

Recommendations for secure networked devices



Table of contents

1	Setting the IP Address Filtering	
1.1	IP Address Filtering.....	3
1.2	Quick IP Filtering.....	3
2	Setting the Encrypted Communication	
2.1	TLS encryption.....	4
2.1.1	HTTP (Web Connection)	4
2.1.2	WebDAVServer	4
2.1.3	IPP.....	5
2.1.4	OpenAPI.....	5
2.1.5	RemotePanel.....	5
2.1.6	DPWS.....	5
2.1.7	POP.....	5
2.1.8	SMTP	5
2.1.9	IEEE802.1X Auth	5
2.1.10	LDAP	6
2.1.11	TCP Socket.....	6
2.2	Other encryption	7
2.2.1	SMBServer.....	7
	SMB Encryption.....	7
	SMB Signature.....	7
2.2.2	SMBClient.....	8
2.2.3	SNMP.....	8
2.2.4	IPsec	8
2.2.5	S/MIME	9
3	Setting the Certificate Validation	
3.1	POP.....	10
3.2	SMTP	10
3.3	IEEE802.1X Auth	10
3.4	IPsec	10
3.5	WebDAVClient	11
3.6	LDAP	11
3.7	DPWS.....	11
3.8	OpenAPI.....	11
3.9	RemotePanel.....	11
4	Additional Security Information	
4.1	Recommendation of best practice.....	12
4.2	Precautions for communicating with legacy systems	13
	IPsec legacy settings	13
4.3	Network interfaces and services available from factory shipment	14
4.4	About input validation	15



About this manual

This manual describes information and settings that enables safe use of devices.

When connecting the machine to the network, use it in an environment protected by a firewall. We also recommend that you set a private IP address for the IP address of the machine.

Setting a private IP address only allows users on a local area network, such as an internal LAN, to access the machine, preventing unauthorized access from outside.

If you need to use a global IP address, be sure to install the machine inside a firewall.

1 Setting the IP Address Filtering

IP address filtering is a function that restricts the devices that can access the machine by the IP address. Setting this function correctly allows you to restrict access from unauthorized devices.

The IP address filtering function of the machine can be set in the following two methods.

1.1 IP Address Filtering

Manually specify the range of IP addresses that allow or deny access.

Setting location: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IP Address Filtering]



Tips

Set the IP addresses to be allowed or denied to suit your environment.

1.2 Quick IP Filtering

The range of IP addresses to allow access is automatically set based on the IP address and subnet mask set in the machine.

Setting location: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [Quick IP Filtering]

Recommended settings: [Synchronize IP Address]/[Synchronize Subnet Mask] *

* Select either one to suit your environment.

2 Setting the Encrypted Communication

We recommend that you use the following encrypted communication to prevent data eavesdropping, data tampering, and session hijacking.

2.1 TLS encryption

We recommend that you configure the following settings to reduce the risk of vulnerabilities.

Setting location: [Utility] - [Administrator] - [Security] - [PKI Settings] - [Enable SSL Version]

Setting item	Recommended setting
[Mode using SSL/TLS]	[Admin. Mode and User Mode]
[SSL/TLS Version Setting]	TLS1.2 TLS1.3 (IEEE802.1X incompatible)
[Encryption Strength]	AES-256

The initial certificate is installed at the factory. If you need a different certificate, register a new one at the following location.

Setting location: [Utility] - [Administrator] - [Security] - [PKI Settings] - [Device Certificate Setting]

Setting item	Recommended setting
[Encryption Key Type]	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

The TLS encryption is supported for the following protocols and services. For details on the setting locations, refer to the following sections.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP Socket

2.1.1 HTTP (Web Connection)

If you enable [Enable SSL Version], the communication mode automatically switches to the TLS encrypted communication (HTTPS).

2.1.2 WebDAVServer

Setting location: [Utility] - [Administrator] - [Network] - [WebDAV Settings] - [WebDAV Server Settings]

Setting item	Recommended setting
[SSL Settings]	[SSL Only]

2.1.3 IPP

Setting location: [Utility] - [Administrator] - [Network] - [HTTP Server Settings]

Setting item	Recommended setting
[IPP-SSL Settings]	[SSL Only]

2.1.4 OpenAPI

Setting location: [Utility] - [Administrator] - [Network] - [OpenAPI Setting] - [OpenAPI Setting]

Setting item	Recommended setting
[SSL/Port Settings]	[SSL Only]

2.1.5 RemotePanel

Setting location: [Utility] - [Administrator] - [Network] - [Remote Panel Settings] - [Remote Panel Server Settings]

Setting item	Recommended setting
[Port No.(SSL)]	[50443]



Tips

If you enable [Enable SSL Version], the communication automatically switches to the TLS encrypted mode. Specify a port number.

2.1.6 DPWS

Setting location: [Utility] - [Administrator] - [Network] - [DPWS Settings] - [DPWS Common Settings]

Setting item	Recommended setting
[SSL Settings]	ON

2.1.7 POP

Setting location: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail RX (POP)]

Setting item	Recommended setting
[Enable SSL]	ON

2.1.8 SMTP

Setting location: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail TX (SMTP)]

Setting item	Recommended setting
[SSL/TLS Settings]	[SMTP over SSL]

2.1.9 IEEE802.1X Auth

Setting location: [Utility] - [Administrator] - [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Setting] - [Supplicant Setting]

Setting item	Recommended setting
[EAP-Type]	Select [EAP-TLS], [EAP-TTLS], or [PEAP].

2.1.10 LDAP

Setting location: [Utility] - [Administrator] - [Network] - [LDAP Setting] - [Setting Up LDAP]

Setting item	Recommended setting
[Enable SSL]	ON

2.1.11 TCP Socket

Setting location: [Utility] - [Administrator] - [Network] - [TCP Socket Setting]

Setting item	Recommended setting
[Use SSL/TLS]	ON

2.2 Other encryption

We recommend that you configure the following settings to reduce the risk of vulnerabilities. For details on the settings for each function, refer to the following sections.

Function	Recommended setting
SMBServer	SMB Encryption, SMB Signature
SMBClient	Kerberos Authentication
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	ON

2.2.1 SMBServer

Using the SMB encryption and SMB signature can reduce the following security risks.

- Eavesdropping: A malicious third party may intercept communications and steal personal or confidential information.
- Data tampering: There is a risk that communication contents may be tampered with by a Man-In-The-Middle Attack (MITM).
- Spoofing: If authentication information is stolen, a third party may pose as a legitimate user to gain unauthorized access.
- Information leakage: Unencrypted communications can be easily intercepted, especially on public Wi-Fi networks, increasing the risk of personal information and credit card information being leaked.

SMB Encryption

Prerequisites

- Create a Public User Box. Also, configure the setting to automatically transfer files from the Public User Box and save them in the SMB folder.
- Specify the password for the User Box.

Setting location: [Utility] - [Administrator] - [Box] - [User Box List]

Setting item	Recommended setting
[SMB Communication Encryption]	[Encrypt]

SMB Signature

Setting location: [Utility] - [Administrator] - [Network] - [SMB Setting] - [SMB Server Settings]

Setting item	Recommended setting
[SMB security Signature Setting]	[Required]

2.2.2 SMBClient

The Kerberos authentication uses strong encryption technology, significantly reducing the risk of credentials being stolen during the authentication process. It also ensures data integrity, preventing data tampering between the sender and receiver as well as NTLM relay attacks.

Setting location: [Utility] - [Administrator] - [Network] - [SMB Setting] - [Client Setting]

Setting item	Recommended setting
[SMB Authentication Setting]	[Kerberos]

2.2.3 SNMP

Set the encryption using SNMPv3. If the authentication setting is also added, you can further increase safety. The security risks are about the same as with SMB.

Setting location: [Utility] - [Administrator] - [Network] - [SNMP Setting]

Setting item	Recommended setting
[SNMP Setting]	[SNMP v3(IP)]
[Encryption Algorithm]	[AES-128]
[Authentication Method]	Select [SHA-256], [SHA-384], or [SHA-512].

2.2.4 IPsec

Setting location: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IPsec] - [IPsec Setting]

[IKEv2]

Setting item	Recommended setting
[Encryption Algorithm]	[AES-CBC] ([256]/[192 and 256]/[All])
[Authentication Algorithm]	[SHA-2] ([256]/[384]/[512]/[256 and 384]/[384 and 512]/[All]), [AES-XCBC]
[Diffie-Hellman Group]	[Group 14], [Group 19]

[SA]

Setting item	Recommended setting
[Encapsulation Mode]	[Tunnel], [Transport]
[Security Protocol]	[ESP]
[Key Exchange Method]	[IKEv2]
[Authentication Method]	[Digital Signature]
[ESP Encryption Algorithm]	[AES-GCM] ([256]/[192 and 256]/[All]), [AES-GCM-64] ([256]/[192 and 256]/[All]), [ENC_NULL_AES_GMAC] ([256]/[192 and 256]/[All])
[Perfect Forward Secrecy]	ON
[Diffie-Hellman Group(IKEv2)] - [Priority1-4]	[Group 14], [Group 19]

2.2.5 S/MIME

If you use the optional S/MIME when sending e-mail, you can encrypt the e-mail content to prevent eavesdropping and verify the sender's identity with an electronic signature. This is an effective measure against spoofing and phishing scams.

Setting location: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [S/MIME]

Setting item	Recommended setting
[Digital Signature]	[Always add signature]
[Digital Signature Type]	[SHA-256]
[E-Mail Text Encrypt. Method]	[AES-256]

3 Setting the Certificate Validation

When using the TLS encrypted communication to reduce the impact of man-in-the-middle attacks, we recommend that you use the certificate validation. For validation items, we recommend that you enable the certificate expiration date and chain at a minimum.

If an attempt is made to connect to a legacy environment that does not have a certificate validation function, the risk of man-in-the-middle attacks increases. We recommend that you use it in a secure network environment.

The certificate validation on the MFP side is recommended in the following MFP client functions. For details on the setting locations, refer to the following sections.

POP, SMTP (Start TLS/SMTP over SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPsec, WebDAV, LDAP, DPWS, RemotePanel



Tips

The certificate validation on the client side connected to the MFP is recommended in the following MFP server functions.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP Socket

3.1 POP

Setting location: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail RX (POP)]

Setting item	Recommended setting
[Certificate Verification Level Settings]	[Expiration Date]: ON [Chain]: ON

3.2 SMTP

Setting location: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail TX (SMTP)]

Setting item	Recommended setting
[Certificate Verification Level Settings]	[Expiration Date]: ON [Chain]: ON

3.3 IEEE802.1X Auth

Setting location: [Utility] - [Administrator] - [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Setting] - [Supplicant Setting]

Setting item	Recommended setting
[Certificate Verification Level Settings]	[Expiration Date]: ON [Chain]: ON

3.4 IPsec

Setting location: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IPsec] - [Enable IPsec]

Setting item	Recommended setting
[Certificate Verification Level Settings]	[Expiration Date]: [Confirm] [Chain]: [Confirm]



Tips

In [IPsec Setting], register items [IKE], [SA], [Peer], and [Protocol Setting] in advance.

3.5 WebDAVClient

Setting location: [Utility] - [Administrator] - [Network] - [WebDAV Settings] - [WebDAV Client Settings]

Setting item	Recommended setting
[Certificate Verification Level Settings]	[Expiration Date]: ON [Chain]: ON

3.6 LDAP

Setting location: [Utility] - [Administrator] - [Network] - [LDAP Setting] - [Setting Up LDAP]

Setting item	Recommended setting
[Certificate Verification Level Settings]	[Expiration Date]: ON [Chain]: ON

3.7 DPWS

Setting location: [Utility] - [Administrator] - [Network] - [DPWS Settings] - [DPWS Common Settings]

Setting item	Recommended setting
[Certificate Verification Level Settings]	[Expiration Date]: ON [Chain]: ON

3.8 OpenAPI

Setting location: [Utility] - [Administrator] - [Network] - [OpenAPI Setting] - [OpenAPI Setting]

Setting item	Recommended setting
[Certificate Verification Level Settings]	[Expiration Date]: ON [Chain]: ON

3.9 RemotePanel

Setting location: [Utility] - [Administrator] - [Network] - [Remote Panel Settings] - [Remote Panel Client Settings]

Setting item	Recommended setting
[Certificate Verification Level Settings]	[Expiration Date]: ON [Chain]: ON

4 Additional Security Information

4.1 Recommendation of best practice

We recommend that the encryption algorithms to be used comply with the best practice settings recommended in the EUCC Guidelines on Cryptography and SOGIS-Agreed-Cryptographic-Mechanisms.

Below is a list of the encryption algorithms and key lengths recommended by the EUCC Guidelines on Cryptography and SOGIS-Agreed-Cryptographic-Mechanisms.

Item	Recommended setting
Encryption algorithms	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Encryption key length	RSA: 2048 bits or more ECC: 256 bits or more AES: 256 bits



Tips

For details, refer to the latest EUCC Guidelines on Cryptography and SOGIS-Agreed-Cryptographic-Mechanisms.

4.2 Precautions for communicating with legacy systems

The following protocols and versions are assumed to be used for communication with legacy systems.

Using legacy settings increases security risks, so please use them in a secure network environment.

Item	Legacy settings
Protocol	SLP FTP SMB (3.0 or earlier version, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Depend on Server/OFF) DPWS TCPSocket
Encryption algorithms	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Encryption key length	RSA: 1024 bits or less ECC: 160 bits or less AES: 128 bits or less DES: 56 bits 3DES: 112 bits

IPsec legacy settings

[IKEv1]

Setting item	Legacy settings
[Encryption Algorithm]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192])
[Authentication Algorithm]	Not used
[Diffie-Hellman Group]	[Group 1], [Group 2], [Group 5]

[IKEv2]

Setting item	Legacy settings
[Encryption Algorithm]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192])
[Authentication Algorithm]	Not used
[Diffie-Hellman Group]	[Group 1], [Group 2], [Group 5]

[SA]

Setting item	Legacy settings
[Key Exchange Method]	[IKEv1]
[Authentication Method]	[Digital Signature]
[ESP Encryption Algorithm]	[3DES-CBC] ([128]/[192]/[128 and 192]) [AES-CTR] ([128]/[192]/[128 and 192]) [AES-GCM] ([128]/[192]/[128 and 192]) [AES-GCM-64] ([128]/[192]/[128 and 192]) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192])
[Perfect Forward Secrecy]	ON
[Diffie-Hellman Group(IKEv1)]	[Group 1], [Group 2], [Group 5]

4.3 Network interfaces and services available from factory shipment

Service Type	Protocol	Port Number
DHCP	UDP	68
HTTP Server	TCP	80
NETBIOS Name Service	UDP	137
NETBIOS Datagram Service	UDP	138
SNMP	UDP	161
HTTP Server over SSL / IPP over SSL	TCP	443
LPD Print	TCP	515
DHCPv6 Client	UDP	546
IPP Print	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-tool)	TCP	8091
RAW Print	TCP	9100
RAW Print	TCP	9112
RAW Print	TCP	9113
RAW Print	TCP	9114
RAW Print	TCP	9115
RAW Print	TCP	9116
OpenAPI	TCP	50001

4.4 About input validation

For the number of characters to be input for network settings, etc., refer to each of the setting items in the User's Guide.

Depending on the encoding of the language, the maximum allowable input (data saved in the MFP) for items that support multibyte characters may be three-times the number of characters.



1	Setting the IP Address Filtering	
1.1	IP Address Filtering.....	3
1.2	Quick IP Filtering.....	3
2	Setting the Encrypted Communication	
2.1	TLS encryption.....	4
2.1.1	HTTP (Web Connection)	4
2.1.2	WebDAVServer	4
2.1.3	IPP.....	5
2.1.4	OpenAPI.....	5
2.1.5	RemotePanel.....	5
2.1.6	DPWS.....	5
2.1.7	POP.....	5
2.1.8	SMTP	5
2.1.9	IEEE802.1X Auth	5
2.1.10	LDAP	6
2.1.11	TCP Socket.....	6
2.2	Other encryption	7
2.2.1	SMBServer.....	7
	SMB Encryption.....	7
	SMB Signature.....	7
2.2.2	SMBClient.....	8
2.2.3	SNMP.....	8
2.2.4	IPsec	8
2.2.5	S/MIME	9
3	Setting the Certificate Validation	
3.1	POP.....	10
3.2	SMTP	10
3.3	IEEE802.1X Auth	10
3.4	IPsec	10
3.5	WebDAVClient	11
3.6	LDAP	11
3.7	DPWS.....	11
3.8	OpenAPI.....	11
3.9	RemotePanel.....	11
4	Additional Security Information	
4.1	Recommendation of best practice.....	12
4.2	Precautions for communicating with legacy systems	13
	IPsec legacy settings	13
4.3	Network interfaces and services available from factory shipment	14
4.4	About input validation	15

Empfehlungen für sichere Netzwerkgeräte

Inhaltsverzeichnis

1 Einrichten der IP-Filterung

1.1	IP-Filterung	1-3
1.2	Schnelle IP-Filterung	1-3

2 Einrichten der verschlüsselten Kommunikation

2.1	TLS-Verschlüsselung	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP	2-5
2.1.4	OpenAPI	2-5
2.1.5	RemotePanel	2-5
2.1.6	DPWS	2-5
2.1.7	POP	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X-Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP-Socket	2-6
2.2	Sonstige Verschlüsselung	2-7
2.2.1	SMBServer	2-7
	SMB-Verschlüsselung	2-7
	SMB-Signatur	2-7
2.2.2	SMBClient	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Einrichten der Zertifikatvalidierung

3.1	POP	3-10
3.2	SMTP	3-10
3.3	IEEE802.1X-Auth.	3-10
3.4	IPsec	3-11
3.5	WebDAVClient	3-11
3.6	LDAP	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	RemotePanel	3-12

4 Zusätzliche Sicherheitsinformationen

4.1	Empfehlung für bewährte Verfahren	4-13
4.2	Hinweise zur Kommunikation mit Legacy-Systemen	4-14
	Legacy-IPsec-Einstellungen	4-14
4.3	Werksseitig verfügbare Netzwerkschnittstellen und -dienste	4-16
4.4	Informationen zur Eingabevalidierung	4-17



Informationen zu dieser Bedienungsanleitung

In dieser Bedienungsanleitung werden Informationen und Einstellungen beschrieben, die die sichere Nutzung der Geräte ermöglichen.

Wenn Sie das System mit dem Netzwerk verbinden, achten Sie darauf, dass die Netzwerkumgebung mit einer Firewall geschützt wird. Wir empfehlen außerdem, eine private IP-Adresse als IP-Adresse des Systems festzulegen.

Durch die Festlegung einer privaten IP-Adresse wird der Zugriff auf das System auf Benutzer beschränkt, die sich in einem lokalen Netzwerk, wie z. B. in einem internen LAN, befinden. Unbefugte externe Zugriffe werden dadurch ausgeschlossen.

Wenn Sie eine globale IP-Adresse verwenden müssen, installieren Sie das System unbedingt hinter einer Firewall.

1 Einrichten der IP-Filterung

Mit der Funktion für die IP-Filterung wird der Zugriff von Geräten auf das System basierend auf der IP-Adresse reguliert. Mit der ordnungsgemäßen Einrichtung dieser Funktion können Sie den Zugriff über nicht autorisierte Geräte unterbinden.

Die Funktion für die IP-Filterung des Systems kann anhand einer der folgenden beiden Methoden eingerichtet werden.

1.1 IP-Filterung

Legen Sie manuell den Bereich der IP-Adressen fest, denen der Zugriff gewährt oder verweigert werden soll.

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [TCP/IP Setting] (TCP/IP-Einstellung) - [IP Address Filtering] (IP-Filterung)



Tipps

Legen Sie die IP-Adressen fest, die innerhalb Ihrer Umgebung zugelassen oder gesperrt werden sollen.

1.2 Schnelle IP-Filterung

Der Bereich der IP-Adressen, denen der Zugriff gewährt wird, wird automatisch basierend auf der im System festgelegten IP-Adresse und Subnet-Maske definiert.

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [TCP/IP Setting] (TCP/IP-Einstellung) - [Quick IP Filtering] (Schnelle IP-Filterung)

Empfohlene Einstellungen: [Synchronize IP Address]/[Synchronize Subnet Mask] (IP-Adresse synchronisieren/Subnet-Maske synchronisieren) *

* Wählen Sie eine der Einstellungen entsprechend Ihrer Umgebung aus.

2 Einrichten der verschlüsselten Kommunikation

Wir empfehlen die Verwendung der im Folgenden beschriebenen verschlüsselten Kommunikation, um das Abhören oder Manipulieren von Daten und das Session-Hijacking zu verhindern.

2.1 TLS-Verschlüsselung

Wir empfehlen, die folgenden Einstellungen einzurichten, um die Gefahr von Schwachstellen zu verringern.

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Security] (Sicherheit) - [PKI Settings] (PKI-Einstellungen) - [Enable SSL Version] (SSL-Version aktivieren)

Einstellungselement	Empfohlene Einstellung
[Mode using SSL/TLS] (Modus mit SSL/TLS)	[Admin. Mode and User Mode] (Administratormodus und Benutzermodus)
[SSL/TLS Version Setting] (SSL/TLS-Versions-einstellung)	TLS1.2 TLS1.3 (inkompatibel mit IEEE802.1X)
[Encryption Strength] (Verschl.stärke)	AES-256

Das Erstzertifikat wird werksseitig installiert. Wenn Sie ein anderes Zertifikat benötigen, registrieren Sie ein neues Zertifikat anhand der folgenden Einstellung.

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Security] (Sicherheit) - [PKI Settings] (PKI-Einstellungen) - [Device Certificate Setting] (Gerätezertifikateinstellung)

Einstellungselement	Empfohlene Einstellung
[Encryption Key Type] (Verschl.schlüsseltyp)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Die TLS-Verschlüsselung wird für die folgenden Protokolle und Dienste unterstützt. Ausführliche Informationen zum Aufrufen der Einstellungselemente finden Sie in den folgenden Abschnitten.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start-TLS, SMTP over SSL)
- IEEE802.1X-Auth. (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP-Socket

2.1.1 HTTP (Web Connection)

Wenn Sie die Option [Enable SSL Version] (SSL-Version aktivieren) aktivieren, wechselt der Kommunikationsmodus automatisch zur TLS-verschlüsselten Kommunikation (HTTPS).

2.1.2 WebDAVServer

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [WebDAV Settings] (WebDAV-Einstellungen) - [WebDAV Server Settings] (WebDAV-Servereinstellungen)

Einstellungselement	Empfohlene Einstellung
[SSL-Einstell.]	[Nur SSL]

2.1.3 IPP

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [HTTP Server Settings] (HTTP-Servereinstellungen)

Einstellungselement	Empfohlene Einstellung
[IPP-SSL-Einstell.]	[Nur SSL]

2.1.4 OpenAPI

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [OpenAPI Setting] (OpenAPI-Einstellung) - [OpenAPI Setting] (OpenAPI-Einstellung)

Einstellungselement	Empfohlene Einstellung
[SSL-/Port-Einstellungen]	[Nur SSL]

2.1.5 RemotePanel

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [Remote Panel Settings] (Remote Panel-Einstellungen) - [Remote Panel Server Settings] (Remote Panel-Servereinstellungen)

Einstellungselement	Empfohlene Einstellung
[Portnummer (SSL)]	[50443]



Tipps

Wenn Sie die Option [Enable SSL Version] (SSL-Version aktivieren) aktivieren, wechselt die Kommunikation automatisch zum TLS-verschlüsselten Modus. Geben Sie eine Portnummer an.

2.1.6 DPWS

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [DPWS Settings] (DPWS-Einstellungen) - [DPWS Common Settings] (Allgemeine DPWS-Einstellungen)

Einstellungselement	Empfohlene Einstellung
[SSL-Einstell.]	ON (EIN)

2.1.7 POP

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [E-mail Setting] (E-Mail-Einstellung) - [E-mail RX (POP)] (E-Mail-Empfang [POP])

Einstellungselement	Empfohlene Einstellung
[SSL aktivieren]	ON (EIN)

2.1.8 SMTP

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [E-mail Setting] (E-Mail-Einstellung) - [E-mail TX (SMTP)] (E-Mail-Übertragung [SMTP])

Einstellungselement	Empfohlene Einstellung
[SSL/TLS-Einstellungen]	[SMTP over SSL]

2.1.9 IEEE802.1X-Auth.

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [IEEE802.1X Authentication Setting] (IEEE802.1X-Authentifizierungseinstellung) - [IEEE802.1X Authentication Setting] (IEEE802.1X-Authentifizierungseinstellung) - [Supplicant Setting] (Antragsteller-Einstellung)

Einstellungselement	Empfohlene Einstellung
[EAP-Typ]	Wählen Sie [EAP-TLS], [EAP-TTLS] oder [PEAP].

2.1.10 LDAP

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [LDAP Setting] (LDAP-Einstellung) - [Setting Up LDAP] (LDAP einrichten)

Einstellungselement	Empfohlene Einstellung
[SSL aktivieren]	ON (EIN)

2.1.11 TCP-Socket

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [TCP Socket Setting] (TCP-Socket-Einstellung)

Einstellungselement	Empfohlene Einstellung
[Use SSL/TLS] (SSL/TLS verwend.)	ON (EIN)

2.2 Sonstige Verschlüsselung

Wir empfehlen, die folgenden Einstellungen einzurichten, um die Gefahr von Schwachstellen zu verringern. Ausführliche Informationen zu den Einstellungen für die einzelnen Funktionen finden Sie in den folgenden Abschnitten.

Funktion	Empfohlene Einstellung
SMBServer	SMB Encryption (SMB-Verschlüsselung), SMB Signature (SMB-Signatur)
SMBClient	Kerberos Authentication (Kerberos-Authentifizierung)
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	ON (EIN)

2.2.1 SMBServer

Mit der SMB-Verschlüsselung und der SMB-Signatur können die folgenden Sicherheitsrisiken verringert werden.

- Abhörmaßnahmen: Böswillige Dritte können die Kommunikation abfangen und persönliche oder vertrauliche Informationen stehlen.
- Datenmanipulation: Es besteht die Gefahr, dass Kommunikationsinhalte per Man-In-The-Middle-Angriffen (MITM) manipuliert werden.
- Spoofing: Wenn Authentifizierungsinformationen gestohlen werden, kann sich ein Dritter als berechtigter Nutzer ausgeben, um unbefugten Zugriff zu erhalten.
- Datenlecks: Unverschlüsselte Kommunikation kann leicht abgefangen werden, insbesondere in öffentlichen WLAN-Netzen. Dadurch steigt die Gefahr, dass persönliche Informationen und Kreditkarteninformationen in die falschen Hände geraten.

SMB-Verschlüsselung

Voraussetzungen

- Erstellen Sie eine öffentliche Box. Richten Sie außerdem die Einstellung ein, mit der Dateien automatisch von der öffentlichen Box übertragen und im SMB-Ordner gespeichert werden.
- Geben Sie das Kennwort für die Relais-Box an.

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Box] - [User Box List] (Boxliste)

Einstellungselement	Empfohlene Einstellung
[SMB-Kommunikationsverschlüssel.]	[Verschl.]

SMB-Signatur

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [SMB Setting] (SMB-Einstellung) - [SMB Server Settings] (SMB-Servereinstellungen)

Einstellungselement	Empfohlene Einstellung
[SMB security Signature Setting] (Einstellung für SMB-Sicherheitssignatur)	[Erforderlich]

2.2.2 SMBClient

Die Kerberos-Authentifizierung verwendet eine starke Verschlüsselungstechnologie, mit der die Gefahr, dass Anmeldedaten während des Authentifizierungsvorgangs gestohlen werden, signifikant verringert wird. Sie stellt außerdem die Datenintegrität sicher, verhindert die Manipulation von Daten zwischen Absender und Empfänger und schützt vor NTLM-Relay-Angriffen.

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [SMB Setting] (SMB-Einstellung) - [Client Setting] (Client-Einstellung)

Einstellungselement	Empfohlene Einstellung
[SMB-Authentifizierungseinstellung]	[Kerberos]

2.2.3 SNMP

Legen Sie die Verschlüsselung mit SNMPv3 fest. Wenn zusätzlich die Authentifizierungseinstellung hinzugefügt wird, können Sie die Sicherheit noch weiter erhöhen. Die Sicherheitsrisiken sind mit denen von SMB vergleichbar.

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [SNMP Setting] (SNMP-Einstellung)

Einstellungselement	Empfohlene Einstellung
[SNMP Setting] (SNMP-Einstellung)	[SNMP v3(IP)]
[Encryption Algorithm] (Verschlüsselungsalgorithmus)	[AES-128]
[Authentication Method] (Authentifizierungsverfahren)	Wählen Sie [SHA-256], [SHA-384] oder [SHA-512].

2.2.4 IPsec

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [TCP/IP Setting] (TCP/IP-Einstellung) - [IPsec] - [IPsec Setting] (IPsec-Einstellung)

[IKEv2]

Einstellungselement	Empfohlene Einstellung
[Encryption Algorithm] (Verschlüsselungsalgorithmus)	[AES-CBC] ([256]/[192 und 256]/[Alle])
[Authentication Algorithm] (Authentifizierungsalgorithmus)	[SHA-2] ([256]/[384]/[512]/[256 und 384]/[384 und 512]/[Alle]), [AES-XCBC]
[Diffie-Hellman-Gruppe]	[Group 14] (Gruppe 14), [Group 19] (Gruppe 19)

[SA]

Einstellungselement	Empfohlene Einstellung
[Kapselungsmodus]	[Tunnel], [Transport]
[Sicherheitsprotokoll]	[ESP]
[Key Exchange Method] (Methode für den Schlüsselaustausch)	[IKEv2]
[Authentication Method] (Authentifizierungsverfahren)	[Digitale Signatur]
[ESP Encryption Algorithm] (ESP-Verschlüsselungsalgorithmus)	[AES-GCM] ([256]/[192 und 256]/[Alle]), [AES-GCM-64] ([256]/[192 und 256]/[Alle]), [ENC_NULL_AES_GMAC] ([256]/[192 und 256]/[Alle])

Einstellungselement	Empfohlene Einstellung
[Perfect Forward Secrecy]	ON (EIN)
[Diffie-Hellman Group(IKEv2)] (Diffie-Hellman-Gruppe [IKEv2]) - [Priority1-4] (Priorität 1-4)	[Group 14] (Gruppe 14), [Group 19] (Gruppe 19)

2.2.5 S/MIME

Wenn Sie beim E-Mail-Versand die optionale S/MIME-Funktion verwenden, können Sie den Inhalt der E-Mail verschlüsseln, um ein Mitlesen durch Dritte zu verhindern und die Identität des Absenders mit einer elektronischen Signatur zu verifizieren. Das ist eine wirkungsvolle Maßnahme gegen Spoofing und Phishing-Betrug.

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [E-mail Setting] (E-Mail-Einstellung) - [S/MIME]

Einstellungselement	Empfohlene Einstellung
[Digitale Signatur]	[Always add signature] (Immer unterzeichnen)
[Typ der digitalen Signatur]	[SHA-256]
[E-Mail-Text-Verschlüss.methode]	[AES-256]

3 Einrichten der Zertifikatvalidierung

Wenn Sie die TLS-verschlüsselte Kommunikation verwenden, um die Auswirkungen von Man-In-The-Middle-Angriffen zu verringern, empfehlen wir die Nutzung der Zertifikatvalidierung. Im Hinblick auf die Validierungselemente empfehlen wir als Mindestanforderung, das Zertifikatsablaufdatum und die Zertifikatskette zu aktivieren.

Wenn versucht wird, eine Verbindung zu einer Legacy-Umgebung herzustellen, die keine Funktion für die Zertifikatvalidierung bietet, steigt die Gefahr von Man-In-The-Middle-Angriffen. Wir empfehlen die Verwendung in einer sicheren Netzwerkumgebung.

Die Zertifikatvalidierung auf der MFP-Seite wird für die folgenden MFP-Client-Funktionen empfohlen. Ausführliche Informationen zum Aufrufen der Einstellungselemente finden Sie in den folgenden Abschnitten. POP, SMTP (Start TLS/SMTP over SSL), IEEE802.1X Auth (EAP-TYP: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel

Tipps

Die Zertifikatvalidierung auf der Seite des mit dem MFP verbundenen Clients wird für die folgenden MFP-Serverfunktionen empfohlen.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP-Socket

3.1 POP

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [E-mail Setting] (E-Mail-Einstellung) - [E-mail RX (POP)] (E-Mail-Empfang [POP])

Einstellungselement	Empfohlene Einstellung
[Zertifikatverifizierungseinstellungen]	[Expiration Date] (Ablaufdatum): ON (EIN) [Kette]: ON (EIN)

3.2 SMTP

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [E-mail Setting] (E-Mail-Einstellung) - [E-mail TX (SMTP)] (E-Mail-Übertragung [SMTP])

Einstellungselement	Empfohlene Einstellung
[Zertifikatverifizierungseinstellungen]	[Expiration Date] (Ablaufdatum): ON (EIN) [Kette]: ON (EIN)

3.3 IEEE802.1X-Auth.

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [IEEE802.1X Authentication Setting] (IEEE802.1X-Authentifizierungseinstellung) - [IEEE802.1X Authentication Setting] (IEEE802.1X-Authentifizierungseinstellung) - [Supplicant Setting] (Antragsteller-Einstellung)

Einstellungselement	Empfohlene Einstellung
[Zertifikatverifizierungseinstellungen]	[Expiration Date] (Ablaufdatum): ON (EIN) [Kette]: ON (EIN)

3.4 IPsec

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [TCP/IP Setting] (TCP/IP-Einstellung) - [IPsec] - [Enable IPsec] (IPsec aktivieren)

Einstellungselement	Empfohlene Einstellung
[Zertifikatverifizierungseinstellungen]	[Expiration Date] (Ablaufdatum): [Confirm] (Bestätigen) [Kette]: [Confirm] (Bestätigen)



Tipps

Registrieren Sie unter [IPsec Setting] (IPsec-Einstellung) vorab die Elemente [IKE], [SA], [Peer] und [Protocol Setting] (Protokolleinstellung).

3.5 WebDAVClient

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [WebDAV Settings] (WebDAV-Einstellungen) - [WebDAV Client Settings] (WebDAV-Client-Einstellungen)

Einstellungselement	Empfohlene Einstellung
[Zertifikatverifizierungseinstellungen]	[Expiration Date] (Ablaufdatum): ON (EIN) [Kette]: ON (EIN)

3.6 LDAP

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [LDAP Setting] (LDAP-Einstellung) - [Setting Up LDAP] (LDAP einrichten)

Einstellungselement	Empfohlene Einstellung
[Zertifikatverifizierungseinstellungen]	[Expiration Date] (Ablaufdatum): ON (EIN) [Kette]: ON (EIN)

3.7 DPWS

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [DPWS Settings] (DPWS-Einstellungen) - [DPWS Common Settings] (Allgemeine DPWS-Einstellungen)

Einstellungselement	Empfohlene Einstellung
[Zertifikatverifizierungseinstellungen]	[Expiration Date] (Ablaufdatum): ON (EIN) [Kette]: ON (EIN)

3.8 OpenAPI

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [OpenAPI Setting] (OpenAPI-Einstellung) - [OpenAPI Setting] (OpenAPI-Einstellung)

Einstellungselement	Empfohlene Einstellung
[Zertifikatverifizierungseinstellungen]	[Expiration Date] (Ablaufdatum): ON (EIN) [Kette]: ON (EIN)

3.9 RemotePanel

Aufrufen der Einstellung: [Utility] (Bedienerprogramm) - [Administrator] - [Network] (Netzwerk) - [Remote Panel Settings] (Remote Panel-Einstellungen) - [Remote Panel Client Settings] (Remote Panel-Client-Einstellungen)

Einstellungselement	Empfohlene Einstellung
[Zertifikatverifizierungseinstellungen]	[Expiration Date] (Ablaufdatum): ON (EIN) [Kette]: ON (EIN)

4 Zusätzliche Sicherheitsinformationen

4.1 Empfehlung für bewährte Verfahren

Wir empfehlen, einen Verschlüsselungsalgorithmus zu verwenden, der den Best-Practice-Einstellungen entspricht, die in den EUCC Guidelines on Cryptography und in den SOGIS-Agreed-Cryptographic-Mechanisms empfohlen werden.

Im Folgenden finden Sie eine Liste der Verschlüsselungsalgorithmen und der Schlüssellängen, die in den EUCC Guidelines on Cryptography und in den SOGIS-Agreed-Cryptographic-Mechanisms empfohlen werden.

Funktion	Empfohlene Einstellung
Verschlüsselungsalgorithmen	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Schlüssellänge	RSA: 2048 Bit oder mehr ECC: 256 Bit oder mehr AES: 256 Bit

Tipps

Ausführliche Informationen finden Sie in den aktuellen EUCC Guidelines on Cryptography und SOGIS-Agreed-Cryptographic-Mechanisms.

4.2 Hinweise zur Kommunikation mit Legacy-Systemen

Die folgenden Protokolle und Versionen werden vorzugsweise für die Kommunikation mit Legacy-Systemen verwendet.

Die Verwendung von Legacy-Einstellungen ist mit höheren Sicherheitsrisiken verbunden. Verwenden Sie sie daher in einer sicheren Netzwerkkumgebung.

Funktion	Legacy-Einstellungen
Protokoll	SLP FTP SMB (3.0 oder frühere Version, NTLMv1/v2) SNMPv1/v2 IEEE802.1X-Auth. (EAP-TYP: Serverabhängig/AUS) DPWS TCPSocket
Verschlüsselungs- algorithmen	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Schlüssellänge	RSA: 1024 Bit oder weniger ECC: 160 Bit oder weniger AES: 128 Bit oder weniger DES: 56 Bit 3DES: 112 Bit

Legacy-IPsec-Einstellungen

[IKEv1]

Einstellungselement	Legacy-Einstellungen
[Encryption Algorithm] (Verschlüsselungs- algorithmus)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 und 192])
[Authentication Algorithm] (Authentifizierungs- algorithmus)	Nicht verwendet
[Diffie-Hellman-Gruppe]	[Group 1] (Gruppe 1), [Group 2] (Gruppe 2), [Group 5] (Gruppe 5)

[IKEv2]

Einstellungselement	Legacy-Einstellungen
[Encryption Algorithm] (Verschlüsselungs- algorithmus)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 und 192])
[Authentication Algorithm] (Authentifizierungs- algorithmus)	Nicht verwendet
[Diffie-Hellman-Gruppe]	[Group 1] (Gruppe 1), [Group 2] (Gruppe 2), [Group 5] (Gruppe 5)

[SA]

Einstellungselement	Legacy-Einstellungen
[Key Exchange Method] (Methode für den Schlüsselaustausch)	[IKEv1]
[Authentication Method] (Authentifizierungsverfahren)	[Digitale Signatur]

Einstellungselement	Legacy-Einstellungen
[ESP Encryption Algorithm] (ESP-Verschlüsselungs- algorithmus)	[3DES-CBC] ([128]/[192]/[128 und 192]) [AES-CTR] ([128]/[192]/[128 und 192]) [AES-GCM] ([128]/[192]/[128 und 192]) [AES-GCM-64] ([128]/[192]/[128 und 192]) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 und 192])
[Perfect Forward Secrecy]	ON (EIN)
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellman-Gruppe (IKEv1))	[Group 1] (Gruppe 1), [Group 2] (Gruppe 2), [Group 5] (Gruppe 5)

4.3 Werksseitig verfügbare Netzwerkschnittstellen und -dienste

Diensttyp	Protokoll	Portnummer
DHCP	UDP	68
HTTP Server	TCP	80
NETBIOS Name Service	UDP	137
NETBIOS Datagram Service	UDP	138
SNMP	UDP	161
HTTP Server over SSL / IPP over SSL	TCP	443
LPD Print	TCP	515
DHCPv6 Client	UDP	546
IPP Print	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-tool)	TCP	8091
RAW Print	TCP	9100
RAW Print	TCP	9112
RAW Print	TCP	9113
RAW Print	TCP	9114
RAW Print	TCP	9115
RAW Print	TCP	9116
OpenAPI	TCP	50001

4.4 Informationen zur Eingabevalidierung

Angaben zur Anzahl der Zeichen, die für die Netzwerkeinstellungen usw. eingegeben werden müssen, finden Sie unter den einzelnen Einstellungselementen in der Bedienungsanleitung.

In Abhängigkeit von der Kodierung der Sprache kann die maximal zulässige Eingabe (im MFP gespeicherte Daten) für Elemente, die Multibyte-Zeichen unterstützen, das Dreifache der Anzahl der Zeichen betragen.

Recommandations pour les périphériques sécurisés en réseau



Table des matières

1 Définition du filtrage IP

1.1	Filtrage IP.....	3
1.2	Filtrage IP rapide.....	3

2 Configuration de la communication cryptée

2.1	Cryptage TLS.....	4
2.1.1	HTTP (Web Connection)	4
2.1.2	WebDAVServer	4
2.1.3	IPP.....	5
2.1.4	OpenAPI.....	5
2.1.5	RemotePanel.....	5
2.1.6	DPWS.....	5
2.1.7	POP.....	5
2.1.8	SMTP	5
2.1.9	Authentification IEEE802.1X	6
2.1.10	LDAP	6
2.1.11	Port TCP	6
2.2	Autre cryptage.....	7
2.2.1	SMBServer	7
	Cryptage SMB	7
	Signature du protocole SMB	7
2.2.2	SMBClient	8
2.2.3	SNMP	8
2.2.4	IPsec	8
2.2.5	S/MIME	9

3 Configuration de la validation de certificat

3.1	POP.....	10
3.2	SMTP.....	10
3.3	Authentification IEEE802.1X.....	10
3.4	IPsec.....	11
3.5	WebDAVClient	11
3.6	LDAP.....	11
3.7	DPWS	11
3.8	OpenAPI	11
3.9	RemotePanel	12

4 Informations de sécurité additionnelles

4.1	Recommandation relative aux meilleures pratiques	13
4.2	Précautions à prendre lors de la communication avec des systèmes existants.....	14
	Paramètres IPsec existants	14
4.3	Interfaces réseau et services disponibles depuis l'expédition de l'usine	16
4.4	À propos de la validation de la saisie.....	17



À propos de ce manuel

Le présent manuel décrit les informations et les paramètres permettant une utilisation sûre des périphériques.

Lorsque vous connectez l'unité principale au réseau, utilisez-la dans un environnement protégé par un pare-feu. Nous vous recommandons également de définir une adresse IP privée pour l'adresse IP de l'unité principale.

La configuration d'une adresse IP privée permet uniquement aux utilisateurs d'un réseau local, tel qu'un réseau local interne, d'accéder à l'unité principale, empêchant ainsi tout accès non autorisé depuis l'extérieur.

Si vous devez utiliser une adresse IP mondiale, veillez à installer l'unité principale dans un pare-feu.

1 Définition du filtrage IP

Filtrage IP est une fonction qui restreint les périphériques qui peuvent accéder à l'unité principale en fonction de l'adresse IP. En définissant correctement cette fonction, vous pouvez restreindre l'accès aux périphériques non autorisés.

La fonction Filtrage IP de l'unité principale peut être définie par les deux méthodes suivantes.

1.1 Filtrage IP

Spécifiez manuellement la plage d'adresses IP qui autorisent ou refusent l'accès.

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [TCP/IP Setting] (Configuration TCP/IP) - [IP Address Filtering] (Filtrage IP)



Définissez les adresses IP à autoriser ou à refuser en fonction de votre environnement.

1.2 Filtrage IP rapide

La plage d'adresses IP autorisant l'accès est définie automatiquement en fonction de l'adresse IP et du masque de sous-réseau définis dans l'unité principale.

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [TCP/IP Setting] (Configuration TCP/IP) - [Quick IP Filtering] (Filtrage rapide IP)

Configuration recommandée : [Synchronize IP Address] (Synchroniser adresse IP)/[Synchronize Subnet Mask] (Synchroniser masque de sous-réseau) *

* Sélectionnez l'une de ces options en fonction de votre environnement.

2 Configuration de la communication cryptée

Nous vous recommandons d'utiliser la communication cryptée suivante afin d'éviter toute interception non autorisée ou falsification des données et tout détournement de session.

2.1 Cryptage TLS

Nous vous recommandons de configurer les paramètres suivants afin de réduire le risque de vulnérabilités.

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Security] (Sécurité) - [PKI Settings] (Paramètres PKI) - [Enable SSL Version] (Activer version SSL)

Élément de configuration	Paramètre recommandé
[Mode utilisant SSL/TLS]	[Admin. Mode and User Mode] (Mode administrateur et Mode utilisateur)
[SSL/TLS Version Setting] (Réglage de la version SSL/TLS)	TLS1.2 TLS1.3 (incompatible avec IEEE802.1X)
[Encryption Strength] (Force chiffrem.)	AES-256

Le certificat initial est installé en usine. S'il vous faut un certificat différent, enregistrez-en un nouveau à l'emplacement suivant.

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Security] (Sécurité) - [PKI Settings] (Paramètres PKI) - [Device Certificate Setting] (Config. certificat périphérique)

Élément de configuration	Paramètre recommandé
[Encryption Key Type] (Type clé de cryptage)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Le cryptage TLS est pris en charge pour les protocoles et services suivants. Pour plus de détails sur les emplacements des paramètres, reportez-vous aux sections suivantes.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Démarrer TLS, SMTP sur SSL)
- Authentification IEEE802.1X (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- Port TCP

2.1.1 HTTP (Web Connection)

Si vous activez [Enable SSL Version] (Activer version SSL), le mode de communication passe automatiquement à la communication à cryptage TLS (HTTPS).

2.1.2 WebDAVServer

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [WebDAV Settings] (Configuration WebDAV) - [WebDAV Server Settings] (Configuration serveur WebDAV)

Élément de configuration	Paramètre recommandé
[Paramètres SSL]	[SSL seulement]

2.1.3 IPP

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [HTTP Server Settings] (Configuration serveur HTTP)

Élément de configuration	Paramètre recommandé
[Paramètres IPP-SSL]	[SSL seulement]

2.1.4 OpenAPI

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [OpenAPI Setting] (Configuration OpenAPI) - [OpenAPI Setting] (Configuration OpenAPI)

Élément de configuration	Paramètre recommandé
[Configuration SSL/port]	[SSL seulement]

2.1.5 RemotePanel

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [Remote Panel Settings] (Config. panneau distant) - [Remote Panel Server Settings] (Configuration serveur panneau distant)

Élément de configuration	Paramètre recommandé
[Port No.(SSL)] (Numéro de port (SSL))	[50443]



Tips

Si vous activez [Enable SSL Version] (Activer version SSL), la communication passe automatiquement au mode de cryptage TLS. Précisez un numéro de port.

2.1.6 DPWS

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [DPWS Settings] (Configuration DPWS) - [DPWS Common Settings] (Configuration générale DPWS)

Élément de configuration	Paramètre recommandé
[Paramètres SSL]	OUI

2.1.7 POP

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [E-mail Setting] (Configuration e-mail) - [E-mail RX (POP)] (Réception e-mail [POP])

Élément de configuration	Paramètre recommandé
[Activer SSL]	OUI

2.1.8 SMTP

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [E-mail Setting] (Configuration e-mail) - [E-mail TX (SMTP)] (Transmission par e-mail [SMTP])

Élément de configuration	Paramètre recommandé
[Réglages SSL/TLS]	[SMTP sur SSL]

2.1.9 Authentification IEEE802.1X

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [IEEE802.1X Authentication Setting] (Configuration authentification IEEE802.1X) - [IEEE802.1X Authentication Setting] (Configuration authentification IEEE802.1X) - [Supplicant Setting] (Configuration du supplicant)

Élément de configuration	Paramètre recommandé
[Type EAP]	Sélectionnez [EAP-TLS], [EAP-TTLS], ou [PEAP].

2.1.10 LDAP

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [LDAP Setting] (Configuration LDAP) - [Setting Up LDAP] (Configurer LDAP)

Élément de configuration	Paramètre recommandé
[Activer SSL]	OUI

2.1.11 Port TCP

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [TCP Socket Setting] (Configuration port TCP)

Élément de configuration	Paramètre recommandé
[Use SSL/TLS] (Utiliser SSL/TLS)	OUI

2.2 Autre cryptage

Nous vous recommandons de configurer les paramètres suivants afin de réduire le risque de vulnérabilités. Pour plus de détails sur la configuration de chaque fonction, reportez-vous aux sections suivantes.

Fonction	Paramètre recommandé
SMBServer	Cryptage SMB, signature du protocole SMB
SMBClient	Authentification Kerberos
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	OUI

2.2.1 SMBServer

L'utilisation du cryptage SMB et de la signature du protocole SMB peut réduire les risques de sécurité suivants.

- Interception non autorisée : Un tiers malveillant peut intercepter les communications et voler des informations personnelles ou confidentielles.
- Falsification des données : Le contenu des communications risque d'être altéré par une attaque par interception (MITM).
- Usurpation : En cas de vol d'informations d'authentification, un tiers peut se faire passer pour un utilisateur légitime afin d'obtenir un accès non autorisé.
- Fuite d'informations : Les communications non cryptées peuvent être facilement interceptées, en particulier sur les réseaux Wi-Fi publics, ce qui augmente le risque de fuite d'informations à caractère personnel et de données de carte de crédit.

Cryptage SMB

Conditions préalables

- Créez une boîte utilisateur publique. Configurez également le paramètre pour transférer automatiquement les fichiers depuis la boîte utilisateur publique et les enregistrer dans le dossier SMB.
- Indiquez le mot de passe pour la Boîte utilisateur.

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Box] (Boîte) - [User Box List] (Liste des boîtes utilisateur)

Élément de configuration	Paramètre recommandé
[Cryptage de communication SMB]	[Encrypt] (Cryptage)

Signature du protocole SMB

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [SMB Setting] (Configuration SMB) - [SMB Server Settings] (Configuration Serveur SMB)

Élément de configuration	Paramètre recommandé
[SMB security Signature Setting] (Configuration de signature sécurité SMB)	[Obligatoire]

2.2.2 SMBClient

L'authentification Kerberos utilise une technologie de cryptage puissante, réduisant considérablement le risque de vol des identifiants lors du processus d'authentification. Elle garantit également l'intégrité des données, en empêchant toute falsification des données entre l'expéditeur et le destinataire, ainsi que les attaques par relais NTLM.

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [SMB Setting] (Configuration SMB) - [Client Setting] (Configuration client)

Élément de configuration	Paramètre recommandé
[Paramétrage authentification SMB]	[Kerberos]

2.2.3 SNMP

Configurez le cryptage au moyen de SNMPv3. Si le paramètre d'authentification est également ajouté, vous pouvez encore renforcer la sécurité. Les risques de sécurité sont à peu près les mêmes qu'avec le protocole SMB.

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [SNMP Setting] (Configuration SNMP)

Élément de configuration	Paramètre recommandé
[Configuration SNMP]	[SNMP v3(IP)]
[Algorithme encryptage]	[AES-128]
[Authentication Method] (Méthode d'authentification)	Sélectionnez [SHA-256], [SHA-384], ou [SHA-512].

2.2.4 IPsec

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [TCP/IP Setting] (Configuration TCP/IP) - [IPsec] (IPsec) - [IPsec Setting] (Configuration IPsec)

[IKEv2]

Élément de configuration	Paramètre recommandé
[Algorithme encryptage]	[AES-CBC] ([256]/[192 et 256]/[All] (Tout))
[Algorith. identification]	[SHA-2] ([256]/[384]/[512]/[256 et 384]/[384 et 512]/[All] (Tout)), [AES-XCBC]
[Groupe Diffie-Hellman]	[Group 14] (Groupe 14), [Group 19] (Groupe 19)

[SA]

Élément de configuration	Paramètre recommandé
[Mode encapsulation]	[Tunnel] (Tunnel), [Transport] (Transport)
[Protocole de sécurité]	[ESP]
[Key Exchange Method] (Méthode échange clé)	[IKEv2]
[Authentication Method] (Méthode d'authentification)	[Signature numérique]
[Algorithme encryptageESP]	[AES-GCM] ([256]/[192 et 256]/[All] (Tout)), [AES-GCM-64] ([256]/[192 et 256]/[All] (Tout)), [ENC_NULL_AES_GMAC] ([256]/[192 et 256]/[All] (Tout))
[Perfect Forward Secrecy]	OUI
[Diffie-Hellman Group(IKEv2)] (Groupe Diffie-Hellman [IKEv2]) - [Priority1-4] (Priorité 1-4)	[Group 14] (Groupe 14), [Group 19] (Groupe 19)

2.2.5 S/MIME

Si vous utilisez l'option S/MIME lors de l'envoi d'e-mails, vous pouvez crypter le contenu des e-mails afin d'empêcher toute interception non autorisée et vérifier l'identité de l'expéditeur à l'aide d'une signature électronique. Il s'agit d'une mesure efficace contre les tentatives d'usurpation et d'hameçonnage.

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [E-mail Setting] (Configuration e-mail) - [S/MIME (S/MIME)]

Élément de configuration	Paramètre recommandé
[Signature numérique]	[Toujours signer]
[Type de signature numérique]	[SHA-256]
[Méthode cryptage Texte E-mail]	[AES-256]

3 Configuration de la validation de certificat

Lorsque vous utilisez la communication à cryptage TLS pour réduire l'impact des attaques par interception, nous vous recommandons d'utiliser la validation de certificat. Pour les éléments de validation, nous vous recommandons d'activer au moins la date d'expiration du certificat et la chaîne.

Si une tentative de connexion à un environnement existant ne disposant pas d'une fonction de validation de certificat est effectuée, le risque d'attaques par interception augmente. Nous vous recommandons de l'utiliser dans un environnement réseau sécurisé.

La validation du certificat côté MFP est recommandée dans les fonctions client suivantes de la MFP. Pour plus de détails sur les emplacements des paramètres, reportez-vous aux sections suivantes.

POP, SMTP (Démarrer TLS/SMTP sur SSL), Authentification IEEE802.1X (TYPE EAP : EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel



Tips

La validation du certificat côté client connecté à la MFP est recommandée dans les fonctions suivantes du serveur MFP.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), port TCP

3.1 POP

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [E-mail Setting] (Configuration e-mail) - [E-mail RX (POP)] (Réception e-mail [POP])

Élément de configuration	Paramètre recommandé
[Réglages Niveau Vérification Certificat]	[Expiration Date] (Date d'expiration) : OUI [Chaîne] : OUI

3.2 SMTP

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [E-mail Setting] (Configuration e-mail) - [E-mail TX (SMTP)] (Transmission par e-mail [SMTP])

Élément de configuration	Paramètre recommandé
[Réglages Niveau Vérification Certificat]	[Expiration Date] (Date d'expiration) : OUI [Chaîne] : OUI

3.3 Authentification IEEE802.1X

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [IEEE802.1X Authentication Setting] (Configuration authentification IEEE802.1X) - [IEEE802.1X Authentication Setting] (Configuration authentification IEEE802.1X) - [Supplicant Setting] (Configuration du supplicant)

Élément de configuration	Paramètre recommandé
[Réglages Niveau Vérification Certificat]	[Expiration Date] (Date d'expiration) : OUI [Chaîne] : OUI

3.4 IPsec

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [TCP/IP Setting] (Configuration TCP/IP) - [IPsec] (IPsec) - [Enable IPsec] (Activer IPsec)

Élément de configuration	Paramètre recommandé
[Réglages Niveau Vérification Certificat]	[Expiration Date] (Date d'expiration) : [Confirm] (Confirmer) [Chaîne] : [Confirm] (Confirmer)



Tips

Dans [IPsec Setting] (Configuration IPsec), enregistrez les éléments [IKE], [SA], [Peer] (Pair), et [Protocol Setting] (Configuration de protocole) au préalable.

3.5 WebDAVClient

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [WebDAV Settings] (Configuration WebDAV) - [WebDAV Client Settings] (Configuration client WebDAV)

Élément de configuration	Paramètre recommandé
[Réglages Niveau Vérification Certificat]	[Expiration Date] (Date d'expiration) : OUI [Chaîne] : OUI

3.6 LDAP

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [LDAP Setting] (Configuration LDAP) - [Setting Up LDAP] (Configurer LDAP)

Élément de configuration	Paramètre recommandé
[Réglages Niveau Vérification Certificat]	[Expiration Date] (Date d'expiration) : OUI [Chaîne] : OUI

3.7 DPWS

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [DPWS Settings] (Configuration DPWS) - [DPWS Common Settings] (Configuration générale DPWS)

Élément de configuration	Paramètre recommandé
[Réglages Niveau Vérification Certificat]	[Expiration Date] (Date d'expiration) : OUI [Chaîne] : OUI

3.8 OpenAPI

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [OpenAPI Setting] (Configuration OpenAPI) - [OpenAPI Setting] (Configuration OpenAPI)

Élément de configuration	Paramètre recommandé
[Réglages Niveau Vérification Certificat]	[Expiration Date] (Date d'expiration) : OUI [Chaîne] : OUI

3.9 RemotePanel

Emplacement du paramètre : [Utility] (Utilitaire) - [Administrator] (Administrateur) - [Network] (Réseau) - [Remote Panel Settings] (Config. panneau distant) - [Remote Panel Client Settings] (Configuration client panneau distant)

Élément de configuration	Paramètre recommandé
[Réglages Niveau Vérification Certificat]	[Expiration Date] (Date d'expiration) : OUI [Chaîne] : OUI

4 Informations de sécurité additionnelles

4.1 Recommandation relative aux meilleures pratiques

Selon nos recommandations, les algorithmes de cryptage utilisés doivent être conformes aux meilleures pratiques recommandées dans les lignes directrices de l'EUCC sur la cryptographie et les mécanismes cryptographiques approuvés par le SOG-IS.

