Cyber Security with Unity Pro

Reference Manual

10/2014

EIO0000001999.00

www.schneider-electric.com

Schneider Electric

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Table of Contents

Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Book

At a Glance

Document Scope

This manual defines the cyber security elements that help you configure a system with Ethernet communication feature that is less susceptible to cyber attacks.

Validity Note

This documentation is valid for Unity Pro V8.1 or later.

The technical characteristics of the devices described in this document also appear online. To access this information online:

Step	Action
1	Go to the Schneider Electric home page *www.schneider-electric.com*.
2	In the **Search** box type the reference of a product or the name of a product range. ● Do not include blank spaces in the model number/product range. ● To get information on grouping similar modules, use asterisks (*).
3	If you entered a reference, go to the **Product Datasheets** search results and click on the reference that interests you. If you entered the name of a product range, go to the **Product Ranges** search results and click on the product range that interests you.
4	If more than one reference appears in the **Products** search results, click on the reference that interests you.
5	Depending on the size of your screen, you may need to scroll down to see the data sheet.
6	To save or print a data sheet as a .pdf file, click **Download XXX product datasheet**.

The characteristics that are presented in this manual should be the same as those characteristics that appear online. In line with our policy of constant improvement, we may revise content over time to improve clarity and accuracy. If you see a difference between the manual and online information, use the online information as your reference.

Related Documents

Title of Documentation	Reference Number
Modicon M340 for Ethernet, Communications Modules and Processors, User Manual	31007131 (English), 31007132 (French), 31007133 (German), 31007494 (Italian), 31007134 (Spanish), 31007493 (Chinese)
Modicon M580 System Planning Guide	HRB62666 (English), HRB65318 (French), HRB65319 (German), HRB65320 (Italian), HRB65321 (Spanish), HRB65322 (Chinese)
Quantum with Unity Pro, TCP/IP Configuration, User Manual	33002467 (English), 33002468 (French), 33002469 (German), 31008078 (Italian), 33002470 (Spanish), 31007110 (Chinese)
Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual	35006192 (English), 35006193 (French), 35006194 (German), 31007214 (Italian), 35006195 (Spanish), 31007102 (Chinese)

You can download these technical publications and other technical information from our website at www.schneider-electric.com.

Chapter 1
Cyber Security

Introduction

Cyber security is a branch of network administration that addresses attacks on or by computer systems and through computer networks that can result in accidental or intentional disruptions. The objective of cyber security is to help provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users.

No single cyber security approach is adequate. Schneider Electric recommends a defense-in-depth approach. Conceived by the National Security Agency (NSA), this approach layers the network with security features, appliances, and processes. The basic components of this approach are:

- risk assessment
- a security plan built on the results of the risk assessment
- a multi-phase training campaign
- physical separation of the industrial networks from enterprise networks using a demilitarized zone (DMZ) and the use of firewalls and routing to establish other security zones
- system access control
- device hardening
- network monitoring and maintenance

This chapter defines the elements that help you configure a system that is less susceptible to cyber attacks. For detailed information on the defense-in-depth approach, refer to the *TVDA: How Can I Reduce Vulnerability to Cyber Attacks in the Control Room* on the *Schneider Electric website*.

What Is in This Chapter?

This chapter contains the following topics:

What is Cyber Security?

Introduction

Cyber threats are deliberate actions or accidents that can disrupt the normal operations of computer systems and networks. These actions can be initiated from within the physical facility or from an external location. Security challenges for the control environment include:

- diverse physical and logical boundaries
- multiple sites and large geographic spans
- adverse effects of security implementation on process availability
- increased exposure to worms and viruses migrating from business systems to control systems as business-control communications become more open
- increased exposure to malicious software from USB devices, vendor and service technician laptops, and the enterprise network
- direct impact of control systems on physical and mechanical systems

Sources of Cyber Attacks

Implement a cyber security plan that accounts for various potential sources of cyber attacks and accidents, including:

Source	Description
internal	● inappropriate employee or contractor behavior ● disgruntled employee or contractor
external opportunistic (non-directed)	● script kiddies* ● recreational hackers ● virus writers
external deliberate (directed)	● criminal groups ● activists ● terrorists ● agencies of foreign states
accidental	
* slang term for hackers who use malicious scripts written by others without necessarily possessing a comprehensive understanding of how the script works or its potential impact on a system	

A deliberate cyber attack on a control system may be launched to achieve a number of malicious results, including:

- disrupt the production process by blocking or delaying the flow of information
- damage, disable, or shut down equipment to negatively impact production or the environment
- modify or disable safety systems to cause intentional harm

How Attackers Gain Access

A cyber attacker bypasses the perimeter defenses to gain access to the control system network. Common points of access include:

- dial-up access to remote terminal unit (RTU) devices
- supplier access points (such as technical support access points)
- IT-controlled network products
- corporate virtual private network (VPN)
- database links
- poorly configured firewalls
- peer utilities

Cyber Security Certifications

Schneider Electric developed cyber security guidelines based on the following recommendations:

- Achilles
- ISA Secure

Questions?

