

DataMan[®] Security Guidelines

2026 July 30

Revision: 26.2.0.19

Legal Notices

The software described in this documentation is provided "as is" and "as available," without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose, and non-infringement. In no event shall Cognex Corporation and its global affiliates (collectively, "Cognex") be liable for any claims, damages, or other liability arising from, out of, or in connection with the software or your use of the software.

Your use of this software is governed by the full terms and conditions of the Cognex Software License Agreement. For complete licensing details and legal terms, please visit <https://www.cognex.com/terms-and-conditions>.

The information in this document is subject to change without notice and should not be construed as a commitment by Cognex. Cognex is not responsible for any errors that may be present in either this document or the associated software.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, nor transferred to any other media or language without the written permission of Cognex Corporation.

Portions of the hardware and software provided by Cognex may be covered by one or more U.S. and foreign patents, as well as pending U.S. and foreign patents listed on the Cognex web site at: cognex.com/patents.

In the event of any inconsistency between the English language version of this documentation and any other language version, the English language version shall take precedence.

Copyright © 2026. Cognex Corporation. All Rights Reserved.

The following are registered U.S. trademarks of Cognex Corporation:

2DMAX, 3D LIGHTBURST TECHNOLOGY, ADVANTAGE, ALIGNPLUS, ASSEMBLYPLUS, COGNEX, COGNEX VISION FOR INDUSTRY, CVL, DATAMAN, DVT, EASYBUILDER, EDGE INTELLIGENCE, HOTBARS, IDMAX, IN-SIGHT, LIGHTBURST, MX, OMNIVIEW, PATFIND, PATFLEX, PATINSPECT, PATMAX, PATMAX REDLINE, PATQUICK, POWERGRID, QUICKSORT, ULTRALIGHT, VISION SOLUTIONS, VISIONPRO, VISIONVIEW

The following are trademarks of the Cognex Corporation:

1DMAX, 3D SYMBOLIC LIGHT, 3D-LOCATE, 3DMAX, ONEVISION, PINPOINT, RANGEMAX, SLX, VIDI, OCRMAX, INSPECTEDGE, VISION SOLUTIONS

Portions copyright © Microsoft Corporation. All rights reserved.

Portions copyright © MadCap Software, Inc. All rights reserved.

Other product and company trademarks identified herein are the trademarks of their respective owners.

Symbols

The following symbols indicate safety precautions and supplemental information:

 **WARNING:** This symbol indicates a hazard that could cause death, serious personal injury or electrical shock.

 **CAUTION:** This symbol indicates a hazard that could result in property damage.

 **Note:** This symbol indicates additional information about a subject.

 **Tip:** This symbol indicates suggestions and shortcuts that might not otherwise be apparent.

Table of Contents

Legal Notices	2
Symbols	3
Table of Contents	4
About this Manual	5
Introduction	5
Earlier Releases	5
Disclaimer	5
Configuration Control APIs	6
Security Hardening	7
List of Open Ports	7
Services & Ports	9
Password Recovery	11
Password Recovery for a Security Hardened Device	11
Password Recovery for DataMan 80-PoE	11
Device Onboarding	12
Encrypted Communications with an X.509 Certificate	12
Generate the Certificate	12
Upload the Certificate	12
Validate the Certificate	14
Renew the Certificate	14
Password Protection	14
Turning on Password Protection	15
Locking the User Interface	15
Forgotten Password	16
Removing the Password	16
Recommendations	17

About this Manual

The *DataMan® Security Guidelines* provides information on security practices for using your DataMan reader.

Introduction

The 26.2.0 DataMan product release introduces improvements to certificate handling.

The **Secure Connection** settings option is replaced with the **Certificates** menu. The **Certificates** menu allows you to manage your TLS and trusted certificates and assign them to various protocols.

Earlier Releases

The 26.1.0 DataMan product release introduces security features aligned with emerging industry standards.

This release focuses on improving device security while preserving existing workflows. The design introduces modern security controls while maintaining compatibility with earlier releases. The goal is to preserve the existing out-of-the-box experience. New security features are optional and disabled by default.

