Release Notes

Gives increased network visibility, real-time troubleshooting, simplified configuration, deployment of Stratix Managed Switches
Version 1.05.01 (released 10/2018)

Catalog Number FactoryTalk Network Manager

AB *Allen-Bradley*

These release notes describe version information for Gives increased network visibility, real-time troubleshooting, simplified configuration, deployment of Stratix Managed Switches, version 1.05.01 (released 10/2018).

Requirements

This release has the following requirements.

System requirements for FactoryTalk Network Manager 1.05.01

FactoryTalk Network Manager version 1.05.01 is supported for use in systems meeting these 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

FactoryTalk Network Manager supports these platforms:

- Stratix 8000/8300 Modular 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

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 7 Enterprise or Professional with SP2
    - Windows Server 2012 R2
    - Windows Server 2016

        Important: 32-bit versions of the Windows and Windows Server operating systems are not supported.
- Web browser
    - Google® Chrome™ browser version 50.0.2661.102 or later
    - Mozilla® Firefox® version 46.01 or later

This software is installed if not already present:

- FactoryTalk Diagnostics version 2.90
- FactoryTalk Activation Manager version 4.03
- .NET Framework 4.5.2

Pre-Configuration Requirements

Follow these steps to update the switch configuration so that FactoryTalk Network Manager can discover a supported device and transition the device from UNLICENSED to LICENSED state.

- 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-pass
word>


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.

- Using standard mode, 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 4
exec-timeout 0 0
login authentication default
transport input all
transport output all
line vty 5 15
exec-timeout 0 0
login authentication default
transport input all
transport output all
```

- Using secure mode, 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 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 4
exec-timeout 0 0
login authentication default
transport input all
transport output all
line vty 5 15
exec-timeout 0 0
login authentication default
transport input all
transport output all
```

Before installing FactoryTalk Network Manager

Confirm that:

- 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)

If the Device Manager configuration requires updating, use these steps to configure Device Manager:

1. Login to Device Manager.
2. Choose **Admin > Users**.
3. Create **Device Access User** and use the same in Access Profile on FactoryTalk Network Manager.
4. Configure **SNMP community string** for **Read Only (ro)**:
    a. Choose **Configure > SNMP**. Select **OK** to confirm enabling SNMP.
    b. Select the check box to enable SNMP Mode globally. Select **Submit**
5. Select **Community Strings** tab. Add a public Community String read only access. By default, this is a Read Only (ro) string.
6. Choose **Admin > Access Management**.
    a. Select **SSH** or **Telnet**. The enabled option determines how the switch communicates with FactoryTalk Network Manager.
    b. Select **Submit**.

Supported IOS Software

FactoryTalk Network Manager supports Stratix switches running these IOS versions:

- IOS version 15.2(6)E1
- IOS version 15.2(6)E0a
- IOS version 15.2(5)EA.fc4
- IOS version 15.2(4a)EA5
- IOS version 15.2(4)EA3
- IOS version 15.2(4)EA
- IOS version 15.2(3)EA1.fc2

Features

This release includes the following system features.

System features for FactoryTalk Network Manager 1.05.01

The FactoryTalk Network Manager version 1.05.01 release has these new and enhanced features:

- Backplane Bridging Discovery
  Supported devices are now detected when bridged to the network through a backplane, communication module, or PLC module.
  To discover bridged devices, from **Operate > Inventory**, select **Discover Bridged Devices**.

- OPC UA Device Discovery
  Devices using OPC UA and the OPC.TCP protocol can be discovered by IP address. Discovery using an OPC UA discovery server is not supported.
  Connections using no security, identity certificates, or both identity certificates and encryption are supported.

- Discovery Protocol Selection
  When configuring Access Profiles, select discovery protocols to limit or expand the protocols used.

- Device Level Ring (DLR) Support
  FactoryTalk Network Manager now supports viewing the topology of and the settings for devices using a Device Level Ring topology. Each device displays its DLR settings on its device details page. The Topology map highlights DLR groups and labels Active supervisor nodes with the DLR ring name.
  To display DLR devices, from **Operate > Topology**, select **Layer > DLR**.