To submit a cyber security question, report security issues, or get the latest news from Schneider Electric, visit our *website*.

Schneider Electric Guidelines

Introduction

Your PC system can run a variety of applications to enhance security in your control environment. The system has factory default settings that require reconfiguration to align with Schneider Electric's device hardening recommendations of the defense-in-depth approach.

The following guidelines describe procedures in a Windows 7 operating system. They are provided as examples only. Your operating system and application may have different requirements or procedures.

Disabling Unused Network Interface Cards

Verify that network interface cards not required by the application are disabled. For example, if your system has 2 cards and the application uses only one, verify that the other network card (Local Area Connection 2) is disabled.

To disable a network card in Windows 7:

Step	Action
1	Open **Control Panel** →**Network and Internet** →**Network and Sharing Center** →**Change Adapter Settings**.
2	Right-click the unused connection. Select **Disable**.

Configuring the Local Area Connection

Various Windows network settings provide enhanced security aligned with the defense-in-depth approach that Schneider Electric recommends.

In Windows 7 systems, access these settings by opening **Control Panel** →**Network and Internet** →**Network and Sharing Center** →**Change Adapter Settings** →**Local Area Connection (x).**

This list is an example of the configuration changes you might make to your system on the **Local Area Connection Properties** screen:

- Disable all IPv6 stacks on their respective network cards. (This system example does not require the IPv6 address range and disabling the IPv6 stacks limits vulnerability to potential IPv6 security risks.
- Deselect all **Local Area Connection Properties** items except for **QoS Packet Scheduler** and **Internet Protocol Version 4**.
- Under the **Wins** tab on **Advanced TCP/IP Settings**, deselect the **Enable LMHOSTS** and **Disable NetBIOS over TCP/IP** check boxes.
- Enable **File and Print Sharing for Microsoft Network**.

Schneider Electric's defense-in-depth recommendations also include the following:

- Define only static IPv4 addresses, subnet masks, and gateways.
- Do not use DHCP or DNS in the control room.

Managing Windows Firewall

Schneider Electric's defense-in-depth approach recommendations include enabling the Windows host firewall on all system PCs. Enable the firewalls for any public or private profile listed.

Managing the Network Time Server

NOTE: The following information is applicable only if the network time server in your system is implemented on a host PC.

Each PC and system in your system receives its time updates from the firewall bounding its security zone. Configure your network time server (NTP), start the service, configure the W32time service settings, and configure the NTP server's host firewall ports, as follows:

Configuring the NTP Server	
1	In a command window, execute `gpedit.msc` to open the Group Policy tool.
2	Open **Administrative Templates** →**System** →**Windows Time Service** →**Time Providers**.
3	Double-click **Enable Windows NTP Server**.
4	On the **Enable Windows NTP Client Properties** page, select **Enabled** →**OK**.
5	On the **Time Providers** page, double-click **Configure Windows NTP Client**.
6	On the **Configure Windows NTP Client Properties page**, set the following values: ● **Configure Windows NTP Client**: enabled ● **NtpServer**: Time-b.nist.gov ● **Type**: NTP
7	Click **OK**.
Starting the Service	
1	In a command window, execute `services.msc` to open the Services tool.
2	Double-click **Windows Time**.
3	On the **Windows Time Properties** screen, change **Startup Type** to **Automatic**.
4	Click **Start** to start the service.
Configuring W32time	
1	In a command window, execute `w32tm /config /sychfromflags:manual /manualpeerlist:time-b.nist.gov /update` **NOTE:** This command configures the windows time service (w32tm) to synchronize with the time-b.nist.gov /update time.
2	In a command window, execute `sc triggerinfor w32time start/networkon stop/networkoff` **NOTE:** Rebooting the server does not automatically start the w32tm service if the system is not in a domain. The `sc triggerinfo` command configures the w32time to start on the first IP address and stop on zero IP address.