Vous trouverez ci-dessous une liste des algorithmes de cryptage et des longueurs de clé recommandés par les lignes directrices de l'EUCC en matière de cryptographie et les mécanismes cryptographiques approuvés par le SOG-IS.

Élément	Paramètre recommandé
Algorithmes de cryptage	AES (Advanced Encryption Standard [norme de cryptage avancée]) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2 [algorithme de hachage de sécurité 2]) ECC (Elliptic Curve Cryptography [cryptographie sur les courbes elliptiques]) HMAC (Hash-based Message Authentication Code [code d'authentification de message haché])
Longueur de la clé de cryptage	RSA : 2048 bits ou plus ECC : 256 bits ou plus AES : 256 bits

Tips

Pour plus de détails, reportez-vous aux dernières lignes directrices de l'EUCC sur la cryptographie et aux mécanismes cryptographiques approuvés par le SOG-IS.

4.2 Précautions à prendre lors de la communication avec des systèmes existants

Les protocoles et versions suivants sont supposés être utilisés pour la communication avec les systèmes existants.

L'utilisation des paramètres existants augmente les risques liés à la sécurité. Veuillez donc les utiliser dans un environnement réseau sécurisé.

Élément	Paramètres existants
Protocole	SLP FTP SMB (3.0 ou version antérieure, NTLMv1/v2) SNMPv1/v2 Authentification IEEE802.1X (TYPE EAP : Dépend du serveur/Désactivé) DPWS Port TCP
Algorithmes de cryptage	SHA-1 (Secure Hash Algorithm 1 [algorithme de hachage de sécurité 1]) DES (Data Encryption Standard [norme de cryptage de données]) 3DES (Triple Data Encryption Standard [Triple norme de cryptage des données]) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Longueur de la clé de cryptage	RSA : 1024 bits ou moins ECC : 160 bits ou moins AES : 128 bits ou moins DES : 56 bits 3DES : 112 bits

Paramètres IPsec existants

[IKEv1]

Élément de configuration	Paramètres existants
[Algorithme encryptage]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 et 192])
[Algorith. identification]	Non utilisé
[Groupe Diffie-Hellman]	[Group 1] (Groupe 1), [Group 2] (Groupe 2), [Group 5] (Groupe 5)

[IKEv2]

Élément de configuration	Paramètres existants
[Algorithme encryptage]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 et 192])
[Algorith. identification]	Non utilisé
[Groupe Diffie-Hellman]	[Group 1] (Groupe 1), [Group 2] (Groupe 2), [Group 5] (Groupe 5)

[SA]

Élément de configuration	Paramètres existants
[Key Exchange Method] (Méthode échange clé)	[IKEv1]
[Authentication Method] (Méthode d'authentification)	[Signature numérique]

Élément de configuration	Paramètres existants
[Algorithme encryptageESP]	[3DES-CBC] ([128]/[192]/[128 et 192]) [AES-CTR] ([128]/[192]/[128 et 192]) [AES-GCM] ([128]/[192]/[128 et 192]) [AES-GCM-64] ([128]/[192]/[128 et 192]) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 et 192])
[Perfect Forward Secrecy]	OUI
[Diffie-Hellman Group(IKEv1)] (Groupe Diffie-Hellman [IKEv1])	[Group 1] (Groupe 1), [Group 2] (Groupe 2), [Group 5] (Groupe 5)

4.3 Interfaces réseau et services disponibles depuis l'expédition de l'usine

Type de service	Protocole	Numéro de port
DHCP	UDP	68
Serveur HTTP	TCP	80
Service nom NetBIOS	UDP	137
NetBIOS Datagram Service	UDP	138
SNMP	UDP	161
Serveur HTTP sur SSL / IPP sur SSL	TCP	443
Impression LPD	TCP	515
Client DHCPv6	UDP	546
Impression IPP	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (outil IWS)	TCP	8091
Impression RAW	TCP	9100
Impression RAW	TCP	9112
Impression RAW	TCP	9113
Impression RAW	TCP	9114
Impression RAW	TCP	9115
Impression RAW	TCP	9116
OpenAPI	TCP	50001

4.4 À propos de la validation de la saisie

Pour connaître le nombre de caractères à saisir pour la configuration réseau, etc., reportez-vous à chacun des éléments de configuration dans le Guide de l'utilisateur.

Selon le codage de la langue, la quantité maximale autorisée (données enregistrées dans la MFP) pour les éléments prenant en charge les caractères multioctets peut être trois fois supérieure au nombre de caractères.

Recomendaciones para proteger los dispositivos conectados en red

Contenido

1 Ajuste del filtrado de IP

1.1	Filtrado de IP	1-3
1.2	Filtrado de IP rápido	1-3

2 Configuración de comunicación cifrada

2.1	Cifrado TLS.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	Panel remoto.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	Aut. IEEE802.1X.....	2-6
2.1.10	LDAP	2-6
2.1.11	Socket TCP.....	2-6
2.2	Otro cifrado	2-7
2.2.1	Servidor SMB.....	2-7
	Cifrado SMB	2-7
	Firma de protocolo SMB.....	2-7
2.2.2	Cliente SMB.....	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Configuración de la validación de certificados

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	Aut. IEEE802.1X.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	Panel remoto	3-12

4 Información adicional de seguridad

4.1	Recomendación de mejores prácticas	4-13
4.2	Precauciones para la comunicación con sistemas heredados.....	4-14
	Configuración IPsec heredada.....	4-14
4.3	Interfaces y servicios de red disponibles desde fábrica.....	4-16
4.4	Acercas de la validación de entradas	4-17



Acerca de este manual

Este manual describe la información y los ajustes que permiten un uso seguro de los dispositivos.

Si conecta la máquina a la red, utilícela en un entorno protegido mediante firewall. También recomendamos configurar una dirección de IP privada para la dirección IP de la máquina.

Si se configura una dirección IP privada, solo pueden acceder a la máquina los usuarios de una red de área local, como por ejemplo una LAN interna, lo que impide el acceso no autorizado desde el exterior.

Si debe utilizar una dirección IP global, asegúrese de instalar la máquina en un firewall.

1 Ajuste del filtrado de IP

El filtrado de IP es una función que permite restringir los dispositivos que pueden acceder a la máquina con la dirección IP. Si se define correctamente esta función, es posible restringir el acceso desde dispositivos no autorizados.

La función de filtrado de IP de la máquina se puede definir por cualquiera de estos dos métodos.

1.1 Filtrado de IP

Especifique manualmente el rango de direcciones IP que permiten o deniegan el acceso.

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [TCP/IP Setting] (Configuración de TCP/IP) - [IP Address Filtering] (Filtrado de IP)



Sugerencias

Configure las direcciones IP permitidas o denegadas para adaptarlas a su entorno.

1.2 Filtrado de IP rápido

El rango de direcciones IP para permitir el acceso se define automáticamente según la dirección IP y la máscara de subred asignada a la máquina.

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [TCP/IP Setting] (Configuración de TCP/IP) - [Quick IP Filtering] (Filtrado de IP rápido)

Configuración recomendada: [Synchronize IP Address] (Sincronizar dirección de IP)/[Synchronize Subnet Mask] (Sincronizar máscara de subred)*

* Seleccione una de las dos para ajustarse a su entorno.

2 Configuración de comunicación cifrada

Le recomendamos que utilice la siguiente comunicación cifrada para evitar la escucha de datos, la manipulación de datos y el secuestro de sesiones.

2.1 Cifrado TLS

Le recomendamos que configure los siguientes parámetros para reducir el riesgo de vulnerabilidades.

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Security] (Seguridad) - [PKI Settings] (Configuración PKI) - [Enable SSL Version] (Activar versión de SSL)

Elemento de ajuste	Configuración recomendada
[Modo usando SSL/TLS]	[Modo admin. y modo usuario]
[SSL/TLS Version Setting] (Configuración de versión SSL/TLS)	TLS1.2 TLS1.3 (IEEE802.1X incompatible)
[Encryption Strength] (Intensid.cifrado)	AES-256

El certificado inicial se instala en fábrica. Si necesita un certificado diferente, registre uno nuevo en la siguiente dirección.

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Security] (Seguridad) - [PKI Settings] (Configuración PKI) - [Device Certificate Setting] (Configuración de certificado de dispositivo)

Elemento de ajuste	Configuración recomendada
[Encryption Key Type] (Tipo clave de cifrado)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

El cifrado TLS es compatible con los siguientes protocolos y servicios. Para obtener más información sobre las ubicaciones de los ajustes, consulte las siguientes secciones.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Iniciar TLS, SMTP sobre SSL)
- Aut. IEEE802.1X (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- Socket TCP

2.1.1 HTTP (Web Connection)

Si se activa [Enable SSL Version] (Activar versión de SSL), el modo de comunicación cambia automáticamente al cifrado TLS (HTTPS).

2.1.2 WebDAVServer

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [WebDAV Settings] (Configuración de WebDAV) - [WebDAV Server Settings] (Configuración de servidor WebDAV)

Elemento de ajuste	Configuración recomendada
[Config. SSL]	[Solo SSL]

2.1.3 IPP

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [HTTP Server Settings] (Configuración de Servidor HTTP)

Elemento de ajuste	Configuración recomendada
[Config. IPP-SSL]	[Solo SSL]

2.1.4 OpenAPI

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [OpenAPI Setting] (Configuración de OpenAPI) - [OpenAPI Setting] (Configuración de OpenAPI)

Elemento de ajuste	Configuración recomendada
[Configuración de SSL/puerto]	[Solo SSL]

2.1.5 Panel remoto

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [Remote Panel Settings] (Configuración del panel remoto) - [Remote Panel Server Settings] (Configuración del servidor del panel remoto)

Elemento de ajuste	Configuración recomendada
[Port No.(SSL)] (Número de puerto[SSL])	[50443]



Sugerencias

Si se activa [Enable SSL Version] (Activar versión de SSL), el modo de comunicación cambia automáticamente al cifrado TLS. Especifique un número de puerto.

2.1.6 DPWS

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [DPWS Settings] (Configuración DPWS) - [DPWS Common Settings] (Configuración común DPWS)

Elemento de ajuste	Configuración recomendada
[Config. SSL]	ACT.

2.1.7 POP

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [E-mail Setting] (Configuración de correo electrónico) - [E-mail RX (POP)] (Recepción de correo electrónico [POP])

Elemento de ajuste	Configuración recomendada
[Habilitar SSL]	ACT.

2.1.8 SMTP

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [E-mail Setting] (Configuración de correo electrónico) - [E-mail TX (SMTP)] (Transmisión de correo [SMTP])

Elemento de ajuste	Configuración recomendada
[Configuración SSL/TLS]	[SMTP sobre SSL]

2.1.9 Aut. IEEE802.1X

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [IEEE802.1X Authentication Setting] (Configuración de autenticación de IEEE802.1X) - [IEEE802.1X Authentication Setting] (Configuración de autenticación de IEEE802.1X) - [Supplicant Setting] (Configuración de suplicante)

Elemento de ajuste	Configuración recomendada
[Tipo EAP]	Seleccione [EAP-TLS], [EAP-TTLS] o [PEAP].

2.1.10 LDAP

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [LDAP Setting] (Configuración de LDAP) - [Setting Up LDAP] (Configurar LDAP)

Elemento de ajuste	Configuración recomendada
[Habilitar SSL]	ACT.

2.1.11 Socket TCP

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [TCP Socket Setting] (Configuración de Socket TCP)

Elemento de ajuste	Configuración recomendada
[Use SSL/TLS] (Utilizar SSL/TLS)	ACT.

2.2 Otro cifrado

Le recomendamos que configure los siguientes parámetros para reducir el riesgo de vulnerabilidades. Para obtener más información sobre los ajustes de cada función, consulte las siguientes secciones.

Función	Configuración recomendada
Servidor SMB	Cifrado SMB, firma de protocolo SMB
Cliente SMB	Autenticación de Kerberos
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	ACT.

2.2.1 Servidor SMB

Si se usa el cifrado SMB y la firma de protocolo SMB, pueden reducirse los siguientes riesgos de seguridad.

- Escucha: un tercero malintencionado puede interceptar las comunicaciones y robar información personal o confidencial.
- Manipulación de datos: existe el riesgo de que el contenido de las comunicaciones sea manipulado por un ataque de intermediario (ataque "man-in-the-middle" o MITM).
- "Spoofing" o suplantación de identidad: si se roba la información de autenticación, un tercero puede hacerse pasar por un usuario legítimo para obtener acceso no autorizado.
- Filtración de información: las comunicaciones no cifradas pueden interceptarse fácilmente, especialmente en redes Wi-Fi públicas, lo que aumenta el riesgo de que se filtren datos personales e información sobre tarjetas de crédito.

Cifrado SMB

Requisitos previos

- Cree una carpeta de usuario pública. Asimismo, configure la opción para transferir automáticamente archivos de la carpeta de usuario pública y guardarlos en la carpeta SMB.
- Especifique la contraseña para la carpeta de usuario.

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Box] (Carpeta) - [User Box List] (Lista de carpetas de usuario)

Elemento de ajuste	Configuración recomendada
[Cifrado de comunicación SMB]	[Cifrar]

Firma de protocolo SMB

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [SMB Setting] (Configuración de SMB) - [SMB Server Settings] (Configuración de servidor SMB)

Elemento de ajuste	Configuración recomendada
[SMB security Signature Setting] (Configuración de firma de seguridad SMB)	[Obligatorio]

2.2.2 Cliente SMB

La autenticación de Kerberos emplea tecnología robusta de cifrado, de forma que reduce considerablemente el riesgo de robo de las credenciales durante el proceso de autenticación. También garantiza la integridad de los datos, ya que impide su manipulación entre el remitente y el destinatario, así como los ataques de retransmisión NTLM.

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [SMB Setting] (Configuración de SMB) - [Client Setting] (Configuración de cliente)

Elemento de ajuste	Configuración recomendada
[Configuración de autenticación SMB]	[Kerberos]

2.2.3 SNMP

Configure el cifrado mediante SNMPv3. Si también se añade la configuración de autenticación, puede aumentar aún más la seguridad. Los riesgos de seguridad son prácticamente los mismos que con SMB.

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [SNMP Setting] (Configuración de SNMP)

Elemento de ajuste	Configuración recomendada
[Configuración SNMP]	[SNMP v3(IP)]
[Algoritmo encriptación]	[AES-128]
[Authentication Method] (Método de autenticación)	Seleccione [SHA-256], [SHA-384] o [SHA-512].

2.2.4 IPsec

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [TCP/IP Setting] (Configuración de TCP/IP) - [IPsec] - [IPsec Setting] (Configuración IPsec)

[IKEv2]

Elemento de ajuste	Configuración recomendada
[Algoritmo encriptación]	[AES-CBC] ([256]/[192 and 256] (192 y 256)/[All] [Todo])
[Algoritmo autenticación]	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 y 384)/[384 and 512] (384 y 512)/[All] [Todo]), [AES-XCBC]
[Grupo Diffie-Hellman]	[Group 14] (Grupo 14), [Group 19] (Grupo 19)

[SA]

Elemento de ajuste	Configuración recomendada
[Modo encapsulación]	[Tunnel] (Túnel), [Transport] (Unidad de transporte)
[Protocolo seguridad]	[ESP]
[Key Exchange Method] (Método intercamb. claves)	[IKEv2]
[Authentication Method] (Método de autenticación)	[Firma digital]
[Algoritmo encript.ESP]	[AES-GCM] ([256]/[192 and 256] (192 y 256)/[All] [Todo]), [AES-GCM-64] ([256]/[192 and 256] (192 y 256)/[All] [Todo]), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 y 256)/[All] [Todo])
[Confid. reenvío perfec.]	ACT.
[Diffie-Hellman Group(IKEv2)] (Grupo Diffie-Hellman [IKEv2]) - [Priority1-4] (Prioridad 1-4)	[Group 14] (Grupo 14), [Group 19] (Grupo 19)

2.2.5 S/MIME

Si utiliza la opción S/MIME para enviar correo electrónico, puede cifrar el contenido del mensaje para evitar escuchas y verificar la identidad del remitente con una firma electrónica. Es una medida eficaz contra la suplantación de identidad y el phishing.

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [E-mail Setting] (Configuración de correo electrónico) - [S/MIME]

Elemento de ajuste	Configuración recomendada
[Firma digital]	[Siempre firmar]
[Tipo de firma digital]	[SHA-256]
[E-Mail Text Encrypt. Method] (Método cifrado texto e-mail)	[AES-256]

3 Configuración de la validación de certificados

Cuando utilice la comunicación de cifrado TLS para reducir el impacto de los ataques de intermediario, le recomendamos que utilice la validación de certificados. Para los elementos de validación, le recomendamos que habilite la fecha de caducidad del certificado y la cadena como mínimo.

Si se intenta conectar a un entorno heredado que no dispone de una función de validación de certificados, aumenta el riesgo de ataques de intermediario. Se recomienda su uso en un entorno de red seguro.

Se recomienda la validación de certificados en el MFP en las siguientes funciones de cliente MFP. Para obtener más información sobre las ubicaciones de los ajustes, consulte las siguientes secciones. POP, SMTP (Iniciar TLS/SMTP sobre SSL), Aut. IEEE802.1X (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPsec, WebDAV, LDAP, DPWS, RemotePanel



Sugerencias

Se recomienda la validación de certificados en el lado del cliente conectado a la MFP en las siguientes funciones de servidor de MFP.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), Socket TCP

3.1 POP

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [E-mail Setting] (Configuración de correo electrónico) - [E-mail RX (POP)] (Recepción de correo electrónico [POP])

Elemento de ajuste	Configuración recomendada
[Configuración del nivel de verificación de certificados]	[Fecha de caducidad]: ACT. [Cadena]: ACT.

3.2 SMTP

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [E-mail Setting] (Configuración de correo electrónico) - [E-mail TX (SMTP)] (Transmisión de correo [SMTP])

Elemento de ajuste	Configuración recomendada
[Configuración del nivel de verificación de certificados]	[Fecha de caducidad]: ACT. [Cadena]: ACT.

3.3 Aut. IEEE802.1X

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [IEEE802.1X Authentication Setting] (Configuración de autenticación de IEEE802.1X) - [IEEE802.1X Authentication Setting] (Configuración de autenticación de IEEE802.1X) - [Supplicant Setting] (Configuración de suplicante)

Elemento de ajuste	Configuración recomendada
[Configuración del nivel de verificación de certificados]	[Fecha de caducidad]: ACT. [Cadena]: ACT.

3.4 IPsec

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [TCP/IP Setting] (Configuración de TCP/IP) - [IPsec] - [Enable IPsec] (Activar IPsec)

Elemento de ajuste	Configuración recomendada
[Configuración del nivel de verificación de certificados]	[Fecha de caducidad]: [Confirmar] [Cadena]: [Confirmar]



Sugerencias

In [IPsec Setting] (Configuración de IPsec), registre los elementos [IKE], [SA], [Peer] y [Protocol Setting] (Configuración de protocolo) antes.

3.5 WebDAVClient

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [WebDAV Settings] (Configuración WebDAV) - [WebDAV Client Settings] (Configuración de cliente WebDAV)

Elemento de ajuste	Configuración recomendada
[Configuración del nivel de verificación de certificados]	[Fecha de caducidad]: ACT. [Cadena]: ACT.

3.6 LDAP

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [LDAP Setting] (Configuración de LDAP) - [Setting Up LDAP] (Configurar LDAP)

Elemento de ajuste	Configuración recomendada
[Configuración del nivel de verificación de certificados]	[Fecha de caducidad]: ACT. [Cadena]: ACT.

3.7 DPWS

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [DPWS Settings] (Configuración DPWS) - [DPWS Common Settings] (Configuración común DPWS)

Elemento de ajuste	Configuración recomendada
[Configuración del nivel de verificación de certificados]	[Fecha de caducidad]: ACT. [Cadena]: ACT.

3.8 OpenAPI

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [OpenAPI Setting] (Configuración de OpenAPI) - [OpenAPI Setting] (Configuración de OpenAPI)

Elemento de ajuste	Configuración recomendada
[Configuración del nivel de verificación de certificados]	[Fecha de caducidad]: ACT. [Cadena]: ACT.

3.9 Panel remoto

Ubicación del ajuste: [Utility] (Utilidad) - [Administrator] (Administrador) - [Network] (Red) - [Remote Panel Settings] (Configuración del servidor del panel remoto) - [Remote Panel Client Settings] (Configuración del cliente del panel remoto)

Elemento de ajuste	Configuración recomendada
[Configuración del nivel de verificación de certificados]	[Fecha de caducidad]: ACT. [Cadena]: ACT.

4 Información adicional de seguridad

4.1 Recomendación de mejores prácticas

Recomendamos que los algoritmos de cifrado que se utilicen cumplan con las mejores prácticas recomendadas en las Directrices sobre criptografía de la EUCC y en los Mecanismos criptográficos acordados por SOGIS.

A continuación figura una lista de los algoritmos de cifrado y longitudes de clave recomendados por las Directrices sobre criptografía de la EUCC y los Mecanismos criptográficos acordados por SOGIS.

Elemento	Configuración recomendada
Algoritmos de cifrado	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Longitud de la clave de cifrado	RSA: 2048 bits o más ECC: 256 bits o más AES: 256 bits.



Sugerencias

Para obtener más información, consulte las Directrices sobre criptografía de la EUCC y los Mecanismos criptográficos acordados por SOGIS más recientes.

4.2 Precauciones para la comunicación con sistemas heredados

Se supone que se utilizan los siguientes protocolos y versiones para la comunicación con sistemas heredados.

El uso de configuraciones heredadas aumenta los riesgos de seguridad, por lo que le rogamos que las utilice en un entorno de red seguro.

Elemento	Configuración heredada
Protocolo	SLP FTP SMB (3.0 o versión anterior, NTLMv1/v2) SNMPv1/v2 Aut. IEEE802.1X (EAP-TYPE: Depende del servidor/Desactivada) DPWS Socket TCP
Algoritmos de cifrado	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Longitud de la clave de cifrado	RSA: 1024 bits o menos ECC: 160 bits o menos AES: 128 bits o menos DES: 56 bits. 3DES: 112 bits.

Configuración IPsec heredada

[IKEv1]

Elemento de ajuste	Configuración heredada
[Algoritmo encriptación]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] [128 y 192])
[Algoritmo autenticación]	No se utiliza
[Grupo Diffie-Hellman]	[Group 1] (Grupo 1), [Group 2] (Grupo 2), [Group 5] (Grupo 5)

[IKEv2]

Elemento de ajuste	Configuración heredada
[Algoritmo encriptación]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] [128 y 192])
[Algoritmo autenticación]	No se utiliza
[Grupo Diffie-Hellman]	[Group 1] (Grupo 1), [Group 2] (Grupo 2), [Group 5] (Grupo 5)

[SA]

Elemento de ajuste	Configuración heredada
[Key Exchange Method] (Método intercamb. claves)	[IKEv1]
[Authentication Method] (Método de autenticación)	[Firma digital]
[Algoritmo encript.ESP]	[3DES-CBC] ([128]/[192]/[128 and 192] [128 y 192]) [AES-CTR] ([128]/[192]/[128 and 192] [128 y 192]) [AES-GCM] ([128]/[192]/[128 and 192] [128 y 192]) [AES-GCM-64] ([128]/[192]/[128 and 192] [128 y 192]) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] [128 y 192])

Elemento de ajuste	Configuración heredada
[Confid. reenvío perfec.]	ACT.
[Diffie-Hellman Group(IKEv1)] (Grupo Diffie-Hellman [IKEv1])	[Group 1] (Grupo 1), [Group 2] (Grupo 2), [Group 5] (Grupo 5)

4.3 Interfaces y servicios de red disponibles desde fábrica

Tipo serv.	Protocolo	Número de puerto
DHCP	UDP	68
Servidor HTTP	TCP	80
Servicio de nombre de NetBIOS	UDP	137
Servicio de datagrama de NetBIOS	UDP	138
SNMP	UDP	161
Servidor HTTP sobre SSL / IPP sobre SSL	TCP	443
Impresión LPD	TCP	515
Cliente DHCPv6	UDP	546
Impresión IPP	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-tool)	TCP	8091
Impresión RAW	TCP	9100
Impresión RAW	TCP	9112
Impresión RAW	TCP	9113
Impresión RAW	TCP	9114
Impresión RAW	TCP	9115
Impresión RAW	TCP	9116
OpenAPI	TCP	50001

4.4 Acerca de la validación de entradas

Para ver el número de caracteres que deben introducirse para la configuración de red, etc., consulte cada uno de los elementos de configuración en el Manual de usuario.

Según la codificación del idioma, la entrada máxima permitida (datos guardados en la MFP) para los elementos que admiten caracteres multibyte puede ser el triple del número de caracteres.

Consigli per i dispositivi collegati in rete in modo sicuro



Sommario

1 Impostazione del Filtro indirizzo IP

1.1	Filtro indirizzo IP	1-3
1.2	Filtraggio IP rapido	1-3

2 Impostazione della comunicazione crittografata

2.1	Crittografia TLS.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel (Pannello remoto)	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth (Autenticaz. IEEE802.1X)	2-6
2.1.10	LDAP	2-6
2.1.11	Socket TCP.....	2-6
2.2	Altri tipi di crittografia.....	2-7
2.2.1	SMBServer (Server SMB).....	2-7
	Crittografia SMB	2-7
	Firma di sicurezza SMB	2-7
2.2.2	SMBClient (Client SMB).....	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Impostazione della Validazione del certificato

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	IEEE802.1X Auth (Autenticaz. IEEE802.1X).....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient (Client WebDAV)	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	RemotePanel (Pannello remoto).....	3-12

4 Informazioni aggiuntive relative alla sicurezza

4.1	Raccomandazioni in materia di migliori pratiche	4-13
4.2	Precauzioni per la comunicazione con sistemi legacy	4-14
	Impostazioni legacy IPsec	4-14
4.3	Interfacce e servizi di rete disponibili fin dalla spedizione dalla fabbrica	4-16
4.4	Informazioni sulla validazione delle immissioni	4-17



Informazioni sul presente manuale

Il presente manuale descrive le informazioni e le impostazioni che consentono un utilizzo in sicurezza dei dispositivi.

Quando si collega alla macchina alla rete, utilizzarla in un ambiente protetto da un firewall. Si consiglia, inoltre, di impostare un indirizzo IP privato come indirizzo IP della macchina.

Impostando un indirizzo IP privato si consentirà di accedere alla macchina solamente agli utenti di una rete locale, ad esempio di una LAN interna, così da impedire accessi non autorizzati dall'esterno.

Qualora sia necessario utilizzare un indirizzo IP globale, accertarsi di installare la macchina dietro un firewall.

1 Impostazione del Filtro indirizzo IP

Il Filtro indirizzo IP è una funzione che limita i dispositivi che possono accedere alla macchina in base all'indirizzo IP. Impostando correttamente questa funzione sarà possibile vietare l'accesso da dispositivi non autorizzati.

La funzione Filtro indirizzo IP della macchina può essere impostata con uno dei seguenti due metodi.

1.1 Filtro indirizzo IP

Specificare manualmente l'intervallo di indirizzi IP a cui consentire o negare l'accesso.

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [TCP/IP Setting] (Impostazioni TCP/IP) - [IP Address Filtering] (Filtro indirizzo IP)

Consigli

Impostare gli indirizzi IP ai quali consentire o negare l'accesso in base al proprio ambiente.

1.2 Filtraggio IP rapido

L'intervallo di indirizzi IP ai quali consentire l'accesso viene impostato automaticamente in base all'indirizzo IP e alla maschera di sottorete impostati nella macchina.

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [TCP/IP Setting] (Impostazioni TCP/IP) - [Quick IP Filtering] (Filtraggio IP rapido)

Impostazioni consigliate: [Synchronize IP Address] (Sincronizza indirizzo IP) [Synchronize Subnet Mask] (Sincronizza maschera sottorete) *

* Selezionare la voce adatta al proprio ambiente.

2 Impostazione della comunicazione crittografata

Si consiglia di utilizzare la seguente comunicazione crittografata per evitare intercettazioni e furti di dati, manomissioni dei dati e dirottamenti di sessione.

2.1 Crittografia TLS

Si consiglia di configurare le seguenti impostazioni per ridurre il rischio di vulnerabilità.

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Security] (Sicurezza) - [PKI Settings] (Impostazioni PKI) - [Enable SSL Version] (Abilita versione SSL)

Voce di impostazione	Impostazione consigliata
[Mode using SSL/TLS] (Modalità che usa SSL/TLS)	[Admin. Mode and User Mode] (Modalità Ammin. e Mod.Utente)
[SSL/TLS Version Setting] (Impostazione versione SSL/TLS)	TLS1.2 TLS1.3 (incompatibile con IEEE802.1X)
[Encryption Strength] (Livello criptat.)	AES-256

Il certificato iniziale è installato in fabbrica. Qualora occorra un differente certificato, registrarne uno nuovo nella seguente posizione.

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Security] (Sicurezza) - [PKI Settings] (Impostazioni PKI) - [Device Certificate Setting] (Impostazione certificato dispositivo)

Voce di impostazione	Impostazione consigliata
[Encryption Key Type] (Tipo chiave criptatura)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

La crittografia TLS è supportata per i seguenti protocolli e servizi. Per informazioni dettagliate sulle posizioni delle impostazioni, fare riferimento alle seguenti sezioni.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel (Pannello remoto))
- DPWS
- POP
- SMTP (Start TLS (Avvio TLS), SMTP over SSL (SMTP su SSL))
- IEEE802.1X Auth (Autenticaz. IEEE802.1X) (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- Socket TCP

2.1.1 HTTP (Web Connection)

Se si abilita [Enable SSL Version] (Abilita versione SSL), la modalità di comunicazione passerà automaticamente alla comunicazione crittografata TLS (HTTPS).

2.1.2 WebDAVServer

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [WebDAV Settings] (Impostazioni WebDAV) - [WebDAV Server Settings] (Impostazioni server WebDAV)

Voce di impostazione	Impostazione consigliata
[Impostaz. SSL]	[Solo SSL]

2.1.3 IPP

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [HTTP Server Settings] (Impostazioni server HTTP)

Voce di impostazione	Impostazione consigliata
[Impostaz. IPP-SSL]	[Solo SSL]

2.1.4 OpenAPI

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [OpenAPI Setting] (Impostazione OpenAPI) - [OpenAPI Setting] (Impostazione OpenAPI)

Voce di impostazione	Impostazione consigliata
[Impostazioni SSL/Porta]	[Solo SSL]

2.1.5 RemotePanel (Pannello remoto)

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [Remote Panel Settings] (Impostazioni Pannello remoto) - [Remote Panel Server Settings] (Impostazioni server Pannello remoto)

Voce di impostazione	Impostazione consigliata
[Port No.(SSL)] (Numero porta (SSL))	[50443]



Consigli

Se si abilita [Enable SSL Version] (Abilita versione SSL), la comunicazione passerà automaticamente alla modalità crittografata TLS. Specificare un numero di porta.

2.1.6 DPWS

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [DPWS Settings] (Impostazioni DPWS) - [DPWS Common Settings] (Impostazioni comuni DPWS)

Voce di impostazione	Impostazione consigliata
[Impostaz. SSL]	ON

2.1.7 POP

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [E-mail Setting] (Impostazione e-mail) - [E-mail RX (POP)] (Ricezione e-mail (POP))

Voce di impostazione	Impostazione consigliata
[Abilita SSL]	ON

2.1.8 SMTP

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [E-mail Setting] (Impostazione e-mail) - [E-mail TX (SMTP)] (Trasmissione e-mail (SMTP))

Voce di impostazione	Impostazione consigliata
[Impostazioni SSL/TLS]	[SMTP over SSL]

2.1.9 IEEE802.1X Auth (Autenticaz. IEEE802.1X)

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [IEEE802.1X Authentication Setting] (Impostazione autenticazione IEEE802.1X) - [IEEE802.1X Authentication Setting] (Impostazione autenticazione IEEE802.1X) - [Supplicant Setting] (Impostazione di richiedente)

Voce di impostazione	Impostazione consigliata
[Tipo EAP]	Selezionare [EAP-TLS], [EAP-TTLS] o [PEAP]).

2.1.10 LDAP

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [LDAP Setting] (Impostazione LDAP) - [Setting Up LDAP] (Imposta LDAP)

Voce di impostazione	Impostazione consigliata
[Abilita SSL]	ON

2.1.11 Socket TCP

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [TCP Socket Setting] (Impostazione socket TCP)

Voce di impostazione	Impostazione consigliata
[Use SSL/TLS] (Usa SSL/TLS)	ON

2.2 Altri tipi di crittografia

Si consiglia di configurare le seguenti impostazioni per ridurre il rischio di vulnerabilità. Per informazioni dettagliate sulle impostazioni di ciascuna funzione, fare riferimento alle seguenti sezioni.

Funzione	Impostazione consigliata
SMBServer (Server SMB)	SMB Encryption, SMB Signature (Crittografia SMB, Firma di sicurezza SMB)
SMBClient (Client SMB)	Kerberos Authentication (Autenticazione Kerberos)
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	ON

2.2.1 SMBServer (Server SMB)

L'utilizzo della Crittografia SMB e della Firma di sicurezza SMB può ridurre i seguenti rischi di sicurezza.

- Intercettazioni e furti di dati: Un soggetto terzo malintenzionato potrebbe intercettare comunicazioni e appropriarsi di informazioni personali o confidenziali.
- Manomissioni dei dati: Vi è un rischio di manomissione dei contenuti delle comunicazioni mediante un attacco di tipo Man-In-The-Middle (MITM).
- Spoofing: Successivamente a un furto di informazioni di autenticazione, una terza parte potrebbe farsi passare per un legittimo utente per ottenere accessi non autorizzati.
- Fughe di informazioni: Le comunicazioni non crittografate possono essere intercettate con facilità, specialmente sulle reti Wi-Fi pubbliche, aumentando il rischio di fughe di informazioni personali e relative alle carte di credito.

Crittografia SMB

Presupposti

- Creare una Casella utente pubblica. Inoltre, configurare l'impostazione in modo da trasferire automaticamente i file dalla Casella utente pubblica e salvarli nella cartella SMB.
- Specificare la password per la Casella utente.

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Box] (Casella) - [User Box List] (Elenco caselle utente)

Voce di impostazione	Impostazione consigliata
[Crittografia comunicazioni SMB]	[Encrypt] (Crittog.)

Firma di sicurezza SMB

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [SMB Setting] (Impostazioni SMB) - [SMB Server Settings] (Impostazioni server SMB)

Voce di impostazione	Impostazione consigliata
[SMB security Signature Setting] (Impostazione di firma di sicurezza SMB)	[Richiesta]

2.2.2 SMBClient (Client SMB)

L'Autenticazione Kerberos utilizza una tecnologia di crittografia robusta, così da ridurre in modo significativo il rischio di furti di credenziali durante il processo di autenticazione. Garantisce inoltre l'integrità dei dati, evitando manomissioni di questi ultimi tra il mittente e il destinatario nonché attacchi di tipo NTLM Relay.

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [SMB Setting] (Impostazioni SMB) - [Client Setting] (Impostazione client)

Voce di impostazione	Impostazione consigliata
[Impostazione autenticazione SMB]	[Kerberos]

2.2.3 SNMP

Impostare la crittografia mediante SNMPv3. È possibile aumentare ulteriormente la sicurezza aggiungendo anche l'impostazione di autenticazione. I rischi di sicurezza sono all'incirca gli stessi presenti con SMB.

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [SNMP Setting] (Impostazione SNMP)

Voce di impostazione	Impostazione consigliata
[Impostazione SNMP]	[SNMP v3(IP)]
[Algoritmo Criptazione]	[AES-128]
[Authentication Method] (Metodo di autenticazione)	Selezionare [SHA-256], [SHA-384] o [SHA-512].

2.2.4 IPsec

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [TCP/IP Setting] (Impostazioni TCP/IP) - [IPsec] - [IPsec Setting] (Impostazione IPsec)

[IKEv2]

Voce di impostazione	Impostazione consigliata
[Algoritmo Criptazione]	[AES-CBC] ([256]/[192 and 256] (192 e 256)/[All] (Tutto))
[Algoritmo Autenticazione]	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 e 384)/[384 and 512] (384 e 512)/[All] (Tutto)), [AES-XCBC]
[Gruppo Diffie-Hellman]	[Group 14] (Gruppo 14), [Group 19] (Gruppo 19)

[SA]

Voce di impostazione	Impostazione consigliata
[Incapsulamento]	[Tunnel], [Transport] (Trasporto)
[Protocollo Sicurezza]	[ESP]
[Key Exchange Method] (Metodo di scambio chiave)	[IKEv2]
[Authentication Method] (Metodo di autenticazione)	[Firma digitale]
[Algoritmo Criptaz. ESP]	[AES-GCM] ([256]/[192 and 256] (192 e 256)/[All] (Tutto)), [AES-GCM-64] ([256]/[192 and 256] (192 e 256)/[All] (Tutto)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 e 256)/[All] (Tutto))
[Alta Sicurezza Inoltro]	ON
[Diffie-Hellman Group(IKEv2)] (Gruppo Diffie-Hellman (IKEv2)) - [Priority1-4] (Priorità 1-4)	[Group 14] (Gruppo 14), [Group 19] (Gruppo 19)

2.2.5 S/MIME

Utilizzando la funzione opzionale S/MIME per la trasmissione delle e-mail sarà possibile crittografare il loro contenuto per evitare intercettazioni e furti e, inoltre, verificare l'identità del mittente mediante una firma elettronica. Si tratta di una misura efficace contro le truffe di tipo phishing e spoofing.

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [E-mail Setting] (Impostazione e-mail) - [S/MIME]

Voce di impostazione	Impostazione consigliata
[Firma digitale]	[Firma sempre]
[Tipo firma digitale]	[SHA-256]
[Metodo crittog. testo e-mail]	[AES-256]

3 Impostazione della Validazione del certificato

Quando si utilizza la comunicazione crittografata TLS per ridurre l'impatto degli attacchi di tipo Man-In-The-Middle, si consiglia di utilizzare la validazione del certificato. Per le voci di validazione si consiglia di attivare almeno la catena e la data di scadenza del certificato.

Qualora venga effettuato un tentativo di connettersi a un ambiente legacy che non disponga di una funzione di validazione del certificato, il rischio di attacchi di tipo Man-In-The-Middle aumenta. Se ne consiglia l'utilizzo in un ambiente sicuro.

Si consiglia la validazione del certificato lato MFP nell'ambito delle seguenti funzioni client MFP. Per informazioni dettagliate sulle posizioni delle impostazioni, fare riferimento alle seguenti sezioni. POP, SMTP (Start TLS/SMTP over SSL (Avvio TLS/SMTP su SSL)), IEEE802.1X Auth (Autenticaz. IEEE802.1X) (EAP-TYPE (TIPO EAP): EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel (Pannello remoto)

Consigli

Si consiglia la validazione del certificato lato client collegato all'MFP nell'ambito delle seguenti funzioni server MFP.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel (Pannello remoto)), TCP Socket (Socket TCP)

3.1 POP

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [E-mail Setting] (Impostazione e-mail) - [E-mail RX (POP)] (Ricezione e-mail (POP))

Voce di impostazione	Impostazione consigliata
[Impostazioni livello verifica certificato]	[Expiration Date] (Data di scadenza): ON [Catena]: ON

3.2 SMTP

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [E-mail Setting] (Impostazione e-mail) - [E-mail TX (SMTP)] (Trasmissione e-mail (SMTP))

Voce di impostazione	Impostazione consigliata
[Impostazioni livello verifica certificato]	[Expiration Date] (Data di scadenza): ON [Catena]: ON

3.3 IEEE802.1X Auth (Autenticaz. IEEE802.1X)

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [IEEE802.1X Authentication Setting] (Impostazione autenticazione IEEE802.1X) - [IEEE802.1X Authentication Setting] (Impostazione autenticazione IEEE802.1X) - [Supplicant Setting] (Impostazione di richiedente)

Voce di impostazione	Impostazione consigliata
[Impostazioni livello verifica certificato]	[Expiration Date] (Data di scadenza): ON [Catena]: ON

3.4 IPsec

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [TCP/IP Setting] (Impostazioni TCP/IP) - [IPsec] - [Enable IPsec] (Abilita IPsec)

Voce di impostazione	Impostazione consigliata
[Impostazioni livello verifica certificato]	[Expiration Date] (Data di scadenza): [Confirm] (Conferma) [Catena]: [Confirm] (Conferma)

Consigli

In [IPsec Setting] (Impostazione IPsec), registrare innanzitutto le voci [IKE], [SA], [Peer] e [Protocol Setting] (Impostazione Protocollo).

3.5 WebDAVClient (Client WebDAV)

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [WebDAV Settings] (Impostazioni WebDAV) - [WebDAV Client Settings] (Impostazioni client WebDAV)

Voce di impostazione	Impostazione consigliata
[Impostazioni livello verifica certificato]	[Expiration Date] (Data di scadenza): ON [Catena]: ON

3.6 LDAP

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [LDAP Setting] (Impostazione LDAP) - [Setting Up LDAP] (Imposta LDAP)

Voce di impostazione	Impostazione consigliata
[Impostazioni livello verifica certificato]	[Expiration Date] (Data di scadenza): ON [Catena]: ON

3.7 DPWS

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [DPWS Settings] (Impostazioni DPWS) - [DPWS Common Settings] (Impostazioni comuni DPWS)

Voce di impostazione	Impostazione consigliata
[Impostazioni livello verifica certificato]	[Expiration Date] (Data di scadenza): ON [Catena]: ON

3.8 OpenAPI

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [OpenAPI Setting] (Impostazione OpenAPI) - [OpenAPI Setting] (Impostazione OpenAPI)

Voce di impostazione	Impostazione consigliata
[Impostazioni livello verifica certificato]	[Expiration Date] (Data di scadenza): ON [Catena]: ON

3.9 RemotePanel (Pannello remoto)

Posizione dell'impostazione: [Utility] (Utilità) - [Administrator] (Amministratore) - [Network] (Rete) - [Remote Panel Settings] (Impostazioni Pannello remoto) - [Remote Panel Client Settings] (Impostazioni client Pannello remoto)

Voce di impostazione	Impostazione consigliata
[Impostazioni livello verifica certificato]	[Expiration Date] (Data di scadenza): ON [Catena]: ON

4 Informazioni aggiuntive relative alla sicurezza

4.1 Raccomandazioni in materia di migliori pratiche

Si consiglia di utilizzare gli algoritmi di crittatura conformemente alle impostazioni delle migliori pratiche raccomandate nelle Linee guida EUCC riguardanti la Crittografia e definite nell'ambito dei SOGIS-Agreed-Cryptographic-Mechanisms.

Segue un elenco di lunghezze delle chiavi e algoritmi di crittatura consigliati nelle Linee guida EUCC riguardanti la Crittografia e definiti nell'ambito dei SOGIS-Agreed-Cryptographic-Mechanisms.

Voce	Impostazione consigliata
Algoritmi di crittatura	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) (Crittografia ellittica) HMAC (Hash-based Message Authentication Code (Codice per l'autenticazione di messaggi basato su una funzione di hash))
Lunghezza della chiave di crittatura	RSA: minimo 2048 bit ECC: minimo 256 bit AES: 256 bit

Consigli

Per maggiori dettagli, fare riferimento alle Linee guida EUCC riguardanti la Crittografia nonché ai SOGIS-Agreed-Cryptographic-Mechanisms più recenti.

4.2 Precauzioni per la comunicazione con sistemi legacy

Si assume che i seguenti protocolli e versioni vengano utilizzati per la comunicazione con sistemi legacy.

L'utilizzo di sistemi legacy aumenta i rischi di sicurezza e, pertanto, si consiglia di utilizzarli in un ambiente di rete sicuro.

Voce	Impostazioni legacy
Protocollo	SLP FTP SMB (3.0 o versione precedente, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (Autenticaz. IEEE802.1X) (EAP-TYPE (TIPO EAP): Depend on Server (Dipende dal server)/OFF) DPWS TCPsocket (Socket TCP)
Algoritmi di crittatura	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher (Cifrario D51Rivest)) RC2-64 (D51Rivest Cipher (Cifrario D51Rivest)) RC2-128 (D51Rivest Cipher (Cifrario D51Rivest))
Lunghezza della chiave di crittatura	RSA: 1024 bit o inferiore ECC: 160 bit o inferiore AES: 128 bit o inferiore DES: 56 bit 3DES: 112 bit

Impostazioni legacy IPsec

[IKEv1]

Voce di impostazione	Impostazioni legacy
[Algoritmo Criptazione]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 e 192))
[Algoritmo Autenticazione]	Non utilizzato
[Gruppo Diffie-Hellman]	[Group 1] (Gruppo 1), [Group 2] (Gruppo 2), [Group 5] (Gruppo 5)

[IKEv2]

Voce di impostazione	Impostazioni legacy
[Algoritmo Criptazione]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 e 192))
[Algoritmo Autenticazione]	Non utilizzato
[Gruppo Diffie-Hellman]	[Group 1] (Gruppo 1), [Group 2] (Gruppo 2), [Group 5] (Gruppo 5)

[SA]

Voce di impostazione	Impostazioni legacy
[Key Exchange Method] (Metodo di scambio chiave)	[IKEv1]
[Authentication Method] (Metodo di autenticazione)	[Firma digitale]
[Algoritmo Criptaz. ESP]	[3DES-CBC] ([128]/[192]/[128 and 192] (128 e 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 e 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 e 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 e 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 e 192))

Voce di impostazione	Impostazioni legacy
[Alta Sicurezza Inoltro]	ON
[Diffie-Hellman Group(IKEv1)] (Gruppo Diffie-Hellman (IKEv1))	[Group 1] (Gruppo 1), [Group 2] (Gruppo 2), [Group 5] (Gruppo 5)

4.3 Interfacce e servizi di rete disponibili fin dalla spedizione dalla fabbrica

Tipo di servizio	Protocollo	Numero di porta
DHCP	UDP	68
Server HTTP	TCP	80
Servizio Nome NetBIOS	UDP	137
Servizio Datagramma NetBIOS	UDP	138
SNMP	UDP	161
Server HTTP su SSL / IPP su SSL	TCP	443
Stampa LPD	TCP	515
Client DHCPv6	UDP	546
Stampa IPP	TCP	631
MFPIF	UDP	1900
Servizio Web	UDP	3702
LLMNR	UDP	5355
HTTP (tool IWS)	TCP	8091
Stampa RAW	TCP	9100
Stampa RAW	TCP	9112
Stampa RAW	TCP	9113
Stampa RAW	TCP	9114
Stampa RAW	TCP	9115
Stampa RAW	TCP	9116
OpenAPI	TCP	50001

4.4 Informazioni sulla validazione delle immissioni

Per quanto riguarda il numero di caratteri da immettere per le impostazioni di rete, ecc., fare riferimento alle singole voci di impostazione riportate nel Manuale d'uso.

A seconda della codifica della lingua, la massima quantità di dati inseribili ammessa (dati salvati nell'MFP) per le voci che supportano caratteri multibyte potrebbe essere pari a tre volte il numero di caratteri.

Препоръки за защитени мрежови устройства



Таблица със съдържание

1 Задаване на филтриране по IP адрес

1.1	Филтриране по IP адрес.....	1-3
1.2	Бързо IP филтриране.....	1-3

2 Настройка на криптираната комуникация

2.1	TLS криптиране.....	2-4
2.1.1	HTTP (Web Connection)	2-5
2.1.2	WebDAVServer	2-5
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel (Отдалечен панел).....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-6
2.1.8	SMTP	2-6
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP порт	2-6
2.2	Друго криптиране.....	2-7
2.2.1	SMB сървър.....	2-7
	SMB криптиране.....	2-7
	SMB подпис	2-7
2.2.2	SMB клиент	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Задаване на валидирането на сертификата

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-12
3.9	RemotePanel (Отдалечен панел)	3-12

4 Допълнителна информация за сигурността

4.1	Препоръка за най-добри практики.....	4-13
4.2	Предпазни мерки за комуникация с наследени системи	4-14
	Наследени настройки на IPsec	4-14
4.3	Мрежови интерфейси и услуги, налични още при доставката от завода	4-16
4.4	За валидирането на входни данни	4-17



За това ръководство

Това ръководство описва информация и настройки, които позволяват безопасно използване на устройствата.

Когато свързвате машината към мрежата, използвайте я в среда, защитена чрез защитна стена. Препоръчваме също така да зададете частен IP адрес за IP адреса на машината.

Задаването на частен IP адрес позволява достъп до машината само на потребители в локална мрежа, например вътрешна LAN, като предотвратява неоторизиран достъп отвън.

Ако трябва да използвате глобален IP адрес, не забравяйте да инсталирате машината в защитна стена.

1 Задаване на филтриране по IP адрес

Филтрирането по IP адрес е функция, която ограничава устройствата, които имат достъп до машината, според IP адреса. Можете да ограничите достъпа на неоторизирани устройства, като настроите правилно тази функция.

Функцията за филтриране по IP адрес на машината може да бъде настроена по следните два начина.

1.1 Филтриране по IP адрес

Ръчно задаване на обхвата от IP адреси, на които е позволен или отказан достъп.

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [TCP/IP Setting] (Настройка на TCP/IP) - [IP Address Filtering] (Филтриране по IP адрес)



Настройте разрешените или забранените IP адреси в съответствие с вашата среда.

1.2 Бързо IP филтриране

Обхватът от IP адреси, на които е позволен достъп, се задава автоматично въз основа на IP адреса и маската на подмрежата, зададени в машината.

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [TCP/IP Setting] (Настройка на TCP/IP) - [Quick IP Filtering] (Бързо IP филтриране)

Препоръчителни настройки: [Synchronize IP Address] (Синхронизиране на IP адреса)/[Synchronize Subnet Mask] (Синхронизиране на маската на подмрежата)

* Изберете един от двата варианта, за да отговаря на вашата среда.

2 Настройка на криптираната комуникация

Препоръчваме ви да използвате следната криптирана комуникация, за да предотвратите подслушване на данни, подправяне на данни и атакуване на сесии.

2.1 TLS криптиране

Препоръчваме ви да конфигурирате следните настройки, за да намалите риска от уязвимости.

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Security] (Сигурност) - [PKI Settings] (Настройки на PKI) - [Enable SSL Version] (Активиране на SSL версия)

Настройка на елемент	Препоръчителна настройка
[Mode using SSL/TLS] (Режим с използване на SSL/TLS)	[Admin. Mode and User Mode] (Админ. режим и потребителски режим)
[SSL/TLS Version Setting] (Настройка на версия на SSL/TLS)	TLS1.2 TLS1.3 (несъвместим с IEEE802.1X)
[Encryption Strength] (Сила на криптиране)	AES-256

Първоначалният сертификат се инсталира фабрично. Ако ви е необходим друг сертификат, регистрирайте нов на следното място.

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Security] (Сигурност) - [PKI Settings] (Настройки на PKI) - [Device Certificate Setting] (Настройка за сертификата на устройството)

Настройка на елемент	Препоръчителна настройка
[Encryption Key Type] (Тип ключ за криптиране)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

TLS криптирането се поддържа за следните протоколи и услуги. За подробности относно местата за настройка вижте следните раздели.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (стартиране на TLS, SMTP през SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP порт

2.1.1 HTTP (Web Connection)

Ако активирате [Enable SSL Version] (Активиране на SSL версия), режимът за комуникация автоматично се превключва на TLS криптирана комуникация (HTTPS).

2.1.2 WebDAVServer

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [WebDAV Settings] (Настройки на WebDAV) - [WebDAV Server Settings] (Настройки на сървър на WebDAV)

Настройка на елемент	Препоръчителна настройка
[SSL Settings] (Настройки на SSL)	[SSL Only] (Само SSL)

2.1.3 IPP

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [HTTP Server Settings] (Настройки на HTTP сървър)

Настройка на елемент	Препоръчителна настройка
[IPP-SSL Settings] (Настройки на IPP-SSL)	[SSL Only] (Само SSL)

2.1.4 OpenAPI

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [OpenAPI Setting] (Настройка на OpenAPI) - [OpenAPI Setting] (Настройка на OpenAPI)

Настройка на елемент	Препоръчителна настройка
[SSL/Port Settings] (Настройки на SSL/порт)	[SSL Only] (Само SSL)

2.1.5 RemotePanel (Отдалечен панел)

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [Remote Panel Settings] (Настройки на отдалечен панел) - [Remote Panel Server Settings] (Настройки на сървър на отдалечен панел)

Настройка на елемент	Препоръчителна настройка
[Port No.(SSL)] (Номер на порт (SSL))	[50443]

Съвети

Ако активирате [Enable SSL Version] (Активиране на SSL версия), комуникацията автоматично превключва в режим на TLS криптиране. Посочете номер на порт.

2.1.6 DPWS

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [DPWS Settings] (Настройки на DPWS) - [DPWS Common Settings] (Общи настройки на DPWS)

Настройка на елемент	Препоръчителна настройка
[SSL Settings] (Настройки на SSL)	ON (ВКЛ)

2.1.7 POP

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [E-mail Setting] (Настройка на имейл) - [E-mail RX (POP)] (Имейл RX (POP))

Настройка на елемент	Препоръчителна настройка
[Enable SSL] (Активиране на SSL)	ON (ВКЛ)

2.1.8 SMTP

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [E-mail Setting] (Настройка на имейл) - [E-mail TX] (Имейл TX)

Настройка на елемент	Препоръчителна настройка
[SSL/TLS Settings] (Настройки на SSL/TLS)	[SMTP over SSL] (SMTP през SSL)

2.1.9 IEEE802.1X Auth

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [IEEE802.1X Authentication Setting] (Настройка IEEE802.1X автентикация) - [IEEE802.1X Authentication Setting] (Настройка IEEE802.1X автентикация) - [Supplicant Setting] (Настройка на заявител)

Настройка на елемент	Препоръчителна настройка
[EAP-Type] (Тип EAP)	Изберете [EAP-TLS], [EAP-TTLS], или [PEAP].

2.1.10 LDAP

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [LDAP Setting] (Настройка LDAP) - [Setting Up LDAP] (Настройване на LDAP)

Настройка на елемент	Препоръчителна настройка
[Enable SSL] (Активиране на SSL)	ON (ВКЛ)

2.1.11 TCP порт

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [TCP Socket Setting] (Настройка на TCP порт)

Настройка на елемент	Препоръчителна настройка
[Use SSL/TLS] (Използване на SSL/TLS)	ON (ВКЛ)

2.2 Друго криптиране

Препоръчваме ви да конфигурирате следните настройки, за да намалите риска от уязвимости. За подробности относно настройките за всяка функция вижте следните раздели.

Функция	Препоръчителна настройка
SMB сървър	SMB криптиране, SMB подпис
SMB клиент	Автентикация чрез Kerberos
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	ON (ВКЛ)

2.2.1 SMB сървър

Използването на SMB криптиране и SMB подпис може да намали следните рискове за сигурността.

- Подслушване: Злонамерена трета страна може да прихване комуникациите и да открадне лична или поверителна информация.
- Подправяне на данни: Съществува риск съдържанието на комуникацията да бъде подправено чрез атака тип "Man-In-The-Middle" ("човек по средата", MITM).
- Измама ("Споофинг"): Ако информацията за удостоверяване бъде открадната, трета страна може да се представи за легитимен потребител и да получи неоторизиран достъп.
- Изтичане на информация: Некриптираните комуникации могат лесно да бъдат прихванати, особено в обществени Wi-Fi мрежи, което увеличава риска от изтичане на лична информация и информация за кредитни карти.

SMB криптиране

Предварителни условия

- Създайте публична потребителска кутия. Също така конфигурирайте настройката за автоматично прехвърляне на файлове от публичната потребителска кутия и записването им в папката SMB.
- Задайте паролата за потребителската кутия.

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Box] (Кутия) - [User Box List] (Списък на потребителска кутия)

Настройка на елемент	Препоръчителна настройка
[SMB Communication Encryption] (SMB криптиране на комуникация)	[Encrypt] (Криптиране)

SMB подпис

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [SMB Setting] (Настройка SMB) - [SMB Server Settings] (Настройки на SMB сървър)

Настройка на елемент	Препоръчителна настройка
[SMB security Signature Setting] (Настройка на SMB подпис за сигурност)	[Required] (Изисквано)

2.2.2 SMB клиент

Автентикацията чрез Kerberos използва технология за силно криптиране, което значително намалява риска от кражба на идентификационни данни по време на процеса на автентикация. То също така осигурява целостта на данните, като предотвратява фалшифицирането на данни между подателя и получателя, както и NTLM атаките.

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [SMB Setting] (Настройка SMB) - [Client Setting] (Настройка на клиент)

Настройка на елемент	Препоръчителна настройка
[SMB Authentication Setting] (Настройка SMB автентикация)	[Kerberos]

2.2.3 SNMP

Задайте криптирането чрез SNMPv3. Ако се добави и настройката за автентикация, можете допълнително да повишите безопасността. Рисковете за сигурността са почти същите като при SMB.

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [SNMP Setting] (Настройка SNMP)

Настройка на елемент	Препоръчителна настройка
[SNMP Setting] (Настройка SNMP)	[SNMP v3(IP)]
[Encryption Algorithm] (Алгоритъм за криптиране)	[AES-128]
[Authentication Method] (Метод за автентикация)	Изберете [SHA-256], [SHA-384], или [SHA-512].

