

Security Guideline for DX-series Controller

NOTE

- This document does not provide detailed instructions for use, including safety precautions. Be sure to obtain the manuals and operating instructions for each device listed in this document and confirm their contents, including *Safety Precautions*, *Precautions for Safe Use*, and *Precautions for Correct Use* and other safety precautions before use.
- All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, mechanical, electronic, photocopying, recording, or otherwise, without the prior written permission of OMRON.
- No patent liability is assumed with respect to the use of the information contained herein. Moreover, because OMRON is constantly striving to improve its high-quality products, the information contained in this guide is subject to change without notice.
- Every precaution has been taken in the preparation of this document. Nevertheless, OMRON assumes no responsibility for errors or omissions.

Trademarks

- Microsoft, Windows, Excel, Visual Basic, and Microsoft Edge are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- ODVA, CIP, CompoNet, DeviceNet, and EtherNet/IP are trademarks of ODVA.
- SpeedBee Synapse is a trademark of SALTYSTER Co., Ltd.
- Grafana is a trademark of Grafana Labs.

Other company names and product names in this document are the trademarks or registered trademarks of their respective companies.

Copyrights

- Microsoft product screen shots used with permission from Microsoft.
- This product incorporates certain third party software. The license and copyright information associated with this software is available at https://www.fa.omron.co.jp/product/tool/dx-info/index_en.html.

Introduction

Purpose of This Document

The purpose of this document is to provide you with an understanding of security initiatives of OMRON on its FA products and propose the security measures that the users of the FA products should take on their own. It describes the security measures that you can implement using the DX-series Data Flow Controller.

Please read this document together with the Security Guideline for Factory Automation System and related manuals.

Intended Audience

This document is intended for the following people who plan, examine, and implement security measures.

- Personnel in charge of designing and operating data utilization systems on a production site.
- Personnel in charge of designing and operating maintenance systems on a production site.

Applicable Products

This document covers the following product.

- DX-series Data Flow Controller (hereinafter referred to as the *DX Controller*.)

Refer to the user's manual for the product for product specifications.

Disclaimer

The recommendations we make to our customers in this document are based on the results of our analysis and study. Appropriate security measures vary with customer environment, so these recommendations do not guarantee prevention of all security breaches in customer environments. Referring to this document, please consider and implement analysis and appropriate countermeasures in line with the customer's environment on your own.

Sections in this Guideline

		1
1	Security Measures Using the DX Controller	2
2	Security Functions of the DX Controller	3
3	Applying Security Patches	4
4	Safely Disposing of Devices	A
A	Appendices	

CONTENTS

Introduction	1
Purpose of This Document	1
Intended Audience	1
Applicable Products	1
Disclaimer	1
Sections in this Guideline	3
Related Guideline and Manuals	6
Revision History	7

Section 1 Security Measures Using the DX Controller

1-1 Operating Environment of the DX Controller	1-2
1-2 Security Functions of the DX Controller in Technical Layers	1-3

Section 2 Security Functions of the DX Controller

2-1 Protecting Data on Communication Lines	2-2
2-1-1 Secure Communication	2-2
2-2 Preventing Unauthorized Connection to the DX Controller.....	2-4
2-2-1 Account Management (User Authentication for DX Controller).....	2-4
2-2-2 USB Port Management	2-5
2-3 Preventing Unauthorized Operations on the DX Controller	2-6
2-3-1 Account Management (Operation Authority Verification for DX Controller)	2-6
2-4 Preventing Unauthorized Connection to Applications.....	2-7
2-4-1 Account Management (User Authentication for Application).....	2-7
2-5 Preventing Unauthorized Operations on Applications	2-8
2-5-1 Operation Authority Verification (Applications).....	2-8
2-6 Preventing Repudiation.....	2-9
2-6-1 Log Function	2-9

Section 3 Applying Security Patches

3-1 Updating the DX Controller.....	3-2
3-1-1 Firmware Update Log.....	3-2
3-2 Updating the OS of Your PC	3-3
3-3 Updating Your Browser	3-4

Section 4 Safely Disposing of Devices

4-1 Erasing Your Data in the DX Controller	4-2
4-1-1 Initialization (Factory Reset).....	4-2

Appendices

A-1	Contact Information for This Guide and Factory Automation Products of OMRON	A-2
-----	---	-----

Related Guideline and Manuals

The followings are the guidelines and manuals related to this document. Read them for reference.

