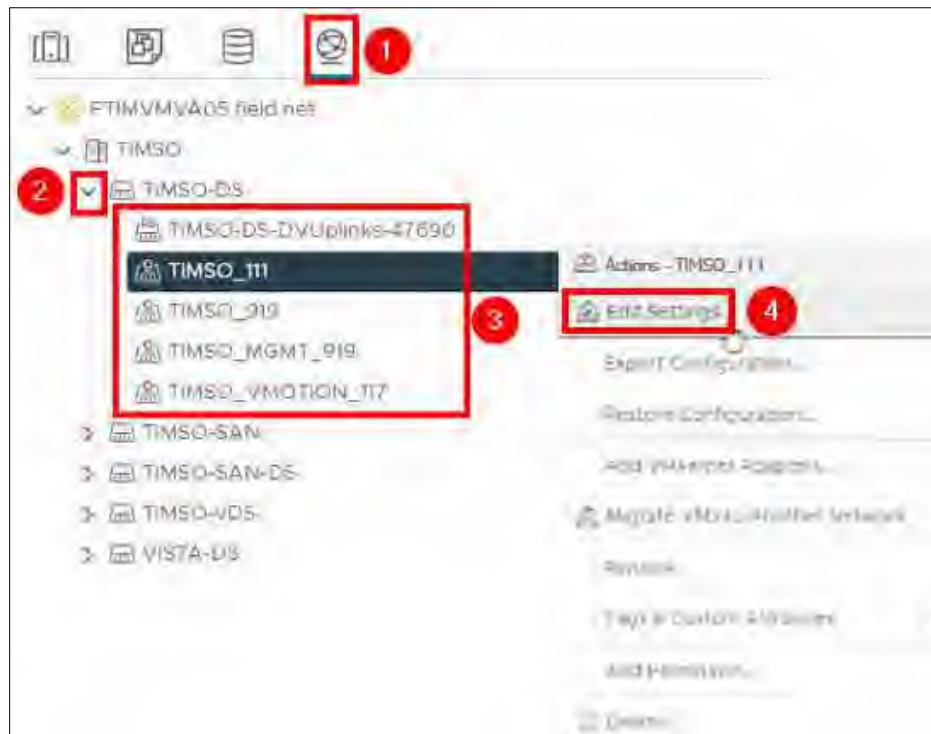


Figure 198. Edit Distributed Port Groups for TIMSO-DS

2. Click Teaming and Failover, move Uplink 1 and Uplink 2 to Unused uplinks.



Figure 199. Move Uplink 1 and Uplink 2 to Unused Uplinks.

3.
 - Move **LAG_1** to Active uplinks.
 - Click **OK**.

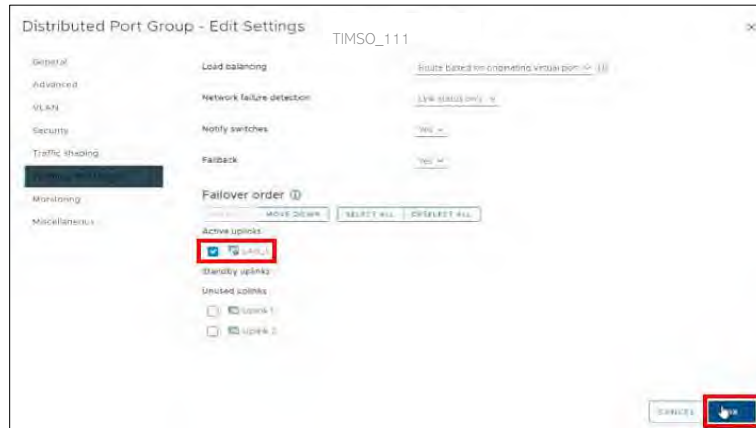


Figure 200. Move LAG_1 to Active Uplinks.

Repeat steps above on all other distributed port groups under TIMSO-DS.

ADD an iSCSI ADAPTER to a HOST

ESXi Configuration: Disk.DiskMaxIOSize = 1024

1. Click tmcvhost02.smartsunguide.com,
 - Click **Configure**, **Advance System Settings**,
 - Click **Edit**.

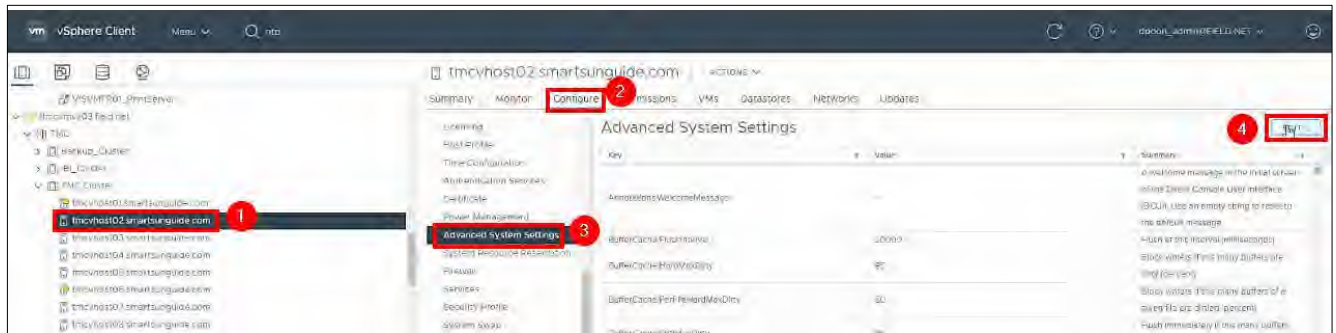


Figure 201. Access Edit Advanced System Settings

2.
 - (1) Enter **Disk.DiskMaxIOSize** in the filter line,
 - (2) Change the value to **1024**,
 - (3) Click **OK**.

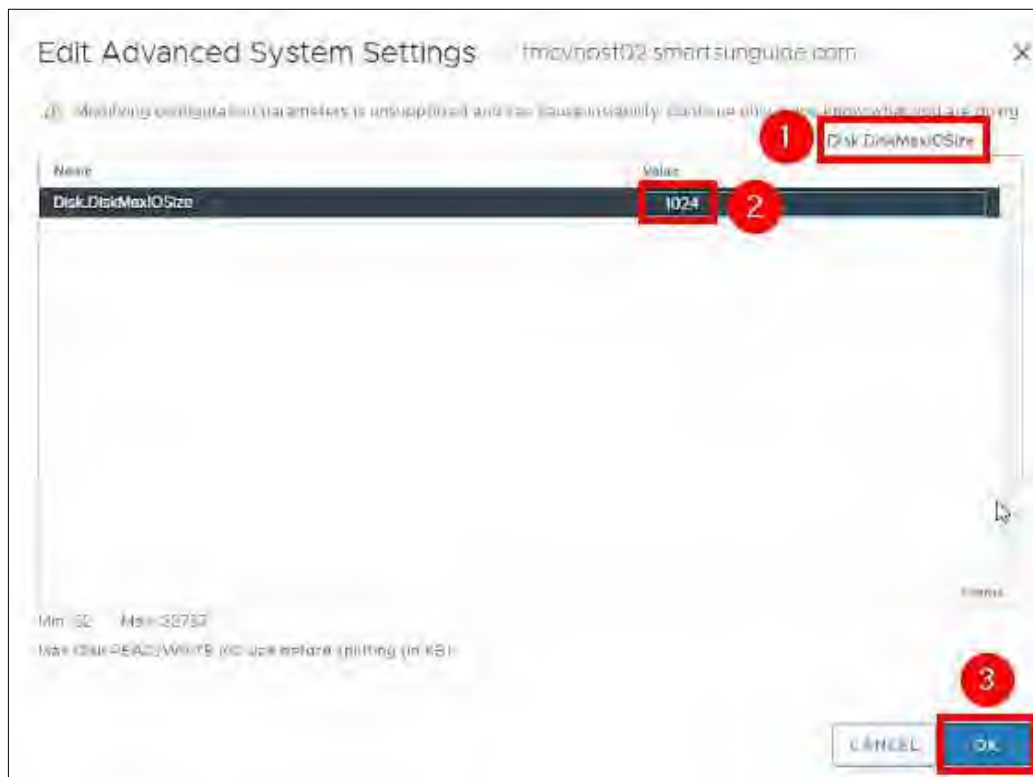


Figure 202. Edit Advanced Systems

3.
 - Click **Storage Adapters**
 - Click **Add Software Adapter**.



Figure 203. Add Software Adapter.

4. With Add Software iSCSI Adapter selected,
 - Click **OK**.



Figure 204. Add Software iSCSI Adapter

Repeat steps above for all other TMC hosts.

CREATE a NEW DISTRIBUTED SWITCH

- # Steps / Screenshots
1.
 - (1) Click **Networking**,
 - (2) Right-click **TMC**,
 - (3) Click Distributed Switch,
 - (4) Click New Distributed Switch

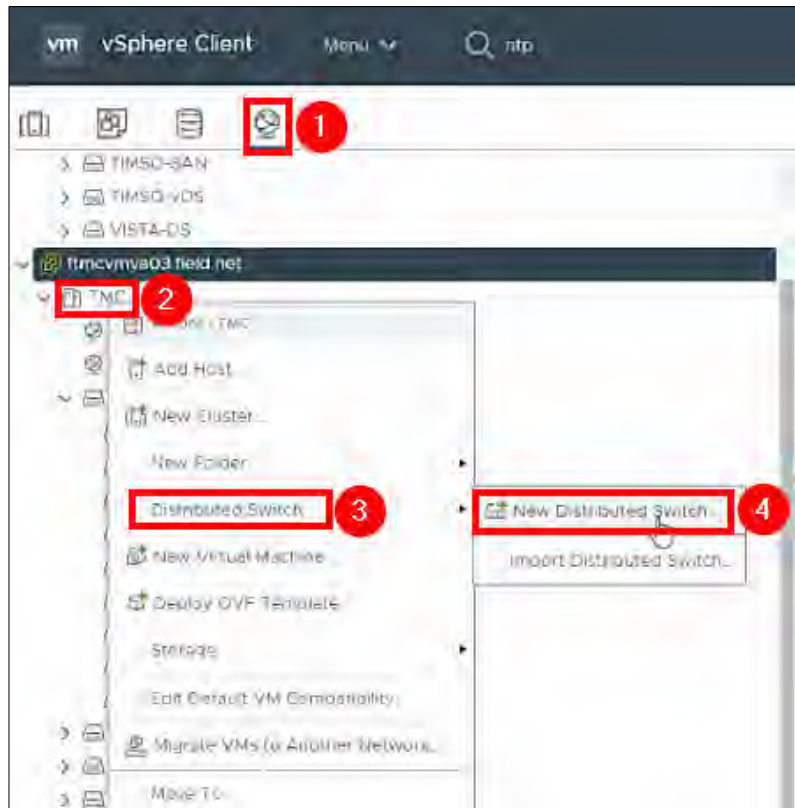


Figure 205. New Distributed Switch

2.
 - Enter **TMC-SAN-DS** in the **Name** field
 - Click **NEXT**.

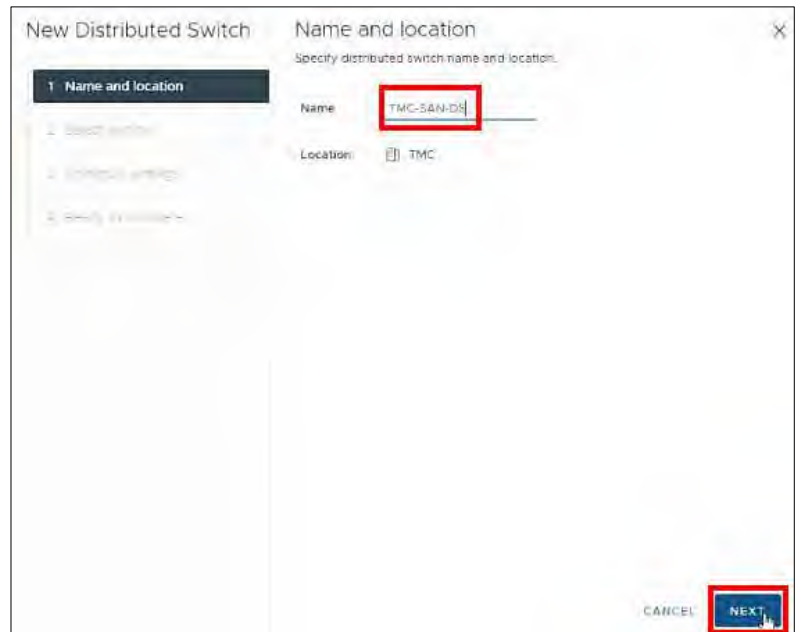


Figure 206. Name and Location.

Steps / Screenshots

3. Click **NEXT**.

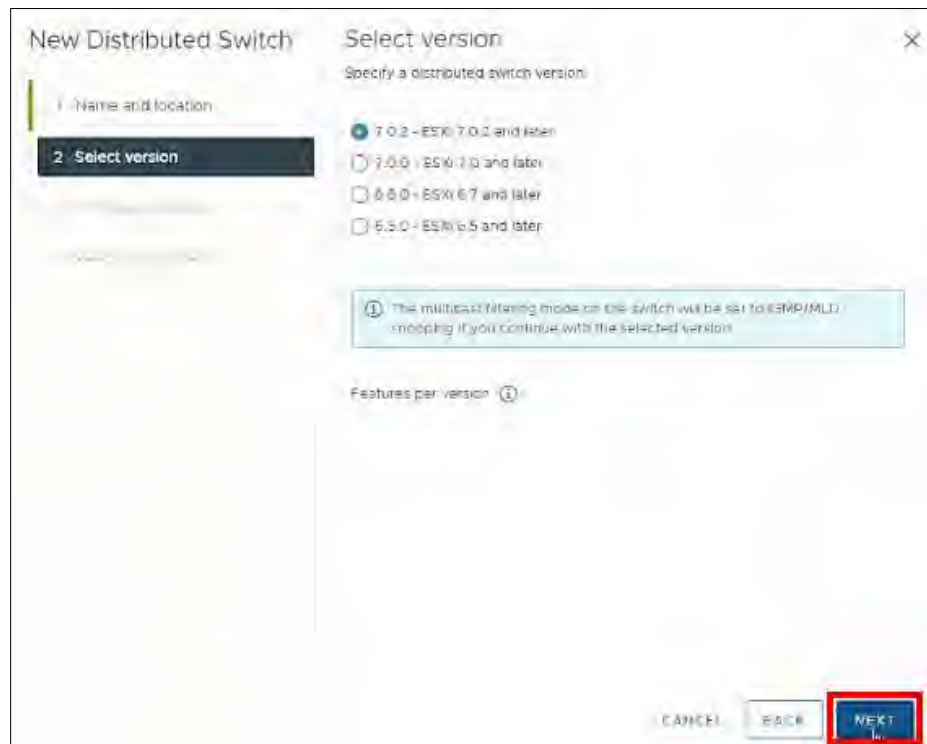


Figure 207. Select Version.

- 4.
 - Enter **2** in the **Number of ports** field.
 - Enter **TMC_SAN_41** in the Port group name field.
 - Click **NEXT**.

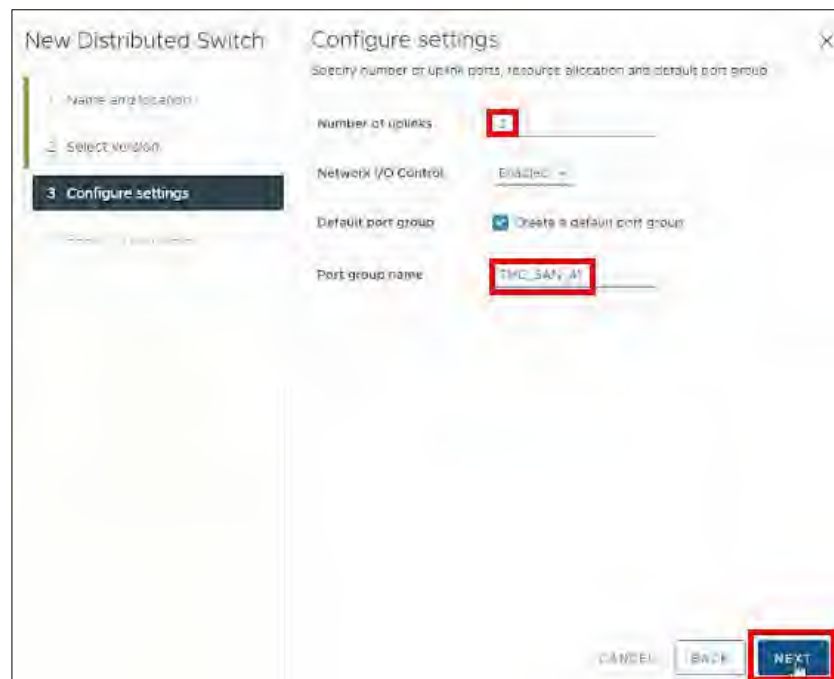


Figure 208. Configure Settings

Steps / Screenshots

5. Click **Finish**.



Figure 209. Ready to Complete.

ENABLE JUMBO FRAMES

Enable Jumbo Frames on the New Distributed Switch

Steps / Screenshots

1. In **vSphere**,
 - Right-Click **TMC-SAN-DS**,
 - Click **Settings**,
 - Select **Edit Settings**.

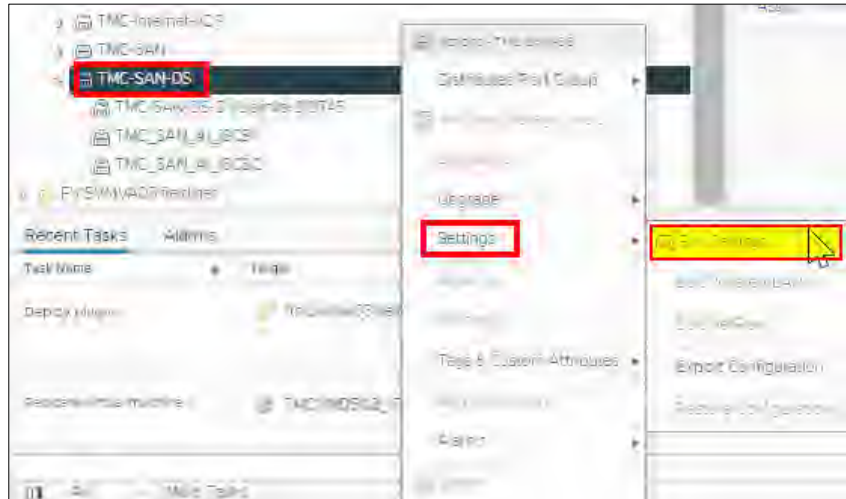


Figure 210. Edit Settings.

2.
 - Click **Advanced**
 - Change the size of the maximum transmission unit (MTU) to 9000 bytes,
 - Click **OK**.

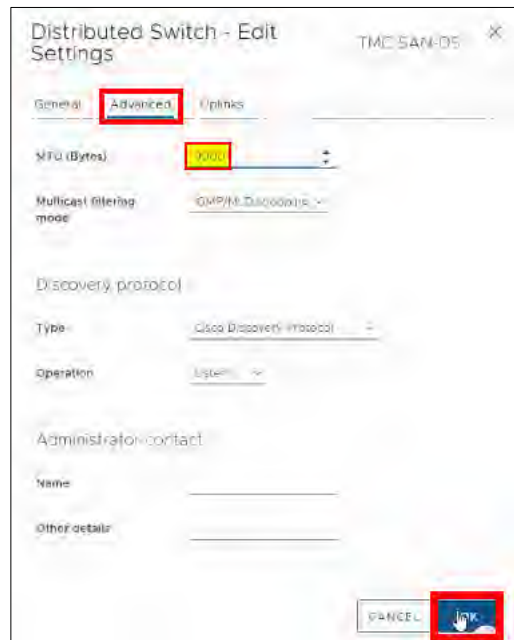


Figure 211. Advanced Settings.

Enable Jumbo Frames on the Cluster

1. In the RTMC-PowerStore SAN,
 - (1) Click Settings
 - (2) Click Cluster MTU.

2.
 - (3) Change the MTU size to **9000** bytes.
 - (4) Click **APPLY**.



Figure 212. Cluster MTU.

HOST GROUPS

Add Hosts to A Distributed Switch

#	Steps / Screenshots
---	---------------------

- (1) Click **Networking**,
 - (2) right Click **TMC_SAN_DS**,
 - (3) Click **Add and Manage Hosts**.

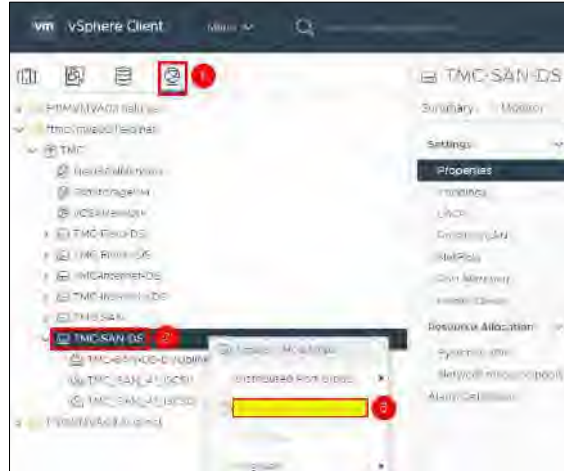


Figure 213. Add and Manage Hosts.

- Click **NEXT**.

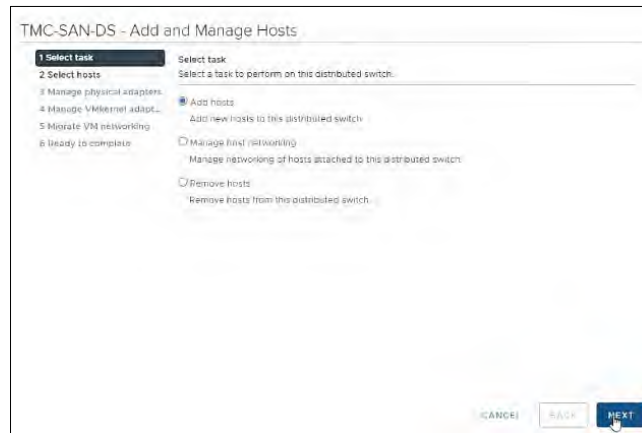


Figure 214. Select Task.

- Click **New Hosts**.



Figure 215. Select Hosts.

Steps / Screenshots

- 4. – Check the box next to **Host** to
- Select all hosts.
- Click **OK**.

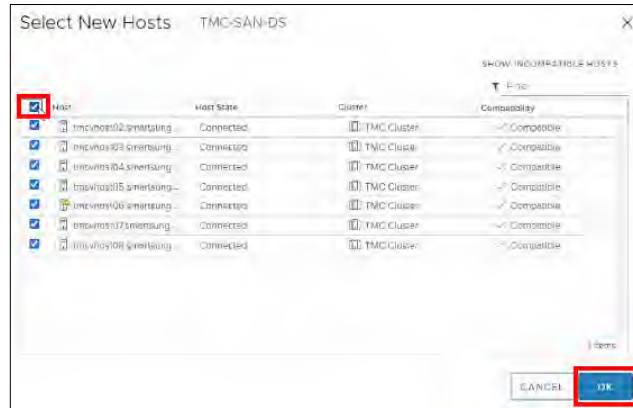


Figure 216. Select All Hosts.

- 5. – Click **NEXT**.

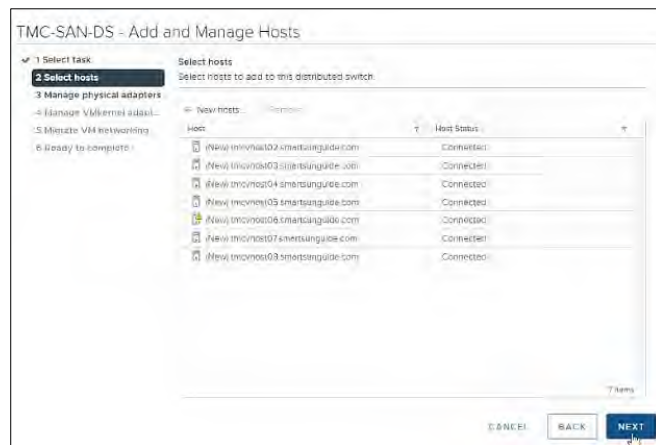


Figure 217. Hosts Selected.

- 6. – Continue clicking on **NEXT** until the **Ready to complete** window appears.
- Click **FINISH**.

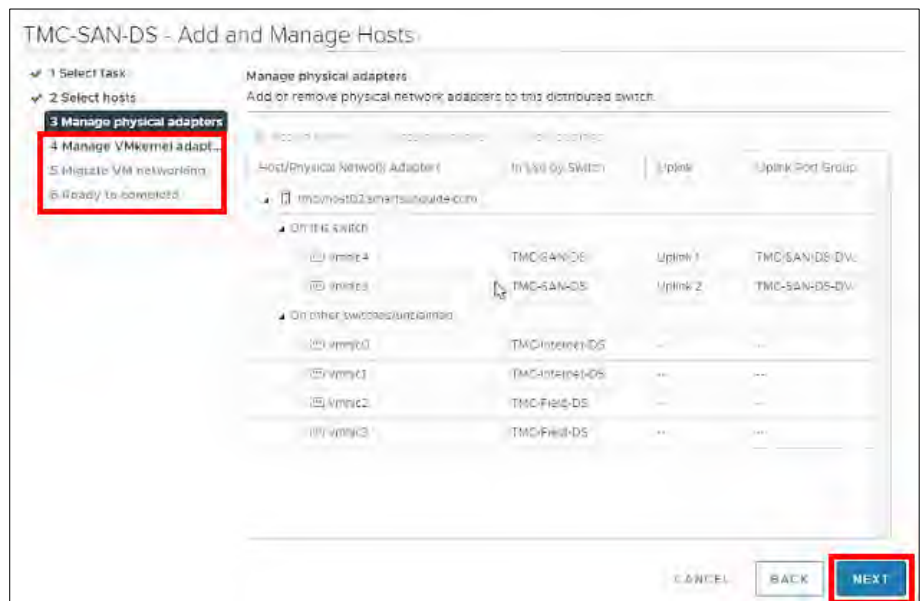


Figure 218. Complete Add and Manage Hosts.

Create A Host Group

1.
 - In the **RTMC-PowerStoreSAN**,
 - Click **Hosts & Host Groups**,
 - Click **ADD HOST GROUP**.



Figure 219. Identify & Add Host Group.

2.
 - Enter the Host Group Name,
 - Select **iSCSI**,
 - Click **Create**.

Add Host Group

Creating a host group will cause all members of the group to function as one. Access to volumes will only be assigned to the entire host group, not to individual hosts within the group.

Host Group Name

Description (optional)

Host Group Members
Choose the protocol type you would like to use for your new host group and select which hosts you want to be included.

iSCSI Fibre Channel

Available Hosts
Hosts with mapped volumes cannot be added to a host group and are not listed.

<input type="checkbox"/>	Name ↑	OS

Figure 220. Add Host Group.

ADD VMKernel ADAPTERS

Add VMkernel Adapters to the Hosts – TMC_SAN_41_iSCSI1

Steps / Screenshots

1.
 - (1) Click Hosts and Clusters,
 - (2) Click the down arrow next to **TMC Cluster**,
 - (3) Click tmcvhost02.smartsunguide.com,
 - (4) Click **Configure**,
 - (5) Click VMkernel adapters,
 - (6) Click Add Networking.

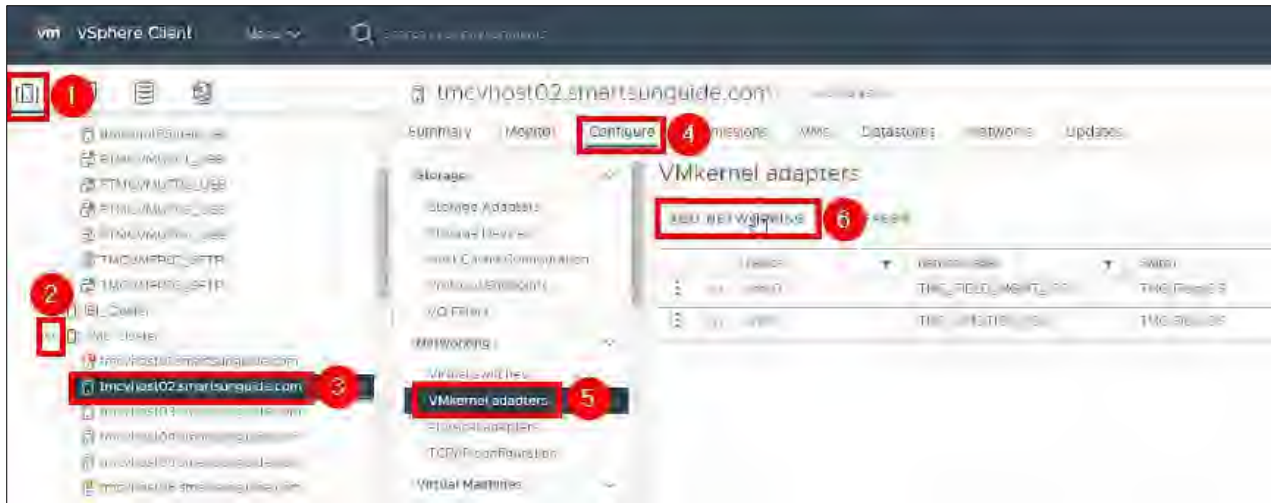


Figure 221. Add Networking.

2. Click **NEXT**.



Figure 222. Select Connection Type.

Steps / Screenshots

3. Click **Browse**.

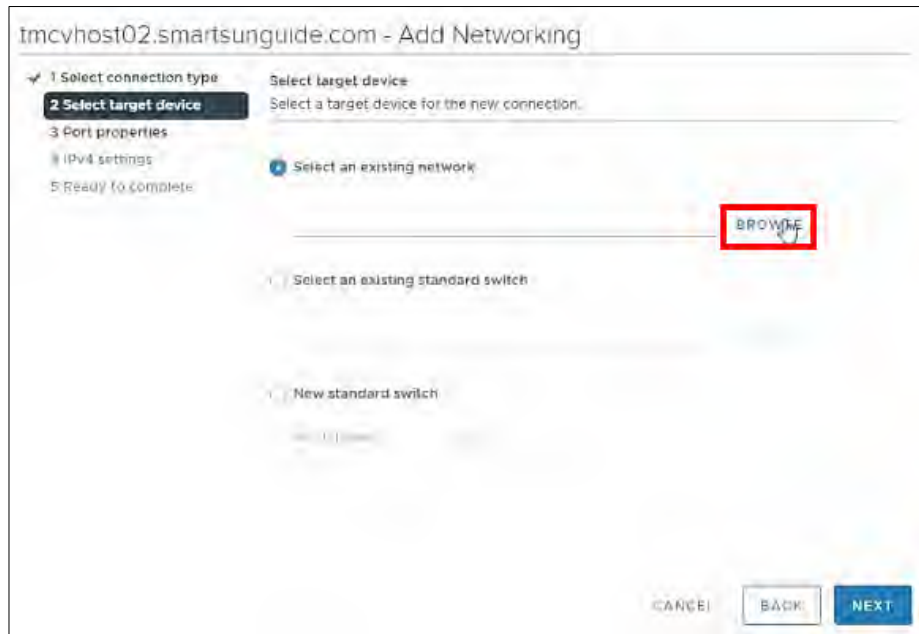


Figure 223. Browse.

- 4. – Select **TMC_SAN_41_iSCSI1**
- Click **OK**.



Figure 224. Select Network – TMC_SAN_41_iSCSI1.

Steps / Screenshots

5. Click **NEXT**.

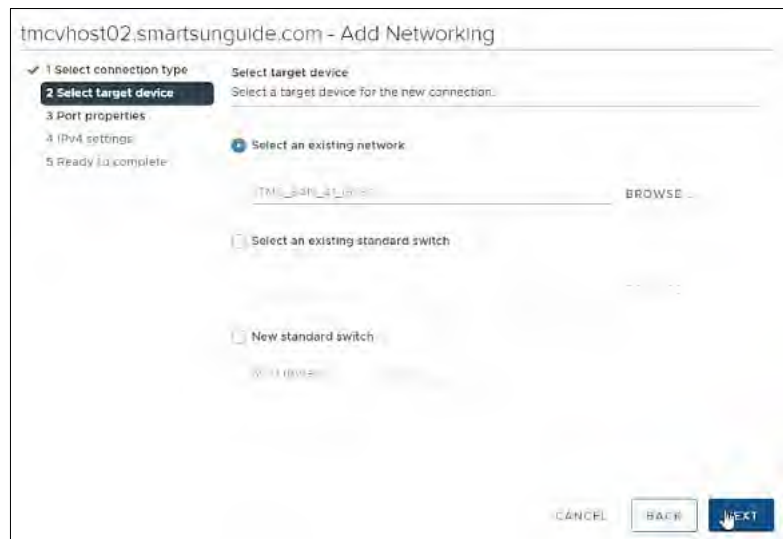


Figure 225. Select Target Device.

6. Click **NEXT**.

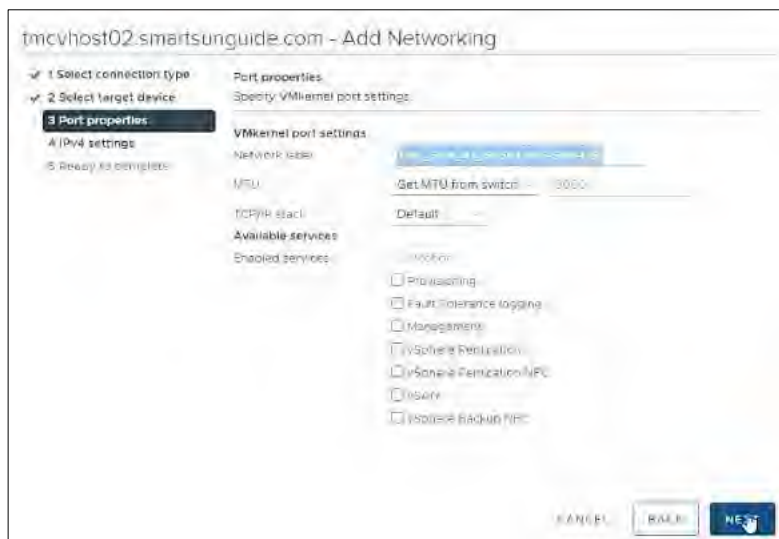


Figure 226. Port Properties.

Steps / Screenshots

- 7.
 - Select Use static IPv4 settings,
 - Enter the **IPv4 address**,
 - Enter the **Subnet mask**,
 - Click **NEXT**.

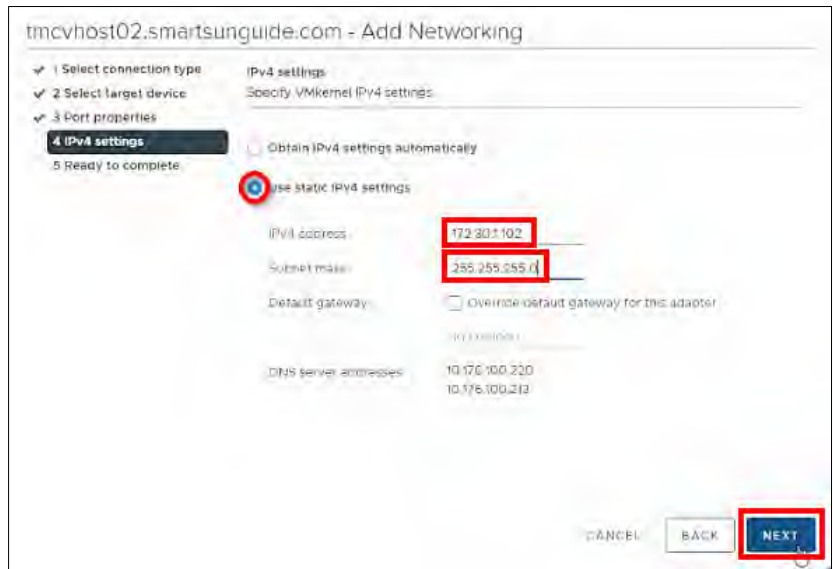


Figure 227. IPV4 Settings.

- 8. Click **FINISH**



Figure 228. Ready to Complete.

Add VMkernel Adapters to the Hosts – TMC_SAN_41_iSCSI2

Steps / Screenshots

1.
 - (1) Click Hosts and Clusters,
 - (2) Click the down arrow next to **TMC Cluster**,
 - (3) Click tmcvhost02.smartsunguide.com,
 - (4) Click Configure,
 - (5) Click VMkernel adapters,
 - (6) Click Add Networking.

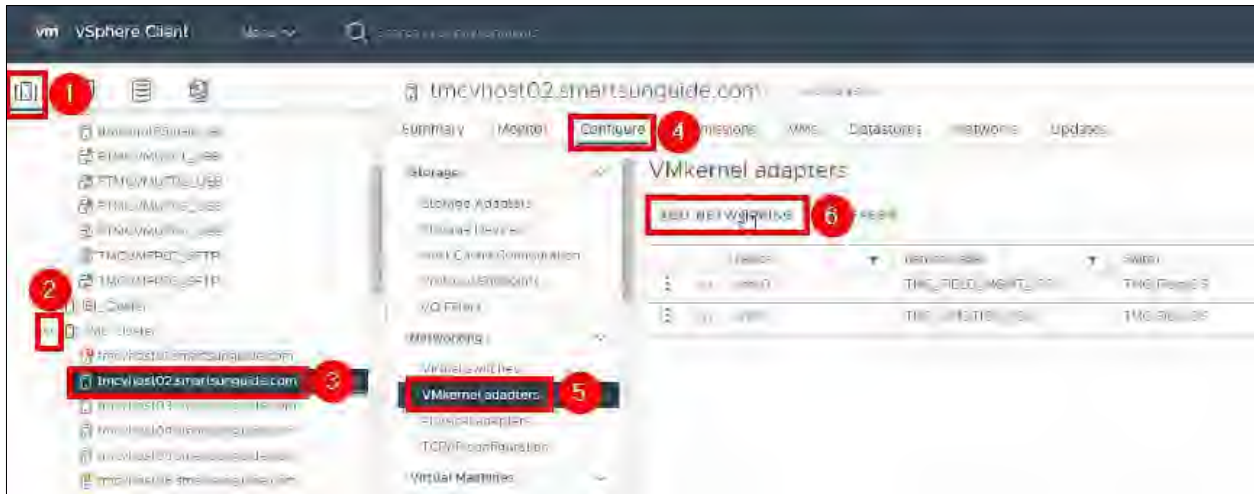


Figure 229. Add Networking.

2. Click **NEXT**.



Figure 230. Select Connection Type.

Steps / Screenshots

3. Click **Browse**.

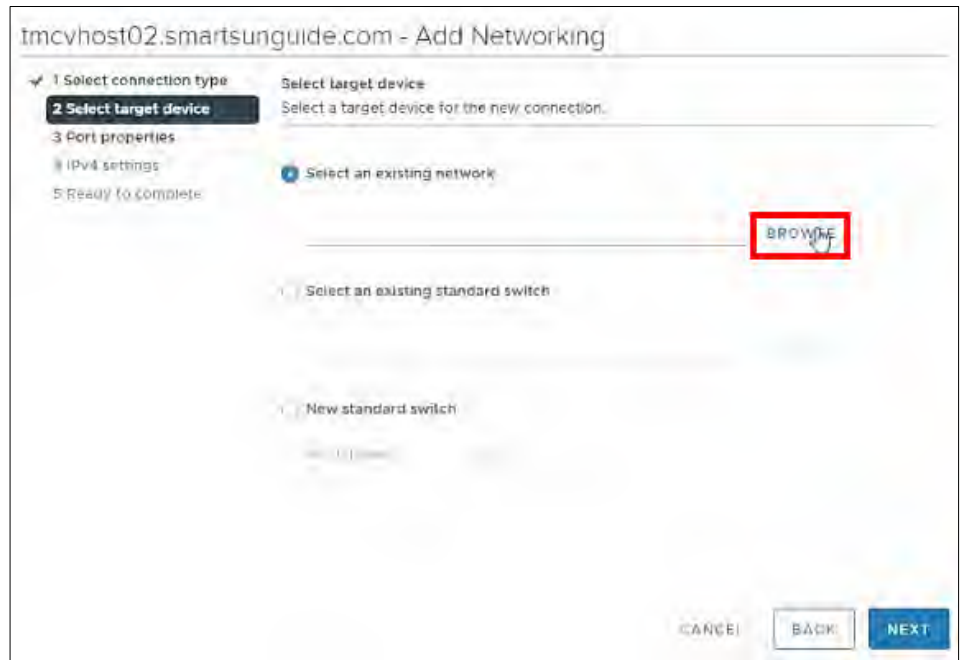


Figure 231. Browse.

- 4. – Select **TMC_SAN_41_iSCSI2**
- Click **OK**.

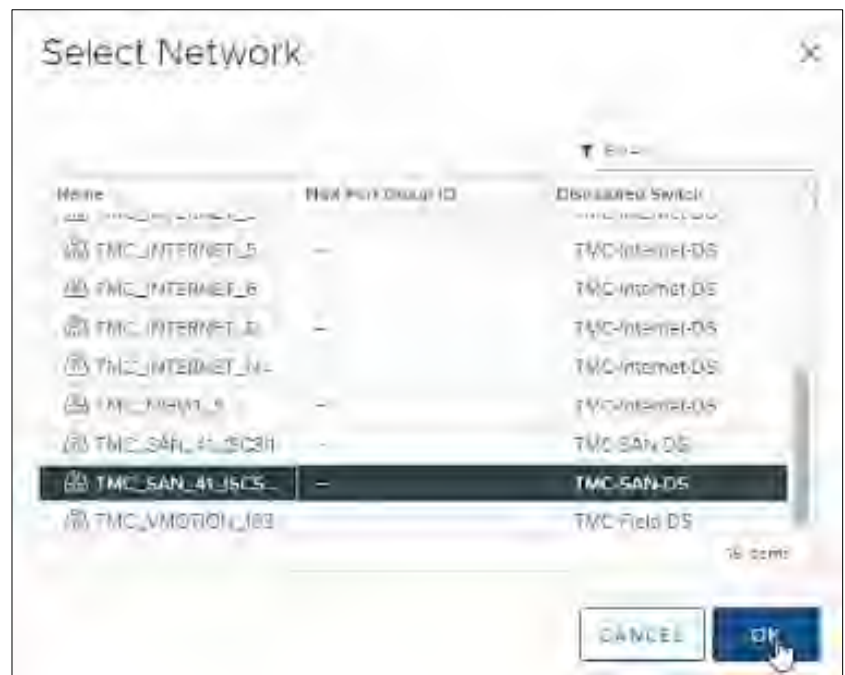


Figure 232. Select Network - TMC_SAN_41_iSCSI2.

Steps / Screenshots

5. Click **NEXT**.



Figure 233. Select Target Device.

6. Click **NEXT**.



Figure 234. Port Properties.

7.
 - Select Use static IPv4 settings,
 - Enter the **IPv4 address**,
 - Enter the **Subnet mask**,
 - Click **NEXT**.

Steps / Screenshots

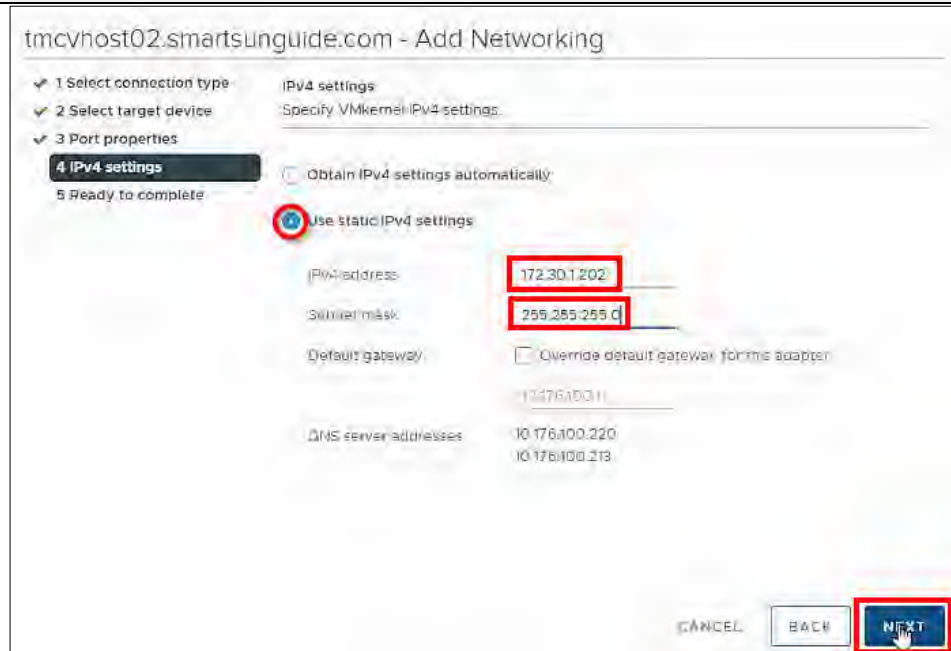


Figure 235. IPv4 Settings.

8. Click **FINISH**.



Figure 236. Ready to Complete.

Add Storage Adapters to the Hosts

Steps / Screenshots

1. – Enable **SSH** on all TMC hosts and execute the Putty command below on all **TMC** hosts:

```
esxcli storage nmp satp rule add -c tpgs_on -e "PowerStore" -M PowerStore -P VMW_PSP_RR -O iops=1 -s VMW_SATP_ALUA -t vendor -V DellEMC -o disable_action_OnRetryErrors
```

Figure 237. Putty Command.

2. – (1) Click hosts and clusters,
 – (2) Click the down arrow next to **TMC Cluster**,
 – (3) Click **tmcvhost02.smartsunguide.com**,
 – (4) Click **Configure**,
 – (5) Click **Storage Adapters**,
 – (6) Click **vmhba64**,
 – (7) Click **Dynamic Discovery**,
 – (8) Click **Add**.

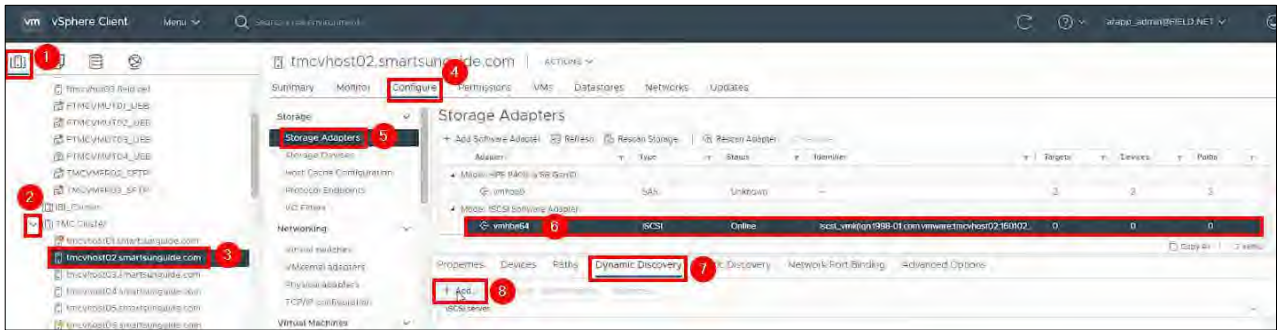


Figure 238. Add Storage Adapters.

3. – Enter the iSCSI Server
 – and Click **OK**.

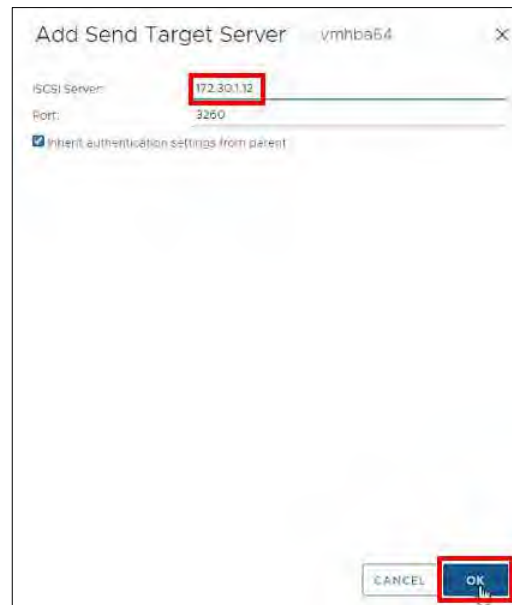


Figure 239. Enter iSCSI Server.

Steps / Screenshots

4. Click **Rescan Storage.**

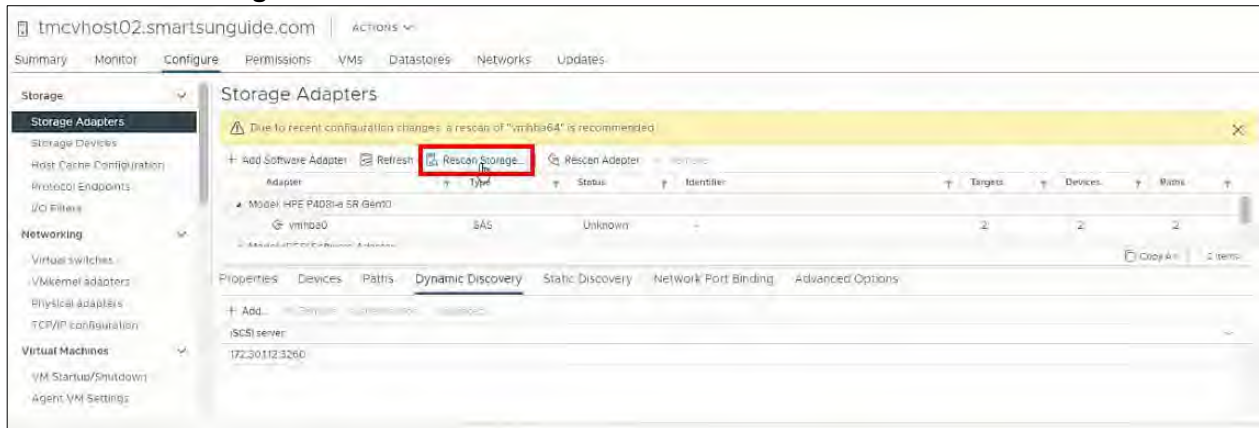


Figure 240. Rescan Storage.

5. Click **OK.**



Figure 241. Scan for New Storage Devices and Scan for New VMFS Volumes

6. In the RTMC-PowerStoreSAN,
- Click **Compute**,
 - Click **Hosts & Host Groups**.

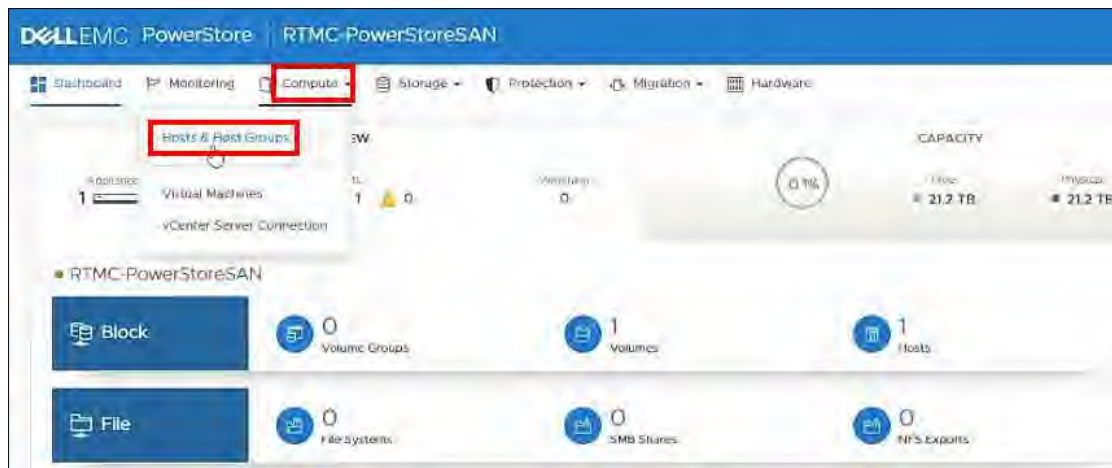


Figure 242. RTMC-PowerStoreSAN – Compute – Hosts & Host Groups.

Steps / Screenshots

7. Click **ADD HOST**.



Figure 243. Add Host.

8.
 - Enter the **Host Friendly Name**,
 - Click the down arrow under **Operating System**,
 - Select **ESXi**,
 - Click **NEXT**.