2.2.4 IPsec

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [TCP/IP Setting] (Настройка на TCP/IP) - [IPsec] - [IPsec Setting] (Настройка IPsec)
[IKEv2]

Настройка на елемент	Препоръчителна настройка
[Encryption Algorithm] (Алгоритъм за криптиране)	[AES-CBC] ([256]/[192 and 256] (192 и 256)/[All] (Всички))
[Authentication Algorithm] (Алгоритъм за автентикация)	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 и 384)/[384 and 512] (384 и 512)/[All] (Всички)), [AES-XCBC]
[Diffie-Hellman Group] (Група Diffie-Hellman)	[Group 14] (Група 14), [Group 19] (Група 19)

[SA]

Настройка на елемент	Препоръчителна настройка
[Encapsulation Mode] (Режим на капсулиране)	[Tunnel] (Тунел), [Transport] (Транспорт)
[Security Protocol] (Протокол за сигурност)	[ESP]
[Key Exchange Method] (Метод за обмен на ключове)	[IKEv2]
[Authentication Method] (Метод за автентикация)	[Digital Signature] (Дигитален подпис)

Настройка на елемент	Препоръчителна настройка
[ESP Encryption Algorithm] (ESP Алгоритъм за криптиране)	[AES-GCM] ([256]/[192 and 256] (192 и 256))/[All] (Всички), [AES-GCM-64] ([256]/[192 and 256] (192 и 256))/[All] (Всички), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 и 256))/[All] (Всички)
[Perfect Forward Secrecy] (Перфектна сигурност на предаването)	ON (ВКЛ)
[Diffie-Hellman Group(IKEv2)] (Група Diffie-Hellman (IKEv2)) - [Priority1-4] (Приоритет 1-4)	[Group 14] (Група 14), [Group 19] (Група 19)

2.2.5 S/MIME

Ако използвате опционалния S/MIME при изпращане на електронна поща, можете да криптирате съдържанието на електронната поща, за да предотвратите подслушване и да потвърдите самоличността на изпращача с електронен подпис. Това е ефективна мярка срещу фалшифициране и фишинг измами.

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [E-mail Setting] (Настройка на имейл) - [S/MIME]

Настройка на елемент	Препоръчителна настройка
[Digital Signature] (Дигитален подпис)	[Always add signature] (Винаги добавяй подпис)
[Digital Signature Type] (Тип дигитален подпис)	[SHA-256]
[E-Mail Text Encrypt. Method] (Метод за криптиране на текста на имейл)	[AES-256]

3 Задаване на валидирането на сертификата

Когато използвате TLS криптирана комуникация, за да намалите въздействието на атаки тип "man-in-the-middle" (MITM), препоръчваме да използвате валидиране на сертификата. За елементите за валидиране препоръчваме да активирате минимум датата на изтичане на сертификата и веригата.

Ако се направи опит за свързване с наследена среда, която не разполага с функция за валидиране на сертификат, рискът от атаки тип MITM се увеличава. Препоръчваме ви да го използвате в защитена мрежова среда.

Валидирането на сертификата от страна на MFP се препоръчва при следните клиентски функции на MFP. За подробности относно местата за настройка вижте следните раздели.

POP, SMTP (Стартиране TLS/SMTP през SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, Отдалечен панел

Съвети

Валидирането на сертификата от страна клиента във връзка с MFP се препоръчва при следните клиентски функции на MFP.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / Отдалечен панел), TCP порт

3.1 POP

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [E-mail Setting] (Настройка на имейл) - [E-mail RX (POP)] (Имейл RX (POP))

Настройка на елемент	Препоръчителна настройка
[Certificate Verification Level Settings] (Настройки на нивото на проверка на сертификата)	[Expiration Date] (Дата на изтичане на срока на валидност): ON (ВКЛ) [Chain] (Верига): ON (ВКЛ)

3.2 SMTP

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [E-mail Setting] (Настройка на имейл) - [E-mail TX] (Имейл TX)

Настройка на елемент	Препоръчителна настройка
[Certificate Verification Level Settings] (Настройки на нивото на проверка на сертификата)	[Expiration Date] (Дата на изтичане на срока на валидност): ON (ВКЛ) [Chain] (Верига): ON (ВКЛ)

3.3 IEEE802.1X Auth

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [IEEE802.1X Authentication Setting] (Настройка IEEE802.1X автентикация)
[IEEE802.1X Authentication Setting] (Настройка IEEE802.1X автентикация) - [Supplicant Setting] (Настройка на заявител)

Настройка на елемент	Препоръчителна настройка
[Certificate Verification Level Settings] (Настройки на нивото на проверка на сертификата)	[Expiration Date] (Дата на изтичане на срока на валидност): ON (ВКЛ) [Chain] (Верига): ON (ВКЛ)

3.4 IPsec

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [TCP/IP Setting] (Настройка на TCP/IP) - [IPsec] - [Enable IPsec] (Активиране на IPsec)

Настройка на елемент	Препоръчителна настройка
[Certificate Verification Level Settings] (Настройки на нивото на проверка на сертификата)	[Expiration Date] (Дата на изтичане на срока на валидност): [Confirm] (Потвърждаване) [Chain] (Верига): [Confirm] (Потвърждаване)

Съвети

В [IPsec Setting] (Настройка IPsec), първо регистрирайте елементи [IKE], [SA], [Peer], и [Protocol Setting] (Настройка протокол).

3.5 WebDAVClient

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [WebDAV Settings] (Настройки на WebDAV) - [WebDAV Client Settings] (Настройки на клиент на WebDAV)

Настройка на елемент	Препоръчителна настройка
[Certificate Verification Level Settings] (Настройки на нивото на проверка на сертификата)	[Expiration Date] (Дата на изтичане на срока на валидност): ON (ВКЛ) [Chain] (Верига): ON (ВКЛ)

3.6 LDAP

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [LDAP Setting] (Настройка LDAP) - [Setting Up LDAP] (Настройване на LDAP)

Настройка на елемент	Препоръчителна настройка
[Certificate Verification Level Settings] (Настройки на нивото на проверка на сертификата)	[Expiration Date] (Дата на изтичане на срока на валидност): ON (ВКЛ) [Chain] (Верига): ON (ВКЛ)

3.7 DPWS

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [DPWS Settings] (Настройки на DPWS) - [DPWS Common Settings] (Общи настройки на DPWS)

Настройка на елемент	Препоръчителна настройка
[Certificate Verification Level Settings] (Настройки на нивото на проверка на сертификата)	[Expiration Date] (Дата на изтичане на срока на валидност): ON (ВКЛ) [Chain] (Верига): ON (ВКЛ)

3.8 OpenAPI

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [OpenAPI Setting] (Настройка на OpenAPI) - [OpenAPI Setting] (Настройка на OpenAPI)

Настройка на елемент	Препоръчителна настройка
[Certificate Verification Level Settings] (Настройки на нивото на проверка на сертификата)	[Expiration Date] (Дата на изтичане на срока на валидност): ON (ВКЛ) [Chain] (Верига): ON (ВКЛ)

3.9 RemotePanel (Отдалечен панел)

Местоположение на настройката: [Utility] (Помощна програма) - [Administrator] (Администратор) - [Network] (Мрежа) - [Remote Panel Settings] (Настройки на отдалечен панел) - [Remote Panel Client Settings] (Настройки на клиент на отдалечен панел)

Настройка на елемент	Препоръчителна настройка
[Certificate Verification Level Settings] (Настройки на нивото на проверка на сертификата)	[Expiration Date] (Дата на изтичане на срока на валидност): ON (ВКЛ) [Chain] (Верига): ON (ВКЛ)

4 Допълнителна информация за сигурността

4.1 Препоръка за най-добри практики

Препоръчваме алгоритмите за криптиране, които ще се използват, да отговарят на настройките на най-добрите практики, препоръчани в Насоките на Агенцията на ЕС за киберсигурност (EUCC) относно криптирането и на механизма, одобрен от Работната група по криптография SOGIS.

По-долу е представен списък на алгоритмите за криптиране и дължините на ключовете, препоръчани в Насоките на EUCC за криптиране в на механизма, одобрен от Работната група по криптография SOGIS.

Елемент	Препоръчителна настройка
Алгоритми за криптиране	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Дължина на ключа за криптиране	RSA: 2048 бита или повече ECC: 256 бита или повече AES: 256 бита

Съвети

За повече подробности вижте най-новите насоки на EUCC за криптиране и механизма на работната група на SOGIS.

4.2 Предпазни мерки за комуникация с наследени системи

Предполага се, че за комуникация с наследените системи се използват следните протоколи и версии.

Използването на наследени настройки увеличава рисковете за сигурността, затова ги използвайте в защитена мрежова среда.

Елемент	Наследени настройки
Протокол	SLP FTP SMB (3.0 или по-ранна версия, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Зависи от сървъра/Изкл.) DPWS TCP порт
Алгоритми за криптиране	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Дължина на ключа за криптиране	RSA: 1024 бита или по-малко ECC: 160 бита или по-малко AES: 128 бита или по-малко DES: 56 бита 3DES: 112 бита

Наследени настройки на IPsec

[IKEv1]

Настройка на елемент	Наследени настройки
[Encryption Algorithm] (Алгоритъм за криптиране)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 и 192))
[Authentication Algorithm] (Алгоритъм за автентикация)	Не се използва
[Diffie-Hellman Group] (Група Diffie-Hellman)	[Group 1] (Група 1), [Group 2] (Група 2), [Group 5] (Група 5)

[IKEv2]

Настройка на елемент	Наследени настройки
[Encryption Algorithm] (Алгоритъм за криптиране)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 и 192))
[Authentication Algorithm] (Алгоритъм за автентикация)	Не се използва
[Diffie-Hellman Group] (Група Diffie-Hellman)	[Group 1] (Група 1), [Group 2] (Група 2), [Group 5] (Група 5)

[SA]

Настройка на елемент	Наследени настройки
[Key Exchange Method] (Метод за обмен на ключове)	[IKEv1]
[Authentication Method] (Метод за автентикация)	[Digital Signature] (Дигитален подпис)

Настройка на елемент	Наследени настройки
[ESP Encryption Algorithm] (ESP Алгоритъм за криптиране)	[3DES-CBC] ([128]/[192]/[128 and 192] (128 и 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 и 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 и 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 и 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 и 192))
[Perfect Forward Secrecy] (Перфектна сигурност на предаването)	ON (ВКЛ)
[Diffie-Hellman Group(IKEv1)] (Група Diffie-Hellman (IKEv1))	[Group 1] (Група 1), [Group 2] (Група 2), [Group 5] (Група 5)

4.3 Мрежови интерфейси и услуги, налични още при доставката от завода

Вид услуга	Протокол	Номер на порт
DHCP	UDP	68
HTTP сървър	TCP	80
Услуга за имена NETBIOS	UDP	137
Услуга NETBIOS Datagram Service	UDP	138
SNMP	UDP	161
HTTP сървър през SSL / IPP през SSL	TCP	443
LPD Отпечатване	TCP	515
DHCPv6 клиент	UDP	546
IPP Отпечатване	TCP	631
MFPIF	UDP	1900
Уеб услуга	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-tool)	TCP	8091
RAW Отпечатване	TCP	9100
RAW Отпечатване	TCP	9112
RAW Отпечатване	TCP	9113
RAW Отпечатване	TCP	9114
RAW Отпечатване	TCP	9115
RAW Отпечатване	TCP	9116
OpenAPI	TCP	50001

4.4 За валидирането на входни данни

За броя на символите, които трябва да се въведат за мрежови настройки, и т.н., вижте всеки от елементите за настройка в Ръководството за потребителя.

В зависимост от кодирането на езика, максималният допустим вход (данни, записани в MFP) за елементи, които поддържат многобайтови символи, може да бъде три пъти повече от броя на символите.

Doporučení pro zabezpečená síťová zařízení

Obsah

1 Nastavení filtrování IP adres

1.1	Filtrování IP adres	1-3
1.2	Rychlé filtrování IP	1-3

2 Nastavení šifrované komunikace

2.1	Šifrování TLS	2-4
2.1.1	HTTP (Web Connection) (webové připojení)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP	2-5
2.1.4	OpenAPI	2-5
2.1.5	RemotePanel	2-5
2.1.6	DPWS	2-5
2.1.7	POP	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	Soket TCP	2-6
2.2	Ostatní šifrování	2-7
2.2.1	SMBServer	2-7
	SMB Encryption (Šifrování složky SMB)	2-7
	Podpis SMB	2-7
2.2.2	SMBCClient	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Nastavení ověření certifikátu

3.1	POP	3-10
3.2	SMTP	3-10
3.3	IEEE802.1X Auth	3-10
3.4	IPsec	3-11
3.5	WebDAVClient	3-11
3.6	LDAP	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	RemotePanel	3-12

4 Další informace o zabezpečení

4.1	Doporučení osvědčených postupů	4-13
4.2	Opatření pro komunikaci se staršími systémy	4-14
	Starší nastavení IPsec	4-14
4.3	Síťová rozhraní a služby dostupné od dodání z výroby	4-15
4.4	O ověřování vstupu	4-16



O této příručce

Tato příručka popisuje informace a nastavení, které umožňují bezpečné používání zařízení.

Při připojování zařízení k síti je používejte v prostředí chráněném bránou firewall. Doporučujeme také nastavit soukromou IP adresu pro IP adresu počítače.

Nastavení soukromé IP adresy umožňuje přístup k zařízení pouze uživatelům v místní síti, například v interní síti LAN, a zabraňuje neoprávněnému přístupu zvenčí.

Pokud potřebujete používat globální IP adresu, nezapomeňte toto zařízení nainstalovat do brány firewall.

1 Nastavení filtrování IP adres

Filtrování IP adres je funkce, která omezuje zařízení, která mohou přistupovat k vašemu zařízení v závislosti na IP adrese. Správným nastavením této funkce můžete omezit přístup z neautorizovaných zařízení.

Funkci filtrování IP adres zařízení lze nastavit jedním z následujících dvou způsobů.

1.1 Filtrování IP adres

Ručně zadejte rozsah IP adres, ke kterým chcete povolit nebo zakázat přístup.

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [TCP/IP Setting] (Nastavení TCP/IP) - [IP Address Filtering] (Filtrování IP adres)



Tipy

Nastavte povolené nebo zakázané IP adresy tak, aby vyhovovaly vašemu prostředí.

1.2 Rychlé filtrování IP

Rozsah IP adres, které umožňují přístup, je automaticky nastaven na základě IP adresy a masky podsítě nastavené v zařízení.

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [TCP/IP Setting] (Nastavení TCP/IP) - [Quick IP Filtering] (Rychlé filtrování IP)

Doporučené nastavení: [Synchronize IP Address] (Synchronizace IP adresy)/[Synchronize Subnet Mask] (Synchronizace masky podsítě) *

* Vyberte si jednu z nich podle svého prostředí.

2 Nastavení šifrované komunikace

Doporučujeme používat následující šifrovanou komunikaci, abyste zabránili odposlechu dat, manipulaci s daty a únosu relace.

2.1 Šifrování TLS

Pro snížení rizika zranitelnosti doporučujeme nakonfigurovat následující nastavení.

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Security] (Zabezpečení) - [PKI Settings] (Nastavení PKI) - [Enable SSL Version] (Povolit verzi SSL)

Položka nastavení	Doporučené nastavení
[Mode using SSL/TLS] (Režim pomocí SSL/TLS)	[Admin. Mode and User Mode] (Režim správce a uživatelský režim)
[SSL/TLS Version Setting] (Nastavení verze SSL/TLS)	TLS1.2 TLS1.3 (nekompatibilní s IEEE802.1X)
[Encryption Strength] (Síla šifrování)	AES-256

Prvotní certifikát je instalován ve výrobním závodě. Pokud potřebujete jiný certifikát, zaregistrujte si nový na následujícím místě.

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Security] (Zabezpečení) - [PKI Settings] (Nastavení PKI) - [Device Certificate Setting] (Nastavení certifikátu zařízení)

Položka nastavení	Doporučené nastavení
[Encryption Key Type] (Typ šifrovacího klíče)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Šifrování TLS je podporováno pro následující protokoly a služby. Podrobné informace o nastavení umístění najdete v následujících částech.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (spustit TLS, SMTP přes SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- Soket TCP

2.1.1 HTTP (Web Connection) (webové připojení)

Pokud povolíte [Enable SSL Version] (Povolit verzi SSL), režim komunikace se automaticky přepne na šifrovanou komunikaci TLS (HTTPS).

2.1.2 WebDAVServer

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [WebDAV Settings] (Nastavení WebDAV) - [WebDAV Server Settings] (Nastavení serveru WebDAV)

Položka nastavení	Doporučené nastavení
[Nastavení SSL]	[SSL Only] (Pouze SSL)

2.1.3 IPP

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [HTTP Server Settings] (Nastavení serveru HTTP)

Položka nastavení	Doporučené nastavení
[IPP-SSL Settings] (Nastavení IPP-SSL)	[SSL Only] (Pouze SSL)

2.1.4 OpenAPI

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [OpenAPI Setting] (Nastavení OpenAPI) - [OpenAPI Setting] (Nastavení OpenAPI)

Položka nastavení	Doporučené nastavení
[SSL/Port Settings] (Nastavení SSL/portu)	[SSL Only] (Pouze SSL)

2.1.5 RemotePanel

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [Remote Panel Settings] (Nastavení dálkového ovládání) - [Remote Panel Server Settings] (Nastavení serveru dálkového ovládání)

Položka nastavení	Doporučené nastavení
[Port No. (SSL)]	[50443]



Tipy

Pokud povolíte [Enable SSL Version] (Povolit verzi SSL), komunikace se automaticky přepne na šifrovanou komunikaci TLS. Zadejte číslo portu.

2.1.6 DPWS

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [DPWS Settings] (Nastavení DPWS) - [DPWS Common Settings] (Obecná nastavení DPWS)

Položka nastavení	Doporučené nastavení
[Nastavení SSL]	ZAP

2.1.7 POP

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [E-mail Setting] (Nastavení e-mailu) - [E-mail RX (POP)]

Položka nastavení	Doporučené nastavení
[Povolit SSL]	ZAP

2.1.8 SMTP

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [E-mail Setting] (Nastavení e-mailu) - [E-mail TX (SMTP)]

Položka nastavení	Doporučené nastavení
[Nastavení SSL/TLS]	[SMTP přes SSL]

2.1.9 IEEE802.1X Auth

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Sít) - [IEEE802.1X Authentication Setting] (Nastavení ověřování IEEE802.1X) - [IEEE802.1X Authentication Setting] (Nastavení ověřování IEEE802.1X) - [Supplicant Setting] (Nastavení žádajícího)

Položka nastavení	Doporučené nastavení
[Typ EAP]	Zvolte [EAP-TLS], [EAP-TTLS] nebo [PEAP].

2.1.10 LDAP

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Sít) - [LDAP Setting] (Nastavení LDAP) - [Setting Up LDAP] (Nastavení LDAP)

Položka nastavení	Doporučené nastavení
[Povolit SSL]	ZAP

2.1.11 Soket TCP

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Sít) - [TCP Socket Setting] (Nastavení soketu TCP)

Položka nastavení	Doporučené nastavení
[Use SSL/TLS] (Použít SSL/TLS)	ZAP

2.2 Ostatní šifrování

Pro snížení rizika zranitelnosti doporučujeme nakonfigurovat následující nastavení. Podrobné informace o nastavení všech funkcí najdete v následujících částech.

Funkce	Doporučené nastavení
SMBServer	SMB Encryption (Šifrování složky SMB), SMB Signature (Podpis SMB)
SMBClient	Kerberos Authentication (Ověřování Kerberos)
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	ZAP

2.2.1 SMBServer

Použití šifrování SMB a podpisu SMB může snížit následující bezpečnostní rizika.

- Odposlouchávání: Zlomyslná třetí strana může zachytit komunikaci a ukrást osobní nebo důvěrné informace.
- Manipulace s daty: Existuje riziko, že obsah komunikace může být narušen útokem MITM (Man-In-The-Middle Attack).
- Spoofing: Pokud jsou ověřovací údaje odcizeny, může se třetí strana vydávat za legitimního uživatele a získat neoprávněný přístup.
- Únik informací: Nešifrovanou komunikaci lze snadno zachytit, zejména ve veřejných sítích Wi-Fi, což zvyšuje riziko úniku osobních údajů a informací o kreditních kartách.

SMB Encryption (Šifrování složky SMB)

Předpoklady

- Vytvořte veřejnou schránku. Nakonfigurujte také nastavení automatického přenosu souborů z veřejné schránky a jejich ukládání do složky SMB.
- Zadejte heslo pro schránku.

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Box] (Schránka) - [User Box List] (Seznam schránek)

Položka nastavení	Doporučené nastavení
[SMB Communication Encryption] (Šifrování komunikace SMB)	[Encrypt] (Šifrování)

Podpis SMB

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [SMB Setting] (Nastavení SMB) - [SMB Server Settings] (Nastavení serveru SMB)

Položka nastavení	Doporučené nastavení
[SMB security Signature Setting] (Nastavení podpisu zabezpečení SMB)	[Vyžadováno]

2.2.2 SMBClient

Ověřování Kerberos využívá silnou šifrovací technologii, která výrazně snižuje riziko odcizení pověření během procesu ověřování. Zajišťuje také integritu dat a zabraňuje manipulaci s daty mezi odesílatelem a příjemcem i útokům na přenos NTLM.

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [SMB Setting] (Nastavení SMB) - [Client Setting] (Nastavení klienta)

Položka nastavení	Doporučené nastavení
[SMB Authentication Setting] (Nastavení ověřování SMB)	[Kerberos]

2.2.3 SNMP

Nastavte šifrování pomocí SNMPv3. Pokud přidáte také nastavení ověřování, můžete bezpečnost ještě zvýšit. Bezpečnostní rizika jsou přibližně stejná jako u SMB.

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [SNMP Setting] (Nastavení SNMP)

Položka nastavení	Doporučené nastavení
[Nastavení SNMP]	[SNMP v3(IP)]
[Algoritmus šifrování]	[AES-128]
[Způsob ověření]	Zvolte [SHA-256], [SHA-384] nebo [SHA-512].

2.2.4 IPsec

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [TCP/IP Setting] (Nastavení TCP/IP) - [IPsec] - [IPsec Setting] (Nastavení IPsec)

[IKEv2]

Položka nastavení	Doporučené nastavení
[Algoritmus šifrování]	[AES-CBC] ([256]/[192 a 256]/[Vše])
[Algoritmus ověření]	[SHA-2] ([256]/[384]/[512]/[256 a 384]/[384 a 512]/[Vše]), [AES-XCBC]
[Skupina Diffie-Hellman]	[Group 14] (Skupina 14), [Group 19] (Skupina 19)

[SA]

Položka nastavení	Doporučené nastavení
[Zapouzdřený režim]	[Tunnel] (Tunel), [Transport] (Doprava)
[Bezpečnostní protokol]	[ESP]
[Metoda výměny klíče]	[IKEv2]
[Způsob ověření]	[Digitální podpis]
[Algoritmus šifrování ESP]	[AES-GCM] ([256]/[192 a 256]/[Vše]), [AES-GCM-64] ([256]/[192 a 256]/[Vše]), [ENC_NULL_AES_GMAC] ([256]/[192 a 256]/[Vše])
[Úplné dopředné utajení]	ZAP
[Diffie-Hellman Group(IKEv2)] (Skupina Diffie-Hellman [IKEv2]) - [Priority1-4] (Priorita 1-4)	[Group 14] (Skupina 14), [Group 19] (Skupina 19)

2.2.5 S/MIME

Pokud při odesílání e-mailů používáte volitelný protokol S/MIME, můžete obsah e-mailu šifrovat, abyste zabránili odposlechu, a ověřit totožnost odesílatele pomocí elektronického podpisu. Jedná se o účinné opatření proti podvodům typu spoofing a phishing.

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [E-mail Setting] (Nastavení e-mailu) - [S/MIME]

Položka nastavení	Doporučené nastavení
[Digitální podpis]	[Always add signature] (Vždy přidejte podpis)
[Typ digitálního podpisu]	[SHA-256]
[E-Mail Text Encrypt. Method] (Způsob šifrování textu e-mailu)	[AES-256]

3 Nastavení ověření certifikátu

Při použití šifrované komunikace TLS pro snížení dopadu útoků typu man-in-the-middle doporučujeme použít ověření certifikátu. U položek ověřování doporučujeme povolit alespoň datum vypršení platnosti certifikátu a řetězec.

Při pokusu o připojení k staršímu prostředí, které nemá funkci ověřování certifikátů, se zvyšuje riziko útoku typu man-in-the-middle. Doporučujeme jej používat v zabezpečeném síťovém prostředí.

Ověření certifikátu na straně multifunkčního zařízení se doporučuje v následujících funkcích klienta multifunkčního zařízení. Podrobné informace o nastavení umístění najdete v následujících částech. POP, SMTP (spustit TLS/SMTP přes SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel

Tipy

Ověření certifikátu na straně klienta připojeného k multifunkčnímu zařízení se doporučuje v následujících funkcích serveru multifunkčního zařízení.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), soket TCP

3.1 POP

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [E-mail Setting] (Nastavení e-mailu) - [E-mail RX (POP)]

Položka nastavení	Doporučené nastavení
[Certificate Verification Level Settings] (Nastavení úrovně ověření certifikátu)	[Expiration Date] (Datum vypršení platnosti): ZAP [Chain] (Řetěz): ZAP

3.2 SMTP

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [E-mail Setting] (Nastavení e-mailu) - [E-mail TX (SMTP)]

Položka nastavení	Doporučené nastavení
[Certificate Verification Level Settings] (Nastavení úrovně ověření certifikátu)	[Expiration Date] (Datum vypršení platnosti): ZAP [Chain] (Řetěz): ZAP

3.3 IEEE802.1X Auth

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Síť) - [IEEE802.1X Authentication Setting] (Nastavení ověřování IEEE802.1X) - [IEEE802.1X Authentication Setting] (Nastavení ověřování IEEE802.1X) - [Supplicant Setting] (Nastavení žádajícího)

Položka nastavení	Doporučené nastavení
[Certificate Verification Level Settings] (Nastavení úrovně ověření certifikátu)	[Expiration Date] (Datum vypršení platnosti): ZAP [Chain] (Řetěz): ZAP

3.4 IPsec

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Sít) - [TCP/IP Setting] (Nastavení TCP/IP) - [IPsec] - [Enable IPsec] (Povolit IPsec)

Položka nastavení	Doporučené nastavení
[Certificate Verification Level Settings] (Nastavení úrovně ověření certifikátu)	[Expiration Date] (Datum vypršení platnosti): [Potvrzení] [Chain] (Řetěz): [Potvrzení]



Tipy

In [IPsec Setting] (Nastavení IPsec) zaregistrujte předem položky [IKE], [SA], [Peer] a [Protocol Setting] (Nastavení protokolu).

3.5 WebDAVClient

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Sít) - [WebDAV Settings] (Nastavení WebDAV) - [WebDAV Client Settings] (Nastavení klienta WebDAV)

Položka nastavení	Doporučené nastavení
[Certificate Verification Level Settings] (Nastavení úrovně ověření certifikátu)	[Expiration Date] (Datum vypršení platnosti): ZAP [Chain] (Řetěz): ZAP

3.6 LDAP

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Sít) - [LDAP Setting] (Nastavení LDAP) - [Setting Up LDAP] (Nastavení LDAP)

Položka nastavení	Doporučené nastavení
[Certificate Verification Level Settings] (Nastavení úrovně ověření certifikátu)	[Expiration Date] (Datum vypršení platnosti): ZAP [Chain] (Řetěz): ZAP

3.7 DPWS

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Sít) - [DPWS Settings] (Nastavení DPWS) - [DPWS Common Settings] (Obecná nastavení DPWS)

Položka nastavení	Doporučené nastavení
[Certificate Verification Level Settings] (Nastavení úrovně ověření certifikátu)	[Expiration Date] (Datum vypršení platnosti): ZAP [Chain] (Řetěz): ZAP

3.8 OpenAPI

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Sít) - [OpenAPI Setting] (Nastavení OpenAPI) - [OpenAPI Setting] (Nastavení OpenAPI)

Položka nastavení	Doporučené nastavení
[Certificate Verification Level Settings] (Nastavení úrovně ověření certifikátu)	[Expiration Date] (Datum vypršení platnosti): ZAP [Chain] (Řetěz): ZAP

3.9 RemotePanel

Nastavení umístění: [Utility] (Nástroje) - [Administrator] (Správce) - [Network] (Sít) - [Remote Panel Settings] (Nastavení dálkového ovládání) - [Remote Panel Client Settings] (Nastavení klienta dálkového ovládání)

Položka nastavení	Doporučené nastavení
[Certificate Verification Level Settings] (Nastavení úrovně ověření certifikátu)	[Expiration Date] (Datum vypršení platnosti): ZAP [Chain] (Řetěz): ZAP

4 Další informace o zabezpečení

4.1 Doporučení osvědčených postupů

Doporučujeme, aby šifrovací algoritmy, které se mají použít, odpovídaly nastavení osvědčených postupů doporučených v pokynech EUCC pro kryptografii a v pokynech SOGIS-Agreed-Cryptographic-Mechanisms.

Níže je uveden seznam šifrovacích algoritmů a délek klíčů doporučených v pokynech EUCC pro kryptografii a SOGIS-Agreed-Cryptographic-Mechanisms.

Položka	Doporučené nastavení
Šifrovací algoritmy	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Délka šifrovacího klíče	RSA: 2 048 bitů nebo více ECC: 256 bitů nebo více AES: 256 bitů

Tipy

Podrobnosti naleznete v nejnovějších pokynech EUCC pro kryptografii a v SOGIS-Agreed-Cryptographic-Mechanisms.

4.2 Opatření pro komunikaci se staršími systémy

Pro komunikaci se staršími systémy se předpokládá použití následujících protokolů a verzí.

Používání starších nastavení zvyšuje bezpečnostní rizika, proto je používejte v zabezpečeném síťovém prostředí.

Položka	Starší nastavení
Protokol	SLP FTP SMB (3.0 nebo starší verze, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Závísí na serveru/VYP) DPWS TCPsocket
Šifrovací algoritmy	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Délka šifrovacího klíče	RSA: 1 024 bitů nebo méně ECC: 160 bitů nebo méně AES: 128 bitů nebo méně DES: 56 bitů 3DES: 112 bitů

Starší nastavení IPsec

[IKEv1]

Položka nastavení	Starší nastavení
[Algoritmus šifrování]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 a 192])
[Algoritmus ověření]	Není použito
[Skupina Diffie-Hellman]	[Group 1] (Skupina 1), [Group 2] (Skupina 2), [Group 5] (Skupina 5)

[IKEv2]

Položka nastavení	Starší nastavení
[Algoritmus šifrování]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 a 192])
[Algoritmus ověření]	Není použito
[Skupina Diffie-Hellman]	[Group 1] (Skupina 1), [Group 2] (Skupina 2), [Group 5] (Skupina 5)

[SA]

Položka nastavení	Starší nastavení
[Metoda výměny klíče]	[IKEv1]
[Způsob ověření]	[Digitální podpis]
[Algoritmus šifrování ESP]	[3DES-CBC] ([128]/[192]/[128 a 192]) [AES-CTR] ([128]/[192]/[128 a 192]) [AES-GCM] ([128]/[192]/[128 a 192]) [AES-GCM-64] ([128]/[192]/[128 a 192]) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 a 192])
[Úplné dopředné utajení]	ZAP
[Diffie-Hellman Group(IKEv1)] (Skupina Diffie-Hellman [IKEv1])	[Group 1] (Skupina 1), [Group 2] (Skupina 2), [Group 5] (Skupina 5)

4.3 Síťová rozhraní a služby dostupné od dodání z výroby

Typ služby	Protokol	Číslo portu
DHCP	UDP	68
Server HTTP	TCP	80
Název služby NETBIOS	UDP	137
Datagramová služba NETBIOS	UDP	138
SNMP	UDP	161
Server HTTP přes SSL / IPP přes SSL	TCP	443
LPD Print (tisk LPD)	TCP	515
Klient DHCPv6	UDP	546
IPP Print (tisk IPP)	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (nástroj IWS)	TCP	8091
RAW Print (tisk RAW)	TCP	9100
RAW Print (tisk RAW)	TCP	9112
RAW Print (tisk RAW)	TCP	9113
RAW Print (tisk RAW)	TCP	9114
RAW Print (tisk RAW)	TCP	9115
RAW Print (tisk RAW)	TCP	9116
OpenAPI	TCP	50001

4.4 O ověřování vstupu

Počet znaků, které je třeba zadat pro síťová nastavení atd., najdete u jednotlivých položek nastavení v uživatelské příručce.

V závislosti na kódování jazyka může být maximální povolený vstup (data uložená v multifunkčním zařízení) pro položky, které podporují vícebajtové znaky, trojnásobný.

Anbefalinger til opnåelse af sikre enheder med netværksforbindelse

Indholdsfortegnelse

1 Sådan indstilles IP-filtrering

1.1	IP-filtrering.....	1-3
1.2	Hurtig IP-filtrering	1-3

2 Indstilling af krypteret kommunikation

2.1	TLS-kryptering	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel (Fjernbetjeningspanel)	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP-stik	2-6
2.2	Anden kryptering	2-7
2.2.1	SMBServer	2-7
	SMB Encryption (Kryptering af SMB-mappe)	2-7
	SMB Signature (SMB-signatur).....	2-7
2.2.2	SMBClient (SMBKlient)	2-8
2.2.3	SNMP	2-8
2.2.4	IPSEC.....	2-8
2.2.5	S/MIME	2-9

3 Indstilling af certifikatvalidering

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPSEC	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	RemotePanel (Fjernbetjeningspanel).....	3-12

4 Yderligere sikkerhedsinformation

4.1	Anbefaling af best practice	4-13
4.2	Forholdsregler for kommunikation med ældre systemer	4-14
	Ældre indstillinger for IPsec	4-14
4.3	Netværksinterfaces og -tjenester til rådighed fra fabrikkens levering	4-16
4.4	Om validering af input	4-17



Om denne vejledning

Denne vejledning beskriver oplysninger og indstillinger, der muliggør sikker brug af enheder.

Når du tilslutter maskinen til netværket, så brug den i et miljø, der er beskyttet af en firewall. Vi anbefaler også, at du indstiller en privat IP-adresse som maskinens IP-adresse.

Indstilling af en privat IP-adresse giver kun brugere på et lokalt netværk, f.eks. et internt LAN, adgang til maskinen og forhindrer uautoriseret adgang udefra.

Hvis du har behov for at bruge en global IP-adresse, skal du installere denne maskine bag en firewall.

1 Sådan indstilles IP-filtrering

IP-filtrering er en funktion, der begrænser enheder, der kan få adgang til maskinen via IP-adressen. Du kan begrænse adgang for uautoriserede enheder ved at indstille denne funktion korrekt.

Funktionen med IP-filtrering på denne maskine kan indstilles med en af de to følgende metoder.

1.1 IP-filtrering

Manuel angivelse af det IP-adresseinterval, som tillader eller nægter adgang.

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [TCP/IP Setting] (TCP/IP-indstilling) - [IP Address Filtering] (IP-filtrering)



Indstil IP-adresserne, som tillader eller nægter adgang, så de passer til dit miljø.

1.2 Hurtig IP-filtrering

Intervallet af IP-adresser, der tillader adgang, baseres automatisk på den IP-adresse og den undernetmaske, der er oprettet i denne maskine.

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [TCP/IP Setting] (TCP/IP-indstilling) - [Quick IP Filtering] (Hurtig IP-filtrering)

Anbefalede indstillinger: [Synchronize IP Address] (Synkroniser IP-adresse)/[Synchronize Subnet Mask] (Synkroniser undernetmaske)*

* Vælg en af dem, der passer til dit miljø.

2 Indstilling af krypteret kommunikation

Vi anbefaler, at du bruger følgende krypterede kommunikation for at forhindre dataaflytning, datamanipulation og session hijacking.

2.1 TLS-kryptering

Vi anbefaler, at du konfigurerer følgende indstillinger for at reducere sikkerhedsrisikoen.

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Security] (Sikkerhed) - [PKI Settings] (PKI-indstillinger) - [Enable SSL Version] (Aktivér SSL-version)

Indstillingselement	Anbefalet indstilling
[Mode using SSL/TLS]	[Admin. Mode and User Mode] (Administratortilstand og Brugertilstand)
[SSL/TLS Version Setting] (Indstilling af SSL/TLS-version)	TLS1.2 TLS1.3 (IEEE802.1X inkompatibel)
[Encryption Strength] (Krypteringsstyrke)	AES-256

Startcertifikatet installeres på fabrikken. Hvis du har brug for et andet certifikat, skal du registrere et nyt på den følgende placering.

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Security] (Sikkerhed) - [PKI Settings] (PKI-indstillinger) - [Device Certificate Setting] (Certifikatindstilling for enhed)

Indstillingselement	Anbefalet indstilling
[Encryption Key Type] (Krypteringsnøgletype)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

TLS-krypteringen understøttes for følgende protokoller og tjenester. For detaljer om indstilling af placeringer, se de følgende afsnit.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP-stik

2.1.1 HTTP (Web Connection)

Hvis du aktiverer [Enable SSL Version] (Aktivér SSL-version), skifter kommunikationstilstanden automatisk til TLS-krypteret kommunikation (HTTPS).

2.1.2 WebDAVServer

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [WebDAV Settings] (WebDAV-indstillinger) - [WebDAV Server Settings] (WebDAV-serverindstillinger)

Indstillingselement	Anbefalet indstilling
[SSL Settings] (SSL-indstillinger)	[Kun SSL]

2.1.3 IPP

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [HTTP Server Settings] (HTTP-serverindstillinger)

Indstillingselement	Anbefalet indstilling
[IPP-SSL Settings] (IPP-SSL-indstillinger)	[Kun SSL]

2.1.4 OpenAPI

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [OpenAPI Setting] (OpenAPI-indstilling) - [OpenAPI Setting] (OpenAPI-indstilling)

Indstillingselement	Anbefalet indstilling
[SSL/Port Settings] (SSL/Port-indstillinger)	[Kun SSL]

2.1.5 RemotePanel (Fjernbetjeningspanel)

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [Remote Panel Settings] (Indstillinger for fjernbetjeningspanel) - [Remote Panel Server Settings] (Serverindstillinger for fjernbetjeningspanel)

Indstillingselement	Anbefalet indstilling
[Port No.(SSL)] (Portnummer (SSL))	[50443]



Tips

Hvis du aktiverer [Enable SSL Version] (Aktivér SSL-version), skifter kommunikationen automatisk til TLS-krypteret tilstand. Angiv et portnummer.

2.1.6 DPWS

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [DPWS Settings] (DPWS-indstillinger) - [DPWS Common Settings] (Almindelig indstilling af DPWS)

Indstillingselement	Anbefalet indstilling
[SSL Settings] (SSL-indstillinger)	TIL

2.1.7 POP

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [E-mail Setting] (E-mailindstilling) - [E-mail RX (POP)] (E-mailmodtagelse (POP))

Indstillingselement	Anbefalet indstilling
[Enable SSL] (Aktivér SSL)	TIL

2.1.8 SMTP

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [E-mail Setting] (E-mailindstilling) - [E-mail TX (SMTP)] (E-mail-TX (SMTP))

Indstillingselement	Anbefalet indstilling
[SSL/TLS-indstillinger]	[SMTP over SSL]

2.1.9 IEEE802.1X Auth

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [IEEE802.1X Authentication Setting] (IEEE802.1X-identifikationsindstilling) - [IEEE802.1X Authentication Setting] (IEEE802.1X-identifikationsindstilling) - [Supplicant Setting] (Supplikantindstilling)

Indstillingselement	Anbefalet indstilling
[EAP-Type] (EAP-type)	Vælg [EAP-TLS], [EAP-TTLS] eller [PEAP].

2.1.10 LDAP

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [LDAP Setting] (LDAP-indstilling) - [Setting Up LDAP] (Opsætning af LDAP)

Indstillingselement	Anbefalet indstilling
[Enable SSL] (Aktivér SSL)	TIL

2.1.11 TCP-stik

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [TCP Socket Setting] (Indstilling for TCP-stik)

Indstillingselement	Anbefalet indstilling
[Use SSL/TLS] (Brug SSL/TLS)	TIL

2.2 Anden kryptering

Vi anbefaler, at du konfigurerer følgende indstillinger for at reducere sikkerhedsrisikoen. For detaljer om indstillingerne af de enkelte funktioner, se de følgende afsnit.

Funktion	Anbefalet indstilling
SMBServer	SMB Encryption (SMB-kryptering), SMB Signature (SMB-signatur)
SMBClient (SMBKlient)	Kerberos Authentication (Kerberos-identifikation)
SNMP	SNMPv3
IPSEC	IKEv2
S/MIME	TIL

2.2.1 SMBServer

Brug af kryptering af SMB-mappe og SMB-signatur kan reducere de følgende sikkerhedsrisici.

- Aflytning: En ondsindet tredjepart kan opsnappe kommunikation og stjæle personlige eller fortrolige oplysninger.
- Datamanipulation: Der er en risiko for, at kommunikationsindholdet kan blive manipuleret af et Man-In-The-Middle-angreb (MITM).
- Forfalskning: Hvis der stjæles identifikationsinformation, kan en tredjepart udgive sig for at være en legitim bruger for at få uautoriseret adgang.
- Informationslæk: Ukrypteret kommunikation kan nemt opsnappes, især på offentlige Wi-Fi-netværk, hvilket øger risikoen for, at personlige oplysninger og kreditkortoplysninger lækkes.

SMB Encryption (Kryptering af SMB-mappe)

Forberedelser

- Opret en offentlig brugerboks. Konfigurer også indstillingen til automatisk at overføre filer fra den offentlige brugerboks og gemme dem i SMB-mappen.
- Angiv adgangskoden til brugerboksen.

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Box] (Brugerboks) - [User Box List] (Brugerboksliste)

Indstillingselement	Anbefalet indstilling
[SMB Communication Encryption] (SMB-kommunikations-kryptering)	[Encrypt] (Krypter)

SMB Signature (SMB-signatur)

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [SMB Setting] (SMB-indstilling) - [SMB Server Settings] (SMB-serverindstillinger)

Indstillingselement	Anbefalet indstilling
[SMB security Signature Setting] (Indstilling af SMB-sikkerhedssignatur)	[Påkrævet]

2.2.2 SMBClient (SMBKlient)

Kerberos-identifikationen bruger stærk krypteringsteknologi, hvilket væsentligt reducerer risikoen for, at legitimationsoplysninger bliver stjålet under identifikationsprocessen. Den sikrer også dataintegritet og forhindrer datamanipulation mellem afsender og modtager samt NTLM Relay-angreb.

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [SMB Setting] (SMB-indstilling) - [Client Setting] (Klientindstilling)

Indstillingselement	Anbefalet indstilling
[SMB Authentication Setting] (SMB-identifikationsindstilling)	[Kerberos]

2.2.3 SNMP

Indstil krypteringen ved at bruge SNMPv3. Hvis identifikationsindstillingen også tilføjes, kan du øge sikkerheden yderligere. Sikkerhedsrisiciene er nogenlunde de samme som med SMB.

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [SNMP Setting] (SNMP-indstilling)

Indstillingselement	Anbefalet indstilling
[SNMP-indstilling]	[SNMP v3(IP)]
[Krypteringsalgoritme]	[AES-128]
[Identifikationsmetode]	Vælg [SHA-256], [SHA-384] eller [SHA-512].

2.2.4 IPSEC

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [TCP/IP Setting] (TCP/IP-indstilling) [IPsec] - [IPsec Setting] (IPsec-indstilling)

[IKEv2]

Indstillingselement	Anbefalet indstilling
[Krypteringsalgoritme]	[AES-CBC] ([256]/[192 and 256] (192 og 256)/[All] (Alle))
[Algoritme til autentic.]	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 og 384)/[384 and 512] (384 og 512)/[All] (Alle)), [AES-XCBC]
[Diffie-Hellman Group]	[Group 14] (Gruppe 14), [Group 19] (Gruppe 19)

[SA]

Indstillingselement	Anbefalet indstilling
[Indkapslingstilstand]	[Tunnel], [Transport]
[Sikkerhedsprotokol]	[ESP]
[Key Exchange Method] (Nøgleudvekslingsmetode)	[IKEv2]
[Identifikationsmetode]	[Digital signatur]
[ESP-krypteringsalgoritme]	[AES-GCM] ([256]/[192 and 256] (192 og 256)/[All] (Alle)), [AES-GCM-64] ([256]/[192 and 256] (192 og 256)/[All] (Alle)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 og 256)/[All] (Alle))
[Perf.viders. sikkerhed]	TIL
[Diffie-Hellman Group(IKEv2)] (Diffie-Hellman-gruppe(IKEv2)) - [Priority1-4] (Prioritet 1-4)	[Group 14] (Gruppe 14), [Group 19] (Gruppe 19)

2.2.5 S/MIME

Hvis du bruger valgfri S/MIME, når du sender e-mail, kan du kryptere e-mailindholdet for at forhindre aflytning og efterprøve afsenderens identitet med en elektronisk signatur. Dette er en effektiv foranstaltning mod forfalskning og phishing-svindel.

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [E-mail Setting] (E-mail-indstilling) - [S/MIME]

Indstillingselement	Anbefalet indstilling
[Digital signatur]	[Always add signature] (Tilføj altid signatur)
[Digital Signature Type] (Type af digital signatur)	[SHA-256]
[E-Mail Text Encrypt. Method] (Metode til kryptering af e-mailtekst)	[AES-256]

3 Indstilling af certifikatvalidering

Når du bruger TLS-krypteret kommunikation for at reducere effekten af man-in-the-middle-angreb, anbefaler vi, at du bruger certifikatvalidering. For valideringselementer anbefaler vi, at du som minimum aktiverer certifikatets udløbsdato og -kæde.

Hvis det forsøges at oprette forbindelse til et ældre miljø, der ikke har en certifikatvalideringsfunktion, øges risikoen for man-in-the-middle-angreb. Vi anbefaler, at du bruger den i et sikkert netværksmiljø.

Certifikatvalidering på MFP-siden anbefales i de følgende MFP-klientfunktioner. For detaljer om indstilling af placeringer, se de følgende afsnit.

POP, SMTP (Start TLS/SMTP over SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel



Tips

Certifikatvalidering på klientsiden, der er tilsluttet MFP, anbefales i de følgende MFP-serverfunktioner. HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP-stik

3.1 POP

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [E-mail Setting] (E-mail-indstilling) - [E-mail RX (POP)] (E-mailmodtagelse (POP))

Indstillingselement	Anbefalet indstilling
[Indstilling af certifikat-godk.niveau]	[Expiration Date] (Udløbsdato): TIL [Chain] (Kæde): TIL

3.2 SMTP

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [E-mail Setting] (E-mailindstilling) - [E-mail TX (SMTP)] (E-mail-TX (SMTP))

Indstillingselement	Anbefalet indstilling
[Indstilling af certifikat-godk.niveau]	[Expiration Date] (Udløbsdato): TIL [Chain] (Kæde): TIL

3.3 IEEE802.1X Auth

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [IEEE802.1X Authentication Setting] (IEEE802.1X-identifikationsindstilling) - [IEEE802.1X Authentication Setting] (IEEE802.1X-identifikationsindstilling) - [Supplicant Setting] (Supplikantindstilling)

Indstillingselement	Anbefalet indstilling
[Indstilling af certifikat-godk.niveau]	[Expiration Date] (Udløbsdato): TIL [Chain] (Kæde): TIL

3.4 IPSEC

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [TCP/IP Setting] (TCP/IP-indstilling) [IPsec] - [Enable IPsec] (Aktivér IPsec)

Indstillingselement	Anbefalet indstilling
[Indstilling af certifikat-godk.niveau]	[Expiration Date] (Udløbsdato): [Status] [Chain] (Kæde): [Status]



Tips

I [IPsec Setting] (IPsec-indstilling) bør du registrere elementerne [IKE], [SA], [Peer] og [Protocol Setting] (Protokolindstilling) på forhånd.

3.5 WebDAVClient

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [WebDAV Settings] (WebDAV-indstillinger) - [WebDAV Client Settings] (WebDAV-klientindstillinger)

Indstillingselement	Anbefalet indstilling
[Indstilling af certifikat-godk.niveau]	[Expiration Date] (Udløbsdato): TIL [Chain] (Kæde): TIL

3.6 LDAP

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [LDAP Setting] (LDAP-indstilling) - [Setting Up LDAP] (Opsætning af LDAP)

Indstillingselement	Anbefalet indstilling
[Indstilling af certifikat-godk.niveau]	[Expiration Date] (Udløbsdato): TIL [Chain] (Kæde): TIL

3.7 DPWS

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [DPWS Settings] (DPWS-indstillinger) - [DPWS Common Settings] (Almindelig indstilling af DPWS)

Indstillingselement	Anbefalet indstilling
[Indstilling af certifikat-godk.niveau]	[Expiration Date] (Udløbsdato): TIL [Chain] (Kæde): TIL

3.8 OpenAPI

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [OpenAPI Setting] (OpenAPI-indstilling) - [OpenAPI Setting] (OpenAPI-indstilling)

Indstillingselement	Anbefalet indstilling
[Indstilling af certifikat-godk.niveau]	[Expiration Date] (Udløbsdato): TIL [Chain] (Kæde): TIL

3.9 RemotePanel (Fjernbetjeningspanel)

Indstillingssted: [Utility] (Hjælpeprogram) - [Administrator] - [Network] (Netværk) - [Remote Panel Settings] (Indstillinger for fjernbetjeningspanel) - [Remote Panel Client Settings] (Klientindstillinger for fjernbetjeningspanel)

Indstillingselement	Anbefalet indstilling
[Indstilling af certifikatgodk.niveau]	[Expiration Date] (Udløbsdato): TIL [Chain] (Kæde): TIL

4 Yderligere sikkerhedsinformation

4.1 Anbefaling af best practice

Vi anbefaler, at de anvendte krypteringsalgoritmer er i overensstemmelse med de anbefalede best practice-indstillinger i EUCC Guidelines on Cryptography (Vejledning til valg af kryptografi) og SOGIS-Agreed-Cryptographic-Mechanisms (SOGIS-aftalte-kryptografiske-mekanismer).

Nedenfor finder du en liste over de krypteringsalgoritmer og nøglelængder, der anbefales af EUCC Guidelines on Cryptography og SOGIS-Agreed-Cryptographic-Mechanisms.

Emne	Anbefalet indstilling
Krypteringsalgoritmer	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Krypteringsnøglelængde	RSA: 2048 bit eller derover ECC: 256 bit eller derover AES: 256 bit



Tips

For detaljer, se de nyeste EUCC Guidelines on Cryptography og SOGIS-Agreed-Cryptographic-Mechanisms.

4.2 Forholdsregler for kommunikation med ældre systemer

Følgende protokoller og versioner antages at blive brugt til kommunikation med ældre systemer.

Brug af ældre indstillinger øger sikkerhedsrisikoen, så brug dem i et sikkert netværksmiljø.

Emne	Ældre indstillinger
Protokol	SLP FTP SMB (3.0 eller ældre version, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Depend on Server/OFF) DPWS TCPSocket
Krypteringsalgoritmer	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Krypteringsnøglelængde	RSA: 1024 bit eller derunder ECC: 160 bit eller derunder AES: 128 bit eller derunder DES: 56 bit 3DES: 112 bit

Ældre indstillinger for IPsec

[IKEv1]

Indstillingselement	Ældre indstillinger
[Krypteringsalgoritme]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 og 192))
[Algoritme til autentic.]	Anvendes ikke
[Diffie-Hellman Group]	[Group 1] (Gruppe 1), [Group 2] (Gruppe 2), [Group 5] (Gruppe 5)

[IKEv2]

Indstillingselement	Ældre indstillinger
[Krypteringsalgoritme]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 og 192))
[Algoritme til autentic.]	Anvendes ikke
[Diffie-Hellman Group]	[Group 1] (Gruppe 1), [Group 2] (Gruppe 2), [Group 5] (Gruppe 5)

[SA]

Indstillingselement	Ældre indstillinger
[Key Exchange Method] (Nøgleudvekslingsmetode)	[IKEv1]
[Identifikationsmetode]	[Digital signatur]
[ESP-krypteringsalgoritme]	[3DES-CBC] ([128]/[192]/[128 and 192] (128 og 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 og 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 og 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 og 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 og 192))
[Perf.viders. sikkerhed]	TIL

Indstillingselement	Ældre indstillinger
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellman-gruppe(IKEv1))	[Group 1] (Gruppe 1), [Group 2] (Gruppe 2), [Group 5] (Gruppe 5)

4.3 Netværksinterfaces og -tjenester til rådighed fra fabrikkens levering

Tjenestetype	Protokol	Portnummer
DHCP	UDP	68
HTTP Server (HTTP-server)	TCP	80
NETBIOS Name Service (NETBIOS-navnetjeneste)	UDP	137
NETBIOS Datagram Service (NETBIOS-datagramtjeneste)	UDP	138
SNMP	UDP	161
HTTP Server over SSL / IPP over SSL	TCP	443
LPD Print (LPD-udskrift)	TCP	515
DHCPv6 Client (DHCPv6-klient)	UDP	546
IPP Print (IPP-udskrift)	TCP	631
MFPIF	UDP	1900
WebService (IT-tjeneste på webserver)	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-tool) (HTTP (IWS-redskab))	TCP	8091
RAW Print (RAW-udskrift)	TCP	9100
RAW Print (RAW-udskrift)	TCP	9112
RAW Print (RAW-udskrift)	TCP	9113
RAW Print (RAW-udskrift)	TCP	9114
RAW Print (RAW-udskrift)	TCP	9115
RAW Print (RAW-udskrift)	TCP	9116
OpenAPI	TCP	50001

4.4 Om validering af input

For antallet af tegn, der skal indtastes for netværksindstillinger osv. henvises til hvert af indstillings-elementerne i brugervejledningen.

Afhængigt af sprogets kodning kan det maksimalt tilladte input (data gemt i MFP) for elementer, der understøtter multibyte-tegn, være tre gange antallet af tegn.

Συστάσεις για ασφαλείς συσκευές σε δίκτυο

Πίνακας Περιεχομένων

1 Ρύθμιση φιλτραρίσματος διεύθυνσης IP

1.1	Φιλτράρισμα διεύθυνσης IP.....	1-3
1.2	Γρήγορο φιλτράρισμα IP.....	1-3

2 Ρύθμιση της κρυπτογραφημένης επικοινωνίας

2.1	Κρυπτογράφηση TLS.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	Υποδοχή TCP.....	2-6
2.2	Άλλη κρυπτογράφηση	2-7
2.2.1	SMBServer	2-7
	Κρυπτογράφηση SMB	2-7
	Υπογραφή SMB	2-7
2.2.2	SMBCClient	2-8
2.2.3	SNMP	2-8
2.2.4	IPSEC.....	2-8
2.2.5	S/MIME	2-9

3 Ρύθμιση της επαλήθευσης πιστοποιητικού

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPSEC	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-12
3.9	RemotePanel	3-12

4 Πρόσθετες πληροφορίες ασφαλείας

4.1	Σύσταση βέλτιστων πρακτικών.....	4-13
4.2	Μέτρα προφύλαξης για την επικοινωνία με υφιστάμενα συστήματα	4-14
	Υφιστάμενες ρυθμίσεις IPsec	4-14
4.3	Οι διεπαφές και οι υπηρεσίες δικτύου είναι διαθέσιμες κατά την εργοστασιακή αποστολή.	4-16
4.4	Σχετικά με την επαλήθευση καταχωρίσεων.....	4-17



Πληροφορίες για αυτό το βιβλίο χειρισμού

Στο παρόν βιβλίο χειρισμού περιγράφονται πληροφορίες και ρυθμίσεις που επιτρέπουν την ασφαλή χρήση συσκευών.

Όταν συνδέετε αυτό το μηχάνημα στο δίκτυο, χρησιμοποιήστε το σε περιβάλλον που προστατεύεται με τείχος προστασίας. Συνιστούμε επίσης να ορίζετε μια ιδιωτική διεύθυνση IP για τη διεύθυνση IP του μηχανήματος.

Η ρύθμιση μιας ιδιωτικής διεύθυνσης IP επιτρέπει μόνο στους χρήστες ενός δικτύου τοπικής περιοχής, όπως ένα εσωτερικό LAN, να αποκτούν πρόσβαση στο μηχάνημα και να αποφεύγεται η μη εξουσιοδοτημένη πρόσβαση από έξω.

Αν θέλετε να χρησιμοποιήσετε μια γενική διεύθυνση IP, να διασφαλίζετε ότι το μηχάνημα είναι εγκατεστημένο μέσα σε τείχος προστασίας.

1 Ρύθμιση φιλτραρίσματος διεύθυνσης IP

Το φιλτράρισμα διεύθυνσης IP είναι μια λειτουργία που περιορίζει τις συσκευές που μπορούν να έχουν πρόσβαση στο μηχάνημα, ανάλογα με τη διεύθυνση IP. Μπορείτε να απαγορεύσετε την πρόσβαση σε μη εξουσιοδοτημένες συσκευές ρυθμίζοντας σωστά αυτή τη λειτουργία.

Η λειτουργία φιλτραρίσματος διεύθυνσης IP του μηχανήματος μπορεί να οριστεί με τις παρακάτω δύο μεθόδους.