Document name	No.	Application
Security Guideline for Factory Automation System	P162	Learning the concept of security for FA systems in general.
DX-series Data Flow Controller User's Manual	V241	Learning the security functions provided in the DX-series Data Flow Controller and their usage.
DX-series Web UI User's Manual	V242	Learning how to set the security functions provided in the DX-series Data Flow Controller.

Revision History

A revision code appears as a suffix to the catalog number on the front and back covers of this document.

Cat. No.

V303-E1-01

Revision code

Revision code	Date	Revised content
01	September 2025	Original production

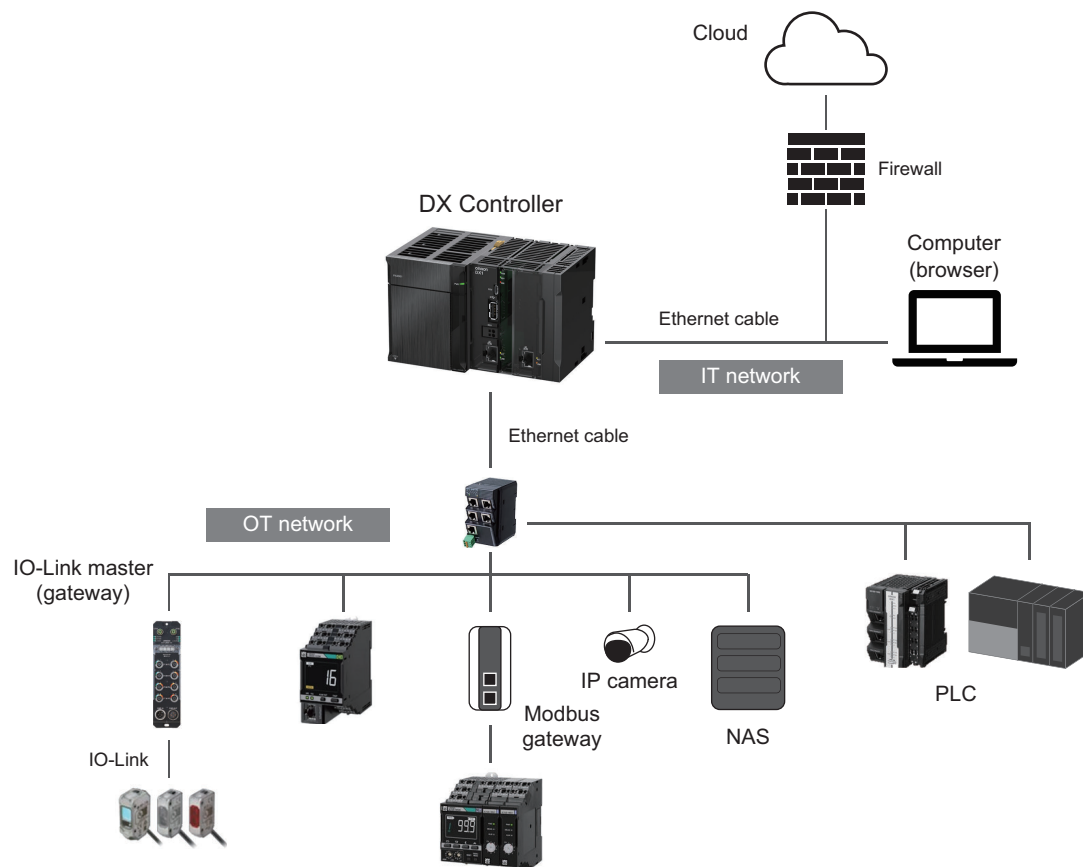
Security Measures Using the DX Controller

The DX Controller provides multiple security functions to achieve Defense in Depth. This section describes environments using the DX Controller and the security functions of the DX Controller.

1-1	Operating Environment of the DX Controller	1-2
1-2	Security Functions of the DX Controller in Technical Layers	1-3

1-1 Operating Environment of the DX Controller

The DX Controller allows you to add data collection and visualization functions while maintaining the security of your system and equipment by utilizing its security functions. The DX Controller prevents unauthorized connections and operations to protect data collected from equipment and devices. In environments using the DX Controller, implement Defense in Depth by combining the measures described in the *Security Guideline for Factory Automation System (Cat. No. P162)* according to the purpose and the type of threat.