Full security protection requires a controlled network and restricted physical access.

Disclaimer

This document is valid for the following Cognex products:

- DataMan 80
- DataMan 280
- DataMan 290
- DataMan 390

This release supports a transition toward improved security practices. This document does not claim regulatory compliance.

Many commonly used industrial protocols, such as PROFINET or Ethernet/IP, transmit data without encryption. To prevent data interception, deploy the reader in a controlled network that restricts unauthorized access.

All procedures in this document need to be executed in the DataMan WebUI, unless otherwise noted.

Configuration Control APIs

To preserve the existing out-of-the-box experience, legacy APIs that do not have user control retain their original access behavior.

The following features prioritize usability and require a controlled network with restricted access for secure operation:

- DataMan Setup Tool: Windows-based graphical client for reader configuration
- DMCC: programmatic API
- Scripting: user-developed code to customize reader behavior

Use the **Services & Ports** setting to disable these features if the reader is deployed in an insecure network.

Security Hardening

Secure operation of the product requires a controlled network and restricted physical access.

To mitigate security risks, the reader provides a set of APIs that you can disable. Less complex network behavior also results in easier IT onboarding of the reader.

Cognex recommends disabling any feature that you do not use. This reduces the attack surface and simplifies system management, while optimizing reader resources.

Consider disabling the following:

- Unused IP ports not required for communication
- Unused Cognex-specific configuration and communication channels

List of Open Ports

The following table lists ports that may be active under specific configurations. Not all ports pose security risks.

Some features lack built-in security and require protected physical and network environments. Those are typically enabled and disabled through configuration:

- *DataMan configuration* refers to configuration options available through the DataMan Setup Tool or using DMCCs.
- *Services & Ports* refers to the settings available in the **Services & Ports** setting menu of the WebUI.

Name	Port	How to Disable	Description
FTP	21	DataMan configuration	Client functionality
SFTP	22	DataMan configuration	Client functionality
DataMan Control Commands (DMCC)	23	Services & Ports to fully disable DataMan configuration to turn off broadcasting	DataMan command API
WebHMI	80	DataMan configuration	Device-internal legacy web server For more information, see <i>WebHMI Reference Manual</i>
WebUI	80 (HTTP)	Cannot be disabled	Device-internal main web server
	443 (HTTPS)	Disabling not recommended	
NTP	123	DataMan configuration	Network Time Protocol RFC 5905
PROFINET-SNMP	161/162	DataMan configuration	SNMP functionality steered through PROFINET
Precision Time Protocol (PTP)	319/320	DataMan configuration	IEEE 1588 Precision Time Protocol (PTP)
Modbus TCP	502	DataMan configuration	Industrial protocol

Name	Port	How to Disable	Description
Device discovery	1069	Cannot be disabled	Cognex device discovery protocol
Device network troubleshooting	1069	Services & Ports	Cognex tool for recovering network misconfiguration on devices
mDNS	5353	DataMan configuration	RFC 6762 Multicast DNS
EI Agent	31871	Services & Ports	RFC 7235 MQTT
SLMP	32704-32768	DataMan configuration	Industrial protocol
PROFINET	34964	DataMan configuration	Industrial protocol
DataMan Setup Tool	44444	Services & Ports	Windows-based graphical client for reader configuration
Ethernet/IP	44818	DataMan configuration	Industrial protocol
	2222		
iQ Sensor Solution	45237	DataMan configuration	Industrial protocol
Multi-Reader Sync (MRS)	51069	DataMan configuration	Cognex device synchronization protocol
CC-Link	61450/61451	DataMan configuration	Industrial protocol
Network Client	Ephemeral	DataMan configuration	DMCC-based peer-to-peer communication protocol. For more information, see the <i>Communications</i> section of the <i>WebUI Manual</i> .
TCP image transfer	Dynamic	DataMan configuration	On-demand image transfer. For more information, see the <i>Transferring Images over TCP</i> section of the <i>DataMan® Communications and Programming Guide</i> .