1.1 Φιλτράρισμα διεύθυνσης IP

Καθορίστε χειροκίνητα το εύρος διευθύνσεων IP που επιτρέπουν ή δεν επιτρέπουν την πρόσβαση.

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [TCP/IP Setting] (Ρύθμιση TCP/IP) - [IP Address Filtering] (Φιλτράρισμα διεύθυνσης IP)



Συμβουλές

Ορίστε τις διευθύνσεις IP που γίνονται ή δεν γίνονται αποδεκτές ανάλογα με το εκάστοτε περιβάλλον.

1.2 Γρήγορο φιλτράρισμα IP

Το εύρος των διευθύνσεων IP που επιτρέπουν την πρόσβαση ορίζεται αυτόματα με βάση τη διεύθυνση IP και τη μάσκα υποδικτύου αυτού του μηχανήματος.

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [TCP/IP Setting] (Ρύθμιση TCP/IP) - [Quick IP Filtering] (Γρήγορο φιλτράρισμα IP)

Προτεινόμενες ρυθμίσεις: [Synchronize IP Address] (Συγχρονισμός διεύθυνσης IP)/[Synchronize Subnet Mask] (Συγχρονισμός μάσκας υποδικτύου) *

* Επιλέξτε ό,τι ταιριάζει στο εκάστοτε περιβάλλον.

2 Ρύθμιση της κρυπτογραφημένης επικοινωνίας

Προτείνουμε να χρησιμοποιείτε την παρακάτω κρυπτογραφημένη επικοινωνία, ώστε να αποτρέπεται η υποκλοπή δεδομένων, η παραποίηση δεδομένων και η υφαρπαγή περιόδου λειτουργίας.

2.1 Κρυπτογράφηση TLS

Προτείνουμε να διαμορφώνετε τις παρακάτω ρυθμίσεις για να μειώνεται ο κίνδυνος ευπαθειών.

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Security] (Ασφάλεια) - [PKI Settings] (Ρυθμίσεις PKI) - [Enable SSL Version] (Ενεργοποίηση έκδοσης SSL)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Mode using SSL/TLS] (Λειτουργία με χρήση SSL/TLS)	[Admin. Mode and User Mode] (Λειτουργία διαχειριστή και λειτουργία χρήστη)
[SSL/TLS Version Setting] (Ρύθμιση έκδοσης SSL/TLS)	TLS1.2 TLS1.3 (IEEE802.1X μη συμβατό)
[Encryption Strength] (Ισχύς κρυπτογράφησης)	AES-256

Το αρχικό πιστοποιητικό εγκαθίσταται στο εργοστάσιο. Αν χρειάζεστε διαφορετικό πιστοποιητικό, δηλώστε ένα νέο στην παρακάτω τοποθεσία.

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Security] (Ασφάλεια) - [PKI Settings] (Ρυθμίσεις PKI) - [Device Certificate Setting] (Ρύθμιση πιστοποιητικού συσκευής)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Encryption Key Type] (Τύπος κλειδιού κρυπτογράφησης)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Η κρυπτογράφηση TLS υποστηρίζεται για τα παρακάτω πρωτόκολλα και υπηρεσίες. Για λεπτομέρειες σχετικά με τη ρύθμιση τοποθεσιών, ανατρέξτε στις παρακάτω ενότητες.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP μέσω SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- Υποδοχή TCP

2.1.1 HTTP (Web Connection)

Αν ενεργοποιήσετε την επιλογή [Enable SSL Version] (Ενεργοποίηση έκδοσης SSL), η λειτουργία επικοινωνίας τίθεται αυτόματα στην κρυπτογραφημένη επικοινωνία TLS (HTTPS).

2.1.2 WebDAVServer

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [WebDAV Settings] (Ρυθμίσεις WebDAV) - [WebDAV Server Settings] (Ρυθμίσεις διακομιστή WebDAV)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[SSL Settings] (Ρυθμίσεις SSL)	[SSL Only] (SSL μόνο)

2.1.3 IPP

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [HTTP Server Settings] (Ρυθμίσεις διακομιστή HTTP)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[IPP-SSL Settings] (Ρυθμίσεις IPP-SSL)	[SSL Only] (SSL μόνο)

2.1.4 OpenAPI

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [OpenAPI Setting] (Ρύθμιση OpenAPI) - [OpenAPI Setting] (Ρύθμιση OpenAPI)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[SSL/Port Settings] (Ρυθμίσεις SSL/θύρας)	[SSL Only] (SSL μόνο)

2.1.5 RemotePanel

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [Remote Panel Settings] (Ρυθμίσεις απομακρυσμένου πίνακα) - [Remote Panel Server Settings] (Ρυθμίσεις διακομιστή απομακρυσμένου πίνακα)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Port No.(SSL)] (Αρ. θύρας (SSL))	[50443]



Συμβουλές

Αν ενεργοποιήσετε την επιλογή [Enable SSL Version] (Ενεργοποίηση έκδοσης SSL), η λειτουργία επικοινωνίας τίθεται αυτόματα στην κρυπτογραφημένη λειτουργία TLS. Καθορίστε έναν αριθμό θύρας.

2.1.6 DPWS

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [DPWS Settings] (Ρυθμίσεις DPWS) - [DPWS Common Settings] (Κοινές ρυθμίσεις DPWS)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[SSL Settings] (Ρυθμίσεις SSL)	ON

2.1.7 POP

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [E-mail Setting] (Ρύθμιση e-mail) - [E-mail RX (POP)]

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Enable SSL] (Ενεργοποίηση SSL)	ON

2.1.8 SMTP

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [E-mail Setting] (Ρύθμιση e-mail) - [E-mail TX (SMTP)]

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[SSL/TLS Settings] (Ρυθμίσεις SSL/TLS)	[SMTP over SSL] (SMTP μέσω SSL)

2.1.9 IEEE802.1X Auth

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [IEEE802.1X Authentication Setting] (Ρύθμιση επαλήθευσης IEEE802.1X) - [IEEE802.1X Authentication Setting] (Ρύθμιση επαλήθευσης IEEE802.1X) - [Supplicant Setting] (Ρύθμιση αίτησης άδειας πρόσβασης)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[EAP-Type] (Τύπος EAP)	Επιλέξτε [EAP-TLS], [EAP-TTLS] ή [PEAP].

2.1.10 LDAP

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [LDAP Setting] (Ρύθμιση LDAP) - [Setting Up LDAP] (Ρυθμίστε το LDAP)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Enable SSL] (Ενεργοποίηση SSL)	ON

2.1.11 Υποδοχή TCP

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [TCP Socket Setting] (Ρύθμιση υποδοχής TCP)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Use SSL/TLS] (Χρήση SSL/TLS)	ON

2.2 Άλλη κρυπτογράφηση

Προτείνουμε να διαμορφώνετε τις παρακάτω ρυθμίσεις για να μειώνεται ο κίνδυνος ευπαθειών. Για λεπτομέρειες σχετικά με τις ρυθμίσεις κάθε λειτουργίας, ανατρέξτε στις παρακάτω ενότητες.

Λειτουργία	Προτεινόμενη ρύθμιση
SMBServer	Κρυπτογράφηση SMB, υπογραφή SMB
SMBClient	Επαλήθευση Kerberos
SNMP	SNMPv3
IPSEC	IKEv2
S/MIME	ON

2.2.1 SMBServer

Η χρήση της κρυπτογράφησης SMB και της υπογραφής SMB μπορεί να μειώσει τους παρακάτω κινδύνους ασφαλείας.

- Υποκλοπές: Ένα κακόβουλο τρίτο μέρος μπορεί να υφαρπάξει επικοινωνίες και να υποκλέψει προσωπικές ή εμπιστευτικές πληροφορίες.
- Παραποίηση δεδομένων: Υπάρχει κίνδυνος παραποίησης περιεχομένων επικοινωνίας μέσω επίθεσης Man-In-The-Middle (MITM).
- Πλαστογράφηση: Αν γίνει υποκλοπή στοιχείων επαλήθευσης, ένα τρίτο μέρος θα μπορούσε να εμφανιστεί ως έγκυρος χρήστης για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση.
- Διαρροή πληροφοριών: Είναι εύκολη η παραβίαση μη κρυπτογραφημένων πληροφοριών, ειδικά σε δημόσια δίκτυα Wi-Fi και έτσι αυξάνεται ο κίνδυνος διαρροής προσωπικών πληροφοριών και πληροφοριών πιστωτικών καρτών.

Κρυπτογράφηση SMB

Προϋποθέσεις

- Δημιουργήστε μια δημόσια θυρίδα χρήστη. Επίσης, διαμορφώστε τη ρύθμιση ώστε να εκτελείται αυτόματη μεταφορά των αρχείων από τη δημόσια θυρίδα χρήστη και να αποθηκεύονται στον φάκελο SMB.
- Ορίστε κωδικό πρόσβασης για τη θυρίδα χρήστη.

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Box] (Θυρίδα) - [User Box List] (Λίστα θυρίδων χρηστών)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[SMB Communication Encryption] (Κρυπτογράφηση επικοινωνίας SMB)	[Encrypt] (Κρυπτογράφηση)

Υπογραφή SMB

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [SMB Setting] (Ρύθμιση SMB) - [SMB Server Settings] (Ρυθμίσεις διακομιστή SMB)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[SMB security Signature Setting] (Ρύθμιση υπογραφής ασφαλείας SMB)	[Required] (Απαιτείται)

2.2.2 SMBClient

Στην επαλήθευση Kerberos χρησιμοποιείται ισχυρή τεχνολογία κρυπτογράφησης, μειώνοντας σημαντικά τον κίνδυνο υποκλοπής διαπιστευτηρίων κατά τη διάρκεια της διαδικασίας επαλήθευσης. Διασφαλίζει επίσης την ακεραιότητα των δεδομένων, αποτρέποντας την παραποίηση δεδομένων μεταξύ του δέκτη και του αποστολέα καθώς και επιθέσεων επαναληπτικής εκτέλεσης NTLM.

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [SMB Setting] (Ρύθμιση SMB) - [Client Setting] (Ρύθμιση υπολογιστή-πελάτη)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[SMB Authentication Setting] (Ρύθμιση επαλήθευσης SMB)	[Kerberos]

2.2.3 SNMP

Ορίστε την κρυπτογράφηση χρησιμοποιώντας το SNMPv3. Αν προστεθεί επίσης η ρύθμιση επαλήθευσης, μπορείτε να ενισχύσετε περαιτέρω την ασφάλεια. Οι κίνδυνοι ασφαλείας είναι περίπου ίδιοι με το SMB.

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [SNMP Setting] (Ρύθμιση SNMP)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[SNMP Setting] (Ρύθμιση SNMP)	[SNMP v3(IP)]
[Encryption Algorithm] (Αλγόριθμος κρυπτογράφησης)	[AES-128]
[Authentication Method] (Μέθοδος επαλήθευσης)	Επιλέξτε [SHA-256], [SHA-384] ή [SHA-512].

2.2.4 IPSEC

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [TCP/IP Setting] (Ρύθμιση TCP/IP) - [IPsec] - [IPsec Setting] (Ρύθμιση IPsec)

[IKEv2]

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Encryption Algorithm] (Αλγόριθμος κρυπτογράφησης)	[AES-CBC] ([256]/[192 and 256] (192 και 256)/[All] (Όλα))
[Authentication Algorithm] (Αλγόριθμος επαλήθευσης)	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 και 384)/[384 and 512] (384 και 512)/[All] (Όλα)), [AES-XCBC]
[Diffie-Hellman Group] (Ομάδα Diffie-Hellman)	[Group 14] (Ομάδα 14), [Group 19] (Ομάδα 19)

[SA]

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Encapsulation Mode] (Λειτουργία ενθυλάκωσης)	[Tunnel] (Τούνελ), [Transport] (Μεταφορά)
[Security Protocol] (Πρωτόκολλο ασφαλείας)	[ESP]
[Key Exchange Method] (Μέθοδος αλλαγής κλειδιού)	[IKEv2]
[Authentication Method] (Μέθοδος επαλήθευσης)	[Digital Signature] (Ψηφιακή υπογραφή)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[ESP Encryption Algorithm] (Αλγόριθμος κρυπτογράφησης ESP)	[AES-GCM] ([256]/[192 and 256] (192 και 256)/[All] (Όλα)), [AES-GCM-64] ([256]/[192 and 256] (192 και 256)/[All] (Όλα)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 και 256)/[All] (Όλα))
[Perfect Forward Secrecy] (Απόλυτη μελλοντική μυστικότητα)	ON
[Diffie-Hellman Group(IKEv2)] (Ομάδα Diffie-Hellman (IKEv2)) - [Priority1-4] (Προτεραιότητα 1-4)	[Group 14] (Ομάδα 14), [Group 19] (Ομάδα 19)

2.2.5 S/MIME

Αν χρησιμοποιήσετε το προαιρετικό S/MIME κατά την αποστολή e-mail, μπορείτε να κρυπτογραφήσετε τα περιεχόμενα του e-mail για την αποφυγή υποκλοπών και την επαλήθευση της ταυτότητας του αποστολέα με ηλεκτρονική υπογραφή. Αυτό είναι ένα αποτελεσματικό μέτρο έναντι πλαστογραφήσεων και παραπλανητικών μηνυμάτων υποκλοπής στοιχείων.

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [E-mail Setting] (Ρύθμιση e-mail) - [S/MIME]

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Digital Signature] (Ψηφιακή υπογραφή)	[Always add signature] (Πάντα προσθήκη υπογραφής)
[Digital Signature Type] (Τύπος ψηφιακής υπογραφής)	[SHA-256]
[E-Mail Text Encrypt. Method] (Μέθοδος κρυπτογράφησης κειμένου e-mail)	[AES-256]

3 Ρύθμιση της επαλήθευσης πιστοποιητικού

Κατά τη χρήση κρυπτογραφημένης επικοινωνίας TLS για τη μείωση του φαινομένου επιθέσεων τύπου man-in-the-middle, προτείνουμε να χρησιμοποιείτε επαλήθευση πιστοποιητικού. Για τα στοιχεία επαλήθευσης, συνιστούμε να ενεργοποιείτε κατ' ελάχιστον την ημερομηνία λήξης και την αλυσίδα πιστοποιητικών.

Αν γίνει μια απόπειρα σύνδεσης σε υφιστάμενο περιβάλλον που δεν έχει λειτουργία επαλήθευσης πιστοποιητικού, αυξάνεται ο κίνδυνος επιθέσεων τύπου man-in-the-middle. Προτείνουμε να χρησιμοποιείτε το σύστημά σας σε ασφαλές περιβάλλον δικτύου.

Η επαλήθευση πιστοποιητικού στην πλευρά MFP προτείνεται στις παρακάτω λειτουργίες υπολογιστή-πελάτη MFP. Για λεπτομέρειες σχετικά με τη ρύθμιση τοποθεσιών, ανατρέξτε στις παρακάτω ενότητες. POP, SMTP (Start TLS/SMTP μέσω SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel



Συμβουλές

Η επαλήθευση πιστοποιητικού στην πλευρά υπολογιστή-πελάτη που συνδέεται στο MFP προτείνεται στις παρακάτω λειτουργίες διακομιστή MFP. HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), υποδοχή TCP

3.1 POP

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [E-mail Setting] (Ρύθμιση e-mail) - [E-mail RX (POP)]

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Certificate Verification Level Settings] (Ρυθμίσεις επιπέδου επαλήθευσης πιστοποιητικού)	[Expiration Date] (Ημερομηνία λήξης): ON [Chain] (Αλυσίδα): ON

3.2 SMTP

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [E-mail Setting] (Ρύθμιση e-mail) - [E-mail TX (SMTP)]

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Certificate Verification Level Settings] (Ρυθμίσεις επιπέδου επαλήθευσης πιστοποιητικού)	[Expiration Date] (Ημερομηνία λήξης): ON [Chain] (Αλυσίδα): ON

3.3 IEEE802.1X Auth

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [IEEE802.1X Authentication Setting] (Ρύθμιση επαλήθευσης IEEE802.1X) - [IEEE802.1X Authentication Setting] (Ρύθμιση επαλήθευσης IEEE802.1X) - [Supplicant Setting] (Ρύθμιση αίτησης άδειας πρόσβασης)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Certificate Verification Level Settings] (Ρυθμίσεις επιπέδου επαλήθευσης πιστοποιητικού)	[Expiration Date] (Ημερομηνία λήξης): ON [Chain] (Αλυσίδα): ON

3.4 IPSEC

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [TCP/IP Setting] (Ρύθμιση TCP/IP) - [IPsec] - [Enable IPsec] (Ενεργοποίηση IPsec)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Certificate Verification Level Settings] (Ρυθμίσεις επιπέδου επαλήθευσης πιστοποιητικού)	[Expiration Date] (Ημερομηνία λήξης): [Confirm] (Επιβεβαίωση) [Chain] (Αλυσίδα): [Confirm] (Επιβεβαίωση)



Συμβουλές

Στο σημείο [IPsec Setting] (Ρύθμιση IPsec), καταχωρίστε εκ των προτέρων στοιχεία [IKE], [SA], [Peer] (Ομότιμο) και [Protocol Setting] (Ρύθμιση πρωτοκόλλου).

3.5 WebDAVClient

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [WebDAV Settings] (Ρυθμίσεις WebDAV) - [WebDAV Client Settings] (Ρυθμίσεις υπολογιστή-πελάτη WebDAV)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Certificate Verification Level Settings] (Ρυθμίσεις επιπέδου επαλήθευσης πιστοποιητικού)	[Expiration Date] (Ημερομηνία λήξης): ON [Chain] (Αλυσίδα): ON

3.6 LDAP

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [LDAP Setting] (Ρύθμιση LDAP) - [Setting Up LDAP] (Ρυθμίστε το LDAP)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Certificate Verification Level Settings] (Ρυθμίσεις επιπέδου επαλήθευσης πιστοποιητικού)	[Expiration Date] (Ημερομηνία λήξης): ON [Chain] (Αλυσίδα): ON

3.7 DPWS

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [DPWS Settings] (Ρυθμίσεις DPWS) - [DPWS Common Settings] (Κοινές ρυθμίσεις DPWS)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Certificate Verification Level Settings] (Ρυθμίσεις επιπέδου επαλήθευσης πιστοποιητικού)	[Expiration Date] (Ημερομηνία λήξης): ON [Chain] (Αλυσίδα): ON

3.8 OpenAPI

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [OpenAPI Setting] (Ρύθμιση OpenAPI) - [OpenAPI Setting] (Ρύθμιση OpenAPI)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Certificate Verification Level Settings] (Ρυθμίσεις επιπέδου επαλήθευσης πιστοποιητικού)	[Expiration Date] (Ημερομηνία λήξης): ON [Chain] (Αλυσίδα): ON

3.9 RemotePanel

Ρύθμιση τοποθεσίας: [Utility] (Λειτουργία) - [Administrator] (Διαχειριστής) - [Network] (Δίκτυο) - [Remote Panel Settings] (Ρυθμίσεις απομακρυσμένου πίνακα) - [Remote Panel Client Settings] (Ρυθμίσεις προγράμματος-πελάτη απομακρυσμένου πίνακα)

Στοιχείο ρύθμισης	Προτεινόμενη ρύθμιση
[Certificate Verification Level Settings] (Ρυθμίσεις επιπέδου επαλήθευσης πιστοποιητικού)	[Expiration Date] (Ημερομηνία λήξης): ON [Chain] (Αλυσίδα): ON

4 Πρόσθετες πληροφορίες ασφαλείας

4.1 Σύσταση βέλτιστων πρακτικών

Προτείνουμε οι αλγόριθμοι κρυπτογράφησης που θα χρησιμοποιηθούν να συμμορφώνονται με τις ρυθμίσεις βέλτιστων πρακτικών που προτείνονται από το Ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (EUCC) και τους συμφωνηθέντες κρυπτογραφικούς μηχανισμούς SOGIS (SOGIS-Agreed-Cryptographic-Mechanisms).

Πιο κάτω ακολουθεί μια λίστα των αλγόριθμων κρυπτογράφησης και των μηκών κλειδιών που προτείνονται από το Ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (EUCC) και τους συμφωνηθέντες κρυπτογραφικούς μηχανισμούς SOGIS (SOGIS-Agreed-Cryptographic-Mechanisms).

Στοιχείο	Προτεινόμενη ρύθμιση
Αλγόριθμοι κρυπτογράφησης	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Μήκος κλειδιού κρυπτογράφησης	RSA: 2048 bit ή περισσότερο ECC: 256 bit ή περισσότερο AES: 256 bit



Συμβουλές

Για λεπτομέρειες, ανατρέξτε στο Ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (EUCC) και τους συμφωνηθέντες κρυπτογραφικούς μηχανισμούς SOGIS (SOGIS-Agreed-Cryptographic-Mechanisms).

4.2 Μέτρα προφύλαξης για την επικοινωνία με υφιστάμενα συστήματα

Θεωρείται ότι χρησιμοποιούνται τα παρακάτω πρωτόκολλα και εκδόσεις για την επικοινωνία με υφιστάμενα συστήματα.

Η χρήση υφιστάμενων ρυθμίσεων αυξάνει τους κινδύνους ασφαλείας και συνεπώς αυτά τα συστήματα πρέπει να χρησιμοποιούνται σε ασφαλές περιβάλλον δικτύου.

Στοιχείο	Υφιστάμενες ρυθμίσεις
Πρωτόκολλο	SLP FTP SMB (3.0 ή προηγούμενη έκδοση, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Ανάλογα με τον διακομιστή/OFF) DPWS Υποδοχή TCP
Αλγόριθμοι κρυπτογράφησης	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Μήκος κλειδιού κρυπτογράφησης	RSA: 1024 bit ή λιγότερο ECC: 160 bit ή λιγότερο AES: 128 bit ή λιγότερο DES: 56 bit 3DES: 112 bit

Υφιστάμενες ρυθμίσεις IPsec

[IKEv1]

Στοιχείο ρύθμισης	Υφιστάμενες ρυθμίσεις
[Encryption Algorithm] (Αλγόριθμος κρυπτογράφησης)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 και 192))
[Authentication Algorithm] (Αλγόριθμος επαλήθευσης)	Δεν χρησιμοποιείται
[Diffie-Hellman Group] (Ομάδα Diffie-Hellman)	[Group 1] (Ομάδα 1), [Group 2] (Ομάδα 2), [Group 5] (Ομάδα 5)

[IKEv2]

Στοιχείο ρύθμισης	Υφιστάμενες ρυθμίσεις
[Encryption Algorithm] (Αλγόριθμος κρυπτογράφησης)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 και 192))
[Authentication Algorithm] (Αλγόριθμος επαλήθευσης)	Δεν χρησιμοποιείται
[Diffie-Hellman Group] (Ομάδα Diffie-Hellman)	[Group 1] (Ομάδα 1), [Group 2] (Ομάδα 2), [Group 5] (Ομάδα 5)

[SA]

Στοιχείο ρύθμισης	Υφιστάμενες ρυθμίσεις
[Key Exchange Method] (Μέθοδος αλλαγής κλειδιού)	[IKEv1]
[Authentication Method] (Μέθοδος επαλήθευσης)	[Digital Signature] (Ψηφιακή υπογραφή)
[ESP Encryption Algorithm] (Αλγόριθμος κρυπτογράφησης ESP)	[3DES-CBC] ([128]/[192]/[128 and 192] (128 και 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 και 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 και 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 και 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 και 192))
[Perfect Forward Secrecy] (Απόλυτη μελλοντική μυστικότητα)	ON
[Diffie-Hellman Group(IKEv1)] (Ομάδα Diffie-Hellman (IKEv1))	[Group 1] (Ομάδα 1), [Group 2] (Ομάδα 2), [Group 5] (Ομάδα 5)

4.3 Οι διεπαφές και οι υπηρεσίες δικτύου είναι διαθέσιμες κατά την εργοστασιακή αποστολή

Τύπος υπηρεσίας	Πρωτόκολλο	Αριθμός θύρας
DHCP	UDP	68
Διακομιστής HTTP	TCP	80
Υπηρεσία ονόματος NETBIOS	UDP	137
Υπηρεσία δεδομενογραμμάτων NETBIOS	UDP	138
SNMP	UDP	161
HTTP Διακομιστής μέσω SSL / IPP μέσω SSL	TCP	443
Εκτύπωση LPD	TCP	515
Υπολογιστής-πελάτης DHCPv6	UDP	546
Εκτύπωση IPP	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (εργαλείο IWS)	TCP	8091
Εκτύπωση RAW	TCP	9100
Εκτύπωση RAW	TCP	9112
Εκτύπωση RAW	TCP	9113
Εκτύπωση RAW	TCP	9114
Εκτύπωση RAW	TCP	9115
Εκτύπωση RAW	TCP	9116
OpenAPI	TCP	50001

4.4 Σχετικά με την επαλήθευση καταχωρίσεων

Για το πλήθος των χαρακτήρων που πρέπει να καταχωρίζονται για ρυθμίσεις δικτύου κ.λπ., ανατρέξτε σε καθένα από τα στοιχεία ρυθμίσεων του οδηγού χρήστη.

Ανάλογα με την κωδικοποίηση της γλώσσας, η μέγιστη επιτρεπόμενη καταχώριση (δεδομένα αποθηκευμένα στο MFP) για στοιχεία που υποστηρίζουν χαρακτήρες πολλαπλών byte είναι τρεις φορές ο αριθμός των χαρακτήρων.

Soovitused turvaliste võrguseadmete kasutamiseks

Sisukord

1 IP-aadressi filtreerimise seadistamine

1.1	IP-aadressi filtreerimine	1-3
1.2	Kiire IP-aadresside filtreerimine	1-3

2 Krüptitud side seadistamine

2.1	TLS-krüptimine.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP-sokli	2-6
2.2	Muu krüptimine	2-7
2.2.1	SMBServer	2-7
	SMB krüptimine	2-7
	SMB-allkiri.....	2-7
2.2.2	SMBClient	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Sertifikaadi valideerimise sätete määramine

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-12
3.9	RemotePanel	3-12

4 Täiendav teave turvalisuse kohta

4.1	Soovituslik parim tava	4-13
4.2	Ettevaatusabinõud suhtlemisel pärandüsteemidega	4-14
	IPsec pärand sätted.....	4-14
4.3	Seadmes tehases lubatud võrguühendused ja teenused	4-16
4.4	Sisestuse valideerimisest.....	4-17



Teave selle kasutusjuhendi kohta

See kasutusjuhend kirjeldab teavet ja seadeid, mis on vajalikud seadmete ohutuks kasutamiseks.

Kui masin ühendatakse võrku, tuleb seda kasutada tulemüüri kaitstud keskkonnas. Samuti soovitame määrata masinale privaatse IP-aadressi.

Privaatse IP-aadressi määramisel pääsevad masinale juurde ainult kohalikku võrgusegmenti kuuluvad kasutajad (nt sisemise kohtvõrgu kaudu), mis välistab volitamata juurdepääsu väljastpoolt.

Kui peate kasutama globaalset IP-aadressi, peab masin olema kindlasti kaitstud tulemüüri.

1 IP-aadressi filtreerimise seadistamine

IP-aadressi filtreerimine on funktsioon, mis piirab seadmetele juurdepääsu masina IP-aadressi alusel. Selle funktsiooni korrektne seadistamine võimaldab piirata masinale volitamata seadmete juurdepääsu.

Masina IP-aadressi filtreerimise funktsiooni seadistamiseks on kaks võimalust.

1.1 IP-aadressi filtreerimine

Määrake käsitsi IP-aadresside vahemik, mis saavad või ei saa juurdepääsu masinale.

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [TCP/IP Setting] (TCP/IP-sätted) - [IP Address Filtering] (IP-aadressi filtreerimine)



Näpunäited

Määrake keskkonnale sobivad IP-aadressid, millele juurdepääs on lubatud või keelatud.

1.2 Kiire IP-aadresside filtreerimine

Juurdepääsu saavate IP-aadresside vahemik määratakse automaatselt masina IP-aadressi ja alamvõrgumaski põhjal.

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [TCP/IP Setting] (TCP/IP-sätted) - [Quick IP Filtering] (Kiir-IP-filtreerimine)

Soovitavad seaded: [Synchronize IP Address] (Sünkrooni IP-aadress) / [Synchronize Subnet Mask] (Sünkrooni alammask) *

* Valige sobiv seadistus vastavalt oma võrgu konfiguratsioonile.

2 Krüptitud side seadistamine

Et vältida andmete pealtkuulamist, võltsimist ja seansikaaperdusi, soovime kasutada alltoodud krüptitud sideprotokolle.

2.1 TLS-krüptimine

Soovime teha allpool toodud seadistused, et vähendada haavatavustega seotud riske.

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Security] (Turve) - [PKI Settings] (PKI sätted) - [Enable SSL Version] (Luba SSL-versioon)

Seadistus	Soovitatav väärtus
[Mode using SSL/TLS] (SSL/TLS kasutusrežiim)	[Admin. Mode and User Mode] (Administraatori režiim ja kasutaja režiim)
[SSL/TLS Version Setting] (SSL/TLS versiooni säte)	TLS1.2 TLS1.3 (IEEE802.1X ühildumatu)
[Encryption Strength] (Krüptimistugevus)	AES-256

Tehaseseadetes on paigaldatud esialgne sert. Kui vajate muud sertifikaati, registreerige see järgmisel aadressil:

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Security] (Turve) - [PKI Settings] (PKI sätted) - [Device Certificate Setting] (Seadme sertifikaadi sätted)

Seadistus	Soovitatav väärtus
[Encryption Key Type] (Krüptovõtme tüüp)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

TLS-krüptimise tugi kehtib järgmiste protokollide ja teenuste puhul. Täpsemat teavet seadistamise asukohtade kohta leiate vastavatest alalõikudest.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP üle SSL-i)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP-sokli

2.1.1 HTTP (Web Connection)

Kui seadistuses [Enable SSL Version] (Luba SSL-versioon) on valitud "ON", lülitub suhtlusrežiim automaatselt TLS-krüpteeritud režiimile (HTTPS).

2.1.2 WebDAVServer

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [WebDAV Settings] (WebDAV-sätted) - [WebDAV Server Settings] (WebDAV-serveri sätted)

Seadistus	Soovitatav väärtus
[SSL Settings] (SSL-seaded)	[SSL Only] (Ainult SSL)

2.1.3 IPP

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [HTTP Server Settings] (HTTP-serveri seaded)

Seadistus	Soovitav väärtus
[IPP-SSL Settings] (IPP-SSL seaded)	[SSL Only] (Ainult SSL)

2.1.4 OpenAPI

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [OpenAPI Setting] (OpenAPI-seaded) - [OpenAPI Setting] (OpenAPI-seaded)

Seadistus	Soovitav väärtus
[SSL/Port Settings] (SSL-/pordi seaded)	[SSL Only] (Ainult SSL)

2.1.5 RemotePanel

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [Remote Panel Settings] (Kaugpaneeli seaded) - [Remote Panel Server Settings] (Kaugpaneeli serveri seaded)

Seadistus	Soovitav väärtus
[Port No.(SSL)]	[50443]



Näpunäited

Kui seadistuses [Enable SSL Version] (Luba SSL-versioon) on valitud "ON", lülitub suhtlus automaatselt TLS-krüpteeritud režiimile. Määrake ka pordinumber.

2.1.6 DPWS

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [DPWS Settings] (DPWS-i sätted) - [DPWS Common Settings] (DPWS-i ühissätted)

Seadistus	Soovitav väärtus
[SSL Settings] (SSL-seaded)	SEES

2.1.7 POP

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [E-mail Setting] (Meili sätted) - [E-mail RX (POP)] (Sissetulev meil (POP))

Seadistus	Soovitav väärtus
[Enable SSL] (Luba SSL)	SEES

2.1.8 SMTP

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [E-mail Setting] (Meili sätted) - [E-mail TX (SMTP)] (Väljaminev meil (SMTP))

Seadistus	Soovitav väärtus
[SSL/TLS Settings] (SSL-/TLS-i sätted)	[SMTP over SSL] (SMTP üle SSL-i)

2.1.9 IEEE802.1X Auth

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentimissäte) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentimissäte) - [Supplicant Setting] (Supplicant-sätted)

Seadistus	Soovitatav väärtus
[EAP-Type] (EAP tüüp)	Valige [EAP-TLS], [EAP-TTLS] või [PEAP].

2.1.10 LDAP

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [LDAP Setting] (LDAP-i sätted) - [Setting Up LDAP] (LDAP-i seadistamine)

Seadistus	Soovitatav väärtus
[Enable SSL] (Luba SSL)	SEES

2.1.11 TCP-sokli

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [TCP Socket Setting] (TCP-sokli sätted)

Seadistus	Soovitatav väärtus
[Use SSL/TLS] (Kasuta SSL-i/TLS-i)	SEES

2.2 Muu krüptimine

Soovitame teha allpool toodud seadistused, et vähendada haavatavustega seotud riske. Iga funktsiooni seadistuste kohta leiate täpsemat teavet vastavatest alalõikudest.

Funktsioon	Soovitav väärtus
SMBServer	SMB-krüptimine, SMB-allkiri
SMBClient	Kerberose autentimine
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	SEES

2.2.1 SMBServer

SMB-krüptimise ja SMB-allkirja kasutamine aitab vähendada järgmisi turvariske.

- Pealtkuulamine: Pahatahtlik kolmas pool võib sideühendust pealt kuulata ja varastada isiklikku või konfidentsiaalset teavet.
- Andmete võltsimine: Eksisteerib oht, et sideühenduse sisu võltsitakse "vahendajarünnaku" (MITM - Man-In-The-Middle) käigus.
- Teesklemine (spoofing): Kui autentimisteave varastatakse, võib kolmas pool teeselda seaduslikku kasutajat, et saada volitamata juurdepääsu.
- Teabeleke: Krüptimata suhtlust on lihtne pealt kuulata, eriti avalikes Wi-Fi-võrkudes, mis suurendab ohtu, et lekitab isiklik või krediitkaardiandmetega seotud teave.

SMB krüptimine

Eeltingimused

- Looge avalik kasutajaboks. Konfigureerige seaded viisil, et failid teisaldatakse automaatselt avalikust kasutajaboksist SMB-kausta.
- Määrake kasutajaboksile parool.

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Box] (Boks) - [User Box List] (Kasutajabokside loend)

Seadistus	Soovitav väärtus
[SMB Communication Encryption] (SMB-side krüptimine)	[Encrypt] (Krüpti)

SMB-allkiri

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [SMB Setting] (SMB-sätted) - [SMB Server Settings] (SMB-serveri sätted)

Seadistus	Soovitav väärtus
[SMB security Signature Setting] (SMB turbeallkirja säte)	[Required] (Nõutav)

2.2.2 SMBClient

Kerberose autentimine kasutab tugevat krüptimistehnoloogiat, vähendades märkimisväärselt riski, et autentimiseavet võidakse autentimisprotsessi käigus varastada. See tagab ka andmete tervikluse, vältides andmete võltsimist saatja ja vastuvõtja vahel ning NTLM-i releerünnakuid.

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [SMB Setting] (SMB-sätted) - [Client Setting] (Kliendisätted)

Seadistus	Soovitav väärtus
[SMB Authentication Setting] (SMB autentimissäte)	[Kerberos]

2.2.3 SNMP

Seadistage krüptimine SNMPv3 abil. Kui lisate ka autentimissäte, saab turvalisust veelgi suurendada. Turvariskid on ligikaudu samad, mis SMB puhul.

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [SNMP Setting] (SNMP säte)

Seadistus	Soovitav väärtus
[SNMP Setting] (SNMP säte)	[SNMP v3(IP)]
[Encryption Algorithm] (Krüptimisalgoritm)	[AES-128]
[Authentication Method] (Autentimismeetod)	Valige [SHA-256], [SHA-384] või [SHA-512].

2.2.4 IPsec

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [TCP/IP Setting] (TCP/IP-sätted) - [IPsec] - [IPsec Setting] (IPsec-i sätted)

[IKEv2]

Seadistus	Soovitav väärtus
[Encryption Algorithm] (Krüptimisalgoritm)	[AES-CBC] ([256]/[192 ja 256]/[Kõik])
[Authentication Algorithm] (Autentimisalgoritm)	[SHA-2] ([256]/[384]/[512]/[256 ja 384]/[384 ja 512]/[Kõik]), [AES-XCBC]
[Diffie-Hellman Group] (Diffie-Hellmani rühm)	[Group 14] (Rühm 14), [Group 19] (Rühm 19)

[SA]

Seadistus	Soovitav väärtus
[Encapsulation Mode] (Kapseldusrežiim)	[Tunnel], [Transport]
[Security Protocol] (Turbeprotokoll)	[ESP]
[Key Exchange Method] (Võtmevahetusmeetod)	[IKEv2]
[Authentication Method] (Autentimismeetod)	[Digital Signature] (Digitaalallkiri)
[ESP Encryption Algorithm] (ESP krüptimisalgoritm)	[AES-GCM] ([256]/[192 ja 256]/[Kõik]), [AES-GCM-64] ([256]/[192 ja 256]/[Kõik]), [ENC_NULL_AES_GMAC] ([256]/[192 ja 256]/[Kõik])
[Perfect Forward Secrecy] (Täielik edasisalastatus)	SEES

Seadistus	Soovitav väärtus
[Diffie-Hellman Group(IKEv2)] (Diffie-Hellmani rühm (IKEv2)) - [Priority1-4] (Prioriteet 1-4)	[Group 14] (Rühm 14), [Group 19] (Rühm 19)

2.2.5 S/MIME

Kui kasutada e-kirjade saatmisel valikulist S/MIME'i, saab kirja sisu krüptida, et vältida pealtkuulamist, ning kontrollida saatja isikut elektroonilise allkirjaga. See on tõhus kaitse teesklemis- (spoofing) ja andmepüügirünnakute (phishing) vastu.

Seadistamise asukoht: [Utility] (Utiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [E-mail Setting] (Meili sätted) - [S/MIME]

Seadistus	Soovitav väärtus
[Digital Signature] (Digitaalallkiri)	[Always add signature] (Lisa alati allkiri)
[Digital Signature Type] (Digitaalallkirja tüüp)	[SHA-256]
[E-Mail Text Encrypt. Method] (E-kirja teksti krüptimismeetod)	[AES-256]

3 Sertifikaadi valideerimise sätete määramine

Kui kasutate TLS-krüptitud sidet "vahendajarünnakute" (MITM - man-in-the-middle) mõju vähendamiseks, soovitate rakendada sertifikaadi valideerimist. Valideerimise puhul soovitate minimaalselt lubada sertifikaadi aegumiskuupäeva ja sertifikaadiahela kontrolli.

Kui üritatakse ühendust võtta pärandüsteemiga, millel puudub sertifikaadi valideerimise funktsioon, suureneb vahendajarünnaku oht. Seetõttu soovitate kasutada selliseid ühendusi ainult turvalises võrgukeskkonnas.

MFP-poolset sertifikaadi valideerimist soovitatakse järgmiste MFP kliendifunktsioonide korral. Täpsemat teavet seadistamise asukohtade kohta leiate vastavatest alalõikudest.

POP, SMTP (Start TLS/SMTP üle SSL), IEEE802.1X Auth (EAP-TÜÜP: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel



Näpunäited

MFP-ga ühendatud kliendipoolel on sertifikaadi valideerimine soovitatav järgmiste MFP-serveri funktsioonide korral:

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP-sokli

3.1 POP

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [E-mail Setting] (Meili sätted) - [E-mail RX (POP)] (Sissetulev meil (POP))

Seadistus	Soovitatav väärtus
[Certificate Verification Level Settings] (Sertifikaadi valideerimise taseme sätted)	[Expiration Date] (Aegumiskuupäev): SEES [Chain] (Sertifikaadiahel): SEES

3.2 SMTP

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [E-mail Setting] (Meili sätted) - [E-mail TX (SMTP)] (Väljaminev meil (SMTP))

Seadistus	Soovitatav väärtus
[Certificate Verification Level Settings] (Sertifikaadi valideerimise taseme sätted)	[Expiration Date] (Aegumiskuupäev): SEES [Chain] (Sertifikaadiahel): SEES

3.3 IEEE802.1X Auth

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentimissäte) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentimissäte) - [Supplicant Setting] (Supplicant-sätted)

Seadistus	Soovitatav väärtus
[Certificate Verification Level Settings] (Sertifikaadi valideerimise taseme sätted)	[Expiration Date] (Aegumiskuupäev): SEES [Chain] (Sertifikaadiahel): SEES

3.4 IPsec

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [TCP/IP Setting] (TCP/IP-sätted) - [IPsec] - [Enable IPsec] (Luba IPsec)

Seadistus	Soovitav väärtus
[Certificate Verification Level Settings] (Sertifikaadi valideerimise taseme sätted)	[Expiration Date] (Aegumiskuupäev): [Confirm] (Kinnita) [Chain] (Sertifikaadiahel): [Confirm] (Kinnita)



Näpunäited

[IPsec Setting] (IPsec-i sätted) menüüs tuleb eelnevalt registreerida järgmised üksused: [IKE], [SA], [Peer] (Partner) ja [Protocol Setting] (Protokollisätted).

3.5 WebDAVClient

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [WebDAV Settings] (WebDAV-sätted) - [WebDAV Client Settings] (WebDAV kliendi sätted)

Seadistus	Soovitav väärtus
[Certificate Verification Level Settings] (Sertifikaadi valideerimise taseme sätted)	[Expiration Date] (Aegumiskuupäev): SEES [Chain] (Sertifikaadiahel): SEES

3.6 LDAP

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [LDAP Setting] (LDAP-i sätted) - [Setting Up LDAP] (LDAP-i seadistamine)

Seadistus	Soovitav väärtus
[Certificate Verification Level Settings] (Sertifikaadi valideerimise taseme sätted)	[Expiration Date] (Aegumiskuupäev): SEES [Chain] (Sertifikaadiahel): SEES

3.7 DPWS

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [DPWS Settings] (DPWS-i sätted) - [DPWS Common Settings] (DPWS-i ühissätted)

Seadistus	Soovitav väärtus
[Certificate Verification Level Settings] (Sertifikaadi valideerimise taseme sätted)	[Expiration Date] (Aegumiskuupäev): SEES [Chain] (Sertifikaadiahel): SEES

3.8 OpenAPI

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [OpenAPI Setting] (OpenAPI-seaded) - [OpenAPI Setting] (OpenAPI-seaded)

Seadistus	Soovitav väärtus
[Certificate Verification Level Settings] (Sertifikaadi valideerimise taseme sätted)	[Expiration Date] (Aegumiskuupäev): SEES [Chain] (Sertifikaadiahel): SEES

3.9 RemotePanel

Seadistamise asukoht: [Utility] (Uutiliidid) - [Administrator] (Administraator) - [Network] (Võrk) - [Remote Panel Settings] (Kaugpaneeli sätted) - [Remote Panel Client Settings] (Kaugpaneeli kliendisätted)

Seadistus	Soovitav väärtus
[Certificate Verification Level Settings] (Sertifikaadi valideerimise taseme sätted)	[Expiration Date] (Aegumiskuupäev): SEES [Chain] (Sertifikaadiahel): SEES

4 Täiendav teave turvalisuse kohta

4.1 Soovituslik parim tava

Soovitame kasutada krüptimisalgoritme, mis vastavad ELi EUCC krüptograafia suunistes ja SOGIS-i kokkulepitud krüptomehhanismides (SOGIS-Agreed-Cryptographic-Mechanisms) soovitatud parimate tavade sätelete.

Allpool on loetelu EUCC krüptograafia suunistes ja SOGIS-i kokkulepitud krüptomehhanismide krüptimisalgoritmide ja soovitatud võtmepikkustest.

Üksus	Soovitatav väärtus
Krüpteerimisalgoritmid	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Krüptovõtme pikkus	RSA: vähemalt 2048 bitti ECC: vähemalt 256 bitti AES: 256 bitti



Näpunäited

Lisateabe saamiseks tutvuge uusimate EUCC krüptograafia soovitustega ning SOGIS-i kokkulepitud krüptomehhanismidega (SOGIS-Agreed-Cryptographic-Mechanisms).

4.2 Ettevaatusabinõud suhtlemisel pärandüsteemidega

Pärandüsteemidega suhtlemisel eeldatakse järgmiste protokollide ja versioonide kasutamist.

Pärandsäete kasutamine suurendab turvariske, seetõttu tuleb neid rakendada ainult turvalises võrgukeskkonnas.

Üksus	Pärandsäted
Protokoll	SLP FTP SMB (3.0 või varasem versioon, NTLMv1/v2) SNMPv1/v2 IEEE802.1X autentimine (EAP-TÜÜP: Sõltub serverist/VÄLJAS) DPWS TCP-sokli
Krüpteerimisalgoritmid	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Krüptovõtme pikkus	RSA: 1024 bitti või vähem ECC: 160 bitti või vähem AES: 128 bitti või vähem DES: 56 bitti 3DES: 112 bitti

IPsec pärandsäted

[IKEv1]

Seadistus	Pärandsäted
[Encryption Algorithm] (Krüptimisalgoritm)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 ja 192])
[Authentication Algorithm] (Autentimisalgoritm)	Ei kasutata
[Diffie-Hellman Group] (Diffie-Hellmani rühm)	[Group 1] (Rühm 1), [Group 2] (Rühm 2), [Group 5] (Rühm 5)

[IKEv2]

Seadistus	Pärandsäted
[Encryption Algorithm] (Krüptimisalgoritm)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 ja 192])
[Authentication Algorithm] (Autentimisalgoritm)	Ei kasutata
[Diffie-Hellman Group] (Diffie-Hellmani rühm)	[Group 1] (Rühm 1), [Group 2] (Rühm 2), [Group 5] (Rühm 5)

[SA]

Seadistus	Pärandsäted
[Key Exchange Method] (Võtmevahetusmeetod)	[IKEv1]
[Authentication Method] (Autentimismeetod)	[Digital Signature] (Digitaalalkiri)

Seadistus	Pärandsätted
[ESP Encryption Algorithm] (ESP krüptimisalgoritm)	[3DES-CBC] ([128]/[192]/[128 ja 192]) [AES-CTR] ([128]/[192]/[128 ja 192]) [AES-GCM] ([128]/[192]/[128 ja 192]) [AES-GCM-64] ([128]/[192]/[128 ja 192]) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 ja 192])
[Perfect Forward Secrecy] (Täielik edasisalastatus)	SEES
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellmani rühm (IKEv1))	[Group 1] (Rühm 1), [Group 2] (Rühm 2), [Group 5] (Rühm 5)

4.3 Seadmes tehasest lubatud võrgühendused ja teenused

Teenuse tüüp	Protokoll	Port
DHCP	UDP	68
HTTP-server	TCP	80
NETBIOS-nimeteenus	UDP	137
NETBIOS-andmegrammiteenus	UDP	138
SNMP	UDP	161
HTTP-server SSL-i kaudu / IPP üle SSL-i	TCP	443
LPD-printimine	TCP	515
DHCPv6 klient	UDP	546
IPP-printimine	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-tool)	TCP	8091
RAW-printimine	TCP	9100
RAW-printimine	TCP	9112
RAW-printimine	TCP	9113
RAW-printimine	TCP	9114
RAW-printimine	TCP	9115
RAW-printimine	TCP	9116
OpenAPI	TCP	50001

4.4 Sisestuse valideerimisest

Võrgu- ja muude sätete sisestusväljade tähemärgipiirangute kohta leiate teavet kasutusjuhendi vastavast jaotisest.

Olenevalt keele kodeeringust võib mitmebaidiseid märke toetavate väljade maksimaalne lubatud sisestus (st MFP-sse salvestatav andmemaht) olla kuni kolm korda suurem kui lubatud märkide arv.

Suojattuja verkkolaitteita koskevat suositukset

Sisällysluettelo

1 IP-suodatuksen asetus

1.1	IP-suodatus	1-3
1.2	Pika-IP-suodatus	1-3

2 Salatun yhteyden asetus

2.1	TLS-salaus	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP	2-5
2.1.4	OpenAPI	2-5
2.1.5	RemotePanel	2-5
2.1.6	DPWS	2-5
2.1.7	POP	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X-todennus	2-6
2.1.10	LDAP	2-6
2.1.11	TCP-vastake	2-6
2.2	Muu salaus	2-7
2.2.1	SMBServer	2-7
	SMB-kansion salaus	2-7
	SMB-allekirjoitus	2-7
2.2.2	SMBCClient	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Varmenteen tarkastuksen määrittäminen

3.1	POP	3-10
3.2	SMTP	3-10
3.3	IEEE802.1X-todennus	3-10
3.4	IPsec	3-11
3.5	WebDAVClient	3-11
3.6	LDAP	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-12
3.9	RemotePanel	3-12

4 Turvallisuuteen liittyviä lisätietoja

4.1	Parhaita käytänteitä koskevat suositukset	4-13
4.2	Vanhojen järjestelmien kanssa tapahtuvaan tietoliikenteeseen liittyvät varotoimenpiteet... Vanhat IPsec-asetukset	4-14
4.3	Verkkoliitännät ja -palvelut saatavilla tehtaalta toimitettaessa	4-16
4.4	Tietoa syötettävien tietojen tarkastuksesta	4-17



Tietoa tästä oppaasta

Tässä oppaassa käydään läpi laitteiden turvallisen käytön mahdollistavat tiedot ja asetukset.

Kun yhdistät pääyksikön verkkoon, käytä sitä palomuurilla suojatussa ympäristössä. Suosittelemme myös määrittämään yksityisen IP-osoitteen pääyksikön IP-osoitetta varten.

Yksityisen IP-osoitteen määrittämisen myötä pääyksikköä voivat käyttää ainoastaan lähiverkon, kuten yrityksen sisäisen LAN-verkon, käyttäjät ja ulkopuolinen luvaton käyttö estetään.

Jos julkisen IP-osoitteen käyttö on tarpeen, asenna palomuri pääyksikön suojaksi.

1 IP-suodatuksen asetus

IP-suodatus on toiminto, jolla pääyksikköä käyttäviä laitteita rajoitetaan IP-osoitteen perusteella. Määrittämällä tämän toiminnon oikein voit rajoittaa luvattomien laitteiden käyttöoikeuksia.

Pääyksikön IP-osoitteen suodatustoiminto voidaan määrittää seuraavilla kahdella tavalla:

1.1 IP-suodatus

Määritä manuaalisesti niiden IP-osoitteiden alue, joiden käyttöoikeudet sallitaan tai estetään.

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [TCP/IP Setting] (TCP-/IP-asetus) - [IP Address Filtering] (IP-suodatus)

Vinkkejä

Määritä sallittavat tai estettävät IP-osoitteet käyttöympäristön mukaan.

1.2 Pika-IP-suodatus

Käytön sallivien IP-osoitteiden alue määritetään automaattisesti pääyksikköön määritetyn IP-osoitteen ja aliverkon peitteen perusteella.

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [TCP/IP Setting] (TCP-/IP-asetus) - [Quick IP Filtering] (IP-pikasuodatus)

Suosittelut asetukset: [Synchronize IP Address] (Synkronoi IP-osoite) / [Synchronize Subnet Mask] (Synkronoi aliverkon peite) *

* Valitse käyttöympäristösi sopiva vaihtoehto.

2 Salatun yhteyden asetukset

Suosittellemme käyttämään seuraavaa salattua yhteyttä tietojen vakoilun ja peukaloinnin sekä istuntojen kaappaamisen estämiseksi.

2.1 TLS-salaus

Suosittellemme määrittämään seuraavat asetukset haavoittuvuusriskien vähentämiseksi.

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Security] (Suojaus) - [PKI Settings] (PKI-asetukset) - [Enable SSL Version] (Ota käyttöön SSL-versio)

Asetusvaihtoehto	Suositteltu asetus
[Mode using SSL/TLS] (SSL-/TLS-käyttötila)	[Admin. Mode and User Mode] (Pääkäyttäjätila ja käyttäjätila)
[SSL/TLS Version Setting] (SSL-/TLS-version asetus)	TLS1.2 TLS1.3 (IEEE802.1X-yhteensopimaton)
[Encryption Strength] (Salausvahvuus)	AES-256

Alkuperäinen varmenne on asennettu tehtaalla. Jos tarvitset muuta varmennetta, rekisteröi uusi varmenne seuraavassa paikassa.

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Security] (Suojaus) - [PKI Settings] (PKI-asetukset) - [Device Certificate Setting] (Laitteen varmenneasetus)

Asetusvaihtoehto	Suositteltu asetus
[Encryption Key Type] (Salausavaimen tyyppi)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

TLS-salausta tuetaan seuraaville protokollille ja palveluille. Asetuksen sijaintiin liittyviä lisätietoja löytyy seuraavista osioista.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X-todennus (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP-vastake

2.1.1 HTTP (Web Connection)

Jos otat käyttöön asetuksen [Enable SSL Version] (Ota käyttöön SSL-versio), yhteydellä muuttuu automaattisesti TLS-salatuksi yhteydeksi (HTTPS).

2.1.2 WebDAVServer

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [WebDAV Settings] (WebDAV-asetukset) - [WebDAV Server Settings] (WebDAV-palvelimen asetukset)

Asetusvaihtoehto	Suositteltu asetus
[SSL Settings] (SSL-asetukset)	[SSL Only] (Vain SSL)

2.1.3 IPP

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [HTTP Server Settings] (HTTP-palvelimen asetukset)

Aetusvaihtoehto	Suositteltu asetus
[IPP-SSL Settings] (IPP-SSL-asetukset)	[SSL Only] (Vain SSL)

2.1.4 OpenAPI

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [OpenAPI Setting] (OpenAPI-asetus) - [OpenAPI Setting] (OpenAPI-asetus)

Aetusvaihtoehto	Suositteltu asetus
[SSL/Port Settings] (SSL-/porttiasetukset)	[SSL Only] (Vain SSL)

2.1.5 RemotePanel

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [Remote Panel Settings] (Etäpaneelin asetukset) - [Remote Panel Server Settings] (Etäpaneelin palvelimen asetukset)

Aetusvaihtoehto	Suositteltu asetus
[Port No.(SSL)] (Portin numero (SSL))	[50443]



Vinkkejä

Jos otat käyttöön asetuksen [Enable SSL Version] (Ota käyttöön SSL-versio), yhteys muuttuu automaattisesti TLS-salattuun tilaan. Määritä portin numero.

2.1.6 DPWS

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [DPWS Settings] (DPWS-asetukset) - [DPWS Common Settings] (DPWS:n yleiset asetukset)

Aetusvaihtoehto	Suositteltu asetus
[SSL Settings] (SSL-asetukset)	PÄÄLLÄ

2.1.7 POP

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [E-mail Setting] (Sähköpostiasetus) - [E-mail RX (POP)] (Sähköpostin vastaanotto (POP))

Aetusvaihtoehto	Suositteltu asetus
[Enable SSL] (Ota SSL käyttöön)	PÄÄLLÄ

2.1.8 SMTP

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [E-mail Setting] (Sähköpostiasetus) - [E-mail TX (SMTP)] (Sähköpostin lähetys (SMTP))

Aetusvaihtoehto	Suositteltu asetus
[SSL/TLS Settings] (SSL/TLS-asetukset)	[SMTP over SSL] (SMTP ennen SSL:ää)

2.1.9 IEEE802.1X-todennus

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [IEEE802.1X Authentication Setting] (IEEE802.1X-todennuksen asetus) - [IEEE802.1X Authentication Setting] (IEEE802.1X-todennuksen asetus) - [Supplicant Setting] (Anoja-asetus)

Aetusvaihtoehto	Suositteltu asetus
[EAP-Type] (EAP-tyyppi)	Valitse [EAP-TLS], [EAP-TTLS] tai [PEAP].

2.1.10 LDAP

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [LDAP Setting] (LDAP-asetus) - [Setting Up LDAP] (LDAP:n asetus)

Aetusvaihtoehto	Suositteltu asetus
[Enable SSL] (Ota SSL käyttöön)	PÄÄLLÄ

2.1.11 TCP-vastake

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [TCP Socket Setting] (TCP-vastakkeen asetus)

Aetusvaihtoehto	Suositteltu asetus
[Use SSL/TLS] (Käytä SSL:ää/TLS:ää)	PÄÄLLÄ

2.2 Muu salaus

Suosittellemme määrittämään seuraavat asetukset haavoittuvuusriskien vähentämiseksi. Kunkin toiminnon asetuksiin liittyviä lisätietoja löytyy seuraavista osioista.

Toiminto	Suositteltu asetus
SMBServer	SMB-kansion salaus, SMB-allekirjoitus
SMBClient	Kerberos-todennus
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	PÄÄLLÄ

2.2.1 SMBServer

Käyttämällä SMB-kansion salausta ja SMB-allekirjoitusta voidaan vähentää seuraavia turvallisuusriskejä.

- Vakoilu: Haitallinen kolmas osapuoli voi siepata viestejä ja varastaa henkilötietoja tai luottamuksellisia tietoja.
- Tietojen peukalointi: On olemassa vaara, että viestien sisältöjä voidaan muuttaa välistävetohyökkäyksen (MITM) avulla.
- Huijaus: Jos todennustiedot varastetaan, kolmas osapuoli voi esiintyä laillisena käyttäjänä saadakseen luvattomasti käyttöoikeudet.
- Tietovuoto: Salaamattomat tiedot voidaan siepata helposti, erityisesti julkisia Wi-Fi-verkkoja käytettäessä, mikä lisää henkilötietojen ja luottokorttitietojen vuotamisen riskiä.