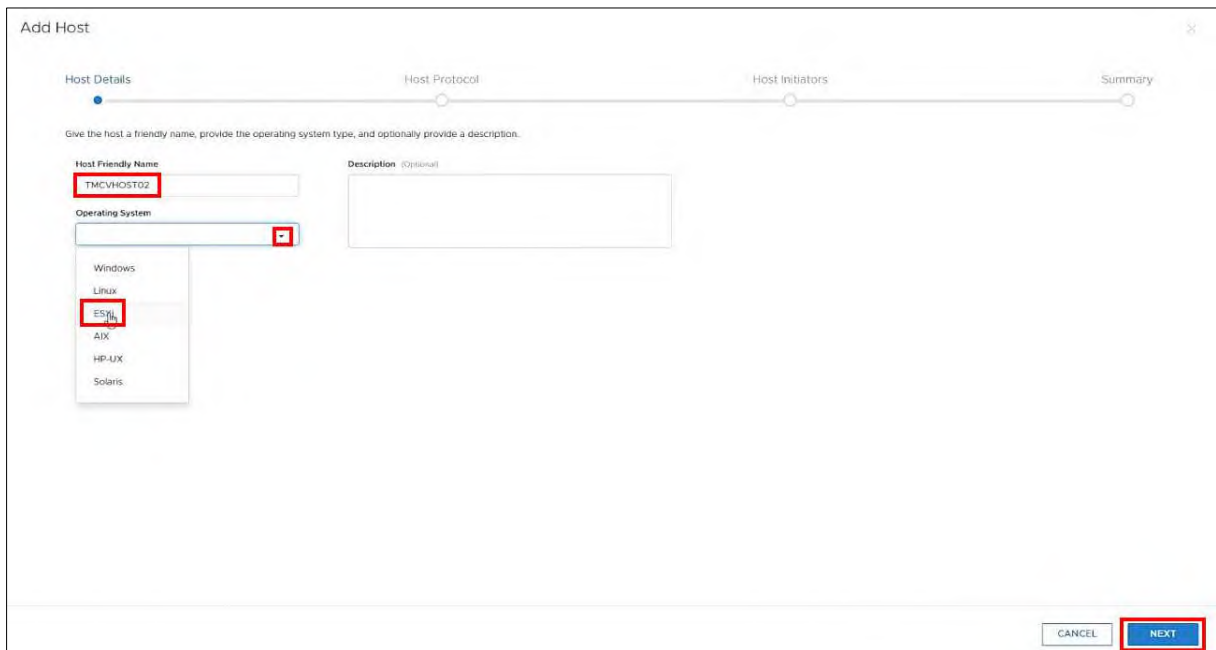


Figure 244. Host Friendly Name and Operating System

Steps / Screenshots

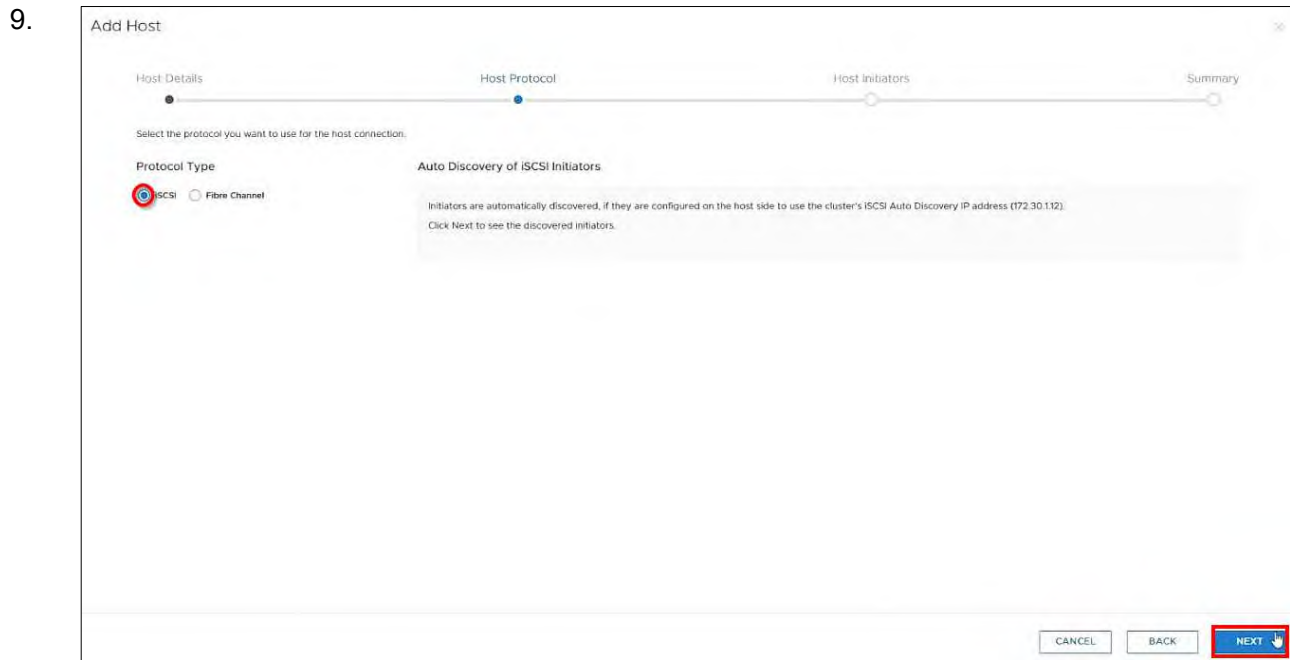


Figure 245. Protocol Type

10. – Select **iSCSI** and Click **NEXT**.
- Check the box next to **iqn...** and
 - Click **NEXT**.

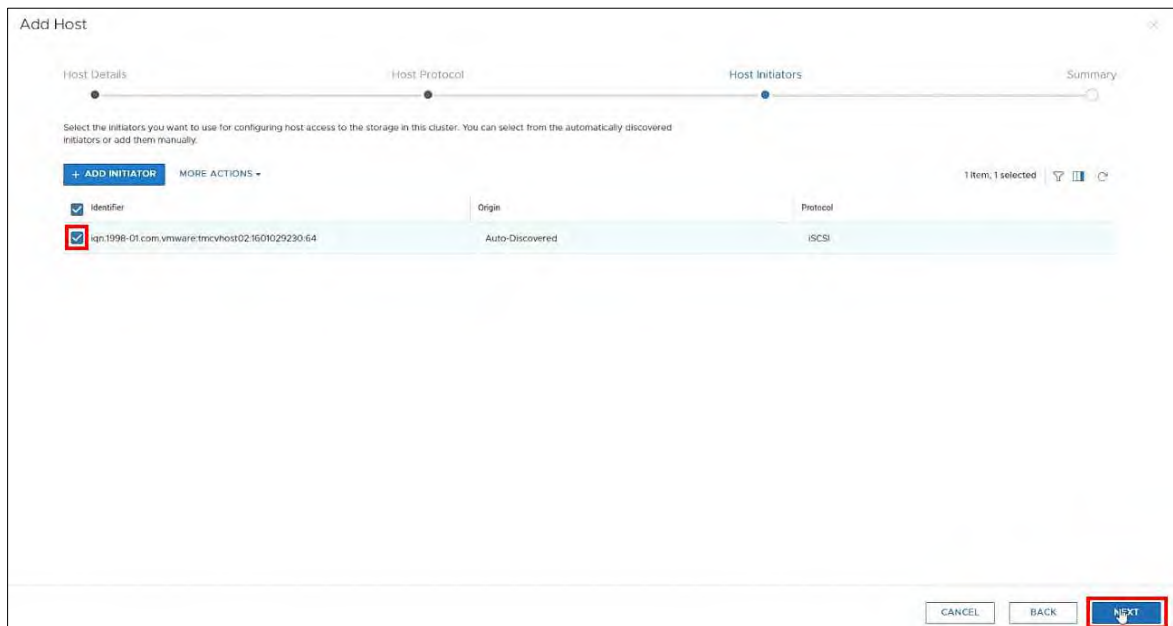


Figure 246. Select Identifier.

Steps / Screenshots

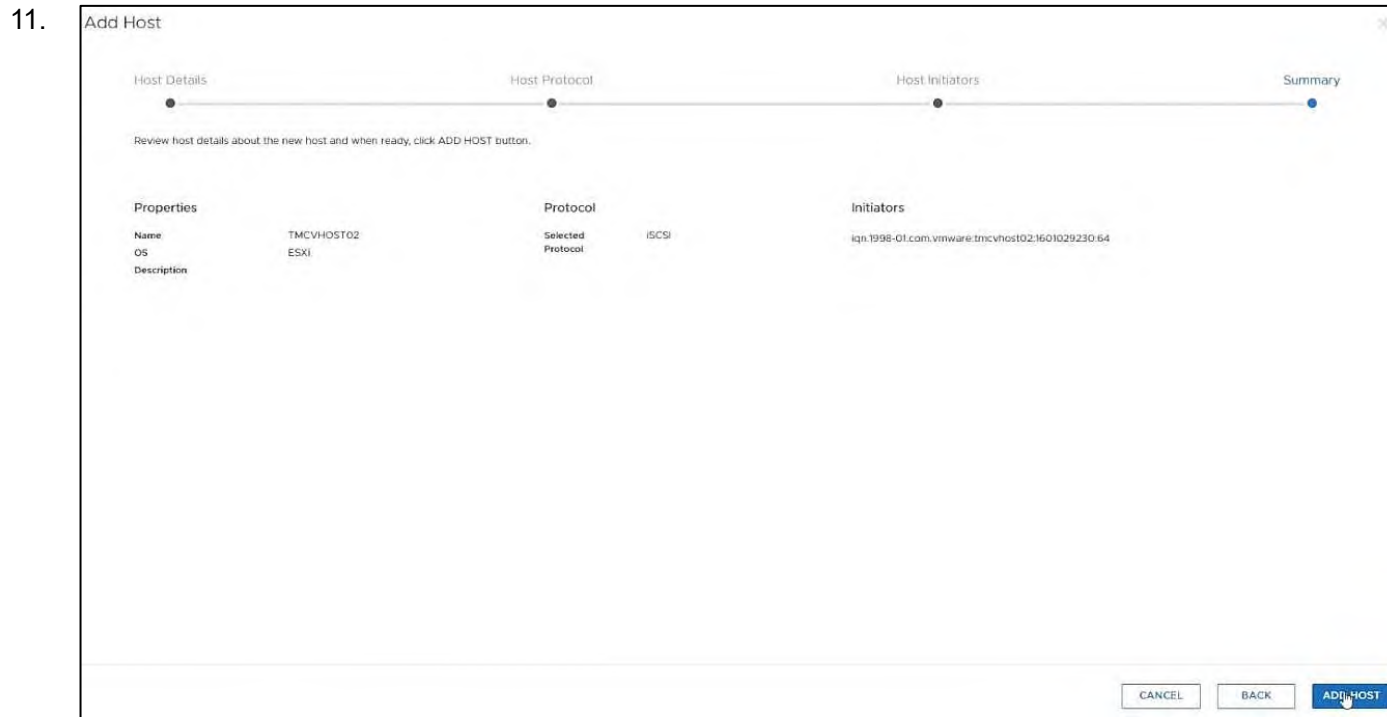


Figure 247. Add Host

12. – Click **ADD HOST**.
- Check the box next to **TMCVHOST**
 - Click **ADD HOST**.



Figure 248. Add Host.

Steps / Screenshots

- 13. – Click **ADD HOST**.

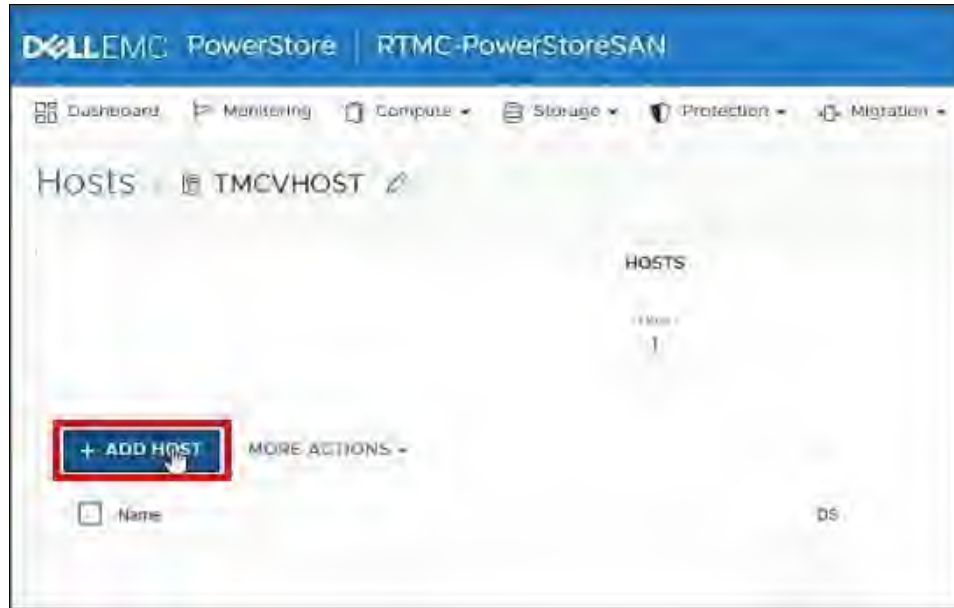


Figure 249. Add Host

- 14. – Check the box next to **TMCVHOST02**
- Click **ADD**.

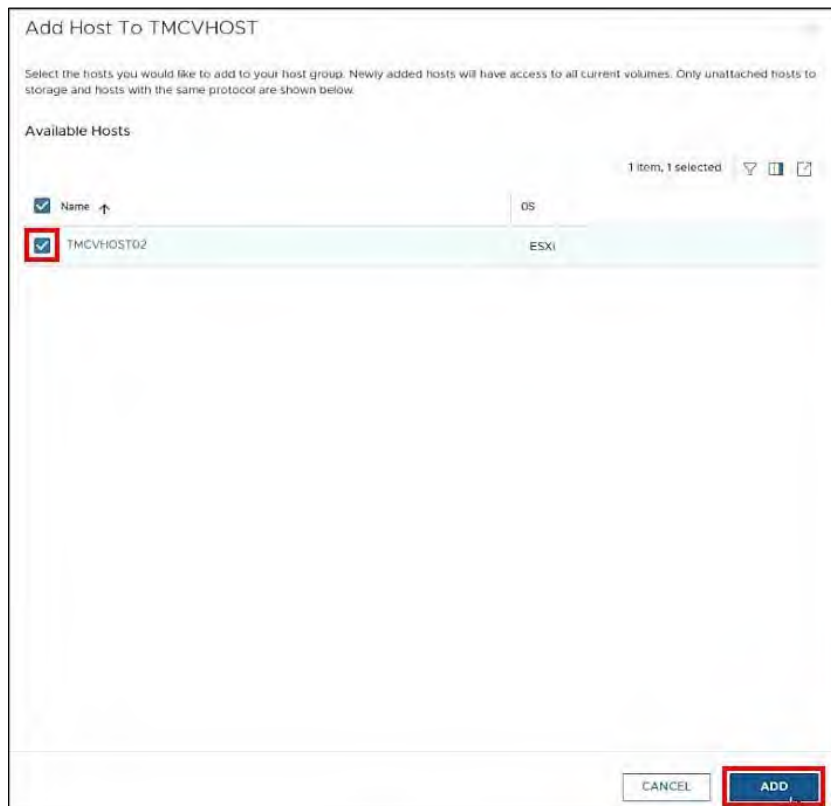


Figure 250. Add Host to TMCVHOST

Steps / Screenshots

- 15. – Click **Storage**
- Click **Volumes**.

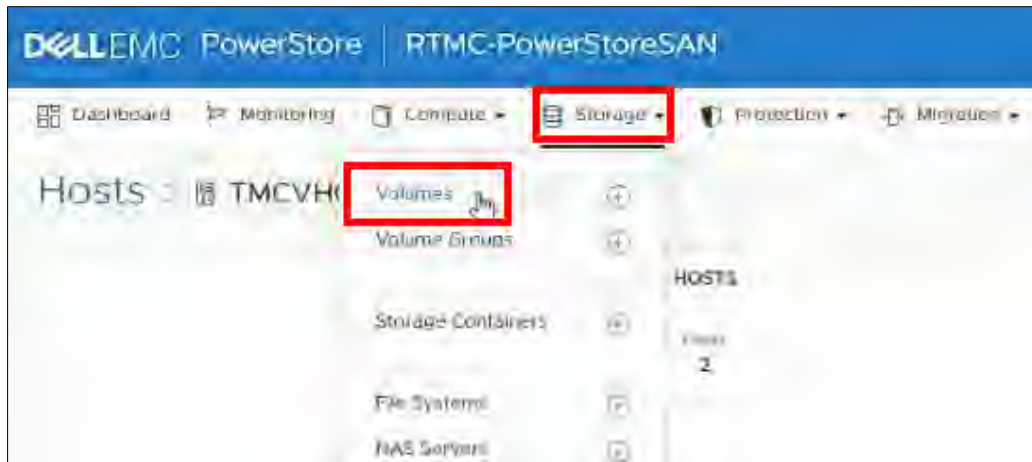


Figure 251. Storage > Volumes.

- 16. – (1) Check the box next to **test**,
- (2) Click MORE ACTIONS,
- (3) Click **Map**.

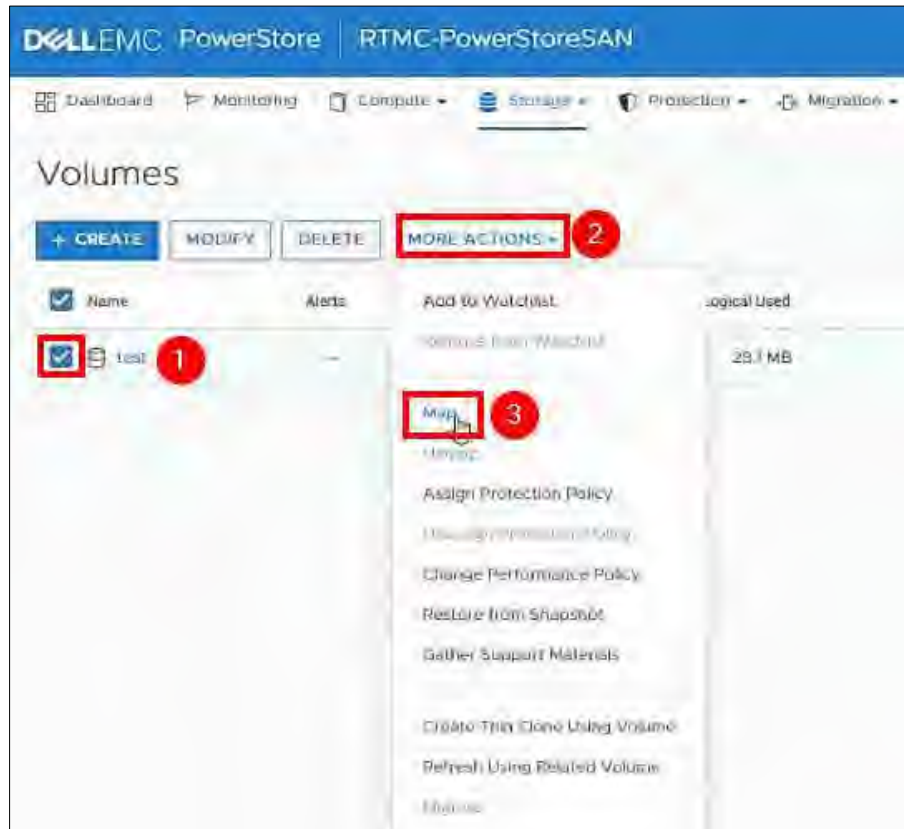


Figure 252. Storage > Volumes > Test > More Actions > Map

Steps / Screenshots

17. – Check the box next to **TMCVHOST**
- Click **APPLY**.

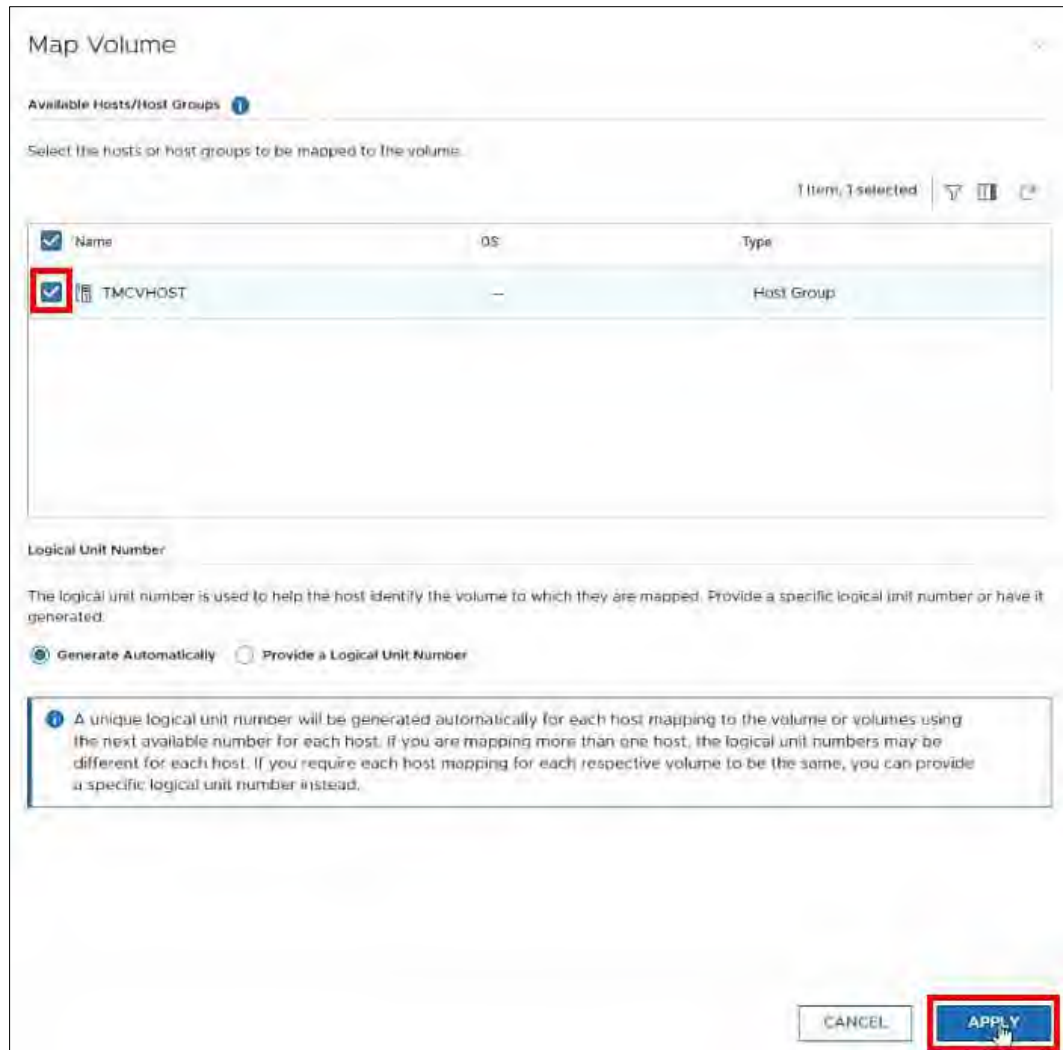


Figure 253. Map Volume

18. – Go back to vSphere,
 - (1) Click hosts and clusters,
 - (2) Click the down arrow next to **TMC Cluster**,
 - (3) Click **tmcvhost02**,
 - (4) Click **Configure**,
 - (5) Click Storage Adapters,
 - (6) Click Rescan Storage.

Steps / Screenshots

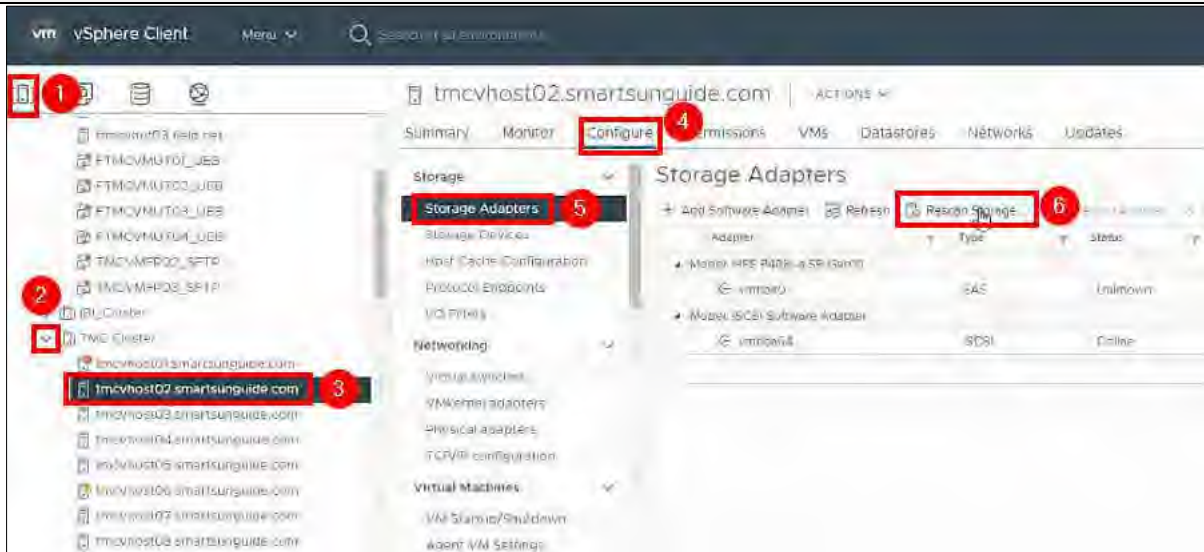


Figure 254. Rescan Storage

19. – Click **OK**.



Figure 255. Rescan Storage

20. – Click **Datastores** and verify that the **test** datastore appears.



Figure 256. Datastores > Test.

Steps / Screenshots

21.
 - (1) Click **storage**,
 - (2) Click the down arrow next to **TMC**,
 - (3) Click **test**,
 - (4) Click **Configure**,
 - (5) Click **Connectivity and Multipathing**,
 - (6) Select **tmcvhost02**,
 - (7) Verify that the **Path Selection Policy** is set to **Round Robin (VMware)**.

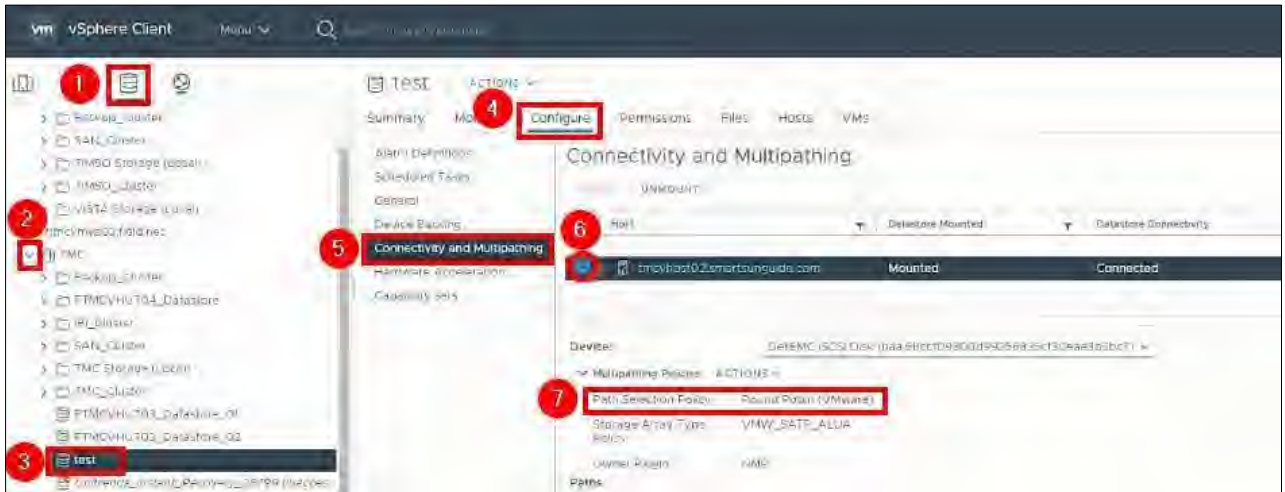


Figure 257. Path Selection Policy - Round Robin VMware

22. Repeat the following procedures for all other TMC hosts:

Add VMkernel Adapters to the Hosts - TMC_SAN_41_iSCSI1
 Add VMkernel Adapters to the Hosts - TMC_SAN_41_iSCSI2
 Add Storage Adapters to the Hosts

CREATE NEW STORAGE VOLUMES, CONTENT LIBRARIES, DATASTORE

Create a New Storage Volume – ContentLibraryTMC

Steps / Screenshots

1. In the **RTMC-PowerStoreSAN**,
 - Click **Storage** and
 - Select **Volumes**

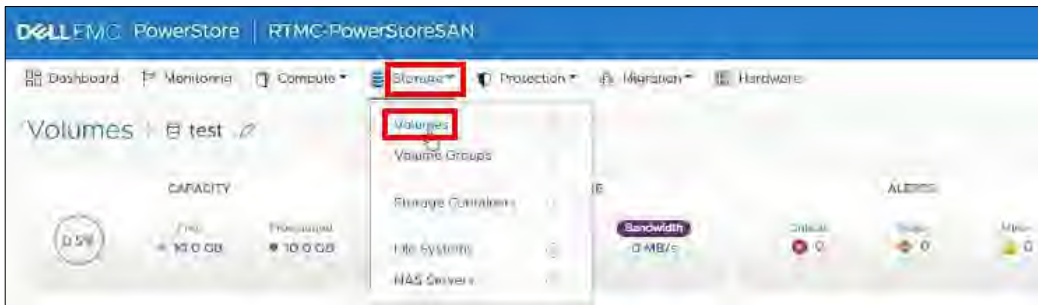


Figure 258. Storage > Volumes.

2. Click **Create**.



Figure 259. Create Storage Volume.

3.
 - Enter the **volume name** (ContentLibrary_TMC),
 - Change the **size** to 500 GB,
 - Click **NEXT**.

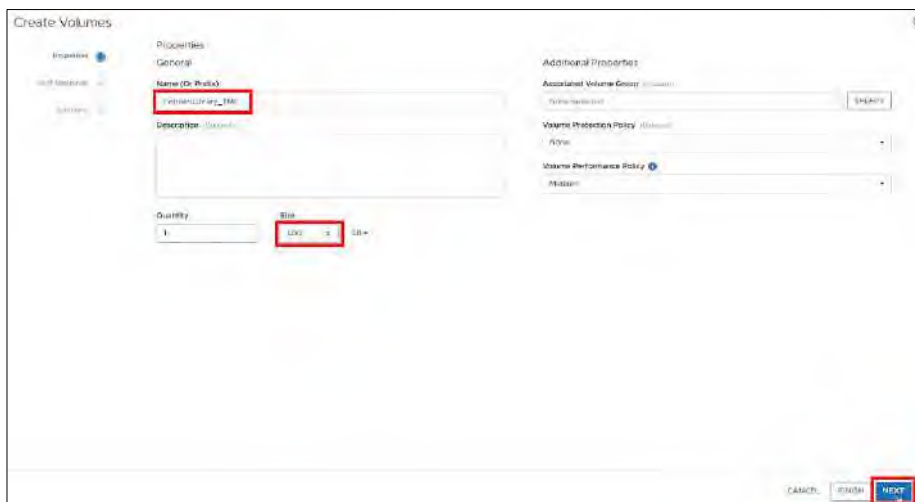


Figure 260. Properties.

Steps / Screenshots

- 4. – Check the box next to **TMCVHOST** and
- Click **NEXT**.

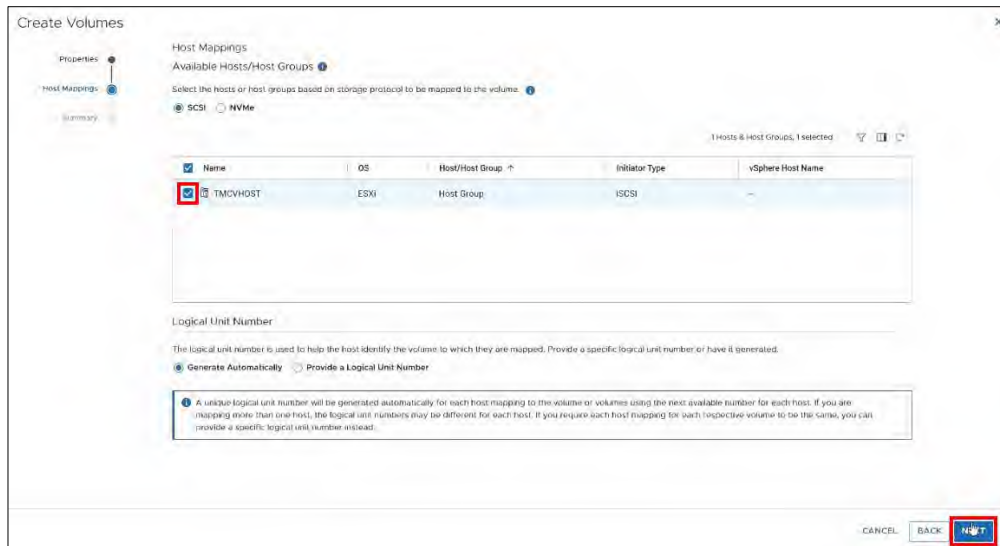


Figure 261. Host Mappings.

- 5. Click **CREATE**.

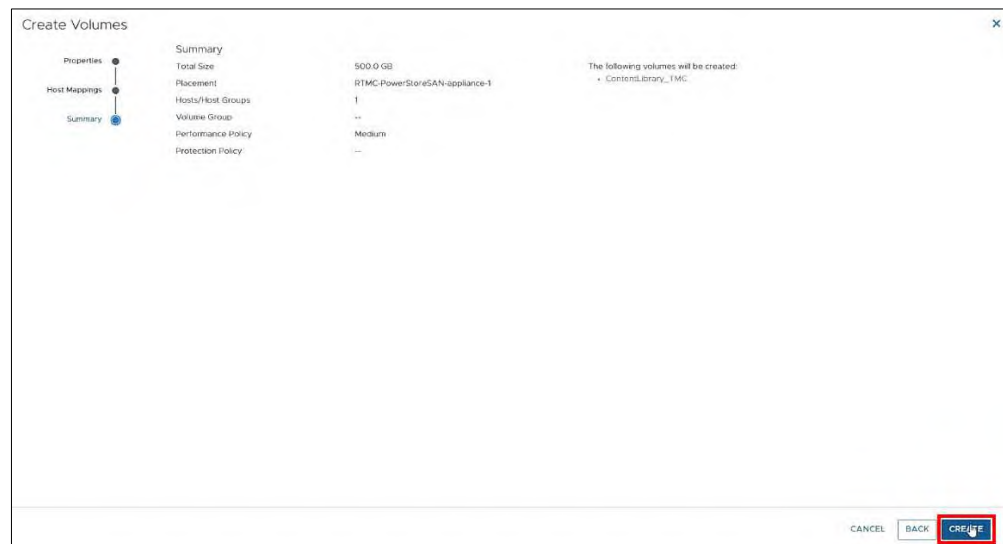


Figure 262. Summary.

Add a New Host

1. In the **RTMC-PowerStoreSAN**,
 - Click Compute,
 - Click Hosts & Host Groups.

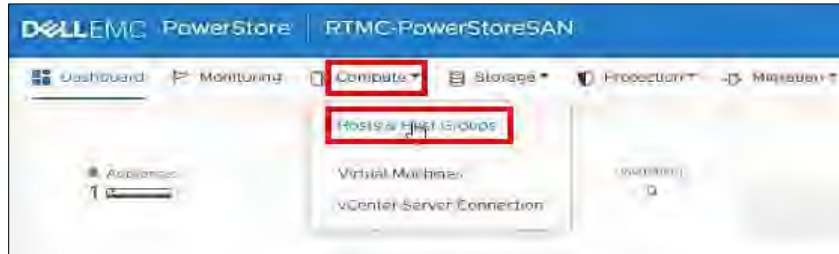


Figure 263. Compute > Hosts & Host Groups.

2. Click **ADD HOST**.



Figure 264. Add Host.

Enter Host Details

Steps / Screenshots

1.
 - Enter the Host Friendly Name, Operating System, Description,
 - Click **NEXT**.

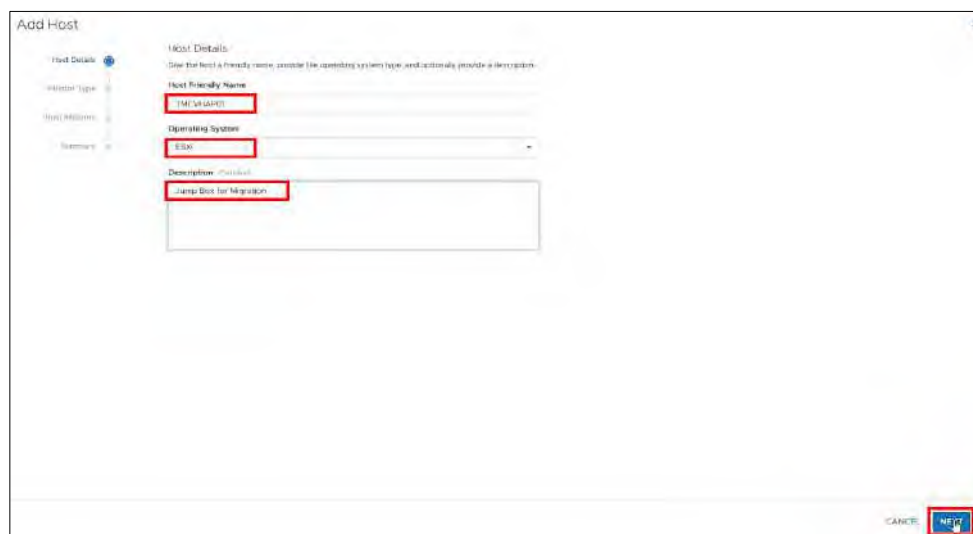


Figure 265. Host Details

Steps / Screenshots

2.
 - Select **iSCSI** and
 - Click **NEXT**.



Figure 266. Initiator Type.

3.
 - Check the box next to **iqn...**
 - Click **NEXT**.

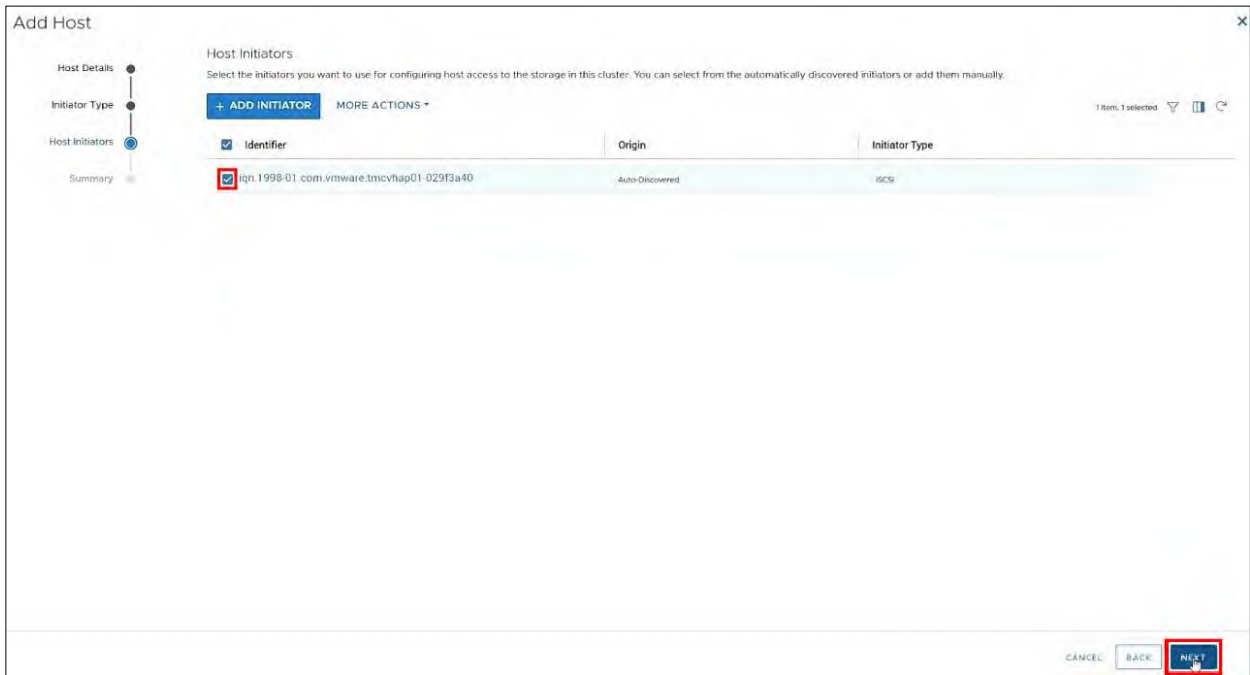


Figure 267. Select Identifier

Steps / Screenshots

4. – Click **ADD HOST**.



Figure 268. Add Host.

Create a New Storage Volume – VMDatastore_TMC

Steps / Screenshots

1. In the RTMC-PowerStoreSAN,
 - Click Storage,
 - Select **Volumes**.

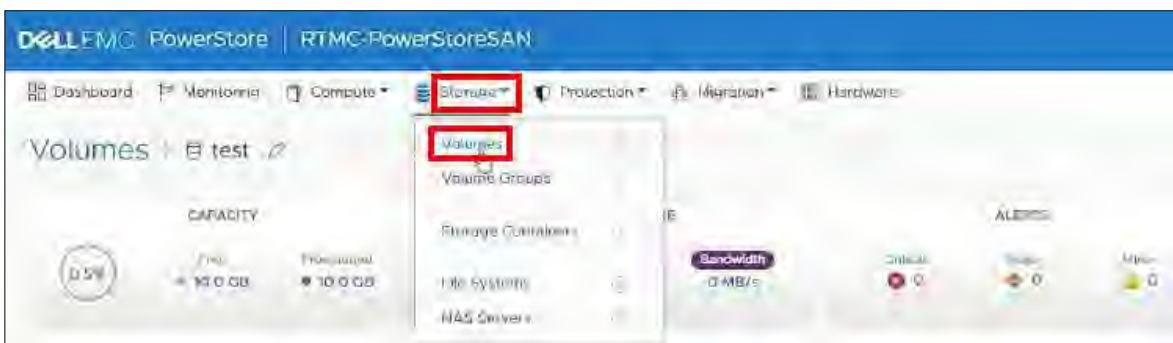


Figure 269. Storage > Volumes

2. – Click **Create**.

Steps / Screenshots



Figure 270. Create Storage Volume

3.
 - Enter the **volume name** (VMDatastore_TMC),
 - Change the **size** to 10 TB,
 - Click **NEXT**.

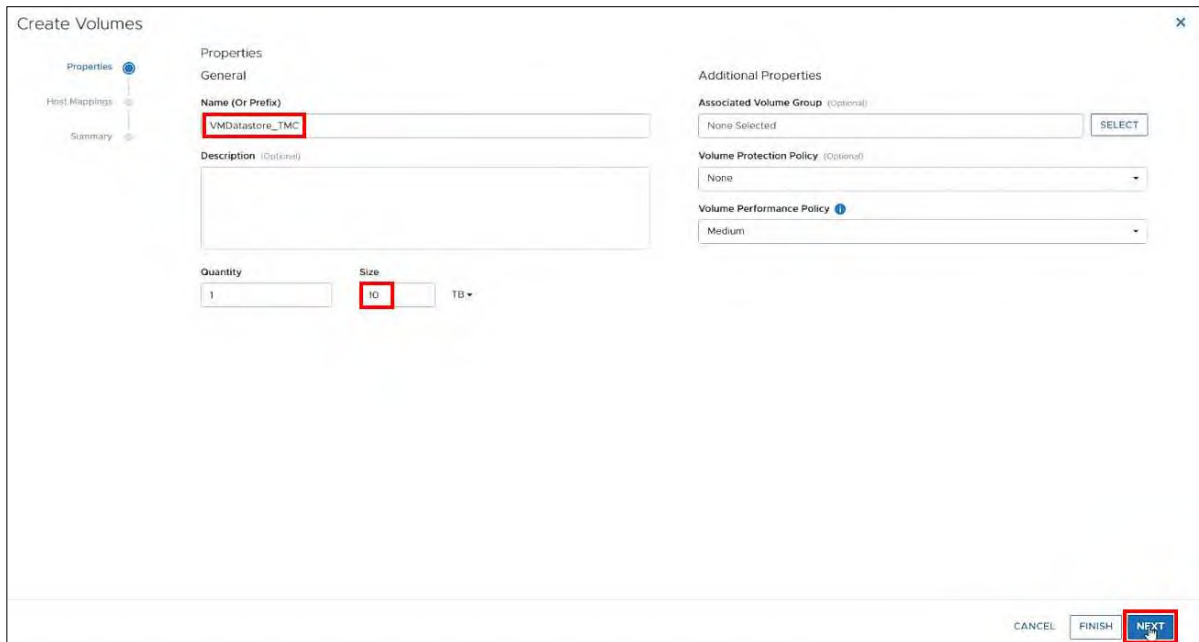


Figure 271. Properties.

4.
 - Check the boxes next to **TMCVHOST** and **TMCVHAP01**
 - Click **NEXT**.

Steps / Screenshots

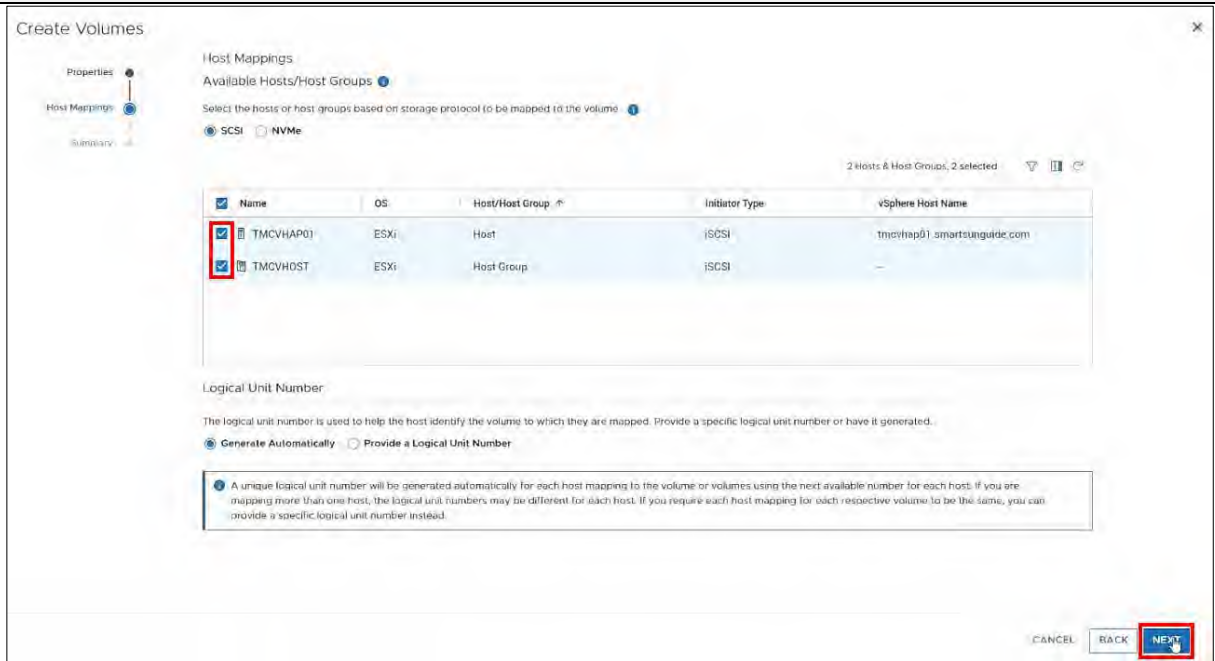


Figure 272. Host Mappings.

5. Click **Create**.



Figure 273. Summary

6.
 - Click **hosts and clusters**,
 - Right-click **TMC Cluster**,
 - Click **Storage**,
 - Click **Rescan Storage**.

Steps / Screenshots

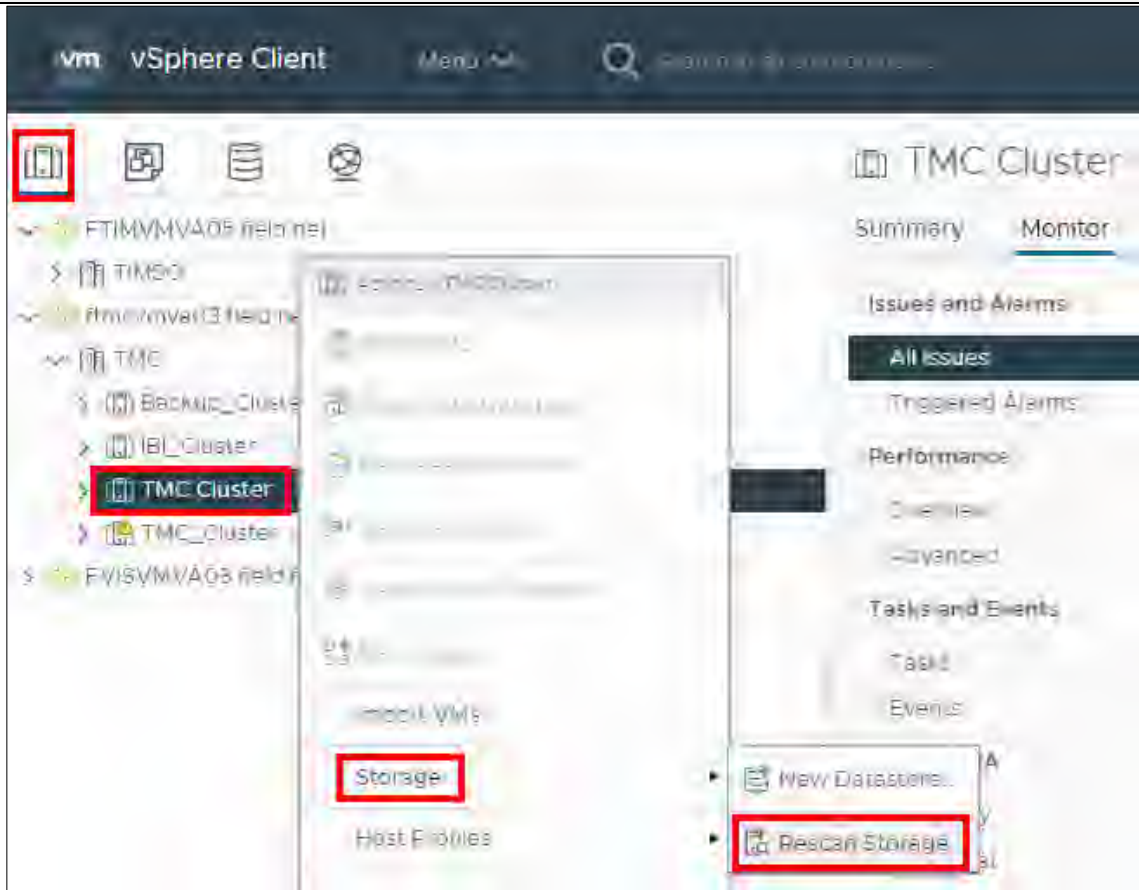


Figure 274. TMC Cluster > Rescan Storage

7. Click **OK**.



Figure 275. Rescan Storage

Create a New Storage Volume Group

- In the RTMC-PowerStoreSAN,
 - Click **Storage** and
 - select Volume Groups.

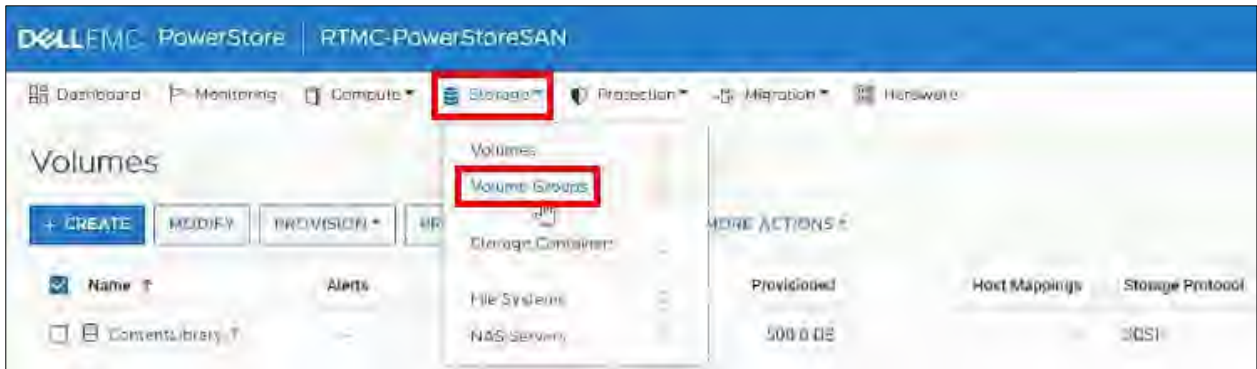


Figure 276. Storage > Volume Groups.

- Click **Create**.



Figure 277. Create Volume Group.

- Enter the **volume group name** (ProductionDatastores)
 - Click **CREATE**.