- Compare Device Configurations
  When a device has more than one configuration backed up in FactoryTalk Network Manager, configurations can be compared to determine the differences between them. Select **Diff-only** to view changes in context, or **Full Configuration** to view the full contents of each configuration. Configurations now contain backup timestamps.
  To compare device configurations, select **Maintain > Configuration Archives**.

- Configuration Change Alarm
  Licensed devices now raise a **Startup Configuration changed** alarm when a "write memory" event occurs.

- CIP Attributes and Metadata
  During discovery, supported devices now send CIP attributes and metadata, such as CIP major and minor revision, device type classifications, PLC program names, and whether or not the device is behind a NAT layer.

- PxGrid
  PxGrid periodically re-registers to the PxGrid Controller to signify the service is active. If re-registration is not successful, FactoryTalk Network Manager displays an error message in **System Settings**.
  PxGrid also collects statistics, such as total counts of PxGrid assets, sync status, bulk request times and asset counts, and information on asset updates. Statistics are shown in all PxGrid screens.

- Configuration Template Push
Configuration templates can be pushed to switches in Running-Config. The default is Start-up Config.

Known Anomalies

This release has the following known anomalies.

Anomalies for FactoryTalk Network Manager 1.05.01

This list identifies the anomalies in FactoryTalk Network Manager version 1.05.01 found during testing for this release. Use the identification information provided in the brackets *[]* to track the anomaly in future releases or when obtaining assistance from Customer Support with a related issue.

Corrected anomalies

- Changing the default listening port of 8443 to any other port results in a loss of access to FactoryTalk Network Manager. First reported in FactoryTalk Network Manager 1.04.01. [Lgx00209612]
In this release, the FactoryTalk Network Manager listening port can be changed to port 443 or any available port in the range 1024 - 65535.

Known anomalies

- FactoryTalk Activation transaction records for FactoryTalk Network Manager in FactoryTalk Diagnostics do not include a user context.
When an activation is checked out or checked in by FactoryTalk Network Manager, the transaction is run using the SYSTEM account. In FactoryTalk Diagnostics the transaction record displays the Full name as blank and the User as SYSTEM. First reported in FactoryTalk Network Manager version 1.03. [49411]
There is no workaround for this anomaly.

- Additional modules in a chassis do not appear in the inventory.
When FactoryTalk Network Manager scans the network to discover a topology, this identifies only the module with the lowest order IP address on a chassis. First reported in FactoryTalk Network Manager version 1.03. [Lgx00202714]
To view the other modules on the same chassis, in Topology view, click the device to open the device details view. The IP addresses of the other modules on the chassis appear. Click the device name to view the device details.

- Laptops reported as two different device types
The Device Type reported for laptops vary depending on whether the laptop is docked or not. A docked laptop appears as an unknown device, while an undocked laptop appears as a Windows host. First reported in FactoryTalk Network Manager version 1.05.01. [Lgx00210532]
There is no workaround for this anomaly.

- PnP not supported by IOS release 15.2(6)E1
Attempting to use PnP will result in intermittent process failures. First reported in FactoryTalk Network Manager version 1.04.01. [Lgx00209441]
There is no workaround for this anomaly.

- Config templates within PnP not supported by IOS release 15.2(6)E0A or IOS Release 15.2(6) E1
When attempting to use config templates within PnP, FactoryTalk Network Manager incorrectly report the status as "Install pending". Instead, the install is complete but the configuration is not pushed to the device. First reported in FactoryTalk Network Manager version 1.05.01. [Lgx00208866]
There is no workaround for this anomaly.

- When performing a PnP medium press on a Stratix switch, FactoryTalk Network Manager does not claim or configure the switch. The switch appears in DHCP Helper but times out and loses its IP lease. First reported in FactoryTalk Network Manager version 1.04.01. [Lgx00208853]
There is no workaround for this anomaly.

- Configuring S2500 via PnP fails when **Windows Date & time > Set time automatically** is disabled
If the **Windows Date & time > Set time automatically** setting on the host machine is disabled, an S2500 device cannot be configured using PnP. First reported in FactoryTalk Network Manager version 1.05.01. [Lgx00213037]
To work around this issue, change the **Windows Date & time > Set time automatically** setting to enabled, then reconfigure the device.

- Uninstalling FactoryTalk Network Manager does not remove the FactoryTalk Network Manager shortcut from the Desktop. First reported in FactoryTalk Network Manager version 1.04.01. [Lgx00209942]
To work around this issue, manually remove the shortcut from the Desktop.