SMB-kansion salaus

Edellytykset

- Luo julkinen käyttäjälaatikko. Määritä lisäksi asetus, jonka myötä tiedostot siirretään automaattisesti julkisesta käyttäjälaatikosta ja tallennetaan SMB-kansioon.
- Määritä käyttäjälaatikon salasana.

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Box] (Käyttäjälaatikko) - [User Box List] (Käyttäjälaatikkoluettelo)

Asetusvaihtoehto	Suositteltu asetus
[SMB Communication Encryption] (SMB-yhteyden salaus)	[Encrypt] (Salaa)

SMB-allekirjoitus

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [SMB Setting] (SMB-asetus) - [SMB Server Settings] (SMB-palvelimen asetukset)

Asetusvaihtoehto	Suositteltu asetus
[SMB security Signature Setting] (SMB-suojauksen allekirjoitusasetus)	[Required] (Pakollinen)

2.2.2 SMBClient

Kerberos-todennus käyttää vahvaa salaustekniikkaa vähentäen näin merkittävästi tunnistetietojen varastamisen riskiä todennusprosessin aikana. Lisäksi se varmistaa tietojen eheyden ja estää lähettäjän ja vastaanottajan välisen viestinnän tietojen peukaloinnin sekä NTLM Relay -hyökkäykset.

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [SMB Setting] (SMB-asetus) - [Client Setting] (Asiakasasetus)

Aetusvaihtoehto	Suositteltu asetus
[SMB Authentication Setting] (SMB-todennuksen asetus)	[Kerberos]

2.2.3 SNMP

Määritä SNMPv3-salaus. Voit parantaa turvallisuutta entisestään lisäämällä myös todennuksen asetuksen. Turvallisuusriskit ovat jotakuinkin samat kuin SMB:n yhteydessä.

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [SNMP Setting] (SNMP-asetus)

Aetusvaihtoehto	Suositteltu asetus
[SNMP Setting] (SNMP-asetus)	[SNMP v3(IP)]
[Encryption Algorithm] (Salausalgoritmi)	[AES-128]
[Authentication Method] (Todennusmenetelmä)	Valitse [SHA-256], [SHA-384] tai [SHA-512].

2.2.4 IPsec

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [TCP/IP Setting] (TCP-/IP-asetus) - [IPsec] - [IPsec Setting] (IPsec-asetus)

[IKEv2]

Aetusvaihtoehto	Suositteltu asetus
[Encryption Algorithm] (Salausalgoritmi)	[AES-CBC] ([256] / [192 and 256] (192 ja 256) / [All] (Kaikki))
[Authentication Algorithm] (Todennusalgoritmi)	[SHA-2] ([256] / [384] / [512] / [256 and 384] (256 ja 384) / [384 and 512] (384 ja 512) / [All] (Kaikki)), [AES-XCBC]
[Diffie-Hellman Group] (Diffie-Hellman-ryhmä)	[Group 14] (Ryhmä 14), [Group 19] (Ryhmä 19)

[SA]

Aetusvaihtoehto	Suositteltu asetus
[Encapsulation Mode] (Kapselointitila)	[Tunnel] (Tunneli), [Transport] (Kuljetus)
[Security Protocol] (Suojausprotokolla)	[ESP]
[Key Exchange Method] (Avaimen vaihtomenetelmä)	[IKEv2]
[Authentication Method] (Todennusmenetelmä)	[Digital Signature] (Digitaalinen allekirjoitus)
[ESP Encryption Algorithm] (ESP-salausalgoritmi)	[AES-GCM] ([256] / [192 and 256] (192 ja 256) / [All] (Kaikki)), [AES-GCM-64] ([256] / [192 and 256] (192 ja 256) / [All] (Kaikki)), [ENC_NULL_AES_GMAC] ([256] / [192 and 256] (192 ja 256) / [All] (Kaikki))

Asetusvaihtoehto	Suositteltu asetus
[Perfect Forward Secrecy] (PFS-salaus)	PÄÄLLÄ
[Diffie-Hellman Group(IKEv2)] (Diffie-Hellman-ryhmä (IKEv2)) - [Priority1-4] (Prioriteetti 1 - 4)	[Group 14] (Ryhmä 14), [Group 19] (Ryhmä 19)

2.2.5 S/MIME

Jos käytät sähköpostin lähetyksen yhteydessä valinnaista S/MIME-standardia, voit salata sähköpostin sisällön vakoilun estämiseksi ja lähettäjän henkilöllisyyden varmistamiseksi sähköisen allekirjoituksen avulla. Tämä on tehokas tapa estää Spoofing-tyyppiset huijausyritykset ja tietojenkalasteluyritykset.

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [E-mail Setting] (Sähköpostiasetus) - [S/MIME]

Asetusvaihtoehto	Suositteltu asetus
[Digital Signature] (Digitaalinen allekirjoitus)	[Always add signature] (Lisää aina allekirjoitus)
[Digital Signature Type] (Digitaalisen allekirjoituksen tyyppi)	[SHA-256]
[E-Mail Text Encrypt. Method] (Sähköpostin tekstin salaustapa)	[AES-256]

3 Varmenteen tarkastuksen määrittäminen

Jos käytät TLS-salattua yhteyttä välistävetohyökkäysten vaikutusten vähentämiseksi, suosittelemme käyttämään varmenteen tarkastusta. Tarkastuskohteiksi suosittelemme ottamaan käyttöön vähintään varmenteen vanhentumispäivän ja varmenneketjun.

Jos yhteyttä yritetään muodostaa vanhaan järjestelmäympäristöön, jossa ei ole varmenteen tarkastustoimintoa, välistävetohyökkäysten riski kasvaa. Suosittelemme käyttämään sitä suojaussa verkkoympäristössä.

Varmenteen tarkastusta MFP:n puolella suositellaan seuraavien MFP-asiakastoimintojen yhteydessä. Asetuksen sijaintiin liittyviä lisätietoja löytyy seuraavista osioista.

POP, SMTP (Start TLS / SMTP over SSL), IEEE802.1X-todennus (EAP-TYYPPI: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel

Vinkkejä

Varmenteen tarkastusta MFP:hen yhdistetyn asiakkaan puolella suositellaan seuraavien MFP-palvelintoimintojen yhteydessä.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP-vastake

3.1 POP

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [E-mail Setting] (Sähköpostiasetus) - [E-mail RX (POP)] (Sähköpostin vastaanotto (POP))

Asetusvaihtoehto	Suosittelut asetus
[Certificate Verification Level Settings] (Varmenteen vahvistustason asetus)	[Expiration Date] (Vanhentumispäivä): PÄÄLLÄ [Chain] (Ketju): PÄÄLLÄ

3.2 SMTP

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [E-mail Setting] (Sähköpostiasetus) - [E-mail TX (SMTP)] (Sähköpostin lähetyksen SMTP)

Asetusvaihtoehto	Suosittelut asetus
[Certificate Verification Level Settings] (Varmenteen vahvistustason asetus)	[Expiration Date] (Vanhentumispäivä): PÄÄLLÄ [Chain] (Ketju): PÄÄLLÄ

3.3 IEEE802.1X-todennus

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [IEEE802.1X Authentication Setting] (IEEE802.1X-todennuksen asetus) - [IEEE802.1X Authentication Setting] (IEEE802.1X-todennuksen asetus) - [Supplicant Setting] (Anoja-asetus)

Asetusvaihtoehto	Suosittelut asetus
[Certificate Verification Level Settings] (Varmenteen vahvistustason asetus)	[Expiration Date] (Vanhentumispäivä): PÄÄLLÄ [Chain] (Ketju): PÄÄLLÄ

3.4 IPsec

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [TCP/IP Setting] (TCP-/IP-asetus) - [IPsec] - [Enable IPsec] (Ota IPsec käyttöön)

Asetusvaihtoehto	Suositteltu asetus
[Certificate Verification Level Settings] (Varmenteen vahvistustason asetus)	[Expiration Date] (Vanhentumispäivä): [Confirm] (Vahvista) [Chain] (Ketju): [Confirm] (Vahvista)

Vinkkejä

Rekisteröi kohdassa [IPsec Setting] (IPsec-asetus) kohdat [IKE], [SA], [Peer] (Vertaislaite) ja [Protocol Setting] (Protokolla-asetus) etukäteen.

3.5 WebDAVClient

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [WebDAV Settings] (WebDAV-asetukset) - [WebDAV Client Settings] (WebDAV-asiakkaan asetukset)

Asetusvaihtoehto	Suositteltu asetus
[Certificate Verification Level Settings] (Varmenteen vahvistustason asetus)	[Expiration Date] (Vanhentumispäivä): PÄÄLLÄ [Chain] (Ketju): PÄÄLLÄ

3.6 LDAP

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [LDAP Setting] (LDAP-asetus) - [Setting Up LDAP] (LDAP:n asetus)

Asetusvaihtoehto	Suositteltu asetus
[Certificate Verification Level Settings] (Varmenteen vahvistustason asetus)	[Expiration Date] (Vanhentumispäivä): PÄÄLLÄ [Chain] (Ketju): PÄÄLLÄ

3.7 DPWS

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [DPWS Settings] (DPWS-asetukset) - [DPWS Common Settings] (DPWS:n yleiset asetukset)

Asetusvaihtoehto	Suositteltu asetus
[Certificate Verification Level Settings] (Varmenteen vahvistustason asetus)	[Expiration Date] (Vanhentumispäivä): PÄÄLLÄ [Chain] (Ketju): PÄÄLLÄ

3.8 OpenAPI

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [OpenAPI Setting] (OpenAPI-asetus) - [OpenAPI Setting] (OpenAPI-asetus)

Asetusvaihtoehto	Suositteltu asetus
[Certificate Verification Level Settings] (Varmenteen vahvistustason asetus)	[Expiration Date] (Vanhentumispäivä): PÄÄLLÄ [Chain] (Ketju): PÄÄLLÄ

3.9 RemotePanel

Asetus löytyy seuraavaa polkua pitkin: [Utility] (Apuohjelma) - [Administrator] (Pääkäyttäjä) - [Network] (Verkko) - [Remote Panel Settings] (Etäpaneelin asetukset) - [Remote Panel Server Settings] (Etäpaneelin asiakasasetukset)

Asetusvaihtoehto	Suositteltu asetus
[Certificate Verification Level Settings] (Varmenteen vahvistustason asetus)	[Expiration Date] (Vanhentumispäivä): PÄÄLLÄ [Chain] (Ketju): PÄÄLLÄ

4 Turvallisuuden liittyviä lisätietoja

4.1 Parhaita käytänteitä koskevat suositukset

Suosittelimme käyttämään EUCC:n salaustekniikkaa koskevissa ohjeissa "Guidelines on Cryptography" ja asiakirjassa "SOGIS-Agreed-Cryptographic-Mechanisms" suositeltuja salausalgoritmeja, jotka täyttävät parhaiden käytänteiden määrittymiset.

Alla on luettelo EUCC:n salaustekniikkaa koskevissa ohjeissa "Guidelines on Cryptography" ja asiakirjassa "SOGIS-Agreed-Cryptographic-Mechanisms" suositelluista salausalgoritmeista ja avaimien pituuksista.

Kohde	Suositteluasetus
Salausalgoritmit	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Salausavaimen pituus	RSA: vähintään 2 048 bittiä ECC: vähintään 256 bittiä AES: 256 bittiä

Vinkkejä

Katso lisätietoja EUCC:n salaustekniikkaa koskevista uusimmista ohjeista "Guidelines on Cryptography" ja asiakirjasta "SOGIS-Agreed-Cryptographic-Mechanisms".

4.2 Vanhojen järjestelmien kanssa tapahtuvaan tietoliikenteeseen liittyvät varoimenpiteet

Oletuksena on, että seuraavia protokollia ja versioita käytetään vanhojen eli nk. perinnejärjestelmien kanssa tapahtuvassa tietoliikenteessä.

Vanhojen asetusten käyttö lisää turvallisuusriskejä, joten käytä niitä suojatussa verkkoympäristössä.

Kohde	Vanhat asetukset
Protokolla	SLP FTP SMB (3.0 tai vanhempi versio, NTLMv1/v2) SNMPv1/v2 IEEE802.1X-todennus (EAP-TYYPPI: Palvelimen mukaan / POIS PÄÄLTÄ) DPWS TCPSocket
Salausalgoritmit	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Salausavaimen pituus	RSA: enintään 1 024 bittiä ECC: enintään 160 bittiä AES: enintään 128 bittiä DES: 56 bittiä 3DES: 112 bittiä

Vanhat IPsec-asetukset

[IKEv1]

Asetusvaihtoehto	Vanhat asetukset
[Encryption Algorithm] (Salausalgoritmi)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128] / [192] / [128 and 192] (128 ja 192))
[Authentication Algorithm] (Todennusalgoritmi)	Ei käytössä
[Diffie-Hellman Group] (Diffie-Hellman-ryhmä)	[Group 1] (Ryhmä 1), [Group 2] (Ryhmä 2), [Group 5] (Ryhmä 5)

[IKEv2]

Asetusvaihtoehto	Vanhat asetukset
[Encryption Algorithm] (Salausalgoritmi)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128] / [192] / [128 and 192] (128 ja 192))
[Authentication Algorithm] (Todennusalgoritmi)	Ei käytössä
[Diffie-Hellman Group] (Diffie-Hellman-ryhmä)	[Group 1] (Ryhmä 1), [Group 2] (Ryhmä 2), [Group 5] (Ryhmä 5)

[SA]

Asetusvaihtoehto	Vanhat asetukset
[Key Exchange Method] (Avaimen vaihtomenetelmä)	[IKEv1]
[Authentication Method] (Todennusmenetelmä)	[Digital Signature] (Digitaalinen allekirjoitus)

Asetusvaihtoehto	Vanhat asetukset
[ESP Encryption Algorithm] (ESP-salausalgoritmi)	[3DES-CBC] ([128] / [192] / [128 and 192] (128 ja 192)) [AES-CTR] ([128] / [192] / [128 and 192] (128 ja 192)) [AES-GCM] ([128] / [192] / [128 and 192] (128 ja 192)) [AES-GCM-64] ([128] / [192] / [128 and 192] (128 ja 192)) [ENC_NULL_AES_GMAC] ([128] / [192] / [128 and 192] (128 ja 192))
[Perfect Forward Secrecy] (PFS-salaus)	PÄÄLLÄ
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellman-ryhmä (IKEv1))	[Group 1] (Ryhmä 1), [Group 2] (Ryhmä 2), [Group 5] (Ryhmä 5)

4.3 Verkkoliitännät ja -palvelut saatavilla tehtaalta toimitettaessa

Palvelutyyppi	Protokolla	Portin numero
DHCP	UDP	68
HTTP-palvelin	TCP	80
NETBIOS Name Service	UDP	137
NETBIOS Datagram Service	UDP	138
SNMP	UDP	161
HTTP Server over SSL / IPP over SSL	TCP	443
LPD Print	TCP	515
DHCPv6 Client	UDP	546
IPP Print	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-työkalu)	TCP	8091
RAW Print	TCP	9100
RAW Print	TCP	9112
RAW Print	TCP	9113
RAW Print	TCP	9114
RAW Print	TCP	9115
RAW Print	TCP	9116
OpenAPI	TCP	50001

4.4 Tietoa syötettävien tietojen tarkastuksesta

Lisätietoja verkkoasetuksia varten syötettävien merkkien määrästä yms. löydät Käyttäjän oppaasta kunkin asetusvaihtoehdon kohdalta.

Kielen salauksesta riippuen syötettävien tietojen sallittu maksimimäärä (MFP:lle tallennetut tiedot) kohteille, jotka tukevat monitavuisia merkkejä, voi olla kolme kertaa merkkien määrä.

Preporuke za sigurno umrežavanje uređaja

Sadržaj

1 Postavljanje značajke IP Address Filtering (Filtriranje IP adresa)

1.1	Filtriranje IP adresa.....	1-3
1.2	Brzo IP filtriranje	1-3

2 Postavljanje značajke Encrypted Communication (Šifrirana komunikacija)

2.1	TLS šifriranje	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-5
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-6
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCPsocket.....	2-6
2.2	Drugo šifriranje.....	2-7
2.2.1	SMBServer	2-7
	SMB šifriranje.....	2-7
	SMB potpis	2-7
2.2.2	SMBCClient	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Postavljanje značajke Certificate Validation (Provjera certifikata)

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-12
3.9	RemotePanel	3-12

4 Dodatne sigurnosne informacije

4.1	Preporuka za najbolju praksu.....	4-13
4.2	Mjere opreza pri komunikaciji sa sustavima sa starijim postavkama	4-14
	Starije postavke za IPsec.....	4-14
4.3	Tvornički zadana aktivirana mrežna sučelja i popis usluga	4-16
4.4	Informacije o potvrdi unosa	4-17



O ovom priručniku

U ovom su priručniku opisane informacije i postavke koje omogućuju sigurnu upotrebu uređaja.

Pri povezivanju uređaja s mrežom, upotrijebite ga u okruženju zaštićenom vatrozidom. Osim toga, preporučujemo da za IP adresu uređaja postavite privatnu IP adresu.

Postavljanje privatne IP adrese omogućuje da samo korisnici na lokalnoj mreži, primjerice internoj LAN mreži, pristupaju uređaju, čime se sprječava neovlašten pristup uređaju.

Ako morate upotrijebiti globalnu IP adresu, obavezno uređaj postavite u vatrozid.

1 Postavljanje značajke IP Address Filtering (Filtriranje IP adresa)

Filtriranje IP adresa je funkcija koja ograničava broj uređaja koji mogu pristupiti ovom uređaju temeljem IP adrese. Ako se ova funkcija pravilno postavi, može se ograničiti pristup s neovlaštenih uređaja.

Funkcija filtriranja IP adrese na uređaju može se postaviti na jedan od dva načina koji su navedeni u nastavku.

1.1 Filtriranje IP adresa

Ručno odredite raspon IP adresa kojima želite omogućiti ili onemogućiti pristup.

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [TCP/IP Setting] (TCP/IP postavka) - [IP Address Filtering] (Filtriranje IP adresa)



Postavite želite li da vaše IP adrese budu dopuštene ili zabranjene u skladu s okruženjem.

1.2 Brzo IP filtriranje

Raspon IP adresa kojima je dopušten pristup postavlja se automatski, temeljem IP adrese i maske pod mreže postavljenih na ovom uređaju.

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [TCP/IP Setting] (TCP/IP postavka) - [Quick IP Filtering] (Brzo IP filtriranje)

Preporučene postavke: [Synchronize IP Address] (Sinkroniziraj IP adrese)/[Synchronize Subnet Mask] (Sinkroniziraj masku pod mreže)*

* Odaberite opciju koja odgovara vašem okruženju.

2 Postavljanje značajke Encrypted Communication (Šifrirana komunikacija)

Preporučujemo vam upotrebu šifriranja komunikacije kako biste izbjegli neovlašten pristup i izmjenu podataka te bilo kakve scenarije otmice podataka.

2.1 TLS šifriranje

Preporučujemo vam da konfigurirate sljedeće postavke kako biste smanjili ranjivost sustava.

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Security] (Sigurnost) - [PKI Settings] (PKI postavke) - [Enable SSL Version] (Omogući SSL verziju)

Postavljanje stavke	Preporučena postavka
[Mode using SSL/TLS] (Način rada koji upotrebljava SSL/TLS)	[Admin. Mode and User Mode] (Način rada administratora i korisnika)
[SSL/TLS Version Setting] (Postavljanje verzije za SSL/TLS)	TLS1.2 TLS1.3 (nije kompatibilno s IEEE802.1X)
[Encryption Strength] (Jačina šifriranja)	AES-256

Prvotni je certifikat instaliran tvornički. Ako trebate drugi certifikat, registrirajte novi na nekoj od lokacija u nastavku.

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Security] (Sigurnost) - [PKI Settings] (PKI postavke) - [Device Certificate Setting] (Postavljanje certifikata uređaja)

Postavljanje stavke	Preporučena postavka
[Encryption Key Type] (Vrsta ključa za šifriranje)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Šifriranje TLS kompatibilno je sa sljedećim protokolima i uslugama. Detalje o lokacijama postavke potražite u odjeljcima u nastavku.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCPSocket

2.1.1 HTTP (Web Connection)

Ako omogućite opciju [Enable SSL Version] (Omogući SSL verziju), način komunikacije automatski će se prebaciti na TLS šifriranu komunikaciju (HTTPS).

2.1.2 WebDAVServer

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [WebDAV Settings] (WebDAV postavke) - [WebDAV Server Settings] (Postavke WebDAV poslužitelja)

Postavljanje stavke	Preporučena postavka
[SSL Settings] (SSL postavke)	[SSL Only] (Samo SSL)

2.1.3 IPP

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [HTTP Server Settings] (Postavke HTTP poslužitelja)

Postavljanje stavke	Preporučena postavka
[IPP-SSL Settings] (IPP-SSL postavke)	[SSL Only] (Samo SSL)

2.1.4 OpenAPI

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [OpenAPI Setting] (OpenAPI postavka) - [OpenAPI Setting] (OpenAPI postavka)

Postavljanje stavke	Preporučena postavka
[SSL/Port Settings] (SSL postavke / postavke porta)	[SSL Only] (Samo SSL)

2.1.5 RemotePanel

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [Remote Panel Settings] (Postavke za RemotePanel) - [Remote Panel Server Settings] (Postavke poslužitelja za RemotePanel)

Postavljanje stavke	Preporučena postavka
[Port No.(SSL)] (Br. porta (SSL))	[50443]



Savjeti

Ako omogućite opciju [Enable SSL Version] (Omogući SSL verziju), komunikacija će se automatski prebaciti na šifrirani način TLS. Navedite broj porta.

2.1.6 DPWS

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [DPWS Settings] (DPWS postavke) - [DPWS Common Settings] (Uobičajene DPWS postavke)

Postavljanje stavke	Preporučena postavka
[SSL Settings] (SSL postavke)	UKLJUČENO

2.1.7 POP

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [E-mail Setting] (Postavka e-pošte) - [E-mail RX (POP)] (E-pošta RX (POP))

Postavljanje stavke	Preporučena postavka
[Enable SSL] (Omogući SSL)	UKLJUČENO

2.1.8 SMTP

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [E-mail Setting] (Postavka e-pošte) - [E-mail TX (SMTP)] (E-pošta TX (SMTP))

Postavljanje stavke	Preporučena postavka
[SSL/TLS Settings] (SSL/TLS postavke)	[SMTP over SSL] (Protokol SMTP over SSL)

2.1.9 IEEE802.1X Auth

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [IEEE802.1X Authentication Setting] (Postavka autentifikacije za IEEE802.1X) - [IEEE802.1X Authentication Setting] (Postavka autentifikacije za IEEE802.1X) - [Supplicant Setting] (Postavke pošiljatelja)

Postavljanje stavke	Preporučena postavka
[EAP-Type] (Vrsta EAP-a)	Odaberite [EAP-TLS], [EAP-TTLS] ili [PEAP].

2.1.10 LDAP

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [LDAP Setting] (LDAP postavka) - [Setting Up LDAP] (Postavljanje LDAP-a)

Postavljanje stavke	Preporučena postavka
[Enable SSL] (Omogući SSL)	UKLJUČENO

2.1.11 TCPSocket

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Network] (Mreža) - [TCP Socket Setting] (Postavka TCP utičnice)

Postavljanje stavke	Preporučena postavka
[Use SSL/TLS] (Upotrijebi SSL/TLS)	UKLJUČENO

2.2 Drugo šifriranje

Preporučujemo vam da konfigurirate sljedeće postavke kako biste smanjili ranjivost sustava. Detalje o postavkama za svaku funkciju potražite u odjeljcima u nastavku.

Funkcija	Preporučena postavka
SMBServer	SMB šifriranje, SMB potpis
SMBCClient	Autentifikacija Kerberos Authentication
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	UKLJUČENO

2.2.1 SMBServer

Upotrebom SMB šifriranja i SMB potpisa mogu se smanjiti sigurnosni rizici koji su navedeni u nastavku.

- Neovlašten pristup ili prisluškivanje: zlonamjerna treća strana može presresti poruke i ukrasti osobne ili povjerljive podatke.
- Neovlaštena izmjena podataka: postoji rizik da se sadržaj poruka neovlašteno izmjeni, tzv. napad "čovjek u sredini" ili na eng. Man-In-The-Middle Attack (MITM).
- Obmana: ako se dogodi krađa podataka za autentifikaciju, treća strana može se predstaviti kao legitiman korisnik i na taj način ostvariti neovlašten pristup.
- Curenje podataka: nešifrirane poruke lako se mogu presretati, posebice na javnim Wi-Fi mrežama, čime se povećava opasnost od curenja osobnih podataka i podataka o kreditnim karticama.

SMB šifriranje

Preduvjeti

- Kreirajte javni User Box. Isto tako, konfigurirajte postavku za automatski prijenos datoteka iz javnog pretinca značajke User Box i njihov spremanje u SMB mapu.
- Izradite lozinku za User Box.

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] - [Box] (Pretinac) - [User Box List] (Popis u funkciji User Box)

Postavljanje stavke	Preporučena postavka
[SMB Communication Encryption] (SMB šifriranje poruka)	[Encrypt] (Šifriraj)

SMB potpis

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [SMB Setting] (SMB postavka) - [SMB Server Settings] (Postavke SMB poslužitelja)

Postavljanje stavke	Preporučena postavka
[SMB security Signature Setting] (Postavka SMB sigurnosnog potpisa)	[Required] (Obavezno)

2.2.2 SMBClient

Autentifikacija Kerberos upotrebljava snažnu tehnologiju šifriranja i značajno smanjuje rizik od krađe podataka za prijavu tijekom postupka autentifikacije. Također jamči integritet podataka i onemogućava neovlaštenu izmjenu i pristup podacima između pošiljatelja i primatelja, kao i NTLM napade.

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [SMB Setting] (SMB postavka) - [Client Setting] (Postavka klijenta)

Postavljanje stavke	Preporučena postavka
[SMB Authentication Setting] (Postavka SMB autentifikacije)	[Kerberos]

2.2.3 SNMP

Postavite šifriranje rabeći SNMPv3. Ako se pritom doda i postavka autentifikacije, može se dodatno povećati sigurnost. Sigurnosni rizici otprilike su isti kao uz SMB.

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [SNMP Setting] (SNMP postavka)

Postavljanje stavke	Preporučena postavka
[SNMP Setting] (SNMP postavka)	[SNMP v3(IP)]
[Encryption Algorithm] (Algoritam za šifriranje)	[AES-128]
[Authentication Method] (Način autentifikacije)	Odaberite [SHA-256], [SHA-384] ili [SHA-512].

2.2.4 IPsec

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [TCP/IP Setting] (TCP/IP postavka) - [IPsec] - [IPsec Setting] (IPsec postavka)

[IKEv2]

Postavljanje stavke	Preporučena postavka
[Encryption Algorithm] (Algoritam za šifriranje)	[AES-CBC] ([256]/[192 and 256] (192 i 256)/[All] (Sve))
[Authentication Algorithm] (Algoritam za autentifikaciju)	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 i 384)/[384 and 512] (384 i 512)/[All] (Sve)), [AES-XCBC]
[Diffie-Hellman Group] (Grupa Diffie-Hellman)	[Group 14] (Grupa 14), [Group 19] (Grupa 19)

[SA]

Postavljanje stavke	Preporučena postavka
[Encapsulation Mode] (Način spajanja podataka)	[Tunnel] (Tunel), [Transport] (Transport)
[Security Protocol] (Sigurnosni protokol)	[ESP]
[Key Exchange Method] (Način razmjene ključa)	[IKEv2]
[Authentication Method] (Način autentifikacije)	[Digital Signature] (Digitalni potpis)
[ESP Encryption Algorithm] (ESP algoritam za šifriranje)	[AES-GCM] ([256]/[192 and 256] (192 i 256)/[All] (Sve)), [AES-GCM-64] ([256]/[192 and 256] (192 i 256)/[All] (Sve)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 i 256)/[All] (Sve))

Postavljanje stavke	Preporučena postavka
[Perfect Forward Secrecy] (Savršena tajnost prosljeđivanja)	UKLJUČENO
[Diffie-Hellman Group(IKEv2)] (Grupa Diffie-Hellman (IKEv2) - [Priority1-4] (Prioritet 1 - 4)	[Group 14] (Grupa 14), [Group 19] (Grupa 19)

2.2.5 S/MIME

Ako upotrebljavate dodatno S/MIME kad šaljete e-poštu, možete šifrirati sadržaj e-poruke kako biste spriječili otkrivanje sadržaja poruka odnosno prisluškivanje i potvrditi identitet pošiljatelja elektroničkim potpisom. Ovo je učinkovita mjera protiv prijevvara u svrhu obmane ili krađe identiteta.

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [E-mail Setting] (Postavka e-pošte) - [S/MIME]

Postavljanje stavke	Preporučena postavka
[Digital Signature] (Digitalni potpis)	[Always add signature] (Uvijek dodaj potpis)
[Digital Signature Type] (Vrsta digitalnog potpisa)	[SHA-256]
[E-Mail Text Encrypt. Method] (Način šifriranja teksta e-poruke)	[AES-256]

3 Postavljanje značajke Certificate Validation (Provjera certifikata)

Kad se upotrebljava TLS šifriranje poruka radi smanjenja učinka napada tipa "čovjek u sredini", preporučujemo upotrebu provjere certifikata. Za stavke provjere preporučujemo da omogućite minimalno provjeru datuma isteka certifikata i lanca.

Pri pokušaju povezivanja s nekim okruženjem sa starijim postavkama koje nema funkciju provjere certifikata, rizik napada tipa "čovjek u sredini" se smanjuje. Preporučujemo da funkciju upotrebljavate u okruženju sigurne mreže.

Provjera certifikata na strani MFP-a preporučuje se za funkcije MFP klijenta u nastavku. Detalje o lokacijama postavke potražite u odjeljcima u nastavku.

POP, SMTP (Start TLS/SMTP over SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel

Savjeti

Provjera certifikata na strani klijenta povezanog s MFP-om preporučuje se za sljedeće funkcije MFP poslužitelja.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCPSocket

3.1 POP

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [E-mail Setting] (Postavka e-pošte) - [E-mail RX (POP)] (E-pošta RX (POP))

Postavljanje stavke	Preporučena postavka
[Certificate Verification Level Settings] (Postavke razine provjere certifikata)	[Expiration Date] (Datum isteka): UKLJUČENO [Chain] (Lanac): UKLJUČENO

3.2 SMTP

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [E-mail Setting] (Postavka e-pošte) - [E-mail TX (SMTP)] (E-pošta TX (SMTP))

Postavljanje stavke	Preporučena postavka
[Certificate Verification Level Settings] (Postavke razine provjere certifikata)	[Expiration Date] (Datum isteka): UKLJUČENO [Chain] (Lanac): UKLJUČENO

3.3 IEEE802.1X Auth

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [IEEE802.1X Authentication Setting] (Postavka autentifikacije za IEEE802.1X) - [IEEE802.1X Authentication Setting] (Postavka autentifikacije za IEEE802.1X) - [Supplicant Setting] (Postavke pošiljatelja)

Postavljanje stavke	Preporučena postavka
[Certificate Verification Level Settings] (Postavke razine provjere certifikata)	[Expiration Date] (Datum isteka): UKLJUČENO [Chain] (Lanac): UKLJUČENO

3.4 IPsec

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [TCP/IP Setting] (TCP/IP postavka) - [IPsec] - [Enable IPsec] (Omogući IPsec)

Postavljanje stavke	Preporučena postavka
[Certificate Verification Level Settings] (Postavke razine provjere certifikata)	[Expiration Date] (Datum isteka): [Confirm] (Potvrdi) [Chain] (Lanac): [Confirm] (Potvrdi)

Savjeti

Pod stavkom [IPsec Setting] (IPsec postavka) registrirajte stavke [IKE], [SA], [Peer] (Glavni) i [Protocol Setting] (Postavka protokola) unaprijed.

3.5 WebDAVClient

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [WebDAV Settings] (WebDAV postavke) - [WebDAV Client Settings] (Postavke WebDAV klijenta)

Postavljanje stavke	Preporučena postavka
[Certificate Verification Level Settings] (Postavke razine provjere certifikata)	[Expiration Date] (Datum isteka): UKLJUČENO [Chain] (Lanac): UKLJUČENO

3.6 LDAP

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [LDAP Setting] (LDAP postavka) - [Setting Up LDAP] (Postavljanje LDAP-a)

Postavljanje stavke	Preporučena postavka
[Certificate Verification Level Settings] (Postavke razine provjere certifikata)	[Expiration Date] (Datum isteka): UKLJUČENO [Chain] (Lanac): UKLJUČENO

3.7 DPWS

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [DPWS Settings] (DPWS postavke) - [DPWS Common Settings] (Uobičajene DPWS postavke)

Postavljanje stavke	Preporučena postavka
[Certificate Verification Level Settings] (Postavke razine provjere certifikata)	[Expiration Date] (Datum isteka): UKLJUČENO [Chain] (Lanac): UKLJUČENO

3.8 OpenAPI

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [OpenAPI Setting] (OpenAPI postavka) - [OpenAPI Setting] (OpenAPI postavka)

Postavljanje stavke	Preporučena postavka
[Certificate Verification Level Settings] (Postavke razine provjere certifikata)	[Expiration Date] (Datum isteka): UKLJUČENO [Chain] (Lanac): UKLJUČENO

3.9 RemotePanel

Lokacija postavke: [Utility] (Uslužni program) - [Administrator] (Administrator) - [Network] (Mreža) - [Remote Panel Settings] (Postavke za RemotePanel) - [Remote Panel Client Settings] (Postavke RemotePanel klijenta)

Postavljanje stavke	Preporučena postavka
[Certificate Verification Level Settings] (Postavke razine provjere certifikata)	[Expiration Date] (Datum isteka): UKLJUČENO [Chain] (Lanac): UKLJUČENO

4 Dodatne sigurnosne informacije

4.1 Preporuka za najbolju praksu

Preporučujemo upotrebu algoritama za šifriranje u skladu s najboljom praksom i preporukama iz EUCC smjernica za šifriranje te potvrđenih mehanizama za šifriranje SOGIS.

U nastavku se nalaze algoritmi za šifriranje i duljine ključeva u skladu s preporukama iz EUCC smjernica za šifriranje i iz potvrđenih mehanizama za šifriranje SOGIS.

Predmet	Preporučena postavka
Algoritmi za šifriranje	AES (eng. Advanced Encryption Standard) RSA (eng. Rivest-Shamir-Adleman) SHA-2 (eng. Secure Hash Algorithm 2) ECC (eng. Elliptic Curve Cryptography) HMAC (eng. Hash-based Message Authentication Code)
Duljina ključa za šifriranje	RSA: 2048 bitova ili više ECC: 256 bitova ili više AES: 256 bitova

Savjeti

Detalje potražite u najnovijim EUCC smjernicama za šifriranje i potvrđenim mehanizmima za šifriranje SOGIS.

4.2 Mjere opreza pri komunikaciji sa sustavima sa starijim postavkama

Protokoli i verzije navedeni u nastavku predviđeni su za komunikaciju sa starijim verzijama sustava.

Upotreba starijih postavki povećava sigurnosne rizike, pa starije postavke upotrebljavate u sigurnom mrežnom okruženju.

Predmet	Starije postavke
Protokol	SLP FTP SMB (3.0 ili novija verzija, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Depend on Server/OFF) DPWS TCPSocket
Algoritmi za šifriranje	SHA-1 (eng. Secure Hash Algorithm 1) DES (eng. Data Encryption Standard) 3DES (eng. Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Duljina ključa za šifriranje	RSA: 1024 bita ili više ECC: 160 bitova ili više AES: 128 bitova ili više DES: 56 bitova 3DES: 112 bitova

Starije postavke za IPsec

[IKEv1]

Postavljanje stavke	Starije postavke
[Encryption Algorithm] (Algoritam za šifriranje)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 i 192))
[Authentication Algorithm] (Algoritam za autentifikaciju)	Ne upotrebljava se
[Diffie-Hellman Group] (Grupa Diffie-Hellman)	[Group 1] (Grupa 1), [Group 2] (Grupa 2), [Group 5] (Grupa 5)

[IKEv2]

Postavljanje stavke	Starije postavke
[Encryption Algorithm] (Algoritam za šifriranje)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 i 192))
[Authentication Algorithm] (Algoritam za autentifikaciju)	Ne upotrebljava se
[Diffie-Hellman Group] (Grupa Diffie-Hellman)	[Group 1] (Grupa 1), [Group 2] (Grupa 2), [Group 5] (Grupa 5)

[SA]

Postavljanje stavke	Starije postavke
[Key Exchange Method] (Način razmjene ključa)	[IKEv1]
[Authentication Method] (Način autentifikacije)	[Digital Signature] (Digitalni potpis)
[ESP Encryption Algorithm] (ESP algoritam za šifriranje)	[3DES-CBC] ([128]/[192]/[128 and 192] (128 i 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 i 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 i 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 i 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 i 192))
[Perfect Forward Secrecy] (Savršena tajnost prosljeđivanja)	UKLJUČENO
[Diffie-Hellman Group(IKEv1)] (Grupa Diffie-Hellman (IKEv1))	[Group 1] (Grupa 1), [Group 2] (Grupa 2), [Group 5] (Grupa 5)

4.3 Tvornički zadana aktivirana mrežna sučelja i popis usluga

Vrsta usluge	Protokol	Broj porta
DHCP	UDP	68
HTTP poslužitelj	TCP	80
Naziv usluge NETBIOS	UDP	137
Datagram usluge NETBIOS	UDP	138
SNMP	UDP	161
HTTP poslužitelj preko SSL-a / IPP preko SSL-a	TCP	443
LPD ispis	TCP	515
DHCPv6 klijent	UDP	546
IPP ispis	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS alat)	TCP	8091
RAW ispis	TCP	9100
RAW ispis	TCP	9112
RAW ispis	TCP	9113
RAW ispis	TCP	9114
RAW ispis	TCP	9115
RAW ispis	TCP	9116
OpenAPI	TCP	50001

4.4 Informacije o potvrdi unosa

Za broj znakova koje treba unijeti za, primjerice, mrežne postavke, pogledajte svaku od stavki u korisničkom vodiču.

Ovisno o šifriranju, najveći dopušteni broj za unos (podataka koji je pohranjen u MFP) za stavke koje podržavaju znakove s više bajtova može biti do trostruko veći od broja znakova.

Ajánlások a biztonságos hálózati eszközökre vonatkozóan



Tartalomjegyzék

1 Az IP szűrés beállítása

1.1	IP szűrés	1-3
1.2	Gyors IP szűrés	1-4

2 A titkosított kommunikáció beállítása

2.1	TLS titkosítás.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP Socket.....	2-6
2.2	Egyéb titkosítás.....	2-7
2.2.1	SMBServer	2-7
	SMB titkosítás.....	2-7
	SMB aláírás.....	2-7
2.2.2	SMBCClient	2-7
2.2.3	SNMP	2-8
2.2.4	IPSEC.....	2-8
2.2.5	S/MIME	2-9

3 A tanúsítvány érvényesítésének beállítása

3.1	POP.....	3-10
3.2	SMTP	3-11
3.3	IEEE802.1X Auth.....	3-12
3.4	IPSEC	3-13
3.5	WebDAVClient	3-14
3.6	LDAP.....	3-15
3.7	DPWS	3-16
3.8	OpenAPI	3-17
3.9	RemotePanel	3-18

4 További biztonsági információ

4.1	Legjobb gyakorlatok ajánlása.....	4-19
4.2	Óvintézkedések a régebbi rendszerekkel való kommunikációhoz.....	4-20
	IPsec örökölt beállítások.....	4-20
4.3	Gyári beállítással elérhető hálózati interfészek és szolgáltatások	4-22
4.4	A bevitel érvényesítéséről	4-23



A kézikönyvről

Ez a kézikönyv olyan információkat és beállításokat ismertet, amelyek lehetővé teszik a készülékek biztonságos használatát.

Amikor a készüléket egy hálózathoz csatlakoztatja, csak egy tűzfalal védett környezetben használja. Javasoljuk továbbá, hogy a készülék IP-címéhez állítson be egy privát IP-címet.

A privát IP-cím beállítása csak egy helyi hálózat, például egy belső helyi hálózat felhasználóinak teszi lehetővé a gép elérését, megakadályozva a kívülről érkező illetéktelen hozzáférést.

Ha globális IP-címet kell használnia, gondoskodjon arról, hogy a készüléket egy tűzfalal védetten telepítse.

1 Az IP szűrés beállítása

Az IP szűrés funkcióval az IP-cím alapján lehet korlátozni a készülék elérését az egyes eszközökről. A funkció megfelelő beállításával korlátozhatja a hozzáférést az arra nem jogosult eszközökről.

Az IP szűrés funkciót az alábbi két módszer egyikével lehet beállítani a készüléken:

1.1 IP szűrés

Kézi módon meghatározva az IP-címtartományt, amelynek engedélyezni vagy tiltani kívánja a hozzáférést.

Beállítási hely: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IP Address Filtering] (Kezelőprogram - Felügyelő - Hálózat - TCP/IP beállítás - IP szűrés)

Tippek

Állítsa be a környezetének megfelelően az engedélyezett vagy megtagadott IP-címeket.

1.2 Gyors IP szűrés

Az IP-cím tartomány, amely részére engedélyezett a hozzáférés, automatikusan kerül beállításra, a készülék IP-címe és a beállított alhálózati maszk alapján.

Beállítási hely: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [Quick IP Filtering] (Kezelőprogram - Felügyelő - Hálózat - TCP/IP beállítás - Gyors IP szűrés)

Ajánlott beállítások: [Synchronize IP Address]/[Synchronize Subnet Mask] (IP-cím szinkronizálása/Alhálózati maszk szinkronizálása)*

* Válassza ki a környezetének megfelelőt.

2 A titkosított kommunikáció beállítása

Az adatok lehallgatásának, meghamisításának és a munkamenet eltérítésének megakadályozása érdekében javasoljuk, hogy a következő titkosított kommunikációt használja.

2.1 TLS titkosítás

A sebezhetőségek kockázatának csökkentése érdekében javasoljuk, hogy konfigurálja a következő beállításokat.

Beállítási hely: [Utility] - [Administrator] - [Security] - [PKI Settings] - [Enable SSL Version] (Kezelőprogram - Felügyelő - Biztonság - PKI beállítások - SSL-verzió engedélyezése)

Beállítási elem	Ajánlott beállítás
[Mode using SSL/TLS] (SSL/TLS-t használó mód)	[Admin. Mode and User Mode] (Felügy. mód és felhasználói mód)
[SSL/TLS Version Setting] (SSL/TLS verzió beállítása)	TLS1.2 TLS1.3 (IEEE802.1X incompatibilis)
[Encryption Strength] (Titkosítási erősség)	AES-256

A kezdeti tanúsítványt a gyárban telepítik. Ha más tanúsítványra van szüksége, regisztráljon újat a következő helyen.

Beállítási hely: [Utility] - [Administrator] - [Security] - [PKI Settings] - [Device Certificate Setting] (Kezelőprogram - Felügyelő - Biztonság - PKI beállítások - Eszköztanúsítvány beállítása)

Beállítási elem	Ajánlott beállítás
[Encryption Key Type] (Titkosító kulcs típusa)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

A TLS-titkosítás a következő protokollok és szolgáltatások esetében támogatott. A beállítások részleteit lásd az alábbi szakaszokban.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP Socket

2.1.1 HTTP (Web Connection)

Ha engedélyezi az [Enable SSL Version] (SSL-verzió engedélyezése) lehetőséget, a kommunikációs mód automatikusan átvált a TLS titkosított kommunikációra (HTTPS).

2.1.2 WebDAVServer

Beállítási hely: [Utility] - [Administrator] - [Network] - [WebDAV Settings] - [WebDAV Server Settings] (Kezelőprogram - Felügyelő - Hálózat - WebDAV beállítás - WebDAV szerver beállítás)

Beállítási elem	Ajánlott beállítás
[SSL Settings] (SSL beállítások)	[SSL Only] (Csak SSL)

2.1.3 IPP

Beállítási hely: [Utility] - [Administrator] - [Network] - [HTTP Server Settings] (Kezelőprogram - Felügyelő - Hálózat - HTTP szerver beállítás)

Beállítási elem	Ajánlott beállítás
[IPP-SSL Settings] (IPP-SSL beállítások)	[SSL Only] (Csak SSL)

2.1.4 OpenAPI

Beállítási hely: [Utility] - [Administrator] - [Network] - [OpenAPI Setting] - [OpenAPI Setting] (Kezelőprogram - Felügyelő - Hálózat - OpenAPI beállítás - OpenAPI beállítás)

Beállítási elem	Ajánlott beállítás
[SSL/Port Settings] (SSL/port beállítások)	[SSL Only] (Csak SSL)

2.1.5 RemotePanel

Beállítási hely: [Utility] - [Administrator] - [Network] - [Remote Panel Settings] - [Remote Panel Server Settings] (Kezelőprogram - Felügyelő - Hálózat - Távoli panel beállításai - Távoli panel szerver beállítás)

Beállítási elem	Ajánlott beállítás
[Port No.(SSL)] (Portsám (SSL))	[50443]

Tippek

Ha engedélyezi az [Enable SSL Version] (SSL-verzió engedélyezése) lehetőséget, a kommunikációs mód automatikusan átvált a TLS titkosított módra. Adjon meg egy portszámot.

2.1.6 DPWS

Beállítási hely: [Utility] - [Administrator] - [Network] - [DPWS Settings] - [DPWS Common Settings] (Kezelőprogram - Felügyelő - Hálózat - DPWS beállítás - DPWS általános beállítás)

Beállítási elem	Ajánlott beállítás
[SSL beállítás]	BE

2.1.7 POP

Beállítási hely: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail RX (POP)] (Kezelőprogram - Felügyelő - Hálózat - E-mail beállítás - E-mail vétel (POP))

Beállítási elem	Ajánlott beállítás
[Enable SSL] (SSL engedélyezése)	BE

2.1.8 SMTP

Beállítási hely: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail TX (SMTP)] (Kezelőprogram - Felügyelő - Hálózat - E-mail beállítás - E-mail tx (SMTP))

Beállítási elem	Ajánlott beállítás
[SSL/TLS Settings] (SSL/TLS beállítások)	[SMTP over SSL]

2.1.9 IEEE802.1X Auth

Beállítási hely: [Utility] - [Administrator] - [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Setting] - [Supplicant Setting] (Kezelőprogram - Felügyelő - Hálózat - IEEE802.1X hitelesítés beállítás - IEEE802.1X hitelesítés beállítás - Ügyfél beállítás)

Beállítási elem	Ajánlott beállítás
[EAP-Type]	Válassza a következőt: [EAP-TLS], [EAP-TTLS] vagy [PEAP].

2.1.10 LDAP

Beállítási hely: [Utility] - [Administrator] - [Network] - [LDAP Setting] - [Setting Up LDAP] (Kezelőprogram - Felügyelő - Hálózat - LDAP beállítás - LDAP beállítása)

Beállítási elem	Ajánlott beállítás
[Enable SSL] (SSL engedélyezése)	BE

2.1.11 TCP Socket

Beállítási hely: [Utility] - [Administrator] - [Network] - [TCP Socket Setting] (Kezelőprogram - Felügyelő - Hálózat - TCP Socket beállítás)

Beállítási elem	Ajánlott beállítás
[Use SSL/TLS] (SSL/TLS használata)	BE

2.2 Egyéb titkosítás

A sebezhetőségek kockázatának csökkentése érdekében javasoljuk, hogy konfigurálja a következő beállításokat. Az egyes funkciók beállításainak részleteit lásd az alábbi szakaszokban.

Funkció	Ajánlott beállítás
SMBServer	SMB titkosítás, SMB aláírás
SMBClient	Kerberos hitelesítés
SNMP	SNMPv3
IPSEC	IKEv2
S/MIME	BE

2.2.1 SMBServer

Az SMB-titkosítás és az SMB-aláírás használatával a következő biztonsági kockázatok csökkenthetők.

- **Lehallgatás:** Egy rosszindulatú harmadik fél lehallgathatja a kommunikációt, és ellophat személyes vagy bizalmas információkat.
- **Adatok meghamisítása:** Fennáll a veszélye annak, hogy a kommunikációs tartalmakat manipulálják egy Man-In-The-Middle Attack (MITM) révén.
- **Azonosítóhamisítás:** Ha a hitelesítési adatokat ellopják, egy harmadik fél jogos felhasználónak adhatja ki magát, hogy jogosulatlan hozzáférést szerezzen.
- **Információszivárogatás:** A titkosítatlan kommunikáció könnyen lehallgatható, különösen a nyilvános Wi-Fi hálózatokon, ami növeli a személyes adatok és a hitelkártyaadatok kiszivárgásának kockázatát.

SMB titkosítás

Előfeltételek

- Hozzon létre egy nyilvános felhasználói fiókot. Emellett konfigurálja a beállítást úgy is, hogy a fájlok automatikusan átkerüljenek a nyilvános felhasználói fiókból, és az SMB mappába mentődjenek.
- Jelszó megadása a felhasználói fiókhoz.

Beállítási hely: [Utility] - [Administrator] - [Box] - [User Box List] (Kezelőprogram - Felügyelő - Felhasználói fiók - Felhasználói fiók lista)

Beállítási elem	Ajánlott beállítás
[SMB Communication Encryption] (SMB kommunikáció titkosítás)	[Encrypt] (Titkosít)

SMB aláírás

Beállítási hely: [Utility] - [Administrator] - [Network] - [SMB Setting] - [SMB Server Settings] (Kezelőprogram - Felügyelő - Hálózat - SMB beállítás - SMB kiszolgáló beállításai)

Beállítási elem	Ajánlott beállítás
[SMB security Signature Setting] (SMB biztonsági aláírás beállítása)	[Required] (Szükséges)

2.2.2 SMBClient

A Kerberos-hitelesítés erős titkosítási technológiát használ, ami jelentősen csökkenti a hitelesítő adatok ellopásának kockázatát a hitelesítési folyamat során. Biztosítja az adatok integritását is, megakadályozva az adatok meghamisítását a feladó és a címzett között, valamint az NTLM relé támadásokat.

Beállítási hely: [Utility] - [Administrator] - [Network] - [SMB Setting] - [Client Setting] (Kezelőprogram - Felügyelő - Hálózat - SMB beállítás - Kliens beállítás)

Beállítási elem	Ajánlott beállítás
[SMB Authentication Setting] (SMB hitelesítési beállítás)	[Kerberos]

2.2.3 SNMP

A titkosítás beállítása az SNMPv3 használatával. Ha a hitelesítési beállítás is hozzáadódik, tovább növelheti a biztonságot. A biztonsági kockázatok nagyjából ugyanazok, mint az SMB esetében.

Beállítási hely: [Utility] - [Administrator] - [Network] - [SNMP Setting] (Kezelőprogram - Felügyelő - Hálózat - SNMP beállítás)

Beállítási elem	Ajánlott beállítás
[SNMP Setting] (SNMP beállítás)	[SNMP v3(IP)]
[Encryption Algorithm] (Titkosítási algoritmus)	[AES-128]
[Authentication Method] (Hitelesítési módszer)	Válassza ki a következők egyikét: [SHA-256], [SHA-384] vagy [SHA-512].

2.2.4 IPSEC

Beállítási hely: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IPsec] - [IPsec Setting] (Kezelőprogram - Felügyelő - Hálózat - TCP/IP beállítás - IPsec - IPsec beállítás)

[IKEv2]

Beállítási elem	Ajánlott beállítás
[Titkosítási algoritmus]	[AES-CBC] ([256]/[192 and 256]/[All]) (AES-CBC (256/192 és 256/Összes))
[Hitelesítési algoritmus]	[SHA-2] ([256]/[384]/[512]/[256 and 384]/[384 and 512]/[All]), [AES-XCBC] (SHA-2 (256/384/512/256 és 384/384 és 512/Összes), AES-XCBC)
[Diffie-Hellman Group] (Diffie-Hellman csoport)	[Group 14], [Group 19] (14. csoport, 19. csoport)

[SA]

Beállítási elem	Ajánlott beállítás
[Encapsulation Mode] (Beágyazás mód)	[Tunnel], [Transport] (Alagút, Szállítóegység)
[Security Protocol] (Biztonsági protokoll)	[ESP]
[Key Exchange Method] (Kulcs konverzió módszere)	[IKEv2]
[Authentication Method] (Hitelesítési módszer)	[Digital Signature] (Digitális aláírás)
[ESP Encryption Algorithm] (ESP titkos. algoritmus)	[AES-GCM] ([256]/[192 and 256]/[All]), [AES-GCM-64] ([256]/[192 and 256]/[All]), [ENC_NULL_AES_GMAC] ([256]/[192 and 256]/[All]) (AES-GCM (256/192 és 256/Összes), AES-GCM-64 (256/192 és 256/Összes), ENC_NULL_AES_GMAC (256/192 és 256/Összes))

Beállítási elem	Ajánlott beállítás
[Perfect Forward Secrecy] (Sérülés utáni titkosságvédelem)	BE
[Diffie-Hellman Group (IKEv2)] - [Priority1-4] (Diffie-Hellman csoport (IKEv2) - Prioritás 1-4)	[Group 14], [Group 19] (14. csoport, 19. csoport)

2.2.5 S/MIME

Ha az opcionális S/MIME-t használja e-mail küldéséhez, titkosíthatja az e-mail tartalmát a lehallgatás megakadályozása érdekében, és elektronikus aláírással igazolhatja a feladó személyazonosságát. Ez hatékony intézkedés azonosítóhamisítás és adathalász csalások ellen.

Beállítási hely: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [S/MIME] (Kezelőprogram - Felügyelő - Hálózat - E-mail beállítás - S/MIME)

Beállítási elem	Ajánlott beállítás
[Digital Signature] (Digitális aláírás)	[Always add signature] (Mindig aláírással)
[Digital Signature Type] (Digitális aláírás típusa)	[SHA-256]
[E-Mail Text Encrypt. Method] (E-mail szöveg titkosítási mód)	[AES-256]

3 A tanúsítvány érvényesítésének beállítása

A TLS titkosított kommunikáció használatakor a man-in-the-middle támadások hatásának csökkentése érdekében javasoljuk a tanúsítvány-érvényesítés használatát. Az érvényesítési elemek esetében javasoljuk, hogy legalább a tanúsítvány lejárat dátumát és láncát engedélyezze.

Ha olyan hagyományos környezethez próbálnak csatlakozni, amely nem rendelkezik tanúsítvány-érvényesítési funkcióval, megnő a man-in-the-middle támadások kockázata. Javasoljuk, hogy biztonságos hálózati környezetben használja.

Az MFP-oldalon a tanúsítvány érvényesítését a következő MFP-ügyfélfunkciókban ajánljuk. A beállítások részleteit lásd az alábbi szakaszokban.

POP, SMTP (Start TLS/SMTP over SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel

Tippek

A kliensoldalon az MFP-hez csatlakoztatva a tanúsítvány érvényesítését a következő MFP-ügyfélfunkciókban ajánljuk.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP Socket

3.1 POP

Beállítási hely: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail RX (POP)] (Kezelőprogram - Felügyelő - Hálózat - E-mail beállítás - E-mail vétel (POP))

Beállítási elem	Ajánlott beállítás
[Certificate Verification Level Settings] (Tanúsítvány ellenőrzési szintjének beállítása)	[Expiration Date] (Lejárat dátuma): BE [Chain] (Lánc): BE

3.2 SMTP

Beállítási hely: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail TX (SMTP)] (Kezelőprogram - Felügyelő - Hálózat - E-mail beállítás - E-mail tx (SMTP))

Beállítási elem	Ajánlott beállítás
[Certificate Verification Level Settings] (Tanúsítvány ellenőrzési szintjének beállítása)	[Expiration Date] (Lejárat dátuma): BE [Chain] (Lánc): BE

3.3 IEEE802.1X Auth

Beállítási hely: [Utility] - [Administrator] - [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Setting] - [Supplicant Setting] (Kezelőprogram - Felügyelő - Hálózat - IEEE802.1X hitelesítés beállítás - IEEE802.1X hitelesítés beállítás - Ügyfél beállítás)

Beállítási elem	Ajánlott beállítás
[Certificate Verification Level Settings] (Tanúsítvány ellenőrzési szintjének beállítása)	[Expiration Date] (Lejárat dátuma): BE [Chain] (Lánc): BE

3.4 IPSEC

Beállítási hely: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IPsec] - [Enable IPsec]
(Kezelőprogram - Felügyelő - Hálózat - TCP/IP beállítás - IPsec - IPsec engedélyezés)

Beállítási elem	Ajánlott beállítás
[Certificate Verification Level Settings] (Tanúsítvány ellenőrzési szintjének beállítása)	[Expiration Date] (Lejárat dátuma): [Confirm] (Száml./ jel.) [Chain] (Lánc): [Confirm] (Száml./ jel.)

Tippek

Az [IPsec Setting] (IPsec beállítás) alatt regisztrálja előre az [IKE], [SA], [Peer] (Társ) és [Protocol Setting] (Protokoll beállítása) elemeket.