Configuring the NTP Server's Host Firewall Ports **NOTE:** NTP servers receive packets over port 123. The following steps open port 123 for inbound connections.	
1	Open **Control Panel** →**Windows Firewall** →**Advanced Settings** →**Inbound Rules**.
2	Click **New Rule**.
3	On the **Rule Type** page, select **Port**. Click **Next**.
4	On the **Protocol and Ports** page: ● Select **UDP** in the **Protocol type** field. ● Select **Specific Ports**. ● Enter **123** in the **Specific Local Ports** field. ● Click **Next**.
5	On the **Action** page, select **Allow this Connection**. Click **Next**.
6	On the **Profile** page, select **Domain**, **Public**, and **Private**. Click **Next**.
7	On the **Name** page, enter **NTP Server** in the **Name** field.
8	Return to the **Inbound Rules** page, and verify that the new rule is present with the following parameter values: ● **Name**: NTP Server ● **Profile**: All ● **Enabled**: Yes ● **Action**: Allow ● **Override**: No ● **Program**: Any ● **Local Address**: Any ● **Remote Address**: Any ● **Protocol**: UPD ● **Local Port**: 123 ● **Remote Port**: Any ● **Allowed Users**: Any ● **Allowed Computers**: Any

Disabling the Remote Desktop Protocol

Schneider Electric's defense-in-depth approach recommendations include disabling remote desktop protocol (RDP) unless your application requires the RDP. The following steps describe how to disable the protocol:

Step	Action
1	In Windows 2008R2 or Windows 7, disable RDP via **Computer** →**System Properties** → **Advanced System Settings**.
2	On the **Remote** tab, deselect the **Allow Remote Assistance Connections to this Computer** check box.
3	Select the **Don't Allow Connection to this Computer** check box.

Updating Security Policies

Update the security policies on the PCs in your system by `gpupdate` in a command window. For more information, refer to the Microsoft documentation on `gpupdate`.

Disabling LANMAN and NTLM

The Microsoft LAN Manager protocol (LANMAN or LM) and its successor NT LAN Manager (NTLM) have vulnerabilities that make their use in control applications inadvisable.

The following steps describe how to disable LM and NTLM in a Windows 7 or Windows 2008R2 system:

Step	Action
1	In a command window, execute `secpol.msc` to open the **Local Security Policy** window.
2	Open **Security Settings** →**Local Policies** →**Security Options**.
3	Select **Send NTLMv2 response only. Refuse LM & NTLM** in the **Network Security: LAN Manger authentication level** field.
4	Select the **Network Security: Do not store LAN Manager hash value on next password change** check box.
5	In a command window, enter `gpupdate` to commit the changed security policy.

Managing Updates

Before deployment, update all PC operating systems using the utilities on Microsoft's **Windows Update** Web page. To access this tool in Windows 2008R2, Windows 7, or Windows XP, select **Start** →**All Programs** →**Windows Update**.

Managing Enhanced Write Filter

Enhanced write filter (EWF) is a feature of Windows XP Embedded and Windows Embedded Standard 7 machines, which filters writes to another volume.

Step	Action
1	Before you load any software on Windows XP Embedded machines, disable the enhanced write filter (EWF) function by executing `ewfmgr c: -commitanddisable -live` in a command window and rebooting the machine.
2	After you install updates or software, enable EWF by executing `ewfmgr c: -enable` in a command window and rebooting the machine.

NOTE: Schneider Electric recommends running the *Microsoft Threat Analyzer* after each application installation and the *Microsoft Baseline Security Analyzer* (MBSA) prior to installing updates or software and after installation. Follow the security remediation suggestions offered by the MBSA, which will record a history of the security changes you make in your system. You can download this program at http://www.microsoft.com.

Managing Accounts

Introduction

Schneider Electric recommends the following regarding account management:

- Create a standard user account with no administrative privileges.
- Use the standard user account to launch applications. Use more privileged accounts to launch an application only if the application requires higher privilege levels to perform its role in the system.
- Use an administrative level account to install applications.

Managing User Account Controls (UAC) (Windows 7)

To block unauthorized attempts to make system changes, Windows 7 grants applications the permission levels of a normal user, with no administrative privileges. At this level, applications cannot make changes to the system. UAC prompts the user to grant or deny additional permissions to an application. Set UAC to its maximum level. At the maximum level, UAC prompts the user before allow an application to make any changes that require administrative permissions.

To access UAC settings in Windows 7, open **Control Panel** →**User Accounts and Family Safety** →**User Accounts** →**Change User Account Control Settings**. Or enter **UAC** in the Windows 7 **Start Menu** search field.