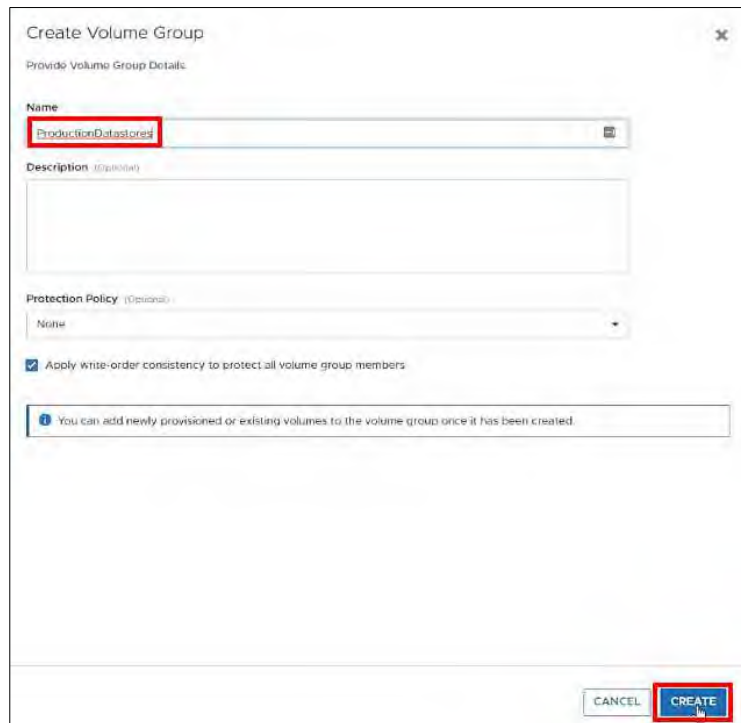


Figure 278. Volume Group Details.

Create a New Storage Folder

1. – (1) In vSphere → Click Storage,
- (2) Right-Click **TMC**,
- (3) Select **New Folder**,
- (4) Click New Storage Folder.

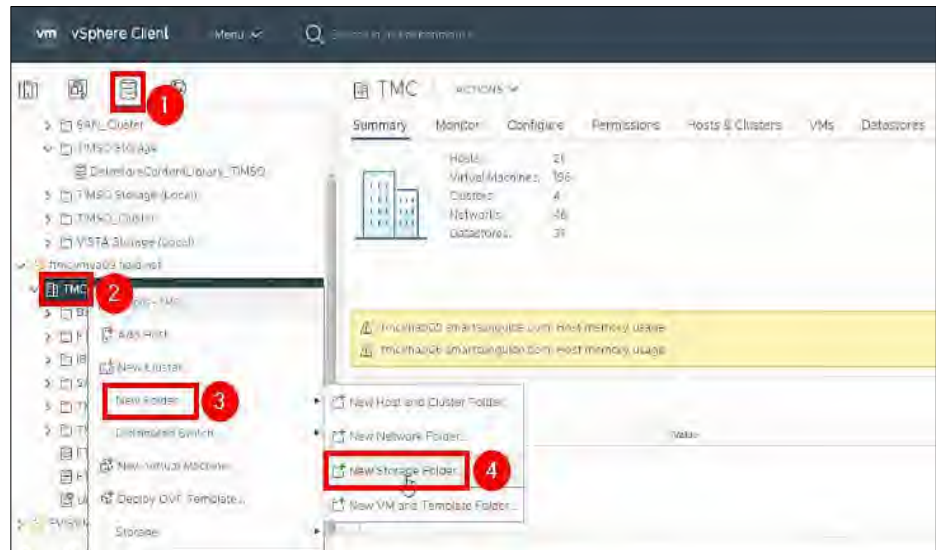


Figure 279. New Storage Folder.

2. – Enter the new **storage folder name** (TMC Storage)
- Click **OK**.



Figure 280. New Storage Folder Name.

Create a New Datastore- DatastoreContentLibrary_TMC

Steps / Screenshots

1.
 - Click **storage**,
 - Right-Click **TMC Storage**,
 - Click **New Datastore**.

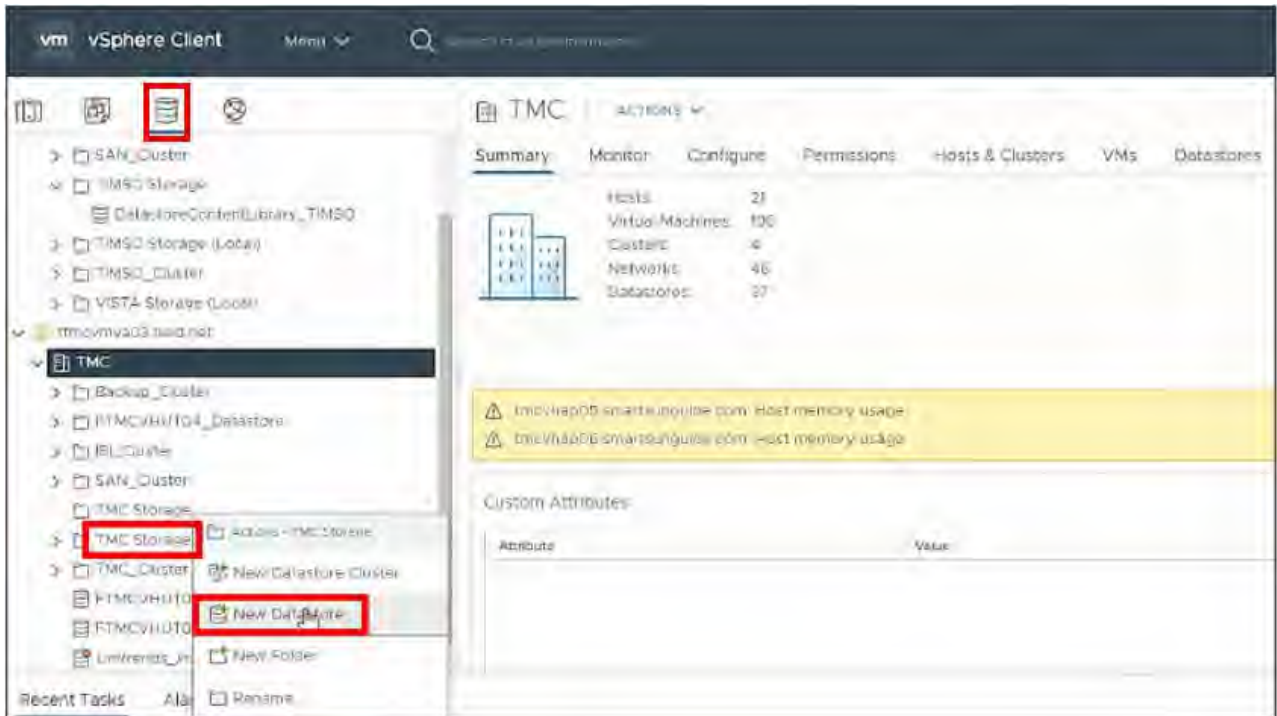


Figure 281. New Datastore.

2. Click **NEXT**.

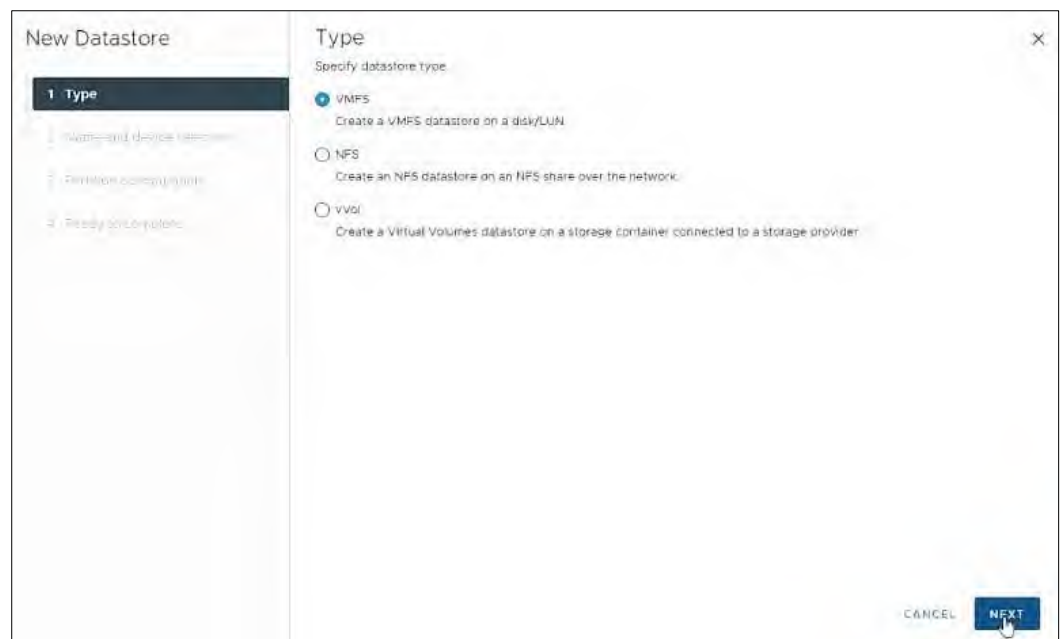


Figure 282. Datastore Type.

Steps / Screenshots

3.
 - Enter the new **datastore name** (DatastoreContentLibrary_TMC),
 - Select a **host**,
 - Click the circle next to **DellEMC iSCSI Disk**,
 - Click **NEXT**.

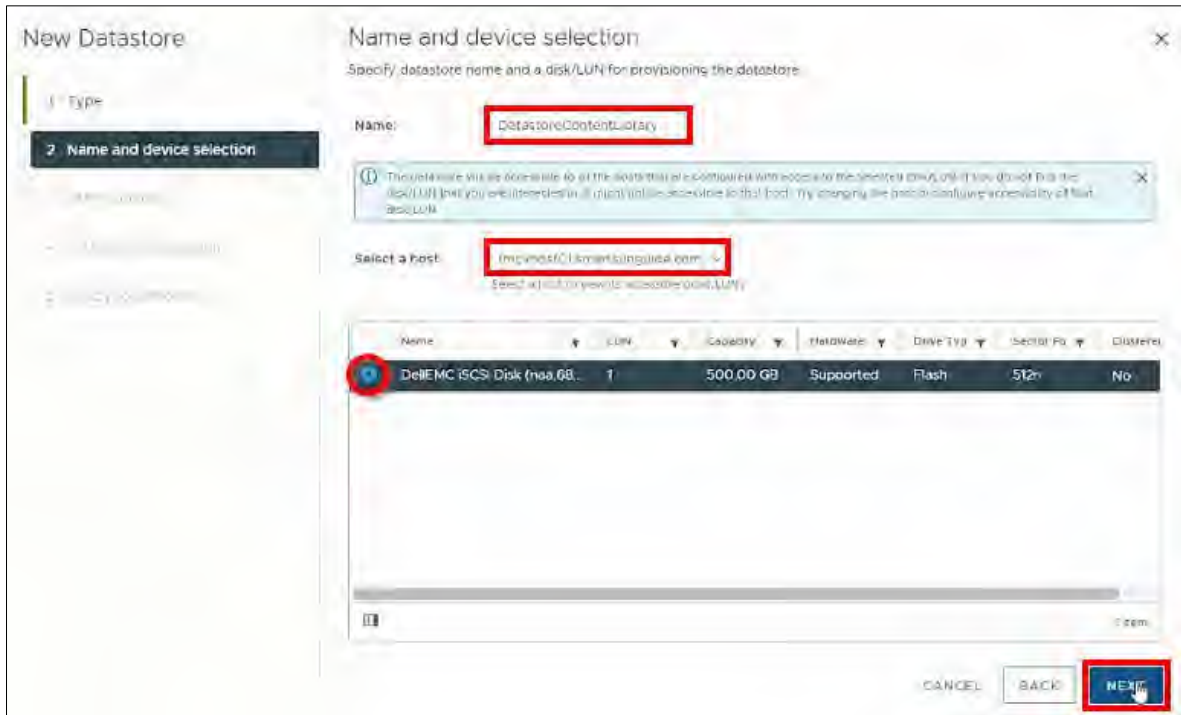


Figure 283. Name and Device Selection.

4. Click **NEXT**.



Figure 284. VMFS Version.

Steps / Screenshots

5. Click **NEXT**.

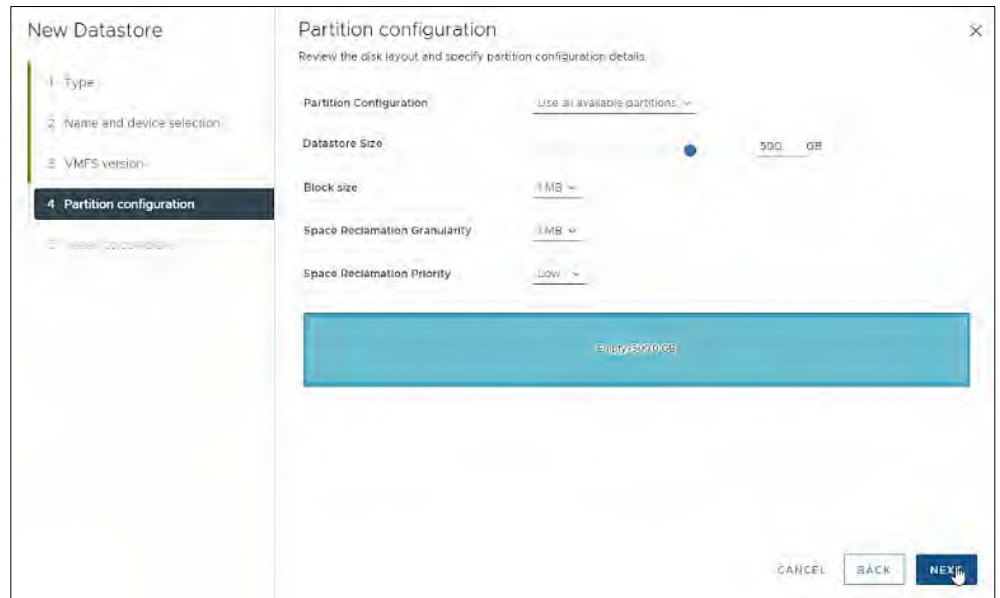


Figure 285. Partition Configuration.

6. Click **FINISH**.

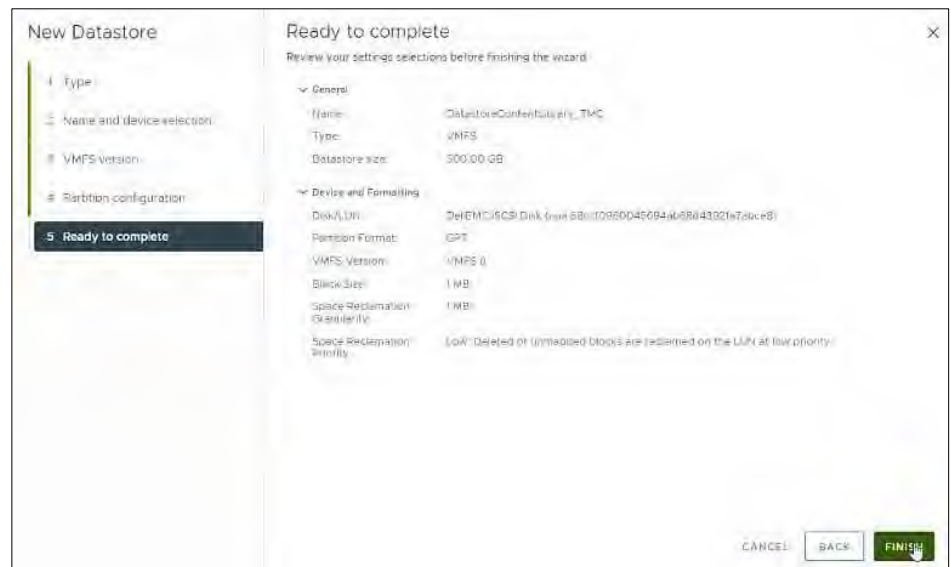


Figure 286. Ready to Complete.

- 7. – Click **hosts and clusters**,
- Right-click **TMC Cluster**,
- Click **Storage**,
- Click **Rescan Storage**.

Steps / Screenshots

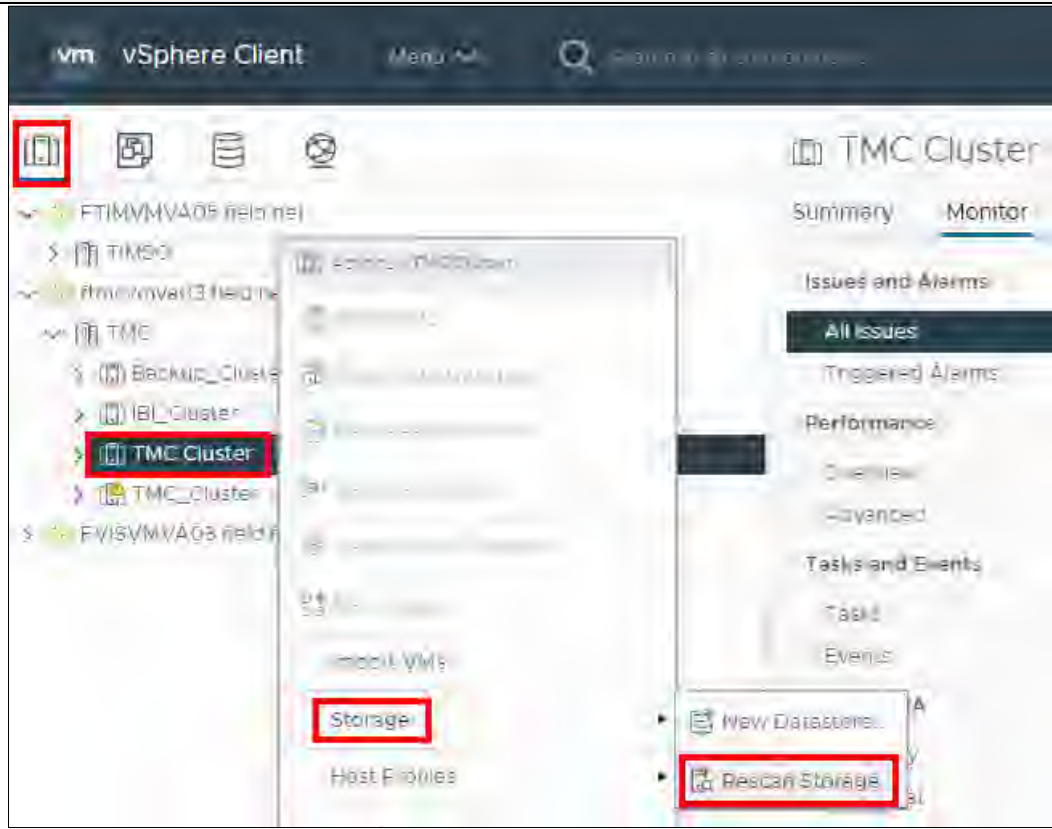


Figure 287. TMC Cluster > Rescan Storage.

8. Click **OK**.



Figure 288. Rescan Storage.

Create a New Content Library – TMC

Steps / Screenshots

1.
 - Click **Menu**
 - Select Content Libraries

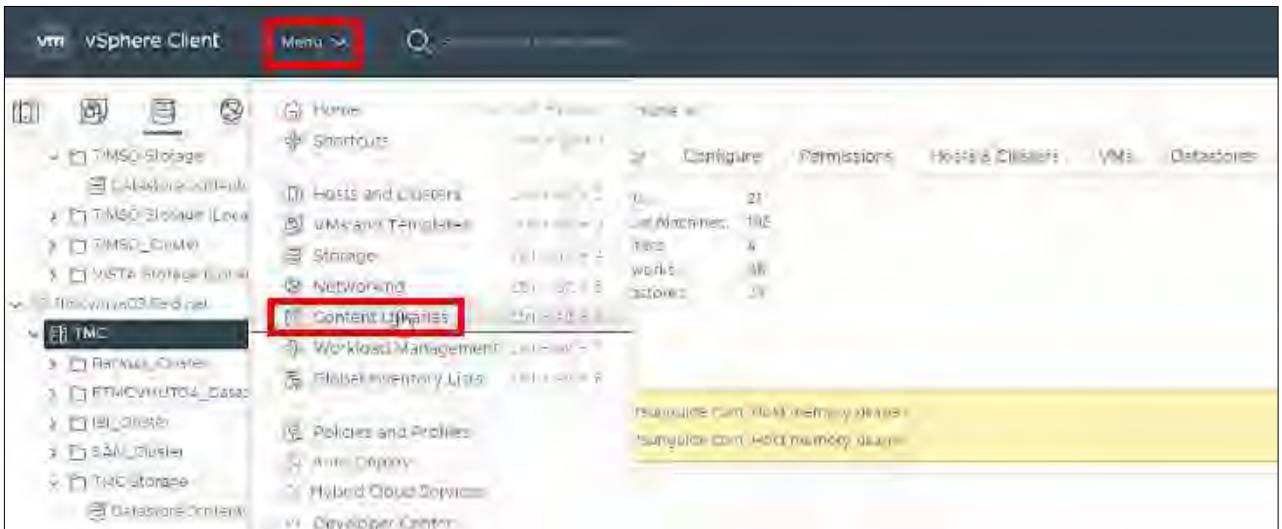


Figure 289. Menu > Content Libraries

2. Click **Create**.

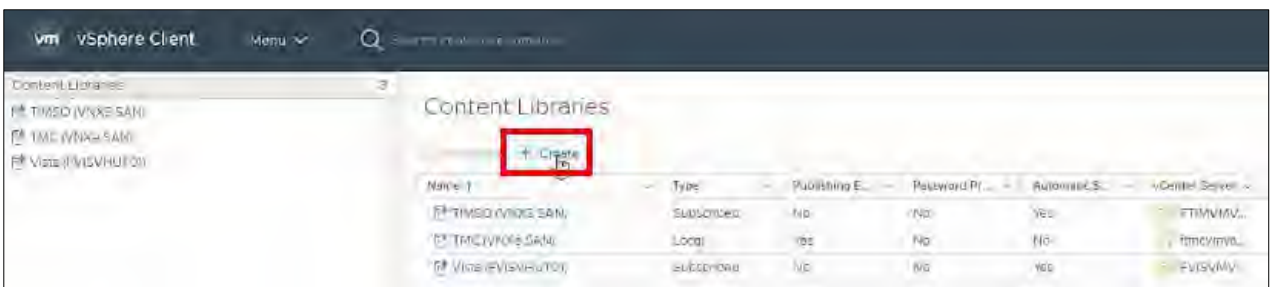


Figure 290. Create Content Library

Steps / Screenshots

3.
 - Enter the new **content library name** (TMC_ContentLibrary),
 - Select the vCenter server,
 - Click **NEXT**.

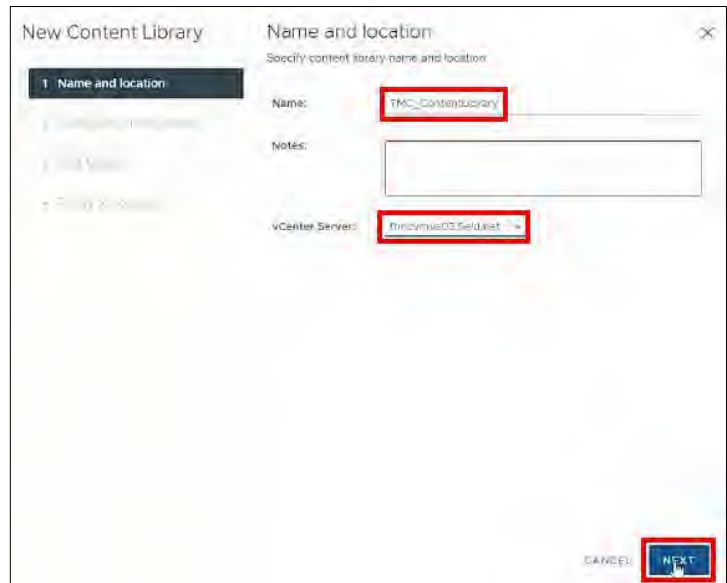


Figure 291. Name and Location.

4.
 - Check the box next to **Enable publishing**
 - Click **NEXT**.

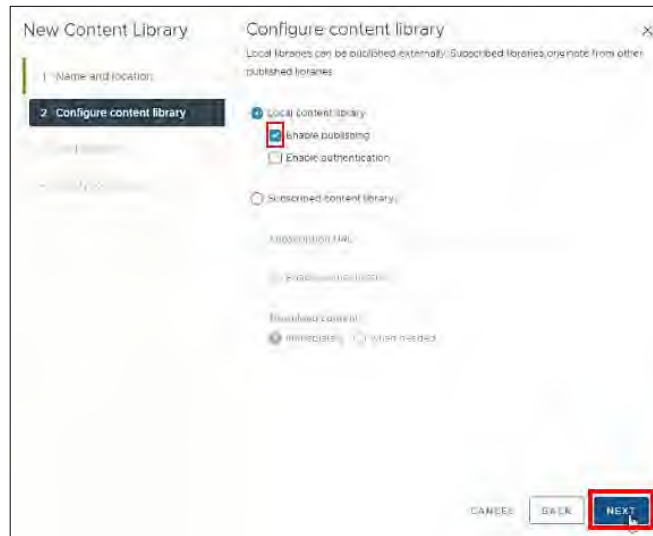


Figure 292. Configure Content Library.

Steps / Screenshots

5.
 - Scroll down,
 - Select DatastoreContentLibrary_TMC
 - Click **NEXT**.

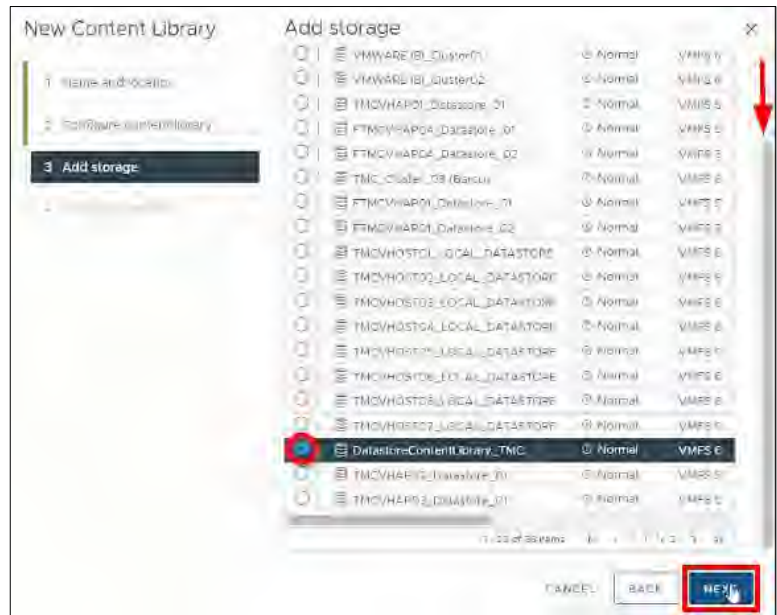


Figure 293. Add Storage.

6. Click **FINISH**.

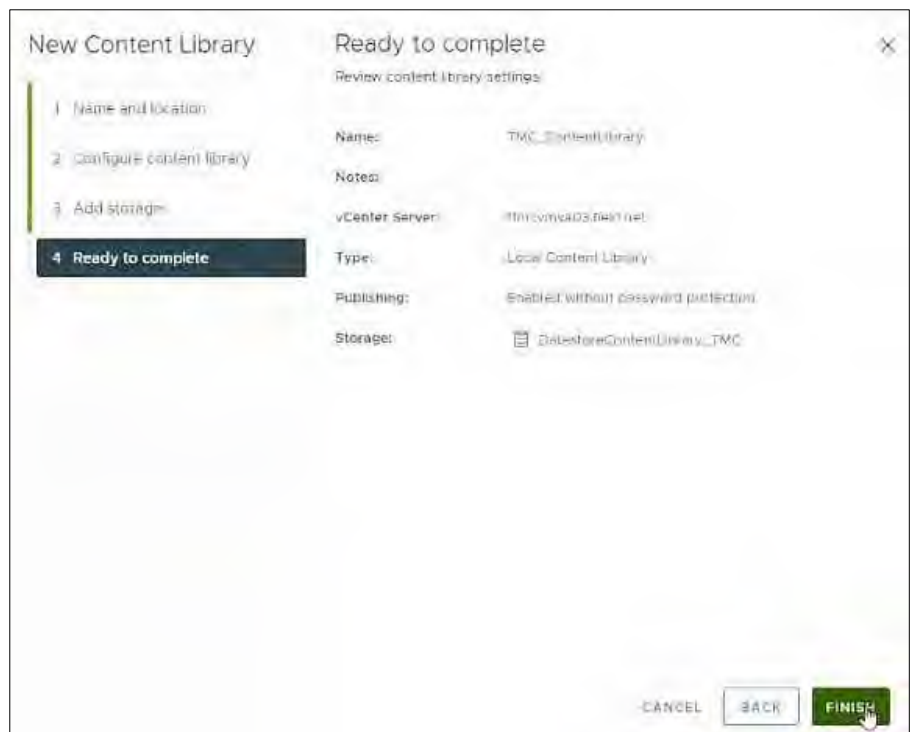


Figure 294. Ready to Complete.

7.
 - Click TMC_Content Library,
 - Click **Summary**,
 - Click **COPY LINK** to capture the subscription URL.

Steps / Screenshots

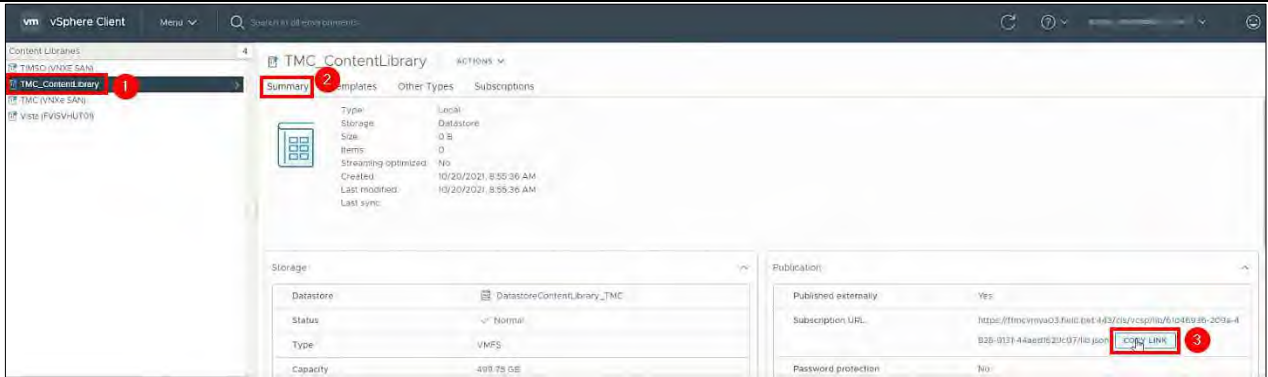


Figure 295. TMC_Content Library - Subscription URL.

Create a New Content Library – TIMSO

Steps / Screenshots

1. Click **Create**.



Figure 296. Create Content Library

2.
 - Enter the new **content library name** (TIMSO_ContentLibrary),
 - Select vCenter server,
 - Click **NEXT**.

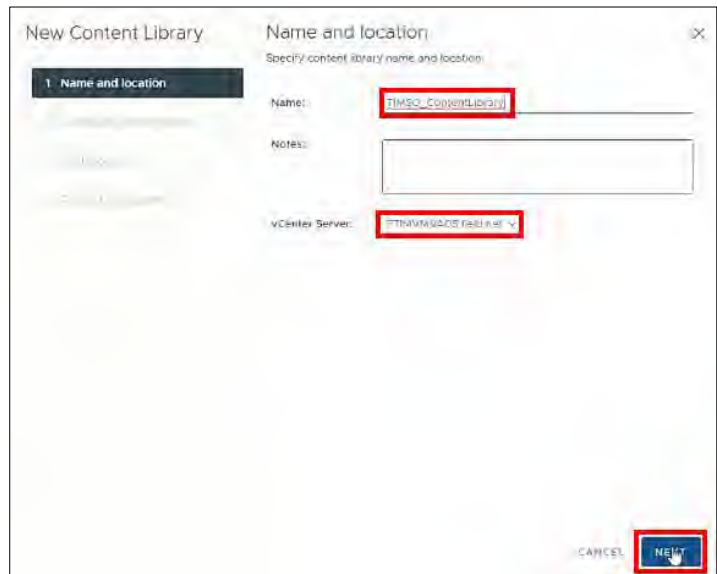


Figure 297. Name and Location.

Steps / Screenshots

3.
 - Select Subscribed content library,
 - Paste the TMC_Content Library - Subscription URL,
 - Click **NEXT**.

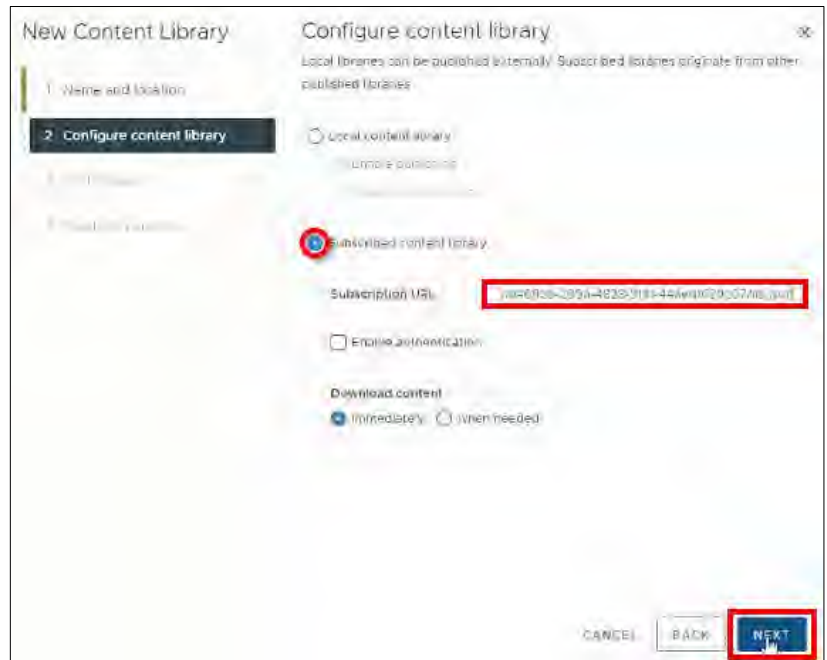


Figure 298. Configure Content Library.

4.
 - Scroll down,
 - Select **DatastoreContentLibrary_TIMSO**,
 - Click **NEXT**.

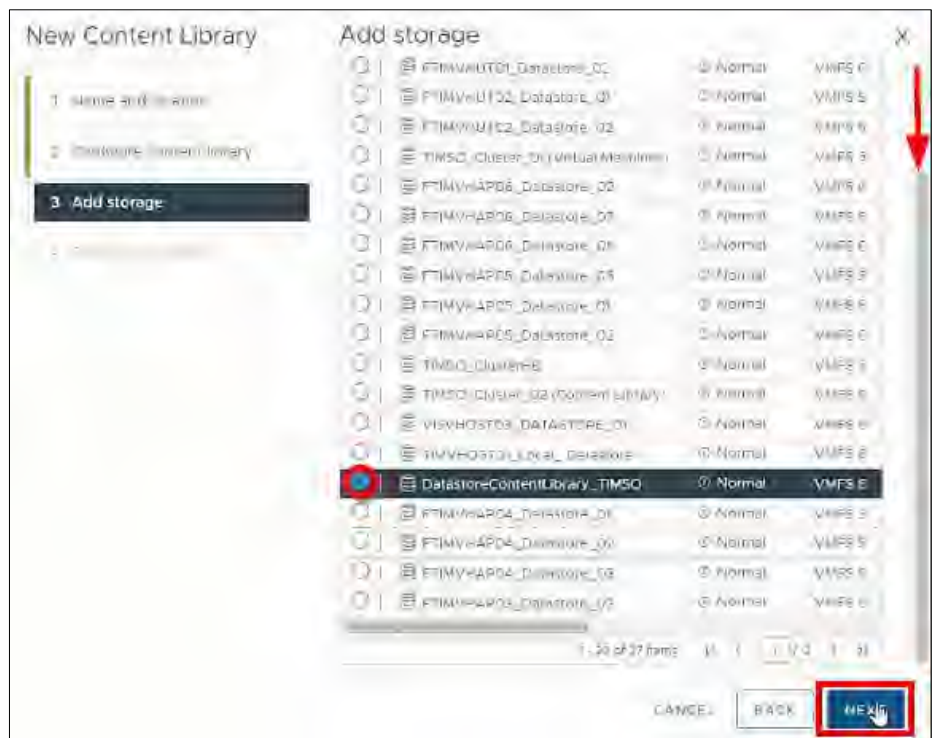


Figure 299. Add Storage.

Steps / Screenshots

5. Click **FINISH**.

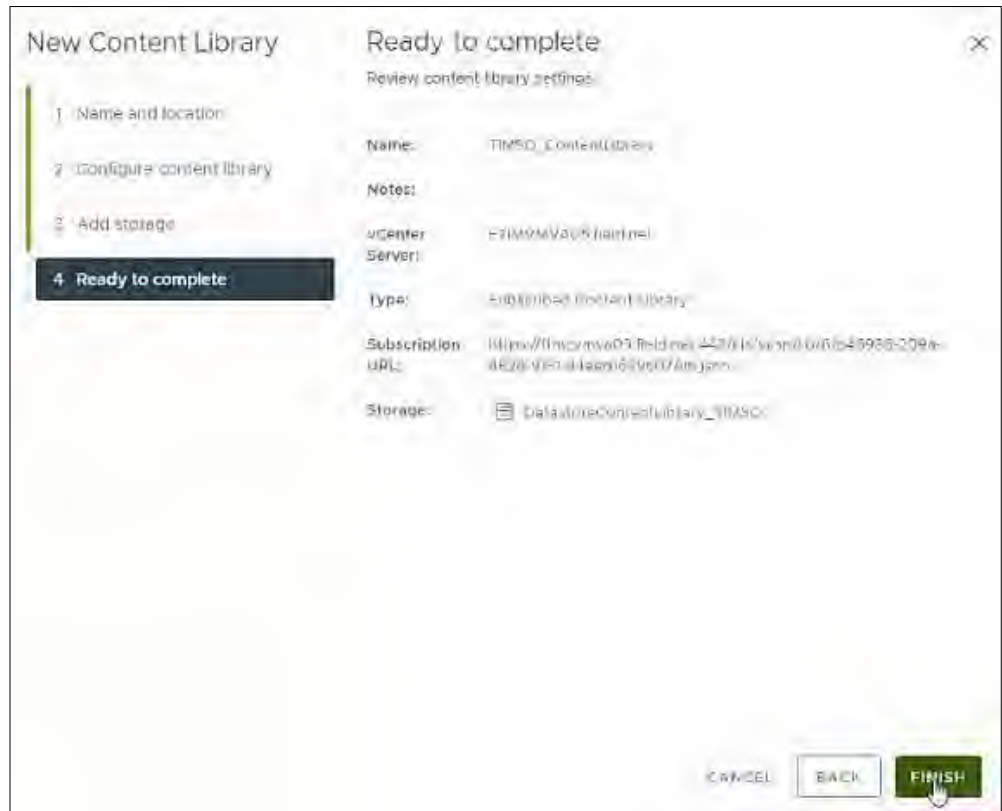


Figure 300. Ready to Complete.

Create a New Datastore – DatastoreVM_TMC

Steps / Screenshots

1.
 - Click **Storage**,
 - Right-Click **TMC Storage**,
 - Click **New Datastore**.

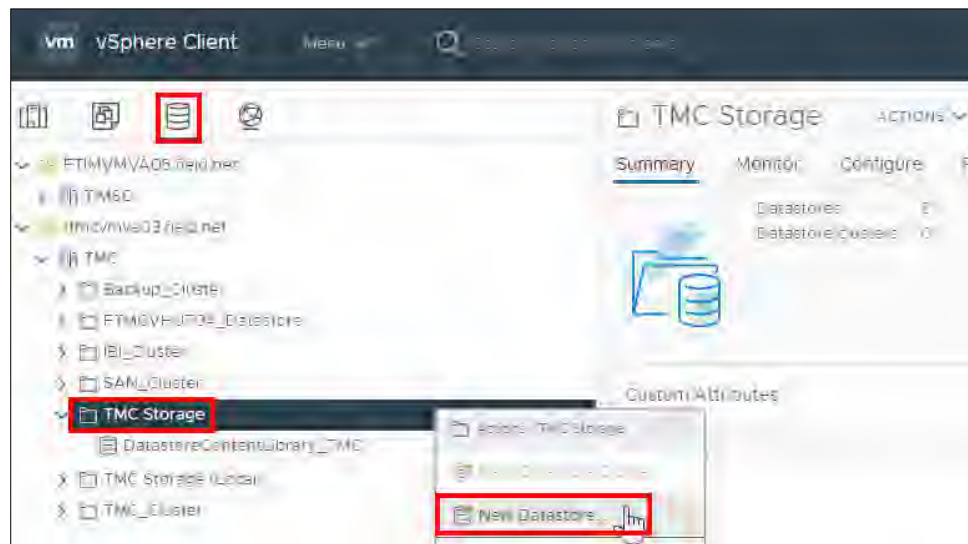


Figure 301. New Datastore.

Steps / Screenshots

2. Click **NEXT**.

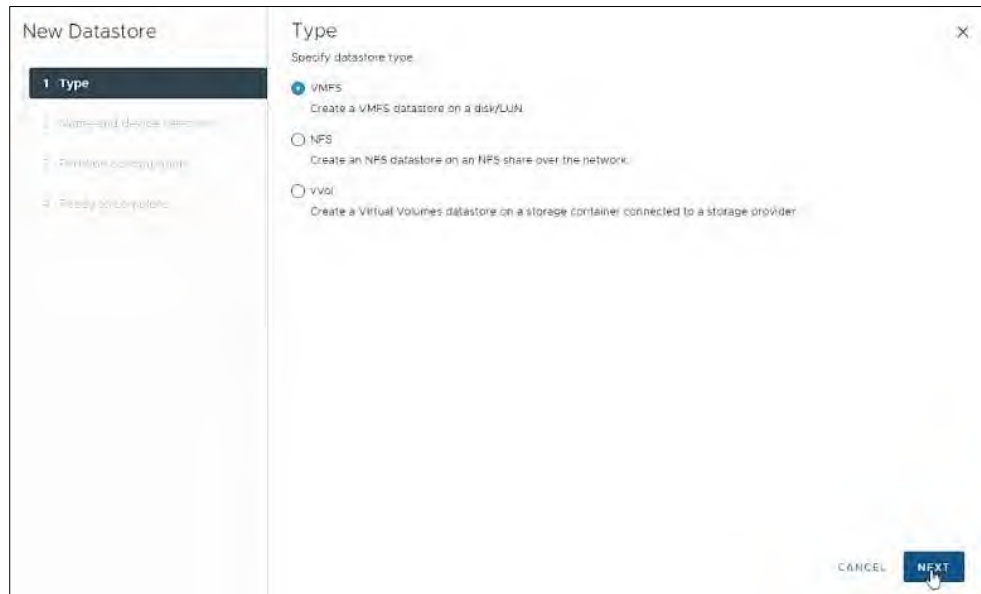


Figure 302. Datastore Type.

- 3. – Enter the new **datastore name** (DatastoreVM_TMC),
- Select a **host**,
- Click the circle next to **DellEMC iSCSI Disk**,
- Click **NEXT**.

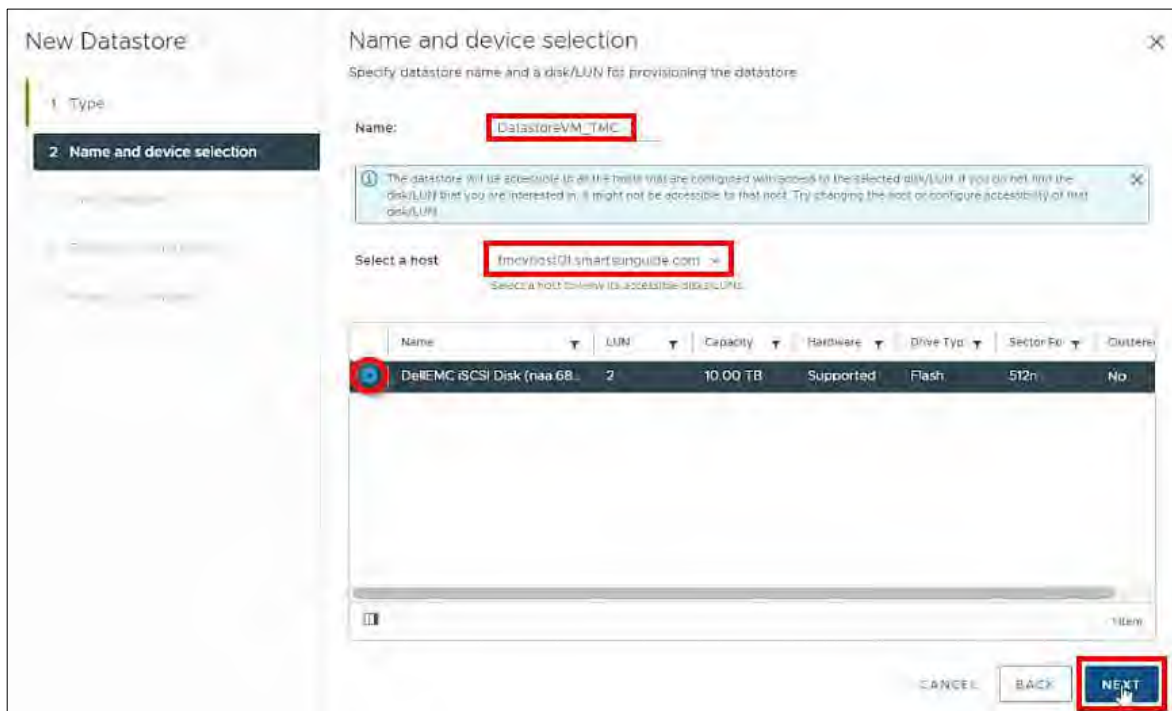


Figure 303. Name and Device Selection.

Steps / Screenshots

4. Click **NEXT**.



Figure 304. VMFS Version.

5. Click **NEXT**.

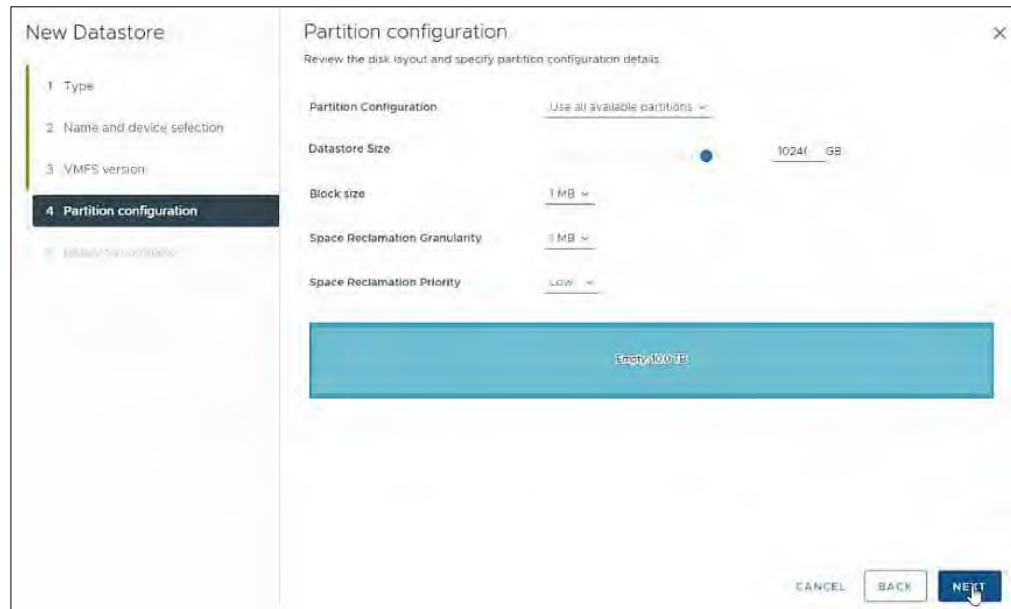


Figure 305. Partition Configuration.

Steps / Screenshots

6. Click **FINISH**.

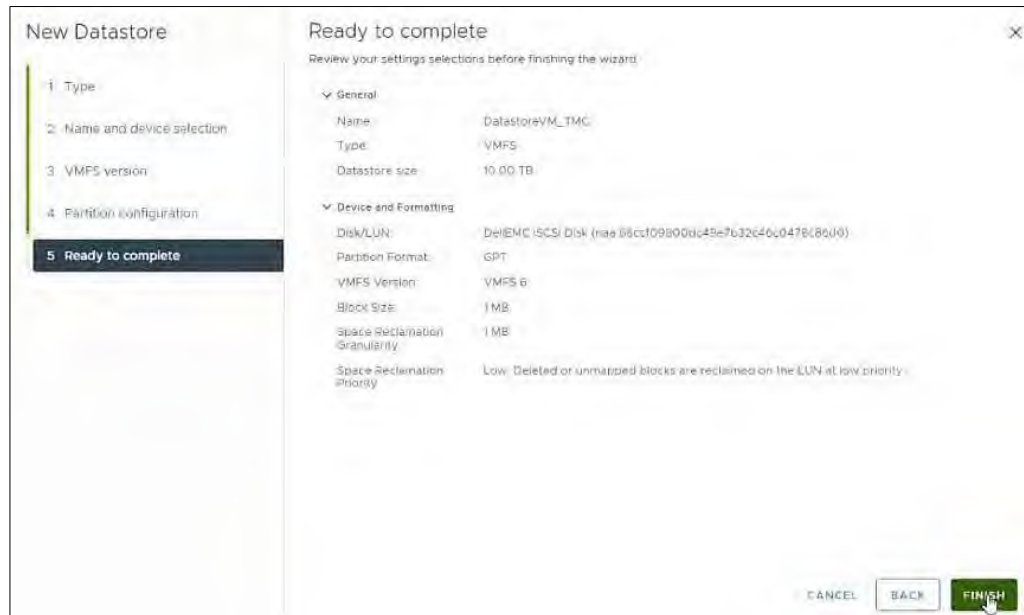


Figure 306. Ready to Complete.

- 7. – Click hosts and clusters,
- Right-Click **TMC Cluster**,
- Click **Storage**,
- Click Rescan Storage.

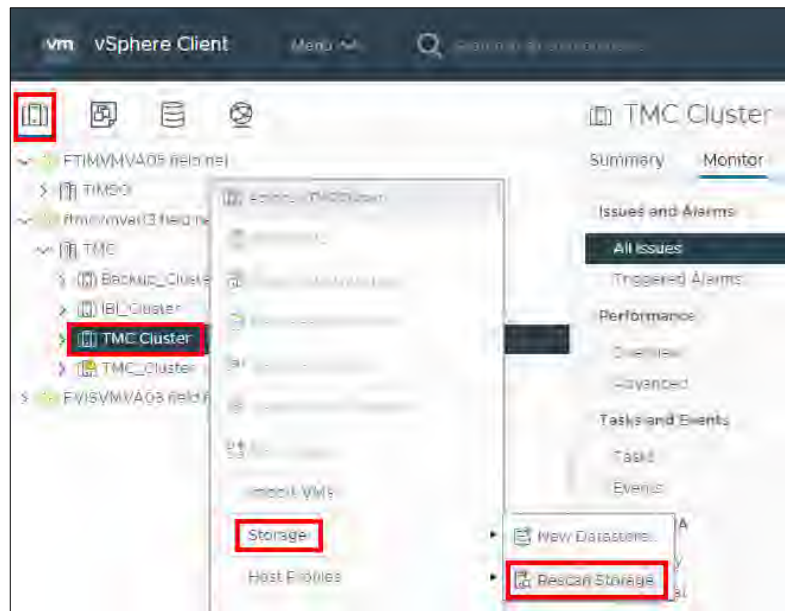


Figure 307. TMC Cluster > Rescan Storage.

Steps / Screenshots

8. Click **OK**.



Figure 308. Rescan Storage.

MIGRATE VMs to a NEW DATASTORE with vMOTION

Note: These procedures cannot be performed by one person, but with a minimum of two people.

Migrate (Compute Only) Virtual Machines (VMs)

1.
 - (1) Click hosts and clusters,
 - (2) Click ftmcvhap02,
 - (3) Click Configure,
 - (4) Click VMkernel adapters,
 - (5) Verify that **VMotion-01** is enabled.