3.5 WebDAVClient

Beállítási hely: [Utility] - [Administrator] - [Network] - [WebDAV Settings] - [WebDAV Client Settings]
(Kezelőprogram - Felügyelő - Hálózat - WebDAV beállítás - WebDAV kliens beállítás)

Beállítási elem	Ajánlott beállítás
[Certificate Verification Level Settings] (Tanúsítvány ellenőrzési szintjének beállítása)	[Expiration Date] (Lejárat dátuma): BE [Chain] (Lánc): BE

3.6 LDAP

Beállítási hely: [Utility] - [Administrator] - [Network] - [LDAP Setting] - [Setting Up LDAP] (Kezelőprogram - Felügyelő - Hálózat - LDAP beállítás - LDAP beállítás)

Beállítási elem	Ajánlott beállítás
[Certificate Verification Level Settings] (Tanúsítvány ellenőrzési szintjének beállítása)	[Expiration Date] (Lejárat dátuma): BE [Chain] (Lánc): BE

3.7 DPWS

Beállítási hely: [Utility] - [Administrator] - [Network] - [DPWS Settings] - [DPWS Common Settings]
(Kezelőprogram - Felügyelő - Hálózat - DPWS beállítás - DPWS általános beállítás)

Beállítási elem	Ajánlott beállítás
[Certificate Verification Level Settings] (Tanúsítvány ellenőrzési szintjének beállítása)	[Expiration Date] (Lejárat dátuma): BE [Chain] (Lánc): BE

3.8 OpenAPI

Beállítási hely: [Utility] - [Administrator] - [Network] - [OpenAPI Setting] - [OpenAPI Setting] (Kezelőprogram - Felügyelő - Hálózat - OpenAPI beállítás - OpenAPI beállítás)

Beállítási elem	Ajánlott beállítás
[Certificate Verification Level Settings] (Tanúsítvány ellenőrzési szintjének beállítása)	[Expiration Date] (Lejárat dátuma): BE [Chain] (Lánc): BE

3.9 RemotePanel

Beállítási hely: [Utility] - [Administrator] - [Network] - [Remote Panel Settings] - [Remote Panel Client Settings] (Kezelőprogram - Felügyelő - Hálózat - Távoli panel beállításai - Távoli panel kliens beállítás)

Beállítási elem	Ajánlott beállítás
[Certificate Verification Level Settings] (Tanúsítvány ellenőrzési szintjének beállítása)	[Expiration Date] (Lejárat dátuma): BE [Chain] (Lánc): BE

4 További biztonsági információ

4.1 Legjobb gyakorlatok ajánlása

Javasoljuk, hogy az alkalmazandó titkosítási algoritmusok feleljenek meg az EUCC kriptográfiára vonatkozó iránymutatásaiban és a SOGIS-Agreed-Cryptographic-Mechanisms (SOGIS-egyezményes kriptográfiai mechanizmusok) által ajánlott legjobb gyakorlatnak.

Az alábbiakban az EUCC kriptográfiára vonatkozó iránymutatásai és a SOGIS-Agreed-Cryptographic-Mechanisms által ajánlott titkosítási algoritmusok és kulcshosszok listája található.

Elem	Ajánlott beállítás
Titkosítási algoritmusok	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Titkosító kulcs hossza	RSA: legalább 2048 bit ECC: legalább 256 bit AES: 256 bit

Tippek

A részleteket lásd az EUCC legújabb kriptográfiai iránymutatásaiban és a SOGIS-Agreed-Cryptographic-Mechanisms című dokumentumban.

4.2 Övintézkedések a régebbi rendszerekkel való kommunikációhoz

A következő protokollokat és verziókat feltételezzük a régi rendszerekkel való kommunikációhoz.

A régi beállítások használata növeli a biztonsági kockázatokat, ezért kérjük, hogy biztonságos hálózati környezetben használja őket.

Elem	Örökölt beállítások
Protokoll	SLP FTP SMB (3.0 vagy korábbi verzió, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Szervertől függ/OFF) DPWS TCPsocket
Titkosítási algoritmusok	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Titkosító kulcs hossza	RSA: 1024 bit vagy kevesebb ECC: 160 bit vagy kevesebb AES: 128 bit vagy kevesebb DES: 56 bit 3DES: 112 bit

IPsec örökölt beállítások

[IKEv1]

Beállítási elem	Örökölt beállítások
[Titkosítási algoritmus]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 és 192))
[Authentication Algorithm] (Hitelesítési algoritmus)	Nem használt
[Diffie-Hellman Group] (Diffie-Hellman csoport)	[Group 1], [Group 2], [Group 5] (1. csoport, 2. csoport, 5. csoport)

[IKEv2]

Beállítási elem	Örökölt beállítások
[Encryption Algorithm] (Titkosítási algoritmus)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 és 192))
[Authentication Algorithm] (Hitelesítési algoritmus)	Nem használt
[Diffie-Hellman Group] (Diffie-Hellman csoport)	[Group 1], [Group 2], [Group 5] (csoport, 2. csoport, 5. csoport)

[SA]

Beállítási elem	Örökölt beállítások
[Key Exchange Method] (Kulcs konverzió módszere)	[IKEv1]
[Authentication Method] (Hitelesítési módszer)	[Digital Signature] (Digitális aláírás)

Beállítási elem	Örökölt beállítások
[ESP Encryption Algorithm] (ESP titkos. algoritmus)	[3DES-CBC] ([128]/[192]/[128 and 192] (128 és 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 és 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 és 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 és 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 és 192))
[Perfect Forward Secrecy] (Sérülés utáni titkosságvédelem)	BE
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellman csoport (IKEv1))	[Group 1], [Group 2], [Group 5] (1. csoport, 2. csoport, 5. csoport)

4.3 Gyári beállítással elérhető hálózati interfészek és szolgáltatások

Szolgáltatás típusa	Protokoll	Portszám
DHCP	UDP	68
HTTP szerver	TCP	80
NETBIOS név szolgáltatás	UDP	137
NETBIOS Datagram szolgáltatás	UDP	138
SNMP	UDP	161
HTTP Server over SSL / IPP over SSL	TCP	443
LPD nyomtatás	TCP	515
DHCPv6 kliens	UDP	546
IPP nyomtatás	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-eszköz)	TCP	8091
RAW nyomtatás	TCP	9100
RAW nyomtatás	TCP	9112
RAW nyomtatás	TCP	9113
RAW nyomtatás	TCP	9114
RAW nyomtatás	TCP	9115
RAW nyomtatás	TCP	9116
OpenAPI	TCP	50001

4.4 A bevitel érvényesítéséről

A hálózati beállításokhoz stb. beírandó karakterek számát lásd a Felhasználói kézikönyv egyes beállítási elemeinél.

A nyelv kódolásától függően a többbájtos karaktereket támogató elemek esetében a maximálisan megengedett bemeneti érték (az MFP-ben elmentett adatok) a karakterek számának háromszorosa lehet.

Rekomendacijos dėl saugių tinklo įrenginių



Turinys

1 IP adreso filtravimo nustatymas

1.1	IP adreso filtravimas	1-3
1.2	Spartusis IP filtravimas.....	1-3

2 Šifruoto ryšio nustatymas

2.1	TLS šifravimas	2-4
2.1.1	HTTP (Web Connection)	2-5
2.1.2	WebDAVServer	2-5
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-6
2.1.8	SMTP	2-6
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP jungtis.....	2-6
2.2	Kitas šifravimas.....	2-7
2.2.1	SMBServer	2-7
	SMB šifravimas	2-7
	SMB parašas.....	2-7
2.2.2	SMBClient	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Sertifikato patvirtinimo nustatymas

3.1	POP.....	3-10
3.2	SMTP	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	RemotePanel	3-12

4 Papildoma saugos informacija

4.1	Geriausios praktikos rekomendacijos	4-13
4.2	Atsargumo priemonės dėl ryšio su senosiomis sistemomis	4-14
	IPsec senesni nustatymai	4-14
4.3	Tinklo sąsajos ir paslaugos prieinamos nuo pat išsiuntimo iš gamyklos.....	4-16
4.4	Apie įvesties patvirtinimą	4-17



Apie šį vadovą

Šiame vadove aprašoma informacija ir nustatymai, leidžiantys saugiai naudoti įrenginius.

Jungdami šį įrenginį prie tinklo, naudokite jį užkarda apsaugotoje aplinkoje. Taip pat rekomenduojame nustatyti privatų įrenginio IP adresą.

Nustačius privatų IP adresą, prie įrenginio gali prisijungti tik vietinio tinklo, pvz., vidinio LAN, naudotojai, o neteisėta prieiga iš išorės neleidžiama.

Jei reikia naudoti visuotinį IP adresą, būtinai įdėkite užkardą šiame įrenginyje.

1 IP adreso filtravimo nustatymas

IP adreso filtravimas yra funkcija, ribojanti kitų įrenginių prieigą prie šio įrenginio pagal IP adresą. Tinkamai nustačius šią funkciją galima apriboti prieigą iš neteisėtų įrenginių.

Šio įrenginio IP adreso filtravimo funkciją galima nustatyti bet kuriuo iš toliau nurodytų dviejų būdų.

1.1 IP adreso filtravimas

Rankiniu būdu nurodykite IP adresų diapazoną, kuriam norite leisti arba drausti prieigą.

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [TCP/IP Setting] (TCP/IP nustatymas) - [IP Address Filtering] (IP adresų filtravimas)

Patarimai

Nustatykite leidžiamus arba draudžiamus IP adresus, kad jie atitiktų jūsų aplinką.

1.2 Spartusis IP filtravimas

IP adresų diapazonas, kuriam automatiškai suteikiama prieiga pagal IP adresą ir šio įrenginio potinklio kaukės nustatymą.

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [TCP/IP Setting] (TCP/IP nustatymas) - [Quick IP Filtering] (Greitas IP filtravimas)

Rekomenduojami nustatymai: [Synchronize IP Address] (Sinchronizuoti IP adresą) / [Synchronize Subnet Mask] (Sinchronizuoti potinklio kaukę)*

* Pasirinkite bet kurį iš jų, kad tiktų jūsų aplinkai.

2 Šifruoto ryšio nustatymas

Kad išvengtumėte duomenų perėmimo, duomenų klastojimo ir sesijos užgrobimo, rekomenduojame naudoti šifruotą ryšį.

2.1 TLS šifravimas

Rekomenduojame sukonfigūruoti šiuos nustatymus, kad sumažintumėte pažeidžiamumo riziką.

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Security] (Sauga) - [PKI Settings] (PKI nustatymai) - [Enable SSL Version] (Leisti SSL versiją)

Nustatomas elementas	Rekomenduojamas nustatymas
[Mode using SSL/TLS] (SSL/TLS naudojimo režimas)	[Admin. Mode and User Mode] (Admin. režimas ir naudotojo režimas)
[SSL/TLS Version Setting] (SSL/TLS versijos nustatymas)	TLS1.2 TLS1.3 (nesuderinamas su IEEE802.1X)
[Encryption Strength] (Šifravimo stiprumas)	AES-256

Pirminis sertifikatas yra įdiegtas gamykloje. Jei reikia kitokio sertifikato, užregistruokite naują sertifikatą toliau nurodytoje vietoje.

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Security] (Sauga) - [PKI Settings] (PKI nustatymai) - [Device Certificate Setting] (Įrenginio sertifikato nustatymas)

Nustatomas elementas	Rekomenduojamas nustatymas
[Encryption Key Type] (Šifravimo rakto tipas)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

TLS šifravimas palaikomas šiems protokolams ir paslaugoms. Išsamesnės informacijos apie nustatymų vietas rasite tolesniuose skyriuose.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP jungtis

2.1.1 HTTP (Web Connection)

Jei įjungiate [Enable SSL Version] (Leisti SSL versiją), ryšio režimas automatiškai persijungia į TLS šifruotą ryšį. (HTTPS).

2.1.2 WebDAVServer

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [WebDAV Settings] (WebDAV nustatymai) - [WebDAV Server Settings] (WebDAV serverio nustatymai)

Nustatomas elementas	Rekomenduojamas nustatymas
[SSL Settings] (SSL nustatymai)	[SSL Only] (Tik SSL)

2.1.3 IPP

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [HTTP Server Settings] (HTTP serverio nustatymai)

Nustatomas elementas	Rekomenduojamas nustatymas
[IPP-SSL Settings] (IPP-SSL nustatymai)	[SSL Only] (Tik SSL)

2.1.4 OpenAPI

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [OpenAPI Setting] (OpenAPI nustatymas) - [OpenAPI Setting] (OpenAPI nustatymas)

Nustatomas elementas	Rekomenduojamas nustatymas
[SSL/Port Settings] (SSL / prievaro nustatymai)	[SSL Only] (Tik SSL)

2.1.5 RemotePanel

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [Remote Panel Settings] (Nuotolinio valdymo skydelio nustatymai) - [Remote Panel Server Settings] (Nuotolinio valdymo skydelio serverio nustatymai)

Nustatomas elementas	Rekomenduojamas nustatymas
[Port No.(SSL)] (Prievaro Nr. (SSL))	[50443]

Patarimai

Jei įjungiate [Enable SSL Version] (Leisti SSL versiją), ryšys automatiškai persijungia į TLS šifruotąjį režimą. Nurodykite prievaro numerį.

2.1.6 DPWS

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [DPWS Settings] (DPWS nustatymai) - [DPWS Common Settings] (DPWS bendrieji nustatymai)

Nustatomas elementas	Rekomenduojamas nustatymas
[SSL Settings] (SSL nustatymai)	ON (Įjungtas)

2.1.7 POP

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [E-mail Setting] (El. pašto nustatymai) - [E-mail RX (POP)] (El. pašto RX (POP))

Nustatomas elementas	Rekomenduojamas nustatymas
[Enable SSL] (Leisti SSL)	ON (Įjungtas)

2.1.8 SMTP

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [E-mail Setting] (El. pašto nustatymai) - [E-mail TX (SMTP)] (El. pašto TX (SMTP))

Nustatomas elementas	Rekomenduojamas nustatymas
[SSL/TLS Settings] (SSL/TLS nustatymai)	[SMTP over SSL] (SMTP per SSL)

2.1.9 IEEE802.1X Auth

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentikavimo nustatymas) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentikavimo nustatymas) - [Supplicant Setting] (Prašytojo nustatymas)

Nustatomas elementas	Rekomenduojamas nustatymas
[EAP-Type] (EAP tipas)	Pasirinkite [EAP-TLS], [EAP-TTLS] arba [PEAP].

2.1.10 LDAP

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [LDAP Setting] (LDAP nustatymas) - [Setting Up LDAP] (LDAP sąranka)

Nustatomas elementas	Rekomenduojamas nustatymas
[Enable SSL] (Leisti SSL)	ON (Įjungtas)

2.1.11 TCP jungtis

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [TCP Socket Setting] (TCP jungties nustatymas)

Nustatomas elementas	Rekomenduojamas nustatymas
[Use SSL/TLS] (Naudoti SSL/TLS)	ON (Įjungtas)

2.2 Kitas šifravimas

Rekomenduojame sukonfigūruoti šiuos nustatymus, kad sumažintumėte pažeidžiamumo riziką. Išsamesnės informacijos apie kiekvieną funkciją rasite tolesniuose skyriuose.

Funkcija	Rekomenduojamas nustatymas
SMBServer	SMB šifravimas, SMB parašas
SMBCClient	"Kerberos" autentifikavimas
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	ON (Įjungtas)

2.2.1 SMBServer

Naudojant SMB šifravimą ir SMB parašą galima sumažinti toliau aprašytas saugumo rizikas.

- Duomenų perėmimas: Piktavališka trečioji šalis gali perimti pranešimus ir pavogti asmeninę ar konfidencialią informaciją.
- Duomenų klastojimas: kyla pavojus, kad komunikacijos turinys gali būti suklastotas naudojant "žmogaus viduryje" (angl. "Man-In-The-Middle", MITM) ataką.
- Apsimetinėjimas: jei autentifikavimo informacija pavagiama, trečioji šalis gali apsimesti teisėtu naudotoju ir gauti neteisėtą prieigą.
- Informacijos nutekėjimas: neužšifruotus pranešimus galima lengvai perimti, ypač viešuosiuose "Wi-Fi" tinkluose, todėl didėja rizika, kad bus nutekinta asmeninė informacija ir kredito kortelių duomenys.

SMB šifravimas

Būtiniosios sąlygos

- Sukurkite viešąją naudotojo dėžutę. Taip pat sukonfigūruokite nustatymą, kad failai būtų automatiškai perkeltami iš viešosios naudotojo dėžutės ir išsaugomi SMB aplanke.
- Nustatykite naudotojo dėžutės slaptažodį.

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Box] (Dėžutė) - [User Box List] (Naudotojų dėžučių sąrašas)

Nustatomas elementas	Rekomenduojamas nustatymas
[SMB Communication Encryption] (SMB ryšio šifravimas)	[Encrypt] (Šifruoti)

SMB parašas

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [SMB Setting] (SMB nustatymas) - [SMB Server Settings] (SMB serverio nustatymas)

Nustatomas elementas	Rekomenduojamas nustatymas
[SMB security Signature Setting] (SMB saugos parašo nustatymas)	[Required] (Būtinasis)

2.2.2 SMBClient

"Kerberos" autentifikavimui naudojama stipri šifravimo technologija, todėl labai sumažėja rizika, kad autentifikavimo proceso metu įgaliojimai bus pavogti. Taip pat užtikrinamas duomenų vientisumas, užkertant kelią duomenų klastojimui tarp siuntėjo ir gavėjo bei NTLM perdavimo atakoms.

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [SMB Setting] (SMB nustatymas) - [Client Setting] (Kliento nustatymas)

Nustatomas elementas	Rekomenduojamas nustatymas
[SMB Authentication Setting] (SMB autentifikavimo nustatymas)	[Kerberos]

2.2.3 SNMP

Nustatykite šifravimą naudodami SNMPv3. Jei taip pat pridedamas autentifikavimo nustatymas, galima dar labiau padidinti saugumą. Saugos rizika yra maždaug tokia pati kaip ir SMB atveju.

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [SNMP Setting] (SNMP nustatymas)

Nustatomas elementas	Rekomenduojamas nustatymas
[SNMP Setting] (SNMP nustatymas)	[SNMP v3(IP)]
[Encryption Algorithm] (Šifravimo algoritmas)	[AES-128]
[Authentication Method] (Autentifikavimo metodas)	Pasirinkite [SHA-256], [SHA-384] arba [SHA-512].

2.2.4 IPsec

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [TCP/IP Setting] (TCP/IP nustatymas) - [IPsec] - [IPsec Setting] (IPsec nustatymas)

[IKEv2]

Nustatomas elementas	Rekomenduojamas nustatymas
[Encryption Algorithm] (Šifravimo algoritmas)	[AES-CBC] ([256]/[192 ir 256]/[All] (Visi)
[Authentication Algorithm] (Autentifikavimo algoritmas)	[SHA-2] ([256]/[384]/[512]/[256 ir 384]/[384 ir 512]/[All] (Visi), [AES-XCBC]
[Diffie-Hellman Group] (Diffie-Hellman grupė)	[Group 14] (14 grupė), [Group 19] (19 grupė)

[SA]

Nustatomas elementas	Rekomenduojamas nustatymas
[Encapsulation Mode] (Įterpimo režimas)	[Tunnel], [Transport]
[Security Protocol] (Saugos protokolas)	[ESP]
[Key Exchange Method] (Keitimosi raktu metodas)	[IKEv2]
[Authentication Method] (Autentifikavimo metodas)	[Digital Signature] (Skaitmeninis parašas)
[ESP Encryption Algorithm] (ESP šifravimo algoritmas)	[AES-GCM] ([256]/[192 ir 256]/[All]), [AES-GCM-64] ([256]/[192 ir 256]/[All] (visi), [ENC_NULL_AES_GMAC] ([256]/[192 ir 256]/[All] (Visi)

Nustatomas elementas	Rekomenduojamas nustatymas
[Perfect Forward Secrecy] (Puikus persiuntimo slaptumas)	ON (Įjungtas)
[Diffie-Hellman Group(IKEv2)] (Diffie-Hellman grupė (IKEv2) - [Priority1-4] (1–4 Prioritetas))	[Group 14] (14 grupė), [Group 19] (19 grupė)

2.2.5 S/MIME

Jei siųsdami el. laiškus naudojate papildomą S/MIME, galite užšifruoti el. laiško turinį, kad būtų išvengta duomenų perėmimo, ir patvirtinti siuntėjo tapatybę elektroniniu parašu. Tai veiksminga priemonė, padedanti apsisaugoti nuo apsimetinėjimo ir sukčiavimo.

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [E-mail Setting] (El. pašto nustatymas) - [S/MIME]

Nustatomas elementas	Rekomenduojamas nustatymas
[Digital Signature] (Skaitmeninis parašas)	[Always add signature] (Visada pridėti parašą)
[Digital Signature Type] (Skaitmeninio parašo tipas)	[SHA-256]
[E-Mail Text Encrypt. Method] (El. laiškų teksto šifrav. metodas)	[AES-256]

3 Sertifikato patvirtinimo nustatymas

Naudojant TLS šifruotą ryšį ir siekiant sumažinti "žmogaus viduryje" (MITM) atakų poveikį, rekomenduojame naudoti sertifikato patvirtinimą. Patvirtinimo elementams rekomenduojame įjungti bent jau sertifikato galiojimo datą ir grandinę.

Jei bandoma prisijungti prie senesnės aplinkos, neturinčios sertifikato patvirtinimo funkcijos, padidėja MITM atakų rizika. Rekomenduojame jį naudoti saugioje tinklo aplinkoje.

Sertifikato patvirtinimą MFP pusėje rekomenduojama naudoti toliau nurodytose MFP kliento funkcijose. Išsamesnės informacijos apie nustatymų vietas rasite tolesniuose skyriuose.

POP, SMTP (Start TLS/SMTP over SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel

Patarimai

Sertifikato patvirtinimą kliento pusėje, prijungtoje prie MFP, rekomenduojama naudoti toliau nurodytose MFP serverio funkcijose.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP Socket

3.1 POP

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [E-mail Setting] (El. pašto nustatymai) - [E-mail RX (POP)] (El. pašto RX (POP))

Nustatomas elementas	Rekomenduojamas nustatymas
[Certificate Verification Level Settings] (Sertifikato patikrinimo lygio nustatymai)	[Expiration Date] (Galiojimo data): ON (įjungta) [Chain] (Grandinė): ON (įjungta)

3.2 SMTP

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [E-mail Setting] (El. pašto nustatymai) - [E-mail TX (SMTP)] (El. pašto TX (SMTP))

Nustatomas elementas	Rekomenduojamas nustatymas
[Certificate Verification Level Settings] (Sertifikato patikrinimo lygio nustatymai)	[Expiration Date] (Galiojimo data): ON (įjungta) [Chain] (Grandinė): ON (įjungta)

3.3 IEEE802.1X Auth

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentikavimo nustatymas) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentikavimo nustatymas) - [Supplicant Setting] (Prašytojo nustatymas)

Nustatomas elementas	Rekomenduojamas nustatymas
[Certificate Verification Level Settings] (Sertifikato patikrinimo lygio nustatymai)	[Expiration Date] (Galiojimo data): ON (įjungta) [Chain] (Grandinė): ON (įjungta)

3.4 IPsec

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [TCP/IP Setting] (TCP/IP nustatymas) - [IPsec] - [Enable IPsec] (Įjungti IPsec)

Nustatomas elementas	Rekomenduojamas nustatymas
[Certificate Verification Level Settings] (Sertifikato patikrinimo lygio nustatymai)	[Expiration Date] (Galiojimo data): [Confirm] (Patvirtinti) [Chain] (Grandinė): [Confirm] (Patvirtinti)

Patarimai

[IPsec Setting] (IPsec nustatymuose) registruokite elementus [IKE], [SA], [Peer] ir [Protocol Setting] (Protokolo nustatymas) iš anksto.

3.5 WebDAVClient

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [WebDAV Settings] (WebDAV nustatymai) - [WebDAV Client Settings] (WebDAV kliento nustatymai)

Nustatomas elementas	Rekomenduojamas nustatymas
[Certificate Verification Level Settings] (Sertifikato patikrinimo lygio nustatymai)	[Expiration Date] (Galiojimo data): ON (Įjungta) [Chain] (Grandinė): ON (Įjungta)

3.6 LDAP

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [LDAP Setting] (LDAP nustatymas) - [Setting Up LDAP] (LDAP sąranka)

Nustatomas elementas	Rekomenduojamas nustatymas
[Certificate Verification Level Settings] (Sertifikato patikrinimo lygio nustatymai)	[Expiration Date] (Galiojimo data): ON (Įjungta) [Chain] (Grandinė): ON (Įjungta)

3.7 DPWS

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [DPWS Settings] (DPWS nustatymai) - [DPWS Common Settings] (DPWS bendrieji nustatymai)

Nustatomas elementas	Rekomenduojamas nustatymas
[Certificate Verification Level Settings] (Sertifikato patikrinimo lygio nustatymai)	[Expiration Date] (Galiojimo data): ON (Įjungta) [Chain] (Grandinė): ON (Įjungta)

3.8 OpenAPI

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [OpenAPI Setting] (OpenAPI nustatymas) - [OpenAPI Setting] (OpenAPI nustatymas)

Nustatomas elementas	Rekomenduojamas nustatymas
[Certificate Verification Level Settings] (Sertifikato patikrinimo lygio nustatymai)	[Expiration Date] (Galiojimo data): ON (Įjungta) [Chain] (Grandinė): ON (Įjungta)

3.9 RemotePanel

Nustatymo vieta: [Utility] (Pagalbinės priemonės) - [Administrator] (Administratorius) - [Network] (Tinklas) - [Remote Panel Settings] (Nuotolinio valdymo skydelio nustatymai) - [Remote Panel Client Settings] (Nuotolinio valdymo skydelio kliento nustatymai)

Nustatomas elementas	Rekomenduojamas nustatymas
[Certificate Verification Level Settings] (Sertifikato patikrinimo lygio nustatymai)	[Expiration Date] (Galiojimo data): ON (Ijungta) [Chain] (Grandinė): ON (Ijungta)

4 Papildoma saugos informacija

4.1 Geriausios praktikos rekomendacijos

Rekomenduojame, kad naudojami šifravimo algoritmai atitiktų geriausios praktikos nustatymus, rekomenduojamus EUCC kriptografijos gairėse ir SOGIS sutartuose kriptografiniuose mechanizmuose.

Toliau pateikiamas šifravimo algoritmų ir raktų ilgių, rekomenduojamų ESKK kriptografijos gairėse ir SOGIS sutartuose kriptografiniuose mechanizmuose, sąrašas.

Elementas	Rekomenduojamas nustatymas
Šifravimo algoritmas	AES (Pažangus šifravimo standartas) RSA (Rivest-Shamir-Adleman) SHA-2 (Saugus hešo algoritmas 2) ECC (Elipsinės kreivės kriptografija) HMAC (Hešu grindžiamas pranešimo autentiškumo patvirtinimo kodas)
Šifravimo rakto ilgis	RSA: 2048 bitai ar daugiau ECC: 256 bitai ar daugiau AES: 256 bitai

Patarimai

Išsamesnės informacijos rasite naujausiose EUCC kriptografijos gairėse ir SOGIS- sutartuose kriptografiniuose mechanizmuose.

4.2 Atsargumo priemonės dėl ryšio su senosiomis sistemomis

Numatoma, kad ryšiui su senosiomis sistemomis bus naudojami šie protokolai ir jų versijos.

Naudojant senesnius nustatymus padidėja saugumo rizika, todėl naudokite juos saugioje tinklo aplinkoje.

Punktas	Senesni nustatymai
Protokolas	SLP FTP SMB (3.0 arba ankstesnė versija, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP TIPAS: priklauso nuo serverio / išjungimo) DPWS TCPSocket
Šifravimo algoritmas	SHA-1 (Saugus hešo algoritmas 1) DES (duomenų šifravimo standartas) 3DES (trigubo duomenų šifravimo standartas) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Šifravimo rakto ilgis	RSA: 1024 bitai ar mažiau ECC: 160 bitų ar mažiau AES: 128 bitai ar mažiau DES: 56 bitai 3DES: 112 bitų

IPsec senesni nustatymai

[IKEv1]

Nustatomas elementas	Senesni nustatymai
[Encryption Algorithm] (Šifravimo algoritmas)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 ir 192])
[Authentication Algorithm] (Autentifikavimo algoritmas)	Nenaudojamas
[Diffie-Hellman Group] (Diffie-Hellman grupė)	[Group 1] (1 grupė), [Group 2] (2 grupė), [Group 5] (5 grupė)

[IKEv2]

Nustatomas elementas	Senesni nustatymai
[Encryption Algorithm] (Šifravimo algoritmas)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 ir 192])
[Authentication Algorithm] (Autentifikavimo algoritmas)	Nenaudojamas
[Diffie-Hellman Group] (Diffie-Hellman grupė)	[Group 1] (1 grupė), [Group 2] (2 grupė), [Group 5] (5 grupė)

[SA]

Nustatomas elementas	Senesni nustatymai
[Key Exchange Method] (Keitimosi raktu metodas)	[IKEv1]
[Authentication Method] (Autentifikavimo metodas)	[Digital Signature] (Skaitmeninis parašas)

Nustatomas elementas	Senesni nustatymai
[ESP Encryption Algorithm] (ESP šifravimo algoritmas)	[3DES-CBC] ([128]/[192]/[128 ir 192]) [AES-CTR] ([128]/[192]/[128 ir 192]) [AES-GCM] ([128]/[192]/[128 ir 192]) [AES-GCM-64] ([128]/[192]/[128 ir 192]) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 ir 192])
[Perfect Forward Secrecy] (Puikus persiuntimo slaptumas)	ON (ijungtas)
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellman grupė(IKEv1))	[Group 1] (1 grupė), [Group 2] (2 grupė), [Group 5] (5 grupė)

4.3 Tinklo sąsajos ir paslaugos prieinamos nuo pat išsiuntimo iš gamyklos

Paslaugos tipas	Protokolas	Prievado numeris
DHCP	UDP	68
HTTP serveris	TCP	80
NETBIOS Name Service	UDP	137
NETBIOS Datagram Service	UDP	138
SNMP	UDP	161
HTTP serveris per SSL / IPP per SSL	TCP	443
LPD spausdinimas	TCP	515
DHCPv6 klientas	UDP	546
IPP spausdinimas	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS įrankis)	TCP	8091
RAW spausdinimas	TCP	9100
RAW spausdinimas	TCP	9112
RAW spausdinimas	TCP	9113
RAW spausdinimas	TCP	9114
RAW spausdinimas	TCP	9115
RAW spausdinimas	TCP	9116
OpenAPI	TCP	50001

4.4 Apie įvesties patvirtinimą

Kiek ženklų reikia įvesti tinklo nustatymams ir t. t., rasite prie kiekvieno nustatymų elemento naudotojo vadove.

Atsižvelgiant į kalbos koduotę, didžiausia leistina įvestis (MPDF išsaugoti duomenys) elementams, kurie palaiko daugiabaitinius simbolius, gali būti tris kartus didesnė už simbolių skaičių.

Ieteikumi attiecībā uz drošām tīkla ierīcēm

Saturs

1 IP adresu filtrēšanas iestatīšana

1.1	IP adresu filtrēšana	1-3
1.2	Ātrā IP filtrēšana.....	1-3

2 Šifrētās komunikācijas iestatīšana

2.1	TLS šifrēšana.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-6
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP ligzda.....	2-6
2.2	Cita šifrēšana.....	2-7
2.2.1	SMBServer	2-7
	SMB šifrēšana.....	2-7
	SMB Signature.....	2-7
2.2.2	SMBClient	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Sertifikāta validācijas iestatīšana

3.1	POP.....	3-10
3.2	SMTP	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	RemotePanel	3-12

4 Papildu informācija par drošību

4.1	Paraugprakses ieteikumi.....	4-13
4.2	Piesardzības pasākumi komunikācijai ar mantotām sistēmām	4-14
	IPsec mantotie iestatījumi	4-14
4.3	Tīkla saskarnes un pakalpojumi, kas pieejami pēc rūpnīcas piegādes.....	4-16
4.4	Par ievades validāciju	4-17



Par šo rokasgrāmatu

Šajā rokasgrāmatā ir aprakstīta informācija un iestatījumi, kas garantē drošu ierīču lietošanu.

Savienojot šo iekārtu ar tīklu, izmantojiet to ar ugunsdzēsības aizsargātā vidē. Tāpat iesakām papildus šīs iekārtas IP adresei iestatīt privātu IP adresi.

Iestatot privāto IP adresi, iekārtai var piekļūt tikai lokālā tīkla, piemēram, iekšējā LAN, lietotāji, tādējādi novēršot nesankcionētu piekļuvi no ārpuses.

Ja ir jāizmanto globāla IP adrese, noteikti instalējiet šo iekārtu ugunsdzēsības aizsargātā vidē.

1 IP adrešu filtrēšanas iestatīšana

IP adrešu filtrēšana ir funkcija, kas ierobežo ierīces, kuras var piekļūt šai iekārtai, atkarībā no IP adreses. Pareizi iestatot šo funkciju, varat ierobežot piekļuvi no nesankcionētām ierīcēm.

Šīs iekārtas IP adrešu filtrēšanas funkciju var iestatīt, izmantojot kādu no šīm divām metodēm.

1.1 IP adrešu filtrēšana

Manuāli norādi IP adrešu diapazonu, kuram vēlaties atļaut vai liegt piekļuvi.

Iestatījumu atrašanās vieta: [Utility] (Utilitārogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [TCP/IP Setting] (TCP/IP iestatījumi) - [IP Address Filtering] (IP adrešu filtrēšana)

Padomi

Nosakiet atļautās vai aizliegtās IP adreses atbilstoši jūsu videi.

1.2 Ātrā IP filtrēšana

IP adrešu diapazons, kam ļauts piekļūt, tiek iestatīts automātiski, pamatojoties uz šajā iekārtā iestatīto IP adresi un apakštīkla masku.

Iestatījumu atrašanās vieta: [Utility] (Utilitārogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [TCP/IP Setting] (TCP/IP iestatījumi) - [Quick IP Filtering] (Ātrā IP filtrēšana)

Ieteicamie iestatījumi: [Synchronize IP Address] (Sinhronizēt IP adresi)/[Synchronize Subnet Mask] (Sinhronizēt apakštīkla masku) *

* Izvēlieties savai videi piemērotāko variantu.

2 Šifrētās komunikācijas iestatīšana

Mēs iesakām izmantot šādu šifrētu komunikāciju, lai novērstu datu pārtveršanu, datu viltošanu un sesijas pārtveršanu.

2.1 TLS šifrēšana

Lai samazinātu ievainojamību risku, iesakām konfigurēt šādus iestatījumus.

Iestatījumu atrašanās vieta: [Utility] (Utilitārogrammas) - [Administrator] (Administrators) - [Security] (Drošība) - [PKI Settings] (PKI iestatījumi) - [Enable SSL Version] (Iespējot SSL versiju)

Iestatījums	Ieteicamais iestatījums
[Mode using SSL/TLS] (Režīms, kurā izmanto SSL/TLS)	[Admin. Mode and User Mode] (Administrators režīms un lietotāja režīms)
[SSL/TLS Version Setting] (SSL/TLS versijas iestatījums)	TLS1.2 TLS1.3 (nesaderīgs ar IEEE802.1X)
[Encryption Strength] (Šifrēšanas stiprums)	AES-256

Sākotnējais sertifikāts tiek instalēts rūpnīcā. Ja nepieciešams cits sertifikāts, reģistrējiet jaunu sertifikātu šeit.

Iestatījumu atrašanās vieta: [Utility] (Utilitārogrammas) - [Administrator] (Administrators) - [Security] (Drošība) - [PKI Settings] (PKI iestatījumi) - [Device Certificate Setting] (Ierīces sertifikāta iestatījumi)

Iestatījums	Ieteicamais iestatījums
[Encryption Key Type] (Šifrēšanas atslēgas tips)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

TLS šifrēšana tiek atbalstīta šādiem protokoliem un pakalpojumiem. Sīkāku informāciju par iestatījumu atrašanās vietām skatiet turpmākajās sadaļās.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP ligzda

2.1.1 HTTP (Web Connection)

Ja iespējot [Enable SSL Version] (Iespējot SSL versiju), komunikācijas režīms automātiski pārslēdzas uz TLS šifrētu komunikāciju (HTTPS).

2.1.2 WebDAVServer

Iestatījumu atrašanās vieta: [Utility] (Utilitārogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [WebDAV Settings] (WebDAV iestatījumi) - [WebDAV Server Settings] (WebDAV servera iestatījumi)

Iestatījums	Ieteicamais iestatījums
[SSL Settings] (SSL iestatījumi)	[SSL Only] (Tikai SSL)

2.1.3 IPP

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [HTTP Server Settings] (HTTP servera iestatījumi)

Iestatījums	Ieteicamais iestatījums
[IPP-SSL Settings] (IPP-SSL iestatījumi)	[SSL Only] (Tikai SSL)

2.1.4 OpenAPI

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [OpenAPI Setting] (OpenAPI iestatījumi) - [OpenAPI Setting] (OpenAPI iestatījumi)

Iestatījums	Ieteicamais iestatījums
[SSL/Port Settings] (SSL/porta iestatījumi)	[SSL Only] (Tikai SSL)

2.1.5 RemotePanel

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [Remote Panel Settings] (Remote Panel iestatījumi) - [Remote Panel Server Settings] (Remote Panel servera iestatījumi)

Iestatījums	Ieteicamais iestatījums
[Port No.(SSL)] (SSL) porta Nr.)	[50443]

Padomi

Ja iespējot [Enable SSL Version] (Iespējot SSL versiju), komunikācija automātiski pārslēdzas uz TLS šifrētas komunikācijas režīmu. Norādiet porta numuru.

2.1.6 DPWS

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [DPWS Settings] (DPWS iestatījumi) - [DPWS Common Settings] (DPWS kopējie iestatījumi)

Iestatījums	Ieteicamais iestatījums
[SSL Settings] (SSL iestatījumi)	IESL.

2.1.7 POP

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [E-mail Setting] (E-pasta iestatījumi) - [E-mail RX (POP)] (E-pasta RX (POP))

Iestatījums	Ieteicamais iestatījums
[Enable SSL] (Iespējot SSL)	IESL.

2.1.8 SMTP

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [E-mail Setting] (E-pasta iestatījumi) - [E-mail TX (SMTP)] ((E-pasta TX (SMTP)))

Iestatījums	Ieteicamais iestatījums
[SSL/TLS Settings] (SSL/TLS iestatījumi)	[SMTP over SSL] (SMTP caur SSL)

2.1.9 IEEE802.1X Auth

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentifikācijas iestatījumi) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentifikācijas iestatījumi) - [Supplicant Setting] (Pieprasītāja iestatījumi)

Iestatījums	Ieteicamais iestatījums
[EAP-Type] (EAP tips)	Izvēlieties [EAP-TLS], [EAP-TTLS] vai [PEAP].

2.1.10 LDAP

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [LDAP Setting] (LDAP iestatījumi) - [Setting Up LDAP] (LDAP iestatīšana)

Iestatījums	Ieteicamais iestatījums
[Enable SSL] (Iespējot SSL)	IESL.

2.1.11 TCP ligzda

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [TCP Socket Setting] (TCP ligzdas iestatījumi)

Iestatījums	Ieteicamais iestatījums
[Use SSL/TLS] (Izmantot SSL/TLS)	IESL.

2.2 Cita šifrēšana

Lai samazinātu ievainojamību risku, iesakām konfigurēt šādus iestatījumus. Sīkāku informāciju par katras funkcijas iestatījumiem skatiet turpmākajās sadaļās.

Funkcija	Ieteicamais iestatījums
SMBServer	SMB Encryption, SMB Signature
SMBClient	Kerberos Authentication
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	IESL.

2.2.1 SMBServer

Izmantojot SMB šifrēšanu un SMB parakstu, var samazināt šādus drošības riskus.

- Pārtveršana: ļaunprātīga trešā persona var pārtvert komunikācijas un piesavināties personisku vai konfidenciālu informāciju.
- Datu viltošana: pastāv risks, ka komunikācijas saturs var tikt viltots, izmantojot pārtvērējuzbrukumu (Man-In-The-Middle Attack, MITM).
- Izlikšanās: ja tiek piesavināta autentifikācijas informācija, trešā persona var uzdoties par likumīgu lietotāju, lai iegūtu nesankcionētu piekļuvi.
- Informācijas noplūde: nešifrētas komunikācijas var viegli pārtvert, jo īpaši publiskos Wi-Fi tīklos, tādējādi palielinot personas datu un kredītkaršu informācijas noplūdes risku.

SMB šifrēšana

Priekšnosacījumi

- Izveidojiet publisku lietotāja bloku. Konfigurējiet arī iestatījumu, lai automātiski pārsūtītu failus no publiskā lietotāja bloka un saglabātu tos SMB mapē.
- Norādiet lietotāja bloka paroli.

Iestatījumu atrašanās vieta: [Utility] (Utilitīprogrammas) - [Administrator] (Administrators) - [Box] (Blok) - [User Box List] (Lietotāju bloku saraksts)

Iestatījums	Ieteicamais iestatījums
[SMB Communication Encryption] (SMB komunikācijas šifrēšana)	[Encrypt] (Šifrēt)

SMB Signature

Iestatījumu atrašanās vieta: [Utility] (Utilitīprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [SMB Setting] (SMB iestatījumi) - [SMB Server Settings] (SMB servera iestatījumi)

Iestatījums	Ieteicamais iestatījums
[SMB security Signature Setting] (SMB drošības paraksta iestatījums)	[Required] (Obligāts)

2.2.2 SMBClient

Kerberos autentifikācijā tiek izmantota spēcīga šifrēšanas tehnoloģija, kas ievērojami samazina risku, ka autentifikācijas procesa laikā varētu tikt piesavināti akreditācijas dati. Tā nodrošina arī datu integritāti, novēršot datu viltošanu starp sūtītāju un saņēmēju, kā arī NTLM relejuzbrukumus.

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [SMB Setting] (SMB iestatījumi) - [Client Setting] (Klienta iestatījumi)

Iestatījums	Ieteicamais iestatījums
[SMB Authentication Setting] (SMB autentifikācijas iestatījums)	[Kerberos]

2.2.3 SNMP

Iestatiet šifrēšanu, izmantojot SNMPv3. Ja tiek pievienots arī autentifikācijas iestatījums, varat vēl vairāk palielināt drošību. Drošības riski ir aptuveni tādi paši kā ar SMB.

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [SNMP Setting] (SNMP iestatījumi)

Iestatījums	Ieteicamais iestatījums
[SNMP Setting] (SNMP iestatījumi)	[SNMP v3(IP)]
[Encryption Algorithm] (Šifrēšanas algoritms)	[AES-128]
[Authentication Method] (Autentifikācijas metode)	Izvēlieties [SHA-256], [SHA-384] vai [SHA-512].

2.2.4 IPsec

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [TCP/IP Setting] (TCP/IP iestatījumi) - [IPsec] - [IPsec Setting] (IPsec iestatījumi)

[IKEv2]

Iestatījums	Ieteicamais iestatījums
[Encryption Algorithm] (Šifrēšanas algoritms)	[AES-CBC] ([256]/[192 and 256] (192 un 256)/[All] (Visi))
[Authentication Algorithm] (Autentifikācijas algoritms)	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 un 384)/[384 and 512] (384 un 512)/[All] (Visi)), [AES-XCBC]
[Diffie-Hellman Group] (Diffie-Hellman grupa)	[Group 14] (Grupa 14), [Group 19] (Grupa 19)

[SA]

Iestatījums	Ieteicamais iestatījums
[Encapsulation Mode] (Iekapsulēšanas režīms)	[Tunnel], [Transport]
[Security Protocol] (Drošības protokols)	[ESP]
[Key Exchange Method] (Atslēgas apmaiņas metode)	[IKEv2]
[Authentication Method] (Autentifikācijas metode)	[Digital Signature] (Digitālais paraksts)
[ESP Encryption Algorithm] (ESP šifrēšanas algoritms)	[AES-GCM] ([256]/[192 and 256] (192 un 256)/[All] (Visi)), [AES-GCM-64] ([256]/[192 and 256] (192 un 256)/[All] (Visi)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 un 256)/[All] (Visi))

iestatījums	ieteicamais iestatījums
[Perfect Forward Secrecy] (Perfekta turpmāka slepenība)	IESL.
[Diffie-Hellman Group(IKEv2)] (Diffie-Hellman grupa (IKEv2)) - [Priority1-4] (Prioritāte1-4)	[Group 14] (Grupa 14), [Group 19] (Grupa 19)

2.2.5 S/MIME

Ja, sūtot e-pastu, izmantojat izvēles S/MIME, varat šifrēt e-pasta saturu, lai novērstu pārtveršanu, un apstiprināt sūtītāja identitāti ar elektronisko parakstu. Tas ir efektīvs līdzeklis pret izlikšanos un pikšķerēšanu.

Iestatījumu atrašanās vieta: [Utility] (Utilitārogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [E-mail Setting] (E-pasta iestatījumi) - [S/MIME]

iestatījums	ieteicamais iestatījums
[Digital Signature] (Digitālais paraksts)	[Always add signature] (Vienmēr pievienot parakstu)
[Digital Signature Type] (Digitālā paraksta tips)	[SHA-256]
[E-Mail Text Encrypt. Method] (E-pasta teksta šifrēšanas metode)	[AES-256]

3 Sertifikāta validācijas iestatīšana

Izmantojot TLS šifrētu komunikāciju, lai mazinātu pārtvērējuzbrukumu ietekmi, mēs iesakām izmantot sertifikāta validāciju. Iesakām iespējot vismaz sertifikāta derīguma termiņa beigu datumu un ķēdes validāciju.

Ja tiek veikts mēģinājums izveidot savienojumu ar novecojušu vidi, kurā nav sertifikāta validācijas funkcijas, pieaug pārtvērējuzbrukumu risks. Mēs iesakām to izmantot drošā tīkla vidē.

Sertifikāta validāciju MFP pusē ieteicams izmantot šādās MFP klienta funkcijās. Sīkāku informāciju par iestatījumu atrašanās vietām skatiet turpmākajās sadaļās.

POP, SMTP (TLS/SMTP palaišana caur SSL), IEEE802.1X Auth (EAP tips: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel



Padomi

Sertifikāta validācija klienta pusē, kas savienota ar MFP, ir ieteicama šādās MFP servera funkcijās. HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP ligzda

3.1 POP

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [E-mail Setting] (E-pasta iestatījumi) - [E-mail RX (POP)] (E-pasta RX (POP))

Iestatījums	Ieteicamais iestatījums
[Certificate Verification Level Settings] (Sertifikāta verifikācijas līmeņa iestatījumi)	[Expiration Date] (Derīguma termiņš): IESL. [Chain] (Ķēde): IESL.

3.2 SMTP

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [E-mail Setting] (E-pasta iestatījumi) - [E-mail TX (SMTP)] (E-pasta TX (SMTP))

Iestatījums	Ieteicamais iestatījums
[Certificate Verification Level Settings] (Sertifikāta verifikācijas līmeņa iestatījumi)	[Expiration Date] (Derīguma termiņš): IESL. [Chain] (Ķēde): IESL.

3.3 IEEE802.1X Auth

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentifikācijas iestatījumi) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentifikācijas iestatījumi) - [Supplicant Setting] (Pieprasītāja iestatījumi)

Iestatījums	Ieteicamais iestatījums
[Certificate Verification Level Settings] (Sertifikāta verifikācijas līmeņa iestatījumi)	[Expiration Date] (Derīguma termiņš): IESL. [Chain] (Ķēde): IESL.

3.4 IPsec

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [TCP/IP Setting] (TCP/IP iestatījumi) - [IPsec] - [Enable IPsec] (Iespējot IPsec)

Iestatījums	Ieteicamais iestatījums
[Certificate Verification Level Settings] (Sertifikāta verifikācijas līmeņa iestatījumi)	[Expiration Date] (Derīguma termiņš): [Confirm] (Apstiprināt) [Chain] (Kēde): [Confirm] (Apstiprināt)

Padomi

Sadaļā [IPsec Setting] (IPsec iestatījumi) iepriekš reģistrējiet vienumus [IKE], [SA], [Peer] un [Protocol Setting] (Protokola iestatījumi).

3.5 WebDAVClient

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [WebDAV Settings] (WebDAV iestatījumi) - [WebDAV Client Settings] (WebDAV klienta iestatījumi)

Iestatījums	Ieteicamais iestatījums
[Certificate Verification Level Settings] (Sertifikāta verifikācijas līmeņa iestatījumi)	[Expiration Date] (Derīguma termiņš): IESL. [Chain] (Kēde): IESL.

3.6 LDAP

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [LDAP Setting] (LDAP iestatījumi) - [Setting Up LDAP] (LDAP iestatīšana)

Iestatījums	Ieteicamais iestatījums
[Certificate Verification Level Settings] (Sertifikāta verifikācijas līmeņa iestatījumi)	[Expiration Date] (Derīguma termiņš): IESL. [Chain] (Kēde): IESL.

3.7 DPWS

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [DPWS Settings] (DPWS iestatījumi) - [DPWS Common Settings] (DPWS kopējie iestatījumi)

Iestatījums	Ieteicamais iestatījums
[Certificate Verification Level Settings] (Sertifikāta verifikācijas līmeņa iestatījumi)	[Expiration Date] (Derīguma termiņš): IESL. [Chain] (Kēde): IESL.

3.8 OpenAPI

Iestatījumu atrašanās vieta: [Utility] (Utilītprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [OpenAPI Setting] (OpenAPI iestatījumi) - [OpenAPI Setting] (OpenAPI iestatījumi)

Iestatījums	Ieteicamais iestatījums
[Certificate Verification Level Settings] (Sertifikāta verifikācijas līmeņa iestatījumi)	[Expiration Date] (Derīguma termiņš): IESL. [Chain] (Kēde): IESL.

3.9 RemotePanel

Iestatījumu atrašanās vieta: [Utility] (Utiļitprogrammas) - [Administrator] (Administrators) - [Network] (Tīkls) - [Remote Panel Settings] (Remote Panel iestatījumi) - [Remote Panel Client Settings] (Remote Panel klienta iestatījumi)

Iestatījums	Ieteicamais iestatījums
[Certificate Verification Level Settings] (Sertifikāta verifikācijas līmeņa iestatījumi)	[Expiration Date] (Derīguma termiņš): IESL. [Chain] (Ķēde): IESL.

4 Papildu informācija par drošību

4.1 Paraugprakses ieteikumi

Mēs iesakām izmantot šifrēšanas algoritmus, kas atbilst EUCC vadlīnijās par kriptogrāfiju un SOGIS saskaņotajās kriptogrāfijas mehānismu vadlīnijās ieteiktajiem paraugprakses iestatījumiem.

Zemāk ir sniegts šifrēšanas algoritmu un atslēgu garumu saraksts, kas ieteikti EUCC vadlīnijās par kriptogrāfiju un SOGIS saskaņotajās kriptogrāfijas mehānismu vadlīnijās.

Vienums	Ieteicamais iestatījums
Šifrēšanas algoritmi	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Šifrēšanas atslēgas garums	RSA: 2048 biti vai vairāk ECC: 256 biti vai vairāk AES: 256 biti

Padomi

Sīkāka informācija atrodama jaunākajās EUCC vadlīnijās par kriptogrāfiju un SOGIS saskaņotajās kriptogrāfijas mehānismu vadlīnijās.

4.2 Piesardzības pasākumi komunikācijai ar mantotām sistēmām

Tiek pieņemts, ka komunikācijai ar mantotām sistēmām tiek izmantoti šādi protokoli un versijas. Izmantojot mantotos iestatījumus, pieaug drošības riski, tāpēc izmantojiet tos tikai drošā tīkla vidē.

Vienums	Mantotie iestatījumi
Protokols	SLP FTP SMB (3.0 vai vecāka versija, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP tips: Atkarībā no servera/lzsl.) DPWS TCPsocket
Šifrēšanas algoritmi	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Šifrēšanas atslēgas garums	RSA: 1024 biti vai mazāk ECC: 160 biti vai mazāk AES: 128 biti vai mazāk DES: 56 biti 3DES: 112 biti

IPsec mantotie iestatījumi

[IKEv1]

Iestatījums	Mantotie iestatījumi
[Encryption Algorithm] (Šifrēšanas algoritms)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 un 192))
[Authentication Algorithm] (Autentifikācijas algoritms)	Netiek izmantots
[Diffie-Hellman Group] (Diffie-Hellman grupa)	[Group 1] (Grupa 1), [Group 2] (Grupa 2), [Group 5] (Grupa 5)

[IKEv2]

Iestatījums	Mantotie iestatījumi
[Encryption Algorithm] (Šifrēšanas algoritms)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 un 192))
[Authentication Algorithm] (Autentifikācijas algoritms)	Netiek izmantots
[Diffie-Hellman Group] (Diffie-Hellman grupa)	[Group 1] (Grupa 1), [Group 2] (Grupa 2), [Group 5] (Grupa 5)

[SA]

Iestatījums	Mantotie iestatījumi
[Key Exchange Method] (Atslēgas apmaiņas metode)	[IKEv1]
[Authentication Method] (Autentifikācijas metode)	[Digital Signature] (Digitālais paraksts)

Iestatījums	Mantotie iestatījumi
[ESP Encryption Algorithm] (ESP šifrēšanas algoritms)	[3DES-CBC] ([128]/[192]/[128 and 192] (128 un 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 un 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 un 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 un 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 un 192))
[Perfect Forward Secrecy] (Perfekta turpmāka slepenība)	IESL.
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellman grupa(IKEv2))	[Group 1], (Grupa 1) [Group 2] (Grupa 2), [Group 5] (Grupa 5)

4.3 Tīkla saskarnes un pakalpojumi, kas pieejami pēc rūpnīcas piegādes

Pakalpojuma veids	Protokols	Porta numurs
DHCP	UDP	68
HTTP serveris	TCP	80
NETBIOS nosaukumu pakalpojums	UDP	137
NETBIOS datagrammu pakalpojums	UDP	138
SNMP	UDP	161
HTTP serveris caur SSL / IPP caur SSL	TCP	443
LPD druka	TCP	515
DHCPv6 klients	UDP	546
IPP druka	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS rīks)	TCP	8091
RAW druka	TCP	9100
RAW druka	TCP	9112
RAW druka	TCP	9113
RAW druka	TCP	9114
RAW druka	TCP	9115
RAW druka	TCP	9116
OpenAPI	TCP	50001

4.4 Par ievades validāciju

Lai uzzinātu tīkla iestatījumu ievadāmo rakstzīmju skaitu utt., skatiet katru iestatījumu elementu lietotāja rokasgrāmatā.

Atkarībā no valodas kodējuma maksimālais pieļaujamais ievades (MFP saglabāto datu) rakstzīmju skaits elementiem, kas atbalsta daudzbitu rakstzīmes, var būt trīs reizes lielāks par rakstzīmju skaitu.

Aanbevelingen voor beveiligde netwerkapparatuur

Inhoud

1 IP-adres filteren instellen

1.1	IP-adres filteren.....	1-3
1.2	Snel IP filteren	1-3

2 Versleutelde communicatie instellen

2.1	TLS-versleuteling	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAV-server	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	Extern paneel	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP socket	2-6
2.2	Andere versleuteling	2-7
2.2.1	SMB-server.....	2-7
	SMB-versleuteling.....	2-7
	SMB-handtekening.....	2-7
2.2.2	SMB-client	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Certificaatvalidatie instellen

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAV-client	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	Extern paneel.....	3-12

4 Aanvullende beveiligingsinformatie

4.1	Aanbeveling voor best practices	4-13
4.2	Voorzorgsmaatregelen bij communicatie met legacy-systemen.....	4-14
	IPsec-legacy-instellingen	4-14
4.3	Netwerkinterfaces en services die bij aflevering uit de fabriek beschikbaar zijn	4-16
4.4	Over invoervalidatie	4-17



Informatie over deze handleiding

Deze handleiding bevat informatie en instellingen die het veilige gebruik van apparaten mogelijk maken.

Gebruik deze machine in een omgeving die door een firewall wordt beschermd wanneer u deze op het netwerk aansluit. We raden ook aan om een privé-IP-adres in te stellen voor het IP-adres van de machine.

Het instellen van een privé-IP-adres zorgt ervoor dat alleen gebruikers op een lokaal netwerk, zoals een interne LAN, toegang hebben tot de machine, waardoor ongeautoriseerde toegang van buitenaf wordt voorkomen.

Als u een globaal IP-adres moet gebruiken, zorg er dan voor dat de machine zich achter een firewall bevindt.

1 IP-adres filteren instellen

IP-adres filteren is een functie waarmee u apparaten die op basis van hun IP-adres toegang hebben tot de machine, kunt beperken. U kunt de toegang door onbevoegde apparaten beperken door deze functie correct in te stellen.

Het IP-adres filteren van deze machine kan op een van de volgende twee manieren worden ingesteld.

1.1 IP-adres filteren

Geef handmatig het bereik van IP-adressen op waarvoor toegang moet worden toegestaan of geweigerd.

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [TCP/IP Setting] (TCP/IP-instelling) - [IP Address Filtering] (IP-adres filteren)

Tips

Stel de IP-adressen in die moeten worden toegestaan of geweigerd, afhankelijk van uw omgeving.

1.2 Snel IP filteren

Het bereik van IP-adressen waarvoor toegang is toegestaan, wordt automatisch ingesteld op basis van het IP-adres en subnetmasker dat in deze machine is geconfigureerd.

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [TCP/IP Setting] (TCP/IP-instelling) - [Quick IP Filtering] (Snel IP filteren)

Aanbevolen instelling: [Synchronize IP Address] (IP-adres synchroniseren)/[Synchronize Subnet Mask] (Subnetmasker synchroniseren) *

* Selecteer een van beide, afhankelijk van uw omgeving.