Things That You Should Do

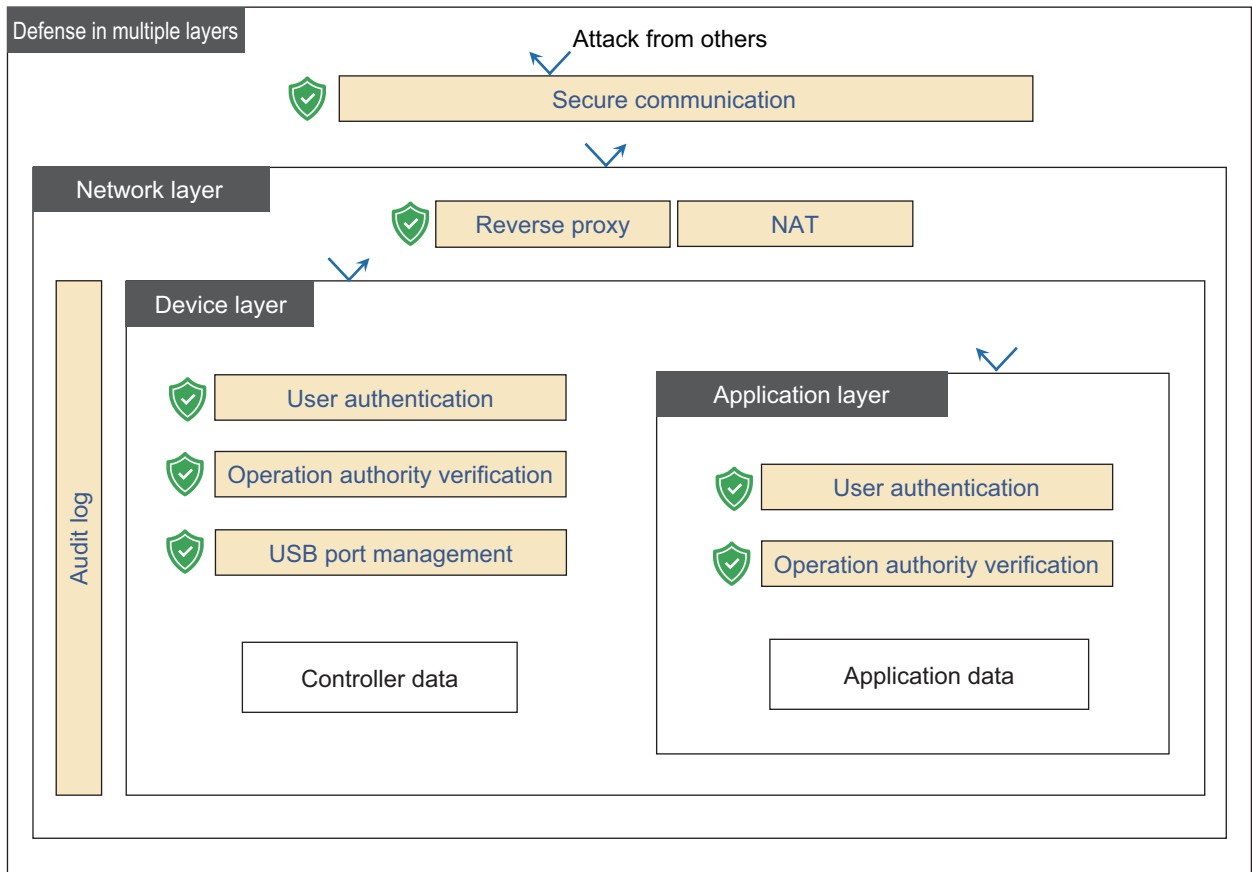
- For networks of equipment and devices, install firewalls and packet filtering.
- Separate IT networks (networks of PCs, servers, MES, etc.) from OT networks (networks of equipment and devices).
- Operate the following protocols, if used, in a network environment that ensures their secure use.
NTP, DNS, mDNS, and DHCP
- Effectively utilize the security functions of the equipment and devices themselves.
- For secure operation, implement access control and physical locking for the system, equipment and devices, and installation area of the DX Controller.