- After rebooting the host computer, FactoryTalk Network Manager may not be accessible for up to 10 minutes. First reported in FactoryTalk Network Manager version 1.04.01. [Lgx00208682]
There is no workaround for this anomaly.

- When the Inventory page is downloaded and saved as CSV using "with selected", the "Connected To" column in the CSV is empty for all devices. First reported in FactoryTalk Network Manager 1.05.01. [Lgx00212045]
There is no workaround for this anomaly.

Functional Changes

This release has the following functional changes from the previous release.

Functional changes for FactoryTalk Network Manager 1.05.01

These functional changes are present in FactoryTalk Network Manager version 1.05.01.

- Discovery and Access Profiles:
  - Discovery Profiles and Access Profiles are now consolidated in **Operate > Discovery**. Existing permissions and profiles are migrated during installation.
  - To view Discovery Profiles, from **Operate > Discovery**, select **Discovery Profiles**.
  - To view Access Profiles, from **Operate > Discovery**, select **Access Profiles**.

- Topology after Device Discovery

    - After Device Discovery has completed, the topology is updated automatically.

Application Notes

This release has the following application notes.

Application notes for FactoryTalk Network Manager 1.05.01

The application notes for the FactoryTalk Network Manager version 1.05.01 release are:

First time login

After installation, login to FactoryTalk Network Manager and configure a new system administrator password.

1. Open either the Chrome browser or Firefox web browser.
2. Enter the URL <https://a.b.c.d:portNum/login>, replacing <a.b.c.d> with the IP address of the computer where FactoryTalk Network Manager is installed and portNum with the port number specified during installation. Login using these credentials:
    - **Username: systemadmin**
    - **Password: admin123**

        Tips:
        - The default port number is 8443.
        - If logging in to a default installation of FactoryTalk Network Manager using the computer on which FactoryTalk Network Manager was installed, use the URL **https://localhost:8443/login**.

3. The **Change Password** page appears.
    a. In **Current Password** type **admin123**
    b. In **New Password** type a new password. Passwords must meet password complexity requirements:
        - 8 character minimum
        - Characters must include at least one numeral, 0-9, and one character -~!@#$%^&*()_=+'{}:;",.?/<>[]

        Important: Make sure to remember the new password. The default password no longer works.
    c. In **Confirm New Password**, type the new password again and then select the arrow or press ENTER.
4. After defining a new password, the application immediately logs out. Re-enter the login and the new password to start the application again.

Link Layer Discovery with hopcountlimit=n

Performing a Link Layer Discovery using the hopcount 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 "1 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 1 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 2 hop neighbors.
7. FactoryTalk Network Manager uses the 2 hop neighbor information to resolve IP addresses for undiscovered devices that are 1 hop neighbors from the seed IP.
8. 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. Go to step 5 using 3 hop neighbors.

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

Finding the system serial number of a PnP 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 PnP Devices table and then click Locate Device. The entry under Serial is the System Serial number required to complete the Plug and Play profile.

Unattended or silent install

Use command-line parameters to perform an unattended or silent installation of the software. The command-line syntax is:

Setup.exe /[option]="value" / [option]="value"

Command-line parameters

This table identifies the installation command-line option parameters. Command-line option parameters are case-insensitive. However, if a specified value includes a space, be sure to enclose the value in quotation marks (for example, "value with spaces").