Managing Passwords

Introduction

Password management is one of the fundamental tools of device hardening, which is the process of configuring a device against communication-based threats. Schneider Electric recommends the following password management guidelines:

- Enable password authentication on all email and Web servers, CPUs, and Ethernet interface modules.
- Change all default passwords immediately after installation, including those for:
  - user and application accounts on Windows, SCADA, HMI, and other systems
  - scripts and source code
  - network control equipment
  - devices with user accounts
  - FTP servers
- Grant passwords only to people who require access. Prohibit password sharing.
- Do not display passwords during password entry.
  - Require passwords that are difficult to guess. They should contain at least 8 characters and should combine upper and lower case letters, digits, and special characters when permitted.
- Require users and applications to change passwords on a scheduled interval.
- Remove employee access accounts when employment has terminated.
- Require different passwords for different accounts, systems, and applications.
- Maintain a secure master list of administrator account passwords so they can be quickly accessed in the event of an emergency.
- Implement password management so that it does not interfere with the ability of an operator to respond to an event such as an emergency shutdown.
- Do not transmit passwords via email or other manner over the insecure Internet.

Managing Passwords in Unity Pro

When you create an application in Unity Pro, create a password.

- Choose a password that contains alphanumeric characters, and is case-sensitive. Unity Pro encrypts the password, and stores it in the application.
- Choose a password that contains a minimum of 8 characters.
- Choose a password that is difficult to guess.
  - The password should combine upper and lower case letters, digits, and special characters.

When you open an existing application, the **Application Password** dialog box opens. Type your password, and click **OK**.

Creating / Changing Application Passwords

To create or change your Unity Pro application password, follow these steps:

Step	Action
1	Right-click **your project name** →**Properties** in the **Project Browser**. **Result**: The **Properties of Project** dialog box opens.
2	Click the **Protection** tab.
3	In the **Application** field, click **Change password**. **Result**: The **Modify Password** dialog box opens.
4	• To enter a ***new*** password, type the password in the **Entry** field. Retype the password in the **Confirmation** field, and click **OK**. • To change an ***existing*** password, type the current password in the **Old password** field. Type the new password in the **Entry** field. Retype the new password in the **Confirmation** field, and click **OK**.
5	In the **Properties of Project** dialog box, click **Apply** to save the changes, or click **OK** to save and close.

Removing Application Passwords

To remove your Unity Pro application password, follow these steps:

Step	Action
1	Right-click **your project name** →**Properties** in the **Project Browser**. **Result**: The **Properties of Project** dialog box opens.
2	Click the **Protection** tab.
3	In the **Application** field, click **Clear password**. **Result**: The **Access Control** dialog box opens.
4	Type the password in the **Password** field, and click **OK**.
5	In the **Properties of Project** dialog box, click **Apply** to save the changes, or click **OK** to save and close.

Managing the Auto Lock Feature

Follow these steps to establish the amount of time that a password is required to activate a locked application.

Step	Action
1	Right-click **your project name** →**Properties** in the **Project Browser**. **Result**: The **Properties of Project** dialog box opens.
2	Click the **Protection** tab.
3	In the **Application** field, select the **Auto-lock** check box.
4	Click the up / down arrows to select the desired number of minutes before a password is required to unlock a locked application.
5	In the **Properties of Project** dialog box, click **Apply** to save the changes, or click **OK** to save and close.

Resetting a Forgotten Password

You have 3 attempts to enter your Unity Pro or CPU application password correctly. If you forget your password, follow these steps to reset it.

Step	Action
1	When the **Application Password** dialog box opens, press **Shift + F2**. **Result**: A grayed number (ex: 57833) appears in the dialog box.
2	Contact your local Schneider Electric customer support. Give this grayed number to the support representative.
3	Type the temporary password in the **Application Password** dialog box that customer support gives you.
4	Modify the temporary password *(see page 18)*.
5	Click **Build** →**Rebuild All Project**.
6	Click Save.

Managing the Data Storage Password

Introduction

By default, the data storage password is **datadownload**.

Unity Pro only allows you to **change** or **reset** the password.

NOTE: When importing a ZEF file, the application data storage password is set to its default value: **datadownload**.

How to Change the Data Storage Password

To change the data storage password:

Step	Action
1	Right-click **your project name** →**Properties** in the **Project Browser**. **Result**: The **Properties of Project** dialog box opens.
2	Click the **Protection** tab.
3	In the **Data Storage** area, click the **Change password ...** button.
4	Enter the old password in the **Old password** field.
5	Type the new password in the **Entry** field.
6	Confirm the new password in the **Confirmation** field.
7	Click **OK** to save the changes. **NOTE:** If you enter an incorrect old password, the message **Wrong Password!** is displayed.

