



# FactoryTalk Network Manager Quick Start Guide

Version 1.11.00

Rockwell Automation Publication FTNM-QS001D-EN-E  
Supersedes Publication FTNM-QS001C-EN-E



## Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.



**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

---



**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

---

**IMPORTANT** Identifies information that is critical for successful application and understanding of the product.

---

Labels may also be on or inside the equipment to provide specific precautions.



**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

---



**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

---



**ARC FLASH HAZARD:** Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

---

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

	<b>Chapter 1</b>	
<b>FactoryTalk Network Manager</b>	System Requirements.....	5
	System Prerequisites .....	7
	Application notes.....	7
	<b>Chapter 2</b>	
<b>Installation</b>	Install FactoryTalk Network Manager .....	11
	<b>Chapter 3</b>	
<b>First Time Setup</b>	FTNM Application.....	13
	Switch configuration for optimal network discovery.....	14
	Network Discovery .....	17
	Purchase FactoryTalk Network Manager Node Licenses.....	18
	Configure a switch for a FactoryTalk Network Manager node license ..	18
	Upgrade an existing FactoryTalk Network Manager install.....	20
	<b>Chapter 4</b>	
<b>Supported Utilities</b>	Reset Database Password.....	23
	Reset System Admin Password.....	23
	Restore Database Backup .....	24



# FactoryTalk Network Manager

FactoryTalk® Network Manager™ software provides insight into the design, performance, and health of an industrial automation network. Use FactoryTalk Network Manager to view your network topology and manage switch-level alarms as they happen. Monitor the health of network devices and reduce downtime to improve overall automation equipment efficiency.

FactoryTalk Network Manager:

- Discovers both network and end devices including devices across a controller backplane.
- Generates an overall topology and a device-centric view of plant floor assets for increased network visibility.
- Captures alarms and events from managed switches in real time for more precise troubleshooting.
- Provides historical data and logging for analysis and resolution.
- Provides configuration backup and firmware revision management of Stratix™ managed switches for simplified deployment and maintenance.

## See also

[Installation](#) on [page 11](#)

[First Time Setup](#) on [page 13](#)

[Supported Utilities](#) on [page 23](#)

## System Requirements

### Hardware requirements

The computer running FactoryTalk Network Manager must meet or exceed these specifications:

- Quad Core 1.8 Ghz CPU
- 8 GB RAM
- 50 GB Free storage space

### Supported Switches

FactoryTalk Network Manager supports:

- Stratix 8000/8300 Modular Managed Ethernet Switches
- Stratix 5800 Industrial Managed Ethernet Switches
- Stratix 5700 Industrial Managed Ethernet Switches
- ArmorStratix 5700 Industrial Ethernet Switches
- Stratix 5410 Industrial Distribution Switches
- Stratix 5400 Industrial Ethernet Switches
- Stratix 2500 Lightly Managed Switches

FactoryTalk Network Manager supports Stratix S8000/8300, 5800, 5700, 5400, and 5410 switches running these IOS versions:

- IOS-XE 17.6
- IOS-XE 17.5
- IOS-XE 17.4
- IOS version 15.2(8)E2
- IOS version 15.2(8)E
- IOS version 15.2(7)E3
- IOS version 15.2(7)E2
- IOS version 15.2(7)E1a
- IOS version 15.2(7)E
- IOS version 15.2(6)E2A
- IOS version 15.2(6)E2
- IOS version 15.2(6)E1
- IOS version 15.2(6)E0a
- IOS version 15.2(5)E2
- IOS version 15.2(5)E1
- IOS version 15.2(5)E
- IOS version 15.2(4)EC2(ED)
- IOS version 15.2(4)EA5
- IOS version 15.2(4)EA2
- IOS version 15.2(4)EA1
- IOS version 15.2(3)E3
- IOS version 15.2(3)E2

FactoryTalk Network Manager supports Stratix S2500 switches running these SPA versions:

- SPA 1.6
- SPA 1.7.0
- SPA 1.8.0
- SPA 1.8.1
- SPA 1.8.2

## Software requirements

FactoryTalk Network Manager requires this software on the host computer:

- Operating system

64-bit versions of the Windows® and Windows Server® operating systems:

Windows 10

Windows Server 2012 R2

Windows Server 2016

---

**IMPORTANT** 32-bit versions of the Windows and Windows Server operating systems are not supported.

---

- Administrator privileges
  - The user installing FactoryTalk Network Manager must have Windows Administrator rights on the host computer.
- Web browser
  - Google® Chrome™ browser version 50.0.2661.102 or later
  - Mozilla® Firefox® version 55.0.3 or later

This software is installed if not already present:

- FactoryTalk Diagnostics version 6.11
- FactoryTalk Activation Manager version 4.04
- .NET Framework 4.6

## System Prerequisites

Verify all of these prerequisites are true in your system environment before installing FactoryTalk Network Manager:

- The user installing FactoryTalk Network Manager has Windows Administrator rights on the host computer.
- No other FTP server is running and listening on port 21.
- No other instance of PostgreSQL database is installed on the system.
- Device Manager is properly configured.
- The following ports are open for both inbound and outbound traffic on the firewall:

TCP Ports 5432, 8088, 8443, 443, 80, 21(FTP), 50000-50050

UDP Port 30162 (SNMP).

## Application notes

### Link Layer Discovery with hopcountlimit=n

Performing a Link Layer Discovery using the hopcountlimit parameter returns accurate data, but the number of hops traversed may be higher than the limit of hops entered. The exact number of hops traversed varies by network topology.

For example, when performing a Link Layer Discovery with hopcountlimit=1:

1. FactoryTalk Network Manager discovers the seed IP.

2. FactoryTalk Network Manager acquires the LLDP, CDP, MAC address, and ARP information from the seed IP.
3. FactoryTalk Network Manager reads the MAC address table from the seed IP to determine all MAC addresses from the access ports that are up. Devices on these ports are considered one hop neighbors even if they do not have a physical link or known IP address.
4. FactoryTalk Network Manager resolves the IP address of each one hop neighbor, then discovers them.
5. If all devices that are 1 hop neighbors from the seed IP are resolved and discovered, Link Layer Discovery ends. If not, another round of discovery begins.
6. FactoryTalk Network Manager acquires the LLDP, CDP, MAC address, and ARP information from discovered two hop neighbors.
7. FactoryTalk Network Manager uses the two hop neighbor information to resolve IP addresses for undiscovered devices that are one hop neighbors from the seed IP.
8. If all devices that are one hop neighbors from the seed IP are resolved and discovered, Link Layer Discovery ends. If not, another round of discovery begins. Go to step 5 using three hop neighbors.

Hop count limits for processes other than Link Layer Discovery exhibit similar behavior.

## **Discovering backplane devices and switches with Redundancy Ethernet Protocol**

When performing On Demand discovery of a network consisting of Backplane Devices and Switches that have Redundancy Ethernet Protocol (REP) enabled in them, do not select **Discover Related Devices** in the Discovery Profile. If selected, modules in the Backplane Devices are added as duplicate devices.

## **PRP channels with both interfaces down**

PRP channels with both participating interfaces down will not report any LAN-A/LAN-B devices that are part of it. FactoryTalk Network Manager will not consider PRP channels with both participating interfaces down for deriving the status of LAN-A/LAN-B devices.



## Finding the system serial number of a Plug and Play device

Supported devices on a network are detected by matching the system serial number from the Plug and Play profile with the system serial number of the device. The system serial number is not the same as the serial number on the device label.

To obtain the system serial number, either:

- Use the command-line interface to display the device information.
- Use the Unclaimed Devices list in FactoryTalk Network Manager to set up the Plug and Play profile for the devices after the initial scan completes. Select the device in the Unclaimed Plug and Play Devices table and then select **Locate Device**. The entry under Serial is the System Serial number required to complete the Plug and Play profile.

## Incorrect link information displayed in Topology View on DLR network

If FactoryTalk Network Manager is unable to resolve ports of a Device Level Ring (DLR) network member and two or more switches are connected via access ports, incorrect links between devices on those switches may appear in **Topology** view. This issue may occur because the DLR ports are blocked or the CDP and LLDP protocols are disabled.

To resolve this scenario, verify CDP and LLDP protocols are enabled on all DLR network members.