1-2 Security Functions of the DX Controller in Technical Layers

The DX Controller provides security functions to protect your data in the Defense in Depth concept. It prevents unauthorized connections and operations by attackers to protect your data.

In this document, things that you should do in particular using the security functions are described.

Read the section in conjunction and take necessary measures.



The table below lists the functions provided in each layer.

Refer to Section 2 for functions that the customer should configure or operate.

Layer to protect data	Purpose	Function provided by OMRON products	Reference
Network layer	Protecting data on communication lines	Secure communication	page 2-2
	Blocking external attacks on the DX Controller	Reverse proxy <ul style="list-style-type: none"> Hides the IP addresses of the application's web servers from the outside and prevents direct access to the applications from outside the network. 	---
		NAT <ul style="list-style-type: none"> Hides the IP address of the Data Flow Controller from the outside and prevents attacks from outside the network. 	---
Device layer	Preventing unauthorized connection to the DX Controller	Account Management (User Authentication for DX Controller)	page 2-4
		USB Port Management	page 2-5
	Preventing unauthorized operations on the DX Controller	Account Management (Operation Authority Verification for DX Controller)	page 2-6
Application layer	Preventing unauthorized connection to applications	Account Management (User Authentication for Application)	page 2-7
	Preventing unauthorized operations on applications	Account Management (Operation Authority Verification for Application)	page 2-8
Common to all layers	Preventing repudiation	Audit log	page 2-9

Security Functions of the DX Controller

This section describes the security functions that the DX Controller provides.

2-1	Protecting Data on Communication Lines	2-2
2-1-1	Secure Communication	2-2
2-2	Preventing Unauthorized Connection to the DX Controller	2-4
2-2-1	Account Management (User Authentication for DX Controller).....	2-4
2-2-2	USB Port Management	2-5
2-3	Preventing Unauthorized Operations on the DX Controller	2-6
2-3-1	Account Management (Operation Authority Verification for DX Controller).....	2-6
2-4	Preventing Unauthorized Connection to Applications	2-7
2-4-1	Account Management (User Authentication for Application).....	2-7
2-5	Preventing Unauthorized Operations on Applications	2-8
2-5-1	Operation Authority Verification (Applications)	2-8
2-6	Preventing Repudiation	2-9
2-6-1	Log Function.....	2-9

2-1 Protecting Data on Communication Lines

Equipment connected to the Internet is subject to the risk of cyberattacks over the network. Use the following functions to prevent information disclosure from data flowing over communication lines, tampering, and denial of service.

2-1-1 Secure Communication

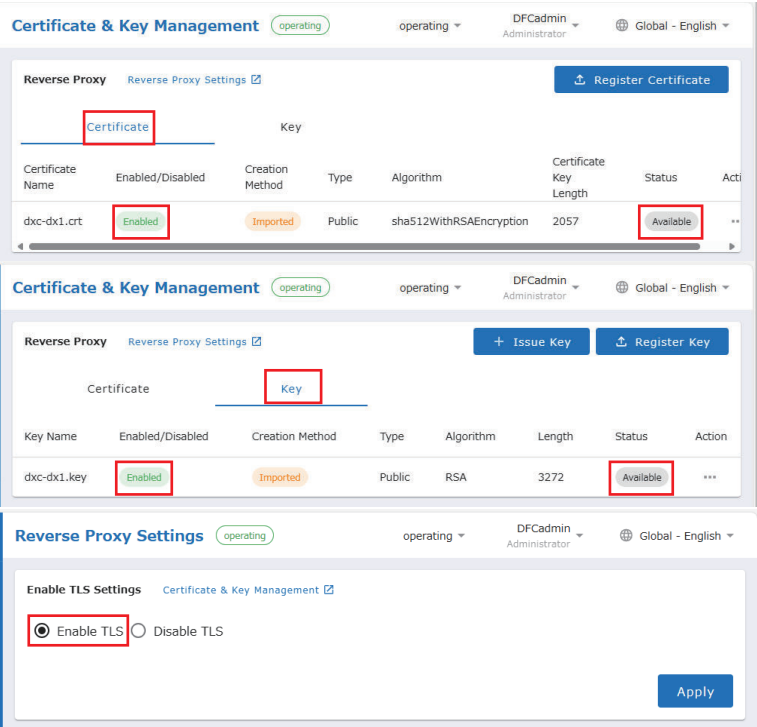
The secure communication function is designed to improve security for communications between the DX Controller and other devices or systems. Since it encrypts and then adds hash values to communications data before sending and receiving, it is useful to prevent eavesdropping and tampering by a third party.