Option Parameter	Value Description
/?	Displays the usage options for installation parameters.
/Q	Silent Install, install runs in a silent (quiet) mode without any user interface.
	This parameter is recommended if deploying the software installation using an IT tool or script, and don't expect to see any error or restart messages. When using this parameter, check the error codes, and respond as needed. For example, if the installation returns error code 1641, then the IT tool or script should restart the computer and relaunch the installation after restart.
	This parameter is required if /QS or /Record is not specified.
/QS	Unattended Install, install runs in unattended (quiet simple) mode. Install progress, error, or completion messages appear.
	When using this parameter, the installation stops and displays a prompt if there are error or restart messages. For example, if an immediate restart is required to complete the install, a restart message displays to confirm the restart. Installation resumes automatically from the point of interruption after restart.
	This parameter is required if /Q or /Record is not specified.
/IAcceptAllLicenseTerms	Acknowledges reading and acceptance of the license terms and agreement to continue the installation.
	This parameter is required for /Q or /QS parameters.
/AutoRestart	(optional) Automatically restarts the computer after the installation is complete. Used when a restart is required to complete the installation.
	If this parameter is not used silent install (/Q) will return either error code 1641 or 3010 if a restart is required, and unattended install (/QS) results in a confirmation prompt that must be agreed to before the installation is completed.
/SetupLanguage="value"	(optional) Specifies which language is displayed during install process.
	The value must be one: - ENU - CHS - DEU - ESP - FRA - ITA - JPN - KOR - PTB
	If this parameter is not used, the default language is the current user or operating system user interface language.
	Note: Not all setup languages are supported product languages.
/Record	(optional) Records the installation choices to a recording file.
/Playback	(optional) Plays back a recording file to perform the installation.
/Product="value"	Specifies which sub-products are installed.
	Only required if sub-products are included with the install package.
	If the software does not include sub-products this parameter is not available.
/ProductLanguage="value"	(optional) Specifies the language version of the software being installed.
	The value must be one:

	- ENU - DEU - ESP - FRA - JPN If this parameter is not used, the default language is the same as the setup language. If the installation media does not include multiple languages this parameter is not available.
/InstallLocation="value"	(optional) Specifies the location to install the software application. If this parameter is not used, the default install locations are: "C:\Program Files (x86)\Rockwell Software\FactoryTalk Network Manager"
/SerialNumber="value"	(optional) Specifies the serial number of the software being installed. This is used to activate the software during installation. If this parameter is not specified the software must be activated manually after installation.
/ProductKey="value"	(optional) Specifies the product key of the software being installed. This is used to activate the software during installation. If this parameter is not specified the software must be activated manually after installation.
/Version="value"	(optional) Specifies the version of the software to activate which corresponds to the product version associated with the SerialNumber and ProductKey. If this parameter is not specified the installer uses the most recent product version available when retrieving the activation.
/HttpPortNumber	(optional) Specifies the HTTP port number to be used for the PnP server. The port specified cannot be in use by another service. Values: 80, 1024 - 65535 If this parameter is not specified the installer uses the default port: 8088
/HttpsPortNumber	(optional) Specifies the HTTPS port number to be used by the web-based administrative user interface. The port specified cannot be in use by another service. Values: 443, 1024 - 65535 If this parameter is not specified the installer uses the default port: 8443

Examples

These examples show how to use the installation commands.

- To install the software with no user interface using the default settings during the installation process. (Silent install)

Setup.exe /Q /IAcceptAllLicenseTerms

- To install the software with customized parameters and display the progress, error, or complete messages during installation and restart the computer if necessary. (Unattended install)

Setup.exe /QS /IAcceptAllLicenseTerms /AutoRestart /SetupLanguage=DEU /InstallLocation="D:\Program Files\Rockwell Software\FactoryTalk Network Manager" /SerialNumber=0123456789 /ProductKey=ABCDE-FGHIJ /Version=1.05.00 /HttpPortNumber=1111 /HttpsPortNumber=2222

Error codes

This table identifies the error codes that can be returned by an installation.

Error Code	Value	Description
ERROR_SUCCESS	0	The installation completed successfully.
ERROR_INVALID_PARAMETER	87	One of the parameters was invalid.
ERROR_INSTALL_USEREXIT	1602	The installation was cancelled by the user.
ERROR_INSTALL_FAILURE	1603	A fatal error occurred during installation.
ERROR_BAD_CONFIGURATION	1610	The configuration data for this product is corrupt. Contact your support personnel.

ERROR_REBOOT_CONTINUE	1641	The computer must be restarted to continue the installation.
ERROR_SUCCESS_REBOOT_REQUIRED	3010	A restart is required to complete the installation. After restart the product is successfully installed.
ERROR_REBOOT_PENDING	3012	A restart of the computer is pending and must be completed before the installation can continue.

VeriSign Universal Root Certification Authority certificate

If the VeriSign Universal Root Certification Authority certificate does not exist on the local computer, the certificate is installed while installing Rockwell Automation software. Use Microsoft Management Console (MMC) to view the certificate in **Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.