## Medium press setup does not cause a Plug and Play request

For S5700, S5400, and S2500 switches using a default configuration, a medium press setup causes a DHCP request but does not cause a Plug and Play request. This behavior is by design. After a short or medium press setup, use Device Manager to connect to the device and assign Plug and Play parameters manually.

For more information, read the *Stratix Managed Switches User Manual*, publication number 1783-UM007, available on Rockwell Automation Literature Library.



## Installation

### Install FactoryTalk Network Manager

The FactoryTalk Network Manager installation file is available for download on the Rockwell Automation Product Compatibility and Download Center (PCDC) website.

#### To install FactoryTalk Network Manager

1. Visit the PCDC website at <https://compatibility.rockwellautomation.com/Pages/home.aspx>
2. Search for FactoryTalk Network Manager.
3. Select Download to download the FactoryTalk Network Manager installation file to your system.
4. Locate and run the FactoryTalk Network Manager installation file.
5. In **Language Selection**, the system language is selected by default. If necessary, select a different language, then select **OK**.
6. In **Setup Wizard**, select **Next**.
7. In **License Agreement**, select **I Agree**.
8. In **Installation Directory**, browse to select an installation directory, then select **Next** to confirm the installation directory.
9. In **Ready to Install**, select **Next** to begin installing FactoryTalk Network Manager.
10. (optional) If the installer detects that TCP port 8443 is already in use, an error window appears. Enter an available port number, then select **OK**.
11. (optional) If the installer detects that TCP port 8088 is already in use, an error window appears. Enter an available port number, then select **OK**.
12. (optional) If the installer detects that an existing third-party postgres file is installed, an error window appears. Remove the existing postgres file, then select **OK**.
13. FactoryTalk Network Manager Services might take up to 8 minutes to initialize. If shown a progress pop-up, use it to estimate the installation progress. Wait for the initialization progress to complete.
14. When FactoryTalk Network Manager installation completes, a window appears with:
  - Username
  - Password
  - URL for the application

15. (optional) Select the checkbox to launch FactoryTalk Network Manager after installation is complete.
16. Select **Finish** to close FactoryTalk Network Manager installation. If the checkbox was selected, FactoryTalk Network Manager loads in the default browser.

### See also

[Upgrade an existing FactoryTalk Network Manager install](#) on [page 20](#)

## First Time Setup

### FTNM Application

FactoryTalk Network Manager is a server application and any client machine that can connect to the host system might connect to FactoryTalk Network Manager.

#### To connect to FactoryTalk Network Manager

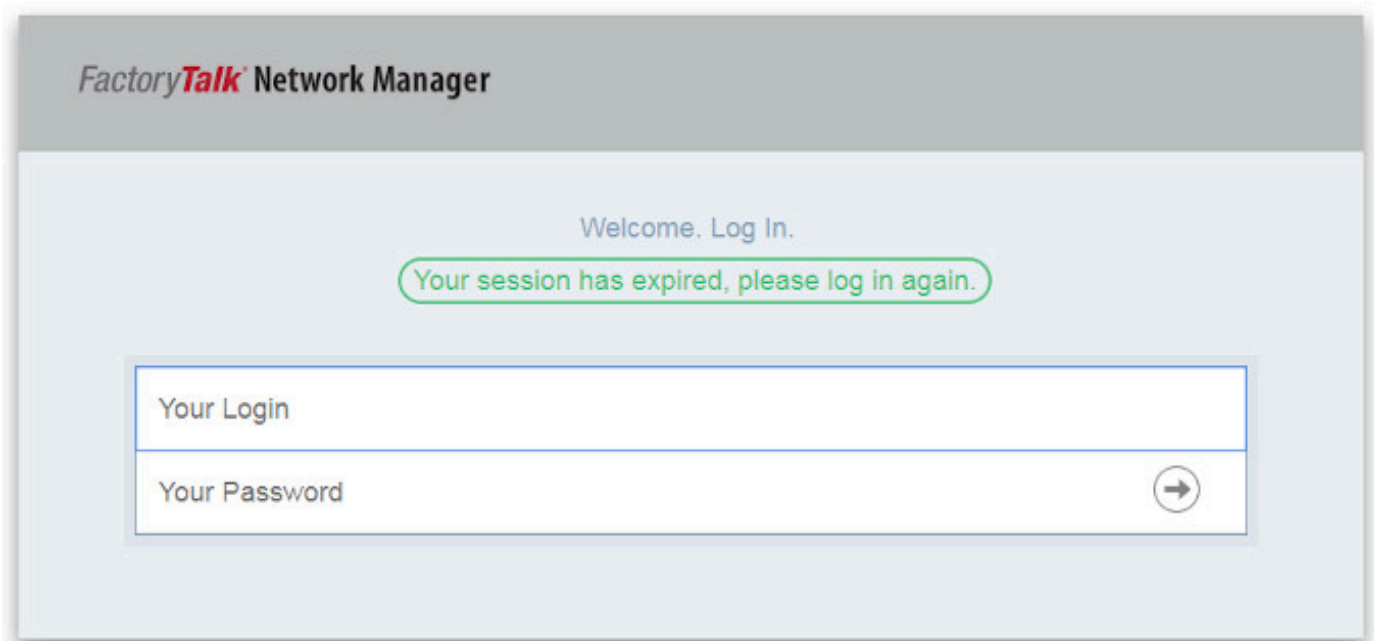
1. On the client machine, open a browser window.
2. Enter the URL **https://a.b.c.d:portNum** provided at the end of the FTNM install, where **a.b.c.d** is the IP address of the host system and **portNum** is the port number set during the install.