How to Reset the Data Storage Password

To reset the data storage password:

Step	Action
1	Right-click **your project name** →**Properties** in the **Project Browser**. **Result**: The **Properties of Project** dialog box opens.
2	Click the **Protection** tab.
3	In the **Data Storage** area, click the **Reset password ...** button.
4	Enter the old password in the **Password** field.
5	Click **OK** to reset the password to its default value:**datadownload**. **NOTE:** If you enter an incorrect old password, the message **Wrong Password!** is displayed.

Managing Integrity Checks

Introduction

You can use an integrity check feature in Unity Pro on an authorized PC to help prevent Unity Pro files from being changed via a virus / malware through the Internet.

The integrity check feature concerns the following components:

- DLLs
- Unity Pro hardware catalog
- libset and object files of EFBs
- DTMs

Performing an Integrity Check

Unity Pro automatically performs an integrity check when you first open an application. Thereafter, the check automatically runs periodically. To perform a manual integrity check in Unity Pro, follow these steps:

Step	Action
1	Click **Help** →**About Unity Pro XXX**.
2	In the **Integrity check** field, click **Perform self-test**. **Result**: The integrity check runs in the background and does not impact your application performance. Unity Pro creates a log of the successful and unsuccessful component logins. The log file contains the IP address, the date and hour, and the result of the login. **NOTE:** If an integrity check displays an unsuccessful component login, the **Event Viewer** displays a message. Click **OK**. Manually fix the items in the log.

Managing Logging Functions

Introduction

Your cyber security system is greatly enhanced by collecting and analyzing system notifications to identify intrusion attempts or problematic routes. Examples of logging methods are *syslog* and *Windows Event Management*.

A syslog server manages the network and security event messages produced by servers and devices. You can configure all firewalls and switches in your system to log data to the syslog server.

Additionally, you can configure Windows servers and work stations to generate security messages that are not collected by the syslog server.

Many devices trigger email messages, particularly on alerts. Firewalls allow the passage of these messages. You can configure Windows servers to act as SMTP server relays to forward mail messages.

Configuring the Syslog Server

To add the server manager feature:

Step	Action
1	Select **Start** →**All Programs** →**Administrative Tools** →**Server Manager**.
2	On the **Features** page, click **Add Features**.
3	Select **Subsystem for UNIX-based Applications** →**Next**.
4	Select **Install**.

To edit the syslog file:

Step	Action
1	Select **Start** →**Korn Shell**.

2	At the **$** prompt in the **Korn Shell** window, enter the following commands:
	`cd/etc/init.d`
	`vi syslog`

3	Remove the `#` symbol from the line that contains `${SYSLOGD}`. (Use the arrow keys to position the cursor under the `#` and type `x`.)
4	To save the file and exit the vi editor, type `:wq!`
5	At the `$` prompt in the **Korn Shell** window, enter the following command to start the server: `/etc/init.d/syslog start`.

Managing Syslog Firewall Rules

The following firewall rules are an example of what values to create on the syslog server's Windows host firewall to allow incoming syslog connections:

Parameter	Value
name	syslog
profile	all
enabled	yes
action	allow
override	no
program	any
local address	any
remote address	any
protocol	UDP
local port	514
remote port	any
allowed users	any
allowed computers	any

The following parameters are an example of what values to create on the ConneXium industrial firewalls to allow syslog server connections:

	Firewall 1	Firewall 2	Firewall 3	Firewall 4
description	outgoing allow syslog	outgoing allow syslog	incoming allow syslog	outgoing allow syslog
active	yes	yes	yes	yes
src IP	$Control	$Control	$DMZ	$DMZ
src port	any	any	any	any
dst IP	$Operation network	$Operation network	$Operation network	$Operation network
dst port	514	514	514	514
protocol	UDP	UDP	UDP	UDP
action	accept	accept	accept	accept

Managing Security Services

Introduction

You can enable/disable Ethernet services using the Ethernet tabs in Unity Pro.

Schneider Electric recommends disabling services that are not being used.

NOTE: Set the Ethernet tabs parameters before you download the application to the CPU. The default settings (maximum security level) reduce the communication capacities and port access.

Ethernet Tabs in Unity Pro

Unity Pro Ethernet tabs description is provided for each of the following platform:

- Modicon M340 *(see page 34)*
- Modicon M580 *(see page 35)*
- Modicon Quantum *(see page 36)*
- Modicon Premium/Atrium *(see page 38)*

Modifying Services in Online Mode

Possible online (STOP or RUN) modifications are:

- Add or remove one line (subnet or IP address)
- Modify a parameter of a line (IP address and/or subnet and/or subnet mask)

Managing FTP and TFTP

Schneider Electric Ethernet devices use *file transfer protocol* (FTP) for various tasks including firmware loading, displaying custom Web pages, and retrieving error logs.