Services & Ports

In the **Services & Ports** tab of **Settings**, you can enable or disable major APIs and interfaces of the reader. Disabling unused interfaces does not affect normal reader operation. The list of configurable interfaces depends on your reader model and configuration.

Note: Disabling most services might leave physical access as the only method to access the reader. Follow the factory reset procedure to access a hardened device with a lost password.

Service Name ↑	Enabled	Configurable Ports
DMCC	☒	
Enterprise Connectivity	☒	
IP Address Recovery	☐	
RP Codes	☒	
Scripting	☐	
Serial	☒	
Serial Over USB	☒	
SetupTool	☒	

Ready

[REVERT](#) [APPLY SETTINGS](#)

You can enable or disable the following functions:

Name	Action	Available in Emergency Boot Mode	Notes	Additional Documentation
DMCC	Enables DataMan Control Commands (DMCCs) for configuring and controlling your reader from a COM port.	No	DMCCs have non-compliant authorization control.	<i>Command Reference</i>
Enterprise Connectivity	Enables communication using the MQTT protocol.	No	N/A	N/A

Name	Action	Available in Emergency Boot Mode	Notes	Additional Documentation
IP Address Recovery	Enables you to change the IP address of the reader outside of the WebUI. For example, from the Repair and Support page of DataMan Setup Tool, or through Station Manager.	No	Uses port 1069.	<i>Troubleshooting a Network Connection</i> section of the <i>DataMan Communications and Programming Guide</i>
RP Codes	Enables the use of Reader Programming Codes, which are special Data Matrix codes to configure your reader without the DataMan Setup Tool or the WebUI.	Yes	N/A	<i>DataMan Configuration Codes</i>
Scripting	Enables the execution of custom scripts uploaded to the reader.	Yes	Scripting is not available on the WebUI.	<i>Scripting</i> section of the <i>DataMan Communications and Programming Guide</i>
Serial	Enables serial communication.	Yes	Requires access to the physical lines on the M12 connector.	N/A
Serial Over USB	Enables serial communication through USB with a virtual COM port.	Yes	Requires a USB cable connected to the reader.	<i>Emulating Serial Functionality</i> in the <i>Reference Manual</i> of your reader
SetupTool	Enables communication with the reader through the DataMan Setup Tool.	No	DataMan Setup Tool has non-compliant authorization control.	<i>Setup Tool Reference Manual</i>
HTTP	Enables access to the WebUI over an unsecured HTTP connection.	No	N/A	N/A
HTTPS	Enables access to the WebUI over an encrypted HTTPS connection.	No	N/A	N/A

Password Recovery

To recover a lost password, you must reset the reader to factory defaults.

Using DMCC:

1. Connect to the reader on port 23 with a Telnet client.
2. Issue the `CONFIG.DEFAULT` command.

Using DataMan Setup Tool:

1. Launch DataMan Setup Tool and connect to the reader.
2. Navigate to the **System > Reset Configuration** menu.
3. Select the **Reset Device to Factory Defaults** option.

Password Recovery for a Security Hardened Device

If reader access through DMCC and DataMan Setup Tool are disabled, the procedure to reset the password requires physical access to the reader:

1. Power on the reader while holding the TRIG/ACT button.
This activates emergency boot mode that temporarily enables some controls until the next reboot.
2. Connect to the reader through serial-over-USB or real serial connection.
3. Issue the `CONFIG.DEFAULT DMCC` command to reset the reader to factory defaults.

For more information, see the *I still cannot connect to my reader: Can I reset it?* section of the *DataMan Setup Tool Q-and-A* document.

Password Recovery for DataMan 80-PoE

You can only reset a DataMan 80-PoE reader to factory defaults by using a reader programming code:

1. Power on the reader while holding the ACT button.
This activates emergency boot mode that temporarily enables some controls until the next reboot.
2. Scan the Reset programming code.

For more information, see the *Reset* section of the *DataMan® Configuration Codes* document.

Device Onboarding

Previous releases did not enforce a secure onboarding procedure. This is sufficient when the reader is in a controlled network and restricted environment. Since Cognex prioritizes stable user experience, the out-of-the-box experience of this release remains the same.