The default port number is 8443.

3. At the log in page, enter the Username and Password values provided at completion of the application install or upgrade.

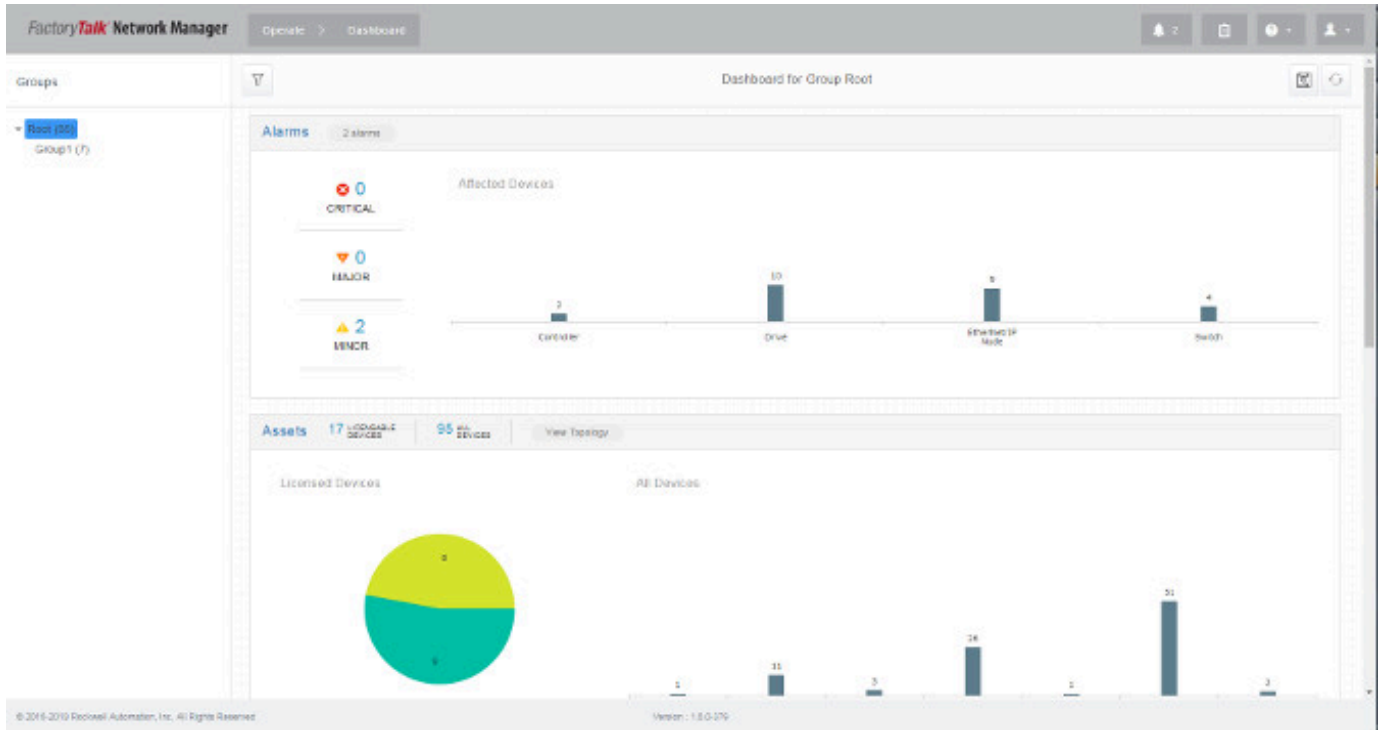
The default username and password are:

- **Username:** systemadmin
- **Password:** admin123



4. In **Your Password**, select the arrow to log in.

5. If this login is the first login for this user, a new password is required. Enter a new password, then select **OK**. Because a new password was defined, FactoryTalk Network Manager automatically logs out.
6. Reenter the login and password to enter the application.
7. When FactoryTalk Network Manager opens, the **Operate > Dashboard for Group Root** page appears.



8. Learn the features of FactoryTalk Network Manager by selecting the question mark (?) icon in the top right-hand corner of the screen, then selecting **Guided Tours**.

**See also**

[Switch configuration for optimal network discovery](#) on [page 14](#)

[Network Discovery](#) on [page 17](#)

**Switch configuration for optimal network discovery**

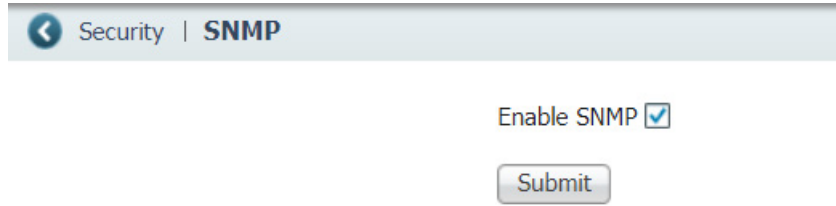
SNMP enabled switches, including Stratix managed switches, must be configured for optimal network discovery. Stratix switches can be configured for SNMP v2 or SNMP v3.



Tip: Perform express setup on a Stratix switch before making these changes.

## Configure SNMP v2c via Device Manager for Stratix 5400/5410, Stratix 5700, Stratix 8000/8300, and Armor Stratix 5700:

1. In **Device Manager**, navigate to **Configure SNMP**.
2. Select **Enable SNMP**, then select **Submit**.




Security | SNMP

Enable SNMP

Submit

3. Under **Community Strings**, select **Add**, then enter the shared community string.
4. In **RO/RW**, select Read-Only (RO), then select **OK**.



Community

RO/RW

OK Cancel



Tip: For more information on SNMP, access the [Stratix User Manual Publication 1783-UM007K](#).

## Configure SNMP v2c via CLI for Stratix 5400/5410, Stratix 5700, Stratix 8000/8300, Armor Stratix 5700, and Stratix 5800:

- To enable SNMP v2 discovery, open the command-line interface to the supported device. Type these commands, ignoring lines starting with # symbols:

```
enable
configure terminal
```

```
# Device Prerequisite Configuration for SNMPv2
snmp-server community <read-community> RO
```

```
exit
```

## Configure SNMP v3 via CLI for Stratix 5400/5410, Stratix 5700, Stratix 8000/8300, Armor Stratix 5700, and Stratix 5800:

- To enable SNMP v3 discovery, open the command-line interface to the supported device. Type these commands, ignoring lines starting with # symbols:

```
enable
configure terminal

# <mode> values are [noauth, auth, priv]:
# noauth: authenticate using only username.
# auth: authenticate using md5 or sha algorithm.
# priv: authenticate using md5 or sha algorithm and
aes 128 or des encryption.
snmp-server group <group-name> v3 <mode>

# <authentication-type> values are [sha, md5], use
only if using auth or priv snmp <mode>.
# <privacy-type> values are [aes 128, des], use only
if using priv snmp <mode>.
# <authentication-password> sets the string that
enables the agent to receive packets from the host.
# <privacy-password> sets the privacy user password.
Must not exceed 64 characters.
snmp-server user <user-name> <group-name> v3 auth
<authentication-type> <authentication-password> priv
<privacy-type> <privacy-password>

exit
```

After configuring the SNMP server, enter one of the UNLICENSED to LICENSED State configurations.