FTP and *trivial file transfer protocol* (TFTP) may be vulnerable to various cyber security attacks. Therefore, Schneider Electric recommends disabling FTP and TFTP they are not needed.

Managing HTTP

Hypertext transfer protocol (HTTP) is the underlying protocol used by the Web. It is used in control systems to support embedded Web servers in control products. Schneider Electric Web servers use HTTP communications to display data and send commands via webpages.

If the HTTP server is not required, disable it. Otherwise, use *hypertext transfer protocol secure* (HTTPS), which is a combination of HTTP and a cryptographic protocol, instead of HTTP if possible. Only allow traffic to specific devices, by implementing access control mechanisms such as a firewall rule that restricts access from specific devices to specific devices.

You can configure HTTPS as the default Web server on the products that support this feature.

Managing SNMP

Simple network management protocol (SNMP) provides network management services between a central management console and network devices such as routers, printers, and PACs. The protocol consists of three parts:

- Manager: an application that manages SNMP agents on a network by issuing requests, getting responses, and listening for and processing agent-issued traps
- Agent: a network-management software module that resides in a managed device. The agent allows configuration parameters to be changed by managers. Managed devices can be any type of device: routers, access servers, switches, bridges, hubs, PACs, drives.
- Network management system (NMS): the terminal through which administrators can conduct administrative tasks

Schneider Electric Ethernet devices have SNMP service capability for network management.

Often SNMP is automatically installed with **public** as the read string and **private** as the write string. This type of installation allows an attacker to perform reconnaissance on a system to create a denial of service.

To help reduce the risk of an attack via SNMP:

- When possible, deactivate SNMP v1 and v2 and use SNMP v3, which encrypts passwords and messages.
- If SNMP v1 or v2 is required, use access settings to limit the devices (IP addresses) that can access the switch. Assign different read and read/write passwords to devices.
- Change the default passwords of all devices that support SNMP.
- Block all inbound and outbound SNMP traffic at the boundary of the enterprise network and operations network of the control room.
- Filter SNMP v1 and v2 commands between the control network and operations network to specific hosts or communicate them over a separate, secured management network.
- Control access by identifying which IP address has privilege to query an SNMP device.

Managing Remote Run/Stop Access

The CPU remote run/stop access management depends on the CPU platform:

Modicon M580: CPU remote access to run/stop allows one of the following:

- Stop or run the CPU remotely via request.
- Stop the CPU remotely via request. Denies to run the CPU remotely by request.
- Denies to run or stop the CPU remotely by request.

Refer to the section on *Managing Run/Stop Input* for CPU configuration options that help prevent remote commands from accessing the Run/Stop modes *(see Modicon M580, Hardware, Reference Manual)*.

Modicon M340: CPU remote access to run/stop allows one of the following:

- Stop or run the CPU remotely via request.
- Stop the CPU remotely via request. Denies to run the CPU remotely by request, only a run controlled by the input is available when a valid input is configured.

Refer to the section on *Configuration of Modicon M340 Processors (see Unity Pro, Operating Modes)*.

Modicon Premium: CPU remote access to run/stop allows one of the following:

- Stop or run the CPU remotely via request.
- Stop the CPU remotely via request. Denies to run the CPU remotely by request, only a run controlled by the input is available when a valid input is configured.

Refer to the section on *Configuration of Premium\Atrium Processors (see Unity Pro, Operating Modes)*.

Modicon Quantum: CPU remote access to run/stop allows to:

- Stop or run the CPU remotely via request.

Managing Backup Functionality

Windows Server Backup

Schneider Electric recommends backing up up data, programs, and settings routinely so that a system can be recovered back to its state that existed prior to any disruption. Additionally, test backup/restoration processes to confirm proper functionality as a best practice.

Step	Action
1	Select **Start** →**All Programs** →**Administrative Tools** →**Server Manager**.
2	On the **Features** page, click **Add Features**.
3	Click **Windows Server Backup Features** →**Windows Server Backup** →**Next**.
4	On the **Confirm Installation Selections** page, click **Install**.