Future regulations may require stricter security measures. Complete the following procedure to prevent unauthorized tampering while complying with state-of-the-art security norms.

To onboard the reader using the WebUI:

1. Use an encrypted communication channel towards the reader to prevent sniffing password operations.
2. Set a secure password.
3. Conduct security hardening:
 - a. Assess the protection needed for the reader in the given environment.
 - b. Disable all reader interfaces that you deem insecure.

Encrypted Communications with an X.509 Certificate

This procedure installs a cryptographically signed certificate that allows the reader to validate its own hostname and set up an encrypted communication channel.

Note: The reader only supports user-generated certificates.

Execute the following steps during a peer-to-peer connection between the host computer and the reader to prevent sniffing attacks:

1. Generate a certificate using an open-source tool, such as OpenSSL.
2. Upload the certificate through the WebUI.
3. Add the certificate to the browser trust store.
4. Renew the certificate when required.

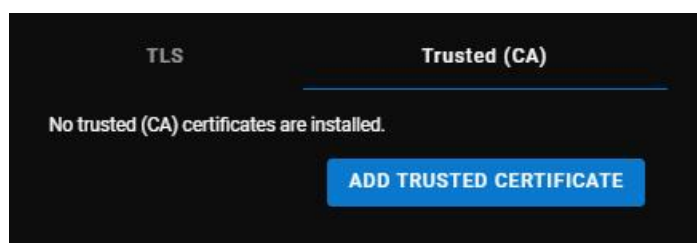
Generate the Certificate

Generate the information that needs to be signed using an open-source tool, such as OpenSSL. This information uniquely identifies the reader. It must contain a unique network qualifier, usually the hostname. The default hostname of Cognex readers is derived from the MAC address.

The hostname is also user configurable. If you change the hostname, you must regenerate the X.509 certificate of the reader.

Upload the Certificate

In the **Certificates** tab of **Settings**, you can install certificates on your reader for secure communication.



You can install the following types of certificates:

- **TLS:** allows other devices to trust your DataMan reader:
 - WebUI (HTTPS)
 - Enterprise Connectivity (MQTT with mTLS)
- **Trusted (Certificate Authority):** The self-signed certificate of the Certificate Authority (CA). It allows your DataMan reader to trust a server configured with a certificate signed by the same Certificate Authority:
 - Enterprise Connectivity (MQTT with TLS)

Note: The reader ships with the pre-installed TLS certificate file *default-tls.crt*. However, Cognex recommends installing your own certificate.

Prerequisites

Before installing any certificates, make sure that your reader and environment fulfill the following requirements:

- An NTP server is configured. Invalid time can cause issues when using or validating certificates.
- When using MQTT with TLS, you must have a local Certificate Authority set up for handling signing requests.

Install a TLS Certificate

You can install a TLS certificate in the following ways:

- The **New Signing Request** option allows you to create a private encryption key on your reader, and generate an accompanying signing request. Once that signing request is signed by a Certificate Authority to produce the certificate file, you can install the signed certificate file. This is the more secure option.
- The **Add Key Pair** option allows you to install an externally generated private key and signed certificate in one step. This option is less secure, but can be more convenient in certain environments.

New Signing Request

To install a TLS certificate with your own private encryption key:

1. Go to the **TLS** tab of the **Certificates** menu and click **New Signing Request** to create a new TLS certificate signing request.

The pop-up dialog automatically populates the required fields.

2. Optionally, enter the following additional signing request details:

- Country Code
- State
- Locality
- Company
- Organizational Unit

3. Click **Generate Signing Request** to create the signing request.

A new certificate appears on the TLS tab of the dialog with **Pending Signing Request** status, and a *.csr* file is saved to your **Downloads** directory.

4. Generate a signed key for the signing request with your local Certificate Authority, and save the *.crt* file to an accessible location.
5. Click the menu icon for the certificate on the **TLS** tab, and select **Complete Signing Request**.
6. Click the **Select Certificate File** field to open the file browser, and select the *.crt* file with the signed key.