For more information on SNMP v3 configuration, see the [SNMPv3 Community MIB Support document](#) available from Cisco.

To configure remote security above and beyond user and group authentication requires implementing Access Control Lists (ACLs). For more information on implementing Access Control Lists, see the [Configuring Network Security with ACLs document](#) available from Cisco.

### Configure SNMP v2c via Device Manager for Stratix S2500 Switch

1. Log in to the **S2500 Device Manager**.
2. Leave the **Username** field blank and enter *switch* as the **Password**.
3. Select **Admin > Users**.
4. Create a **Device Access User** and use the same user in the **Access Profile** on the system.



5. Configure the **SNMP community** string for Read Only (RO):
6. Select **Configure > SNMP**. Select **OK** in the pop-up window to confirm enabling SNMP.
7. Select the checkbox to enable **SNMP Mode** globally. Select **Submit**.
8. Select the **Community Strings** tab. Add a public Community String with read-only access. (By default, this string is a RO string).
9. Select **Submit**.

### Configure SNMP v3 via Device Manager for Stratix S2500 Switch

1. Log in to the **S2500 Device Manager**.
2. Leave the **Username** field blank and enter *switch* as the **Password**.
3. Select **Admin > Users**.
4. Create a **Device Access User** and use the same user in the **Access Profile** on the system.
5. Configure the **SNMP community** string for Read Only (RO):
6. Select **Configure > SNMP**. Select **OK** in the pop-up window to confirm enabling SNMP.
7. Select the checkbox to enable **SNMP Mode** globally. Select **Submit**.
8. Select the **Community Strings** tab. Add a public Community String with read-only access. (By default, this string is a RO string).
9. Select the **Users** tab, then add an **snmpv3** user with name, security level, authentication protocol, authentication password, privacy protocol, and privacy password. Select **OK**.
10. Select the **Group** tab, select the created user, and specify the group name. Select **OK**.
11. Select **Submit**.

### See also

[Network Discovery](#) on [page 17](#)

## Network Discovery

FactoryTalk Network Manager discovers all devices on the network and presents them graphically in the **Operate > Topology** screen.

For best network discovery results, complete the switch configuration before performing network discovery.

### To perform Network Discovery

- Create a **Discovery Profile** and an **Access Profile**. Use the **Create Device Access Profile** and **Discover Assets** guided tours for step-by-step instructions.

## Purchase FactoryTalk Network Manager Node Licenses

### See also

[Switch configuration for optimal network discovery](#) on [page 14](#)

FactoryTalk Network Manager basic features are available at no charge. FactoryTalk Network Manager does not require a license to download. Some features such as Managed Switch View, switch port parameter configuration, and switch configuration backups are enabled with a node license. A node license is applied to a licensable device (also known as a node). Licenses are available as a 1 year subscription.

### To purchase FactoryTalk Network Manager Node Licenses:

1. Visit <https://portal.rockwellsoftware.com>.
2. Log in or register as a new user.
3. Locate FactoryTalk Network Manager, then select **Continue**.
4. Select a package, support level, and quantity.
5. Select **Add to Cart**.
6. From the shopping cart, select **Checkout**, then complete the checkout and billing process.
7. When you receive the **Serial Number** and **Product Key**, open **FactoryTalk Activation Manager** on the FactoryTalk Network Manager host computer.
8. Select **Get New Activations**.
9. Enter the Serial Number and Product Key, then select **Validate Activation**.
10. Enter the number of licenses to download to the host computer, then select **Download activation**.
11. Once complete, select **Find Available Activations**, then select **Refresh**.

The activation is now listed under **Available Activations**.

For troubleshooting or more assistance with FactoryTalk Activation Manager, view FactoryTalk Activation Manager Help.

### See also

[Configure a switch for a FactoryTalk Network Manager node license](#) on [page 18](#)

## Configure a switch for a FactoryTalk Network Manager node license

Switches that can be licensed (also known as nodes) must be configured to communicate with FactoryTalk Network Manager and accept a license. Configuration may occur using the command line, Device Manager, or WebUI.

Follow these steps to update the switch configuration so that FactoryTalk Network Manager can transition a switch from the UNLICENSED to LICENSED state to access additional features.