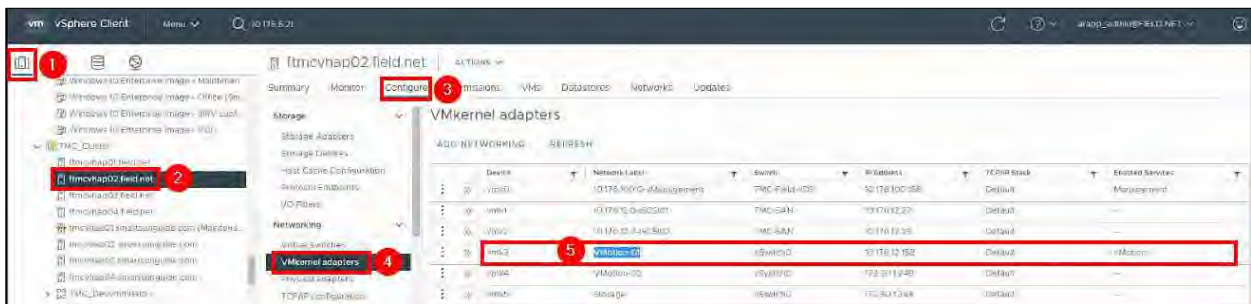


Figure 309. VMotion-01 Enabled

2. Perform a compute migration of VMs into **ftmcvhap02**.

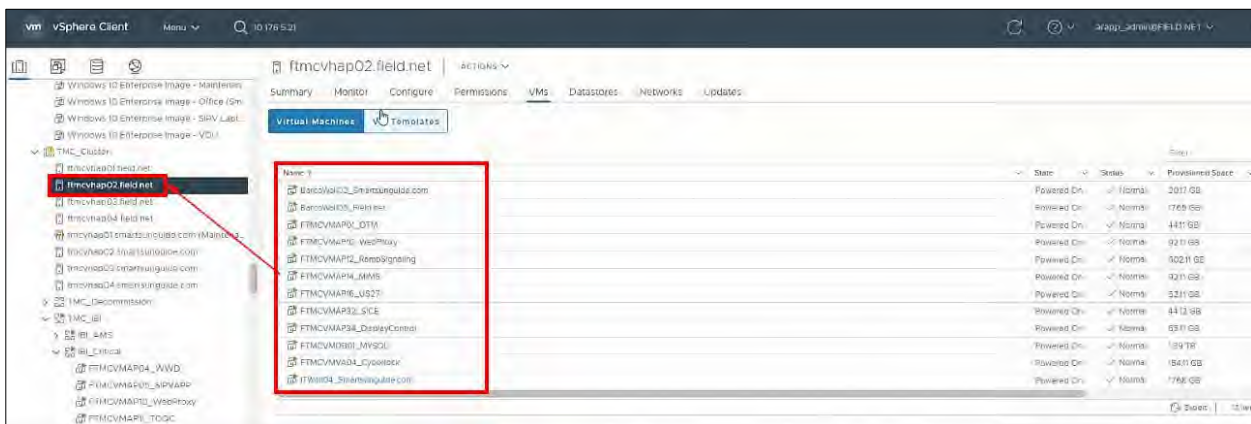


Figure 310. Compute Migration of VMs.

Migrate Storage Only

Steps / Screenshots

1.
 - (1) Click hosts and clusters,
 - (2) Click ftmchvap02,
 - (3) Click Configure,
 - (4) Click VMkernel adapters,
 - (5) Click the three dots next to vmk4,
 - (6) Click Edit.

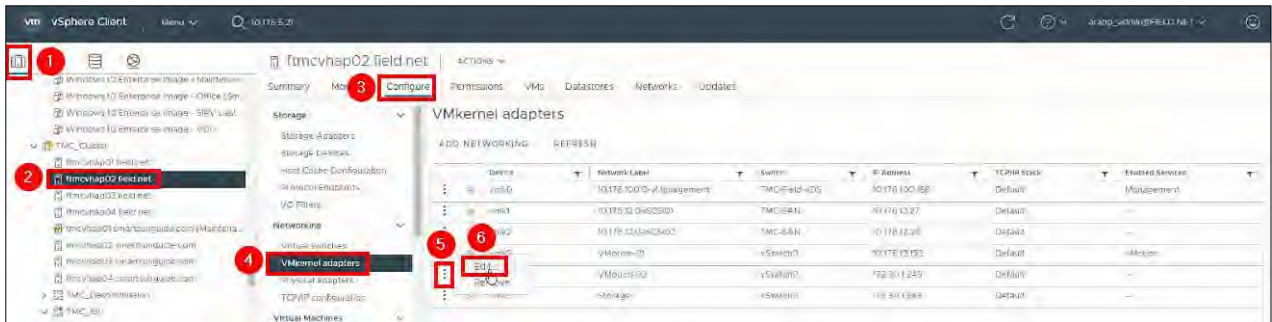


Figure 311. Edit VMkernel Adapters

2.
 - Check the box next to **vMotion**
 - Click **OK**

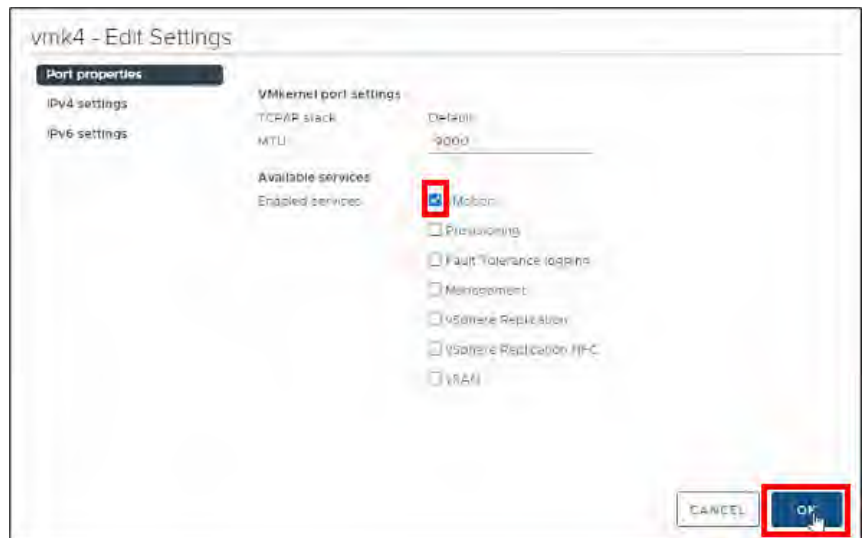


Figure 312. Port Properties - Select vMotion

Steps / Screenshots

3. Verify that VMotion-02 is enabled.

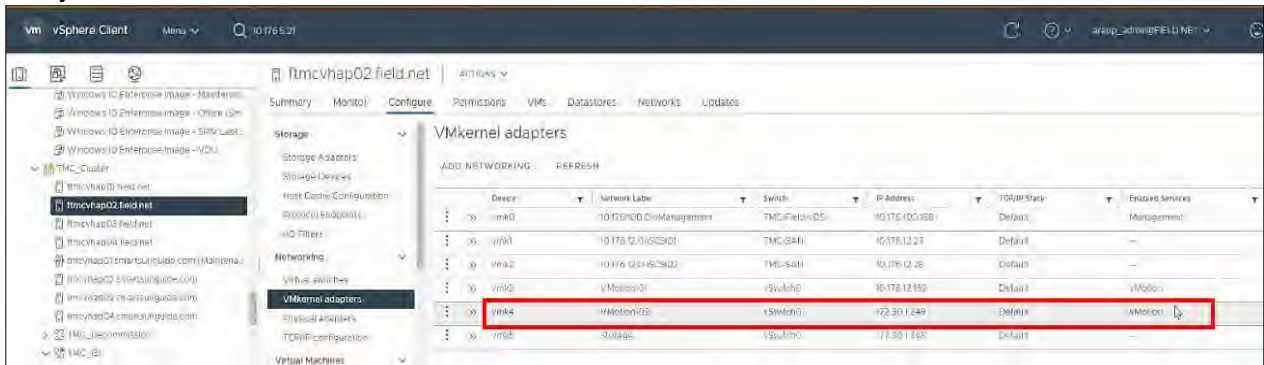


Figure 313. VMotion-02 Enabled.

4.
 - (1) Click **VMs** and highlight all VMs listed.
 - (2) Right click →
 - (3) Select **Migrate**.

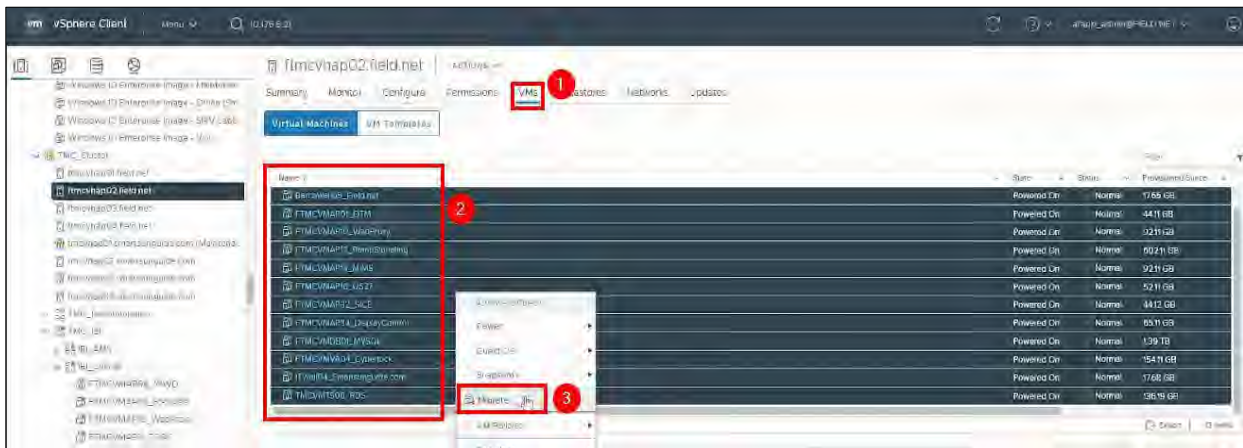


Figure 314. Migrate VMs.

5. Click **YES** to confirm the migration of all VMs listed



Figure 315. Confirm Migration

6.
 - Select Change storage only.
 - Click **NEXT**.

Steps / Screenshots

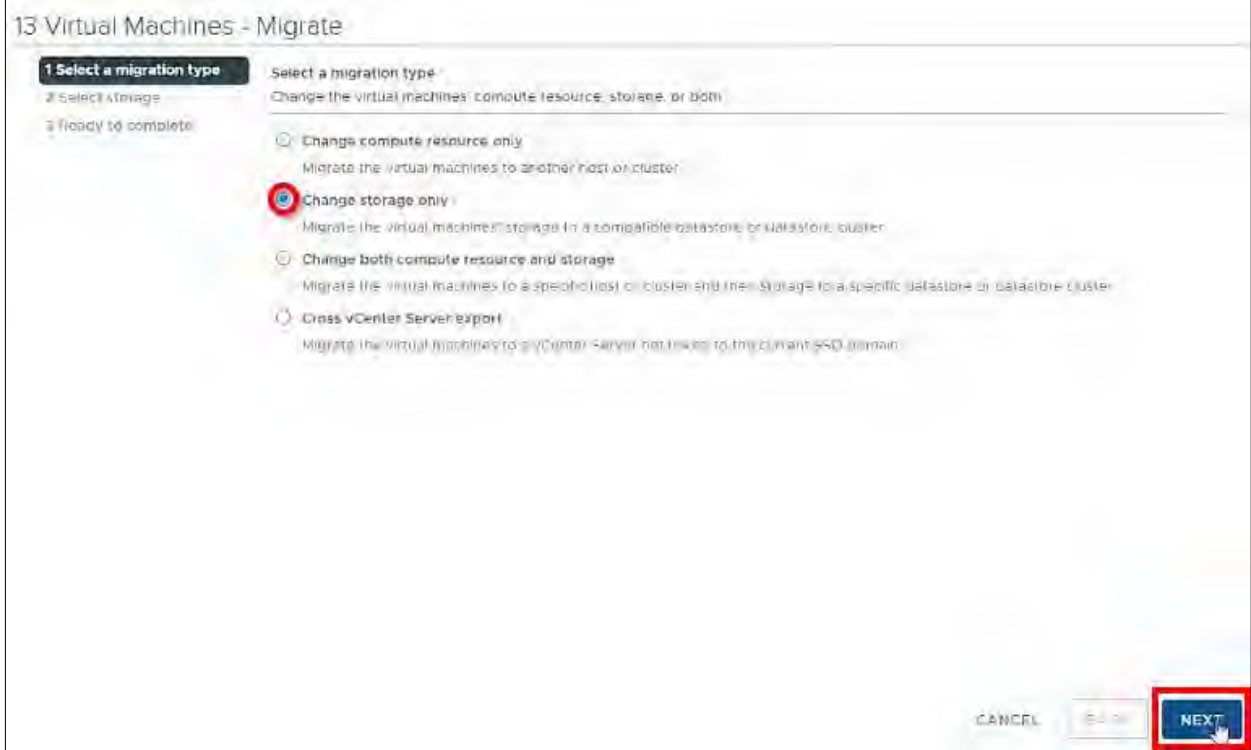


Figure 316. Change Storage Only

- Select the new datastore **DatastoreVM_TMC**.
 - Click **NEXT**.

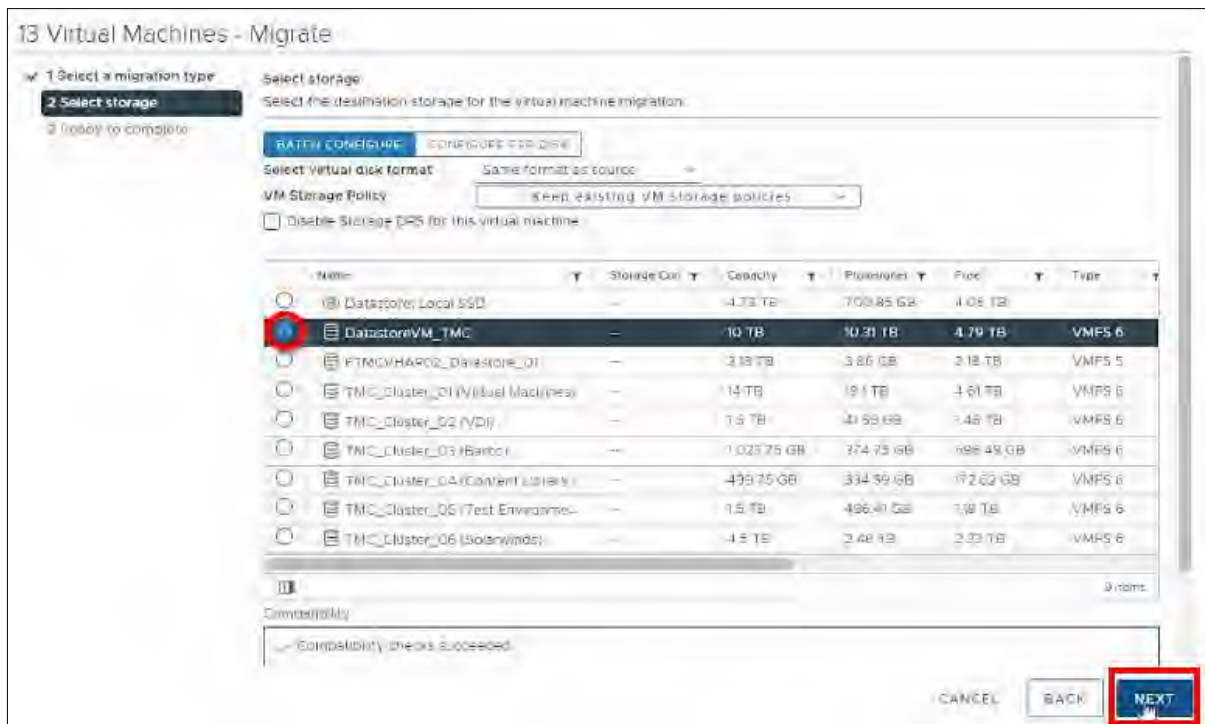


Figure 317. Select DatastoreVM_TMC

Steps / Screenshots

8. Click **FINISH**.



Figure 318. Ready to Complete

9. Repeat the following procedures for all other TMC hosts:
- Migrate (Compute Only) Virtual Machines (VMs)
 - Migrate Storage Only



7.22 Video Wall Configuration

Document History

Version #	Date	Author	Changes
1.0	12/20/2023	Yana Neishlos	Initial Draft

Table of Contents

VIDEO WALL CONFIGURATION 4

VIDEO WALL CONFIGURATION

The RTMC manages a multi-site enterprise video wall system. This Video Wall system consist of over 60 Individual Video Wall Displays.

1. The Primary wall → Used by the RTMC Control Room; consists of 44 x 70" Rear LED Projection Engines creating a single Display.
2. Two secondary Walls within the RTMC Control Room → Consists of 12 x 55" UniSee panels in a 6 x 2 layout.
3. One Backup Video Wall System → At the Treasure Coast location - consists of 14 x 50" LED Monitors clustered together.
4. One Annex Video Wall out of Palm Beach → Consists of 8 x 50" LED Monitors; clustered together used by Palm Beach Operations.
5. Three Separate Accessory Video Wall Systems → Consists of 4 x 55" 4k LED Monitors each used by Broward Maintenance and the IT Department.
6. Fifty-two Individual Video Wall Displays → Spread throughout the RTMC, Fort Lauderdale, Palm Beach, and Treasure Coast.

All devices are controlled by Centralized Clusters of Control Servers capable of managing all devices on the private RTMC TSM&O Video Network.

All Hardware, Software, Development, and Administration falls on the IT Department.



7.23 Barco Configuration

Table of Content

INTRODUCTION	4
Add a User to the Barco Control Panel	4
Delete / Remove a User from the Barco Control Panel	7
BARCO DEMARCATION RULES for non-TMC HARDWARE (NTH)	11
Maintenance	11
Barco Initial Installation	12
Barco continual servicing	12
Barco Upgrading Servicing and Common Troubleshooting	12
BARCO NTH PERSONNEL	13
BARCO INSTRUCTIONS	14
Overview	14
Procedure	14

Document History

Version #	Date	Author	Changes
1.0	3/14/2024	Yana Neishlos	Initial Draft

INTRODUCTION

Barco Sidebar is a standard application for images. If need to install separately, go to <https://10.176.3.238>.

Sidebar, control panel and display agent are java runtime applications pulled from the server based upon the java applet. Running the applet and clicking on next-next-finish will install the program.



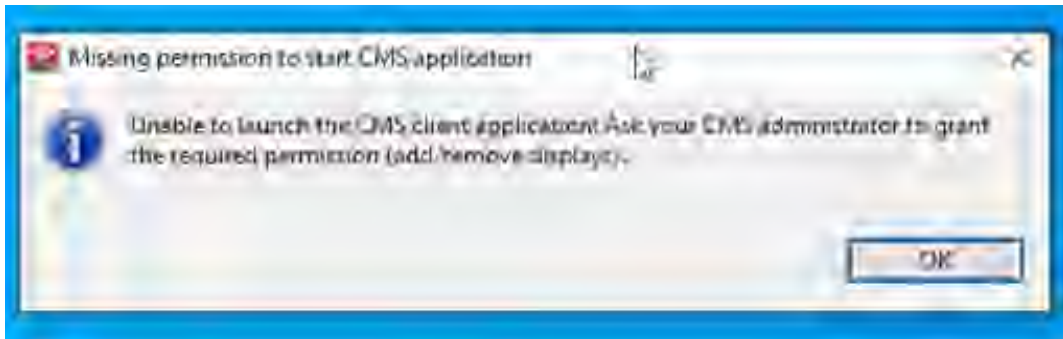
Individual customizations of roles and rules are based upon the naming standards and user creation rules, which can be found in the SolarWinds Service Desk at the following links:

Add a User to the Barco Control Panel

Barco accounts are automatically created for users when they log into their computers and launch Sidebar for the first time.

Steps / Screenshots

1. Users will receive a message stating that *they are missing permissions when Sidebar first opens*. Hence, a user will either be calling someone from the IT Team, or they will be visiting the IT Office to relay that they are unable to view anything within Sidebar.

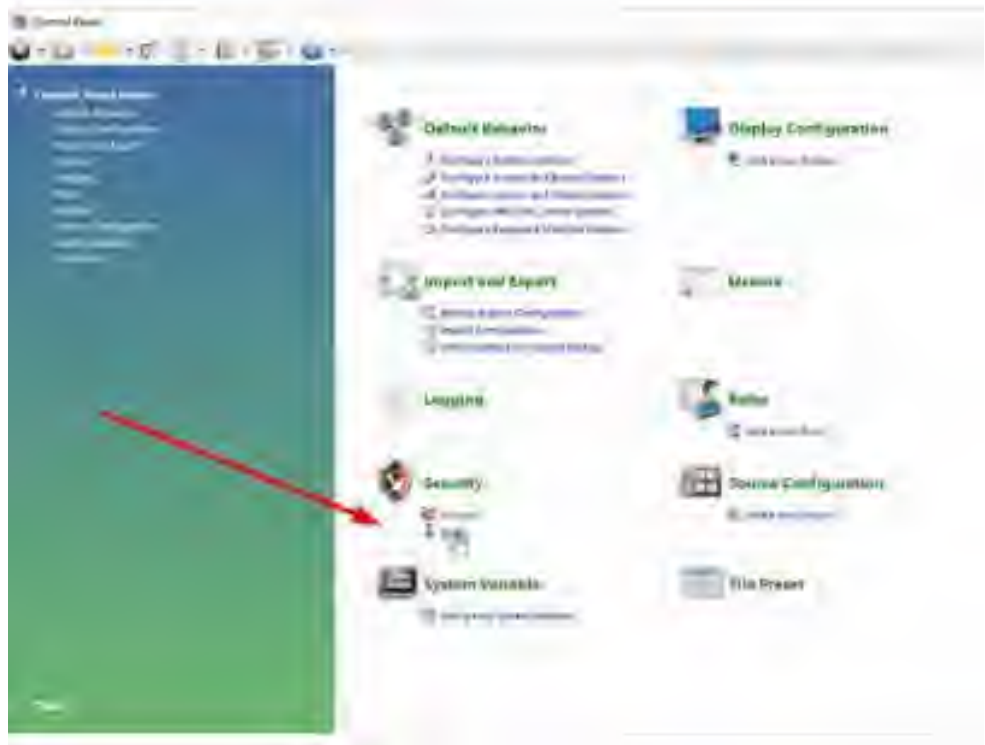


2. Open **Control Panel**.



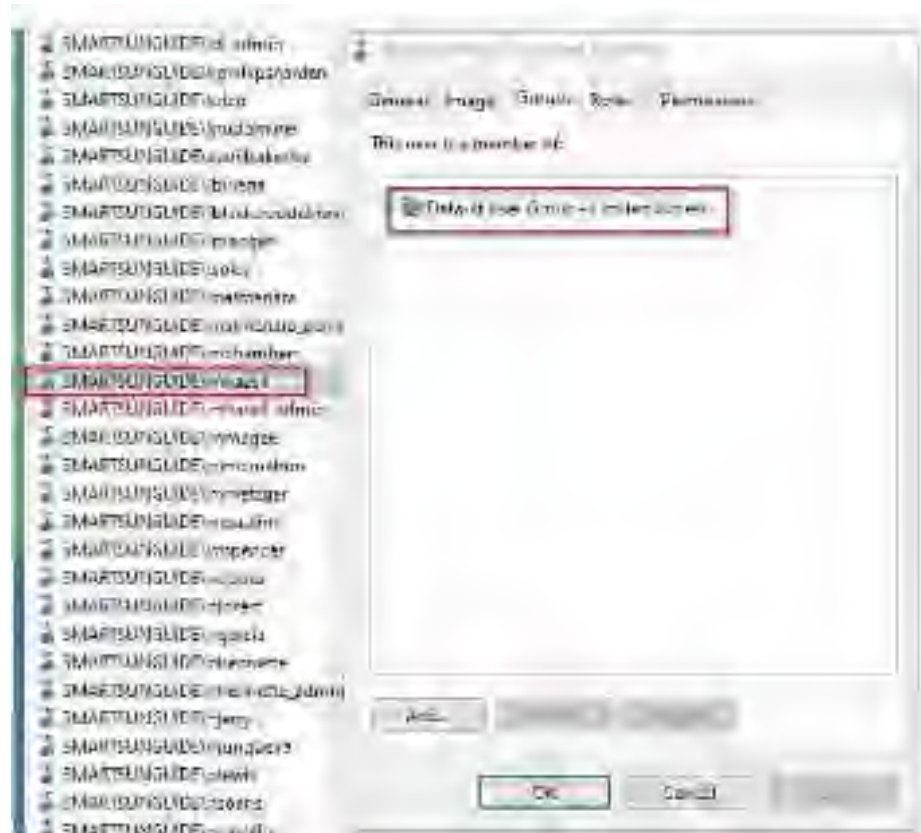
Steps / Screenshots

3. Within Control Panel, locate **Users** under the **Security** category.



4.
 - Right-click on the user in question
 - Select Properties.

By default, new users in the system will be assigned the **Default User Group - Limited Access.**



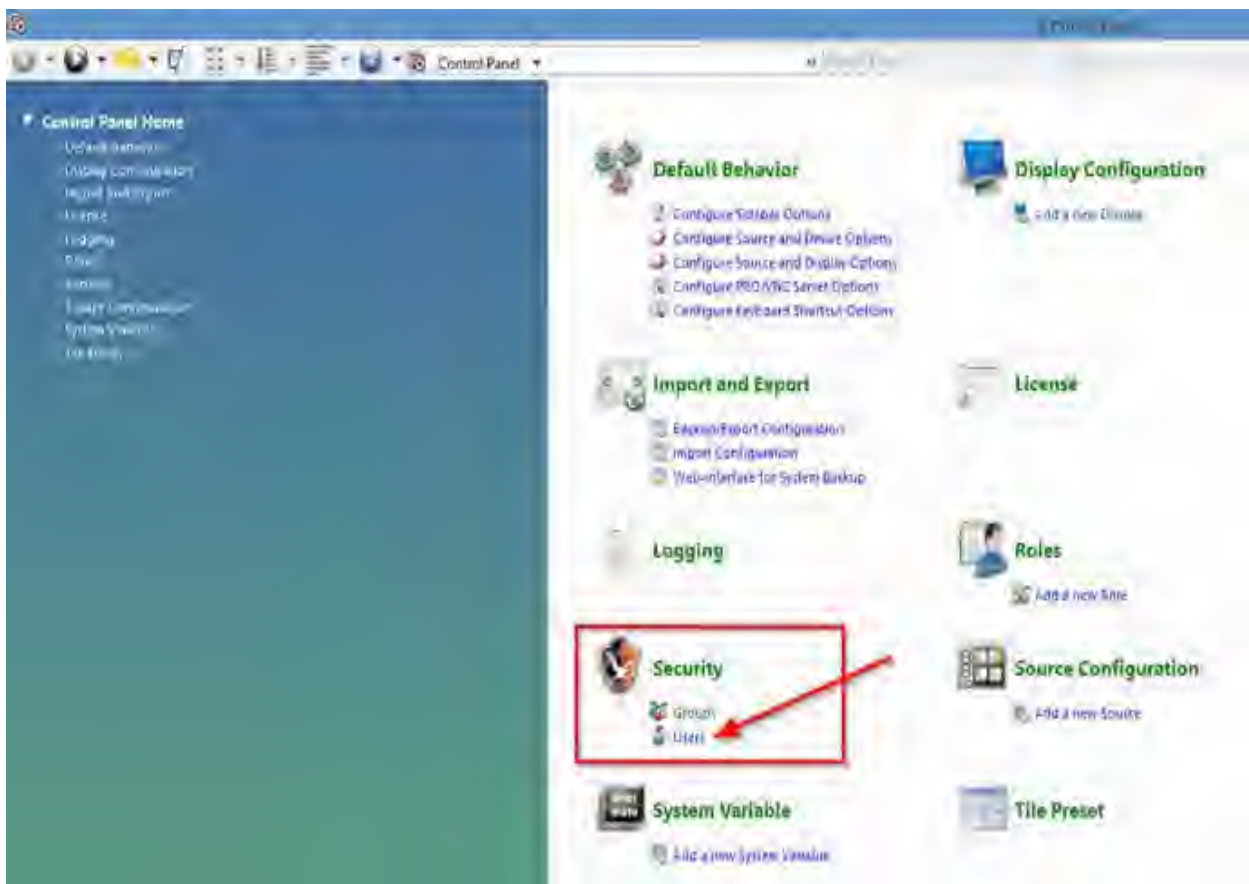
Delete / Remove a User from the Barco Control Panel

Steps / Screenshots

1. Locate the **Barco Control Panel** application and launch



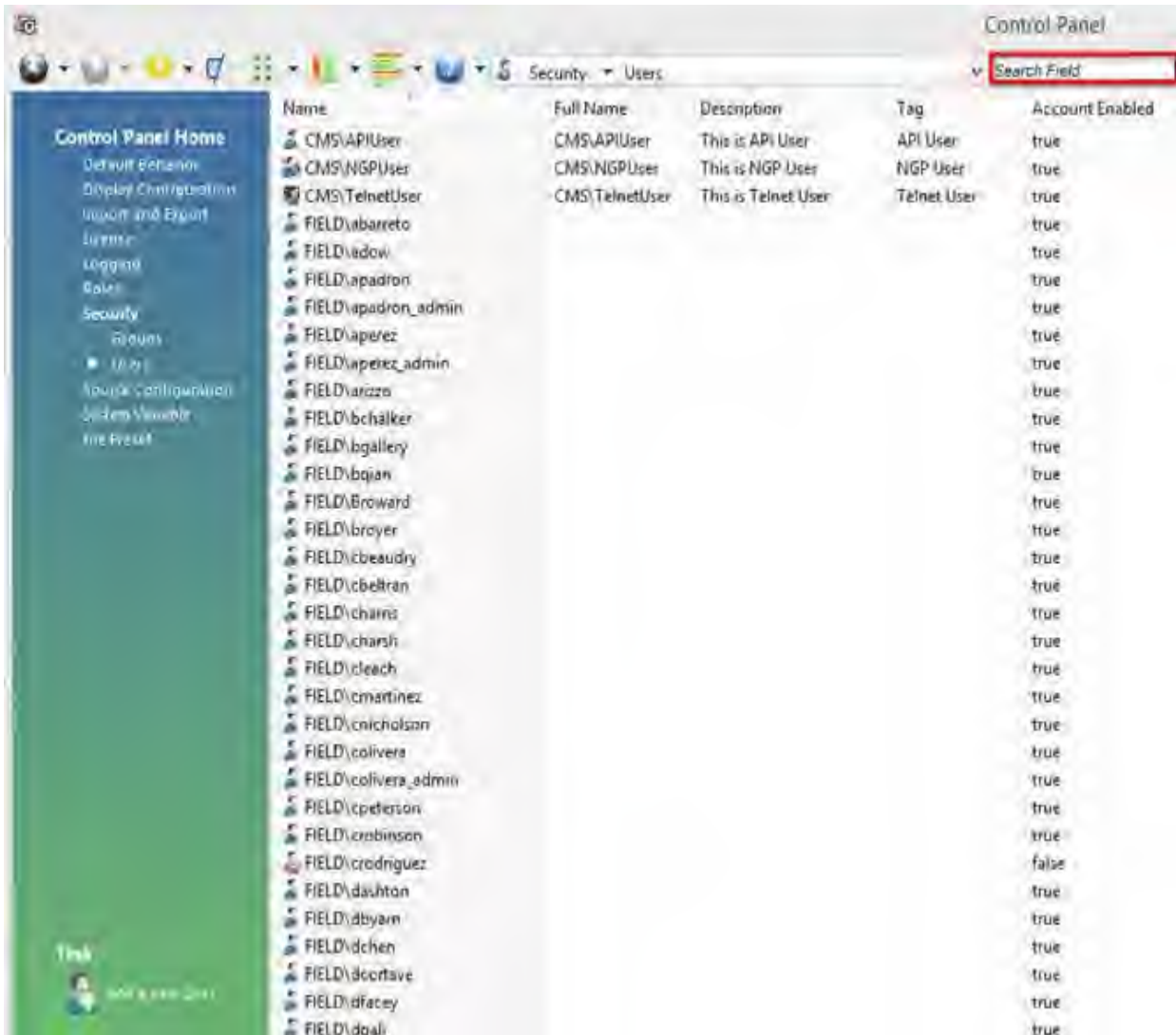
2. Once the application has opened,
 - Find **Security** category.
 - Click **Users** under the **Security** category. (It takes a moment to open.)



Steps / Screenshots

- Once the user list populates, you will see a large list of all user accounts linked with the Barco system.

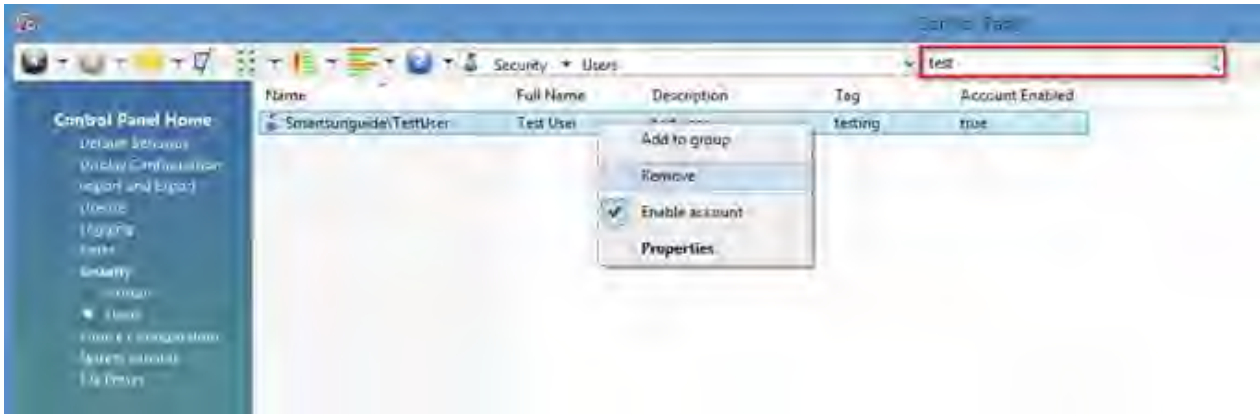
Locate the user to be removed from the list. (If you cannot find the user, look for a search button on the top-right of the current window).



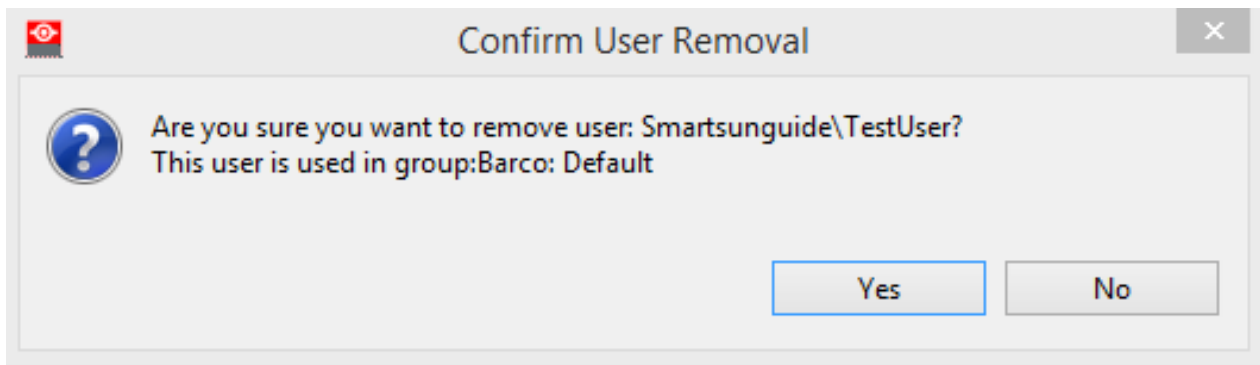
Steps / Screenshots

- 4.
- Right-click the user's account
 - Click **Remove** option.

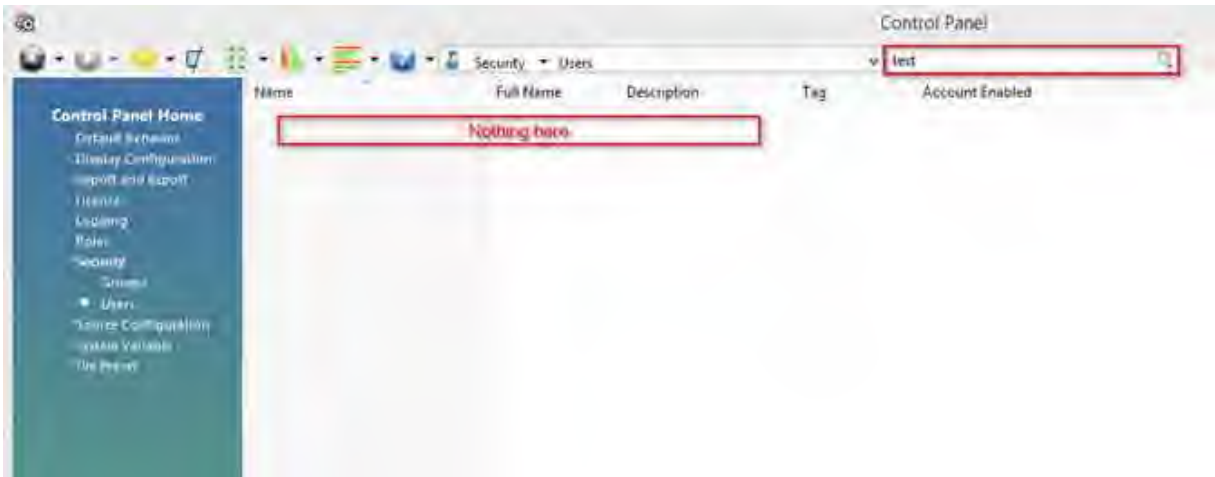
Note. Be sure to remove both domain accounts for user. This example only shows Smartsunguide for testing.



5. See this prompt.
- Select "Yes" to completely remove the user account entry.



No additional prompts will appear. You will notice that the account is no longer present.



BARCO DEMARCATION RULES for non-TMC HARDWARE (NTH)

When the Barco Video Distribution system is utilized by personnel outside of the users within the TMC the following rules apply.

Here are the four steps (click each of these internal cross-reference links for details) of Responsibility Demarcation and details:

1. Maintenance
2. Barco Initial Installation
3. Barco continual servicing
4. Barco Upgrading Servicing and Common Troubleshooting.

Maintenance

When NTH is utilized by NTH personnel, only the Barco Software on the NTH is responsible for TMC personnel to troubleshoot.

The Agency or non-TMC personnel providing the hardware is responsible for repairing any physical defects within the NTH, as well as providing installation and maintenance of anything related to separate agency software (e.g., endpoint software) including the underlying operating system (e.g., windows licenses, security and maintenance). The personnel managing the NTH will be responsible for the physical installation, location and maintenance of any day-to-day tasks per their own configuration rules of the NTH equipment.



Barco Initial Installation

RTMC personnel will assist any NTH personnel with the installation and training of the Barco software with NTH personnel. Instructions will be provided on basic usage, instruction on understanding the management of expectations of the system. This includes any questions fielded for feature requests, how-to-dos, changes or additions to the system.

RTMC personnel will provide “best effort” availability of the system and is not entitled or obligated in any type of guaranteed contract of services. All NTH personnel have the understanding that such equipment is provided as a gesture of cooperation between RTMC and NTH personnel, and no such productivity or production task will be tied to any type of day-to-day utilization of such system that is dependent on the continual functioning and services needs of the RTMC staff.

The NTH personnel will be responsible for the day-to-day usage of the Barco software on their system and will be expected to (independently with their own staff), control and interact with their NTH using the software independent of assistance from RTMC personnel.

Barco continual servicing

All NTH personnel requests listed in steps 2 ([Barco Initial Installation](#)) are not binding contractually or otherwise required to be fulfilled by anyone within the RTMC, but instead provided out of gesture of good-will and cooperation between the 2 groups. If such request cannot be fulfilled (due to technical limitation, IT governance rules within the RTMC, or prioritization of needs of the RTMC being greater), communication will be provided to any liaison person of NTH personnel to inform them of inability to accommodate their requests.

All resources viewable within the Barco system are prioritized for the TMC operations (including VISTA and TIMSO), maintenance and IT staff to assist in the completion of their contractual goals.

Any deviations in availability of resources outside of these three locations will be investigated for potential resolution, however, are not prioritized nor obligated in any way contractually or otherwise to have a resolution.

Barco Upgrading Servicing and Common Troubleshooting

When a new version of the Barco application comes up, a scheduled upgrade will occur. The RTMC will assist in any installation issues like step 1 ([Maintenance](#)) working in conjunction with NTH personnel, however, if modifications to NTH equipment causes incompatibility issues with the newer version of the Barco software, the RTMC will let the NTH personnel know the issue.

The NTH personnel will be responsible for making changes to allow such compatibility with the Barco system to occur again.

The Barco system is designed to be a self-repairing system, however, there will be times when NTH equipment may need to be reset, rebooted or have other basic performance tasks accomplished to establish or fix. This will be the responsibility of NTH personnel and not RTMC personnel.

BARCO NTH PERSONNEL

The following list is the current responsible parties representing NTH personnel that utilize equipment linked to the primary Barco Video Wall System.

Information below is the list of positions/personnel that are responsible for handling/maintaining all demarcation work described in SOP Section BARCO DEMARCATION RULES for non-TMC HARDWARE (NTH).

It is the job of the responsible party listed below to ensure any user training, contact with help, and potential feature requests are funneled through the appropriate list of positions below. All TSM&O personnel will refer all work required to be performed by NTH to one of the parties listed below.

Any communications | questions about current issues | outages | problems | changes within the Barco System can be communicated through Barco-Support-DL@smartsunguide.com. Communication will be returned at the earliest convenience of the IT personnel within the TMC.

The TMC IT department will prioritize any issues that are impacting the general and major functionality of the system to help restore communication if IT department is partially responsible (per demarcation requirements of SOP Section 7.23.01).

If an emergency response is required, RTMC IT Support Manager can be contacted at 954-847-2794. Emergencies are classified as complete system down status.

- | | |
|---|---|
| 1. FDOT 3400 (and Accessory buildings) Equipment: | Responsible Contact Party: FDOT AMS/FMS Specialist IT Manager. |
| 2. Broward County: | Responsible Contact Party: Broward County Traffic Manager Center Network Administrator. |
| 3. Broward Sherriff Office: | Responsible Contact Party: BSO Homeland Security Coordinator. |

BARCO INSTRUCTIONS

Overview

This SOP Section provides the procedure for changing video feeds using Sidebar through Remote Desktop Connection (RDP). This procedure is applicable to users without a smartsunguide.com account.

However, physical computer access on the smartsunguide network is required.

Procedure

Steps / Screenshots

1. In the computer search field:
 - Enter "remote desktop"
 - Click **Open** to access RDP app.

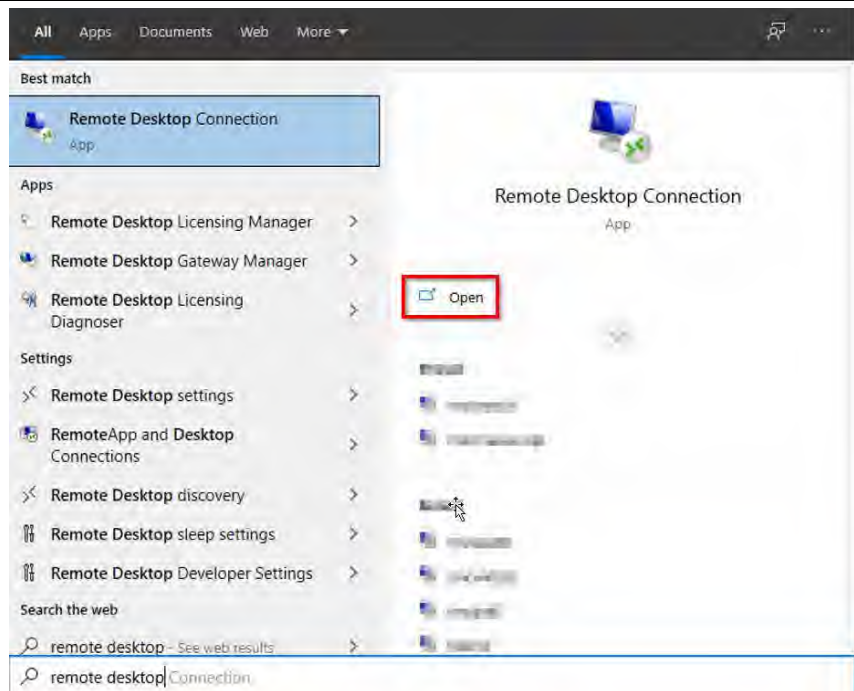


Figure 1. Accessing the RDP App

2. In the "Computer" field,
 - Enter tmcvmnts02.smartsunguide.com
 - Click Connect



Figure 2. RDP Connection

Steps / Screenshots

- 3, Log in to the SmartSunguide domain as follows:
 - Enter the credentials below:
 Username: SmartSunguide/Barco_3400
 Password: Sidebar!!!
 - Click **OK**.

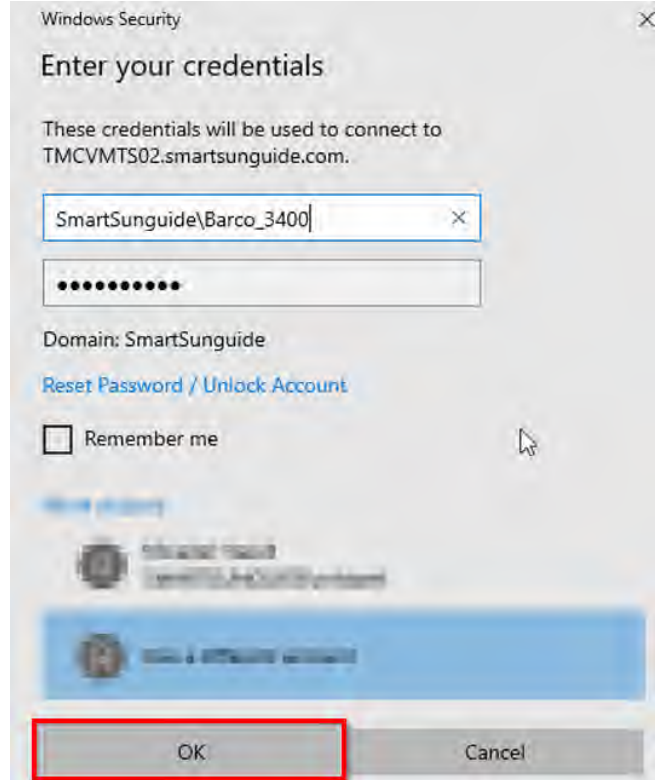


Figure 3. Logging in to the SmartSunguide Domain

4.
 - Double-click on the Barco Sidebar icon
 - Open the application



Figure 4. Opening the Barco Sidebar Application

5. If the roles are not already activated,
 - Select all roles.
 - Click **Apply**.

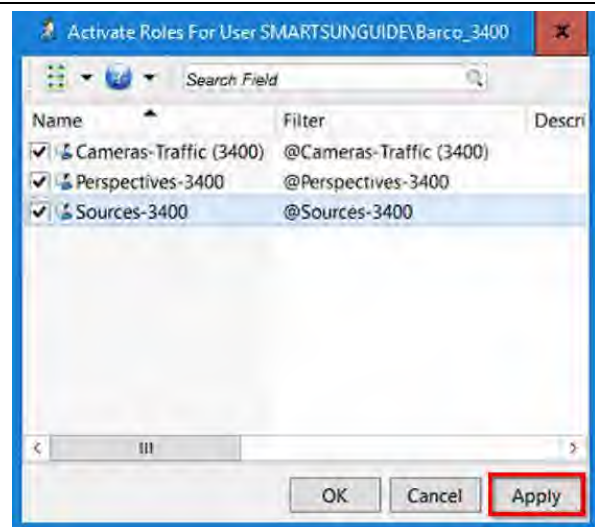


Figure 5. Activating All Roles

Steps / Screenshots

6. Open your perspective only

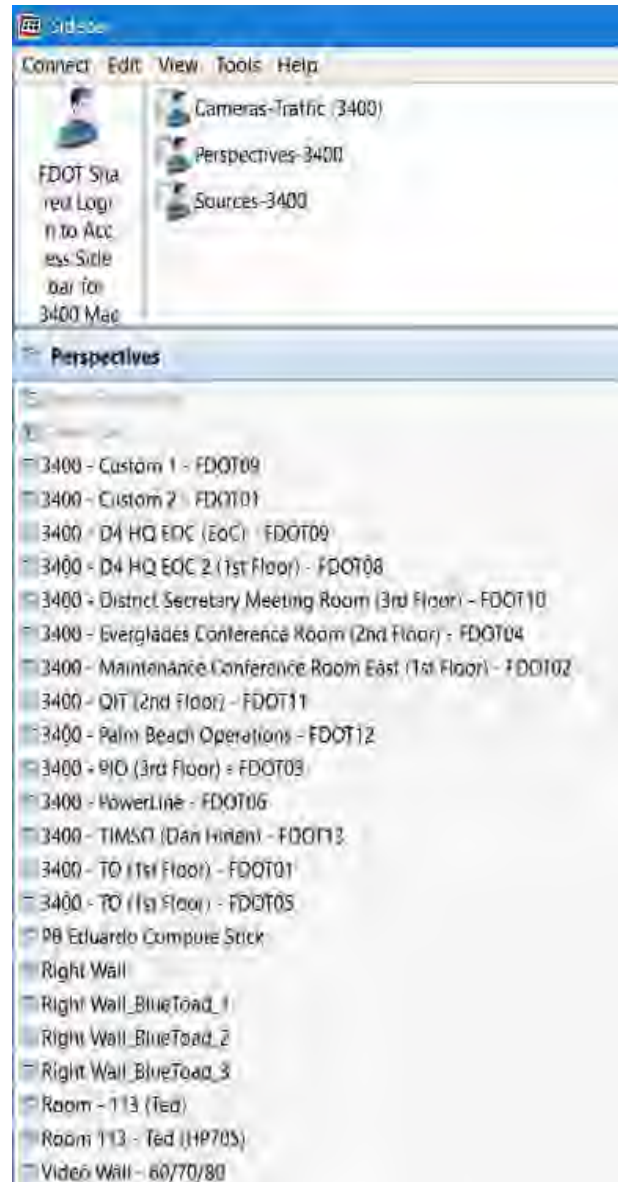


Figure 6. Opening Your Perspective

Steps / Screenshots

- Under sources, drag any cameras you would like into your perspective view.

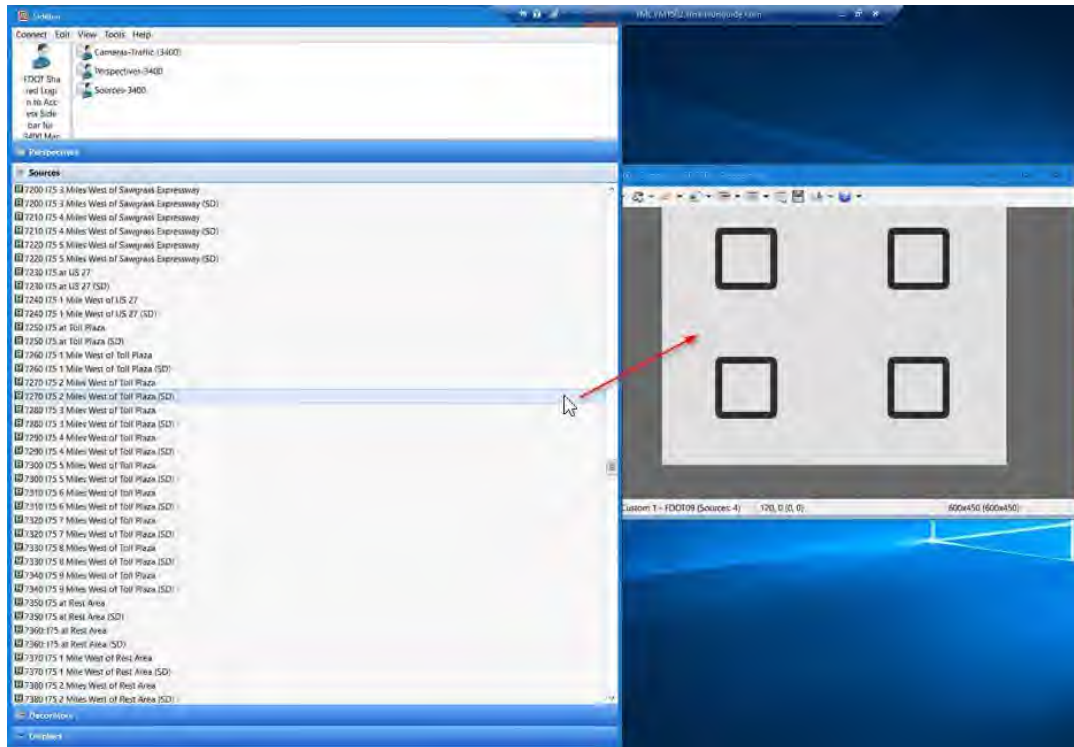


Figure 7. Dragging Cameras to Your Perspective View

- If your display is not showing your perspective,
 - Activate your personal view under **displays** (your display only)

Select **personal**:

- Right-click your display.



7.24 Periodic Tasks

Table of Content

PERIODIC TASKS.....	4
----------------------------	----------

Document History

Version #	Date	Author	Changes
1.0	12/20/2023	Yana Neishlos	Initial Draft

PERIODIC TASKS

The following list is periodic tasks required by the IT Department to perform.

1. Monthly updates occur on all Virtual Machine templates.
2. Quarterly updates occur on all Smart Deploy Images.
3. Twice a day checks of the small and large conference room equipment.
4. Daily check of projectors within the control room.
5. Weekly patch management of all Windows endpoints.
6. Quarterly Firmware Updates on all Desktops, Laptops, Servers and Printers.
7. Daily, Weekly and Monthly Check of Antivirus EndPoint Status.