Chapter 2
Cyber Security Services Availability by CPU

Cyber Security Services Availability by CPU

Overview

Each system provides various levels of services regarding cyber security. The minimum firmware level and available cyber security services are provided for the CPUs and Ethernet modules on the following platforms:

- Modicon M340 *(see page 29)* and Modicon X80 *(see page 30)* modules
- Modicon M580 *(see page 30)*
- Modicon Momentum *(see page 30)* (cyber security services are not implemented)
- Modicon Quantum *(see page 31)*
- Modicon Premium/Atrium *(see page 32)*

Cyber Security Services in Modicon M340 CPU

Minimum firmware version and cyber security services availability in Modicon M340 CPU:

CPU		Cyber security services			
Reference	**Minimum firmware version**	**Password**	**FTP check**	**HTTP check**	**Access control**
BMX P34 1000	2.60	X	–	–	–
BMX P34 2000	2.60	X	–	–	–
BMX P34 2010	2.60	X	–	–	–
BMX P34 20102	2.60	X	–	–	–
BMX P34 2020	2.60	X	X	X	X
BMX P34 2030	2.60	X	X	X	X
BMX P34 20302	2.60	X	X	X	X
X Available **–** Not available					

Cyber Security Services in Modicon X80 Modules

Modicon X80 modules supporting cyber security services:

Module		Cyber security services			
Reference	**Minimum firmware version**	**Password**	**FTP check**	**HTTP check**	**Access control**
BMX NOC 0401.2	–	–	X	X	X
BMX NOE 0100.2	–	–	X	X	X
BMX NOE 0110.2	–	–	X	X	X
BMX PRA 1000	2.60	X	X	X	X
X Available **–** Not available					

Cyber Security Services in Modicon M580 CPU:

Minimum firmware version and cyber security services availability in Modicon M580 CPU:

CPU		Cyber security services			
Reference	**Minimum firmware version**	**Password**	**FTP check**	**HTTP check**	**Access control**
BME P58 1020	1.00	X	X	X	X
BME P58 2020	1.00	X	X	X	X
BME P58 2040	1.00	X	X	X	X
BME P58 3020	1.00	X	X	X	X
BME P58 3040	1.00	X	X	X	X
BME P58 4020	1.00	X	X	X	X
BME P58 4040	1.00	X	X	X	X
X Available **–** Not available					

Cyber Security Services in Modicon Momentum CPU:

Cyber security services are not implemented in Modicon Momentum CPUs.

Cyber Security Services in Modicon Quantum CPU and Modules

Minimum firmware version and cyber security services availability in Modicon Quantum CPU:

CPU		Cyber security services			
Reference	**Minimum firmware version**	**Password**	**FTP check**	**HTTP check**	**Access control**
140 CPU 311 10	3.20	X	–	–	–
140 CPU 434 12•	3.20	X	–	–	–
140 CPU 534 14•	3.20	X	–	–	–
140 CPU 651 •0	3.20	X	X	X	X
140 CPU 652 60	3.20	X	X	X	X
140 CPU 658 60	3.20	X	X	X	X
140 CPU 670 60	3.20	X	X	X	X
140 CPU 671 60	3.20	X	X	X	X
140 CPU 672 6•	3.20	X	X	X	X
140 CPU 678 61	3.20	X	X	X	X
X Available **–** Not available					

Modicon Quantum modules supporting cyber security services:

Module		Cyber security services			
Reference	**Minimum firmware version**	**Password**	**FTP check**	**HTTP check**	**Access control**
140 NOC 771 0•	1.00	–	X (1)	X (1)	X
140 NOC 780 00	2.00	–	X (2)	X (2)	X (2)
140 NOC 781 00	2.00	–	X (2)	X (2)	X (2)
140 NOE 771 ••	X (3)	–	X (3)	X (3)	–
140 NWM 100 00	–	–	X	X	–
X Available **–** Not available **(1)** FTP and HTTP services are always enabled. **(2)** FTP, HTTP, and access control services are always enabled on lower firmware versions. **(3)** Services availability varies with firmware version and they are accessed through the configuration tabs *(see page 36)*.					

Cyber Security Services in Modicon Premium/Atrium CPU and Modules

Minimum firmware version and cyber security services availability in Modicon Premium/Atrium CPU:

CPU		Cyber security services			
Reference	**Minimum firmware version**	**Password**	**FTP check**	**HTTP check**	**Access control**
TSX H57 •4M	3.10	X	–	–	–
TSX P57 0244M	3.10	X	–	–	–
TSX P57 •04M	3.10	X	–	–	–
TSX P57 •54M	3.10	X	–	–	–
TSX P57 1634M TSX P57 2634M TSX P57 3634M (through ETY port)	3.10	X	X	X	X
TSX P57 4634M TSX P57 5634M TSX P57 6634M (embedded Ethernet port)	3.10	X	X	X	X
TSX PCI ••4M	3.10	–	–	–	–
X Available **–** Not available					

Modicon Premium/Atrium modules supporting cyber security services:

Module		Cyber security services			
Reference	**Minimum firmware version**	**Password**	**FTP check**	**HTTP check**	**Access control**
TSX ETC 101.2	–	–	X	X	X
TSX ETY 110	–	–	X	X	X
TSX ETY •103	–	–	X	X	X
X Available **–** Not available					

Chapter 3
Security Services Description

What Is in This Chapter?