The DX Controller allows you to use secure communications with the following devices.

- Browser (computer)
- Other DX Controllers

Refer to the *DX-series CPU Unit User's Manual (Cat. No. V241)* for the procedure to enable secure communications with a browser (computer). Note that secure communications with the browser (computer) are enabled when the settings are configured as follows.

- The certificate and key are registered with **Enabled/Disabled** being **Enabled** and **Status** being **Available** for each.
- The **Enable TLS** check box is selected in **Enable TLS Settings**.



Refer to the *DX Series User's Manual Factory Monitoring Package Edition (Cat. No. N702)* for the procedure to enable secure communications between DX Controllers.

Threats That Can Be Addressed

Spoofting	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Yes	Yes		Yes	Yes	

Things That You Should Do

- To improve security, use PCs and devices with operating systems that are within their support periods.
- For networks of control systems and equipment, install a firewall (blocking unused communications ports and restricting communications hosts) to isolate them from IT networks. Make sure that the PCs are connected to the DX Controller inside the firewall.
- Place NTP, DHCP, and DNS servers in a trusted internal network and take security measures for these servers.
- When you use an application function to communicate with other devices, it is recommended to use encrypted communications, if available.
For example, some components of SpeedBee Synapse provide a setting for encrypted communications. Refer to the *DX-series SpeedBee Synapse User's Manual (Cat. No. V243)* for the components of SpeedBee Synapse. For components that support encrypted communications, a description of the encryption function is provided.
If you cannot use encrypted communications, for secure operation, implement access control and physical locking for the system, equipment and devices, and installation areas of DX Controller.
- Security issues such as unauthorized data acquisition, data tampering, and loss of communications may occur due to theft, information leaks, and tampering of server certificates or private keys related to secure communications by third parties. Take adequate measures for the management of certificates and private keys and for the prevention of theft, information leaks, and tampering. Especially, use an encrypted safe communications path, etc. when obtaining the private key to avoid information leaks. Furthermore, store the private key in a safe location where the risk of information leakage is extremely low.

2-2 Preventing Unauthorized Connection to the DX Controller

To protect your important production information and data from theft and unauthorized utilization, use this function to authenticate users when they connect to the DX Controller so that unauthorized users cannot easily access the DX Controller.

2-2-1 Account Management (User Authentication for DX Controller)

This function performs user authentication by user name and password when a user attempts to go online to identify who will perform online operations.

User authentication is a function that identifies who will operate the DX Controller online by registering users to operate the DX Controller in the DX Controller in advance. When a user attempts to go online with the DX Controller, the user is asked to enter a user name and password. The user cannot go online unless the user name and password match the pre-defined settings.

Furthermore, each user is assigned one of the following roles: Administrator, Designer, or Maintainer. This ensures that users can operate the DX Controller online only within the scope of the roles assigned to them.

User authentication settings such as the user name, password, and information on the role of the user are saved in the DX Controller. Therefore, user authentication can be used even when you connect to the DX Controller from a different PC.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Yes	Yes	Yes	Yes	Yes	Yes

User authentication allows you to operate the DX Controller within the scope of permissions of the assigned role by entering your user name and password when you go online with the Web UI of the DX Controller from your PC. Refer to the *DX-series Web UI Operation Manual (Cat. No. V242)* for details on how to operate this function.

Things That You Should Do

- Disable user account that is registered by default.
- Change your password by yourself on a periodic basis.
- Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks.
- The DX Controller supports generating an access token (authentication key) for each user to enable access to the DX Controller from external systems. Keep your access token strictly secure so that it is not disclosed to third parties.

2-2-2 USB Port Management

Leaving the USB ports on the DX Controller enabled when they are not in use poses a risk of unauthorized access to the DX Controller through the USB ports. This function disables the USB ports when they are not in use to prevent third parties from accessing the DX Controller through the USB ports.