7.25 Notifications and Help Desk

Document History

Version #	Date	Author	Changes
1.0	12/21/2023	Yana Neishlos	Initial Draft

Table of Contents

- TROUBLESHOOTING4**
 - Overview.....4
 - SUNGUIDE.....4
- JOYSTICK CONFIGURATION5**
 - Cluster Administrator5
 - Enter the configuration (CONFIG) mode of the Joystick5
 - Reset the Joystick to Mfr. Defaults.....5
 - Configure the Joystick for use with SunGuide6
- BROWARD COUNTY BUILDING ISSUES.....7**
- FORCE IMMEDIATE UPDATE OF GAL AND COPY TO OUTLOOK8**
 - Force Update of Global Address List (GAL)8
 - Force Outlook to download the updated Global Address List (GAL)8
- SYNCHRONIZING LAPTOPS.....9**
- HELP DESK ISSUES10**
 - Help Desk Support – Process10
 - Prioritizing Problems10
 - When on Call10

TROUBLESHOOTING

Overview

For systematic problems, create a case file where issues are documented. These standards apply to the use of any kind of server.

1. When console-type access is needed to a server, these are the only approved methods:
 - Physically at the server console/KVM.
 - Use IP KVM.
 - Use Microsoft Remote Desktop feature.
 - Use HP ILO.
2. When finished, immediately log off the server. Do not intentionally leave the server logged on or "X" out of the RDP session.
3. Avoid using the Internet on the server, whenever possible. If you need to research a problem, do it from another location.
4. Do not load the SunGuide Application/SunGuide Map from any server (including the SunGuide servers).
5. Do not load any unnecessary tools on the server. To clarify, if you could load it on your workstation and accomplish the same task, it was unnecessary to load it on the server. An example of this is Wireshark. If you wanted to monitor the data to and from the server, load Wireshark on your workstation and port monitor the server. Do not load Wireshark on the server itself.
6. No end-user software should be loaded on a server. For example, it would be acceptable to load the files to install Office on a network share, but it would not be acceptable to load Office itself on the server as an executable application.

SUNGUIDE

In general, IBI takes care of SunGuide issues, but there are times when no one from IBI Group is available. IT is responsible for the server itself, so at times the responsibilities may blur.

JOYSTICK CONFIGURATION

Cluster Administrator

Check for the MCP Group on the appropriate clustered server in Palm Beach or Broward (depending on which joystick needs to be repaired) and on that MCP Cluster Service:

1. Notify the operator/s you are taking down the joystick(s).
2. Take the MCP Cluster Group offline.
3. Once it is offline, move the group (which will bring it up on the other server of the cluster) or bring group online where it is.

If after 5 minutes, the service is not yet fully offline:

- Notify Jacques DuPuy of what is happening.
 - Login to the actual server and either 1) stop the service in Services manager or 2) kill the process tree in Task manager for the MCP. This will take the service fully offline back in Cluster Administrator.
4. Once it is online, wait 5 minutes before telling the operator to try the joystick/s again. If that does not work, then try reconfiguring the individual joystick (below).

Enter the configuration (CONFIG) mode of the Joystick

1. Power-ON the Joystick.
2. Immediately and simultaneously press the keys at the TOP LEFT and BOTTOM LEFT on the keyboard.

Reset the Joystick to Mfr. Defaults

Press the BLUE PLAY key while in CONFIG mode.

Configure the Joystick for use with SunGuide

1. Press the BLUE RECORD button while in CONFIG mode.
2. Select RS232 mode
Press ENTER.
3. Power cycle and enter CONFIG mode again.
4. Press the BLACK REWIND key.
5. Select RS232 and 38400
Press ENTER.
6. Power cycle and enter CONFIG mode again.
7. Press the BLACK FAST FORWARD key.
8. Turn OFF sound
Press ENTER.
9. Power cycle and enter CONFIG mode again.
10. Press the BLUE CAMERA key to the LEFT of the Joystick.
11. Select REPEAT MODE
Press ENTER.
12. Power Cycle one last time.

BROWARD COUNTY BUILDING ISSUES

For an alarm such as for a UPS, security, or fire system, in an area of the RTMC not controlled by RTMC employees, report the problem immediately to Broward County employees.

FORCE IMMEDIATE UPDATE OF GAL AND COPY TO OUTLOOK

Force Update of Global Address List (GAL)

1. On mail server, in System Manager
Click to expand Recipients > **Offline Address Lists**.
2. Right-click **Default Offline Address List**, and,
Select **Rebuild**.

You will receive a message stating the rebuild may take some time however, due to the size of our system it runs very quickly.

Force Outlook to download the updated Global Address List (GAL)

1. Click **Tools à Send/Receive à Download Address Book**.
2. Uncheck selection **Download changes since last send/repair**.
3. Ensure **Full Details** and **Global Address List** are selected.
4. Click **OK**.

SYNCHRONIZING LAPTOPS

For laptops that only occasionally connect to the network for synchronization, here is the procedure:

1. Logon **OFF NETWORK**.
2. Connect the network Ethernet Cable.
3. Once connected, logoff the computer. This starts the sync running.
4. When the computer logs off, you are done.

HELP DESK ISSUES

Help Desk Support – Process

The following process is used for regular and after hours help desk support. The notification to the IT group comes when Operations creates a help desk ticket, or a MIMS ticket for a field device issue.

This procedure is valid 24/7 but works best when the IT analyst is onsite.

1. In all cases, Operations opens a help desk ticket or a MIMS ticket to report field devices issues.
2. If this is a serious issue (as defined in the Operations SOP), an operator contacts the on-duty supervisor.
3. If a supervisor cannot fix the problem or provide a reasonable workaround, a supervisor calls the on-duty IT employee.
4. An IT employee determines the nature of the problem and arranges for repairs personally. If the problem needs to be referred to another department, an IT employee contacts an on-call contact for either Maintenance or the software contractor.

If an on-call contact does not answer, Operations calls the supervisor, being a backup contact.

5. An IT employee is responsible for the incident until it is either resolved or successfully taken over by another party. A voicemail is not considered a successful handoff.

Prioritizing Problems

For most daily issues, Operations gets priority for help with equipment and devices.

Other IT support that is time-sensitive may also need to be dealt with as soon as possible, such as an employee who needs help setting up a teleconference call.

When on Call

IT staff members rotate weekly for on-call duty support. If a user requests support, an on-call IT staff member must respond within two hours. IT support staff members may require coming to the RTMC on short notice after hours and weekends.

Staff coverage should be always maintained for user support at the RTMC. If any member of the IT staff is out sick, an IT Support Manager must arrange and ensure that an IT staff member will always be in the office for early and late hours.



7.26 Purchasing

Document History

Version #	Date	Author	Changes
1.0	12/21/2023	Yana Neishlos	Initial Draft

Table of Contents

OPERATING CAPITAL OUTLAY (OCO)	4
EXPENSE	6
SERVICES	8
FDOT REPLACEMENT MONEY	10
TSM&O RESOURCE PROJECTS	12
AECOM SPECIAL SERVICES	13
FDOT WORK PROGRAM MONEY	15

OPERATING CAPITAL OUTLAY (OCO)

General purchase rules	Purchases must be physical assets over \$1,000.
Examples of past purchases	Servers, switches, and generally something that gets an asset tag. Items can be returned to 3400 at the end of its life.
Purchasing process	<p>Purchases should be made as soon as possible, as needed, using the following process:</p> <ul style="list-style-type: none"> • The FDOT Traffic Ops Office Manager determines if funds are available. • The IT Department writes a justification and obtains three quotes. • The justification and three quotes are sent to the FDOT Traffic Ops Office Manager. • The FDOT Traffic Ops Office Manager obtains approval to make purchase for anything over \$100. • If an IRR is needed, the District TSM&O Resource Manager submits it. • Once everything is approved, the order is placed with a purchase card (Pcard) by the TMC Office Manager or through ARIBA (online purchasing system) by the FDOT Traffic Ops Office Manager (depends on Pcard purchase limit). • The IT Department must notify the TMC Office Manager when the order has arrived at 2300 or 3400 and provide the packaging slip.
# of quotes required	Three.
Vendors to get quotes from	<p>Quotes should be from vendors on state contracts, if possible. If products are only available from one vendor, use the FDOT Documentation for items not purchased from state contract form. The TMC Office Manager can request this from the FDOT Traffic Ops Office Manager. The form must be signed by the District TSM&O Resource Program Manager under Request made by and by the District Traffic Operations Engineer under Cost Center Manager.</p> <p>In addition to completing the form, documentation must be obtained and kept with the paperwork from at least 2 additional vendors stating they do not carry the product.</p>
Money available each year	There is no set amount available from year to year. Amount provided is based on need.

	<p>Amount needed must be determined by June 15 prior to the start of the new fiscal year. Additional money can be obtained throughout the fiscal year if needed, if other departments are not using it.</p> <p>In order to capitalize on this opportunity, IT should have a wish list ready well in advance of the end of the fiscal year (July 1 – June 30). Prices for items on the wish list should be overestimated in order to cover the possible increase in prices in the coming year or the chance that an upgraded (more expensive) model becomes available.</p>
Staff in charge of ordering	The FDOT Traffic Ops Office Manager makes all orders through ARIBA. The TMC Office Manager should always follow up on the order. IT should remain in contact with the vendor. IT should notify the TMC Office Manager of product arrival and provide the packing slip.
Written justification requirements	Written justification is required for every item purchased. About one paragraph per item is sufficient. It should define why the item is critical and the consequences of not being approved to purchase it.
HW tags requirements	Yes, an HW tag is required.
IRR requirements	Yes, an IRR is required.
IT's contact for purchase	TMC Office Manager.
Purchasing time frame	Pcard purchases must be ordered/received by June 15. ARIBA purchases must be received by June 30. Both are preferred to occur much earlier in the fiscal year.
Shipping address	Everything should ship to 3400 unless it is a large item requiring a forklift (e.g. servers). The FDOT Traffic Ops Office Manager will make sure OIT is aware of ordered items. If shipping to the TMC, provide serial numbers and packing list with request for HW tags ASAP.

EXPENSE

General purchase rules	Purchases must be for items under \$1,000 ordered by Pcard or through ARIBA.
Examples of past purchases	Copy machine rental, MetroEthernet, travel, office supplies, toner, website domain names, miscellaneous IT items, software (cost doesn't matter, can be over \$1,000), furniture if under \$1,000, replacement computers/laptops.
Purchasing process	<p>Purchases should be made as needed, and without delay, using the following process:</p> <ul style="list-style-type: none"> • The FDOT Traffic Ops Office Manager determines if funds are available. • The IT Department writes a justification and obtains three quotes. • The justification and three quotes are sent to the FDOT Traffic Ops Office Manager. • The FDOT Traffic Ops Office Manager obtains approval to make purchase for anything over \$100. (If under \$100 it doesn't need approval.) • If an IRR is needed, the District TSM&O Resource Manager submits it. • Once everything is approved, the order is placed with a Pcard by the TMC Office Manager or through ARIBA by the FDOT Traffic Ops Office Manager (depends on Pcard purchase limit). • The IT Department must notify the TMC Office Manager when the order has arrived at 2300 or 3400 and provide the packaging slip.
Number of quotes required	Three if it is a larger IT purchase. If it is smaller (like cables), no quotes are needed but an IRR and justification are still required.
Vendors to get quotes from	State contract vendors must be used for IT stuff. Office Depot can be used for office supplies.
Money available each year	Budget has to be provided in advance of the fiscal year. Budget cuts occur frequently.
Staff in charge of ordering	The TMC Office Manager can help with Pcard purchases. The FDOT Traffic Ops Office Manager must complete ARIBA purchases.
Written justification requirements	Written justification is required for any IT materials. About one paragraph per item is sufficient. It should define why the item is critical and the consequences of not being approved to purchase it.
HW tags requirements	Yes, HW tags are required for any IT materials.

IRR requirements	Yes, an IRR is required for any IT materials.
IT's contact for purchase	TMC Office Manager.
Purchasing time frame	Pcard purchases must be ordered/received by June 15. ARIBA purchases must be received by June 30. Both are preferred to occur much earlier in the fiscal year.
Shipping address	Can ship to the TMC if it doesn't need an HW tag.

SERVICES

General purchase rules	Funds used to purchase any type of service. Purchase is made through ARIBA or Pcard (depending on card limit).
Examples of past purchases	Software license renewal, support costs, maintenance updates, anti-virus, extended warranties (Beware of buying extensions. Make sure it adds to the existing contract and doesn't double up service.) lawn care, carpet cleaning.
Purchasing process	<p>Purchases should be made as soon as possible, as needed, using the following process:</p> <ul style="list-style-type: none"> • The FDOT Traffic Ops Office Manager determines if funds are available. • The IT Department writes a justification and obtains three quotes. • The justification and three quotes are sent to the FDOT Traffic Ops Office Manager. • The FDOT Traffic Ops Office Manager obtains approval to make purchase for anything over \$100. • If an IRR is needed, the District TSM&O Resource Manager it. • Once everything is approved, the order is placed with a Pcard by the TMC Office Manager or through ARIBA by the FDOT Traffic Ops Office Manager (depends on Pcard purchase limit). • The IT Department must notify the TMC Office Manager when the order has arrived (an email has been received advising that the new service contract is active) at 2300 or 3400.
# of quotes required	Three
Vendors to get quotes from	State contractors must be used.
Money available each year	<p>Money available each year is largely based on what was available the previous year or based on need.</p> <p>Amount needed must be determined by June 15 prior to the start of the new fiscal year. Additional money can be obtained throughout the fiscal year if needed, if other departments are not using it.</p>
Staff in charge of ordering	The TMC Office Manager and the FDOT Traffic Ops Office Manager.

Written justification requirements	<p>Written justification is required. About one paragraph per item is sufficient. It should define why the item is critical and the consequences of not being approved to purchase it. Because these are recurring items, simply cut and paste the justification from the previous year.</p> <p>Note. There is a general objection to buying more than one year at a time unless it can be proved that there are significant savings in a multi-year contract.</p>
HW tags requirements	Since these are services, HW tags do not apply.
IRR requirements	Yes, an IRR is required for any IT materials.
IT's contact for purchase	TMC Office Manager
Purchasing time frame	Pcard purchases must be ordered/received by June 15. ARIBA purchases must be received by June 30. Both are preferred to occur much earlier in the fiscal year.
Shipping address	Shipping occurs via email. IT must be constantly in touch with the TMC Office Manager and Program Manager for any confirmation emails. If no emails are received, confirmation can be obtained by calling the vendor and asking for a verbal confirmation.

FDOT REPLACEMENT MONEY

General purchase rules	This funding is to purchase a replacement for an item already owned. The item must fill the same need, but it doesn't have to be an exact match (e.g. can be an upgrade).
Examples of past purchases	Furniture, dynamic message signs, Visio pad machines, servers.
Purchasing process	<p>Purchases must be made without delay using the following processes:</p> <hr/> <p>A. Work with the FDOT TSM&O Resource Manager.</p> <hr/> <p>B.</p> <ul style="list-style-type: none"> • FDOT Traffic Ops Office Manager determines if funds are available. • IT Department writes a justification and obtains three quotes. • The justification and three quotes are sent to FDOT Traffic Ops Office Manager. • FDOT Traffic Ops Office Manager obtains approval to make purchase for anything over \$100. • If yes for IRR, District TSM&O Resource Manager submits it. • Once approved, an order is placed through ARIBA by FDOT Traffic Ops Office Manager. <p>IT Department must notify the TMC Office Manager when the order has arrived at 2300 or 3400 and provide the packaging slip.</p>
Number of quotes required	Three quotes or the FDOT TSM&O Resource Manager can put out an advertisement and see who responds.
Vendors to get quotes from	Quotes must be obtained from a state approved vendor. Responses to advertisements can be from anyone.
Money available each year	Varies each year.
Staff in charge of ordering	FDOT Traffic Ops Office Manager for quotes. FDOT TSM&O Resource Manager for advertisements.

Written justification requirements It is required. One paragraph per item is sufficient. It must define critical reason for a purchase and the consequences of disapproval.

HW tags requirements - Yes HW tags are required, and IT will be returning an equivalent number of old HW tags to OIT.

IRR requirements - Yes IRR is required.

IT's contact for purchase FDOT TSM&O Resource Manager.

Purchasing time frame By fiscal year-end (June 30).

Shipping address If it is a large item, ship it to the TMC. If it is a small item, ship it to 3400.

TSM&O RESOURCE PROJECTS

General purchase rules	This funding can be used to purchase anything. It can include products, services, hardware or software.
Items of past purchases	For projects on highways- SolarWinds, servers, software, firewall, network access control, video wall upgrades.
Purchasing process	
# of quotes required - none	Items are purchased directly through the contractor.
Vendors to get quotes from	The contractor chooses the vendor.
Money available each year	It varies. IT must discuss needs with TSM&O Resource Manager well in advance for requested items.
Staff in charge of ordering	The contractor that wins the bid.
Written justification requirements	Requests included in TSM&O Resource contract. Prime contractors in charge. Watch for vendor's ownership.
HW tags requirements	Generally, no HW tags are required because the item is part of ITS on the road. Check with the TSM&O Resource Manager for exceptions.
IRR requirements - none	Check with TSM&O Resource Manager for exceptions.
IT's contact for purchase	FDOT TSM&O Resource Manager.
Purchasing time frame	It is decided by a prime contractor for purchases.
Shipping address	Items can be shipped to the TMC or wherever IT finds most convenient to ship.

AECOM SPECIAL SERVICES

General purchase rules Funding can be used to purchase items outside of other categories.

Examples of past purchases Projectors, blinds, libraries.

Purchasing process

- IT Support Manager, FDOT client discuss needs. Determine that this is the only way to procure.
- Write a letter to FDOT Operations Manager with 2 quotes, recommending the cheaper option.
- AECOM Operations Project Administrator signs and delivers the letter to the FDOT Operations Manager.
- FDOT Operations Manager issues AECOM a notice to proceed.
- AECOM Project Administrator orders through AECOM procurement.
- AECOM Project Administrator informs AECOM approvers about the purchase for FDOT; it will be fully reimbursed.
- IT must review the order if the quote was not used.
- AECOM Project Administrator includes expense in monthly invoice to FDOT once items are received.

of quotes required Two

Vendors to get quotes from Any vendor may be used. AECOM strongly prefers one already on their approved list.

Money available each year FDOT Operations Manager will advise of amount available for the fiscal year (July 1 – June 30).

Staff in charge of ordering

- AECOM Operations Project Administrator
- AECOM procurement office

Written justification requirements

HW tags requirements No HW tags are required, only IT tags.

IRR requirements No IRR is required.

IT's contact for purchase The FDOT client and AECOM Project Administrator

Purchasing time frame Purchases are fiscal year based (July 1 – June 30)

Shipping address Orders **must** be shipped to the TMC and labeled as AECOM to an AECOM staff person. Do not ship to 3400.

FDOT WORK PROGRAM MONEY

General purchase rules	Purchase cost is unlimited, depending on the state funding. The best to manage funds is to maintain a "wish list" when funding becomes available.
# of quotes required	Three.
Vendors to get quotes from	State contract vendors.
Staff in charge of ordering	TMC Program Manager.
Written justification requirements	Written justification is required.
HW tags requirements	Yes, HW tags are required for any IT materials.
IRR requirements	Yes, an IRR is required for any IT materials.
IT's contact for purchase	TMC Program Manager.
Shipping address	Can ship to the TMC if it doesn't need an HW tag.



7.27 Inventory Procedures

Document History

Version #	Date	Author	Changes
1.0	12/21/2023	Yana Neishlos	Initial Draft

Table of Contents

INVENTORY PROCEDURES OVERVIEW 5

- Receiving Equipment from OIT 5
- Receiving Equipment - except for OIT 5
- Exception Property 5
- Property Items with A Value under \$5,000 6

FDOT / ITS PROPERTY TRANSFER..... 7

RTMC INVENTORY PROCESS..... 8

FDOT INVENTORY SCANNING – FDOT INTERNAL (NH/HW AND IT TAGGED)..... 9

EQUIPMENT ISSUES 10

- Lost Equipment 10
- Inventory Change Control..... 10
 - Equipment Tracking Process 10
 - Moving Equipment 10
 - Retiring It Tagged Equipment Within RTMC 11
 - Process For Returning Nh Tagged Equipment to OIT 11
- Surplus of NH/HW Tagged Equipment 12

REFERENCES 13

ELECTRONIC MEDIA and DEVICE SANITIZATION PROCESS 14

- Process Overview 14
- Electronic Media and Device Sanitization Definitions..... 14
- Devices Exempt from Process..... 15

FDOT TOPICS and GUIDELINES 16

- FDOT Topic No. 350-090-310 Tangible Personal Property Procedure 16
- FDOT ITS Inventory Management Guidance..... 16
 - Purpose and References 16
 - Procedures 16
- FDOT Topic No. 350-090-005 Surplus Property Disposal Procedure..... 17

RMA PROCEDURES FOR ITS DEVICES 18

- Overview and Procedures 18
- IT Tagged ITS Devices..... 18
 - Sending an IT Tagged ITS Device out for RMA 18
 - Receiving a Repaired IT Tagged ITS Device 18
 - Receiving a Replaced IT Tagged ITS Device 18
- NH/HW Tagged ITS Devices 19

Sending an NH/HW Tagged ITS Device out for RMA 19

Receiving a Repaired NH/HW Tagged ITS Device 19

Receiving a Replaced NH/HW Tagged ITS Device 19

TSM&O PROPERTY TRACKING STANDARDS 20

Overview 20

Standards..... 20

Property Decals 20

Inventory Database..... 20

Property Tracking..... 20

INVENTORY PROCEDURES OVERVIEW

These guidelines outline the required steps for tracking the FDOT ITS equipment inventory within the District Four TSM&O Regional Transportation Management Center (RTMC).

Receiving Equipment from OIT

1. When equipment is received from OIT, ensure that an HW decal is properly affixed to the equipment.
2. Configuration of equipment received must be documented on the RTMC New PC Form by the IT Department. The RTMC New PC Form can be found in the D4 EXT TSM&O IT Property channel at: [DOCX File viewer | Microsoft Teams](#).

Receiving Equipment - except for OIT

All ITS equipment with a unit cost of \$5,000 or more requires an HW tag.

Exception Property

As defined by the FDOT procedure on Tangible Personal Property ([Topic No. 350-090-310](#)), exception property items with a value of less than \$5,000, are considered "attractive" and subject to risk of being stolen, or are covered by a lost or stolen insurance policy in accordance with the FDOT procedure on Property Insurance ([Topic No. 010-000-020-i](#)).

The exception property items listed below require an HW tag and must be recorded in the FLAIR Property Subsystem regardless of the unit cost.

- Workstations (i.e., laptops and personal computers).
- Digital Cameras.
- Monitors (larger than 32").

Note. "The property record for the number assigned to the central processing unit (CPU) may include the value of the monitor and any upgrades valued at \$1,000 or more that are added to the computer. Any components that are included in the value of the computer must be noted in the description field in FLAIR and provided in the description field on the bar code decal.

Property Items with A Value under \$5,000

District 4 TSM&O IT and Maintenance Departments track the following department owned equipment categories when HW tags are not required:

- Cisco IP Phone Wired and Wireless Phones.
- LCD Monitors (all types under 5,000 USD).
- VisioPad Analyzers.
- vBrick Decoders.
- Rack Mounted KVM Switches.
- Voice Routers.
- Room Alert Environment Analyzers.
- Printers.
- UPS (all types under 5,000 USD).
- Cameras (all types under 5,000 USD).
- Camcorders (all types under 5,000 USD).
- Projectors (all types under 5,000 USD).
- Cisco Wireless Routers.
- Video Wall Removable Parts.
- Field UPS Devices (all types under 5,000 USD).
- Layer 2 Field Switches.

All equipment that falls in the above categories is assigned a unique ITS tracking tag that starts with IT (Information Technology) or MT (Maintenance) and are entered in the Maintenance and Inventory Management System (MIMS).

FDOT / ITS PROPERTY TRANSFER

The IT Department uses MIMS to accurately track the location and party responsible for all FDOT equipment with an NH/HW tag and ITS equipment with an IT/MT tag.

1. When transferring equipment between contractors, all equipment should be received from the original contractor in full. All items must be checked and validated for resubmission to the new contractor.
2. IT Department updates MIMS to reflect the new location/owner and notifies the TSM&O Resource Manager of the changes via email.
3. The equipment is transferred to a new contractor.
4. When IT Department removes NH/HW equipment from service and prior to returning it to OIT, if not immediate, the equipment should be stored in a secure locked location.

RTMC INVENTORY PROCESS

Inventory Locations		Address	Phone
RTMC		2300 W. Commercial Boulevard, Fort Lauderdale, FL 33309	(954) 847-2785
TIMSO	FDOT Treasure Coast Operations Center	3601 Oleander Avenue, Fort Pierce, FL 34982	(561) 681-4380
FHP	Lake Worth Regional Communications Center	Turnpike Mile Marker 94, Lake Worth, FL 33416	(772) 742-8399
FDOT	Maintenance Yard	5548 Powerline Road, Fort Lauderdale, FL 33309	(954) 776-4300
Palm Beach Operations	Maintenance Yard	7900 Forest Hill Boulevard, West Palm Beach, FL 33413	(561) 432-4966
Vista Center		2300 N Jog Road, West Palm Beach, FL 33411	

1. Inventory is conducted twice a year starting on the first Friday of January and July and should be completed by the second Friday of the same month.
2. The Unit Custodian is responsible for overseeing the inventory process through coordination with the IT Support Manager. IT staff is responsible for conducting the actual inventory scanning.
3. Once the schedule has been received by the Unit Custodian and IT staff has been identified, the Unit Custodian will check the availability of an FDOT employee for transportation in the FDOT vehicle.
4. IT Support Manager is responsible for sending emails to the RTMC Operations Manager as follows:
 - a. Initial: A detailed plan once a schedule has been established.
 - b. Each day of inventory: Percentage complete and the plan for the following day.
 - c. Completion: Final report indicating percentage found and list of missing items (if any).

Note. Once scanning of a location is complete, data from scanner should be uploaded into MIMS.

FDOT INVENTORY SCANNING – FDOT INTERNAL (NH/HW AND IT TAGGED)

1. FDOT staff is responsible for obtaining a scanner and logging in using FDOT credentials.
2. Prior to starting inventory, IT staff generates a MIMS report to show the last location of all equipment to be scanned.
3. IT staff is to scan all equipment that has either a silver FDOT NH/HW tag and/or a white IT200## tag. (Note: Not all items will have both stickers. Scan a sticker that is affixed to the item or both if applicable.)
4. Equipment that cannot be located should be reported to the IT Support Manager to determine if it has been moved. If an IT Support Manager cannot locate the equipment, verify current location with the party that received the equipment. If an item has been moved, rescan the item and change the location in MIMS on the scanner to reflect the correct location
5. Once all equipment has been scanned, print another report from MIMS to document that all equipment has been properly located.
6. If an item cannot be located, it must be documented on the report and followed up with the last responsible party in MIMS and referred to the FDOT TSM&O Resource Manager.

EQUIPMENT ISSUES

Lost Equipment

1. All equipment, misdirected from its proper location, can and must be recuperated.
2. All equipment deemed lost must be reported to the TSM&O Resource Manager immediately.

Note. The IT Department Manager will be assigned PC equipment that has not been assigned to a specific user or location.

Inventory Change Control

Changes made to an IT-managed inventory, (e.g., servers, databases) must be noted and stored. Use the following process to keep a record of the equipment location.

<p>Equipment Tracking Process</p> <p>This process monitors equipment locations, which will help with the year-end inventory.</p>	
1.	If a laptop or other item is taken out of a truck or office temporary, the lending party must have the borrower sign off for temporary responsibility by utilizing the equipment signoff sheet, which can be found in the D4 EXT TSM&O IT Property channel at: PDF File viewer Microsoft Teams .
2.	All relevant information needs to be supplied on the equipment signoff sheet.
3.	When the item is returned to its original location, the equipment signoff sheet is updated.
4.	Store the original equipment signoff sheet in a file.
<p>For permanently transferring a piece of equipment from one contractor to another, see: FDOT / ITS Property Transfer section.</p> <p>Note. The inventory is not updated if the equipment is only temporarily located away from where it belongs permanently.</p>	
<p>Moving Equipment</p> <p>If equipment changes locations, update the item's permanent location in one of the following:</p>	
1.	<ul style="list-style-type: none"> • Handheld scanner.
2.	<ul style="list-style-type: none"> • Inventory software (MIMS).
<p>Note. For NH/HW and IT/MT tagged items, if the equipment owner changes, MIMS needs to be updated (see FDOT / ITS Property Transfer section).</p>	

Retiring It Tagged Equipment Within RTMC	
1.	When a piece of equipment that has an IT tag needs to be retired, the IT Department will retire it in MIMS (pending approval) and send a list of the retired equipment via e-mail to the FDOT TSM&O Resource Manager for review.
2.	Once approved, the TSM&O Resource Manager will permanently retire the equipment in MIMS.
3.	The part may be discarded by the IT Department.
<p>Note. All electronic devices and media must be sanitized prior to disposal. Refer to SOG Section 7.27.01.</p>	
Process For Returning Nh Tagged Equipment to OIT	
<p>OIT is not responsible for surplus of HW tagged equipment (see Surplus of HW Tagged Equipment below).</p>	
1.	<p>IT Department receives new equipment from FDOT OIT (see section receiving Equipment from OIT).</p> <ul style="list-style-type: none"> Identify placement of new equipment and install.
2.	<p>IT Department gathers old equipment for return to FDOT OIT.</p> <ul style="list-style-type: none"> IT Department must confirm configuration of equipment to be returned. All equipment that is set to be returned to OIT must be approved by the TSM&O Resource Manager. Once approval is obtained, the TSM&O Resource Manager will return to OIT
3.	Provide list of equipment to FDOT TSM&O Resource Manager for approval prior to sending back to OIT.
4.	<p>Once approved, email the NH numbers of the equipment being returned to OIT (currently Pam Zain) and copy the TMS&O Resource Manager.</p> <ul style="list-style-type: none"> IT Department coordinates with OIT to return equipment.
5.	Prior to returning, IT Department must scan the equipment (3400 (surplus) and update in MIMS.
6.	Once the equipment is inspected and cleared for return, pictures must be taken of the entire piece of equipment showing that none of the components are missing using the RTMC Surplus PC Returned form. RTMC Surplus PC Form can be found in the D4 EXT TSM&O IT Property channel at: DOTX File viewer Microsoft Teams .

Surplus of NH/HW Tagged Equipment

1. The IT Staff will fill out form no. 350-090-05, Certification of Surplus Property for the equipment that will be 'surplused' (with the information in steps a.-d. below only), print, scan, and submit it to the RTMC IT Support Manager via e-mail for approval. The Certificate of Surplus Property form can be found in the D4 EXT TSM&O IT Property channel at: [PDF File viewer | Microsoft Teams](#).
 - a. Inventory Control # (Column 2). This will either be the FDOT/FLAIR asset tag number or the serial number. If the FDOT/FLAIR number is missing, enter the serial number.
 - b. QTY (Column 3). Enter a numeric value for the quantity per line number.
 - c. Description of Property (Column 4). Enter the description of the property as it appears in MIMS.
 - d. Cond (Column 6). Enter one of the following condition codes (alpha character only) for the property:

• E – Excellent	• F – Fair	• S – Scrap
• G – Good	• P – Poor	
2. Once approved, RTMC IT Support Manager will save the Certification of Surplus Property form on D4 EXT TSM&O IT Property channel and submit it to the TSM&O Resource Manager for completion.
3. FDOT TSM&O Resource Manager will complete the form, to include obtaining the proper signatures, and upload it to the D4 SharePoint site for advertisement to other Districts in the State that equipment is available for use.
4. This advertisement will be posted for 2 weeks. After expiration, TSM&O Resource Manager will coordinate with the Surplus Property Coordinator for pickup of the property and complete form no. [350-090-06, Surplus Property Receipt](#).
5. Once the property is removed from the building, IT Department can decommission it from MIMS.

Note: All electronic devices and media must be sanitized prior to surplus. Refer to SOG Section 7.27.01.

REFERENCES

- Topic No. 325-000-002 Transportation Technology Manual, Chapter 11, Electronic Device and Media Sanitization - SOG Section 7.01.05
- Topic No. 350-090-310 Tangible Personal Property Procedure - SOG Section 7.27.02
- Intelligent Transportation Systems (ITS) Inventory Management Guidance Document - SOG Section 7.27.03
- Topic No. 010-000-020 Property Insurance Procedure SOG Section 7.27.05

ELECTRONIC MEDIA and DEVICE SANITIZATION PROCESS

Process Overview

The [Electronic Device and Media Sanitization Process](#) document ensures compliance with the Florida Department of Transportation (FDOT) Transportation Technology Resource User's Manual (Topic No. 325-000-002), [Chapter 11 Electronic Device and Media Sanitization](#). This process applies to FDOT District 4 (D4) Transportation Systems Management and Operations (TSM&O).

Electronic Media and Device Sanitization Process document shall be used to ensure compliance for the sanitization of electronic media and devices exists under FDOT D4 TSM&O's area of responsibility. The document is regularly updated and found at the following link: [Electronic Media and Device Sanitization Process](#).

Electronic Media and Device Sanitization Definitions

Degaussing	The exposing of magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. Degaussing can be an effective method for purging damaged media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. Any degausser equal to the Garner Products HDTD-8200 degausser, issued to the Department's OIT Offices, shall be used for this task. This type degausser renders magnetic media and devices inoperable after degaussing.
Disposal	The act of discarding media or devices from Department use in a manner short of destruction. FDOT Topic No. 350-090-005 Surplus Property Disposal Procedure, defines the practices that shall be followed for the proper disposal of electronic media vice properties.
Destruction	The highest level / ultimate form of sanitization. The result will ensure that media cannot be reused as originally intended; information is impossible to recover or expensive. Physical destruction can be accomplished with a variety of methods, i.e., disintegration, incineration, pulverization, shredding, melting, sanding, d chemical treatment.
Erase	Process will render magnetically stored information or data irretrievable by normal means.
Reimage	The process of removing and deleting any previously stored data and software on a computer and reinstalling, in its place, pre-configured operating system and software.
Return Merchandise or Material Authorization (RMA)	A transaction whereby the recipient of a defective product arranges its return to the supplier to have the product repaired or replaced or to receive a refund or credit for another product from the same retailer or corporation.
Sanitizing	Using a utility that provides a minimum of three passes of overwriting all addressable locations with a character, its complement, then a random character and verifying. DOD 5220.22-M requirements accomplish this. This includes erasing data and/or reformatting magnetic tape media. FDOT D4 TSM&O Unit will utilize Active@Killdisk Enterprise to accomplish this task.

Surplus	Electronic media and devices that are no longer used by the Department and shall not be owned by the Florida Department of Transportation. These items are typically donated, or RMA returns to other entities or organizations outside the Florida Department of Transportation or are destroyed to prevent further use.
Transfer	Changes in ownership of electronic media and devices from one Cost Center to another Cost Center. This can be within or across Districts. Ownership of transferred items always remains within the Florida Department of Transportation's chain of custody.

Devices Exempt from Process

Some ITS Devices only collect data that is subject to public record and therefore are not subject to sanitization. This device list must be updated when new devices utilized within ITS come online that conform to the previous statement. These devices are:

- Closed-circuit television (CCTV)
- Encoders
- Decoders
- Video Walls
- Media Converters
- Vehicle Detection Systems (VDS)
- Terminal Servers for field devices
- Dynamic Message Signs (DMS)
- Signal Controllers
- Signal Cabinet Equipment
- Adaptive Signal Control Equipment

FDOT TOPICS and GUIDELINES

FDOT Topic No. 350-090-310 Tangible Personal Property Procedure

Section 7.27.00 references the FDOT Procedure for Tangible Personal Property. This document is updated on a regular basis and can be found at the following link: [FDOT Topic No. 350-090-310 Tangible Personal Property Procedure](#).

FDOT ITS Inventory Management Guidance

Purpose and References

This document defines requirements regarding accountability and reporting related to ITS tangible personal property and infrastructure assets within the Florida Department of Transportation.

The references are:

- Tangible Personal Property, Office of Comptroller and General Accounting, [Topic No. 350-090-310](#).
- ITS Maintenance Scope of Services.

Procedures

Tangible Personal Property

- For control, ITS equipment within a Transportation Management Center (TMC) or TMC backup site operated by FDOT, excluding any warehouse area will be considered tangible personal property and will follow [Topic No. 350-090-310](#). A Transportation Management Center is a building housing at least one FDOT owned workstation permanently connected to the ITS Network for purposes of operating the Freeway Management System.
- Video wall items must be tagged individually due to requirement that the property group records only contain items purchased within one fiscal year.
- Property items valued under \$5,000 and not considered Exception Property ([Topic No. 350-090-310](#)) are not required to be recorded in the FLAIR Property Subsystem for control or tracking purposes. Districts can record these items in the FLAIR Property Subsystem for control and tracking purposes on an optional basis.
- Tangible personal property must be disposed of in accordance with Surplus Property Disposal, (Office of Support Services [Topic No. 350-090-005](#)).

Infrastructure Assets

- ITS equipment outside the Transportation Management Center (TMC) or TMC back up site operated by FDOT, including any warehouse area will be considered as infrastructure and shall be inventoried with the District's Maintenance Management Inventory Database at least once each fiscal year. A Transportation Management Center is a building housing at least one FDOT owned workstation permanently connected to the ITS Network for purposes of operating the Freeway Management System.
- District Maintenance Management Inventory Database device records must include but are not limited to:
 - Device location, number, and type.

- Model and serial number.
- Manufacturer.
- Ownership date.
- The Facility Management System database will generate reports with the above information.
- Infrastructure assets, being surplus, must be documented. A review team composed of two employees must certify infrastructure as surplus using Form No. 350-090-05. Property serial numbers shall be used for inventory and surplus control. Certification forms must be completed for all surplus property and must contain as much detailed information about the property as possible. A property disposition file must be maintained for all surplus property. The file will contain records reflecting the disposition of all items of property. The method of disposition must be noted for each item. A detailed list of property delivered to recycling operators, landfill operations, or placed in dumpster or scrap bins should be maintained with receipts signed by a witness as supporting documentation for disposal.

ITS Equipment/Systems List

In TMC or TMC backup site with HW tag (items on ITS Network):	<ul style="list-style-type: none"> ● Video wall system (controller, video wall display, bulb) ● Workstation system ● Servers ● Video encoders/decoders ● Mobile devices (Tablet, Smartphone, Radio)
In TMC or TMC backup site with NH tag (Items on OIS network):	<ul style="list-style-type: none"> ● Workstation system ● Servers
Field Infrastructure (Tracked through District Maintenance Management Inventory Database)	<ul style="list-style-type: none"> ● Roadway <ul style="list-style-type: none"> – CCTV – Traffic Detection Systems – RWIS – DMS – HAR – Field Hub – Ramp Metering System (Signal, controller, detection) – Field Switch – Generator
	<ul style="list-style-type: none"> ● Warehouse (spare parts, spare units, generators)

FDOT Topic No. 350-090-005 Surplus Property Disposal Procedure

Sections 7.27.01 and 7.27.03 reference the FDOT Procedure for Surplus Property Disposal.

This document is updated on a regular basis and can be found at the following link: [FDOT Topic No. 350-090-005 Surplus Property Disposal Procedure.](#)

RMA PROCEDURES FOR ITS DEVICES

Overview and Procedures

This SOP Section outlines the steps for sending an ITS device out for RMA, receiving a repaired ITS device from a vendor, and receiving a replaced ITS device from a vendor.

The procedures below are separated by the tag type (i.e., IT, NH, or HW) affixed to the ITS devices. IT tagged ITS devices have a white decal affixed to them; and NH/HW tagged ITS devices have a silver decal affixed to them.

IT Tagged ITS Devices

Sending an IT Tagged ITS Device out for RMA

- A.**
 1. The IT Workstation team removes the decal from the ITS device.
 2. The IT Workstation team sends the ITS device to the vendor for RMA.

Receiving a Repaired IT Tagged ITS Device

- B.**
 1. When a repaired ITS device is received from a vendor, the IT Workstation team sends an email notification to the IT Security Manager, requesting a new decal with the same information that was on the old decal.
 2. The IT Workstation team properly affixes the new decal to the repaired ITS device and updates MIMS accordingly.

Receiving a Replaced IT Tagged ITS Device

- C.**
 1. When a replaced ITS device is received from a vendor, the IT Workstation team sends an email notification to the to the IT Security Manager, requesting a new decal with new information that matches the new or refurbished ITS device.
 2. Once the new decal is received, the IT Workstation team properly affixes it to the replaced ITS device, and updates MIMS accordingly, to include decommissioning the old decal.

NH/HW Tagged ITS Devices

Sending an NH/HW Tagged ITS Device out for RMA

1. The IT Workstation team sends an email notification to the TSM&O Resource Manager, which includes all pertinent information for the ITS device that needs to be sent out for RMA (e.g., device name, decal info, etc.).
- A. 2. The TSM&O Resource Manager responds to the email, to let the IT Workstation team know that the ITS device can be sent out for RMA.
3. The IT Workstation team removes the decal from the ITS device and retains it for delivery to the TSM&O Resource Manager.
4. The IT Department sends the ITS device to the vendor for RMA.

Receiving a Repaired NH/HW Tagged ITS Device

- B. 1. When a repaired ITS device is received from a vendor, the IT Workstation team sends an email notification to the TSM&O Resource Manager, requesting a new decal with the same information that was on the old decal.
2. The IT Workstation team properly affixes the new decal to the repaired ITS device, and updates MIMS accordingly.

Receiving a Replaced NH/HW Tagged ITS Device

- C. 1. When a replaced ITS device is received from a vendor, the IT Workstation team sends an email notification to the TSM&O Resource Manager, requesting a new decal with new information that matches the new or refurbished ITS device.
2. Once the new decal is received, the IT Workstation team properly affixes it to the replaced ITS device, and updates MIMS accordingly.
3. The TSM&O Resource Manager decommissions the old decal in MIMS.

TSM&O PROPERTY TRACKING STANDARDS

Overview

As stated in Section 2.4 of the FDOT procedure on Tangible Personal Property, [Topic No. 350-090-310](#), “Occasionally, a District, Office, or the Turnpike Enterprise may determine that additional property items with values under \$5,000 should be recorded in the FLAIR Property Subsystem for control or tracking purposes. These types of property items should be limited in number. They should only be recorded in the FLAIR Property Subsystem unless there is a better way to track the property.”

These Standards outline the required steps for tracking the following FDOT D4 TSM&O property items by TSM&O property decals in the local Maintenance Inventory Management System (MIMS):

- Property items that are not tracked by FDOT property decals.
- Property items with a purchase value above \$300 and below \$5,000.
- Property items below \$300 but are considered to have an attractive value.

Standards

Property Decals

Upon procurement of IT devices, the TSM&O Purchasing Agent performs the following:

- Identifies assets to be tracked by FDOT property decals.
- Submits the necessary requests to create and print the FDOT property decals.
- Submits assets that are not be tracked by FDOT property decals to the IT Support Manager.

Inventory Database

Properties are to be entered in the local MIMS. Assets are to be approved and the status is to be updated to reflect the correct standing of use.

Property Tracking

All property items not tracked by FDOT property decals and have a purchase value over \$300 and below \$5,000, are to be tracked by TSM&O property decals. Some property items with a purchase value below \$300, but having an attractive value, must also be tracked by TSM&O property decals.

The list of property items with an attractive value, includes but is not limited to:

- Monitors (31 inches and below).
- Laptops.
- Bluetooth headphones.
- Workstations and other easily removable networking devices.

Property deployed or moved should be audited with the local inventory system; a location should be modified to reflect the current location. A yearly property audit is performed using MIMS and the FDOT Property Audit System.



7.28 Emergency Procedures

Table of Contents

EMERGENCY PROCEDURES	4
Coronavirus Scenarios.....	4
Scenario A.....	4
Scenario B.....	4
Scenario C	5
THE HURRICANE IMPACT PLAN	6
Introduction	6
Purpose.....	6
Scope of Hurricane Plan	6
Definitions – Track Forest Cones.....	6
Track Forecast Cone	6
5-Day Track Forecast Cone.....	6
3-Day Track Forecast Cone.....	6
FULL DATACENTER POWER SHUTDOWN TECHNICAL PLAN	7
Assumptions.....	7
Timeline.....	7
Project Team	8
Communication Plan.....	9
Prior to the Outage.....	9
After the Outage Procedures’ Completion	10
Relocation Procedures.....	11
To Be Completed 48 Hours before Shutdown	11
After the Shutdown	11
After the Startup.....	11
Shutdown Procedures.....	12
Post Disaster Restoration Procedures.....	15
Post Test Outage After-Action Items.....	15
Post Main Outage After-Action Items.....	15
WORKSTATIONS – IT ON-CALL STANDARD OPERATING PROCEDURE (SOP)	17
Purpose.....	17
How to Access.....	17
Reference for Operations.....	17
Recommended contact Path for Operations.....	17
Ticket Creation	17
Initial Troubleshooting	17
On-Site Troubleshooting (if required).....	18
Workaround Documentation	18
Communication Protocol.....	18
Post-On-Call Review.....	18

Document History

Version #	Date	Author / Reviewer / Editor	Changes
1.0	2/07/2024	Yana Neishlos	Initial Draft
1.1	5/07/2024	Aaron Rapp / Yana Neishlos	Shutdown Plan included
1.2	5/29	Aaron Rapp / Yana Neishlos	Included IT ON-CALL standard operating procedures from 7.18.04

EMERGENCY PROCEDURES

Coronavirus Scenarios

If telecommuting is required, the following scenarios and procedures will be used to instruct and inform both management, and personnel, on the steps to take to achieve each scenario.

Items in bold will be considered "pre-requisites" to executing the plan and are not resources currently on-hand. This plan references the "TMC Operations Plan: Continuing Operations under Corona Virus Threat."

Scenario A

In this scenario, it is expected that operations continue, but spread among other offices within the Broward RTMC.

- 2 Stations in Control Room
- Room 110
- Room 112
- Room 114
- Room 115
- Room 116

When activated, the IT department will setup stations with the following configuration:

1. Workstation
 - HP 705G4 R7
 - Image
 - SunGuide
 - Sidebar
 - Outlook
2. Use existing monitors. (Minimum of two.)
3. Handheld Radio.
4. Configure existing video wall monitors for primary incidents.

Scenario B

Setups for Scenario B are identical to Scenario A, but with less required stations.

Scenario C

It is expected that operations continue, but with "Operators" working from their homes.

If activated, the following will take place. A 24-hour lead time will be required, after resource procurement, for this plan.

1. Decision will be made whether all 30 operators will receive devices.

If an answer is **Yes**, see **1.a**. If answer is **No**, see **1.b**.

- a. All 30 operators will receive equipment.

- 21 laptops will be purchased.
- 10 handheld radios will be purchased.
- Once laptops are received, they will be labeled and imaged with the following:
- Outlook
 - SunGuide Terminal Server Shortcut
 - Cisco VPN
 - Copy of VPN instructions on desktop
 - Copy of Terminal Server instructions on desktop
- Handheld radios will be provisioned with FirstNet and labeled with phone number.
- SunGuide terminal servers (coronavirus.smartsunguide.com), will be turned on. 16GB of additional RAM will be added.
- Barco Wall and IT Wall Servers will be shut down in VMware.
 - Barco XX
 - IT Wall XX
- Once laptops are ready, a log will be created to track which laptops and their owners/operators.
- Once added to the log, the Operator will login to the machine using their Smartsunguide credentials.
- A handheld radio will be assigned and logged to each operator.
- After successful login, IT staff will ensure their login works before they depart.
- Once the above configurations are completed, an Operator will receive further instructions from the Operations Management.

- b. Equipment will be distributed in the same configuration as **1(a)**, except only allowing the maximum amount of equipment on hand. (i.e., 9 laptops and 15 radios, would result in 9 operators receiving equipment.)

- Operators are expected to use their home internet to conduct business.
- Schedules and shifts will be created by Operations Management.

2. In either event, the helpdesk hunt group will be altered to ring all IT department phones at once. The helpdesk phone number will be included in the VPN instructions on the desktop.

THE HURRICANE IMPACT PLAN

Introduction

The Hurricane Impact plan is a comprehensive document that describes the series of critical action steps to be executed in the event of an impending hurricane. This plan serves as a strategic blueprint, offering clear and decisive guidance and response to this formidable natural disaster. The plan will ensure the safety and well-being of our personnel and the safeguarding of our valuable assets.

Purpose

The Hurricane Impact plan provides a comprehensive roadmap for the TSM&O IT Department to follow in the event of an impending hurricane. Its primary objective is to guarantee the seamless continuity of our critical operations, even in the face of the imminent threat posed by a hurricane.

Scope of Hurricane Plan

The development of this Hurricane Impact plan is tailored for the TSM&O IT Department to ensure the operational continuity during hurricane events. This plan is a dynamic and responsive document, tied to the ever-evolving track forecast cone of an approaching hurricane.

Definitions – Track Forecast Cones

Track Forecast Cone

The "forecast cone" is the graphical representation illustrating the likely path of the central point of a tropical cyclone that displays its anticipated movement and **trajectory**¹.

5-Day Track Forecast Cone²

IT Department will implement a temporary suspension of all Change Orders across all areas of its responsibility. During this period, regular Change Orders, involving the planned modifications and updates, will not be processed. Emergency Change Orders, pertaining to critical and time-sensitive issues, will be permitted.

3-Day Track Forecast Cone³

CyberKey access will be extended to a duration of seven days. Hence, users with CyberKeys will have an extended window of seven days to access secured areas before requiring reauthorization.

¹ <https://www.nhc.noaa.gov/aboutcone.shtml>

² <https://www.nhc.noaa.gov/gtwo.php?basin=atlc&fdays=5>

³ <https://www.nhc.noaa.gov/gtwo.php?basin=atlc&fdays=2>

FULL DATACENTER POWER SHUTDOWN TECHNICAL PLAN

This document will be used for a full datacenter power shutdown at the District 4 RTMC.

Assumptions

The following services/applications will not be available during this shutdown.

• Test FHP/Davie Fire Radio (TEST THIS)	• FDOTD4Traffic.com	• Arterial Cameras
• InService App	• MIMS (internal/external)	• ITS WAN connection
• InService Manager	• iVDS	• RTMC VPN
• InService MOT	• External API that BSO uses to view cameras	• SMTP Server
• InService SIRV	• TOQC	• Maxview
• SIRV App	• SELS/ELS	• SIEM
• 595express.info	• TrafficCast viewing of cameras	• WWED
	• SolarWinds Orion	

The Emergency Operations Center (EOC) at District 4 HQ will be available for Operational needs during this outage.

The remaining services will be moved to the Treasure Coast Operations Center datacenter through the below procedures.

The following items will be set up at the EOC to facilitate the operators and services to be run from there:

- 6 Operator stations with 2 monitors
- 1 Virtual Host that will house the CMS Pro server for the EOC video wall.
- 1 Cisco phone per operator

A VCenter host will be moved down to the EOC and run on VLAN 3. This will house the CMS Pro server for the EOC video wall.

A Cisco switch will be configured for use at the EOC for workstations and phones.

Timeline

1. Outage #1 (Test Outage) – Sunday, November 12th
2. Saturday, November 11th @ 08:00 - Move operators to EOC. Set them up and verify things are working as intended. The Workstation team will send a notification to RTMC IT Support Manager of completion.
3. Saturday, November 11th @ 09:00 - Shutdown procedures will begin.
4. Saturday, November 11th @ 10:30 - After shutdown procedures have been completed, verification will begin and be documented. Any assumptions that behave differently than expected will be thoroughly investigated and resolutions will be investigated.
5. Saturday, November 11th @ 12:00 - Startup procedures should be started. Application verification will be performed.

6. Saturday, November 11th @ 14:00 - Move operators back from EOC. Set them up and verify things are working as intended. The Workstation team will send a notification to RTMC IT Support Manager of completion.
7. Outage #2 (Main Outage) – Friday, January 12th – Monday, January 15th
8. Friday, January 12th @ 08:00 – Setup workstations, VCenter Host, and other appropriate items at the EOC. Setup will be completed, and configurations verified by the end of the business day.
9. Friday, January 12th @ 19:00 – Move operators to EOC. Set them up and verify things are working as intended. The Workstation team will send a notification to RTMC IT Support Manager of completion.
10. Friday, January 12th @ 20:00 – Shutdown procedures will begin.
11. Friday, January 12th @ 22:00 – After shutdown procedures have been completed, verification will begin and be documented. Any assumptions that behave differently than expected will be thoroughly investigated and resolutions will be investigated. Monitoring will begin.
12. Friday, January 12th @ 00:00 – Monitoring of operators, applications, services, and status of electrical work will begin. Monitoring will continue throughout the outage window.
13. Monday, January 15th @ 13:00 – Startup procedures should be started. Application verification will be performed.
14. Monday, January 15th @ 16:00 – Move operators back from EOC. Set them up and verify things are working as intended. The Workstation team will send a notification to RTMC IT Support Manager of completion.

Project Team

Project teams comprises the following individuals:

- District 4 TSM&O Program Engineer
- District 4 TSM&O Resource Manager
- District 4 TSM&O Information Technology Manager
- RTMC Project Manager
- RTMC Assistant Manager (AECOM)
- RTMC Assistant Manager (WSP)
- RTMC Outage Project Manager
- RTMC IT Support Manager

Communication Plan

There are several stakeholders that should be informed of this outage.