2 Versleutelde communicatie instellen

We raden aan de volgende versleutelde communicatiemethode te gebruiken om gegevensafluistering, gegevensmanipulatie en sessiekaping te voorkomen.

2.1 TLS-versleuteling

We raden aan de volgende instellingen te configureren om het risico op kwetsbaarheden te verkleinen.

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Security] (Beveiliging) - [PKI Settings] (PKI-instellingen) - [Enable SSL Version] (SSL-versie inschakelen)

Instelitem	Aanbevolen instelling
[Mode using SSL/TLS] (Modus via SSL/TLS)	[Admin. Mode and User Mode] (Beheerdersmodus en gebruikersmodus)
[SSL/TLS Version Setting] [SSL-/TLS-versie-instelling]	TLS1.2 TLS1.3 (IEEE802.1X incompatibel)
[Encryption Strength] (Versleutelingssterkte)	AES-256

Het initiële certificaat wordt in de fabriek geïnstalleerd. Als u een ander certificaat nodig hebt, registreer dan een nieuw certificaat op de volgende locatie.

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Security] (Beveiliging) - [PKI Settings] (PKI-instellingen) - [Device Certificate Setting] (Instelling apparaatcertificaat)

Instelitem	Aanbevolen instelling
[Encryption Key Type] [Versleutelingsstelseltype]	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

De TLS-versleuteling wordt ondersteund voor de volgende protocollen en services. Raadpleeg de volgende secties voor meer informatie over de instellingslocaties.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP over SSL)SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP socket

2.1.1 HTTP (Web Connection)

Als u [Enable SSL Version] (SSL-versie inschakelen) inschakelt, schakelt de communicatiemodus automatisch over naar de TLS-versleutelde communicatie (HTTPS).

2.1.2 WebDAV-server

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [WebDAV Settings] (WebDAV-instellingen) - [WebDAV Server Settings] (WebDAV-serverinstellingen)

Instelitem	Aanbevolen instelling
[SSL Settings] (SSL-instellingen)	[SSL Only] [Alleen SSL]

2.1.3 IPP

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [HTTP Server Settings] (Instelling HTTP server)

Instelitem	Aanbevolen instelling
[IPP-SSL Settings] (IPP-SSL-instellingen)	[SSL Only] (Alleen SSL)

2.1.4 OpenAPI

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [OpenAPI Setting] (OpenAPI instelling) - [OpenAPI Setting] (OpenAPI instelling)

Instelitem	Aanbevolen instelling
[SSL/Port Settings] [SSL/voortinstellingen]	[SSL Only] (Alleen SSL)

2.1.5 Extern paneel

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [Remote Panel Settings] (Instellingen extern paneel) - [Remote Panel Server Settings] (Serverinstellingen extern paneel)

Instelitem	Aanbevolen instelling
[Port No. (SSL)] (Poortnummer (SSL))	[50443]



Tips

Als u [Enable SSL Version] (SSL-versie inschakelen) inschakelt, schakelt de communicatie automatisch over naar de TLS-versleutelde modus. Geef een poortnummer op.

2.1.6 DPWS

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [DPWS Settings] (DPWS-instellingen) - [DPWS Common Settings] (Algemene DPWS-instellingen)

Instelitem	Aanbevolen instelling
[SSL Settings] (SSL-instellingen)	AAN

2.1.7 POP

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [E-mail Setting] (E-mailinstelling) - [E-mail RX (POP)] (E-mailontvangst (POP))

Instelitem	Aanbevolen instelling
[Enable SSL] (SSL inschakelen)	AAN

2.1.8 SMTP

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [E-mail Setting] (E-mailinstelling) - [E-mail TX (SMTP)] (E-mail TX (SMTP))

Instelitem	Aanbevolen instelling
[SSL/TLS Settings] [SSL/TLS-instellingen]	[SMTP over SSL]

2.1.9 IEEE802.1X Auth

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [IEEE802.1X Authentication Setting] (IEEE802.1X authenticatie-instelling) - [IEEE802.1X Authentication Setting] (IEEE802.1X authenticatie-instelling) - [Supplicant Setting] (Instelling aanvrager)

Instelitem	Aanbevolen instelling
[EAP-Type]	Selecteer [EAP-TLS], [EAP-TTLS], of [PEAP].

2.1.10 LDAP

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [LDAP Setting] (LDAP-instelling) - [Setting Up LDAP] (LDAP installeren)

Instelitem	Aanbevolen instelling
[Enable SSL] (SSL inschakelen)	AAN

2.1.11 TCP socket

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [TCP Socket Setting] (Instelling TCP socket)

Instelitem	Aanbevolen instelling
[Use SSL/TLS] (SSL/TLS gebruiken)	AAN

2.2 Andere versleuteling

We raden aan de volgende instellingen te configureren om het risico op kwetsbaarheden te verkleinen. Raadpleeg de volgende secties voor meer informatie over de instellingen van elke functie.

Functie	Aanbevolen instelling
SMB-server	SMB-versleuteling, SMB-handtekening
SMB-client	Kerberos-authenticatie
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	AAN

2.2.1 SMB-server

Het gebruik van SMB-versleuteling en SMB-handtekening kan de volgende beveiligingsrisico's verminderen.

- Gegevensaf luistering: Een kwaadwillende derde partij kan communicatie onderscheppen en persoonlijke of vertrouwelijke informatie stelen.
- Gegevensmanipulatie: Er bestaat een risico dat communicatie-inhoud wordt gemanipuleerd door een Man-in-the-Middle-aanval (MITM).
- Spoofing: Als authenticatie-informatie wordt gestolen, kan een derde partij zich voordoen als een legitieme gebruiker om ongeautoriseerde toegang te verkrijgen.
- Informatielek: Niet-versleutelde communicatie kan gemakkelijk worden onderschept, vooral op openbare wifi-netwerken, waardoor het risico op het lekken van persoonlijke en creditcardinformatie toeneemt.

SMB-versleuteling

Voorwaarden

- Maak een openbare gebruikersbox aan. Configureer ook de instelling om bestanden automatisch over te dragen vanuit de openbare gebruikersbox en op te slaan in de SMB-map.
- Geef het wachtwoord voor de gebruikersbox op.

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Box] (Gebruikersbox) - [User Box List] (Lijst gebruikersboxen)

Instelitem	Aanbevolen instelling
[SMB Communication Encryption] (Versleuteling van SMB-communicatie)	[Encrypt] (Versleutelen)

SMB-handtekening

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [SMB Setting] (SMB-instelling) - [SMB Server Settings] (SMB-serverinstellingen)

Instelitem	Aanbevolen instelling
[SMB security Signature Setting] (Beveiligingsinstelling voor SMB-handtekening)	[Required] (Vereist)

2.2.2 SMB-client

De Kerberos-authenticatie gebruikt sterke versleutelingstechnologie, waardoor het risico dat inloggegevens worden gestolen tijdens het authenticatieproces aanzienlijk wordt verminderd. Het waarborgt ook de integriteit van gegevens en voorkomt zowel manipulatie tussen zender en ontvanger als NTLM-relay-aanvallen.

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [SMB Setting] (SMB-instelling) - [Client Setting] (Clientinstelling)

Instelitem	Aanbevolen instelling
[SMB Authentication Setting] (SMB-authenticatie-instelling)	[Kerberos]

2.2.3 SNMP

Stel de versleuteling in met SNMPv3. Als u ook de authenticatie-instelling toevoegt, kunt u de veiligheid verder vergroten. De beveiligingsrisico's zijn ongeveer hetzelfde als bij SMB.

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [SNMP Setting] (SNMP-instelling)

Instelitem	Aanbevolen instelling
[SNMP Setting] (SNMP-instelling)	[SNMP v3(IP)]
[Encryption Algorithm] (Versleutelingsalgoritme)	[AES-128]
[Authentication Method] (Authenticatiemethode)	Selecteer [SHA-256], [SHA-384] of [SHA-512].

2.2.4 IPsec

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [TCP/IP Setting] (TCP/IP-instelling) - [IPsec] (IPsec) - [IPsec Setting] (IPsec-instelling)

[IKEv2]

Instelitem	Aanbevolen instelling
[Encryption Algorithm] (Versleutelingsalgoritme)	[AES-CBC] ([256]/[192 en 256]/[All])
[Authentication Algorithm] (Authenticatie-algoritme)	[SHA-2] ([256]/[384]/[512]/[256 en 384]/[384 en 512]/[All]), [AES-XCBC]
[Diffie-Hellman Group] (Diffie-Hellman-groep)	[Group 14] (Groep 14), [Group 19] (Groep 19)

[SA]

Instelitem	Aanbevolen instelling
[Encapsulation Mode] (Ingekapselde modus)	[Tunnel], [Transport]
[Security Protocol] (Beveiligingsprotocol)	[ESP]
[Key Exchange Method] (Toetsuitwisselingsmethode)	[IKEv2]
[Authentication Method] (Authenticatiemethode)	[Digital Signature] (Digitale handtekening)

Instelitem	Aanbevolen instelling
[ESP Encryption Algorithm] (ESP-versleutelings- algoritme)	[AES-GCM] ([256]/[192 en 256]/[All]), [AES-GCM-64] ([256]/[192 en 256]/[All]), [ENC_NULL_AES_GMAC] ([256]/[192 en 256]/[All])
[Perfect Forward Secrecy] (Perfecte geheimhouding doorsturen)	AAN
[Diffie-Hellman Group(IKEv2)] (Diffie-Hellman-groep (IKEv2)) - [Priority1-4] (Prioriteit1-4)	[Group 14] (Groep 14), [Group 19] (Groep 19)

2.2.5 S/MIME

Als u bij het verzenden van e-mail gebruikmaakt van de optionele S/MIME, kunt u de inhoud versleutelen om af luisteren te voorkomen en met een elektronische handtekening de identiteit van de afzender verifiëren. Dit is een effectieve maatregel tegen spoofing en phishing-aanvallen.

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [E-mail Setting] (E-mailinstelling) - [S/MIME]

Instelitem	Aanbevolen instelling
[Digital Signature] (Digitale handtekening)	[Always add signature] (Altijd ondertek.)
[Digital Signature Type] (Type digitale handtekening)	[SHA-256]
[E-Mail Text Encrypt. Method] [Versleutelingsmethode e-mailtekst]	[AES-256]

3 Certificaatvalidatie instellen

Bij gebruik van TLS-versleutelde communicatie om de impact van man-in-the-middle-aanvallen te verminderen, raden we aan de certificaatvalidatie te gebruiken. Voor validatie-items raden we aan om minimaal de certificaatvervaldatum en de certificaatketen in te schakelen.

Als u verbinding probeert te maken met een legacy-omgeving zonder certificaatvalidatie, neemt het risico op man-in-the-middle-aanvallen toe. We raden aan om dit in een beveiligde netwerkomgeving te gebruiken.

Certificaatvalidatie aan de MFP-zijde wordt aanbevolen voor de volgende MFP-clientfuncties. Raadpleeg de volgende secties voor meer informatie over de instellingslocaties.

POP, SMTP (Start TLS/SMTP over SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel



Tips

Certificaatvalidatie aan de clientzijde die met de MFP is verbonden, wordt aanbevolen voor de volgende MFP-serverfuncties.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP socket

3.1 POP

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [E-mail Setting] (E-mailinstelling) - [E-mail RX (POP)] (E-mailontvangst (POP))

Instelitem	Aanbevolen instelling
[Certificate Verification Level Settings] (Instellingen certificaat verificatieniveau)	[Expiration Date] (Vervaldatum): AAN [Chain] (Keten): AAN

3.2 SMTP

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [E-mail Setting] (E-mailinstelling) - [E-mail TX (SMTP)] (E-mail TX (SMTP))

Instelitem	Aanbevolen instelling
[Certificate Verification Level Settings] (Instellingen certificaat verificatieniveau)	[Expiration Date] (Vervaldatum): AAN [Chain] (Keten): AAN

3.3 IEEE802.1X Auth

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [IEEE802.1X Authentication Setting] (IEEE802.1X authenticatie-instelling) - [IEEE802.1X Authentication Setting] (IEEE802.1X authenticatie-instelling) - [Supplicant Setting] (Instelling aanvrager)

Instelitem	Aanbevolen instelling
[Certificate Verification Level Settings] (Instellingen certificaat verificatieniveau)	[Expiration Date] (Vervaldatum): AAN [Chain] (Keten): AAN

3.4 IPsec

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [TCP/IP Setting] (TCP/IP-instelling) - [IPsec] (IPsec) - [Enable IPsec] (IPsec inschakelen)

Instelitem	Aanbevolen instelling
[Certificate Verification Level Settings] (Instellingen certificaat verificatieniveau)	[Expiration Date] (Vervaldatum): [Confirm] (Bevestigen) [Chain] (Keten): [Confirm] (Bevestigen)



Tips

Registreer vooraf in de [IPsec Setting] (IPsec-instelling) de items [IKE], [SA], [Peer] en [Protocol Setting] (Protocolinstelling).

3.5 WebDAV-client

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [WebDAV Settings] (WebDAV-instellingen) - [WebDAV Client Settings] (WebDAV-client-instellingen)

Instelitem	Aanbevolen instelling
[Certificate Verification Level Settings] (Instellingen certificaat verificatieniveau)	[Expiration Date] (Vervaldatum): AAN [Chain] (Keten): AAN

3.6 LDAP

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [LDAP Setting] (LDAP-instelling) - [Setting Up LDAP] (LDAP installeren)

Instelitem	Aanbevolen instelling
[Certificate Verification Level Settings] (Instellingen certificaat verificatieniveau)	[Expiration Date] (Vervaldatum): AAN [Chain] (Keten): AAN

3.7 DPWS

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [DPWS Settings] (DPWS-instellingen) - [DPWS Common Settings] (Algemene DPWS-instellingen)

Instelitem	Aanbevolen instelling
[Certificate Verification Level Settings] (Instellingen certificaat verificatieniveau)	[Expiration Date] (Vervaldatum): AAN [Chain] (Keten): AAN

3.8 OpenAPI

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [OpenAPI Setting] (OpenAPI instelling) - [OpenAPI Setting] (OpenAPI instelling)

Instelitem	Aanbevolen instelling
[Certificate Verification Level Settings] (Instellingen certificaat verificatieniveau)	[Expiration Date] (Vervaldatum): AAN [Chain] (Keten): AAN

3.9 Extern paneel

Instellingslocatie: [Utility] (Hulpprogramma) - [Administrator] (Beheerder) - [Network] (Netwerk) - [Remote Panel Settings] (Instellingen extern paneel) - [Remote Panel Client Settings] (Client-instellingen extern paneel)

Instelitem	Aanbevolen instelling
[Certificate Verification Level Settings] (Instellingen certificaat verificatieniveau)	[Expiration Date] (Vervaldatum): AAN [Chain] (Keten): AAN

4 Aanvullende beveiligingsinformatie

4.1 Aanbeveling voor best practices

We raden aan dat de te gebruiken versleutelingsalgoritmes voldoen aan de best practices-instellingen zoals aanbevolen in de EUCC Guidelines on Cryptography en de SOGIS-Agreed-Cryptographic-Mechanisms.

Hieronder volgt een lijst van versleutelingsalgoritmes en bijbehorende sleutellengtes, zoals aanbevolen in de 'EUCC Guidelines on Cryptography en de SOGIS-Agreed-Cryptographic-Mechanisms'.

Item	Aanbevolen instelling
Versleutelingsalgoritmes	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Lengte van de versleutelingsleutel	RSA: 2048 bits of meer ECC: 256 bits of meer AES: 256-bits

Tips

Raadpleeg voor meer informatie de nieuwste EUCC Guidelines on Cryptography en SOGIS-Agreed-Cryptographic-Mechanisms.

4.2 Voorzorgsmaatregelen bij communicatie met legacy-systemen

Voor communicatie met legacy-systemen worden de volgende protocollen en versies verondersteld te worden gebruikt.

Het gebruik van legacy-instellingen vergroot de beveiligingsrisico's. Gebruik ze daarom alleen in een beveiligde netwerkgeving.

Item	Legacy-instellingen
Protocol	SLP FTP SMB (3.0 of een eerdere versie, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Afhankelijk van server/UIT) DPWS TCPsocket
Versleutelingsalgoritmes	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Lengte van de versleutelingsleutel	RSA: 1024 bits of minder ECC: 160 bits of minder AES: 128 bits of minder DES: 56-bits 3DES: 112-bits

IPsec-legacy-instellingen

[IKEv1]

Instelitem	Legacy-instellingen
[Encryption Algorithm] (Versleutelingsalgoritme)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 en 192])
[Authentication Algorithm] (Authenticatie-algoritme)	Niet gebruikt
[Diffie-Hellman Group] (Diffie-Hellman-groep)	[Group 1] (Groep 1), [Group 2] (Groep 2), [Group 5] (Groep 5)

[IKEv2]

Instelitem	Legacy-instellingen
[Encryption Algorithm] (Versleutelingsalgoritme)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 en 192])
[Authentication Algorithm] (Authenticatie-algoritme)	Niet gebruikt
[Diffie-Hellman Group] (Diffie-Hellman-groep)	[Group 1] (Groep 1), [Group 2] (Groep 2), [Group 5] (Groep 5)

[SA]

Instelitem	Legacy-instellingen
[Key Exchange Method] (Toetsuitwisselingsmethode)	[IKEv1]
[Authentication Method] (Authenticatiemethode)	[Digital Signature] (Digitale handtekening)

Instelitem	Legacy-instellingen
[ESP Encryption Algorithm] (ESP-versleutelings- algoritme)	[3DES-CBC] ([128]/[192]/[128 en 192]) [AES-CTR] ([128]/[192]/[128 en 192]) [AES-GCM] ([128]/[192]/[128 en 192]) [AES-GCM-64] ([128]/[192]/[128 en 192]) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 en 192])
[Perfect Forward Secrecy] (Perfecte geheimhouding doorsturen)	AAN
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellman-groep (IKEv1))	[Group 1] (Groep 1), [Group 2] (Groep 2), [Group 5] (Groep 5)

4.3 Netwerkinterfaces en services die bij aflevering uit de fabriek beschikbaar zijn

Servicetype	Protocol	Poortnummer
DHCP	UDP	68
HTTP-server	TCP	80
NETBIOS Name Service	UDP	137
NETBIOS Datagram Service	UDP	138
SNMP	UDP	161
HTTP-server over SSL/?/IPP?over?SSL	TCP	443
LPD-afdruk	TCP	515
DHCPv6-client	UDP	546
IPP-afdruk	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-tool)	TCP	8091
RAW-afdruk	TCP	9100
RAW-afdruk	TCP	9112
RAW-afdruk	TCP	9113
RAW-afdruk	TCP	9114
RAW-afdruk	TCP	9115
RAW-afdruk	TCP	9116
OpenAPI	TCP	50001

4.4 Over invoervalidatie

Raadpleeg voor het aantal in te voeren tekens voor netwerkinstellingen, enz. de afzonderlijke instellingen in de handleiding.

Afhankelijk van de taalcodering kan de maximaal toegestane invoer (in de MFP opgeslagen gegevens) voor items met multibyte-ondersteuning driemaal zo groot zijn als het aantal tekens.

Anbefalinger for sikkert nettverkstilkoblet utstyr

Innholdsfortegnelse

1 Konfigurasjon av IP-adressefiltreringen

1.1	IP-adressefiltrering	1-3
1.2	Hurtig IP-filtrering	1-3

2 Konfigurasjon av den krypterte kommunikasjonen

2.1	TLS-kryptering	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP Socket.....	2-6
2.2	Annen kryptering	2-7
2.2.1	SMBServer	2-7
	SMB-kryptering.....	2-7
	SMB-signatur.....	2-7
2.2.2	SMBClient	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Konfigurasjon av sertifikatvalideringen

3.1	POP.....	3-10
3.2	SMTP	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	RemotePanel	3-12

4 Ytterligere sikkerhetsinformasjon

4.1	Anbefalinger om beste praksis.....	4-13
4.2	Forholdsregler for kommunikasjon med eldre systemer	4-14
	Eldre IPsec-innstillinger	4-14
4.3	Nettverkgrensesnitt og tjenester som er tilgjengelige fra fabrikkforsendelse	4-16
4.4	Om inndatavalidering.....	4-17



Om denne bruksanvisningen

Denne bruksanvisningen beskriver informasjon og innstillinger som gjør det mulig å bruke utstyr på en sikker måte.

Når du kobler denne maskinen til nettverket, må du bruke den i et miljø som er beskyttet av en brannmur. Vi anbefaler også at du konfigurerer en privat IP-adresse som IP-adresse til maskinen.

Konfigurasjon av en privat IP-adresse gir brukere bare på et lokalnett, for eksempel et internt lokalnett, tilgang til maskinen, noe som hindrer uautorisert tilgang utenfra.

Hvis du må bruke en global IP-adresse, må du sørge for å installere maskinen i en brannmur.

1 Konfigurasjon av IP-adressefiltreringen

IP-adressefiltrering er en funksjon som begrenser hvilket utstyr som har tilgang til maskinen gjennom IP-adressen. Du kan begrense tilgang fra uautorisert utstyr ved å stille inn denne funksjonen riktig.

IP-adressefiltreringsfunksjonen på maskinen kan stilles inn ved hjelp av følgende to metoder.

1.1 IP-adressefiltrering

Spesifiser manuelt hvilket IP-adresseområde du ønsker å tillate eller nekte tilgang.

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [TCP/IP Setting] (TCP/IP-innstilling) - [IP Address Filtering] (IP-adressefiltrering)



Tips

Angi IP-adressene du ønsker å tillate eller nekte for å passe miljøet ditt.

1.2 Hurtig IP-filtrering

IP-adresseområdet som gis tilgang, stilles inn automatisk basert på IP-adressen og nettverksmasken som er angitt i maskinen.

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [TCP/IP Setting] (TCP/IP-innstilling) - [Quick IP Filtering] (Hurtig IP-filtrering)

Anbefalte innstillinger: [Synchronize IP Address]/[Synchronize Subnet Mask] (Synkroniser IP-adresse / Synkroniser nettverksmaske)*

* Velg den som passer miljøet ditt.

2 Konfigurasjon av den krypterte kommunikasjonen

Vi anbefaler at du bruker følgende krypterte kommunikasjon for å hindre tyvlytting av data, datamanipulering og øktkapring.

2.1 TLS-kryptering

Vi anbefaler at du konfigurerer følgende innstillinger for å redusere risikoen for sårbarheter.

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Security] (Sikkerhet) - [PKI Settings] (PKI-innstillinger) - [Enable SSL Version] (Aktiver SSL-versjon)

Innstilling	Anbefalt innstilling
[Mode using SSL/TLS] (Modus med SSL/TLS)	[Admin. Mode and User Mode] (Adminmodus og brukermodus)
[SSL/TLS Version Setting] (SSL/TLS-versjons- innstilling)	TLS1.2 TLS1.3 (IEEE802.1X-inkompatibel)
[Encryption Strength] (Krypteringsstyrke)	AES-256

Det opprinnelige sertifikatet er installert på fabrikken. Hvis du trenger et annet sertifikat, må du registrere et nytt på følgende sted.

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Security] (Sikkerhet) - [PKI Settings] (PKI-innstillinger) - [Device Certificate Setting] (Enhetssertifikatinnstilling)

Innstilling	Anbefalt innstilling
[Encryption Key Type] (Krypteringsnøkkeltype)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

TLS-krypteringen støttes for følgende protokoller og tjenester. Mer informasjon om plassering av innstillinger finnes i følgende avsnitt.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP Socket

2.1.1 HTTP (Web Connection)

Hvis du aktiverer [Enable SSL Version] (Aktiver SSL-versjon), skifter kommunikasjonsmodusen automatisk til TLS-kryptert kommunikasjon (HTTPS).

2.1.2 WebDAVServer

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [WebDAV Settings] (WebDAV-innstillinger) - [WebDAV Server Settings] (WebDAV-serverinnstillinger)

Innstilling	Anbefalt innstilling
[SSL Settings] (SSL-innstillinger)	[SSL Only] (Kun SSL)

2.1.3 IPP

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [HTTP Server Settings] (HTTP-serverinnstillinger)

Innstilling	Anbefalt innstilling
[IPP-SSL Settings] (IPP-SSL-innstillinger)	[SSL Only] (Kun SSL)

2.1.4 OpenAPI

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [OpenAPI Setting] (OpenAPI-innstilling) - [OpenAPI Setting] (OpenAPI-innstilling)

Innstilling	Anbefalt innstilling
[SSL/Port Settings] (SSL-/portinnstillinger)	[SSL Only] (Kun SSL)

2.1.5 RemotePanel

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [Remote Panel Settings] (Innstillinger for fjernstyrt panel) - [Remote Panel Server Settings] (Serverinnstillinger for fjernstyrt panel)

Innstilling	Anbefalt innstilling
[Port No.(SSL)] (Portnr. (SSL))	[50443]

Tips

Hvis du aktiverer [Enable SSL Version] (Aktiver SSL-versjon), skifter kommunikasjonsmodusen automatisk til TLS-kryptert kommunikasjon. Spesifiser et portnummer.

2.1.6 DPWS

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [DPWS Settings] (DPWS-innstillinger) - [DPWS Common Settings] (DPWS-fellesinnstillinger)

Innstilling	Anbefalt innstilling
[SSL Settings] (SSL-innstillinger)	PÅ

2.1.7 POP

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [E-mail Setting] (E-postinnstilling) - [E-mail RX (POP)] (E-post RX (POP))

Innstilling	Anbefalt innstilling
[Enable SSL] (Aktiver SSL)	PÅ

2.1.8 SMTP

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [E-mail Setting] (E-postinnstilling) - [E-mail TX (SMTP)] (E-post TX (SMTP))

Innstilling	Anbefalt innstilling
[SSL/TLS Settings] (SSL/TLS-innstillinger)	[SMTP over SSL]

2.1.9 IEEE802.1X Auth

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [IEEE802.1X Authentication Setting] (IEEE802.1X-autentiseringsinnstilling) - [IEEE802.1X Authentication Setting] (IEEE802.1X-autentiseringsinnstilling) - [Supplicant Setting] (Vikarinnstilling)

Innstilling	Anbefalt innstilling
[EAP-Type]	Velg [EAP-TLS], [EAP-TTLS] eller [PEAP].

2.1.10 LDAP

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [LDAP Setting] (LDAP-innstilling) - [Setting Up LDAP] (Konfigurere LDAP)

Innstilling	Anbefalt innstilling
[Enable SSL] (Aktiver SSL)	PÅ

2.1.11 TCP Socket

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [TCP Socket Setting] (TCP Socket-innstilling)

Innstilling	Anbefalt innstilling
[Use SSL/TLS] (Bruk SSL/TLS)	PÅ

2.2 Annen kryptering

Vi anbefaler at du konfigurerer følgende innstillinger for å redusere risikoen for sårbarheter. Mer informasjon om innstillingene for hver funksjon finnes i følgende avsnitt.

Funksjon	Anbefalt innstilling
SMBServer	SMB-kryptering, SMB-signatur
SMBClient	Kerberos-autentisering
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	PÅ

2.2.1 SMBServer

Bruk av SMB-kryptering og SMB-signatur kan redusere følgende sikkerhetsrisikoer.

- Tyvlytting: En ondsinnet tredjepart kan avskjære kommunikasjon og stjele personlig eller konfidensiell informasjon.
- Datamanipulering: Det finnes en risiko for at kommunikasjoninnhold kan manipuleres med et Man-In-The-Middle-angrep (MITM).
- Spoofing: Hvis autentiseringsinformasjon blir stjålet, kan en tredjepart fremstå som en legitim bruker for å få uautorisert tilgang.
- Informasjonslekkasje: Ukryptert kommunikasjon kan enkelt avskjæres, spesielt på offentlige wifi-nettverk, noe som øker risikoen for at personlig informasjon og kredittkortinformasjon lekkes.

SMB-kryptering

Forutsetninger

- Opprett en offentlig brukerboks. Konfigurer også innstillingen for automatisk å overføre filer fra den offentlige brukerboksen og lagre dem i SMB-mappen.
- Spesifiser passordet for brukerboksen.

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Box] (Boks) - [User Box List] (Brukerboksliste)

Innstilling	Anbefalt innstilling
[SMB Communication Encryption] (SMB-kommunikasjonskryptering)	[Encrypt] (Krypter)

SMB-signatur

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [SMB Setting] (SMB-innstilling) - [SMB Server Settings] (SMB-serverinnstillinger)

Innstilling	Anbefalt innstilling
[SMB security Signature Setting] (SMB-sikkerhetssignaturinnstilling)	[Required] (Påkrevd)

2.2.2 SMBClient

Kerberos-autentiseringen bruker sterk krypteringsteknologi og reduserer vesentlig risikoen for at informasjon blir stjålet under autentiseringsprosessen. Det sikrer også dataintegritet og hindrer datamanipulering mellom sender og mottaker samt NTLM-reléangrep.

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [SMB Setting] (SMB-innstilling) - [Client Setting] (Klientinnstilling)

Innstilling	Anbefalt innstilling
[SMB Authentication Setting] (SMB-autentiserings-innstilling)	[Kerberos]

2.2.3 SNMP

Angi krypteringen med SNMPv3. Hvis autentiseringsinnstillingen også legges til, kan du øke sikkerheten ytterligere. Sikkerhetsrisikoene er omtrent de samme som med SMB.

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [SNMP Setting] (SNMP-innstilling)

Innstilling	Anbefalt innstilling
[SNMP Setting] (SNMP-innstilling)	[SNMP v3(IP)]
[Encryption Algorithm] (Krypteringsalgoritme)	[AES-128]
[Authentication Method] (Autentiseringsmetode)	Velg [SHA-256], [SHA-384] eller [SHA-512].

2.2.4 IPsec

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [TCP/IP Setting] (TCP/IP-innstilling) - [IPsec] (IPsec) - [IPsec Setting] (IPsec-innstilling)

[IKEv2]

Innstilling	Anbefalt innstilling
[Encryption Algorithm] (Krypteringsalgoritme)	[AES-CBC] ([256]/[192 and 256] (192 og 256)/[All] (Alle))
[Authentication Algorithm] (Autentiseringsalgoritme)	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 og 384)/[384 and 512] (384 og 512)/[All] (Alle)), [AES-XCBC]
[Diffie-Hellman Group] (Diffie-Hellman-gruppe)	[Group 14] (Gruppe 14), [Group 19] (Gruppe 19)

[SA]

Innstilling	Anbefalt innstilling
[Encapsulation Mode] (Innkapslingsmodus)	[Tunnel], [Transport]
[Security Protocol] (Sikkerhetsprotokoll)	[ESP]
[Key Exchange Method] (Nøkkelutvekslingsmetode)	[IKEv2]
[Authentication Method] (Autentiseringsmetode)	[Digital Signature] (Digital signatur)
[ESP Encryption Algorithm] (ESP-krypteringsalgoritme)	[AES-GCM] ([256]/[192 and 256] (192 og 256)/[All] (Alle)), [AES-GCM-64] ([256]/[192 and 256] (192 og 256)/[All] (Alle)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 og 256)/[All] (Alle))

Innstilling	Anbefalt innstilling
[Perfect Forward Secrecy] (PFS)	PÅ
[Diffie-Hellman Group(IKEv2)] (Diffie-Hellman-gruppe (IKEv2)) - [Priority1-4] (Prioritet 1-4)	[Group 14] (Gruppe 14), [Group 19] (Gruppe 19)

2.2.5 S/MIME

Hvis du bruker valgfri S/MIME når du sender e-post, kan du kryptere e-postinnholdet for å hindre tyvlytting og verifisere senderens identitet med elektronisk signatur. Dette er et effektivt tiltak mot spoofing- og phishing-svindler.

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [E-mail Setting] (E-postinnstilling) - [S/MIME] (S/MIME)

Innstilling	Anbefalt innstilling
[Digital Signature] (Digital signatur)	[Always add signature] (Alltid legg til signatur)
[Digital Signature Type] (Digital signaturtype)	[SHA-256]
[E-Mail Text Encrypt. Method] (Krypteringsmetode for e-posttekst)	[AES-256]

3 Konfigurasjon av sertifikatvalideringen

Når TLS-kryptert kommunikasjon brukes til å redusere påvirkningen fra man-in-the-middle-angrep, anbefaler vi at du bruker sertifikatvalideringen. For valideringselementer anbefaler vi at du aktiverer sertifikatets utløpsdato og kjede som et minimum.

Hvis det gjøres forsøk på å koble til et eldre miljø som ikke har en sertifikatvalideringsfunksjon, øker risikoen for man-in-the-middle-angrep. Vi anbefaler at du bruker den i et sikkert nettverksmiljø.

Sertifikatvalideringen på MFP-siden anbefales i følgende MFP-klientfunksjoner. Mer informasjon om plassering av innstillinger finnes i følgende avsnitt.

POP, SMTP (Start TLS/SMTP over SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPsec, WebDAV, LDAP, DPWS, RemotePanel



Tips

Sertifikatvalideringen på klientsidene tilkoblet MFP anbefales i følgende MFP-serverfunksjoner. HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP Socket

3.1 POP

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [E-mail Setting] (E-postinnstilling) - [E-mail RX (POP)] (E-post RX (POP))

Innstilling	Anbefalt innstilling
[Certificate Verification Level Settings] (Innstillinger for sertifikatkontrollnivå)	[Expiration Date] (Utløpsdato): PÅ [Chain] (Kjede): PÅ

3.2 SMTP

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [E-mail Setting] (E-postinnstilling) - [E-mail TX (SMTP)] (E-post TX (SMTP))

Innstilling	Anbefalt innstilling
[Certificate Verification Level Settings] (Innstillinger for sertifikatkontrollnivå)	[Expiration Date] (Utløpsdato): PÅ [Chain] (Kjede): PÅ

3.3 IEEE802.1X Auth

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [IEEE802.1X Authentication Setting] (IEEE802.1X-autentiseringsinnstilling) - [IEEE802.1X Authentication Setting] (IEEE802.1X-autentiseringsinnstilling) - [Supplicant Setting] (Vikarinnstilling)

Innstilling	Anbefalt innstilling
[Certificate Verification Level Settings] (Innstillinger for sertifikatkontrollnivå)	[Expiration Date] (Utløpsdato): PÅ [Chain] (Kjede): PÅ

3.4 IPsec

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [TCP/IP Setting] (TCP/IP-innstilling) - [IPsec] (IPsec) - [Enable IPsec] (Aktiver IPsec)

Innstilling	Anbefalt innstilling
[Certificate Verification Level Settings] (Innstillinger for sertifikat-kontrollnivå)	[Expiration Date] (Utløpsdato): [Confirm] (Bekreft) [Chain] (Kjede): [Confirm] (Bekreft)

Tips

I [IPsec Setting] (IPsec-innstilling) registrer du elementene [IKE] (IKE), [SA] (SA), [Peer] (Likenett) og [Protocol Setting] (Protokollinnstilling) på forhånd.

3.5 WebDAVClient

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [WebDAV Settings] (WebDAV-innstillinger) - [WebDAV Client Settings] (WebDAV-klientinnstillinger)

Innstilling	Anbefalt innstilling
[Certificate Verification Level Settings] (Innstillinger for sertifikat-kontrollnivå)	[Expiration Date] (Utløpsdato): PÅ [Chain] (Kjede): PÅ

3.6 LDAP

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [LDAP Setting] (LDAP-innstilling) - [Setting Up LDAP] (Konfigurere LDAP)

Innstilling	Anbefalt innstilling
[Certificate Verification Level Settings] (Innstillinger for sertifikat-kontrollnivå)	[Expiration Date] (Utløpsdato): PÅ [Chain] (Kjede): PÅ

3.7 DPWS

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [DPWS Settings] (DPWS-innstillinger) - [DPWS Common Settings] (DPWS-fellesinnstillinger)

Innstilling	Anbefalt innstilling
[Certificate Verification Level Settings] (Innstillinger for sertifikat-kontrollnivå)	[Expiration Date] (Utløpsdato): PÅ [Chain] (Kjede): PÅ

3.8 OpenAPI

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [OpenAPI Setting] (OpenAPI-innstilling) - [OpenAPI Setting] (OpenAPI-innstilling)

Innstilling	Anbefalt innstilling
[Certificate Verification Level Settings] (Innstillinger for sertifikat-kontrollnivå)	[Expiration Date] (Utløpsdato): PÅ [Chain] (Kjede): PÅ

3.9 RemotePanel

Plassering av innstillinger: [Utility] (Verktøy) - [Administrator] (Administrator) - [Network] (Nettverk) - [Remote Panel Settings] (Innstillinger for fjernstyrt panel) - [Remote Panel Client Settings] (Klientinnstillinger for fjernstyrt panel)

Innstilling	Anbefalt innstilling
[Certificate Verification Level Settings] (Innstillinger for sertifikat-kontrollnivå)	[Expiration Date] (Utløpsdato): PÅ [Chain] (Kjede): PÅ

4 Ytterligere sikkerhetsinformasjon

4.1 Anbefalinger om beste praksis

Vi anbefaler at krypteringsalgoritmene som skal brukes, overholder innstillingene for beste praksis som anbefales i EUCC Guidelines on Cryptography og SOGIS-Agreed-Cryptographic-Mechanisms.

Nedenfor er en liste over krypteringsalgoritmer og nøkkellengder som anbefales av EUCC Guidelines on Cryptography og SOGIS-Agreed-Cryptographic-Mechanisms.

Element	Anbefalt innstilling
Krypteringsalgoritmer	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Lengde på krypteringsnøkkel	RSA: 2048 bits eller mindre ECC: 256 bits eller mindre AES: 256 bits

Tips

Mer informasjon finnes i de nyeste EUCC Guidelines on Cryptography og SOGIS-Agreed-Cryptographic-Mechanisms.

4.2 Forholdsregler for kommunikasjon med eldre systemer

Følgende protokoller og versjoner forutsettes brukt for kommunikasjon med eldre systemer.

Bruk av eldre innstillinger øker sikkerhetsrisikoene, så bruk dem i et sikkert nettverksmiljø.

Element	Eldre innstillinger
Protokoll	SLP FTP SMB (3.0 eller tidligere versjon, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Avhengig av server/AV) DPWS TCPsocket
Krypteringsalgoritmer	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Lengde på krypteringsnøkkel	RSA: 1024 bits eller mindre ECC: 160 bits eller mindre AES: 128 bits eller mindre DES: 56 bits 3DES: 112 bits

Eldre IPsec-innstillinger

[IKEv1]

Innstilling	Eldre innstillinger
[Encryption Algorithm] (Krypteringsalgoritme)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 og 192))
[Authentication Algorithm] (Autentiseringsalgoritme)	Brukes ikke
[Diffie-Hellman Group] (Diffie-Hellman-gruppe)	[Group 1] (Gruppe 1), [Group 2] (Gruppe 2), [Group 5] (Gruppe 5)

[IKEv2]

Innstilling	Eldre innstillinger
[Encryption Algorithm] (Krypteringsalgoritme)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 og 192))
[Authentication Algorithm] (Autentiseringsalgoritme)	Brukes ikke
[Diffie-Hellman Group] (Diffie-Hellman-gruppe)	[Group 1] (Gruppe 1), [Group 2] (Gruppe 2), [Group 5] (Gruppe 5)

[SA]

Innstilling	Eldre innstillinger
[Key Exchange Method] (Nøkkelutvekslingsmetode)	[IKEv1]
[Authentication Method] (Autentiseringsmetode)	[Digital Signature] (Digital signatur)

Innstilling	Eldre innstillinger
[ESP Encryption Algorithm] (ESP-krypteringsalgoritme)	[3DES-CBC] ([128]/[192]/[128 and 192] (128 og 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 og 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 og 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 og 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 og 192))
[Perfect Forward Secrecy] (PFS)	PÅ
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellman-gruppe (IKEv2))	[Group 1] (Gruppe 1), [Group 2] (Gruppe 2), [Group 5] (Gruppe 5)

4.3 Nettverksgrensesnitt og tjenester som er tilgjengelige fra fabrikkforsendelse

Tjenestetype	Protokoll	Portnummer
DHCP	UDP	68
HTTP-server	TCP	80
NETBIOS-navnetjeneste	UDP	137
NETBIOS-datagramtjeneste	UDP	138
SNMP	UDP	161
HTTP Server over SSL / IPP over SSL	TCP	443
LPD-utskrift	TCP	515
DHCPv6-klient	UDP	546
IPP-utskrift	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-verktøy)	TCP	8091
RAW-utskrift	TCP	9100
RAW-utskrift	TCP	9112
RAW-utskrift	TCP	9113
RAW-utskrift	TCP	9114
RAW-utskrift	TCP	9115
RAW-utskrift	TCP	9116
OpenAPI	TCP	50001

4.4 Om inndatavalidering

Antallet tegn som skal legges inn for nettverksinnstillinger osv., finnes i hver av innstillingene i brukerveiledningen.

Avhengig av kodingen av språket kan største tillatte inndata (data lagret i MFP) for elementer som støtter tegn med flere byte, være tre ganger antallet tegn.

Zalecenia dotyczące bezpieczeństwa urządzeń podłączonych do sieci

Spis treści

1 Ustawianie filtrowania adresów IP

1.1	Filtrowanie adresów IP	1-3
1.2	Szybkie filtrowanie IP	1-3

2 Ustawianie komunikacji zaszyfrowanej

2.1	Szyfrowanie TLS	2-4
2.1.1	HTTP (Połączenie sieci Web)	2-4
2.1.2	Serwer WebDAV	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	Panel zdalny.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	Uwierzytelnienie IEEE802.1X	2-6
2.1.10	LDAP	2-6
2.1.11	Gniazdo TCP.....	2-6
2.2	Inne sposoby szyfrowania	2-7
2.2.1	Serwer SMB	2-7
	Szyfrowanie folderu SMB	2-7
	Podpisywanie SMB.....	2-7
2.2.2	Klient SMB	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Ustawienie walidacji certyfikatu

3.1	POP	3-10
3.2	SMTP	3-10
3.3	Uwierzytelnienie IEEE802.1X	3-10
3.4	IPsec	3-11
3.5	Klient WebDAV	3-11
3.6	LDAP	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	Panel zdalny	3-12

4 Dodatkowe informacje o zabezpieczeniach

4.1	Zalecane najlepsze rozwiązania	4-13
4.2	Środki ostrożności dotyczące połączeń ze starszymi systemami	4-14
	Stare ustawienia IPsec.....	4-14
4.3	Interfejsy i usługi instalowane fabrycznie	4-16
4.4	Informacje o walidacji wprowadzanych danych	4-17



Informacje na temat niniejszej instrukcji

W niniejszej instrukcji opisano informacje i ustawienia umożliwiające bezpieczne korzystanie z urządzenia.

Podłączając urządzenie do sieci należy pamiętać, by korzystać z niego w środowisku chronionym przez zaporę. Zaleca się również ustawienie prywatnego adresu IP jako adresu IP urządzenia.

Skonfigurowanie prywatnego adresu IP pozwala na dostęp do urządzenia jedynie użytkownikom podłączonym do sieci lokalnej, a tym samym zapobiega nieautoryzowanemu dostępowi z zewnątrz.

Jeśli konieczne jest korzystanie z globalnego adresu IP, należy pamiętać, by urządzenie zainstalować za zaporą.

1 Ustawianie filtrowania adresów IP

Filtrowanie adresów IP to funkcja ograniczająca urządzenia, w zależności od ich adresów IP, które mogą uzyskiwać dostęp do urządzenia. Jeśli ta funkcja zostanie poprawnie skonfigurowana, możliwe będzie ograniczenie dostępu do urządzenia przez nieuprawnione urządzenia.

Funkcja filtrowania adresów IP w urządzeniu może być skonfigurowana z wykorzystaniem dwóch poniższych metod.

1.1 Filtrowanie adresów IP

Ręczne określić zakres adresów IP, które mogą lub nie mogą uzyskiwać dostęp do urządzenia.

Lokalizacja ustawienia: [Utility] (Narzędzie) - [Administrator] (Administrator) - [Network] (Sieć) - [TCP/IP Setting] (Ustawienie TCP/IP) - [IP Address Filtering] (Filtrowanie adresów IP)



Wskazówki

Należy skonfigurować takie dozwolone lub niedozwolone adresy IP, które będą odpowiednie dla środowiska, w którym używane jest urządzenie.

1.2 Szybkie filtrowanie IP

Zakres adresów IP, który umożliwia dostęp, jest ustawiany automatycznie w oparciu o adres IP i maskę podsieci skonfigurowane w urządzeniu.

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [TCP/IP Setting] (Ustawienie TCP/IP) - [Quick IP Filtering] (Szybkie filtrowanie IP)

Zalecane ustawienia: [Synchronize IP Address] (Synchronizuj adres IP)/[Synchronize Subnet Mask] (Synchronizuj maskę podsieci) *

* Należy wybrać jedną z tych opcji, najlepiej odpowiadającą środowisku, w którym używane jest urządzenie.

2 Ustawianie komunikacji zaszyfrowanej

Zaleca się korzystanie z następujących połączeń szyfrowanych, aby nie dopuścić do podsłuchiwania, fałszowania danych i przechwytywania sesji.

2.1 Szyfrowanie TLS

Zaleca się skonfigurowanie następujących ustawień, aby zredukować ryzyko wystąpienia luk w zabezpieczeniach.

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Security] (Zabezpieczenia) - [PKI Settings] (Ustawienia PKI) - [Enable SSL Version] (Włącz wersję SSL)

Element ustawienia	Zalecane ustawienie
[Mode using SSL/TLS] (Tryb korzystający z SSL/TLS)	[Admin. Mode and User Mode] (Tryb administratora i Tryb użytkownika)
[SSL/TLS Version Setting] (Ustawienie wersji SSL/TLS)	TLS1.2 TLS1.3 (niezgodny z IEEE802.1X)
[Encryption Strength] (Siła szyfrowania)	AES-256

Początkowy certyfikat jest instalowany fabrycznie. Jeśli wymagany będzie inny certyfikat, należy go zarejestrować w następującej lokalizacji.

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Security] (Zabezpieczenia) - [PKI Settings] (Ustawienia PKI) - [Device Certificate Setting] (Ustawienie certyfikatu urządzenia)

Element ustawienia	Zalecane ustawienie
[Encryption Key Type] (Rodzaj klucza szyfrowania)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Szyfrowanie TLS jest obsługiwane przez następujące protokoły i usługi. Aby poznać szczegóły na temat lokalizacji ustawień, patrz kolejne sekcje.

- HTTP (Połączenie sieci Web, Serwer WebDAV, IPP, OpenAPI, Panel zdalny)
- DPWS
- POP
- SMTP (Start TLS, SMTP z wykorzystaniem SSL)
- Uwierzytelnienie IEEE802.1X (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- Gniazdo TCP

2.1.1 HTTP (Połączenie sieci Web)

Jeśli włączone zostanie ustawienie [Enable SSL Version] (Włącz wersję SSL), tryb połączeń automatycznie przełączony będzie do opcji połączeń szyfrowanych TLS (HTTPS).

2.1.2 Serwer WebDAV

Lokalizacja ustawienia: [Utility] (Narzędzia)- [Administrator] (Administrator) - [Network] (Sieć) - [WebDAV Settings] (Ustawienia WebDAV) - [WebDAV Server Settings] (Ustawienia serwera WebDAV)

Element ustawienia	Zalecane ustawienie
[SSL Settings] (Ustawienia SSL)	[SSL Only] (Tylko SSL)

2.1.3 IPP

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [HTTP Server Settings] (Ustawienia serwera HTTP)

Element ustawienia	Zalecane ustawienie
[IPP-SSL Settings] (Ustawienie IPP-SSL)	[SSL Only] (Tylko SSL)

2.1.4 OpenAPI

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [OpenAPI Setting] (Ustawienie OpenAPI) - [OpenAPI Setting] (Ustawienie OpenAPI)

Element ustawienia	Zalecane ustawienie
[SSL/Port Settings] (Ustawienia portu/SSL)	[SSL Only] (Tylko SSL)

2.1.5 Panel zdalny

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [Remote Panel Settings] (Ustawienia panelu zdalnego) - [Remote Panel Server Settings] (Ustawienia serwera panelu zdalnego)

Element ustawienia	Zalecane ustawienie
[Port No. (SSL)]	[50443]



Wskazówki

Jeśli włączone zostanie ustawienie [Enable SSL Version] (Włącz wersję SSL), połączenia automatycznie przełączone będą w tryb szyfrowania TLS. Należy określić numer portu.

2.1.6 DPWS

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [DPWS Settings] (Ustawienia DPWS) - [DPWS Common Settings] (Ustawienia ogólne DPWS)

Element ustawienia	Zalecane ustawienie
[SSL Settings] (Ustawienia SSL)	Wł.

2.1.7 POP

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [E-mail Setting] (Ustawienie e-mail) - [E-mail RX (POP)] (Odbieranie e-maili (POP))

Element ustawienia	Zalecane ustawienie
[Enable SSL] (Włącz SSL)	Wł.

2.1.8 SMTP

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [E-mail Setting] (Ustawienie e-mail) - [E-mail TX (SMTP)] (TX e-maila (SMTP))

Element ustawienia	Zalecane ustawienie
[Ustawienia SSL/TLS]	[SMTP przed SSL]

2.1.9 Uwierzytelnienie IEEE802.1X

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [IEEE802.1X Authentication Setting] (Ustawienie autoryzacji IEEE802.1X) - [IEEE802.1X Authentication Setting] (Ustawienie autoryzacji IEEE802.1X) - [Supplicant Setting] (Ustawienie suplikanta)

Element ustawienia	Zalecane ustawienie
[EAP-Type]	Wybrać [EAP-TLS], [EAP-TTLS] lub [PEAP].

2.1.10 LDAP

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] - [Network] (Sieć) - [LDAP Setting] (Ustawienie LDAP) - [Setting Up LDAP] (Konfiguracja LDAP)

Element ustawienia	Zalecane ustawienie
[Enable SSL] (Włącz SSL)	WŁ.

2.1.11 Gniazdo TCP

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [TCP Socket Setting] (Ustawienie gniazda TCP)

Element ustawienia	Zalecane ustawienie
[Use SSL/TLS] (Użyj SSL/TLS)	WŁ.

2.2 Inne sposoby szyfrowania

Zaleca się skonfigurowanie następujących ustawień, aby zredukować ryzyko wystąpienia luk w zabezpieczeniach. Aby poznać szczegóły na temat ustawień każdej z funkcji, patrz kolejne sekcje.

Funkcja	Zalecane ustawienie
Serwer SMB	Szyfrowanie folderu SMB, Podpisywanie SMB
Klient SMB	Autoryzacja Kerberos
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	WŁ.

2.2.1 Serwer SMB

Korzystanie z szyfrowania SMB i podpisywania SMB może przyczynić się do zredukowania następujących zagrożeń bezpieczeństwa.

- **Podsluchiwanie:** Złośliwa strona trzecia może przechwytywać połączenia i kraść informacje osobiste lub poufne.
- **Falszowania danych:** Istnieje ryzyko, że treść komunikacji może być modyfikowana przez ataki typu Man-In-The-Middle (MITM).
- **Falszowania adresu IP:** Jeśli informacje o autoryzacji zostaną skradzione, strona trzecia może podawać się za uprawnionego użytkownika, aby uzyskać nieautoryzowany dostęp.
- **Wycieków informacji:** Połączenia nieszyfrowane mogą z łatwością być przechwytywane, szczególnie w publicznych sieciach Wi-Fi, co zwiększa zagrożenie wycieku informacji osobistych lub dot. kart kredytowych.

Szyfrowanie folderu SMB

Warunki konieczne

- Należy utworzyć Skrzynkę użytkownika publicznego. Ponadto, skonfigurować ustawienie umożliwiające automatyczne przesyłanie plików ze Skrzynki użytkownika publicznego i zapisywanie ich w Folderze SMB.
- Skonfigurować hasło do Skrzynki użytkownika.

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Box] (Skrzynka użytkownika) - [User Box List] (Lista skrzynek użytkownika)

Element ustawienia	Zalecane ustawienie
[SMB Communication Encryption] (Szyfrowanie połączeń SMB)	[Encrypt] (Szyfruj)

Podpisywanie SMB

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [SMB Setting] (Ustawienie SMB) - [SMB Server Settings] (Ustawienia serwera SMB)

Element ustawienia	Zalecane ustawienie
[SMB security Signature Setting] (Ustawienie podpisu zabezpieczeń SMB)	[Wymagana]

2.2.2 Klient SMB

Autoryzacja Kerberos wykorzystuje technologię silnego szyfrowania, w znacznej mierze redukując zagrożenie kradzieżą danych uwierzytelniających w procesie autoryzacji. Zapewnia również integralność danych, uniemożliwiając ich fałszowanie pomiędzy nadawcą i odbiorcą, a także ataki NTLM Relay.

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [SMB Setting] (Ustawienie SMB) - [Client Setting] (Ustawienie klienta)

Element ustawienia	Zalecane ustawienie
[SMB Authentication Setting] (Ustawienie autoryzacji SMB)	[Kerberos]

2.2.3 SNMP

Należy skonfigurować szyfrowanie z wykorzystaniem SNMPv3. Jeśli dodane zostanie również ustawienie autoryzacji, umożliwi to zwiększenie bezpieczeństwa. Zagrożenia dot. bezpieczeństwa są mniej więcej podobne jak w przypadku SMB.

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [SNMP Setting] (Ustawienie SMTP)

Element ustawienia	Zalecane ustawienie
[SNMP Setting] (Ustawienie SNMP)	[SNMP v3(IP)]
[Algorytm kodowania]	[AES-128]
[Authentication Method] (Metoda autoryzacji)	Wybrać [SHA-256], [SHA-384] lub [SHA-512].

2.2.4 IPsec

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [TCP/IP Setting] (Ustawienie TCP/IP) - [IPsec] (IPsec) - [IPsec Setting] (Ustawienie IPsec)

[IKEv2]

Element ustawienia	Zalecane ustawienie
[Algorytm kodowania]	[AES-CBC] ([256]/[192 i 256]/[All] (Wszystkie))
[Algorytm uwierzyteln.]	[SHA-2] ([256]/[384]/[512]/[256 i 384]/[384 i 512]/[All] (Wszystkie)), [AES-XCBC]
[Grupa Diffiego-Hellmana]	[Group 14] (Grupa 14), [Group 19] (Grupa 19)

[SA]

Element ustawienia	Zalecane ustawienie
[Encapsulation Mode] (Tryb hermetyzacji)	[Tunnel] (Tunel), [Transport] (Transport)
[Protokół zabezpieczeń]	[ESP]
[Metoda wymiany klucza]	[IKEv2]
[Authentication Method] (Metoda autoryzacji)	[Podpis cyfrowy]
[Algorytm kodowania ESP]	[AES-GCM] ([256]/[192 i 256]/[All] (Wszystkie)), [AES-GCM-64] ([256]/[192 i 256]/[All] (Wszystkie)), [ENC_NULL_AES_GMAC] ([256]/[192 i 256]/[All] (Wszystkie))
[Przekazywanie utajnione]	WŁ.

Element ustawienia	Zalecane ustawienie
[Diffie-Hellman Group(IKEv2)] (Grupa Diffiego-Hellmana (IKEv2)) - [Priority1-4] (Priorytet 1-4)	[Group 14] (Grupa 14), [Group 19] (Grupa 19)

2.2.5 S/MIME

Jeśli podczas wysyłania e-mail używany jest opcjonalny S/MIME, możliwe jest zaszyfrowanie treści wiadomości, aby zabezpieczyć ją przed podsłuchaniem oraz zweryfikowanie tożsamości nadawcy z wykorzystaniem podpisu elektronicznego. Jest to efektywne zabezpieczenie przed podszywaniem się pod nadawcę e-mail i wyłudzeniem informacji.

Lokalizacja ustawienia: [Utility] (Narzędzie) - [Administrator] (Administrator) - [Network] (Sieć) - [E-mail Setting] (Ustawienie e-mail) - [S/MIME] (S/MIME)

Element ustawienia	Zalecane ustawienie
[Podpis cyfrowy]	[Always add signature] (Zawsze dodawaj podpis)
[Digital Signature Type] (Rodzaj podpisu cyfrowego)	[SHA-256]
[E-Mail Text Encrypt. Method] (Metoda szyfrowania treści e-maila)	[AES-256]

3 Ustawienie walidacji certyfikatu

Kiedy używane są połączenia szyfrowane z użyciem TLS, aby zredukować wpływ ataków Man-In-The-Middle, zaleca się wykorzystanie walidacji certyfikatu. W elementach walidacji zaleca się włączenie co najmniej daty wygaśnięcia certyfikatu i łańcucha.

Jeśli nastąpi próba uzyskania połączenia ze starszą wersją środowiska, nieposiadającego funkcji walidacji certyfikatu, ryzyko ataków Man-In-The-Middle wzrasta. Zaleca się używanie jej w bezpiecznym środowisku sieciowym.

Walidacja certyfikatu po stronie MFP jest zalecana w następujących funkcjach klienta MFP. Aby poznać szczegóły na temat lokalizacji ustawień, patrz kolejne sekcje.

POP, SMTP (Start TLS/SMTP z wykorzystaniem SSL), Uwierzytelnienie IEEE802.1X (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, Panel zdalny



Wskazówki

Walidacja certyfikatu po stronie klienta podłączonego do MFP jest zalecana w następujących funkcjach serwera MFP.