Add Key Pair

To install an externally generated private encryption key and signed certificate:

1. Go to the **TLS** tab of the **Certificates** menu and click **Add Key Pair**.
2. In the pop-up dialog that opens, click the **Select Certificate File** field to open the file browser, and select the *.der* file for the certificate you want to use.
3. Click the **Select Private Key File** field to open the file browser, and select the *.der* file you want to use as the private key.
4. In the **Password** field, enter the password for the private key file.
5. Click **Add Certificate + Key** to submit your certificate.

Assign TLS Certificate to HTTPS Connection

To assign a signed certificate to enable secure communication:

1. Click the menu icon for the certificate on the **TLS** tab and click **Assign Protocols**.
2. Enable the **HTTPS** toggle
3. Click **Assigned Protocols**.

 **Note:** You can only use one certificate for HTTPS connection at a given time.

Install a Trusted Certificate

To add a trusted certificate for your Certificate Authority:

1. Go to the **Trusted (CA)** tab of the **Certificates** menu.
2. Click **Add Trusted Certificate**.
3. In the pop-up that opens, click the **Select Certificate File** field to open the file browser, and select the *.crt* file for the certificate you want to add.

Validate the Certificate

Include the certificate in the list of valid certificates that your browser accepts. For example, you can do this through the browser, the computer, or corporate Active Directory settings.

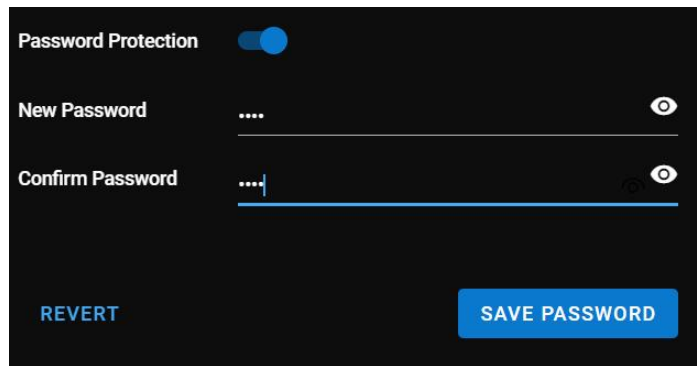
Renew the Certificate

Certificates have an expiration date. While typical certificate validity can span several years, Cognex recommends renewing certificates regularly.

Renewing the certificate means that you regenerate and reinstall the certificate on the reader.

Password Protection

In the **Password Protection** tab of **Settings**, you can set up a password for the reader. When you enable password protection and lock the WebUI, users cannot modify the reader configuration without a password. Use this feature to protect your settings from unwanted changes.

A dark-themed settings screen for password protection. At the top, 'Password Protection' is a toggle switch that is turned on (blue). Below it are two password input fields: 'New Password' and 'Confirm Password', both showing masked characters (dots). Each field has a small eye icon to its right for toggling visibility. At the bottom, there are two buttons: 'REVERT' on the left and 'SAVE PASSWORD' on the right.

Turning on Password Protection

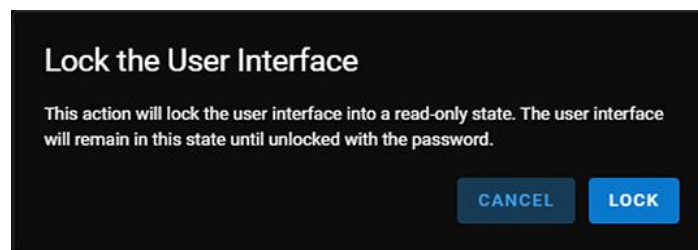
To turn on password protection:

1. Enable the **Password Protection** toggle.
2. Enter the new password in the **New Password** and **Confirm Password** fields.
3. Click **Save Password**.