The Outage Project Team will remain on all communications regarding the outage.

Prior to the Outage

For a planned outage, the following procedures will be used.

1. **One week**, or more, prior to the outage, the TSM&O Resource Manager will ensure a notification is sent to all FDOT District Program Engineers, informing them of the outage, impacted areas, and the timeline for the outage.
2. **One week, or more**, prior to the outage, the TSM&O Resource Manager will ensure a notification is sent to the following stakeholders, informing them of the outage, what will be affected, and the timeline for the outage.

TERL	D4 HQ Facilities
Tolls Email List	ITS Maintenance
District 4 Management	Central Office ITS
Total Traffic Networks Contacts	The people requiring it - This notification will include instructions on changes in work schedules, VPN Access instructions, and work locations during the outage.

3. **Three days** prior to the outage, an RTMC Manager will ensure a notification is sent to the following stakeholders, informing them of the outage, impacted areas, and the timeline for the outage, including procedural changes required during this outage.
 - a. Districts 1, 5, 6, and Turnpike.
 - b. Road Ranger Project Managers
 - c. SIRV Project Managers
 - d. FHP Regional Communications Center
4. **One hour** prior to the shutdown, the RTMC Outage Project Manager will send a notification to all the previous stakeholders in steps 1-3, notifying them that the outage is about to take place.
5. If any of the outage assumptions or timelines change during the outage duration, the RTMC Outage Project Manager will alert the previous stakeholder list of those changes.
6. When notification is received that the outage is ending, the RTMC Outage Project Manager will notify the project team, as well as the following lists → **Turnpike Email List**

This notification will recall all appropriate project members to standby for “**Startup Procedures**”.

After the Outage Procedures' Completion

After startup procedures are completed and service restoration has been verified, the RTMC Outage Project Manager will send a notification to all previous stakeholders in steps 1-3, notifying them that the outage has been completed and all services should be available.

Sample Communication:

FDOT District 4 TSM&O Notification

Name of Notification	RTMC Outage #2
Date and Time of Outage	Friday, January 12th, 2024 7:00 PM - Tuesday, January 16 th , 2024 2:00 AM
Services that will be affected	<u>The following will be unavailable:</u> 595Express.info Website FDOTD4Traffic.com Website iVDS/DIVAS ITS WAN Connection MIMS RTMC VPN Viewing of D4 cameras from anywhere outside the D4 network (exception: D6).
Operational Changes	<u>The following operational changes will be required:</u> <ol style="list-style-type: none"> 1. The main number of (954) 847-2777 should continue to function; however, if issues are being experienced with this number, please try (772) 742-8394. 2. All ITS related activities, including testing and integration, shall not take place during this outage timeframe. I TS activities can resume after receiving confirmation from District 4 that the outage has been completed.

Relocation Procedures

One hour prior to the start of the shutdown procedures, the RTMC IT Support Manager will coordinate with the IT team and the Operations team to move all necessary operators to the EOC.

To Be Completed 48 Hours before Shutdown

- Moving SunGuide to TIMSO
- Putting in ticket to AT&T to forward main phone number to backup phone number
- Move CMS Pro backup server to temporary host at EOC.
- Failover ITSQL instance to node in TIMSO
- Failover Milestone Recording Server. SRM: Management Server move
- Move FSMO roles to TIMSO
- Move the primary ISE to TIMSO

After the Shutdown

The following are the systems to be tested after a Shutdown:

Sending and Receiving phone calls to Control Center	IntraSmart	DNS (Including Cisco Umbrella connection)	ISE
FMS SunGuide Application	SELS/ELS	VCenter	Password Manager – Read-Only
Internet Connectivity	Sidebar	Storage Shares	FHP/Davie Fire Radio
Zello	Barco Wall	VPN Connection	Arterial Cameras

After the Startup

The following are the systems/applications to be tested after a Startup:

Sending and Receiving phone calls to Control Center	vCenter	DNS (Including Cisco Umbrella connection)
FMS SunGuide Application	File Shares	Password Manager Pro
AMS SunGuide Application	VPN Connection	Milestone xProtect
Zello	IntraSmart	Comcast Cable
SELS/ELS	Printing	Internet Connectivity
Sidebar	Wireless Access	ISE
Barco Wall	Cyberlock	IntraSmart
		FHP/Davie Fire Radio

Shutdown Procedures

Phase	IT Department	Procedural Steps
0	Applications	<p>Ensure SELS/ELS are posted at \$0.00 tolls and ready for shutdown.</p>
1	Network	<p>Cisco Unified Communication Manager (CUCM)</p> <p>In case of a potential crash, the Publisher on the CUCM must be manually shut down. With the two CUCM Subscribers up and running, the CUCM will keep working, but no changes can be made. The steps below can be completed in 3-5 minutes.</p> <ol style="list-style-type: none"> 1) SSH to Call Manager 2) Use OS admin for the CUCM. 3) Issue command: utils system shutdown. <p>Wireless Controller</p> <ul style="list-style-type: none"> – Log into the CIMC
1	Workstations	<ol style="list-style-type: none"> 4) Ensure that the main Video Wall in the Control Room is safely powered down via controller. <p>Power down the following:</p> <ul style="list-style-type: none"> – All unused consoles to reduce power consumption. – All NEC monitors throughout the building to reduce power consumption. – All Barco NDNs throughout the environment to reduce power consumption. <p>Ensure the Intrasmart website is hosted from Timso server. Intrasmart DNS entry needs to have IP of Timso Intrasmart server.</p> <p>After replication, → refresh Intrasmart website to confirm site functionality.</p>
1	Database Admin.	<p>Failover SunGuide to TIMSO.</p> <p>Export SELS/ELS databases. Import to TIMSO instance of applications. Confirm this process is completed before continuing.</p>
1	Security	<ol style="list-style-type: none"> 5) Okta Active Directory. <ul style="list-style-type: none"> – Ensure that the service is running on the agent server at TIMSO. <p>Internet communication to Okta tenant https://smartsunguide.okta.com is required.</p> <p>Okta Radius.</p> <ul style="list-style-type: none"> – Ensure the service is running on the agent server at TIMSO. <p>Internet communication to Okta tenant https://smartsunguide.okta.com is required.</p> <ul style="list-style-type: none"> – Password Manager.

Phase	IT Department	Procedural Steps
0	Applications	<p>Ensure SELS/ELS are posted at \$0.00 tolls and ready for shutdown.</p> <ul style="list-style-type: none"> – Verify that the read-only Password Manager server has service running and that it can access the encryption key located on the Distributed File System (DFS) – Edit Key file to point to path of encryption Key on DFS <p>Login to backup password manager system.</p> <p>The Password Manager is Okta tenant dependent. If communication with Okta fails:</p> <ul style="list-style-type: none"> – Bypass Security Assertion Markup Language (SAML) Single Sign-On (SSO) – Login with local database credentials. – ITSQL Instance. – Execute a SQL command to perform a graceful failover to the replica located at TIMSO, before gracefully shutting down the replicas at the RTMC. – Milestone Recording Server. – Verify failover of the recording server to the server located at TIMSO. – Shutdown of the ISE. <p style="padding-left: 40px;">a) Move from Primary to Secondary</p> <p>NOTE: The Milestone Management server is located at the RTMC, and the database is on ITSQL Instance. To access the database, a Management server needs to be put in place at TIMSO.</p>
1	Servers	<p>Transfer the Domain Flexible Single Master Operation (FSMO) Roles to TIMSO</p> <ul style="list-style-type: none"> 6) Determine the current location of the FSMO roles by using the netdom query fsmo command. Sample output below: 7) Transfer all FSMO roles to TIMSO.
1	Servers	<p>Start Powering Down Systems</p> <p>CAUTION: Do not shutdown the storage until all other systems have been powered down.</p> <p>NOTE: All databases (where applicable) must be gracefully shut down prior to the server being powered down (SQL instances to be attached).</p> <ul style="list-style-type: none"> • ITSQL • SolarWinds Orion <p>8) Ensure that all relevant SunGuide databases are transferred to TIMSO and confirm functionality with the Applications Team.</p> <p>Ensure that all needed applications are transferred to TIMSO and confirm functionality with the application owners.</p>

Phase	IT Department	Procedural Steps
0	Applications	<p>Ensure SELS/ELS are posted at \$0.00 tolls and ready for shutdown.</p> <ol style="list-style-type: none"> a. Okta Radius (Security). b. Okta Active Directory (Security). c. Password Manager Read-Only (Security). d. Milestone Recording Server (Security). e. DFS (Password Manager Dependent) (Security and Servers). f. Network Time Protocol (NTP) (Servers). g. Cisco Umbrella OpenDNS (Security).
		<p>Before proceeding to Phase 2, the DRC must confirm functionality of all SunGuide databases with the Applications Group as well as confirm functionality of all needed applications with the application owners, as outlined in steps 1. & 2. above.</p>
2	Servers	<ol style="list-style-type: none"> 9) Log in to vSphere and begin performing a graceful shutdown of all systems. Once all systems on a particular host are down, log in to the ILO of that host and gracefully shutdown the host. <p>Note. Record which host the local vCenter is hosted on. This host and the vCenter appliance will be the last to go down and the first to come up post-disaster.</p> <ol style="list-style-type: none"> 10) Log in to the storage array's and perform a shutdown.
2	Workstations	Power down all remaining consoles.
2	Database Admin.	Shutdown two servers.
2	All Depts.	<p>Unplug power from wall on all critical systems.</p> <ul style="list-style-type: none"> • Barco Wall • Console Devices • Office Machines • Host Servers • SAN • Physical Servers • Switches/Routers
		<p>At this point we are either on generator power with sufficient UPS power remaining or we are on Florida Power & Light (FP&L) power. We cannot proceed if on generator power with no UPS charge to support a switch back.</p>

Post Disaster Restoration Procedures

Phase	IT Department	Procedural Steps
3	Network	If the internet access is not automatically restored at the RTMC or Vista Center, the routing entries from the IP routing table on the Cisco Core switch at TIMSO will need to be cleared by entering the following command: clear ip route * .
3	Servers	<ul style="list-style-type: none"> – Manually power on the storage arrays and wait several minutes for initialization. – Log in to the ILO of the host that contains vCenter and power it on. This process can also be done by physically powering each host, if needed. – Check each host to ensure it is properly connecting to the storage. – Log in to vCenter and verify that all systems are powered on. – Coordinate with the application owners to ensure that all applications are working properly.
3	Workstations	<ol style="list-style-type: none"> 1. Start up all workstations. 2. Start up all Barco NDNs throughout the environment. 3. Start up all NEC monitors throughout the building. 4. Start up the main Video Wall in the Control Room. 5. Verify connectivity to applications.

Post Test Outage After-Action Items

- TIMSO DNS scopes were not included on the DHCP Scopes. Added those. Work has already been done.
- DNS Settings in virtual center. Could not access VCenter in TIMSO.
- Addressed MAC addressing to manual in VCenter.
- Shutdown ISE in the TMC before domain controllers.
- Working on IPKVM in accessing the ISE's.
- The setup at the EOC was done very well.
- Firewall at TIMSO was a problem. Replace that firewall at TIMSO. Too small.
- Need to add static route from D4 to D6 network and vice versa before shutdown of core field switch, add to procedure.
- Communicate with FHP with new phone number.
- Encountered an issue with MFA authentication once TMC radius was brought down.
- Lost multicast with 595 after we came online. ***
- Add construction contracts to communication plan, send to construction engineers, Broward ops, treasure coast, PBC.

Post Main Outage After-Action Items

1. What did we intend to accomplish (what was our strategy)?

Answer: We intended to continue operations that TSM&O has during a UPS replacement that needed to happen at the RTMC in district 4.

2. What did we do (how did we execute relative to our strategy)?

Answer: We came up with a plan on how to do that using the EOC. We came up communication plans.

- a. We knew needed to verify assumptions by performing a test outage. Documented that during outage.
- b. We documented a procedure for powering down and powering on systems.
- c. Good. Information that was sent. There weren't a lot of emails or phone calls going back and forth.
- d. Greg – The teams' ability to come up with a plan was done very well. Planned out very well in a very little amount of time.
- e. Troubleshooting – system integrated devices that have been networked for a while don't like to be turned off. When they come back, it's not positive what will happen when they come back on.
- f. Timeline – resumption of tolls. No way to know that. Though we were close. Estimated 7pm and brought it back up at 5pm. Had to bring SELS/ELS down fully.
- g. Thank you to the Arcadis team for the tolling tables. When we were back again, it was extremely helpful for the hyper care office. Made their job a lot easier.

Have SELS process mirrored.

WORKSTATIONS – IT ON-CALL STANDARD OPERATING PROCEDURE (SOP)

Purpose

This document outlines the standard operating procedures relating to the structure and usage of the IT On-Call schedule hosted within the Microsoft Teams environment. The document serves as an instructional tool for all departments to understand how the IT Department On-Call schedule works.

How to Access

The IT On-Call schedule is accessible on Microsoft Teams under the name "**IT On Call Schedule.**" This schedule is regularly updated to include the names and contact details of IT staff members currently on call.

Reference for Operations

Operations personnel should consult the "**IT On Call Schedule**" in Teams to identify the designated IT On-Call Emergency Technical Support Personnel for any given period.

If Emergency IT support is required, Operations should make the initial contact with the designated IT On-Call Technical Support Personnel.

Recommended contact Path for Operations

If Operations is unable to reach the designated IT On-Call technician, the following steps should be followed:

1. Contact the previous week's IT On-Call Technical Support Personnel. (Reference IT On-Call Schedule within Teams for contact details)
2. Contact the upcoming week's IT On-Call Technical Support Personnel. (Reference IT On-Call Schedule within Teams for contact details)
3. If both contacts are unreachable, contact the Desktop Manager.
4. If all three contacts are unreachable, contact the IT Support Manager.

Ticket Creation

Operations is responsible for creating a support ticket in the IT ticketing system, detailing the issue at hand. If Operations is unable to create the ticket, the contacted IT personnel will initiate the ticket creation process. There are two methods available for creating a ServiceDesk ticket.

- Login to ServiceDesk portal to create a ticket. URL: <https://support.smartsunguide.com/>
- Send an email to support@floridadot.samanage.com. The subject of the email is the ticket title. The body of the email is the ticket details.

Initial Troubleshooting

The designated IT On-Call Technical Support Personnel will perform remote troubleshooting upon receiving the support ticket. If the issue cannot be resolved remotely, the IT On-Call Technical Support Personnel will assess the severity of the issue and, if deemed critical, arrange to visit the Traffic Management Center (TMC) for further troubleshooting.

On-Site Troubleshooting (if required)

In cases where on-site troubleshooting is necessary, the designated IT On-Call Technical Support Personnel will promptly visit the TMC for a hands-on resolution.

Coordination with Operations or relevant personnel on-site may be required to facilitate access and provide additional information.

Workaround Documentation

If a workaround is implemented to address the reported issue, the IT On-Call technician must document all relevant details and comments on the associated support ticket.

This documentation ensures that the IT team can follow up promptly the following business day for a comprehensive resolution.

Communication Protocol

Effective communication between Operations and IT is vital. All updates, progress, and resolution details should be promptly communicated through the support ticket.

Regular updates on the support ticket will ensure a smooth handover of information for any follow-up actions during normal business hours.

Post-On-Call Review

At the end of the on-call shift, the IT On-Call technician:

- Should review and update the support ticket,
- Ensure that all relevant information is documented for future reference.
- Communicate and address any outstanding issues or tasks for the IT team during the next business day.

Note. This SOP is subject to periodic review and updates. Any changes to the IT On-Call schedule or procedures will be communicated promptly to all relevant stakeholders.



7.34 Security Software

Document History

Version #	Date	Author	Changes
1.0	12/28/2023	Yana Neishlos	Initial Draft

Table of Contents

PASSWORD MANAGER	4
Password Manager Secondary Read-Only Server Configuration.....	4
Update To Password Manager Pro	5
TREND MICRO DEEP SECURITY - MANAGING APPLICATION CONTROL	7
Overview	7
Procedures.....	7
UPGRADES.....	8
Upgrade Trend Micro Deep Security Manager.....	8
AVTECH Room Alert Manager Upgrade	11
CONFIGURE OKTA RADIUS.....	12
INTEGRATE OKTA RADIUS WITH CISCO ASA.....	15
Add AAA Server Group.....	15
Add AAA Server.....	16
Modify IPSec (IKEv2) Connection Profile.....	17
SECURITY EVENT MANAGER DEPLOYMENT	18
Overview	18
Deploy a SEM Appliance	19
Activate a SEM License.....	20
Deploy a SEM Agent Locally on Endpoint Machines.....	21
Deploy a SEM Agent Remotely to Endpoint Machines.....	22
Verify a SEM Agent Connection.....	24
Install a SEM Reports Application.....	24
Connect a SEM Reports Application to Your Sem Database.....	24
INSTALLATIONS.....	26
Trend Micro Workload Security Agent – Installation	26
Trend Micro Apexone Security Agent Installation	29
SolarWinds Access Rights Manager (Arm) Client Installation	31
SOLARWINDS SERVICE DESK AUTO PROVISIONING WITH OKTA.....	35
Service Desk Admin Authentication Token	35
Okta Provisioning Steps	37
Assigning Users	39
TREND MICRO WORKLOAD SECURITY AGENT - TURN ON MAINTENANCE MODE.....	41

PASSWORD MANAGER

Password Manager Secondary Read-Only Server Configuration

Steps / Screenshots

1. On the Secondary server, → Uninstall the old version of Password Manager Pro (if installed).
2. Install a new version of Password Manager, currently running on a Primary server (versions must be the same).
3. Create a Data Replication Pack for High Availability in Primary server:
 - Stop the Password Manager Pro service on the Primary server (and Secondary server, if running). Ensure that the postgres process of PMP is NOT running.
 - Open an elevated command prompt; navigate to the **M:\ManageEngine\PMP\bin** directory.
 - Execute command **HASetup.bat FQDN of PMP Primary Server FQDN OF PMP Secondary Server**.

To run this script → Pass the fully qualified domain names of the host where the PMP Primary and Secondary servers are installed as command line arguments.

Example. If a Primary server is running at **primary-server in the domain zohocorpin.com** and the Secondary server is running at **secondary-server in the domain zohocorpin.com**:

execute the above script as follows:

In Windows: **HASetup.bat primary-server.zohocorpin.com secondary-server.zohocorpin.com**

```
M:\ManageEngine\PMP\bin>HASetup.bat TIMVMSM02.smartsunguide.com TIMVMSM02.smartsunguide.com
Creating high availability slave package.
Database server successfully started...
Going to update Secondary server details.....
Secondary server details updated.
Going to clear rr_pending_changes table entries.....
rr_pending_changes table entries cleared.
Database server already running.
Shutdown completed....
Adding PostgreSQL data.....[Completed]
Adding imported images.....[Completed]
Adding SSHD CLI API data.....[Completed]
Adding PostgreSQL configuration files.....[Completed]
High availability slave package HAPack.zip is available in M:\ManageEngine\PMP\scripts\..\replication directory.
Move and extract the zip file under PMP installation directory of TIMVMSM02.smartsunguide.com (secondary server).
```

This will create a replication package named "**HAPack.zip**" under the **M:\ManageEngine\PMP\replication** folder and contains the database package for the Secondary.

4. Start the Password Manager Pro service on the Primary server.

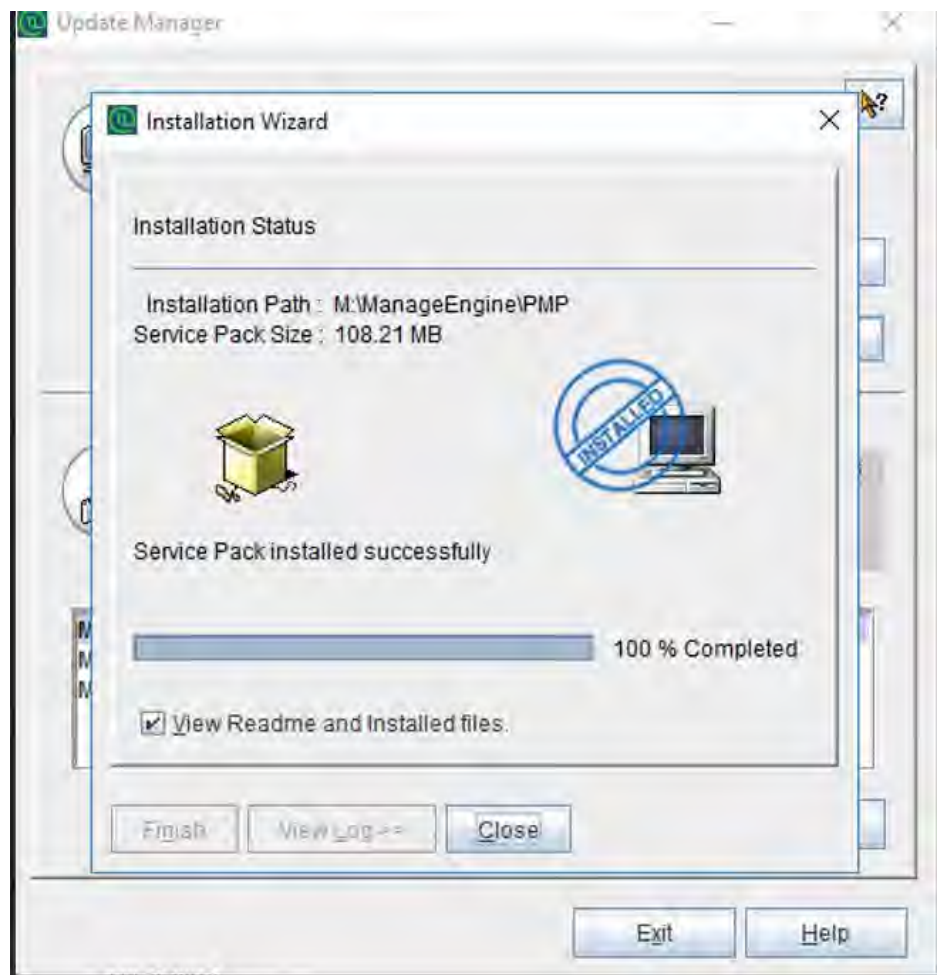
#	Steps / Screenshots
5.	Copy the "HAPack.zip" replication package, place it in the machine where the PMP Secondary server installation is running, and unzip it.
6.	Place the extracted folders under the M:\ManageEngine\PMP folder only. It will overwrite the existing data files.
7.	After extracting "HAPack.zip" in the PMP Secondary server, navigate to the " /conf" folder, edit "manage_key.conf" and ensure the location of the pmp_key.key: \\tmcvmcl03-namen\Share_Drive\Software\Security\Password Manager Pro Key\8600\pmp_key.key.
8.	Copy the Conf/server.xml file and .pfx file (Keystore file) from the Primary server to M:\ManageEngine\PMP\Conf folder of the Secondary server.
9.	Change the <i>Password Manager Pro</i> service logon account (Due to the sensitivity of the information in this document, it is only accessible by IT personnel at the following link 7.34 Security Software SD.pdf). Sensitive documents, such as "Security Software", are placed in PDF - IT Documents folder.
10.	Start the Password Manager Pro service.

Update To Password Manager Pro

#	Steps / Screenshots
1.	Login with Password Manager service account: (Due to the sensitivity of the information in this document, it is only accessible by IT personnel at the following link 7.34 Security Software SD.pdf). Sensitive documents, such as "Security Software" are placed in PDF - IT Documents folder.
2.	Disable antivirus on server.
3.	Stop Password Manager Pro service - both primary and secondary Read-Only Server.
4.	Exit Password Manager Pro service on the tray icon.
5.	On the elevated command prompt, execute M:\ManageEngine\PMP\bin\ StopDB.bat .
6.	<ul style="list-style-type: none"> – Backup the entire Password Manager Pro installation folder. – Store it in some other location (Zip entire Folder).
7.	Ensure all postgres tasks have ended.
8.	On the elevated command prompt, → Execute M:\ManageEngine\PMP\bin\ UpdateManager.bat .

Steps / Screenshots

9. – Click **Browse**.
- Select the .ppm file - [downloaded](#).
- Install.



Note. Upgrade to each newer upgrade-pack one at a time.

- 10 Start the Password Manager Pro service.

TREND MICRO DEEP SECURITY- MANAGING APPLICATION CONTROL

Overview

Application Control is one of Deep Security's security features, in place to prevent unrecognized and unauthorized software changes from altering the servers covered by the respective policy. However, if updates/changes are made to a server while maintenance mode is inactive, it can result in high administrator workloads, while causing Application Control to stop functioning.

Procedures

If any updates/changes are planned, → Enable maintenance mode before completing the process below, to prevent issues with this feature.

1. Verify that a server is not compromised from an external or third-party attack: examine the machine's processes and security events. It is to determine the cause of Application Control's failure. This may be due to updates/changes to a machine while maintenance mode is inactive.

If a software triggers that this alert is not removed, Application Control will ignore it once this entire process has been completed. It will not appear in the "Actions" tab. If executed, the system will not create logs or alerts until the machine is rebooted.

2. Disable/schedule updates, including automatic ones, to prevent re-occurrence. Maintenance mode should be enabled for the scheduled updates to occur. In the case of manual Windows Updates from IT staff change requests, maintenance mode should be turned on during the patching process.

To turn on **Maintenance** mode:

- Navigate to the upper toolbar in Deep Security
- Select **Computers**, → Right-click the desired machine.
- Select **Actions**.
- Turn on **Maintenance** Mode.

3. **Application Control** should now be reset on the affected machine(s). As such:

- Select the machine(s): double-click them to open the full computer details.
- Select **Application Control** tab: Under **Configuration** dropdown → Select **Off**.
- Once the Agent has acknowledged the reset → turn Application Control **on** again by navigating to the same dropdown mentioned above.
- Select **On**.

At times, an agent may not automatically acknowledge it during the reset process. Hence, alerts are displayed. Then,

- Clear the warnings for the machine(s) experiencing this issue, and, after a brief period,
- Re-enable Application Control as mentioned above.

UPGRADES

Upgrade Trend Micro Deep Security Manager

Note. Before proceeding with the steps below, a change request must be submitted and approved. Please ensure the change request is complete, and then – you can proceed.

Steps / Screenshots

1. The first step is to verify that the current DSM version is compatible with the intended version update. [This documentation](#) can assist in determining version compatibility.

If the current version is not compatible with the intended installation version:

- Upgrade to the latest possible version (see above link), and,
- Proceed from there.

All these steps are applicable to any version installation.

2. Notify the IT team of impending changes. Users and admins may experience downtime or difficulty during the implementation of the changes.



Figure 1. Notify the IT Team of Impending Changes

3. Turn on maintenance mode for servers that will be updated.
 - Navigate to the machines in Deep Security.
 - Right-click the desired machine.
 - Select **Actions**.
 - Click **Turn On Maintenance Mode**.



Figure 2. Turn on Maintenance Mode

4. Create snapshots in vCenter for the same machines that will be updated. These will be used as restore points if there are unforeseen complications with the update process.

Steps / Screenshots

Figure 3. Create Snapshots

5. Back up the DSM manager on the database server. Like the snapshot, this will serve as a failsafe in the event any issues occur. Depending on access rights, this will be done by another member of the IT team.
 - Open SQL Server Management Studio on the DB server.
 - Navigate to **Databases** → TrendMicroDeepSecurity
 - Right-click,
 - Select **Tasks** → **Back Up**. From there, make any adjustments as needed, e.g., save location, and back up the database.

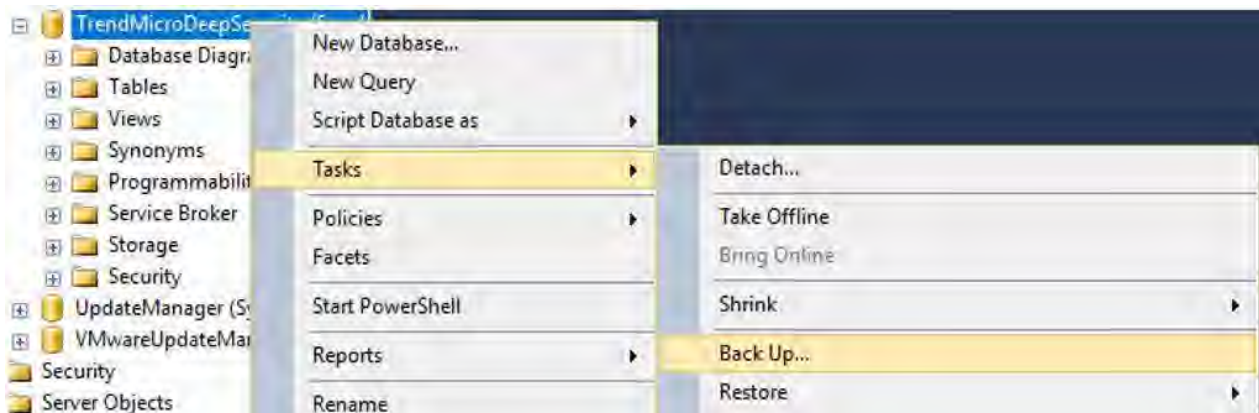


Figure 4. Back up the DSM Manager on the Database Server

6. Once the steps above are complete, → Stop all manager nodes to be updated, → Start installing on the first node.

Note. Do not run the installer on multiple nodes simultaneously, as this can corrupt the database, which must be restored with the database backup above.

Once the first node has completed updating, → Upgrade the next node. Continue the update process.

- The first node will take over as a primary while other nodes are being upgraded; as it will be the only available manager, performance may be noticeably reduced during this time.

Steps / Screenshots

For a list of manager software required for this update → Click the link below:

<https://help.deepsecurity.trendmicro.com/software.html>

- Run the application on the manager node to start the installation process.
- Ensure that the current version is compatible with the update.

Manager Windows

Software	Release Type	Build	Reason	Release Date	Download
Deep Security Manager 20.0.482 for Windows-x64 (20 LTS Update 2021-08-25)	LTS	20.0.482	Update	Aug 25, 2021	
Deep Security Manager 20.0.463 for Windows-x64 (20 LTS Update 2021-07-22)	LTS	20.0.463	Update	Jul 22, 2021	

Figure 5. Manager Software Required

7. Once all manager nodes are upgraded → Verify: all Trend Micro related applications and features are still functional.
 - If operational → Monitor Deep Security alerts for update-related issues within relays and nodes.
 - For unforeseen errors → Identify the cause; revert snapshots, database backups as needed.
 - Check related log files to identify schema changes or other errors that occurred.
8. If the update was successful and no issues have been detected, → Perform a brief testing → Delete snapshots if desired.

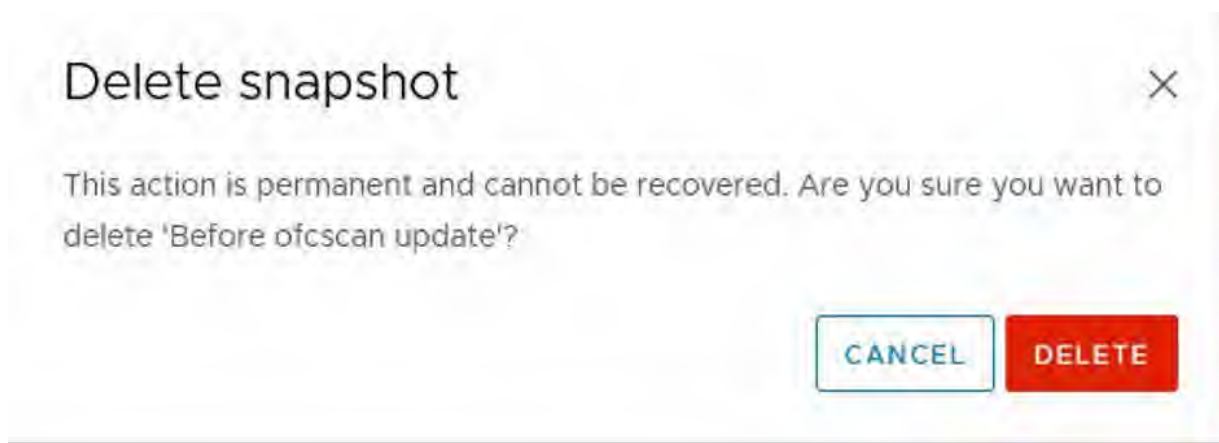


Figure 6. Delete Snapshots

9. For further documentation, refer to the links below:

- [Deep Security On-Premise Manager Upgrade](#)
- [Deep Security On-Prem Manager Installation](#)

AVTECH Room Alert Manager Upgrade

1. Download update <https://account.roomalert.com/downloads> (support credentials located in Password Manager Pro).
2. Disable Antivirus agent.
3. Execute installer.
4. Follow the on-screen prompts to upgrade Room Alert Manager at path **E:\AVTECH Room Alert Manager**.
5. Once complete, verify firmware for each device and update <https://avtech.com/articles/164/>.
 - To the right of the screen for each device, select the ellipsis to view the available options for that device.
 - Select **Update Firmware**.
 - Browse to <http://roomalert.smartsunguide.com:9393/> and login.

CONFIGURE OKTA RADIUS

Steps/Screenshots

1. Login to Okta tenant as Admin.

2. Navigate to **Security > Multifactor**.

3. Configure **Factor Types**.

4. Create **Cisco ASA VPN RADIUS** application.
 - a. Navigate to **Applications > Applications > Browse App Catalog**.

 - b. Search **Cisco ASA VPN (RADIUS)**.

 - c. Select **Add**.

5. Install and configure the **RADIUS Agent**.
 - a. In Okta tenant, navigate to **Settings > Downloads > Okta RADIUS Server Agent**.

 - b. On the server, run the **Okta RADIUS installer**.

 - c. Proceed through the installation wizard to the "**Important Information**" and "**License Information**" screens.

 - d. Choose the Installation folder and click the **Install** button.

 - e. In the **Okta RADIUS Agent Configuration** screen,

Enter your **RADIUS Shared Secret key** and **RADIUS Port number**.

Steps/Screenshots

- f. In the **Register Okta RADIUS Agent** screen, enter Subdomain <https://smartsunguide.okta.com>.

- g. Click the **Next** button to continue to an **Okta Sign In** page.

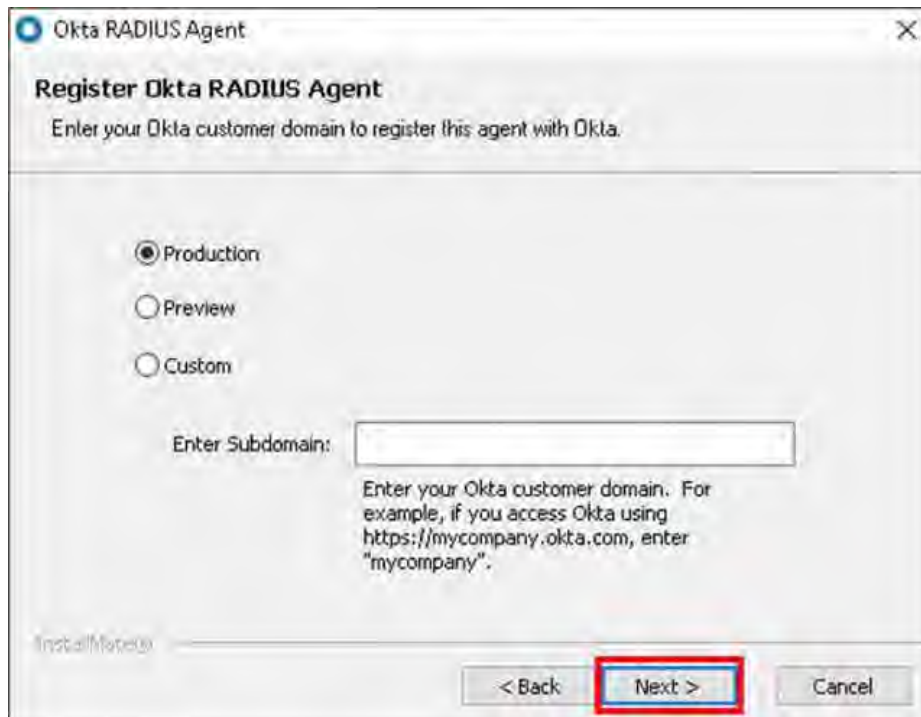


Figure 7. Register Okta RADIUS Agent

- h. Sign in with service specific Okta account **Okta Admin-Service** on the Sign In screen.
- i. Click **Allow Access** button.
- j. The confirmation screen appears. Click the **Finish** button to complete the installation.
- k. – Complete configuration of RADIUS app from Step 4 in Okta
– Configure the RADIUS Agent port, shared secret, and advanced RADIUS settings.

Steps/Screenshots

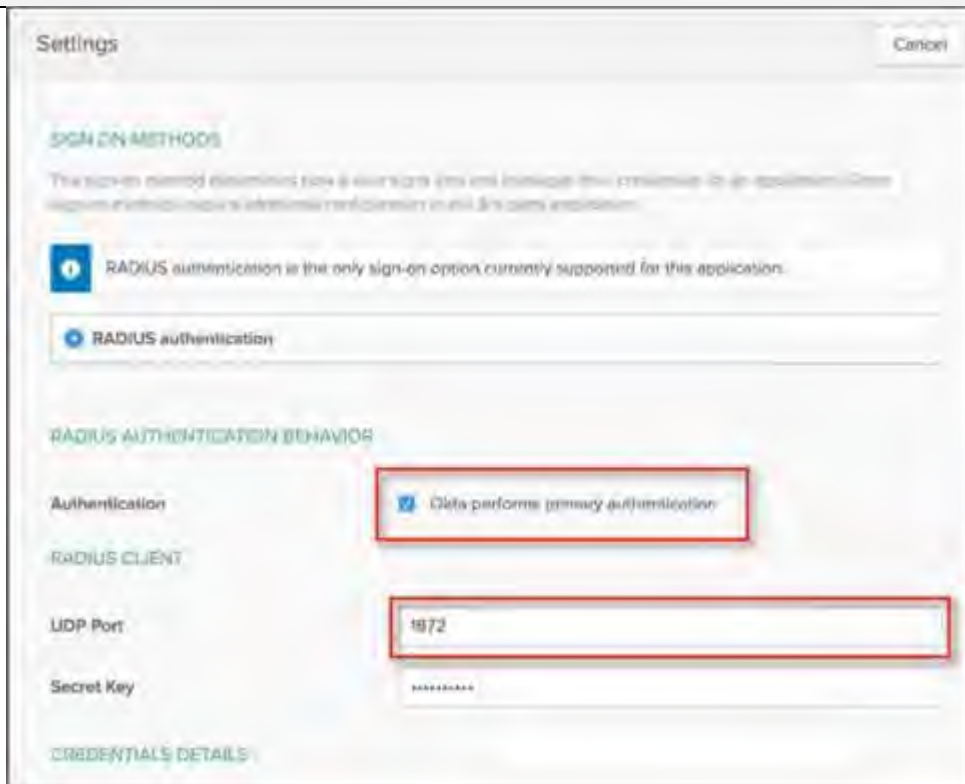


Figure 8. Radius Authentication

INTEGRATE OKTA RADIUS WITH CISCO ASA

Add AAA Server Group

1. Log in to **Cisco Adaptive Security Device Manager (ASDM)**.
2. Navigate to **Configuration > Remote Access VPN > AAA/Local users > AAA server groups**.
3. Click **Add** to create a new group.
4. **Add AAA Server Group** dialog displays.
5. Leave the **default settings** except for the following:
 - a. **AAA Server Group** – Create a name to identify the group for the MFA server.
 - b. Protocol – select **RADIUS**.
6. Click **OK**.



Figure 9. Add AAA Server Group

7. Select the server group just created.
8. Under **Servers in the Selected Group**, → Click **Add**.

Add AAA Server

1. Specify the following, leaving all other fields unchanged.:
 - a. **Interface Name** – Select **Inside**.
 - b. **Server Name or IP Address** – Specify the IP address of the Okta RADIUS Agent.
 - c. **Timeout** (seconds) – **60** seconds.
 - d. **Server Authentication port** – Enter the required port number. E.g., Port 1812.
 - e. **Server Accounting Port** – 1646. This value is not used; must be entered for setup.
 - f. **Retry Interval** – Leave default at **60** seconds.
 - g. **Server Secret Key** – Provided secret defined when setting up the app in Okta.
 - h. **Common Password** – Leave blank.
 - i. Uncheck **Microsoft CHAPv2 Capable** (important).
2. Click **OK**.



Figure 10. Add AAA Server

3. Click **APPLY** to save the configuration.

Modify IPsec (IKEv2) Connection Profile

1. Click **Configuration**.
2. Select **Remote Access VPN**.
3. Expand **Network (Client) Access**.
4. Select **IPsec (IKEv2) Connection Profiles**.
5. Select **Connection Profile** → Click **Edit**.
6. Under **User Authentication**,
 - Select **Server Group**
 - Click **OK**.

The screenshot shows the configuration window for an IPsec Remote Access Connection Profile. The 'Basic' tab is selected in the left-hand navigation pane. The main area contains several sections:

- Name:** OktaPreview_AnyConnect
- IKE Peer Authentication:**
 - Preshared Key
 - Enable Certificate Authentication
 - Enable peer authentication using EAP (If this is enabled, only Certificate is allowed for Local Authentication)
- Mobike RRC:**
 - Enable Return Routability Check for mobike
- RSA Signature:**
 - Enable RSA Signature Hash
- IKE Local Authentication:**
 - Enable local authentication
- User Authentication:**
 - Server Group:** OktaRadiusGroup_VISTA (highlighted with a red box)
 - Fallback:** Use LOCAL if Server Group fails
- Client Address Assignment:**
 - DHCP Servers:** (empty field)
 - Radio buttons: None, DHCP Link, DHCP Subnet
 - Client Address Pools:** IT_Anyconnect (with a 'Select...' button)
- Default Group Policy:**
 - Group Policy:** OKTA_AnyConnect (with a 'Manage...' button)
 - (Following field is an attribute of the group policy selected above.)
 - Enable IKEV2 Protocol

At the bottom of the window, the 'OK' button is highlighted with a red box, along with 'Cancel' and 'Help' buttons.

Figure 11. Edit IPsec Remote Access Connection Profile

SECURITY EVENT MANAGER DEPLOYMENT

Due to the sensitivity of the information included in this document, it is only accessible by IT personnel at the following link: [DOCX File viewer | Microsoft Teams](#).

Overview

This SOP Section includes the following procedures:

- *Deploy a SEM Appliance*
-

- *Activate a SEM License*
-
- *Deploy a SEM Agent Remotely to Endpoint Machines* Deploy a SEM Agent Remotely to Endpoint Machines
- *Verify a SEM Agent Connection*
- *Install a SEM Reports Application*
- *Connect a SEM Reports Application to Your Sem Database*

Deploy a SEM Appliance

1. Download the VMware ova file from <https://customerportal.solarwinds.com/>
2. Deploy the SEM open virtualization appliance.
3. Edit hardware requirements to match listed requirements for environment size [SEM 2021.1 system requirements \(solarwinds.com\)](#).
4. Start the SEM VM.
5. Open a web browser and connect to the SEM Console using the URL listed on the appliance console (e.g., <http://IPAddress>).
6. Enter default username (**admin**) and password (**password**), and then click Login.
7. Accept the terms of license agreement.
8. Enter and confirm your new password.
9. Enter your email address for contact and download verification.
10. Click **Start Using SEM**.

Activate a SEM License

Steps / Screenshots

1. Open the SEM appliance console.
2. Tab to **Advanced Configuration** on the main console screen → Press **Enter** for the command prompt.

```

SolarWinds Security Event Manager - 2021.4

The virtual appliance is successfully installed and running.

To monitor and configure SolarWinds Security Event Manager, use the
Security Event Manager Web Console or standalone Console application.

Hostname           : TMCUASEM01
IP Address         : 10.176.5.174
Web Console        : https://TMCUASEM01/
                   : https://10.176.5.174/

License            : SolarWinds Security Event Mgr (formerly LEM)-SEM500
Product Support Key : CBQFB-NZXUE-HNQH-U7K7-HXANS-W79F9

* Advanced Configuration          Use Arrow Keys to navigate
  Set Timezone (US/Eastern)      and <ENTER> to select your choice.

```

Figure 12. SolarWinds Security Event Manager - 2021.4.

3. Enter the username (**cmc**) and the default password (**password**).
4. At the **cmc>** prompt,
 - Type **appliance**,
 - Press **Enter**.

The prompt changes to **cmc::appliance>** to indicate you reached *appliance configuration* menu.

5. Type **activate**, → Press **Enter**. The Activation splash screen appears.
6. To go to the next screen, → Press **Enter**.
7. When prompted, → Select **Yes** to configure a static IP address for the SEM VM.
8. At the **cmc::appliance>** prompt,
 - Type **netconfig**,
 - Press **Enter**.

Follow the steps on your screen to configure the **Manager Appliance network** parameters.

Steps / Screenshots

9. Record the IP address assigned to SEM VM. Use this IP address for logging into SEM console.
10. When prompted to change the **hostname**, → Select **Yes** to specify a hostname.
11. As prompted to specify a list of IP addresses to access reports, → per SolarWinds: Select **Yes**.
12. Confirm your network configuration.
 - Type **viewnetconfig** at the **cmc::appliance>** prompt. → Follow the prompts to export the certificate to a network share.

An accessible network share is required. Once the export is successful, a following message appears: *Exporting CA Cert to \\server\share\SWICAer -hostname.crt ... Success.*

Deploy a SEM Agent Locally on Endpoint Machines

Steps

1. Configure exceptions in TrendMicro.
 - C:\Windows\system32\ContegoSPOP
 - C:\Windows\sysWOW64\contegoSPOP
 - **Turn off** any anti-malware or endpoint protection applications on host systems during the installation process, to prevent an impact on the process of *file transfer* installation to the hosts.
 - Extract the contents of the installer ZIP file to a local or network location.
2. Run the **.exe** file.
3. Click **Next** to start the installation wizard.
4. Accept the End User License Agreement if you agree. → Click **Next**.
5.
 - Specify a temporary folder on your computer to use for the installation process and
 - Click **Next**.

The default is C:\SolarWindsSEMMultiInstall.
6.
 - Enter the hostname of your SEM Manager in the Manager Host field.
 - Click **Next**. Do not change the default port values.
7. Select Get hosts automatically or Get hosts from file (One host per line), → Click **OK**.
8. Select the check boxes next to the computers to install a SEM Agent. → Click **Next**.
9. Confirm the list is correct. → Click **Next**.
10. Specify the Windows destination for the remote installation. → Click **Next**.

Steps

11. Specify whether you want to install **USB-Defender** with the **SEM Agent**, → Click **Next**.
The installer will include **USB-Defender** by default.
To omit this from the installation, → Clear the **Install USB-Defender** option box.
12. Confirm the settings on the **Pre-Installation Summary**. → Click **Install**.
13. Once the installer finishes, → Click **Next** to start the SEM Agent service.
14. Inspect the **Agent Log** for any errors. → Click **Next**.
15. Click **Done** to exit the installer.

Deploy a SEM Agent Remotely to Endpoint Machines

Steps / Screenshots

1. Download Remote Agent Installer from <https://customerportal.solarwinds.com/>.

2. Execute **SolarWinds-SEM-2021.4-Agent-WindowsRemoteInstaller.exe** as an administrator.



Figure 13. SolarWinds Security Event Manager Agent 2021.4 Remote Installer.

3. Accept the License Agreement.
4. Leave the temporary folder at default setting: C:\SolarWindsLEMMultiInstall.

Steps / Screenshots

5. - Enter the hostname or IP Address
- Leave ports to default settings.



Figure 14. IP Address/Hostname and Ports

6. Select text file with list of machines for agent install.

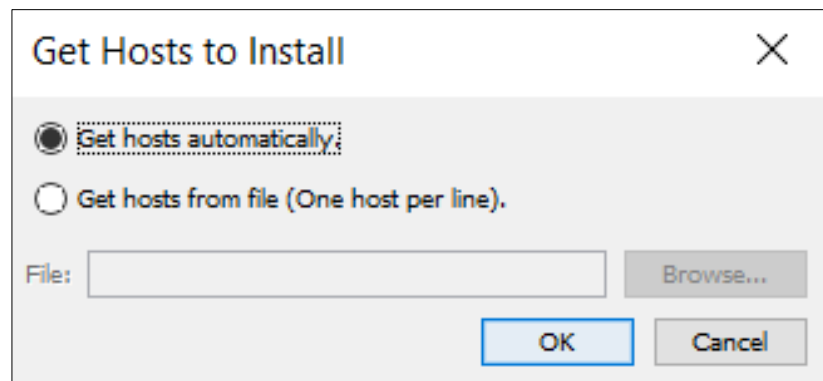


Figure 15. Get Hosts to Install.

7.
 - Specify whether you want to install **USB-Defender** with the **SEM Agent**.
 - Click **Next**.

The installer will include **USB-Defender** by default.

To omit this from the installation, → Clear the **Install USB-Defender** option box.

8. Confirm settings on the **Pre-Installation Summary**, → Click **Install**.
9. Once the installer finishes, → Click **Next** to start the SEM Agent service.
10. Inspect the **Agent Log** for any errors, → Click **Next**.
11. Click **Done** → Exit the installer.

Verify a SEM Agent Connection

Note: After you install the SEM Agent on your Agent nodes, verify that the Agent connected to the SEM Manager.

1. On the SEM Console, navigate to **Configure > Nodes**.
2. Under Refine results, click the Agent and Connected check boxes.
3. In the agent node list, ensure all connected nodes display a green check mark indicator.

Install a SEM Reports Application

Note. This installer also installs the Crystal Reports Runtime.

1. If necessary, copy the SolarWinds Security Event Manager installation folder to a local drive and open the folder
2. Right-click the file Install Next - SEM Reporting Software.exe, Select **Open**.
A dialog box appears prompting you to allow the app to make changes to your device.
3. Click **Yes** to continue.
4. The Welcome screen appears.
5. Click **Next**, to review the Requirements for Installation.
6. Click **Next**, → Click **Begin Install** to start the installation process.
7. When the **Installation Complete** dialog displays, → Click **Close**.

Connect a SEM Reports Application to Your Sem Database

When you enter a SEM Manager IP address into the SEM reports application, you create a connection between the reports application and the SEM database server running on the SEM Manager VM.

Before you start, you will need the IP address of the SEM VM and your SEM console login credentials.

1.
 - Right-click the **Reports application** icon on your desktop
 - Select Run as administrator.
 - Right-click the Reports shortcut → Select **Properties**.
 - Click **Advanced**
 - Select **Run as administrator** option.
 - Click **OK**.
 - In the reports Properties window → Click **OK**.

2. Click **Yes** in the antivirus dialog box → Continue.
3. Click **OK** in the information box → Create a list containing at least one Manager.
4. Enter the **hostname** or **IP address** of your SEM appliance in the **Manager Name** field.
5. Enter a **username** and a **password** used to log in to the SEM console.
6. *(Optional)* Select a **Use TLS connection** check box to use the transport layer security protocol for a secure connection.
7. Click **Test Connection** to verify the connection between the **SEM database server** and the **SEM reports application**.
8. A reports application pings the SEM database and verifies the connection. If a ping is successful, → **Ping Successful** displays in the dialog box.
9.
 - Click **Syslog Server (Host Name)** field to add the IP address to your SEM Manager list.
 - Click **Yes** to confirm.
10. Click **Close**.

The reports application is connected to your SEM database and displays on your screen.

INSTALLATIONS

Trend Micro Workload Security Agent – Installation

Steps / Screenshots

1, Sign to **Okta**.

- a. Click the following link to access the Okta website: <https://smartsunguide.okta.com>.

Note. The UserPrincipalName (UPN) format (i.e., username@domain.com) is required when entering your username in a username field to sign in to Okta, as shown below:

- b. Using the UPN format,
- Enter your SMART SunGuide credentials.
 - Click **Sign in**.



Figure 16. Okta Sign in Page

2. Once signed in,

- Click the **Trend Micro Workload Security Agent** app.



Figure 17. Trend Micro Workload Security App

Steps / Screenshots

Note. For air-gapped machines, perform step 3.b. Select that the proxies from the **Proxy to Contact Workload Security Manager** and **Proxy to Relay(s)** drop-down menus.

3.
 - Navigate to **Support** in the top right-hand corner of the screen.
 - Click the **down arrow**.

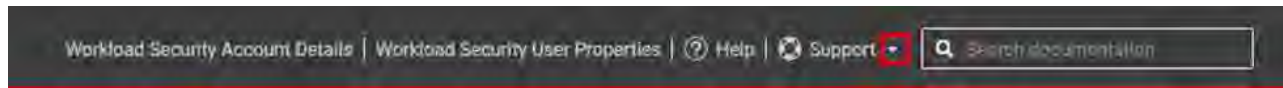


Figure 18. Trend Micro Workload Security Support

- a. Select **Deployment Scripts** from the drop-down menu.