This chapter contains the following topics:

Modicon M340 Security Services

Overview

Security services settings description is provided for the Modicon M340 CPU and Modicon X80 Ethernet modules in different manuals as described in the following topics.

Modicon M340 CPU with Embedded Ethernet Ports

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

Access control: Refer to section on *Messaging Configuration Parameters (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

BMX NOC 0401.2 Module

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

Access control: Refer to section on *Configuring Access Control (see Modicon M340, BMX NOC 0401 Ethernet Communication Module, User Manual)*.

BMX NOE 0100.2 and BMX NOE 0110.2 Module

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

Access control: Refer to section on *Messaging Configuration Parameters (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

BMX PRA 1000 Module

The BMX PRA 1000 is configured as a Modicon M340 CPU. Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

Access control: Refer to section on *Messaging Configuration Parameters (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

Modicon M580 Security Services

Modicon M580 CPU

Description of cyber security related parameters is provided in the section on *Managing Security Services (see Modicon M580, System Planning Guide)*.

Modicon Quantum Security Services

Overview

Security services settings description is provided for the Modicon Quantum CPU and Ethernet modules in different manuals as described in the following topics.

Modicon Quantum CPU with Embedded Ethernet Ports

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (Enable / Disable HTTP, FTP, and TFTP) (see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*.

Access control: Refer to section on *Modicon Quantum with Unity Ethernet Controller Messaging Configuration (see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*.

140 NOC 771 0x Module

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (Enable / Disable HTTP, FTP, and TFTP) (see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*.

Access control: Refer to section on *Configuring Access Control (see Quantum, 140 NOC 771 01 Ethernet Communication Module, User Manual)*.

140 NOC 780 00 Module

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (see Quantum EIO, Control Network, Installation and Configuration Guide)*.

Access control: Refer to section on *Configuring Access Control (see Quantum EIO, Control Network, Installation and Configuration Guide)*.

140 NOC 781 00 Module

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (see Quantum EIO, Control Network, Installation and Configuration Guide)*.

Access control: Refer to section on *Configuring Access Control (see Quantum EIO, Control Network, Installation and Configuration Guide)*.

140 NOE 771 xx Module

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (Enable / Disable HTTP, FTP, and TFTP) (see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*, the section on *Security (see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*, and the section on *Establishing HTTP and Write Passwords (see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*.

140 NWM 100 00 Module

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (Enable / Disable HTTP, FTP, and TFTP) (see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*.

Modicon Premium/Atrium Security Services

Overview

Security services settings description is provided for the Modicon Premium/Atrium CPU and Ethernet modules in different manuals as described in the following topics.

Modicon Premium/Atrium CPU with Embedded Ethernet Ports

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security Service Configuration Parameters (see Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual)*.

Access control: Refer to section on *Configuration of TCP/IP Messaging (TSX P57 6634/5634/4634) (see Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual)*.

Modicon Premium/Atrium CPU through ETY Ports

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security Service Configuration Parameters (see Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual)*.

Access control: Refer to section on *Configuration of TCP/IP Messaging (see Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual)*.

TSX ETC 101.2 Module

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security (see Premium, TSX ETC 101 Ethernet Communication Module, User Manual)*.

Access control: Refer to section on *Configuring Access Control (see Premium, TSX ETC 101 Ethernet Communication Module, User Manual)*.

TSX ETY 110 Module

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security Service Configuration Parameters (see Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual)*.

Access control: Refer to section on *Configuration of Messaging on the TCP/IP Profile or the ETHWAY Profile (see Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual)*.

TSX ETY x103 Module

Description of cyber security related parameters is provided in the listed topics:

Security (FTP, TFTP, HTTP): Refer to section on *Security Service Configuration Parameters (see Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual)*.

Access control: Refer to section on *Configuration of TCP/IP Messaging (see Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual)*.

Glossary

C

CPU

(*central processing unit*) The CPU, also known as the processor or controller, is the brain of an industrial manufacturing process. It automates a process as opposed to relay control systems. CPUs are computers suited to survive the harsh conditions of the industrial environment.

F

FTP

(*file transfer protocol*) A protocol that copies a file from one host to another over a TCP/IP-based network, such as the internet. FTP uses a client-server architecture as well as separate control and data connections between the client and server.

H

HMI

(*human machine interface*) System that allows interaction between a human and a machine.

Index

P

Q

R

S