## Configure Telnet/SSH for all supported switches via Device Manager:

1. Select Admin > Access Management.
2. Check the box to enable SSH for secure communications over HTTPS or Telnet for HTTP.

## Configure Stratix 5400/5410, Stratix 5700, Stratix 8000/8300, Armor Stratix 5700, and Stratix 5800 switches for node licenses via CLI:

- Using TELNET/HTTP, to transition the supported device from UNLICENSED to LICENSED state, open the command-line interface to the supported device. Type these commands, ignoring lines starting with # symbols:

```
# Configure user account with privilege level 15
# This should match the device access username and
password specified in the system Access Profile
username <username> privilege 15 password 0 <password>
# Configure AAA
aaa new-model
aaa authentication login default local
aaa authorization exec default local
# Configure HTTP server
ip http server
ip http authentication aaa login-authentication
default
# Configure VTY
line vty 0 15
login authentication default
transport input all
transport output all
```

- Using SSH/HTTPS, to transition the supported device from UNLICENSED to LICENSED state, open the command-line interface to the supported device. Type these commands, ignoring lines starting with # symbols:

```
# Configure user account with privilege level 15
# This should match the device access username &
password specified in the system Access Profile
username <username> privilege 15 password 0 <password>

# Configure AAA
aaa new-model
aaa authentication login default local
aaa authorization exec default local
```

```
# Configure SSH server
ip ssh version 2

# Configure HTTPS server
ip http secure-server
ip http authentication aaa login-authentication
default
ip http secure-ciphersuite aes-256-cbc-sha

# Configure VTY
line vty 0 15
login authentication default
transport input all
transport output all
```

### See also

[Purchase FactoryTalk Network Manager Node Licenses](#) on [page 18](#)

The FactoryTalk Network Manager installation file is available for download on the Rockwell Automation Product Compatibility and Download Center (PCDC) website.

## Upgrade an existing FactoryTalk Network Manager install

### To upgrade an existing FactoryTalk Network Manager install

1. Visit the PCDC website at <https://compatibility.rockwellautomation.com/Pages/home.aspx>
2. Search "FactoryTalk Network Manager"
3. Select **Download** to download the FactoryTalk Network Manager installation file to your system.
4. Locate and run the FactoryTalk Network Manager installation file.
5. In **Language Selection**, the system language is selected by default. If necessary, select a different language, then select **OK**.
6. A pop-up window appears, asking you to confirm you want to upgrade your current FactoryTalk Network Manager application to a new version. Select **Yes** to upgrade or select **No** to cancel the upgrade.
7. In **Setup Wizard**, select **Next**.
8. In **License Agreement**, select **I Agree**.
9. In **Ready to Install**, select **Next** to begin installing FactoryTalk Network Manager.
10. FactoryTalk Network Manager Services might take up to 8 minutes to initialize. If shown a progress pop-up, use it to estimate the installation progress. Wait for the initialization progress to complete.

11. When FactoryTalk Network Manager installation completes, a window appears with:
  - URL for the application

---

**IMPORTANT** Be sure to record this information before you exit the screen.

---

12. (optional) Select the checkbox to launch FactoryTalk Network Manager after installation is complete.
13. Select **Finish** to close FactoryTalk Network Manager installation. If the checkbox was selected, FactoryTalk Network Manager loads in the default browser.

### See also

[Install FactoryTalk Network Manager](#) on [page 11](#)



## Supported Utilities

FTNM supports these three utilities:

- Reset Database Password
- Reset System Admin Password
- Restore Database Backup

### Reset Database Password

#### To reset the database password

1. In Windows, run the `ftnm-resetdatabasepassword.exe` utility to reset the FTNM Database password.
2. Select **Reset Database Password**. A window appears asking you to confirm that you want to reset the database password.
3. Select **Yes**, then click **Next**.
4. At the prompt, enter a new database password and confirm that entry.
5. Select **Save** to save the password.

#### See also

[Reset System Admin Password](#) on [page 23](#)

[Restore Database Backup](#) on [page 24](#)

### Reset System Admin Password

As a System Admin, you can reset the password when you are locked out of FTNM because you have either forgotten your credentials or your credentials have expired.