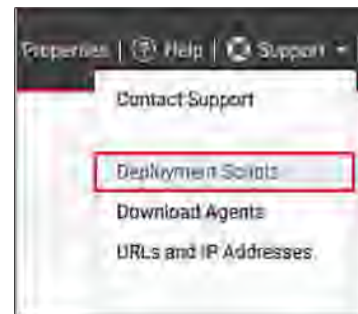


Figure 19. Support > Deployment Scripts

- Select **OS Platform** from drop-down menu.
- Select **Security Policy** from the drop-down menu.
- Click **Save to File**.

Deployment Scripts

Deep Security Agents can be deployed using tools such as RightScale, Chef, Puppet, or SSH. Use this deployment script generator to generate the scripts required.

For platforms other than Windows and Linux, please see the installation guide:

Platform: Linux Agent Deployment ▼ 1

Activate Agent autor Linux Agent Deployment (to assign a security policy)

Security Policy: Solaris Agent Deployment ▼ 2

Computer Group: Primary Tenant Relay Group ▼

Relay Group: Primary Tenant Relay Group ▼

Proxy to contact Workload Security Manager: Select a proxy... ▼

Proxy to contact Relay(s): Select a proxy... ▼

NOTE Hostname, description, unique identifiers and other properties can also be set on agent-initiated activation. See the [Command Line Instructions](#) page in the online help for more information.

Validate Workload Security Manager TLS certificate. [Learn More](#)

Validate the digital signature on the agent installer. [Learn More](#)

1 Save to File...
Copy to Clipboard
Close

Figure 20. Deployment Scripts > OS Platform and Security Policy Selections

Steps / Screenshots

- b. Air-Gapped Machines. For a machine located on an isolated VLAN,
- Click **down arrow** next to **Support**.
 - Select **Deployment Scripts** from the drop-down menu.

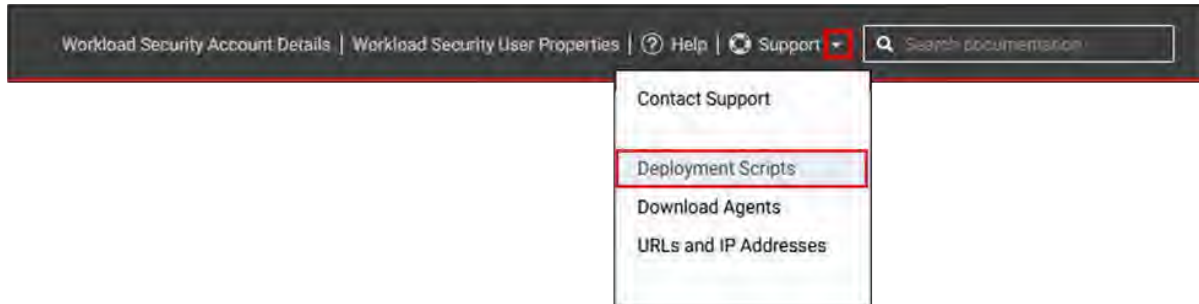


Figure 21. Trend Micro Workload Security Support > Deployment Scripts

- (1) Select **OS Platform** from the drop-down menu.
- (2) Select **Security Policy** from the drop-down menu.
- (3) Select a proxy from **Proxy to contact Workload Security Manager** drop-down menu.
- (4) Select the proxy from **Proxy to contact Relay(s)** drop-down menu.
- (5) Click **Save to File**.

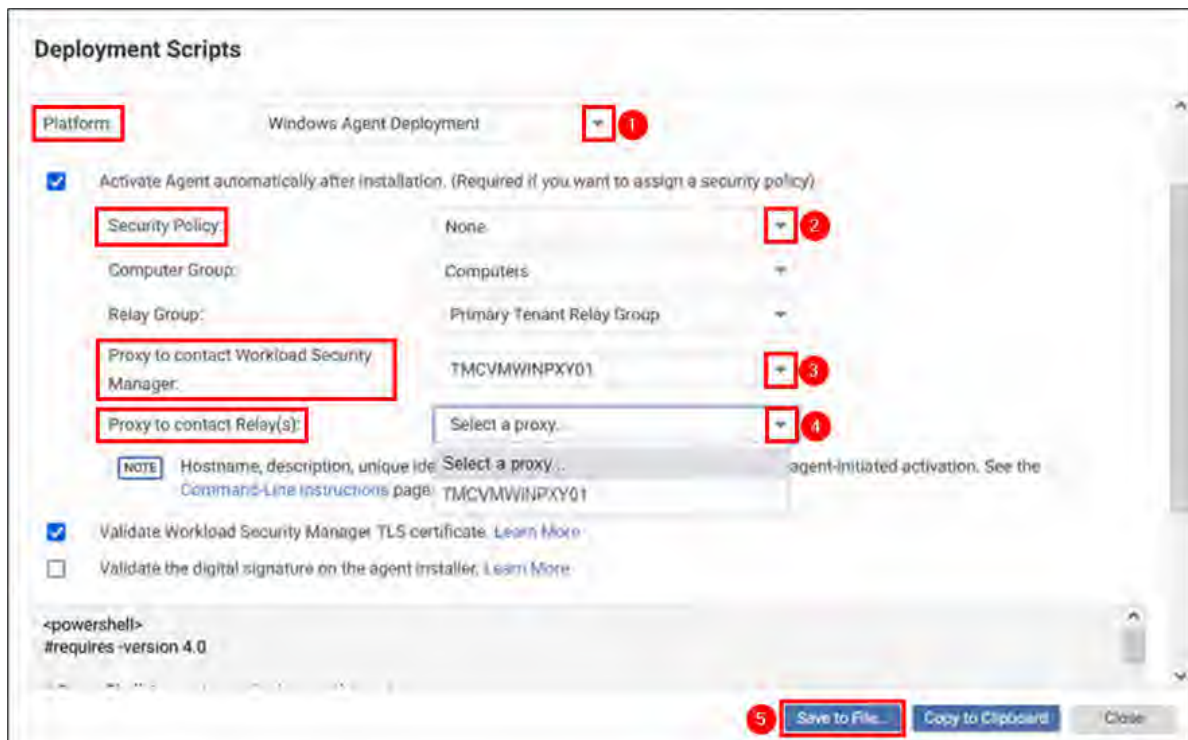


Figure 22. Deployment Scripts for Air Gapped Machines

Trend Micro ApexOne Security Agent Installation

Steps/Screenshots

1 Sign to Okta.

- a. Click the following link to access the Okta website: <https://smartsunguide.okta.com>.

Note. The UserPrincipalName (UPN) format (i.e., username@domain.com) is required when entering your username in the username field to sign in Okta.

- b. Using the UPN format,
 - Enter your SMART SunGuide credentials.
 - Click **Sign in**.



Figure 23. Okta Sign in Page

2. Once signed in,
 - Click the **Trend Micro ApexOne Security Agent** app.



Figure 24. Trend Micro ApexOne Security App

Steps/Screenshots

3. a. – Click **Administration** tab.
- Select **Security Agent Download** from the drop-down menu.

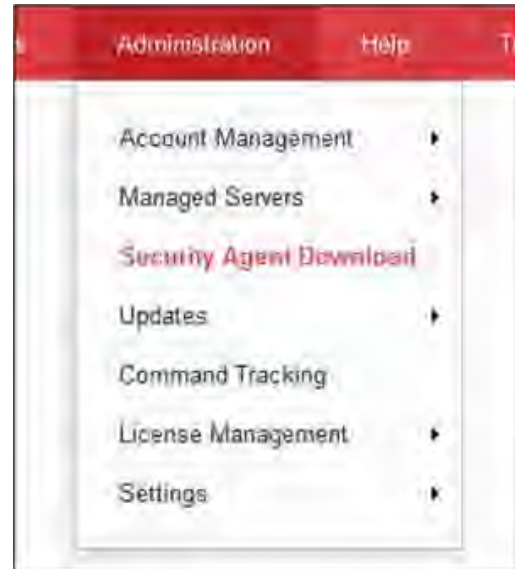


Figure 25. Administration > Security Agent Download

- b. – Select **Operating system**.
- Select **Installation mode**.
 - Select **Package type**.
 - Click **Download Installer**.

 A screenshot of a web form titled 'Security Agent Download'. The form asks to 'Specify your requirements for the Security Agent installation package'. It contains several sections:

- Operating system:** Radio buttons for 'Windows 64-bit' (selected), 'Windows 32-bit', and 'Mac'.
- Installation mode:** Radio buttons for 'Full feature set' (selected) and 'Coexist' (with an information icon).
- Package type:** Radio buttons for 'Standalone' (selected, with an information icon) and 'Web installer' (with an information icon).
- Server:** A text field containing 'Apex One as a Service'.
- Note:** A text field containing '- To ensure that all Security Agents can prop'.

 At the bottom, there are two buttons: 'Download Installer' (blue) and 'Get Download Link' (grey).

Figure 26. Security Agent Download

SolarWinds Access Rights Manager (Arm) Client Installation

Steps / Screenshots

1. Execute **ARM Setup.exe** as an administrator.
 - a.
 - Select **Advanced Installation**
 - Click **Next**.

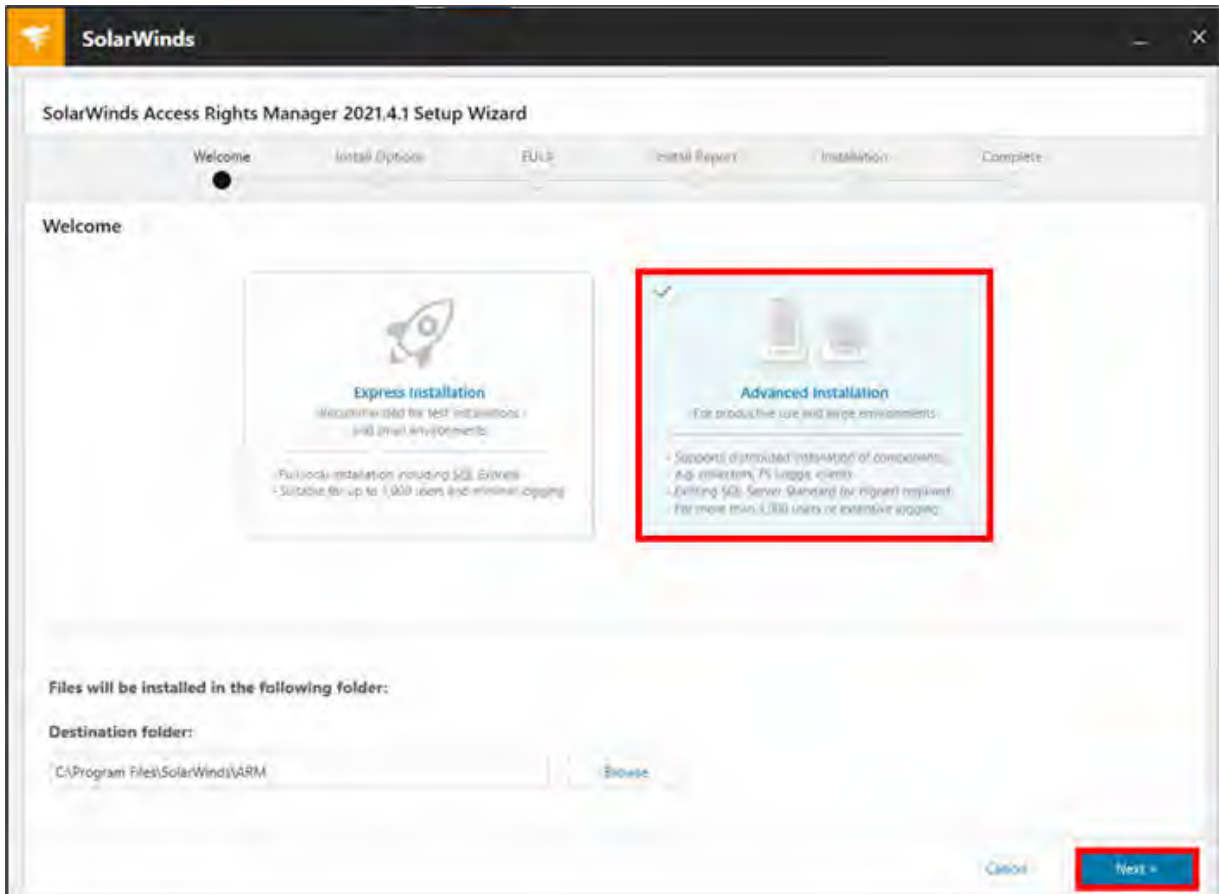


Figure 27. Advanced Installation

- b.
 - Select **Custom Installation**; ensure that only **ARM Rich Client** and **ARM Configuration Client** are checked.
 - Click **Next**.

Steps / Screenshots

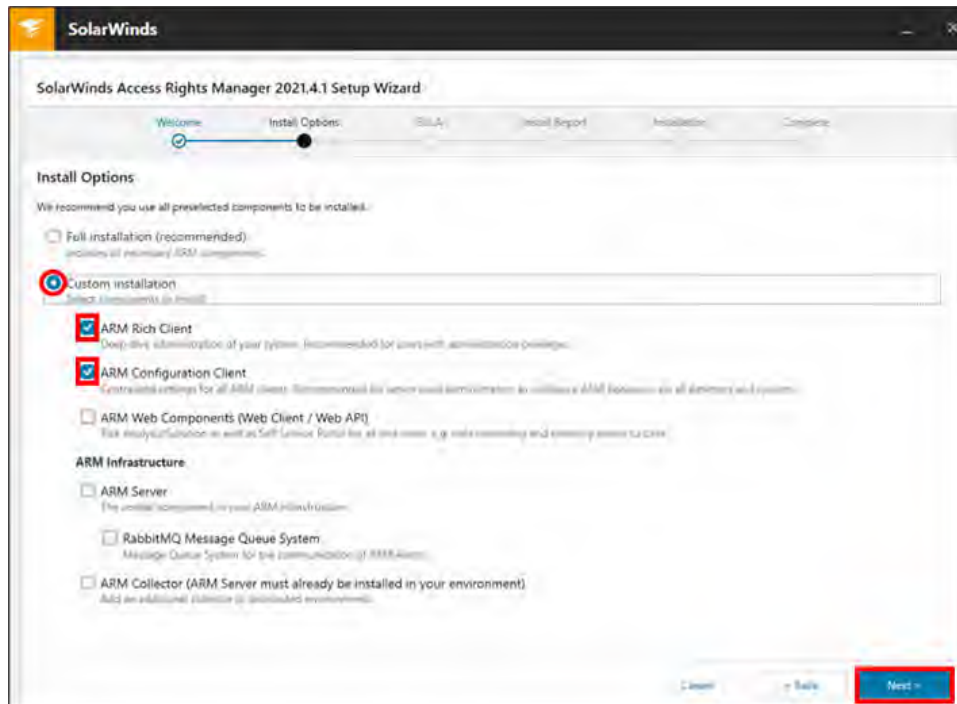


Figure 28. Custom Installation

c. Accept the **End User License Agreement** and Click **Next**.

Figure 29. End User License Agreement

Steps / Screenshots

- d. Verify the **System Check Results** and Click **Next**.

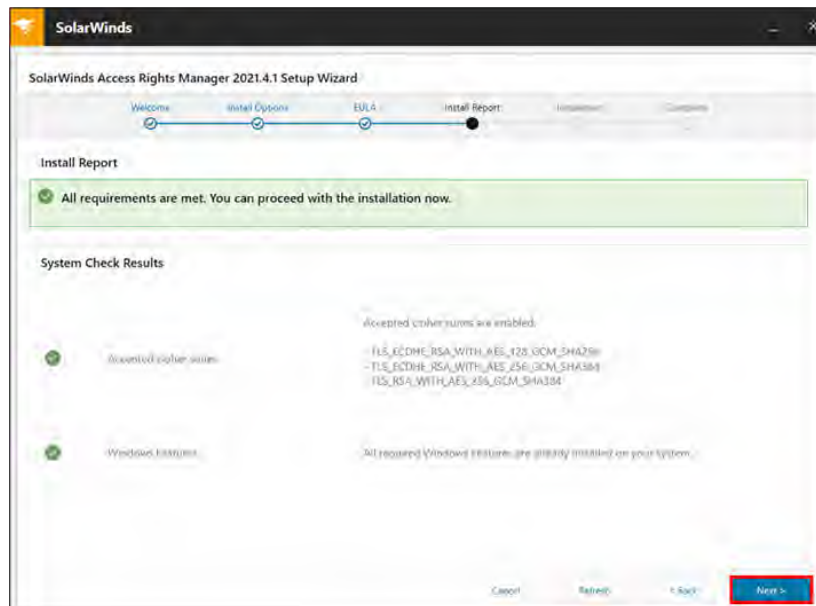


Figure 30. System Check Results

2. Once the installation is complete, launch the **ARM Client**.

- a. – Click the **Options** icon.
 – Enter the **ARM Server Fully Qualified Domain Name (FQDN)**.
 – Leave the default **port number** in place.

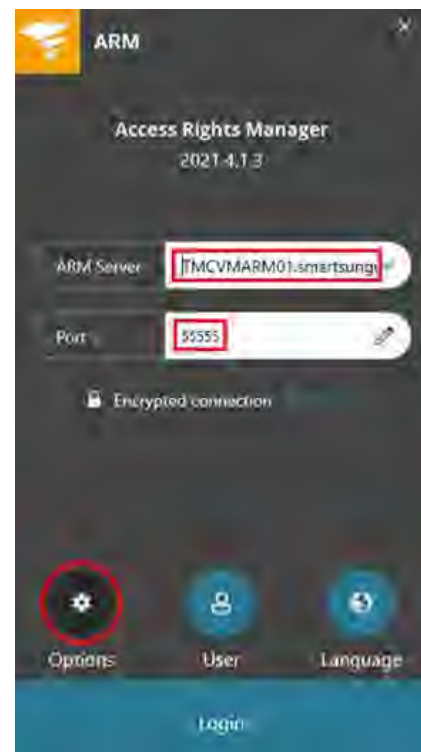


Figure 31. Options > ARM Server FQDN > Default Port Number

Steps / Screenshots

- b.
- Click the User icon.
 - Enter your admin account credentials.
 - Click **Login**.

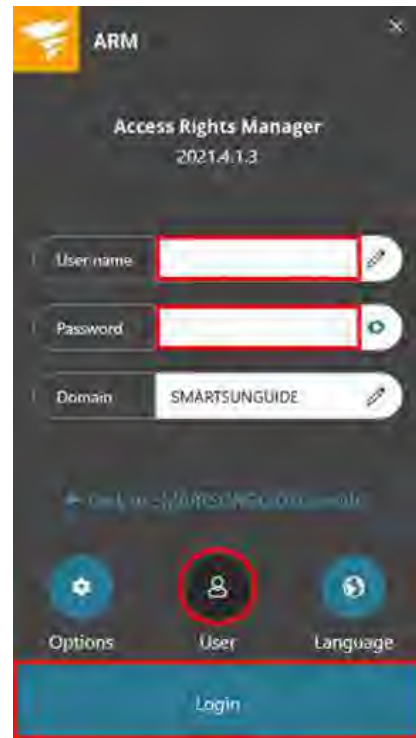


Figure 32. User > Admin Account Credentials > Login

SOLARWINDS SERVICE DESK AUTO PROVISIONING WITH OKTA

Service Desk Admin Authentication Token

Steps/Screenshots

1. Log in to the **SolarWinds Service Desk** tenant using the local administrator credentials (found in Password Manager).
2. Select **Setup** from the menu on the left-hand side of the screen.

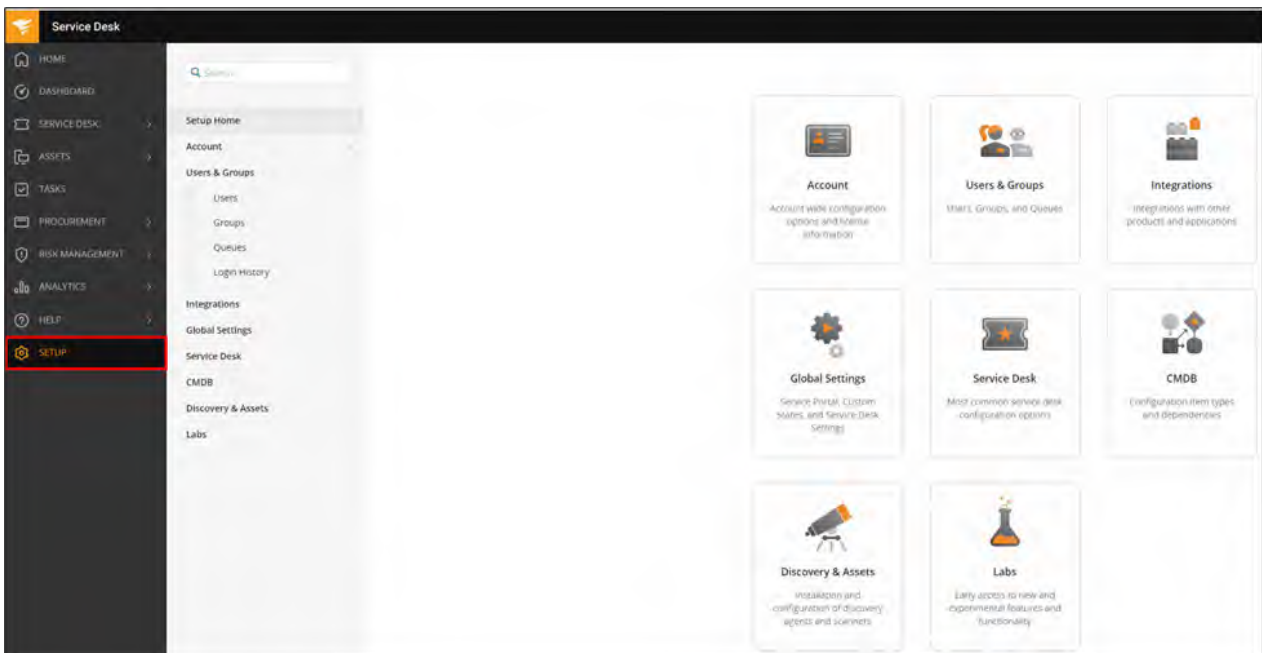


Figure 33. SolarWinds Service Desk Setup

Steps/Screenshots

3. – Click **Users**.

Then,

- Find and Select **admin** user.

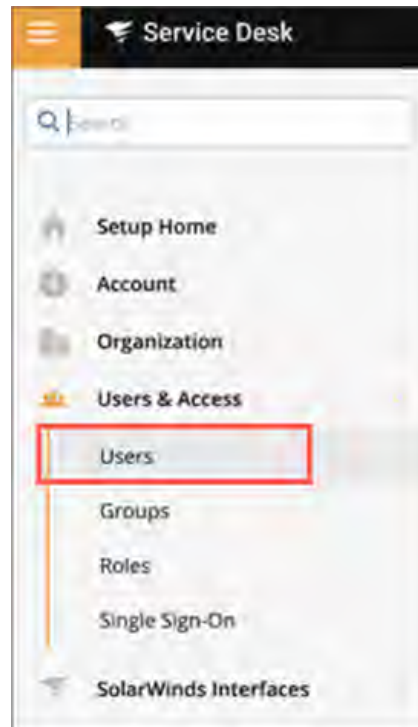


Figure 34. SolarWinds Service Desk Users

4. – Click **Show Token**.

- Copy the **Authentication Token**.



Figure 35. Show Token

Okta Provisioning Steps

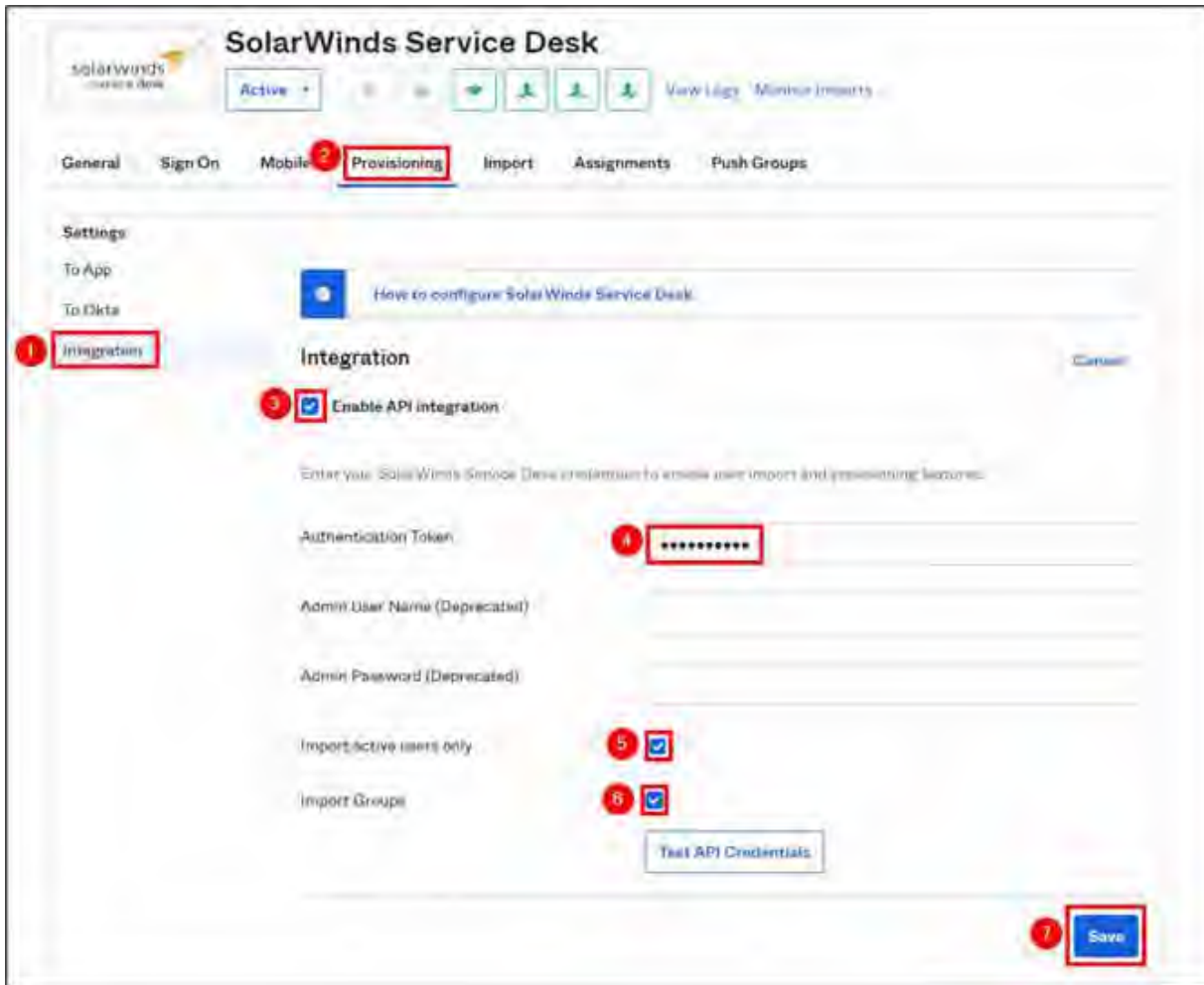


Figure 36. Okta Provisioning - Integration

#	Steps / Screenshots
1.	Navigate to Application and Click Integration .
2.	Click Provisioning tab.
3.	Check the box next to Enable API Integration .
4.	In the Authentication Token field, → Paste the Authentication Token that you copied in Step 1.d. above.
5.	Check the box next to Import active users only .
6.	Check the box next to Import Groups .
7.	Click Save .

Steps / Screenshots

8.
 - Click **To App**.
 - Select the **Provisioning** features you want to enable.
 - Click **Save**.

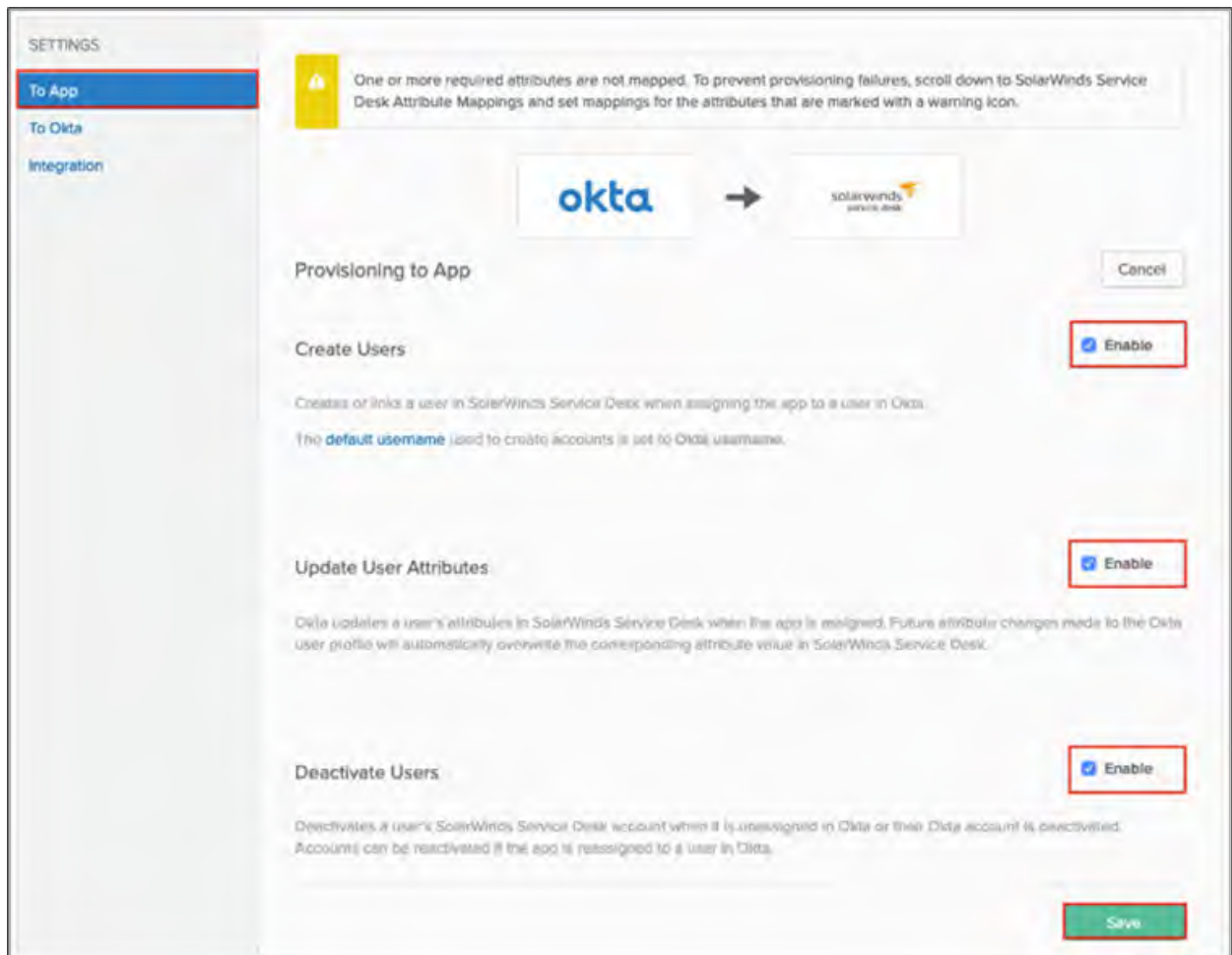


Figure 37. Okta Provisioning - To App

Assigning Users

Steps/Screenshots

1. Click the **Assignments** tab.
2.
 - Click **Assign**.
 - Select **Assign to Groups**.



Figure 38. Assignments > Assign > Assign. to Groups

3. Select the appropriate AD Group.
4. Select the **User role**, **User site**, and **User department**.
5. Click **Save**.

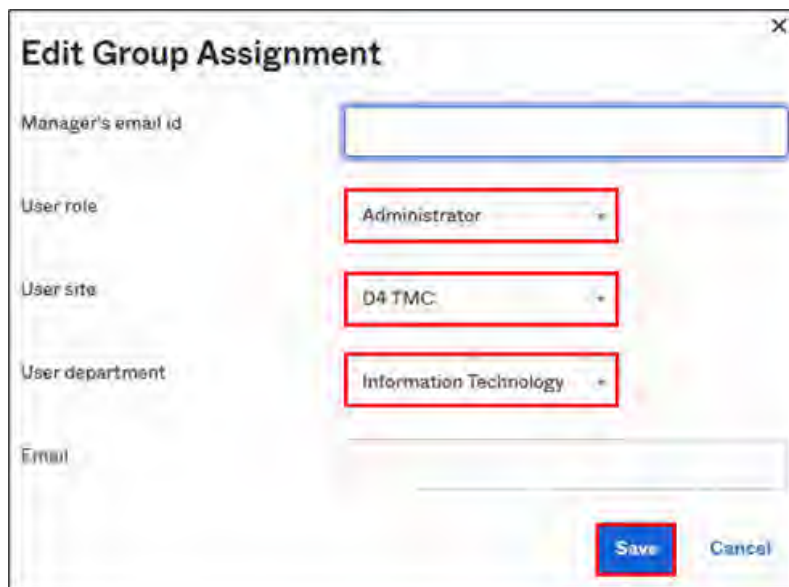


Figure 39. Edit Group Assignment

Steps/Screenshots

6. Repeat steps 2 - 5 above until you have completed all group assignments.

The screenshot displays the 'SolarWinds Service Desk' interface, specifically the 'Assignments' tab. The page features a navigation bar with options like 'General', 'Sign On', 'Mobile', 'Provisioning', 'Import', 'Assignments', and 'Push Groups'. Below the navigation, there are buttons for 'Assign' and 'Convert assignments', along with a search bar and a 'Groups' dropdown. A table lists the assignments with the following data:

Filters	Priority	Assignment		
People		ServiceDesk_Administrators		
Groups	1	smartsunguide.com/TMC Groups/Security Groups/SolarWinds Service Desk/ServiceDesk_Administrators		
	2	ServiceDesk_ServiceAgent		
	3	ServiceDesk_HumanResource		
	4	ServiceDesk_Requestor		
	5	ServiceDesk_HelpDeskAgent		

Figure 40. SolarWinds Service Desk Group Assignments

TREND MICRO WORKLOAD SECURITY AGENT- TURN ON MAINTENANCE MODE

Steps/Screenshots

1. Sign to **Okta**.

- a. Click the following link to access the Okta website: <https://smartsunguide.okta.com>.

Note: The UserPrincipalName (UPN) format (i.e., username@domain.com) is required when entering your username in the username field to sign to Okta.

- b. Using the UPN format,

- Enter your SMART SunGuide admin credentials.
- Click **Sign in**.

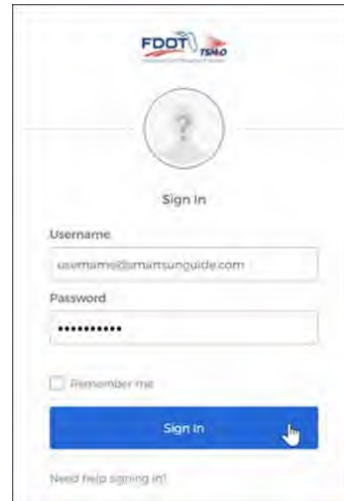


Figure 41. Okta Sign in Page

2. Once signed in,
Click **Trend Micro Workload Security Agent** app.



Figure 42. Trend Micro Workload Security App

- a. Click **Computers**.

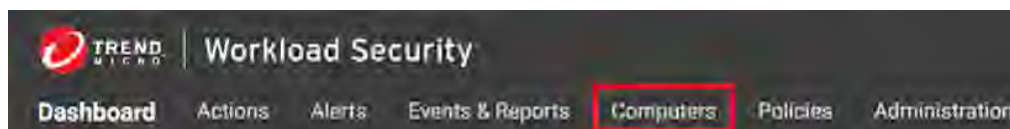


Figure 43. Workload Security > Computers

- b. From the list of computers → Select **server** you are going to patch.

Steps/Screenshots

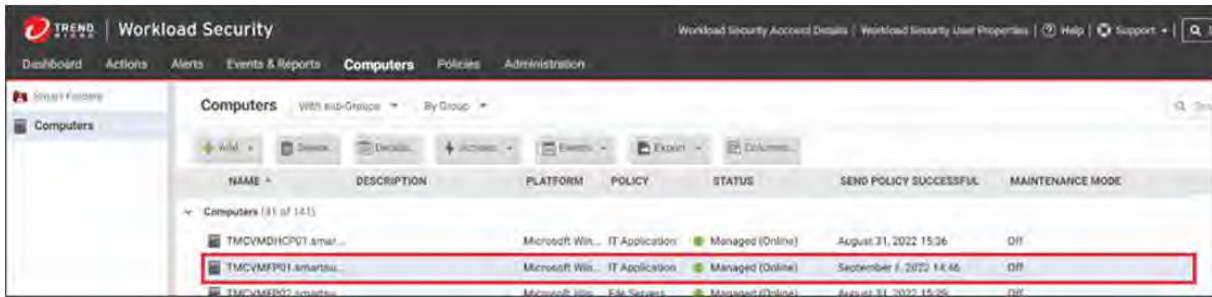


Figure 44. Select the Server

- (1) Right Click the **server**.
- (2) Click **ACTIONS**.
- 3) Click **Turn On Maintenance Mode**.
- 4) Select the **time duration** for the outage.

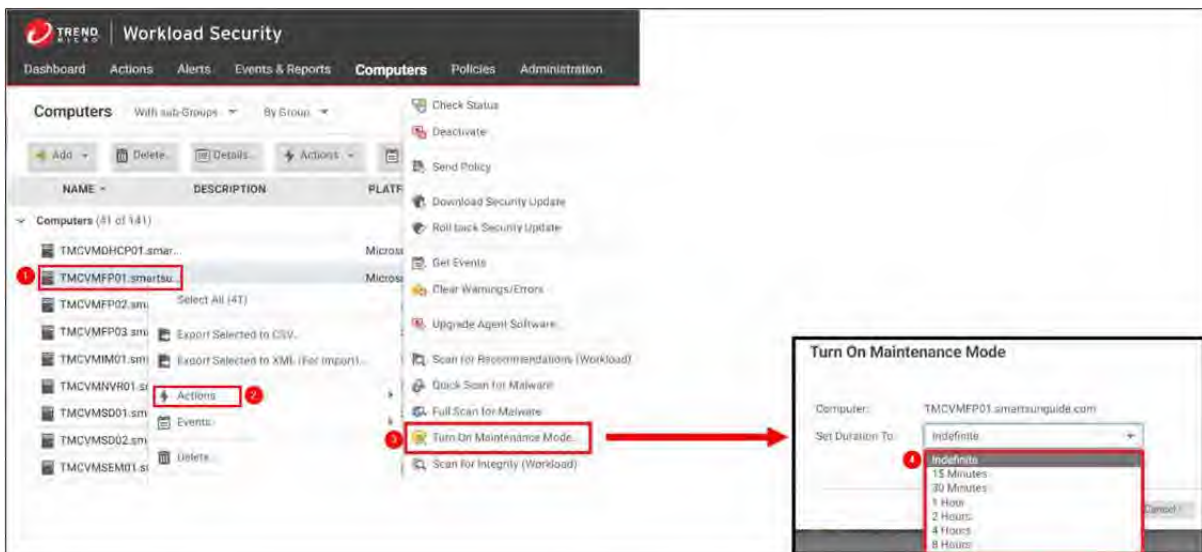


Figure 45. Turn On Maintenance Mode

Note. The server entry will change to **Start Requested** and then, -- to a **duration** you selected. Here, a duration was selected as **indefinite**.

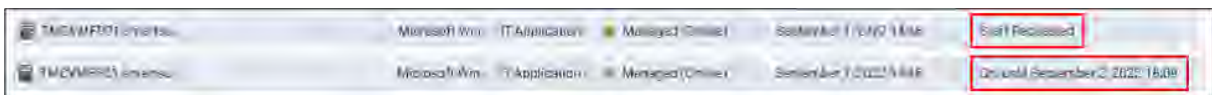


Figure 46. Server Entry - Start Requested > Duration

- c. Prior to moving to the next server → Ensure the current server is not in **Maintenance Mode**.



7.35 Servers Software

Document History

Version #	Date	Author	Changes
1.0	2/08/2024	Yana Neishlos	Initial Draft

Table of Contents

UPGRADE THE SOFTWARE PACKAGE ON THE DELL EMC POWERSTORE SAN	4
---	---

UPGRADE THE SOFTWARE PACKAGE ON THE DELL EMC POWERSTORE SAN

Steps / Screenshots

1. In **RTMC-PowerStoreSAN**, Click **Settings**, Click **Upgrades**, check the box next to **2.01.1-1471924-retail**, and Click **HEALTH CHECK**.

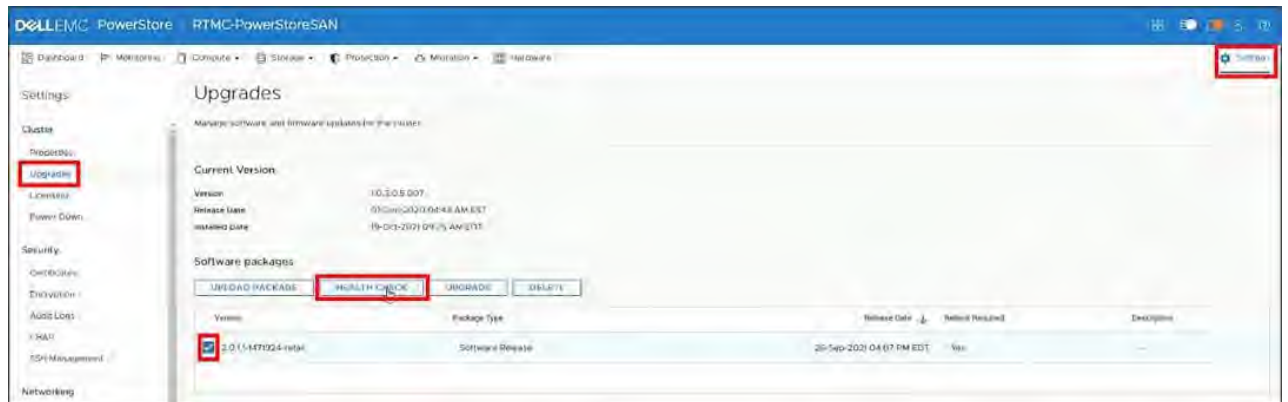


Figure 1. Perform Pre-Upgrade Health Check

2. Once the **Pre-Upgrade Health Check** is completed, → proceed to step 3.



Figure 2. Pre-Upgrade Health Check Completed

3. Check the box next to **2.01.1-1471924-retail**.
Click **UPGRADE**.



Figure 3. Pre-Upgrade Health Check Completed

Steps / Screenshots

4. Click **UPGRADE NOW**.

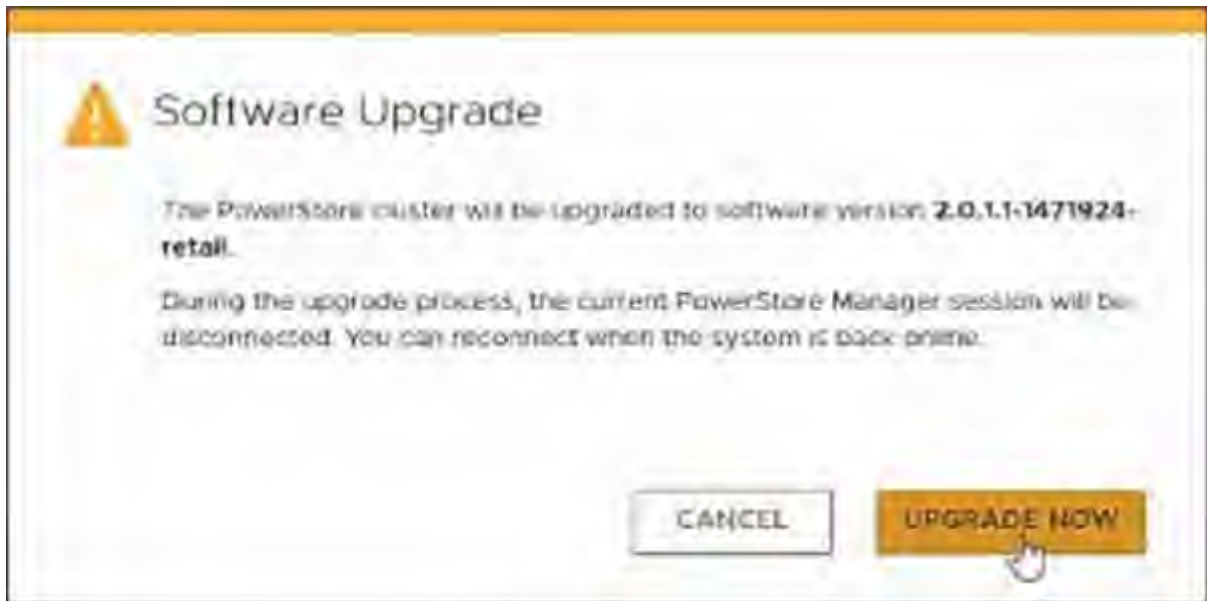


Figure 4. Software Upgrade



7.36 Workstations Software

Document History

Version #	Date	Author	Changes
1.0	12/28/2023	Yana Neishlos	Initial Draft

Table of Contents

MICROSOFT WINDOWS UPDATE MANAGEMENT.....	4
Overview	4
Procedures.....	4
Standard Updates.....	4
Emergency Security Updates.....	5
SET UP THE MICROSOFT MANAGEMENT CONSOLE	6
Overview	6
Procedures.....	7
Launch the Windows Console Root	7
Add/Remove Snap-Ins.....	9
Save the Console Root Under Standard User > Downloads Folder	18
Save the Console Root in Common Desktop	19

MICROSOFT WINDOWS UPDATE MANAGEMENT

Overview

When Microsoft releases Windows updates, the IT Department deploys them to all applicable workstations (i.e., desktops and laptops).

To confirm functionality of all Windows updates prior to deployment, they are properly tested as outlined in the procedures below.

Procedures

Standard Updates

1. Newly released Windows updates for applicable desktop versions are deployed on virtual desktop test virtual machines. Once deployed, preliminary functionality testing is performed on pre-installed applications.
2. After an introductory testing is complete, Windows updates are approved and deployed on all IT staff workstations. A four-day lead time testing is performed on these workstations.
3. Once a functionality is confirmed on all IT workstations Windows updates are:
 - Deployed on Lead Operator workstations in the Control Room, and,
 - Tested for seven days.

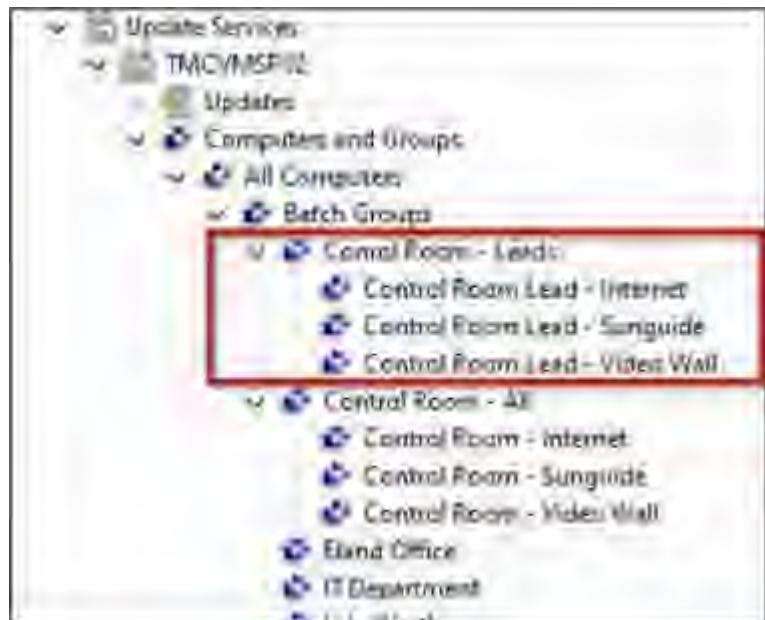


Figure 1. Lead Operator Workstations

4. After seven days of a confirmed functionality, updates are deployed on all workstations.

Emergency Security Updates

1. Newly released security updates for applicable desktop versions are deployed on virtual desktop test virtual machines.

Once deployed preliminary functionality testing is performed on pre-installed applications.

2. After introductory testing is complete, security updates are approved and deployed on all IT staff workstations.

A two-day lead time testing is performed on these workstations.

3. Once functionality is confirmed on IT workstations, updates are deployed on Lead Operator workstations in the Control Room (Figure 1 above) and tested for five days.

4. After five days of confirmed functionality updates are deployed on all workstations.

SET UP THE MICROSOFT MANAGEMENT CONSOLE

Overview

Procedures below are provided for customers frequently using the Microsoft Management Console (MMC) as a single sign-on to the Windows administrative tools.

Instead of signing to these Windows administrative tools individually, you can get access to all of them by signing to the MMC with your SunGuide admin account credentials one time.

These procedures outline the steps to add/save the following frequently used Windows administrative tools to your Console Root (ToolBox):

- Active Directory for Domains and Trust
- Active Directory Sites and Services
- Active Directory Users and Computers
- Computer Management
- DFS Management
- DHCP
- DNS
- Local Users and Groups
- Patch Manager.

Procedures

Launch the Windows Console Root

Steps / Screenshots

1. – Press the **Windows+R** keys.
– Launch the “Run” command window.

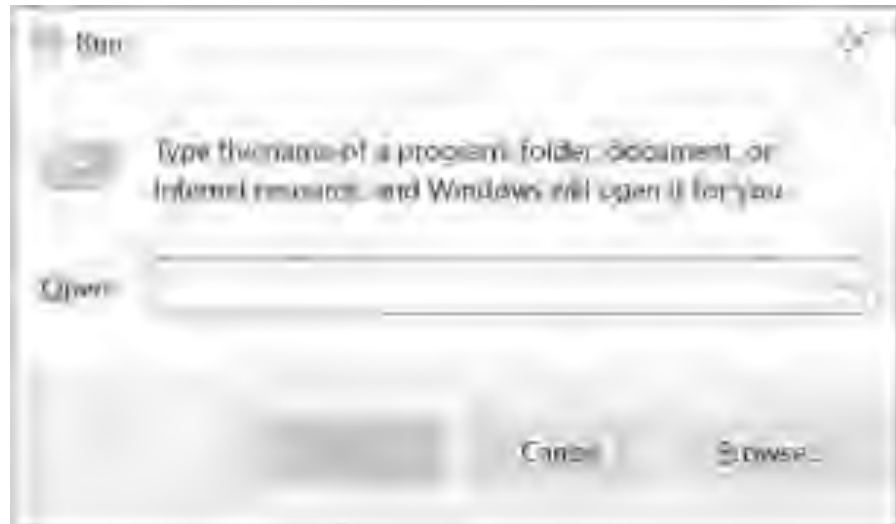


Figure 2. Launch "Run" Command Window

2. – Type “**mmc**” in the “Run” command window.
– Click **OK**.

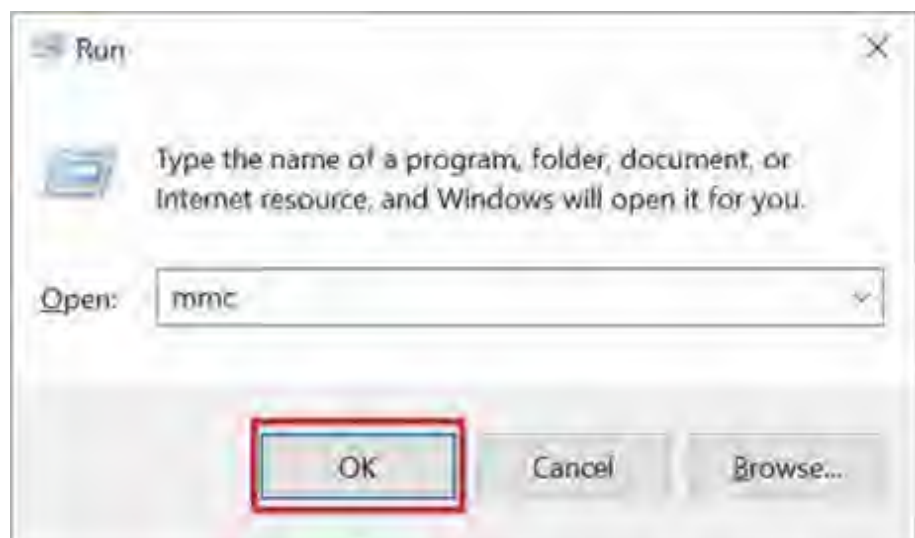


Figure 3. Type “mmc” in the “Run” Command Window

Steps / Screenshots

- Press the **Control+Shift+Enter** keys.
- Launch the MMC login screen: Enter your SunGuide admin account credentials to launch the Windows Console Root.