Locking the User Interface

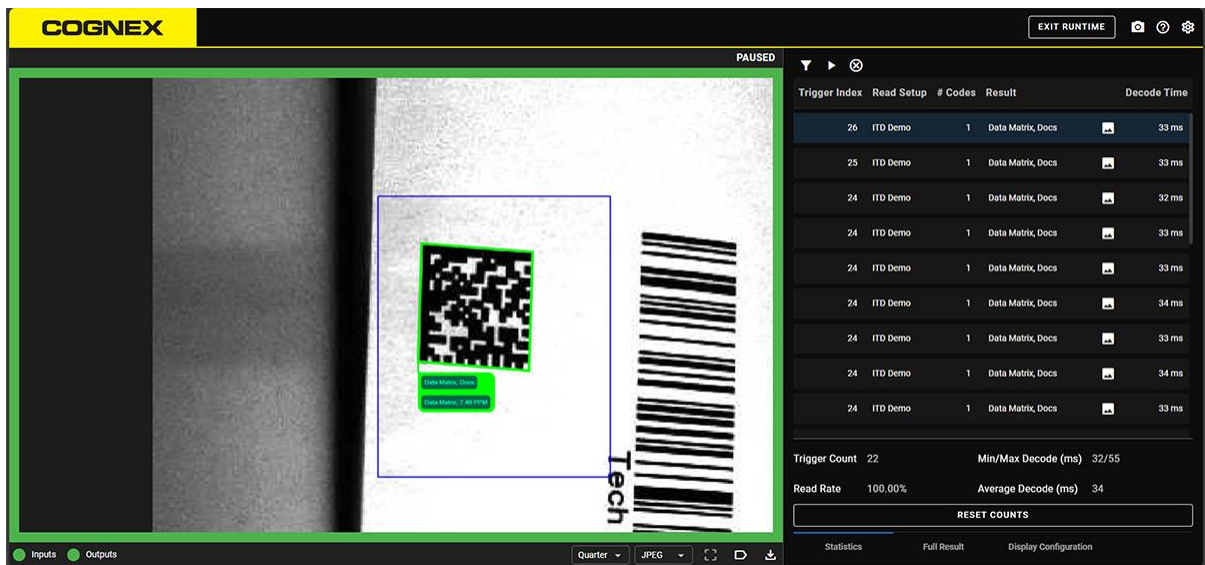
To lock the user interface:

1. Turn on password protection.
2. Click on the lock icon at the top right of the screen. The **Lock the User Interface** dialog appears.

A dark-themed dialog box titled 'Lock the User Interface'. The text inside reads: 'This action will lock the user interface into a read-only state. The user interface will remain in this state until unlocked with the password.' At the bottom right, there are two buttons: 'CANCEL' and 'LOCK'.

- Click **Lock**.

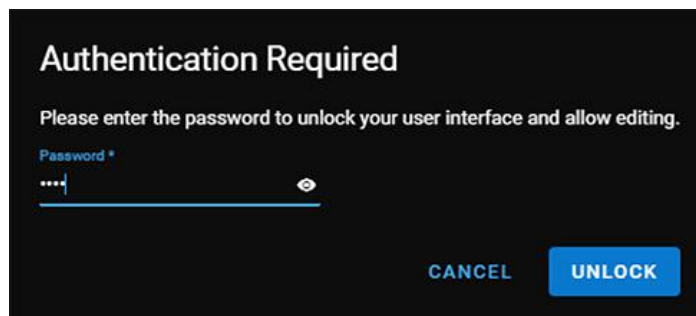
The user interface is locked, and you can only view the **Runtime** step.



To unlock the user interface:

- Exit the **Runtime** step.

The **Authentication Required** dialog appears:



- Fill in the **Password** field and click **Unlock**.

Note: The WebUI locks you out after a few minutes of inactivity.

Forgotten Password

Reset your DataMan reader to factory settings.

Removing the Password

Disable the **Password Protection** toggle, then click **Turn off** on the pop-up.

Recommendations

Cognex recommends that you comply with following security considerations:

- Follow established security best practices and industry guidance.
- Refer to NIST, IEC, and ISO security guidelines where applicable.
- Apply advanced security measures only when risk analysis requires them.
- Cognex recommends using SHA-256 fingerprints for SFTP communication. SHA-1 and MD5 are also available for legacy applications, but are cryptographically weak.