Refer to the description of USB port management in the *DX-series Web UI Operation Manual (Cat. No. V242)* for the method for disabling the USB port.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
	Yes		Yes	Yes	

2-3 Preventing Unauthorized Operations on the DX Controller

Prevent unauthorized operations on the DX Controller to protect your important production information and data from theft, unauthorized utilization, and system malfunctions.

Things That You Should Do

- For secure operation, implement access control and physical locking for the system, equipment and devices, and installation area of the DX Controller.

2-3-1 Account Management (Operation Authority Verification for DX Controller)

Changing data in the DX Controller poses the risk of damage, such as inability to collect or utilize data correctly due to operating mistakes. Prevent operating mistakes by restricting the functions that operators can perform based on their roles.

Using the operator authority verification function, administrators can set a role for each operator according to the role that the operator should perform.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
	Yes		Yes	Yes	Yes

Refer to the *DX-series Web UI Operation Manual (Cat. No. V242)* for setting the operation authority verification function.

Things That You Should Do

- Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks.
- Change your password by yourself on a periodic basis.

2-4 Preventing Unauthorized Connection to Applications

To protect your important production information and data from theft and unauthorized utilization, use this function to authenticate users when they connect to each application so that unauthorized users cannot easily access the data collection and visualization applications in the DX Controller.

2-4-1 Account Management (User Authentication for Application)

This function performs user authentication by user name and password when a user attempts to connect to an application on the DX Controller in order to identify who will operate the application online. It improves security by implementing user authentication based on individual account management for each application, in addition to the user authentication for connecting to the DX Controller.

User authentication for application is a function that identifies users who will operate an application online by registering them in the application in advance. When a user attempts to connect to an application on the DX Controller, the user is asked to enter a user name and password. The user cannot connect to the application unless the user name and password match the pre-defined settings.

Furthermore, each user is assigned a set of permissions. This ensures that users can only operate the application within the scope of the permissions assigned to them.

User authentication settings such as the user name, password, and information on the user's permissions are saved in the DX Controller. Therefore, user authentication for application can be used even when you connect to the DX Controller from a different PC.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Yes	Yes	Yes	Yes	Yes	Yes

User authentication for application allows you to operate a specific application within the scope of the assigned permissions by entering your user name and password when you connect to the application in the DX Controller. For details on how to operate this function, refer to the *DX-series SpeedBee Synapse User's Manual (Cat. No. V243)* for SpeedBee Synapse and the manual for Grafana for Grafana. Refer to the *DX-series Dashboard Generator User's Manual (Cat. No. N700)* for the Packages.

Things That You Should Do

- Disable or delete user accounts that are registered by default.
- Change your password by yourself on a periodic basis.
- Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks.
- Keep your access token strictly secure so that it is not disclosed to third parties.

2-5 Preventing Unauthorized Operations on Applications

Prevent unauthorized operations on applications installed on the DX Controller to protect your important production information and data from theft, unauthorized utilization, and system malfunctions.

Things That You Should Do

- If exported files contain confidential information, encrypt and manage them strictly so that they are not leaked to third parties or tampered with. In addition, when obtaining data to import, check that the hash value matches the expected value to ensure it has not been tampered with.

2-5-1 Operation Authority Verification (Applications)

Changing data in an applications poses the risk of damage, such as inability to collect or utilize data correctly due to operating mistakes. Prevent operating mistakes by restricting the functions that operators can perform based on the permissions assigned to them.

Using the operator authority verification function, administrators can set permissions for each operator according to the role that the operator should perform.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
	Yes		Yes	Yes	Yes

For setting the operation authority verification function, refer to the *DX-series SpeedBee Synapse User's Manual (Cat. No. V243)* for SpeedBee Synapse and the Grafana manual for Grafana.

Things That You Should Do

- Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks.
- Change your password by yourself on a periodic basis.

2-6 Preventing Repudiation

To protect your data, it is also important to grasp the fact that they have been subjected to unauthorized operations. In addition, in the event of a security incident, it is necessary to determine the cause and circumstances of the incident. Recording security breaches and cyberattacks allows you to confirm who did what and when, and can be used as a repudiation preventive measure when problems occur.

2-6-1 Log Function

The DX Controller registers important security-related online operations that users perform on it using the Web UI as an operation log. The operation log records the operation details, time, user name, and result (success or failure). Applications on the DX Controller also register their own logs, among which those related to security are available for use as audit logs. Note that application logs are divided into two types: logs that are registered in the Data Flow Controller and logs that are registered in the application itself.