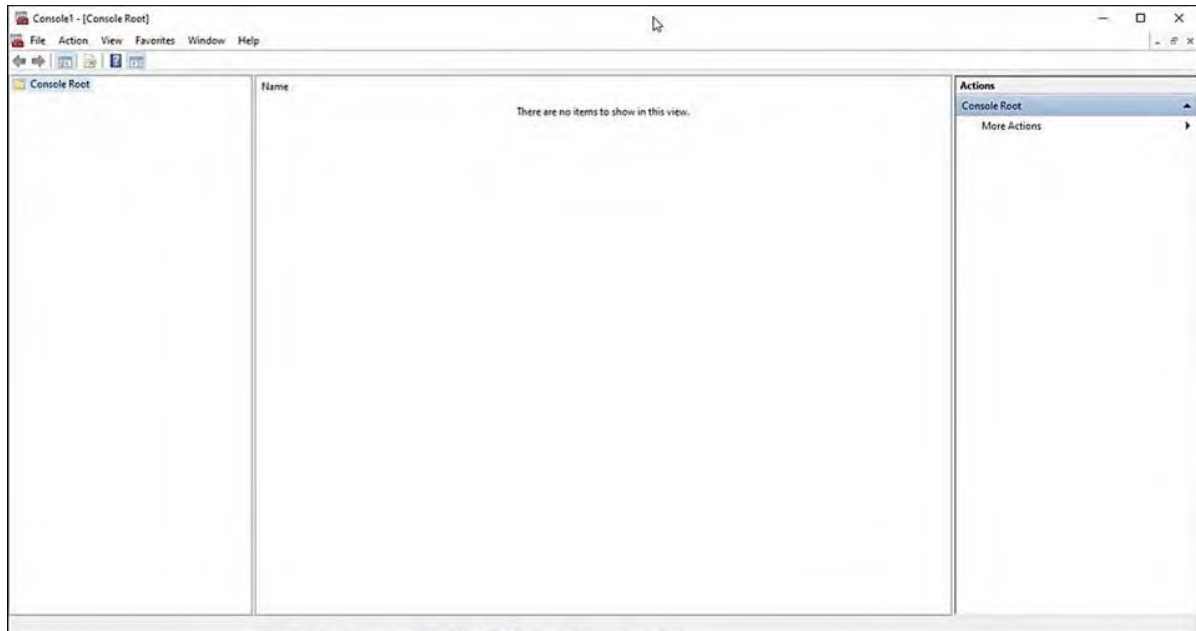


Figure 4. Windows Console Root

- Click **File**
- Select **Add/Remove Snap-ins** from the drop-down menu.
- Launch the Add or Remove Snap-ins window.

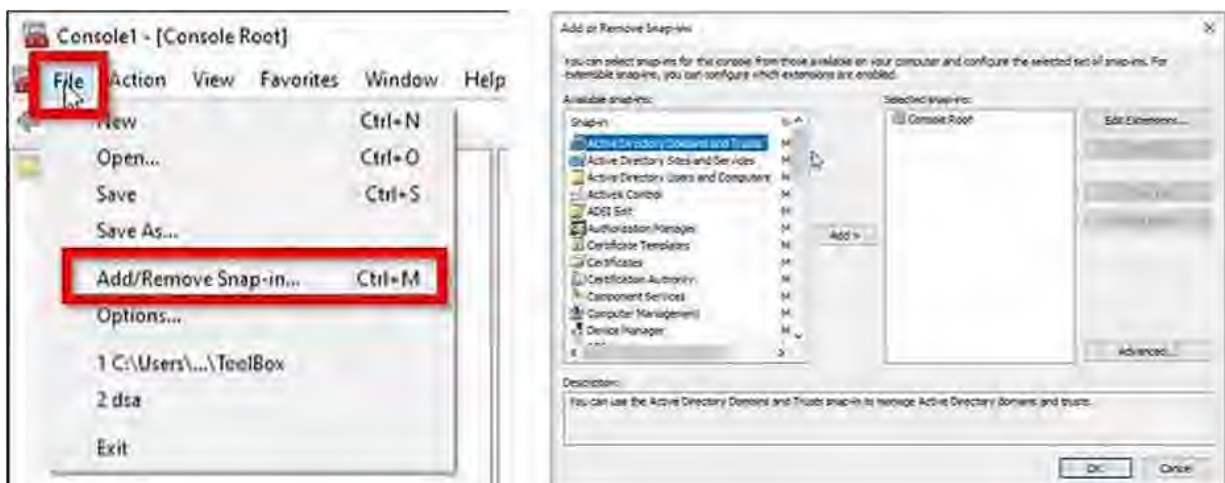


Figure 5. Add/Remove Snap-ins

Add/Remove Snap-Ins

Notes / Steps / Screenshots

Note.

The left-hand column lists the available snap-ins on a device.

The Console Root is on the right-hand column.

Perform the steps below to add frequently used IT administrative tools /snap-ins to the Console Root:



Figure 6. Available Snap-ins on a Device

1. Add **Active Directory for Domains and Trust, Active Directory Sites and Services, and Active Directory Users and Computers** to the Console Root.

- a.
 - Double-click **Active Directory for Domains and Trust**.
 - Add it to the Console Root.

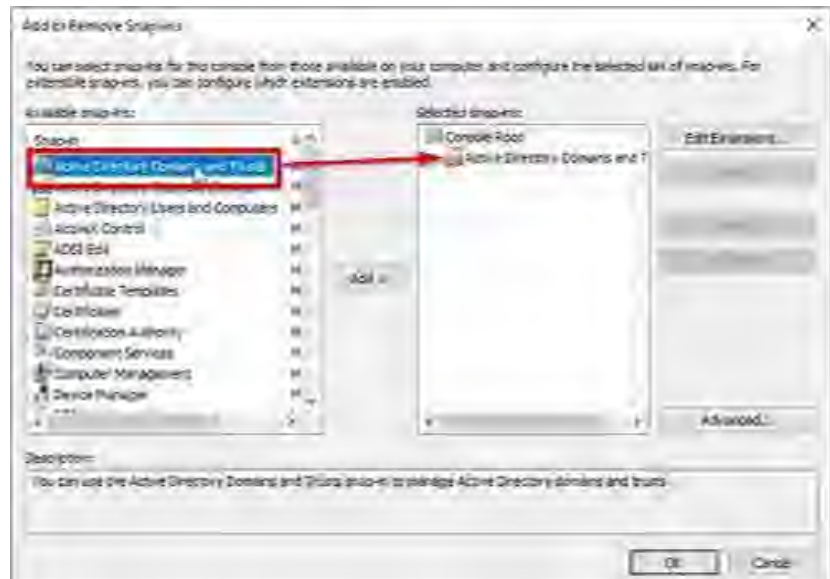


Figure 7. Add Active Directory Domains and Trusts

Notes / Steps / Screenshots

- b. – Double-click on **Active Directory Sites and Services**
- Add it to the Console Root.



Figure 8. Add Active Directory Sites and Services

- c. – Double-click **Active Directory Users and Computers**
- Add it to the Console Root (Figure 9).

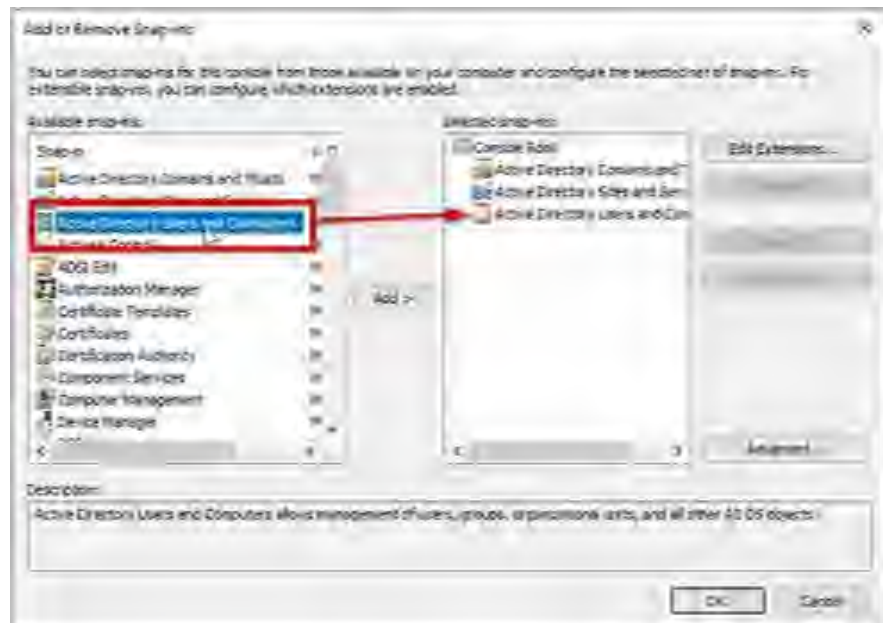


Figure 9. Add Active Directory Users and Computers.

Notes / Steps / Screenshots

2. Add Computer Management to the Console Root.

a. Double click on **Computer Management**.

b. In the **Computer Management** window,

- Select Local computer.
- Check the box to Allow a selected computer to be changed when launching from the command line (to switch between a local computer and another computer).

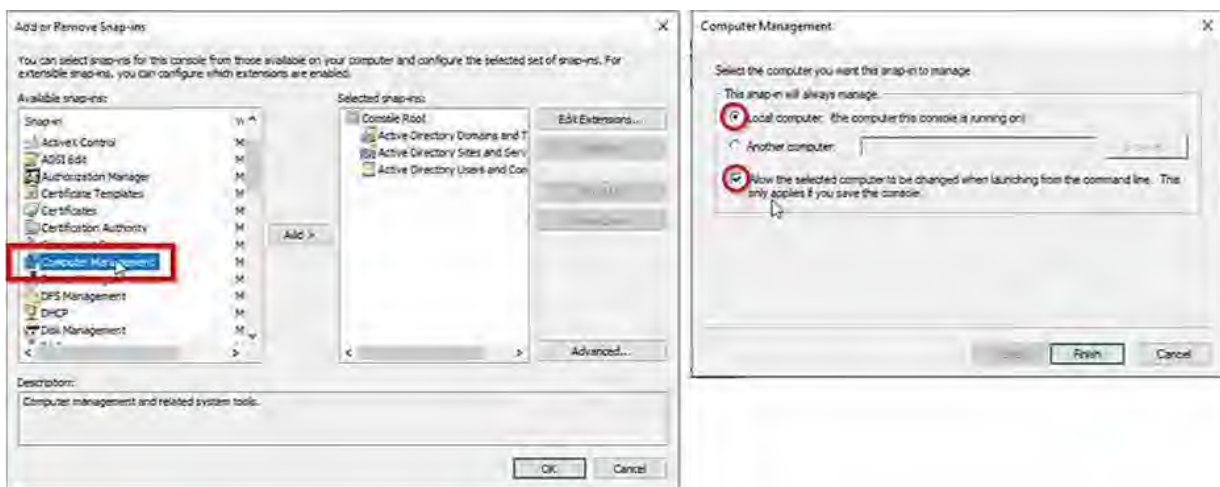


Figure 10. Computer Management Selection

c. Click **Finish** to close the Computer Management window and add Computer Management to the Console Root.

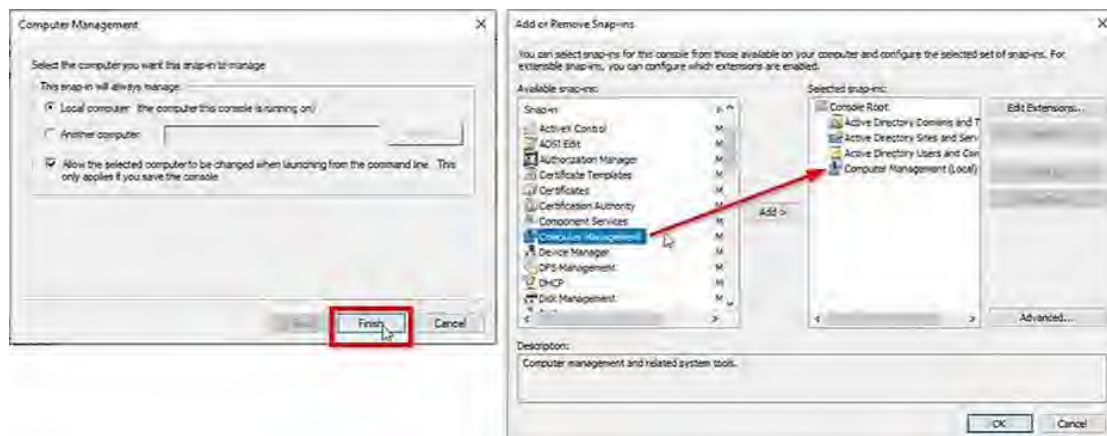


Figure 11. Add Computer Management

Notes / Steps / Screenshots

3. Add DFS Management, DHCP, and DNS to the Console Root.

- a. – Double click on **DFS Management**
- Add it to the Console Root.

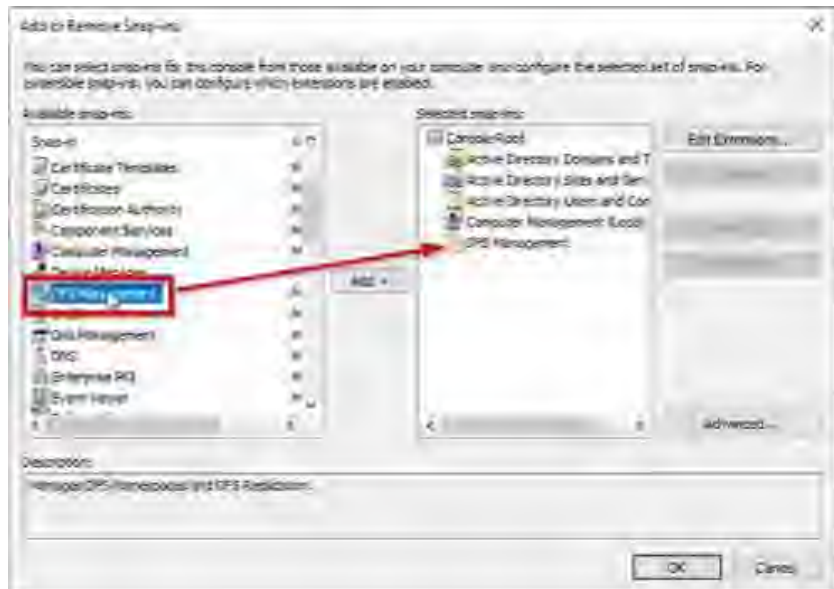


Figure 12. Add DFS Management

- b. – Double-click **DHCP**.
- Add it to the Console Root.



Figure 13. Add DHCP

Notes / Steps / Screenshots

- c. – Double click on **DNS**
- Add it to the Console Root.

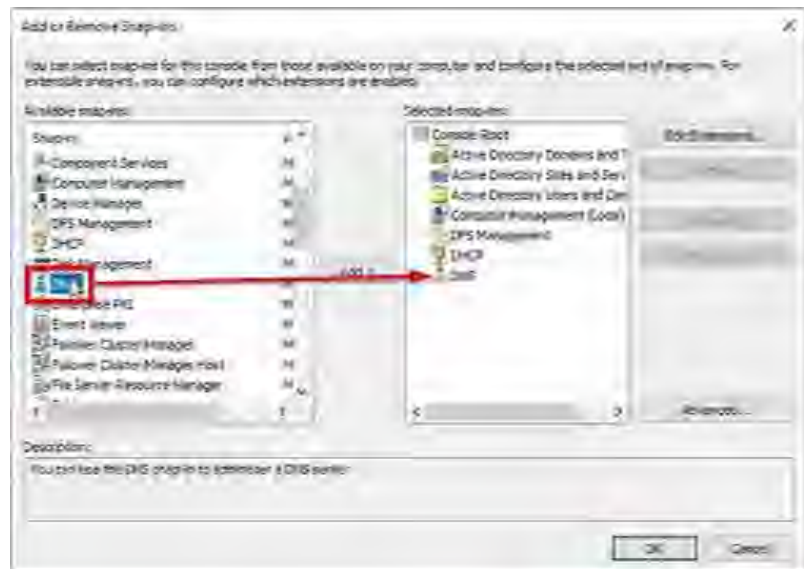


Figure 14. Add DNS

4. Add **Local Users and Groups** to the Console Root.

- a. Double-click **Local Users and Groups**.
- b. In the **Choose Target Machine** window,
- Select **Local computer**, and,
 - Check the box to **Allow the selected computer to be changed when launching from the command line** (to switch between a local computer and another computer).

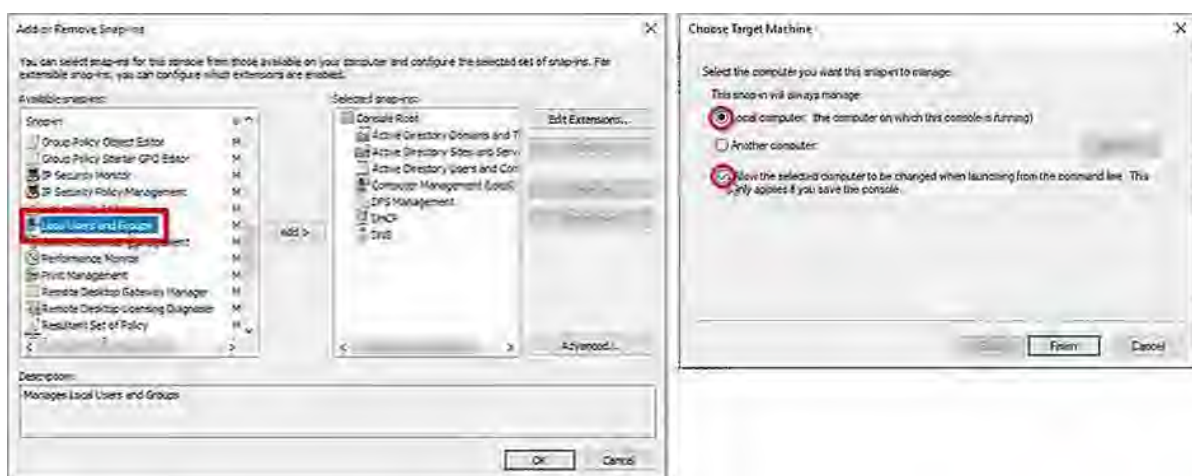


Figure 15. Local Users and Groups Options

Notes / Steps / Screenshots

- c.
 - Click **Finish** to close the Choose Target Machine window, and,
 - Add Local Users and Groups to the Console Root.

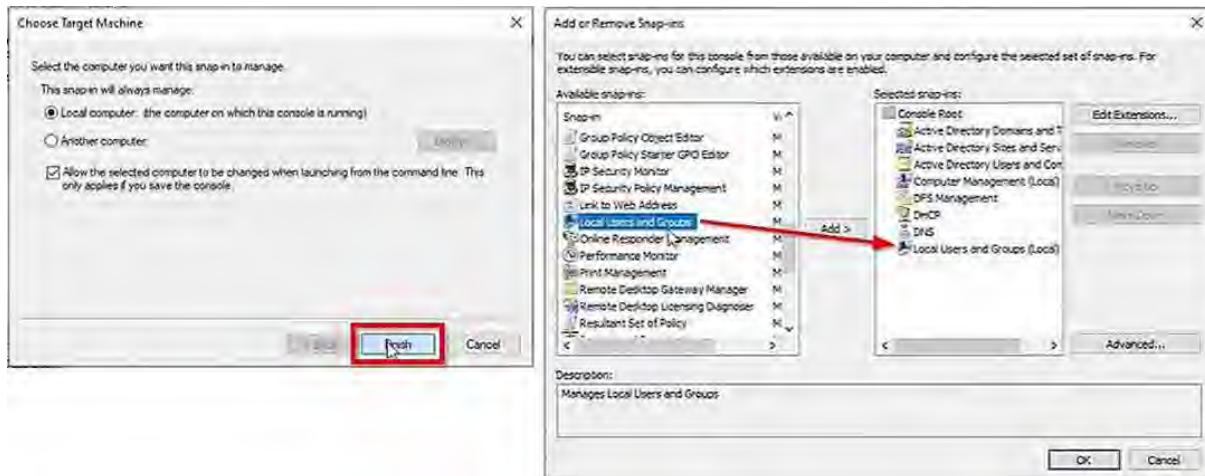


Figure 16. Add Local Users and Groups

5. Add Print Management to the Console Root.

- a. Double click on **Print Management**.
- b. In the **Specify Print Server** field of the Configure Print Management window,
 - Enter TMCVMFP01
 - Click **Add to List**.

Notes / Steps / Screenshots

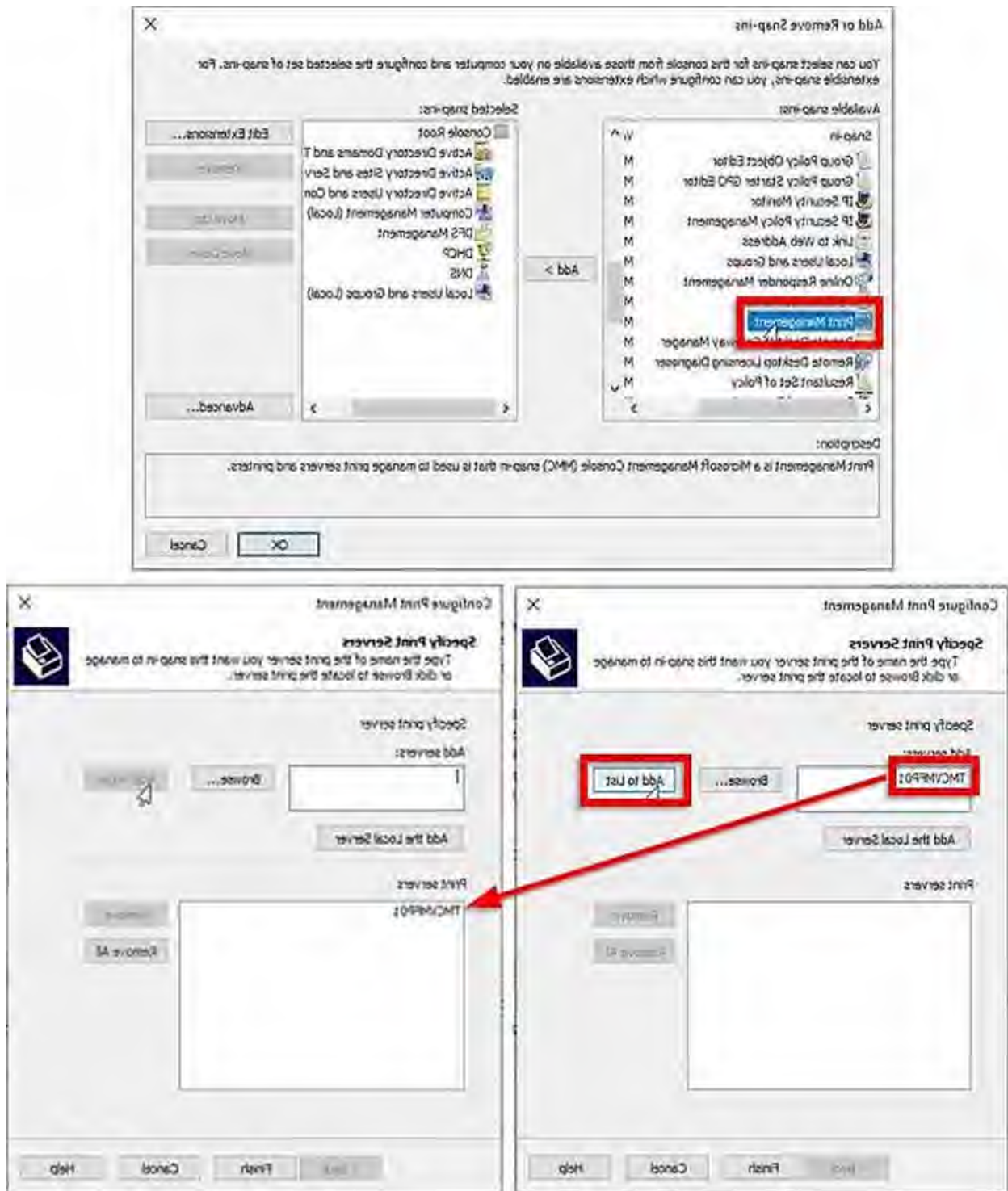


Figure 17. Add Print Server

Notes / Steps / Screenshots

- c.
 - Click **Finish** to close the Configure Print Management window, and,
 - Add **Print Management** to the Console Root.

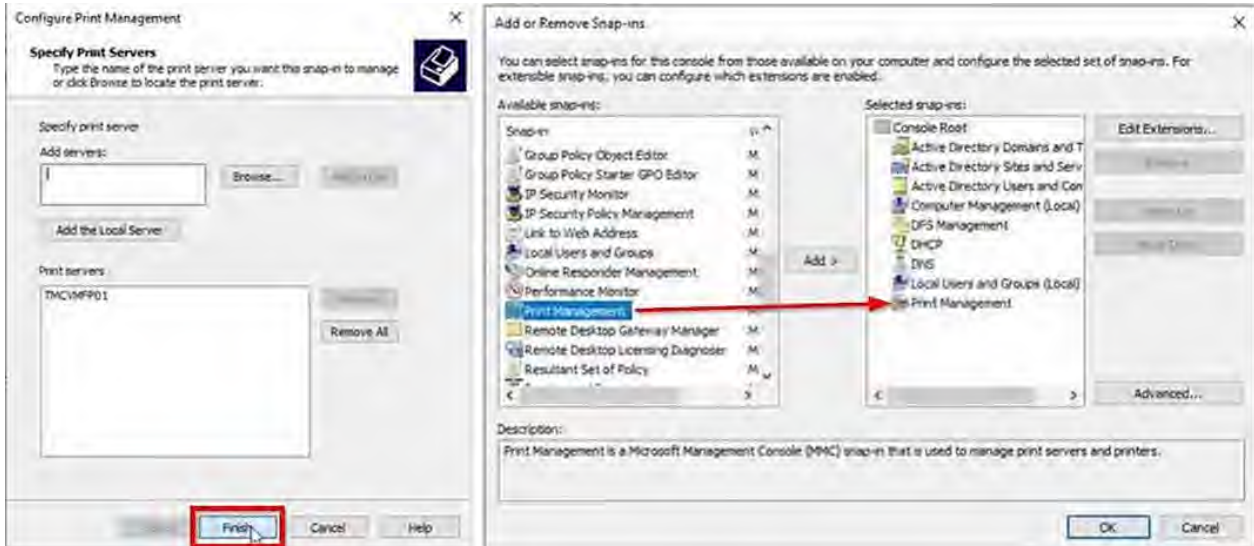


Figure 18. Add Print Management

6. Add **Patch Manager** to the Console Root.

- Double-click **SolarWinds Patch Manager**
- Add it to the Console Root.

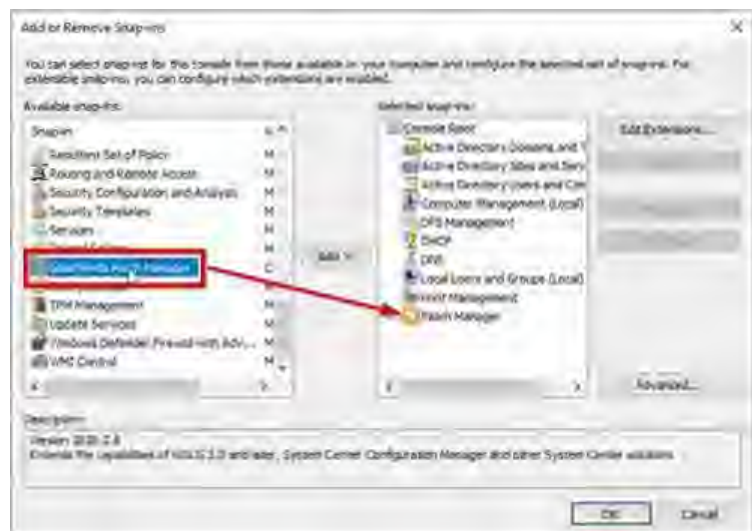


Figure 19. Add Patch Manager

Notes / Steps / Screenshots

7. Add selected snap-ins under the Console Root.

- a. Click **OK** to close the **Add or Remove Snap-ins** window.

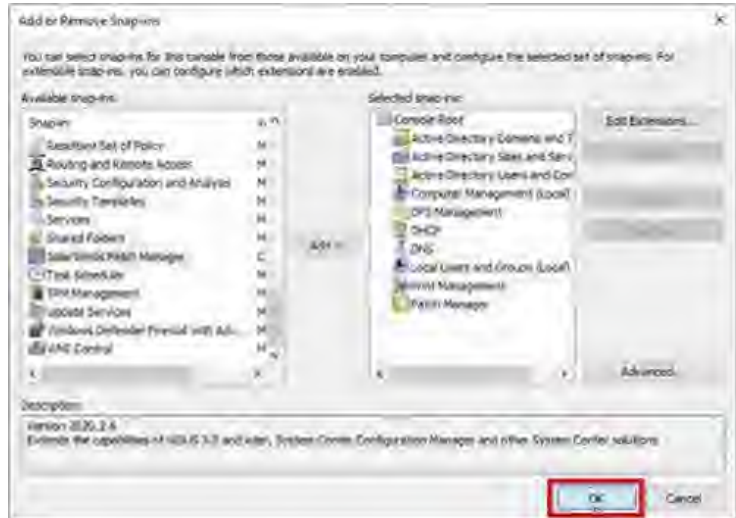


Figure 20. Close the Add or Remove Snap-ins Window

- b. The selected snap-ins are added under the **Console Root**.

You are signed to all of them with your single sign-on SunGuide admin account credentials.



Figure 21. Snap-ins Added Under the Console Root

Save the Console Root Under Standard User > Downloads Folder

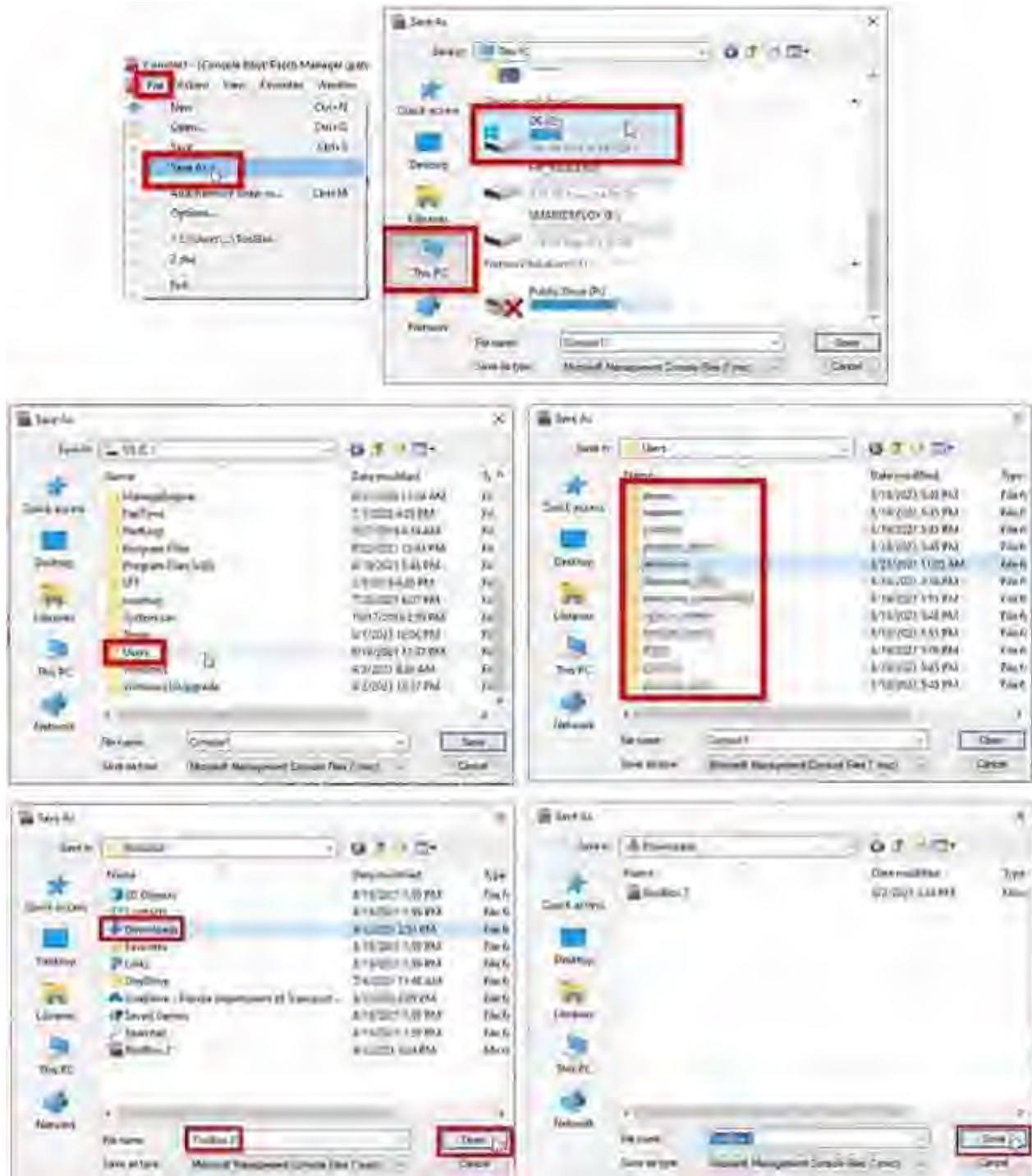


Figure 22. Save the Console Root under the Standard User > Downloads Folder

Refer to the Figure 22 above and complete the following procedure below:

1. – Click **File**
– Select **Save As**.

2.
 - Click **This PC**
 - Click **OS (C:)**
3. Click the **Users** folder.
4. Select your user folder.
5.
 - Click **Downloads**
 - Enter a name in the **File name** field.
 - Click **Open**.
6. Click **Save**.

Save the Console Root in Common Desktop

1.
 - Press the **Windows+R** keys.
 - Launch the “Run” command window.
2.
 - Type “**shell:common desktop**” in the “Run” command window
 - Click on **OK**.

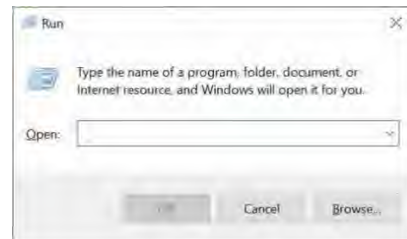


Figure 23. Launch "Run" Command Window

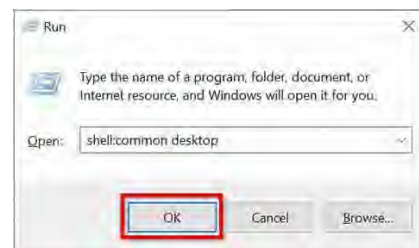


Figure 24. "shell:common desktop

Note: When launching your Toolbox from the saved location:

Right-click, and,

Select **Run as Administrator** with your SunGuide admin account credentials.

Otherwise, added Windows administrative tools / snap-ins will not be accessible with a single sign-on, as needed.

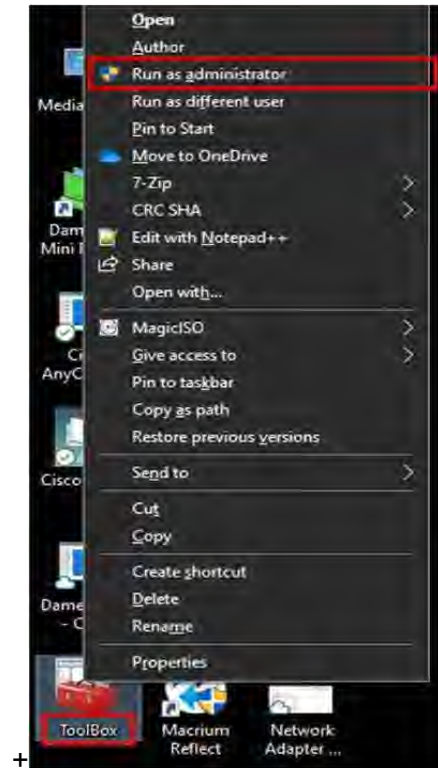


Figure 25. Run as Administrator



7.41.00 High-Profile Visiting Dignitary Plan

Table of Contents

INTRODUCTION.....4

 Purpose4

 Scope.....4

BLOCK CCTV on IVDS, DIVAS and FL511.....5

 Block Broadcast to Media Stations5

 DMS Messages6

Document Version History

Version #	Date	Author	Changes
1.0	2/07/2024	Yana Neishlos	Initial Draft

INTRODUCTION

The High-Profile Visiting Dignitary Plan is a comprehensive set of protocols and strategies to manage the visit of a distinguished member of the Presidential Office of the United States of America.

The primary objective of this plan is to ensure that all pertinent action steps are clearly delineated and coordinated among all involved parties.

Purpose

The plans will ensure that all necessary advanced preparations are in place, thus minimizing the potential for any unforeseen disruptions or challenges during the visit.

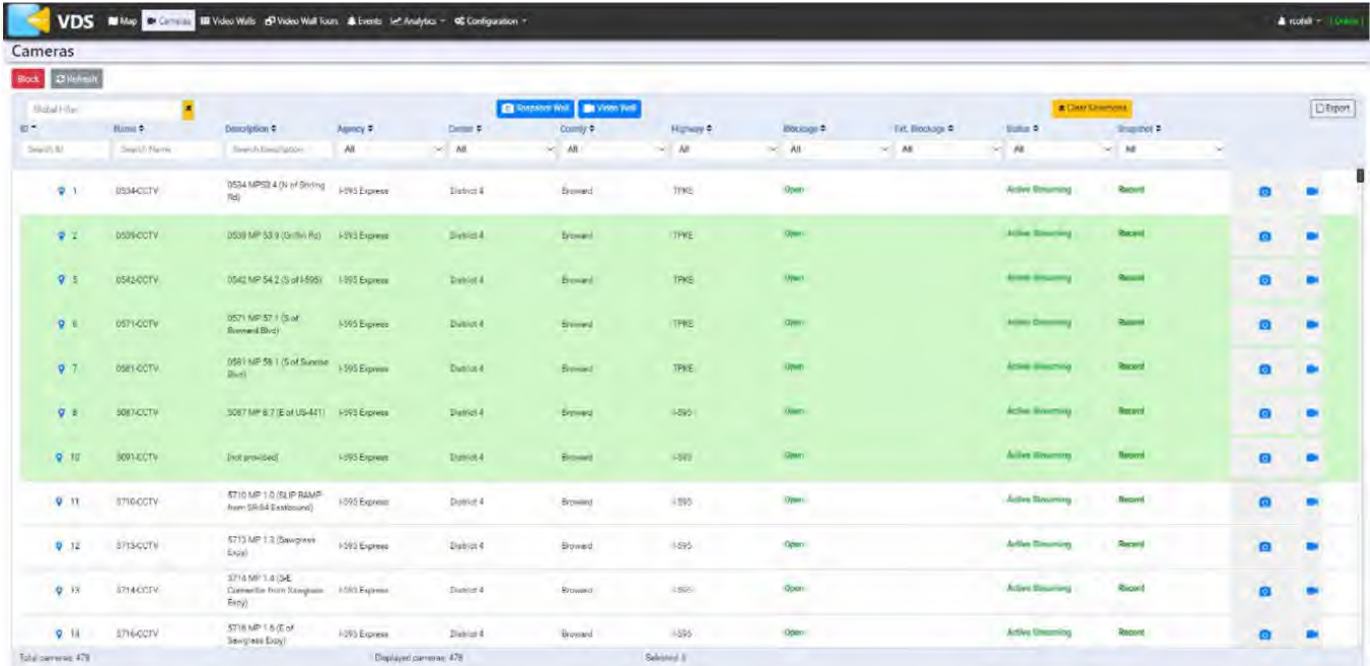
Scope

The High-Profile Visiting Dignitary Plan is developed for TSM&O Operations and affiliated agencies.

Action steps will involve reducing the visibility of the transportation route used during the visit of the High-Profile Visiting Dignitary.

BLOCK CCTV on IVDS, DIVAS and FL511

- iVDS - Internet Video Distribution System
- DIVAS - Data Integration and Video Aggregation System
- FL511 – Florida 511 Travel Information System.



1. Login to the user interface.
2. For a user with sufficient permissions:
 - a. Select one or more cameras in the grid.
 - b. Click the 'Block' or 'Unblock' buttons to block or unblock those cameras, respectively.
3. Once all desired cameras are selected → Complete the blockage → Click **Save**.

Block Broadcast to Media Stations

- Block communication to all media outlets and TV Stations including [TrafficLand](#) Incorporated.
- Contact District VI ITS and request to shut down the uplink for the duration of the visit:

Name	Contact
Thomas Miller	Thomas.Miller@sunguide.info
Juan Lopez	Juan.Lopez@sunguide.info
Alex Mirones	Alex.Mirones@sunguide.info

DMS Messages

The Operations Center will ensure that no messages will be displayed on the DMS signs along the motorcade route throughout the duration of the visit.



Acronyms & Glossary of Terms

Table of Contents

The List of Acronyms	4
Glossary of Terms	13

Document & Version History

Version #	Date	Author	Changes
1.0	12/13/2023	Yana Neishlos	Initial Draft

The List of Acronyms

A - L

Acronym	Description
AARF	Automated Access Request Form
ACL	Access Control List
AD	Active Directory
ADAPT	Active Device and Performance monitor Dashboard
ADMS	Arterial Dynamic Message Signs
AMS	Arterial Maintenance System
AOR	Area of Responsibility
ASA	Adaptive Security Appliance
ATIS	Advanced Traveler Information System
ATMS	Advanced Traffic Management System
AUA	Acceptable Use Agreement
AVI	Automatic Vehicle Detection
BCT	Broward County Transit
BCTED	Broward County Traffic Engineering Department
CAB	Change Advisory Board
CAD	Computer Aided Dispatch
CADD	Computer Aided Drafting and Design
CCTV	Closed-Circuit Television
CD-ROM	Compact Disk - Read Only Memory
CFX	Central Florida Expressway Authority
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer

Acronym	Description
CISA	Cybersecurity & Infrastructure Security Agency
CITS	Contract Invoice Transmittal System
CMDB	Configuration Management Database
CPU	Central Processing Unit
COBIT	Control Objectives for Information and Related Technologies
COOP	Continuity of Operations Plan
COTS	Commercial-off-the-Shelf
CPM	Certified Public Manager
CPU	Central Processing Unit
CSAR	Computer Security Access Request
CUCM	Cisco Unified Communications Manager
CVSS	Common Vulnerability Scoring System
D4	District Four
DART	Data Analysis and Reporting Tool
DDoS	Distributed Denial of Service
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DID	Direct Inward Dialing
DISM	District Information System Manager
DMS	Dynamic Message Sign
DMZ	Demilitarized Zone
DNS	Domain Name System
DOD	Department of Defense
DOT	Department of Transportation

Acronym	Description
DR	Disaster Recovery
DVD	Digital Video Disk
ELS	Express Lane System
EOC	Emergency Operations Center
ESRI	Environmental System Research Institute
ESU	Emergency Shoulder Use
F.A.C.	Florida Administrative Code
F.S.	Florida Statute
FDOT	Florida Department of Transportation
FHP	Florida Highway Patrol
FION	Florida ITS Operations Network
FIPS	Federal Information Processing Standards
FL511	Florida 511
FLAIR	Florida Accounting Information Resource
FLATIS	Florida's Advanced Traveler Information System
FLL	Fort Lauderdale-Hollywood International Airport
FMS	Freeway Maintenance System
FP&L	Florida Power & Light
FSMO	Flexible Single Master Operation
FTA	File Transfer Appliance
FTE	Florida Turnpike Enterprise
FTP	File Transfer Protocol
GAL	Global Address List
GB	Gigabyte

Acronym	Description
GIS	Geographic Information Systems
GPS	Geographic Positioning System
GUI	Graphical User Interface
HAR	Highway Advisory Radio
HARB	Highway Advisory Radio Beacon
HART	Highway Advisory Radio Transmitter
HD	High Definition
HOT	High-Occupancy Toll
HOV	High Occupancy Vehicle
HQ	Headquarters
HTTPS	Hyper Text Transfer Protocol Secure
HW	Highway
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IRR	Information Resource Request
iSCSI	Internet Small Computer Systems Interface
ISE	Identity Services Engine
ISM	Information Security Manager
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITS	Intelligent Transportation Systems
ITSFM	ITS Facility Management

Acronym	Description
iVDS	Internet Video Distribution System
iVEDDS	Interagency Video Event Data Distribution System
KVM	Keyboard, Video Monitor, and Mouse
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting-Diode

M - Z

Acronym	Description
MDM	Mobile Device Manager
MDX	Miami-Dade Expressway Authority
MFA	Multifactor Authentication
MIMS	Maintenance and Inventory Management System
MOT	Maintenance of Traffic
MT	Maintenance
MTTR	Mean Time to Respond
MUTCD	Manual of Uniform Traffic Control Devices
MVDS	Microwave Vehicle Detection System
NAS	Network Attached Storage
NAT	Network Address Translation
NH	Non-Highway
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NMS	Network Management Systems

Acronym	Description
NTH	Non TMC Hardware
NTP	Network Time Protocol
OCO	Operating Capital Outlay
OIT	Office of Information Technology
OOB	Out-of-Band
OS	Operating System
OSPF	Open Shortest Path First
P3	Public-Private Partnership
PBX	Private Branch Exchange
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Portable Digital Assistant
PIO	Public Information Office
PMR	Property Management Report
PMRS	Property Management Report System
PRI	Primary Rate Interface
PTR	Property Transfer Receipt
PTZ	Pan-Tilt-Zoom
RA	Room Alert
RACF	Resource Access Control Facility
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RAS	Remote Access Server
RDP	Remote Desktop Protocol
RFC	Request for Change

Acronym	Description
RFID	Radio Frequency Identification
RISC	Rapid Incident Scene Clearance
RITIS	Regional Integrated Transportation Information System
RMA	Return Merchandise or Material Authorization
ROM	Read-Only Memory
RPO	Recovery Point Objective
RSTP	Rapid Spanning Tree Protocol
RTMC	Regional Transportation Management Center
RTO	Recovery Time Objective
RWIS	Road Weather Information Systems
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDLC	Software Development Life Cycle
SERFTOC	Southeast Florida Regional TMC Operations Committee
SELS	Statewide Express Lanes Software
SES	Select Exempt Service
SFRTA	South Florida Regional Transportation Authority
SFTP	Secure File Transfer Protocol
SIRV	Severe Incident Response Vehicle
SKU	Stock Keeping Unit
SLA	Service Level Agreement
SMART	System Management for Advanced Roadway Technologies

Acronym	Description
SMS	Senior Management Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOG	Standard Operating Guidelines
SOP	Standard Operating Procedure
SQL	Structured Query Language
SSH	Secure Shell
SSO	Single Sign-On
STMC	Satellite Transportation Management Center
STP	Spanning Tree Protocol
TAC	Technical Assistance Center
TB	Terabyte
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TIM	Traffic Incident Management
TIMSO	Traffic Incident Management Support Office
TMC	Transportation Management Center
TOQC	TMC Operations Quality Control
TSM&O	Transportation Systems Management and Operations
UC	Unified Communications
USB	Universal Serial Bus
UPS	Uninterruptible Power Supply
VDS	Vehicle Distribution Systems
VDU	Virtual Display Unit / Video Display Unit
VID	Video Incident Detection

Acronym	Description
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMS	Video Management System
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
VPR	Vulnerability Priority Rating
WAN	Wide Area Network
WSUS	Windows Server Update Services
WWD	Wrong Way Driver
WWW	World Wide Web

Glossary of Terms

Term	Description
Access	An ability to acquire, read, write, or delete data or information; make use of an information technology resource; enter a room or facility. (Source: Rule 71A-1.002, F.A.C.)
Access Point	A station that transmits and receives data e.g., a wireless access point. (Source: Rule 71A-1.002, F.A.C.)
Active Directory	<p>A Microsoft service, a central component of the Windows® operating system platform. A directory service:</p> <ul style="list-style-type: none"> – Provides a place to store information about network-based entities, e.g., applications, files, printers, and people. – Provides a consistency to name, describe, locate, access, manage, and secure information on information resources. – Acts as the main switchboard of the network operating system. It is the central authority that manages identities and brokers, the relationships among the distributed information resources to work together. – Supplies fundamental network operating system functions. – Must be synchronized with the management and security mechanisms of the operating system to ensure the network integrity and privacy. <p>It is critical to define/maintain the network infrastructure, system administration, and control user experience of the Department information systems.</p>
Active Directory Domain	A single security boundary of a Windows-based computer network. There are multiple domains; they can span more than one physical location. On a standalone workstation, a domain is a computer itself. Every domain has its own security policies and security relationships with other domains. When multiple domains are connected by trust relationships and share a common schema, configuration, and global catalog, they constitute a domain tree. Multiple domain trees can be connected to create a forest.
Active Directory Group	A Windows group that simplifies security by allowing access rights to be granted to a group of people rather than individuals.
Application	A computer-based information system; supports a specific business function of the Department. An application includes both manual and computerized procedures for source transaction origination, data processing, record keeping, and report preparation.
Authentication	A process to validate credentials for claiming a digital identity. (Source: Rule 74-5.001, F.A.C.)
ATMS	Advanced Traffic Management Systems. ATMS deployment along arterials within Broward and Palm Beach County includes the city of Boca Raton.

Term	Description
Broward County Advanced ITS	A combination of arterial DMS, highway advisory radio (HAR), road weather information systems (RWIS) and a wireless redundant communications system (Voice over IP).
Broward RTMC	Broward Regional Transportation Management located at Florida Department of Transportation District Four.
Broward Phases I and II	This phase took place in 2006-2007. This portion of the Broward ITS deployment included Palm Beach TMC construction, northern counties satellite control room design, and the development of detailed design as requests for proposals for Palm Beach and northern county deployments. .
Broward Phase II	This phase took place in 2007. This portion of the Broward ITS deployment included development and execution of memorandums of understanding for sharing fiber with local agencies as part of Palm Beach and Northern Counties ITS, and the northern counties satellite control room installation. .
Browser	A computer program or a software application allowing a user Web access and display of documents.
Change Management	A method to monitoring and controlling change within the project.
File Transfer Protocol (FTP)	A protocol commonly used in the moving files over a network or the Internet without a using a web browser.
511/FLATIS	Florida 511 is the Florida DOT telephone traffic information system. 511 is part of Florida's Advanced Traveler Information System (FLATIS) program that is operated under the SunGuide Software.
Hypertext Markup Language (HTML)	A primary coding language to create web pages and parts of web applications; HTML code – for a browser to produce the final appearance of a web page or web application.
Hypertext Transport Protocol (HTTP)	A protocol to move files across a network, primarily HTML; intended to be viewed/interpreted by a browser.
I-595	This portion of the ITS and new express/toll lanes along I-595; to be designed, constructed, and managed by I-595 Express LLC, in a public-private partnership with the FDOT for a 35-year period.
I-75 Safety Project	This initiative along I-75 in Alligator Alley uses speed and smoke detectors, along with speed warning messages for motorists to drive safer, slower along this portion of I-75.
I-95 Express	<p>The opening of this toll express lane on I-95 occurred in three phases.</p> <p><i>Phase 1A</i> – open; runs northbound on I-95 from I-195/SR-112 to the Golden Glades area north of 151st Street in Miami-Dade County.</p> <p><i>Phase 1B</i> - opened for tolling in 2010; runs southbound on I-95 from south of Miami Gardens Drive/NW 186th Street to north of I-395/SR-836; this phase</p>

Term	Description
	<p>has extended the northbound express lanes to the south from north of I-195/SR 112 to I-395/SR-836.</p> <p><i>Phase II</i> – has extended the express lanes for a continuous facility between I-395/SR-836 in Miami-Dade County and Broward Boulevard in Broward County. With anticipated project funding, Phase II - under construction from September 2010; open to traffic in Spring 2012.</p>
Least Privilege	<p>The principle grants the minimum possible privileges to permit a legitimate action to enhance data protection and functionality from faults and malicious behavior.</p>
Multifactor Authentication	<p>An authentication using two or more different factors. Factors include something one knows (e.g., password or personal identification number), something one has (e.g., cryptographic identification device, token), or something one is (e.g., physical location, biometric). (Source: Rule 74-5.001, F.A.C.)</p>
Northern Three Counties	<p>These counties include Martin, St Lucie, and Indian River.</p>
Northern Counties ITS Deployment	<p>This portion of the implementation of the northern counties ITS along I-95 in Martin, St Lucie, and Indian River counties – completed in 2010.</p>
Palm Beach ITS Deployment Phases A and B	<p>The Palm Beach County ITS deployment is divided into two phases along I-95: Phase A, south of PGA Boulevard, and Phase B to the north. As of 2010, the design is complete for Phase A, with 85% of the underground infrastructure constructed, and 30% of field devices installed. Scheduled completion for Phase A - September 2010, and February 2012 for Phase B.</p>
Remote Access	<p>Any access to an agency’s internal network through a network, device, or medium that is not controlled by the agency (such as the Internet, public phone line, wireless carriers, or other external connectivity). Remote access example: a virtual private network client connection (Source: Rule 71A-1.002, F.A.C.).</p>
Sanitizing	<p>Using a utility that provides a minimum of three passes of overwriting all addressable locations with a character, its complement, a random character and verifying. DOD 5220.22-M requirements accomplish this. This includes erasing data and/or reformatting magnetic tape media.</p>
TIMSO	<p>Traffic Incident Management Support Office, located in Fort Pierce.</p>
Virtual Private Network	<p>A communications network tunneled through another communications network. (Source: Rule 71A-1.002, F.A.C.)</p>
Web Application	<p>An application, hosted on a separate server and accessed via a Web Browser, vs. applications installed on a user's computer.</p>