#### To reset the system admin password

1. In Windows, run the `ftnm-resetpassword.exe` utility to reset the FTNM System Admin password.
2. Select **Reset System Admin Password**.
3. In the password change confirmation panel, click **Next**.
4. In **Reset System Admin Password**, enter the new password in both the **Enter Password** and **Confirm Password** fields.



Tip: For guidelines on creating FactoryTalk Network Manager passwords, select the **i** icon next to the **New Password** field. A panel with password requirements displays.

5. Select **Next**.
6. Select **Save** to save the password.

## See also

[Reset Database Password](#) on [page 23](#)

[Restore Database Backup](#) on [page 24](#)

## Restore Database Backup

To restore an FTNM database from a previous FTNM backup, you must have administrative rights to the Windows location where the FTNM application is installed.

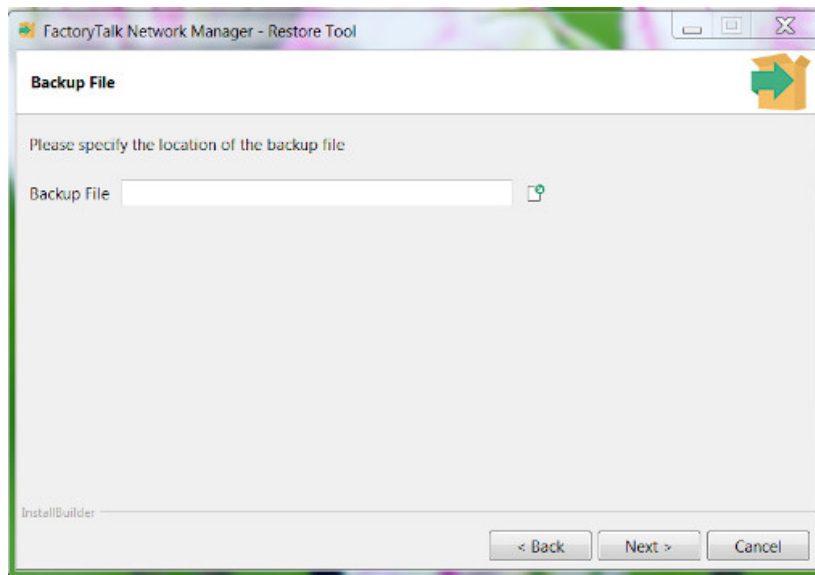
---

**IMPORTANT** Restoring from backup overwrites any data currently present in FactoryTalk Network Manager.

---

### To restore a database backup

1. In Windows, run the `ftnm-restore.exe` utility to restore an FTNM database from a previous FTNM database backup.
2. Select **Restore**.
3. Select **Yes** to confirm.
4. Enter or browse to the location of the database backup file, then select **Next**.



## See also

[Reset Database Password](#) on [page 23](#)

[Reset System Admin Password](#) on [page 23](#)



## Rockwell Automation support

Use these resources to access support information.

<b>Technical Support Center</b>	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	<a href="http://rok.auto/support">rok.auto/support</a>
<b>Knowledgebase</b>	Access Knowledgebase articles.	<a href="http://rok.auto/knowledgebase">rok.auto/knowledgebase</a>
<b>Local Technical Support Phone Numbers</b>	Locate the telephone number for your country.	<a href="http://rok.auto/phonesupport">rok.auto/phonesupport</a>
<b>Literature Library</b>	Find installation instructions, manuals, brochures, and technical data publications.	<a href="http://rok.auto/literature">rok.auto/literature</a>
<b>Product Compatibility and Download Center (PCDC)</b>	Get help determining how products interact, check features and capabilities, and find associated firmware.	<a href="http://rok.auto/pcdc">rok.auto/pcdc</a>

## Documentation feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at [rok.auto/docfeedback](http://rok.auto/docfeedback).

## Waste Electrical and Electronic Equipment (WEEE)



At the end of life, this equipment should be collected separately from any unsorted municipal waste.





Rockwell Automation maintains current product environmental information on its website at [rok.auto/pec](http://rok.auto/pec).

Allen-Bradley, expanding human possibility, Logix, Rockwell Automation, and Rockwell Software are trademarks of Rockwell Automation, Inc.

EtherNet/IP is a trademark of ODVA, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.    

**rockwellautomation.com** — expanding **human possibility**™

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846