Refer to the *DX-series CPU Unit User's Manual (Cat. No. V241)* for the DX Controller logs.

For the application logs, refer to the *DX-series SpeedBee Synapse User's Manual (Cat. No. V243)* for SpeedBee Synapse and the manual for Grafana for Grafana. Refer to the *DX-series Dashboard Generator User's Manual (Cat. No. N700)* for the Packages.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
		Yes			

Things That You Should Do

- If the date and time of recorded logs are not accurate, you may not be able to prevent repudiation. Set the correct time on both the DX Controller and the computer. To maintain the correct date and time, it is recommended to set the date and time via NTP.
- If the logs are deleted, you cannot prevent repudiation. If the number of events exceeds the number of records permitted, the log will be deleted from older information. In addition, performing initialization (factory reset) erases application logs. It is recommended to download logs periodically based on your environment and the log retention period for your operation, and store them for a certain period of time.

3

Applying Security Patches

To protect your data from cyberattacks progressing day by day, it is effective to keep your devices up-to-date for higher security strength.
This section describes the functions that the DX Controller provides for updates.

3-1	Updating the DX Controller	3-2
3-1-1	Firmware Update Log	3-2
3-2	Updating the OS of Your PC	3-3
3-3	Updating Your Browser	3-4

3-1 Updating the DX Controller

To add functionality, improve ease of operation, and enhance security, always keep the DX Controller updated to the latest version for use.
Refer to the *DX-series CPU Unit User's Manual (Cat. No. V241)* for details on firmware update.

Things That You Should Do

- Use a USB memory device to update the DX Controller. To ensure that updates are performed only by authorized operators, set appropriate operation authority and implement access control, physical locking, etc.
- To use USB memory devices for updates, you must enable the USB port. If the USB port is disabled before an update, disable it again after the update is completed.

3-1-1 Firmware Update Log

Check the firmware update log in the DX Controller logs.
Refer to the *DX-series Web UI Operation Manual (Cat. No. V242)* for details on how to check the DX Controller logs.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
		Yes			

3-2 Updating the OS of Your PC

To avoid security risks arising from vulnerabilities in the OS, always keep the OS of your PC on which the Web UI is running up-to-date.

3-3 Updating Your Browser

To avoid security risks arising from vulnerabilities in your browser, always keep the browser that connects to the Web UI up-to-date.

4

Safely Disposing of Devices

This section describes the functions that the DX Controller provides for disposal.

4-1	Erasing Your Data in the DX Controller.....	4-2
4-1-1	Initialization (Factory Reset).....	4-2

4-1 Erasing Your Data in the DX Controller

Disposing of or transferring your OMRON products poses the risk of information disclosure, allowing third parties to view user data and other information saved in the devices.

Before disposing of or transferring the products, erase the user data with your responsibility.

4-1-1 Initialization (Factory Reset)

Initialization (factory reset) is a function that resets the DX Controller to the factory default settings. It also erases all user-configured data.

Refer to the *DX-series CPU Unit User's Manual (Cat. No. V241)* for details on the factory reset function.

Things That You Should Do

- The DX Controller has DIP switches for enabling functions such as initializing its settings (factory reset). For secure operation, take measures to prevent unauthorized operation of the DIP switches. For example, implement access control, physical locking, etc.



Appendices

A-1	Contact Information for This Guide and Factory Automation Products of OMRON.....	A-2
-----	---	-----



A-1 Contact Information for This Guide and Factory Automation Products of OMRON


If you have any questions about this guide or FA products of OMRON, please contact your nearest OMRON branch or sales office from the following links.

https://www.ia.omron.com/global_network/

OMRON Corporation Industrial Automation Company

Kyoto, JAPAN

Contact : www.ia.omron.com

 Contact for inquiries for this product (only for DX-series)

DataPF-contactdesk-OC@omron.com

Operation Hours: 9:00 to 17:00 (except Saturdays, Sundays, and Dec. 31 to Jan. 3), JST



Tutorial Video

<https://www.fa.omron.co.jp/dx1/video-manual/en/>



Authorized Distributor:

©OMRON Corporation 2025 All Rights Reserved.
In the interest of product improvement,
specifications are subject to change without notice.

Cat. No. V303-E1-01 0925