HTTP (Połączenie sieci Web / WebDAV / IPP / DPWS / OpenAPI / Panel zdalny), Gniazdo TCP

3.1 POP

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [E-mail Setting] (Ustawienie e-mail) - [E-mail RX (POP)] (Odbieranie e-maili (POP))

Element ustawienia	Zalecane ustawienie
[Certificate Verification Level Settings] (Ustawienia poziomu weryfikacji certyfikatu)	[Expiration Date] (Data wygaśnięcia): WŁ. [Chain] (Łańcuch): WŁ.

3.2 SMTP

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [E-mail Setting] (Ustawienie e-mail) - [E-mail TX (SMTP)] (TX e-maila (SMTP))

Element ustawienia	Zalecane ustawienie
[Certificate Verification Level Settings] (Ustawienia poziomu weryfikacji certyfikatu)	[Expiration Date] (Data wygaśnięcia): WŁ. [Chain] (Łańcuch): WŁ.

3.3 Uwierzytelnienie IEEE802.1X

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [IEEE802.1X Authentication Setting] (Ustawienie autoryzacji IEEE802.1X) - [IEEE802.1X Authentication Setting] (Ustawienie autoryzacji IEEE802.1X) - [Supplicant Setting] (Ustawienie suplikanta)

Element ustawienia	Zalecane ustawienie
[Certificate Verification Level Settings] (Ustawienia poziomu weryfikacji certyfikatu)	[Expiration Date] (Data wygaśnięcia): WŁ. [Chain] (Łańcuch): WŁ.

3.4 IPsec

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [TCP/IP Setting] (Ustawienie TCP/IP) - [IPsec] (IPsec) - [IPsec Setting] (Ustawienie IPsec)

Element ustawienia	Zalecane ustawienie
[Certificate Verification Level Settings] (Ustawienia poziomu weryfikacji certyfikatu)	[Expiration Date] (Data wygaśnięcia): [Sprawdź] [Chain] (Łańcuch): [Sprawdź]



Wskazówki

W [IPsec Setting] (Ustawienie IPsec) z wyprzedzeniem zarejestrować elementy [IKE] (IKE), [SA] (Skojarzenie zabezpieczeń), [Peer] (Urządzenie równorzędne) i [Protocol Setting] (Ustawienie protokołu).

3.5 Klient WebDAV

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [WebDAV Settings] (Ustawienia WebDAV) - [WebDAV Client Settings] (Ustawienia klienta WebDAV)

Element ustawienia	Zalecane ustawienie
[Certificate Verification Level Settings] (Ustawienia poziomu weryfikacji certyfikatu)	[Expiration Date] (Data wygaśnięcia): WŁ. [Chain] (Łańcuch): WŁ.

3.6 LDAP

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [LDAP Setting] (Ustawienie LDAP) - [Setting Up LDAP] (Konfiguracja LDAP)

Element ustawienia	Zalecane ustawienie
[Certificate Verification Level Settings] (Ustawienia poziomu weryfikacji certyfikatu)	[Expiration Date] (Data wygaśnięcia): WŁ. [Chain] (Łańcuch): WŁ.

3.7 DPWS

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [DPWS Settings] (Ustawienia DPWS) - [DPWS Common Settings] (Ustawienia ogólne DPWS)

Element ustawienia	Zalecane ustawienie
[Certificate Verification Level Settings] (Ustawienia poziomu weryfikacji certyfikatu)	[Expiration Date] (Data wygaśnięcia): WŁ. [Chain] (Łańcuch): WŁ.

3.8 OpenAPI

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [OpenAPI Setting] (Ustawienie OpenAPI) - [OpenAPI Setting] (Ustawienie OpenAPI)

Element ustawienia	Zalecane ustawienie
[Certificate Verification Level Settings] (Ustawienia poziomu weryfikacji certyfikatu)	[Expiration Date] (Data wygaśnięcia): WŁ. [Chain] (Łańcuch): WŁ.

3.9 Panel zdalny

Lokalizacja ustawienia: [Utility] (Narzędzia) - [Administrator] (Administrator) - [Network] (Sieć) - [Remote Panel Settings] (Ustawienia panelu zdalnego) - [Remote Panel Client Settings] (Ustawienia klienta panelu zdalnego)

Element ustawienia	Zalecane ustawienie
[Certificate Verification Level Settings] (Ustawienia poziomu weryfikacji certyfikatu)	[Expiration Date] (Data wygaśnięcia): WŁ. [Chain] (Łańcuch): WŁ.

4 Dodatkowe informacje o zabezpieczeniach

4.1 Zalecane najlepsze rozwiązania

Zaleca się, by używane algorytmy szyfrowania były zgodne z ustawieniami najlepszych rozwiązań polecanych w EUCC Guidelines on Cryptography oraz SOGIS-Agreed-Cryptographic-Mechanisms.

Poniżej zamieszczono listę algorytmów szyfrowania oraz długości kluczy zalecanych w EUCC Guidelines on Cryptography oraz SOGIS-Agreed-Cryptographic-Mechanisms.

Element	Zalecane ustawienie
Algorytmy szyfrowania	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Algorytm bezpiecznego haszowania 2) ECC (Kryptografia krzywych eliptycznych) HMAC (Haszujący kod autoryzacji wiadomości)
Długość klucza szyfrowania	RSA: 2048 bitów lub więcej ECC: 256 bitów lub więcej AES: 256 bitów



Wskazówki

Aby poznać szczegóły, patrz najnowsze EUCC Guidelines on Cryptography oraz SOGIS-Agreed-Cryptographic-Mechanisms.

4.2 Środki ostrożności dotyczące połączeń ze starszymi systemami

Poniższe protokoły i wersje powinny być używane do komunikacji ze starszymi systemami.

Korzystanie ze starszych ustawień zwiększa zagrożenia związane z bezpieczeństwem, dlatego należy ich używać w bezpiecznym środowisku sieciowym.

Element	Starsze ustawienia
Protokół	SLP FTP SMB (3.0 lub wcześniejsza wersja, NTLMv1/v2) SNMPv1/v2 Uwierzytelnienie IEEE802.1X (EAP-TYPE: Zależnie od serwera/WYŁ.) DPWS Gniazdo TCP
Algorytmy szyfrowania	SHA-1 (Algorytm bezpiecznego haszowania 1) DES (algorytm Data Encryption Standard) 3DES (potrójny algorytm Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Długość klucza szyfrowania	RSA: 1024 bity lub mniej ECC: 160 bity lub mniej AES: 128 bitów lub mniej DES: 56 bitów 3DES: 112 bitów

Stare ustawienia IPsec

[IKEv1]

Element ustawienia	Starsze ustawienia
[Algorytm kodowania]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 i 192))
[Algorytm uwierzyteln.]	Nie wykorzystywana
[Grupa Diffiego-Hellmana]	[Group 1] (Grupa 1), [Group 2] (Grupa 2), [Group 5] (Grupa 5)

[IKEv2]

Element ustawienia	Starsze ustawienia
[Algorytm kodowania]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 i 192))
[Algorytm uwierzyteln.]	Nie wykorzystywana
[Grupa Diffiego-Hellmana]	[Group 1] (Grupa 1), [Group 2] (Grupa 2), [Group 5] (Grupa 5)

[SA]

Element ustawienia	Starsze ustawienia
[Metoda wymiany klucza]	[IKEv1]
[Authentication Method] (Metoda autoryzacji)	[Podpis cyfrowy]
[Algorytm kodowania ESP]	[3DES-CBC] ([128]/[192]/[128 and 192] (128 i 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 i 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 i 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 i 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 i 192))
[Przekazywanie utajnione]	WŁ.

Element ustawienia	Starsze ustawienia
[Diffie-Hellman Group(IKEv1)] (Grupa Diffiego-Hellmana (IKEv1))	[Group 1] (Grupa 1), [Group 2] (Grupa 2), [Group 5] (Grupa 5)

4.3 Interfejsy i usługi instalowane fabrycznie

Typ usługi	Protokół	Numer portu
DHCP	UDP	68
Serwer HTTP	TCP	80
Usługa nazw NETBIOS	UDP	137
Usługa datagramów NETBIOS	UDP	138
SNMP	UDP	161
Serwer HTTP z użyciem SSL / IPP z użyciem SSL	TCP	443
Drukowanie LPD	TCP	515
Klient DHCPv6	UDP	546
Drukowanie IPP	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (narzędzie IWS)	TCP	8091
Drukowanie RAW	TCP	9100
Drukowanie RAW	TCP	9112
Drukowanie RAW	TCP	9113
Drukowanie RAW	TCP	9114
Drukowanie RAW	TCP	9115
Drukowanie RAW	TCP	9116
OpenAPI	TCP	50001

4.4 Informacje o walidacji wprowadzanych danych

W przypadku pewnej liczby znaków, które są wprowadzane w ramach ustawień sieciowych, itp., należy zapoznać się z każdym elementem ustawienia w Podręczniku użytkownika.

Zależnie od kodowania języka maksymalna dozwolona liczba wprowadzanych danych (danych zapisywanych w MFP) dla elementów, które obsługują znaki wielobajtowe, może być trzykrotnie wyższa, niż liczba znaków.

Recomendações para dispositivos seguros ligados em rede

Conteúdo

1 Definição da filtragem IP

1.1	Filtragem IP	1-3
1.2	Filtragem IP rápida.....	1-3

2 Definir a comunicação encriptada

2.1	Encriptação TLS.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	Servidor WebDAV	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	Painel remoto.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	Autenticação IEEE802.1X	2-6
2.1.10	LDAP	2-6
2.1.11	Tomada TCP	2-6
2.2	Outra encriptação	2-7
2.2.1	Servidor SMB.....	2-7
	Encriptação SMB	2-7
	Assinatura SMB	2-7
2.2.2	Cliente SMB	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Definir a validação do certificado

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	Autenticação IEEE802.1X.....	3-10
3.4	IPsec.....	3-11
3.5	Cliente WebDAV	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	Painel remoto	3-12

4 Informações adicionais de segurança

4.1	Recomendação de melhores práticas	4-13
4.2	Precauções para comunicar com sistemas antigos	4-14
	Definições antigas IPsec.....	4-14
4.3	Interfaces e serviços de rede disponíveis a partir do envio de fábrica	4-16
4.4	Sobre a validação de entradas	4-17



Sobre este manual

Este manual descreve informações e definições que permitem a utilização segura de dispositivos.

Ao ligar a máquina à rede, use-a num ambiente protegido por uma firewall. Também recomendamos que defina um endereço IP privado como endereço IP da máquina.

A definição de um endereço IP privado apenas permite o acesso à máquina por utilizadores numa rede local, como uma LAN interna, impedindo o acesso não autorizado a partir do exterior.

Se tiver de usar um endereço IP global, certifique-se de que instala a máquina numa firewall.

1 Definição da filtragem IP

A filtragem IP é uma função que restringe os dispositivos que podem aceder à máquina em função do endereço IP. Definir esta função corretamente permite-lhe restringir o acesso a dispositivos não autorizados.

A função de filtragem IP da máquina pode ser definida através de um dos dois métodos seguintes.

1.1 Filtragem IP

Especifique manualmente o intervalo de endereços IP com acesso permitido ou negado.

Localização da definição: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IP Address Filtering] (Utilitário - Administrador - Rede - Definições TCP/IP - Filtragem IP)



Sugestões

Defina os endereços IP permitidos ou negados de modo adequado ao seu ambiente.

1.2 Filtragem IP rápida

O intervalo de endereços IP com permissão de acesso é definido automaticamente com base no endereço IP e máscara de sub-rede definidos na máquina.

Localização da definição: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [Quick IP Filtering] (Utilitário - Administrador - Rede - Definições TCP/IP - Filtragem IP rápida)

Definições recomendadas: [Synchronize IP Address]/[Synchronize Subnet Mask] (Sincronizar endereço IP / Sincronizar máscara de subrede)*

* Selecione uma das opções para se adaptar ao seu ambiente.

2 Definir a comunicação encriptada

Recomendamos que utilize a seguinte comunicação encriptada para evitar a espionagem de dados, a manipulação de dados e o sequestro de sessões.

2.1 Encriptação TLS

Recomendamos que configure as definições seguintes para reduzir o risco de vulnerabilidades.

Localização da definição: [Utility] - [Administrator] - [Security] - [PKI Settings] - [Enable SSL Version] (Utilitário - Administrador - Segurança - Definições PKI - Ativar versão SSL)

Item de definição	Definição recomendada
[Mode using SSL/TLS] (Modo utilizando SSL/TLS)	[Admin. Mode and User Mode] (Modo admin. e Modo utilizador)
[SSL/TLS Version Setting] (Definição da versão SSL/TLS)	TLS1.2 TLS1.3 (incompatível com IEEE802.1X)
[Encryption Strength] (Força de encriptação)	AES-256

O certificado inicial é instalado na fábrica. Se precisar de um certificado diferente, registre um novo na localização seguinte.

Localização da definição: [Utility] - [Administrator] - [Security] - [PKI Settings] - [Device Certificate Setting] (Utilitário - Administrador - Segurança - Definições PKI - Definições do certificado do dispositivo)

Item de definição	Definição recomendada
[Encryption Key Type] (Tipo de chave de encriptação)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

A encriptação TLS é suportada para os protocolos e serviços seguintes. Para detalhes sobre as localizações da definição, consulte as secções seguintes.

- HTTP (Web Connection, Servidor WebDAV, IPP, OpenAPI, Painel remoto)
- DPWS
- POP
- SMTP (Iniciar TLS, SMTP sobre SSL)
- Autenticação IEEE802.1X (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- Tomada TCP

2.1.1 HTTP (Web Connection)

Se ativar [Enable SSL Version] (Ativar versão SSL), o modo de comunicação muda automaticamente para a comunicação encriptada TLS (HTTPS).

2.1.2 Servidor WebDAV

Localização da definição: [Utility] - [Administrator] - [Network] - [WebDAV Settings] - [WebDAV Server Settings] (Utilitário - Administrador - Rede - Definições WebDAV - Definições de servidor WebDAV)

Item de definição	Definição recomendada
[SSL Settings] (Definições de SSL)	[SSL Only] (Apenas SSL)

2.1.3 IPP

Localização da definição: [Utility] - [Administrator] - [Network] - [HTTP Server Settings] (Utilitário - Administrador - Rede - Definições de servidor HTTP)

Item de definição	Definição recomendada
[IPP-SSL Settings] (Definições IPP-SSL)	[SSL Only] (Apenas SSL)

2.1.4 OpenAPI

Localização da definição: [Utility] - [Administrator] - [Network] - [OpenAPI Setting] - [OpenAPI Setting] (Utilitário - Administrador - Rede - Definição de OpenAPI - Definição de OpenAPI)

Item de definição	Definição recomendada
[SSL/Port Settings] (Definições de SSL/porta)	[SSL Only] (Apenas SSL)

2.1.5 Painel remoto

Localização da definição: [Utility] - [Administrator] - [Network] - [Remote Panel Settings] - [Remote Panel Server Settings] (Utilitário - Administrador - Rede - Definições do painel remoto - Definições de servidor do painel remoto)

Item de definição	Definição recomendada
[Port No.(SSL)] (Número da porta (SSL))	[50443]



Sugestões

Se ativar [Enable SSL Version] (Ativar versão SSL), a comunicação muda automaticamente para o modo encriptado TLS. Especifique um número da porta.

2.1.6 DPWS

Localização da definição: [Utility] - [Administrator] - [Network] - [DPWS Settings] - [DPWS Common Settings] (Utilitário - Administrador - Rede - Definições DPWS - Definições comuns DPWS)

Item de definição	Definição recomendada
[SSL Settings] (Definições de SSL)	ON

2.1.7 POP

Localização da definição: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail RX (POP)] (Utilitário - Administrador - Rede - Definição de e-mail - Receção de e-mail (POP))

Item de definição	Definição recomendada
[Enable SSL] (Ativar SSL)	ON

2.1.8 SMTP

Localização da definição: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail TX (SMTP)] (Utilitário - Administrador - Rede - Definição de e-mail - Transmissão de e-mail (SMTP))

Item de definição	Definição recomendada
[SSL/TLS Settings] (Definições SSL/TLS)	[SMTP over SSL] (SMTP sobre SSL)

2.1.9 Autenticação IEEE802.1X

Localização da definição: [Utility] - [Administrator] - [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Setting] - [Supplicant Setting] (Utilitário - Administrador - Rede - Definição de autenticação IEEE802.1X - Definição de autenticação IEEE802.1X - Definição suplicante)

Item de definição	Definição recomendada
[EAP-Type] (Tipo EAP)	Selecione [EAP-TLS], [EAP-TTLS] ou [PEAP].

2.1.10 LDAP

Localização da definição: [Utility] - [Administrator] - [Network] - [LDAP Setting] - [Setting Up LDAP] (Utilitário - Administrador - Rede - Definições LDAP - Definir LDAP)

Item de definição	Definição recomendada
[Enable SSL] (Ativar SSL)	ON

2.1.11 Tomada TCP

Localização da definição: [Utility] - [Administrator] - [Network] - [TCP Socket Setting] (Utilitário - Administrador - Rede - Definição de tomada TCP)

Item de definição	Definição recomendada
[Use SSL/TLS] (Usar SSL/TLS)	ON

2.2 Outra encriptação

Recomendamos que configure as definições seguintes para reduzir o risco de vulnerabilidades. Para detalhes sobre as definições de cada função, consulte as secções seguintes.

Função	Definição recomendada
Servidor SMB	Encriptação SMB, Assinatura SMB
Cliente SMB	Autenticação Kerberos
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	ON

2.2.1 Servidor SMB

Utilizar a encriptação SMB e a assinatura SMB pode reduzir os seguintes riscos de segurança.

- Espionagem: uma terceira pessoa mal intencionada pode interceptar comunicações e roubar informações pessoais ou confidenciais.
- Manipulação de dados: existe o risco de os conteúdos das comunicações serem manipulados por um ataque "man-in-the-middle" (MITM).
- Spoofing: se a informação de autenticação for roubada, uma terceira pessoa pode fazer-se passar por um utilizador legítimo para obter acesso não autorizado.
- Fuga de informação: as comunicações não encriptadas podem ser facilmente interceptadas, especialmente em redes Wi-Fi públicas, aumentando o risco de fuga de informações pessoais e de cartões de crédito.

Encriptação SMB

Pré-requisitos

- Crie uma caixa de utilizador pública. Além disso, configure a definição para transferir automaticamente ficheiros da caixa de utilizador pública e guardá-los na pasta SMB.
- Especifique a palavra-passe para a caixa de utilizador.

Localização da definição: [Utility] - [Administrator] - [Box] - [User Box List] (Utilitário - Administrador - Caixa de utilizador - Lista da caixa de utilizador)

Item de definição	Definição recomendada
[SMB Communication Encryption] (Encriptação de comunicação SMB)	[Encrypt] (Encriptar)

Assinatura SMB

Localização da definição: [Utility] - [Administrator] - [Network] - [SMB Setting] - [SMB Server Settings] (Utilitário - Administrador - Rede - Definição de SMB - Definições servidor SMB)

Item de definição	Definição recomendada
[SMB security Signature Setting] (Definição de assinatura de segurança SMB)	[Required] (Obrigatória)

2.2.2 Cliente SMB

A autenticação Kerberos usa tecnologia de encriptação forte, reduzindo significativamente o risco de roubo de credenciais durante o processo de autenticação. Também garante a integridade dos dados, impedindo a manipulação de dados entre o remetente e o destinatário, bem como ataques de retransmissão NTLM.

Localização da definição: [Utility] - [Administrator] - [Network] - [SMB Setting] - [Client Setting] (Utilitário - Administrador - Rede - Definição de SMB - Definição de cliente)

Item de definição	Definição recomendada
[SMB Authentication Setting] (Definição de autenticação SMB)	[Kerberos]

2.2.3 SNMP

Defina a encriptação utilizando SNMPv3. Se a definição de autenticação também for adicionada, pode aumentar ainda mais a segurança. Os riscos de segurança são praticamente os mesmos que os de SMB.

Localização da definição: [Utility] - [Administrator] - [Network] - [SNMP Setting] (Utilitário - Administrador - Rede - Definições SNMP)

Item de definição	Definição recomendada
[SNMP Setting] (Definições SNMP)	[SNMP v3(IP)]
[Encryption Algorithm] (Algoritmo de encriptação)	[AES-128]
[Authentication Method] (Método de autenticação)	Selecione [SHA-256], [SHA-384] ou [SHA-512].

2.2.4 IPsec

Localização da definição: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IPsec] - [IPsec Setting] (Utilitário - Administrador - Rede - Definições TCP/IP - IPsec - Definição IPsec)

[IKEv2]

Item de definição	Definição recomendada
[Encryption Algorithm] (Algoritmo de encriptação)	[AES-CBC] ([256]/[192 e 256]/[All] (Tudo))
[Authentication Algorithm] (Algoritmo de autenticação)	[SHA-2] ([256]/[384]/[512]/[256 e 384]/[384 e 512]/[All] (Tudo)), [AES-XCBC]
[Diffie-Hellman Group] (Grupo Diffie-Hellman)	[Group 14], [Group 19] (Grupo 14, Grupo 19)

[SA]

Item de definição	Definição recomendada
[Encapsulation Mode] (Modo de encapsulamento)	[Tunnel], [Transport] (Túnel, Transporte)
[Security Protocol] (Protocolo de segurança)	[ESP]
[Key Exchange Method] (Método alteração tecla)	[IKEv2]
[Authentication Method] (Método de autenticação)	[Digital Signature] (Assinatura digital)
[ESP Encryption Algorithm] (Algoritmo de encriptação ESP)	[AES-GCM] ([256]/[192 e 256]/[All] (Tudo)), [AES-GCM-64] ([256]/[192 e 256]/[All] (Tudo)), [ENC_NULL_AES_GMAC] ([256]/[192 e 256]/[All] (Tudo))

Item de definição	Definição recomendada
[Perfect Forward Secrecy] (Sigilo de encaminhamento perfeito)	ON
[Diffie-Hellman Group(IKEv2)] - [Priority1-4] (Grupo Diffie-Hellman(IKEv2) - Prioridade1-4)	[Group 14], [Group 19] (Grupo 14, Grupo 19)

2.2.5 S/MIME

Se utilizar o S/MIME opcional ao enviar e-mails, pode encriptar o conteúdo do e-mail para evitar espionagem e verificar a identidade do remetente com uma assinatura eletrónica. Trata-se de uma medida eficaz contra as burlas por spoofing e phishing.

Localização da definição: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [S/MIME] (Utilitário - Administrador - Rede - Definição de e-mail - S/MIME)

Item de definição	Definição recomendada
[Digital Signature] (Assinatura digital)	[Always add signature] (Adicionar sempre a assinatura)
[Digital Signature Type] (Tipo de assinatura digital)	[SHA-256]
[E-Mail Text Encrypt. Method] (Método encriptação de texto e-mail)	[AES-256]

3 Definir a validação do certificado

Ao utilizar a comunicação encriptada TLS para reduzir o impacto dos ataques "man-in-the-middle", recomendamos que utilize a validação do certificado. Para itens de validação, recomendamos que ative, no mínimo, a data de expiração e a cadeia de certificados.

Se for feita uma tentativa de ligação a um ambiente antigo que não tenha uma função de validação de certificados, o risco de ataques "man-in-the-middle" aumenta. Recomendamos a sua utilização num ambiente de rede seguro.

A validação do certificado do lado da MFP é recomendada nas seguintes funções de cliente da MFP. Para detalhes sobre as localizações da definição, consulte as secções seguintes.

POP, SMTP (Iniciar TLS/SMTP sobre SSL), Autenticação IEEE802.1X (Tipo EAP: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, Painel remoto



Sugestões

A validação do certificado do lado do cliente ligado à MFP é recomendada nas seguintes funções de servidor da MFP.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / Painel remoto), Tomada TCP

3.1 POP

Localização da definição: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail RX (POP)] (Utilitário - Administrador - Rede - Definição de e-mail - Receção de e-mail (POP))

Item de definição	Definição recomendada
[Certificate Verification Level Settings] (Definições para nível de verificação de certificado)	[Expiration Date] (Data de expiração): ON [Chain] (Cadeia): ON

3.2 SMTP

Localização da definição: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail TX (SMTP)] (Utilitário - Administrador - Rede - Definição de e-mail - Transmissão de e-mail (SMTP))

Item de definição	Definição recomendada
[Certificate Verification Level Settings] (Definições para nível de verificação de certificado)	[Expiration Date] (Data de expiração): ON [Chain] (Cadeia): ON

3.3 Autenticação IEEE802.1X

Localização da definição: [Utility] - [Administrator] - [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Setting] - [Supplicant Setting] (Utilitário - Administrador - Rede - Definição de autenticação IEEE802.1X - Definição de autenticação IEEE802.1X - Definição suplicante)

Item de definição	Definição recomendada
[Certificate Verification Level Settings] (Definições para nível de verificação de certificado)	[Expiration Date] (Data de expiração): ON [Chain] (Cadeia): ON

3.4 IPsec

Localização da definição: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IPsec] - [Enable IPsec] (Utilitário - Administrador - Rede - Definições TCP/IP - IPsec - Ativar IPsec)

Item de definição	Definição recomendada
[Certificate Verification Level Settings] (Definições para nível de verificação de certificado)	[Expiration Date] (Data de expiração): [Confirm] (Confirmar) [Chain] (Cadeia): [Confirm] (Confirmar)



Sugestões

Em [IPsec Setting] (Definição IPsec), registre itens [IKE], [SA], [Peer] (Homólogo) e [Protocol Setting] (Definição de protocolo) antecipadamente.

3.5 Cliente WebDAV

Localização da definição: [Utility] - [Administrator] - [Network] - [WebDAV Settings] - [WebDAV Client Settings] (Utilitário - Administrador - Rede - Definições WebDAV - Definições de cliente WebDAV)

Item de definição	Definição recomendada
[Certificate Verification Level Settings] (Definições para nível de verificação de certificado)	[Expiration Date] (Data de expiração): ON [Chain] (Cadeia): ON

3.6 LDAP

Localização da definição: [Utility] - [Administrator] - [Network] - [LDAP Setting] - [Setting Up LDAP] (Utilitário - Administrador - Rede - Definições LDAP - Definir LDAP)

Item de definição	Definição recomendada
[Certificate Verification Level Settings] (Definições para nível de verificação de certificado)	[Expiration Date] (Data de expiração): ON [Chain] (Cadeia): ON

3.7 DPWS

Localização da definição: [Utility] - [Administrator] - [Network] - [DPWS Settings] - [DPWS Common Settings] (Utilitário - Administrador - Rede - Definições DPWS - Definições comuns DPWS)

Item de definição	Definição recomendada
[Certificate Verification Level Settings] (Definições para nível de verificação de certificado)	[Expiration Date] (Data de expiração): ON [Chain] (Cadeia): ON

3.8 OpenAPI

Localização da definição: [Utility] - [Administrator] - [Network] - [OpenAPI Setting] - [OpenAPI Setting] (Utilitário - Administrador - Rede - Definição de OpenAPI - Definição de OpenAPI)

Item de definição	Definição recomendada
[Certificate Verification Level Settings] (Definições para nível de verificação de certificado)	[Expiration Date] (Data de expiração): ON [Chain] (Cadeia): ON

3.9 Painel remoto

Localização da definição: [Utility] - [Administrator] - [Network] - [Remote Panel Settings] - [Remote Panel Client Settings] (Utilitário - Administrador - Rede - Definições do painel remoto - Definições de cliente do painel remoto)

Item de definição	Definição recomendada
[Certificate Verification Level Settings] (Definições para nível de verificação de certificado)	[Expiration Date] (Data de expiração): ON [Chain] (Cadeia): ON

4 Informações adicionais de segurança

4.1 Recomendação de melhores práticas

Recomendamos que os algoritmos de encriptação a utilizar cumpram as definições de boas práticas recomendadas nas diretrizes EUCC sobre criptografia e mecanismos criptográficos aprovados pelo SOGIS.

Abaixo, encontra-se uma lista dos algoritmos de encriptação e comprimentos de chave recomendados pelas diretrizes EUCC sobre criptografia e mecanismos criptográficos aprovados pelo SOGIS.

Item	Definição recomendada
Algoritmos de encriptação	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Comprimento da chave de encriptação	RSA: 2048 bits ou mais ECC: 256 bits ou mais AES: 256 bits



Sugestões

Para mais informações, consulte a versão mais recente das diretrizes EUCC sobre criptografia e mecanismos criptográficos aprovados pelo SOGIS.

4.2 Precauções para comunicar com sistemas antigos

Presume-se que sejam utilizados os seguintes protocolos e versões para a comunicação com os sistemas antigos.

A utilização de definições antigas aumenta os riscos de segurança; por isso, utilize-as num ambiente de rede seguro.

Item	Definições antigas
Protocolo	SLP FTP SMB (versão 3.0 ou anterior, NTLMv1/v2) SNMPv1/v2 Autenticação IEEE802.1X (Tipo EAP: consoante o servidor/OFF) DPWS Tomada TCP
Algoritmos de encriptação	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Comprimento da chave de encriptação	RSA: 1024 bits ou menos ECC: 160 bits ou menos AES: 128 bits ou menos DES: 56 bits 3DES: 112 bits

Definições antigas IPsec

[IKEv1]

Item de definição	Definições antigas
[Encryption Algorithm] (Algoritmo de encriptação)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 e 192])
[Authentication Algorithm] (Algoritmo de autenticação)	Não utilizado
[Diffie-Hellman Group] (Grupo Diffie-Hellman)	[Group 1], [Group 2], [Group 5] (Grupo 1, Grupo 2, Grupo 5)

[IKEv2]

Item de definição	Definições antigas
[Encryption Algorithm] (Algoritmo de encriptação)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 e 192])
[Authentication Algorithm] (Algoritmo de autenticação)	Não utilizado
[Diffie-Hellman Group] (Grupo Diffie-Hellman)	[Group 1], [Group 2], [Group 5] (Grupo 1, Grupo 2, Grupo 5)

[SA]

Item de definição	Definições antigas
[Key Exchange Method] (Método alteração tecla)	[IKEv1]
[Authentication Method] (Método de autenticação)	[Digital Signature] (Assinatura digital)
[ESP Encryption Algorithm] (Algoritmo de encriptação ESP)	[3DES-CBC] ([128]/[192]/[128 e 192]) [AES-CTR] ([128]/[192]/[128 e 192]) [AES-GCM] ([128]/[192]/[128 e 192]) [AES-GCM-64] ([128]/[192]/[128 e 192]) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 e 192])
[Perfect Forward Secrecy] (Sigilo de encaminhamento perfeito)	ON
[Diffie-Hellman Group(IKEv1)] (Grupo Diffie-Hellman(IKEv1))	[Group 1], [Group 2], [Group 5] (Grupo 1, Grupo 2, Grupo 5)

4.3 Interfaces e serviços de rede disponíveis a partir do envio de fábrica

Tipo de serviço	Protocolo	Número da porta
DHCP	UDP	68
Servidor HTTP	TCP	80
Serviço de nome NETBIOS	UDP	137
Serviço de datagrama NETBIOS	UDP	138
SNMP	UDP	161
Servidor HTTP sobre SSL / IPP sobre SSL	TCP	443
Impressão LPD	TCP	515
Cliente DHCPv6	UDP	546
Impressão IPP	TCP	631
MFPIF	UDP	1900
Serviço Web	UDP	3702
LLMNR	UDP	5355
HTTP (ferramenta IWS)	TCP	8091
Impressão RAW	TCP	9100
Impressão RAW	TCP	9112
Impressão RAW	TCP	9113
Impressão RAW	TCP	9114
Impressão RAW	TCP	9115
Impressão RAW	TCP	9116
OpenAPI	TCP	50001

4.4 Sobre a validação de entradas

Para conhecer o número de caracteres a introduzir para as definições de rede, etc., consulte cada um dos itens de definição no Manual de Operação.

Dependendo da codificação do idioma, a entrada máxima permitida (dados guardados na MFP) para itens que suportam caracteres multibyte pode ser o triplo do número de caracteres.

Recomandări pentru dispozitivele de rețea securizate

Cuprins

1 Setarea filtrării adresei IP

1.1	Filtrarea adresei IP.....	1-3
1.2	Filtrare rapidă IP.....	1-3

2 Configurarea comunicației criptate

2.1	Criptare TLS.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	Autentificare IEEE802.1X	2-6
2.1.10	LDAP	2-6
2.1.11	Mufă TCP	2-6
2.2	Alt mod de criptare	2-7
2.2.1	Server SMB.....	2-7
	Criptare folder SMB	2-7
	Semnătură SMB.....	2-7
2.2.2	Client SMB	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Configurarea validării certificatului

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	Autentificare IEEE802.1X.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	RemotePanel	3-12

4 Informații de securitate suplimentare

4.1	Recomandări de bune practici.....	4-13
4.2	Măsuri de precauție pentru comunicația cu sistemele vechi	4-14
	Setări moștenite IPsec	4-14
4.3	Interfețe de rețea și servicii disponibile de la livrarea din fabrică.....	4-16
4.4	Despre validarea introducerilor	4-17



Despre acest manual

Acest manual descrie informații și setări care permit utilizarea în siguranță a dispozitivelor.

Atunci când conectați unitatea principală la rețea, utilizați-o într-un mediu protejat cu un paravan de protecție. De asemenea, vă recomandăm să setați o adresă IP privată pentru adresa IP a unității principale.

Setarea unei adrese IP private permite doar utilizatorilor dintr-o rețea locală, cum ar fi o rețea LAN internă, să acceseze unitatea principală, prevenind accesul neautorizat din exterior.

Dacă trebuie să utilizați o adresă IP globală, asigurați-vă că unitatea principală este instalată într-un paravan de protecție.

1 Setarea filtrării adresei IP

Filtrarea adresei IP este o funcție care restricționează dispozitivele care pot accesa unitatea principală prin intermediul adresei IP. Setarea corectă a acestei funcții vă permite să restricționați accesul dispozitivelor neautorizate.

Funcția de filtrare a adreselor IP de pe această unitate principală poate fi setată prin una dintre următoarele două metode.

1.1 Filtrarea adresei IP

Specificați manual intervalul de adrese IP căruia doriți să-i acordați sau să-i refuzați accesul.

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [TCP/IP Setting] (Setare TCP/IP) - [IP Address Filtering] (Filtrare adresă IP)



Recomandări

Setați adresele IP permise sau refuzate în funcție de mediul dumneavoastră.

1.2 Filtrare rapidă IP

Intervalul de adrese IP cărora le este permis accesul este setat automat pe baza adresei IP și a măștii de subrețea setate pe această unitate principală.

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [TCP/IP Setting] (Setare TCP/IP) - [Quick IP Filtering] (Filtrare rapidă IP)

Setări recomandate: [Synchronize IP Address] (Sincronizare adresă IP)/[Synchronize Subnet Mask] (Sincronizare mască de subrețea) *

* Selectați una dintre acestea, în funcție de mediul dumneavoastră.

2 Configurarea comunicației criptate

Vă recomandăm să utilizați următoarele metode de comunicație criptată, pentru a preveni interceptarea datelor, modificarea datelor și deturnarea sesiunii.

2.1 Criptare TLS

Pentru a reduce riscul apariției vulnerabilităților, vă recomandăm să configurați următoarele setări.

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Security] (Securitate) - [PKI Settings] (Setări PKI) - [Enable SSL Version] (Activare versiune SSL)

Element de setare	Setare recomandată
[Mode using SSL/TLS] (Mod utilizare SSL/TLS)	[Admin. Mode and User Mode] (Mod administrator și Mod utilizator)
[SSL/TLS Version Setting] (Setare versiune SSL/TLS)	TLS1.2 TLS1.3 (IEEE802.1X incompatibil)
[Encryption Strength] (Putere de criptare)	AES-256

Certificatul inițial este instalat din fabrică. Dacă aveți nevoie de un alt certificat, înregistrați unul nou în următoarea locație.

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Security] (Securitate) - [PKI Settings] (Setări PKI) - [Device Certificate Setting] (Setare certificat dispozitiv)

Element de setare	Setare recomandată
[Encryption Key Type] (Tip cod de criptare)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Criptarea TLS este acceptată pentru următoarele protocoale și servicii. Pentru detalii privind locațiile setărilor, consultați secțiunile următoare.

- HTTP (Web Connection, WebDAVServer, IPP, Open API, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP peste SSL)
- Autentificare IEEE802.1X (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- Mufă TCP

2.1.1 HTTP (Web Connection)

Dacă activați [Enable SSL Version] (Activare versiune SSL), modul de comunicație comută automat la comunicația criptată TLS (HTTPS).

2.1.2 WebDAVServer

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [WebDAV Settings] (Setări WebDAV) - [WebDAV Server Settings] (Setări server WebDAV)

Element de setare	Setare recomandată
[SSL Settings] (Setări SSL)	[SSL Only] (Numai SSL)

2.1.3 IPP

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [HTTP Server Settings] (Setări server HTTP)

Element de setare	Setare recomandată
[IPP-SSL Settings] (Setări IPP-SSL)	[SSL Only] (Numai SSL)

2.1.4 OpenAPI

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [OpenAPI Setting] (Setare Open API) - [OpenAPI Setting] (Setare Open API)

Element de setare	Setare recomandată
[SSL/Port Settings] (Setări SSL/Port)	[SSL Only] (Numai SSL)

2.1.5 RemotePanel

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [Remote Panel Settings] (Setare panou de la distanță) - [Remote Panel Server Settings] (Setări server panou de la distanță)

Element de setare	Setare recomandată
[Port No.(SSL)] (Nr. port (SSL))	[50443]



Recomandări

Dacă activați [Enable SSL Version] (Activare versiune SSL), modul de comunicație comută automat la modul de criptare TLS. Specificați un număr de port.

2.1.6 DPWS

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [DPWS Settings] (Setări DPWS) - [DPWS Common Settings] (Setări generale DPWS)

Element de setare	Setare recomandată
[SSL Settings] (Setări SSL)	ON (PORNIT)

2.1.7 POP

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [E-mail Setting] (Setare e-mail) - [E-mail RX (POP)] (Recepție e-mail (POP))

Element de setare	Setare recomandată
[Enable SSL] (Activare SSL)	ON (PORNIT)

2.1.8 SMTP

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [E-mail Setting] (Setare e-mail) - [E-mail TX (SMTP)] (Transmisie pe e-mail (SMTP))

Element de setare	Setare recomandată
[SSL/TLS Settings] (Setări SSL/TLS)	[SMTP over SSL] (SMTP peste SSL)

2.1.9 Autentificare IEEE802.1X

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [IEEE802.1X Authentication Setting] (Setare autentificare IEEE802.1X) - [IEEE802.1X Authentication Setting] (Setare autentificare IEEE802.1X) - [Supplicant Setting] (Setare solicitare)

Element de setare	Setare recomandată
[EAP-Type] (Tip EAP)	Selectați [EAP-TLS], [EAP-TTLS], sau [PEAP].

2.1.10 LDAP

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [LDAP Setting] (Setare LDAP) - [Setting Up LDAP] (Setare LDAP)

Element de setare	Setare recomandată
[Enable SSL] (Activare SSL)	ON (PORNIT)

2.1.11 Mufă TCP

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [TCP Socket Setting] (Setare mufă TCP)

Element de setare	Setare recomandată
[Use SSL/TLS] (Utilizare SSL/TLS)	ON (PORNIT)

2.2 Alt mod de criptare

Pentru a reduce riscul apariției vulnerabilităților, vă recomandăm să configurați următoarele setări. Pentru detalii despre setările pentru fiecare funcție, consultați secțiunile următoare.

Funcție	Setare recomandată
Server SMB	Criptare folder SMB, Semnătură SMB
Client SMB	Autentificare Kerberos
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	ON (PORNIT)

2.2.1 Server SMB

Utilizarea criptării SMB și a semnăturii SMB poate reduce următoarele riscuri de securitate.

- **Interceptare:** Un terț rău intenționat poate intercepta comunicațiile și fura informații personale sau confidențiale.
- **Modificarea datelor:** Există riscul ca informațiile comunicate să fie modificate de un atac de tip Man-In-The-Middle (MITM).
- **Falsificare:** Dacă informațiile de autentificare sunt furate, un terț se poate preface că este un utilizator legitim pentru a obține acces neautorizat.
- **Scurgere de informații:** Comunicațiile necriptate pot fi ușor interceptate, în special în rețelele Wi-Fi publice, crescând riscul scurgerii de informații personale și a informațiilor despre cardurile de credit.

Criptare folder SMB

Cerințe preliminare

- Crearea unei casete de utilizator public. De asemenea, configurați setarea pentru transferul automat al fișierelor din Public User Box (Casetă de utilizator public) și salvarea acestora în folderul SMB.
- Specificați parola pentru caseta de utilizator.

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Box] (Casetă de utilizator) - [User Box List] (Listă casete de utilizator)

Element de setare	Setare recomandată
[SMB Communication Encryption] (Criptare comunicație SMB)	[Encrypt] (Criptare)

Semnătură SMB

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [SMB Setting] (Setare SMB) - [SMB Server Settings] (Setări server SMB)

Element de setare	Setare recomandată
[SMB security Signature Setting] (Setare semnătură de securitate SMB)	[Required] (Necesar)

2.2.2 Client SMB

Autentificarea Kerberos utilizează o tehnologie puternică de criptare, reducând semnificativ riscul furtului de acreditări în timpul procesului de autentificare. De asemenea, asigură integritatea datelor, prevenind modificarea datelor între expeditor și destinatar, precum și atacurile de tip retransmisie NTLM.

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [SMB Setting] (Setare SMB) - [Client Setting] (Setare client)

Element de setare	Setare recomandată
[SMB Authentication Setting] (Setare autentificare SMB)	[Kerberos]

2.2.3 SNMP

Configurați criptarea folosind SNMPv3. Dacă adăugați și setarea de autentificare, puteți crește și mai mult siguranța. Riscurile de securitate sunt aproximativ aceleași ca în cazul SMB.

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [SNMP Setting] (Setare SNMP)

Element de setare	Setare recomandată
[SNMP Setting] (Setare SNMP)	[SNMP v3(IP)]
[Encryption Algorithm] (Algoritm de criptare)	[AES-128]
[Authentication Method] (Metodă de autentificare)	Selectați [SHA-256], [SHA-384], sau [SHA-512].

2.2.4 IPsec

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [TCP/IP Setting] (Setare TCP/IP) - [IPsec] - [IPsec Setting] (Setare IPsec)

[IKEv2]

Element de setare	Setare recomandată
[Encryption Algorithm] (Algoritm de criptare)	[AES-CBC] ([256]/[192 and 256] (192 și 256)/[All] (Toate))
[Authentication Algorithm] (Algoritm autentificare)	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 și 384)/[384 and 512] (384 și 512)/[All] (Toate)), [AES-XCBC]
[Diffie-Hellman Group] (Grup Diffie-Hellman)	[Group 14] (Grup 14), [Group 19] (Grup 19)

[SA]

Element de setare	Setare recomandată
[Encapsulation Mode] (Mod de încapsulare)	[Tunnel] (Tunelare), [Transport] (Unitate de transport)
[Security Protocol] (Protocol de securitate)	[ESP]
[Key Exchange Method] (Metodă schimbare cheie)	[IKEv2]
[Authentication Method] (Metodă de autentificare)	[Digital Signature] (Semnătură digitală)
[ESP Encryption Algorithm] (Algoritm de criptare ESP)	[AES-GCM] ([256]/[192 and 256] (192 și 256)/[All] (Toate)), [AES-GCM-64] ([256]/[192 and 256] (192 și 256)/[All] (Toate)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 și 256)/[All] (Toate))

Element de setare	Setare recomandată
[Perfect Forward Secrecy] (Confidențialitate totală la expediere)	ON (PORNIT)
[Diffie-Hellman Group(IKEv2)] (Grup Diffie-Hellman(IKEv2)) - [Priority1-4] (Prioritate1-4)	[Group 14] (Grup 14), [Group 19] (Grup 19)

2.2.5 S/MIME

Dacă utilizați opțiunea S/MIME atunci când trimiteți e-mailuri, puteți cripta conținutul e-mail-ului pentru a preveni interceptarea și a verifica identitatea expeditorului printr-o semnătură electronică. Aceasta este o măsură eficientă împotriva atacurilor de tip spoofing și phishing.

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [E-mail Setting] (Setare e-mail) - [S/MIME]

Element de setare	Setare recomandată
[Digital Signature] (Semnătură digitală)	[Always add signature] (Adăugare semnătură de fiecare dată)
[Digital Signature Type] (Tip de semnătură digitală)	[SHA-256]
[E-Mail Text Encrypt. Method] (Metodă de criptare text e-mail)	[AES-256]

3 Configurarea validării certificatului

Atunci când utilizați comunicația criptată TLS pentru a reduce impactul atacurilor de tip man-in-the-middle, vă recomandăm să utilizați validarea certificatelor. Pentru elementele de validare, vă recomandăm să activați cel puțin data de expirare a certificatului și lanțul.

În cazul în care se încearcă conectarea la un mediu vechi care nu are o funcție de validare a certificatelor, riscul unor atacuri de tip man-in-the-middle crește. Vă recomandăm să îl utilizați într-un mediu de rețea securizat.

Validarea certificatului pe partea MFP este recomandată pentru următoarele funcții client MFP. Pentru detalii privind locațiile setărilor, consultați secțiunile următoare.

POP, SMTP (Start TLS/SMTP pe SSL), autentificare IEEE802.1X (TIP-EAP: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel



Recomandări

Validarea certificatului pe partea clientului conectată la MFP este recomandată pentru următoarele funcții server MFP.

HTTP (Web Connection/WebDAV/IPP/DPWS/OpenAPI/RemotePanel), TCP Socket (Mufă TCP)

3.1 POP

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [E-mail Setting] (Setare e-mail) - [E-mail RX (POP)] (Recepție e-mail (POP))

Element de setare	Setare recomandată
[Certificate Verification Level Settings] (Setări pentru nivel verificare certificat)	[Expiration Date] (Dată de expirare): ON (PORNIT) [Chain] (Lanț): ON (PORNIT)

3.2 SMTP

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [E-mail Setting] (Setare e-mail) - [E-mail TX (SMTP)] (Transmisie pe e-mail (SMTP))

Element de setare	Setare recomandată
[Certificate Verification Level Settings] (Setări pentru nivel verificare certificat)	[Expiration Date] (Dată de expirare): ON (PORNIT) [Chain] (Lanț): ON (PORNIT)

3.3 Autentificare IEEE802.1X

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [IEEE802.1X Authentication Setting] (Setare autentificare IEEE802.1X) - [IEEE802.1X Authentication Setting] (Setare autentificare IEEE802.1X) - [Supplicant Setting] (Setare solicitare)

Element de setare	Setare recomandată
[Certificate Verification Level Settings] (Setări pentru nivel verificare certificat)	[Expiration Date] (Dată de expirare): ON (PORNIT) [Chain] (Lanț): ON (PORNIT)

3.4 IPsec

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [TCP/IP Setting] (Setare TCP/IP) - [IPsec] - [Enable IPsec] (Activare IPsec)

Element de setare	Setare recomandată
[Certificate Verification Level Settings] (Setări pentru nivel verificare certificat)	[Expiration Date] (Dată de expirare): [Confirm] (Confirmare) [Chain] (Lanț): [Confirm] (Confirmare)



Recomandări

În [Setare IPsec], înregistrați elementele [IKE], [SA], [Peer] (Pereche) și [Protocol Setting] (Setare protocol) în avans.

3.5 WebDAVClient

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [WebDAV Settings] (Setări WebDAV) - [WebDAV Client Settings] (Setări client WebDAV)

Element de setare	Setare recomandată
[Certificate Verification Level Settings] (Setări pentru nivel verificare certificat)	[Expiration Date] (Dată de expirare): ON (PORNIT) [Chain] (Lanț): ON (PORNIT)

3.6 LDAP

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [LDAP Setting] (Setare LDAP) - [Setting Up LDAP] (Setare LDAP)

Element de setare	Setare recomandată
[Certificate Verification Level Settings] (Setări pentru nivel verificare certificat)	[Expiration Date] (Dată de expirare): ON (PORNIT) [Chain] (Lanț): ON (PORNIT)

3.7 DPWS

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [DPWS Settings] (Setări DPWS) - [DPWS Common Settings] (Setări generale DPWS)

Element de setare	Setare recomandată
[Certificate Verification Level Settings] (Setări pentru nivel verificare certificat)	[Expiration Date] (Dată de expirare): ON (PORNIT) [Chain] (Lanț): ON (PORNIT)

3.8 OpenAPI

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [OpenAPI Setting] (Setare Open API) - [OpenAPI Setting] (Setare Open API)

Element de setare	Setare recomandată
[Certificate Verification Level Settings] (Setări pentru nivel verificare certificat)	[Expiration Date] (Dată de expirare): ON (PORNIT) [Chain] (Lanț): ON (PORNIT)

3.9 RemotePanel

Configurarea locației: [Utility] (Utilitar) - [Administrator] - [Network] (Rețea) - [Remote Panel Settings] (Setare panou de la distanță) - [Remote Panel Client Settings] (Setări client panou de la distanță)

Element de setare	Setare recomandată
[Certificate Verification Level Settings] (Setări pentru nivel verificare certificat)	[Expiration Date] (Dată de expirare): ON (PORNIT) [Chain] (Lanț): ON (PORNIT)

4 Informații de securitate suplimentare

4.1 Recomandări de bune practici

Vă recomandăm ca algoritmi de criptare folosiți să respecte setările de bune practici recomandate în instrucțiunile EUCC privind criptografia și mecanismele criptografice convenite în cadrul SOGIS.

Mai jos este o listă a algoritmilor de criptare și a lungimilor de cheie recomandate de Instrucțiunile EUCC privind criptografia și mecanismele criptografice convenite în cadrul SOGIS.

Element	Setare recomandată
Algoritmi de criptare	AES (Advanced Encryption Standard - Standard avansat de criptare) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2 - Algoritm hash securizat 2) ECC (Elliptic Curve Cryptography - Criptografie cu curbe eliptice) HMAC (Hash-based Message Authentication Code - Cod de autentificare a mesajelor bazat pe hash)
Lungime cod de criptare	RSA: 2048 biți sau mai mult ECC: 256 biți sau mai mult AES: 256 biți



Recomandări

Pentru detalii, consultați cele mai recente Instrucțiuni EUCC cu privire la criptografie și mecanismele criptografice convenite în cadrul SOGIS.

4.2 Măsuri de precauție pentru comunicația cu sistemele vechi

Se presupune că următoarele protocoale și versiuni sunt utilizate pentru comunicația cu sistemele vechi.

Utilizarea setărilor moștenite crește riscurile de securitate, așadar vă rugăm să le utilizați într-un mediu de rețea securizat.

Element	Setări moștenite
Protocol	SLP FTP SMB (3.0 sau o versiune anterioară, NTLMv1/v2) SNMPv1/v2 Autentificare IEEE802.1X (TIP-EAP: În funcție de server/OPRIT) DPWS TCPSocket (Mufă TCP)
Algoritmi de criptare	SHA-1 (Secure Hash Algorithm 1 - Algoritm hash securizat 1) DES (Data Encryption Standard - Standard de criptare a datelor) 3DES (Triple Data Encryption Standard - Standard de criptare triplă a datelor) RC2-40 (D51Rivest Cipher - Cifru D51Rivest) RC2-64 (D51Rivest Cipher - Cifru D51Rivest) RC2-128 (D51Rivest Cipher - Cifru D51Rivest)
Lungime cod de criptare	RSA: 1024 biți sau mai puțin ECC: 160 biți sau mai puțin AES: 128 biți sau mai puțin DES: 56 biți 3DES: 112 biți

Setări moștenite IPsec

[IKEv1]

Element de setare	Setări moștenite
[Encryption Algorithm] (Algoritm de criptare)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 și 192))
[Authentication Algorithm] (Algoritm autentificare)	Nu este utilizat
[Diffie-Hellman Group] (Grup Diffie-Hellman)	[Group 1] (Grup 1), [Group 2] (Grup 2), [Group 5] (Grup 5)

[IKEv2]

Element de setare	Setări moștenite
[Encryption Algorithm] (Algoritm de criptare)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 și 192))
[Authentication Algorithm] (Algoritm autentificare)	Nu este utilizat
[Diffie-Hellman Group] (Grup Diffie-Hellman)	[Group 1] (Grup 1), [Group 2] (Grup 2), [Group 5] (Grup 5)

[SA]

Element de setare	Setări moștenite
[Key Exchange Method] (Metodă schimbare cheie)	[IKEv1]
[Authentication Method] (Metodă de autentificare)	[Digital Signature] (Semnătură digitală)

Element de setare	Setări moștenite
[ESP Encryption Algorithm] (Algoritm de criptare ESP)	[3DES-CBC] ([128]/[192]/[128 and 192] (128 și 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 și 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 și 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 și 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 și 192))
[Perfect Forward Secrecy] (Confidențialitate totală la expediere)	ON (PORNIT)
[Diffie-Hellman Group(IKEv1)] (Grup Diffie-Hellman(IKEv1))	[Group 1] (Grup 1), [Group 2] (Grup 2), [Group 5] (Grup 5)

4.3 Interfețe de rețea și servicii disponibile de la livrarea din fabrică

Tip serviciu	Protocol	Număr port
DHCP	UDP	68
Server HTTP	TCP	80
Serviciu nume NetBIOS	UDP	137
Serviciu datagrame NETBIOS	UDP	138
SNMP	UDP	161
Server HTTP pe SSL/IPP pe SSL	TCP	443
Imprimare LPD	TCP	515
Client DHCPv6	UDP	546
Imprimare IPP	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (instrument-IWS)	TCP	8091
Imprimare RAW	TCP	9100
Imprimare RAW	TCP	9112
Imprimare RAW	TCP	9113
Imprimare RAW	TCP	9114
Imprimare RAW	TCP	9115
Imprimare RAW	TCP	9116
OpenAPI	TCP	50001

4.4 Despre validarea introducerilor

Pentru numărul de caractere care trebuie introduse pentru setările de rețea etc., consultați fiecare element de setare din manualul de operare.

În funcție de codificarea limbii, numărul maxim admis de date de intrare (date salvate în MFP) pentru elementele care acceptă caractere cu biți multipli poate fi de trei ori mai mare decât numărul de caractere.

Рекомендации для безопасных сетевых устройств

Оглавление

1	Настройка фильтрации IP-адресов	
1.1	Фильтрация IP-адресов.....	1-3
1.2	Быстрая фильтрация IP.....	1-3
2	Настройка обмена данными с шифрованием	
2.1	Шифрование с помощью TLS	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	Сокет TCP	2-6
2.2	Другое шифрование	2-7
2.2.1	SMBServer.....	2-7
	Шифрование SMB.....	2-7
	Подпись SMB.....	2-7
2.2.2	SMBClient.....	2-8
2.2.3	SNMP	2-8
2.2.4	IPSEC.....	2-8
2.2.5	S/MIME	2-9
3	Настройка проверки подлинности сертификата	
3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPSEC	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-12
3.9	RemotePanel	3-12
4	Дополнительная информация по безопасности	
4.1	Рекомендации на основе передовой практики	4-13
4.2	Меры предосторожности при обмене данными с устаревшими системами	4-14
	Устаревшие настройки IPsec	4-14
4.3	Сетевые интерфейсы и сервисы, доступные при поставке с завода	4-16
4.4	Проверка вводимых данных.....	4-17



О руководстве

Настоящее руководство содержит информацию и настройки, обеспечивающие безопасную эксплуатацию устройств.

При подключении аппарата к сети используйте его в среде, защищенной брандмауэром. Кроме того, мы рекомендуем вам задать частный IP-адрес в качестве IP-адреса аппарата.

При использовании частного IP-адреса доступ к аппарату имеют только пользователи локальной сети, например внутренней ЛВС, что позволит предотвратить несанкционированный доступ извне.

При необходимости использования глобального IP-адреса обязательно защитите аппарат брандмауэром.

1 Настройка фильтрации IP-адресов

Функция фильтрации IP-адресов позволяет ограничить круг устройств, имеющих доступ к аппарату, на основе их IP-адресов. Правильно настроив эту функцию, можно ограничить доступ с несанкционированных устройств.

Настройка функции фильтрации IP-адресов на аппарате осуществляется следующими двумя способами.

1.1 Фильтрация IP-адресов

Задайте диапазон IP-адресов, которым нужно разрешить или запретить доступ к аппарату, в ручном режиме.

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IP Address Filtering] (Утилиты - Администратор - Сеть - Настройка TCP/IP - Фильтрация IP-адресов)



Советы

Задайте IP-адреса, которым нужно разрешать или запрещать доступ, в соответствии с особенностями среды.

1.2 Быстрая фильтрация IP

Диапазон IP-адресов, которым разрешен доступ, задается автоматически на основе IP-адреса и маски подсети, настроенных на аппарате.

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [Quick IP Filtering] (Утилиты - Администратор - Сеть - Настройка TCP/IP - Быстрая фильтрация IP)

Рекомендуемые настройки: [Synchronize IP Address]/[Synchronize Subnet Mask] * (Синхронизировать IP-адрес/Синхронизировать маску подсети)

* Выберите одну из настроек в зависимости от особенностей среды.

2 Настройка обмена данными с шифрованием

Мы рекомендуем использовать функцию обмена данными с шифрованием для предотвращения прослушивания и фальсификации данных и перехвата сеансов.

2.1 Шифрование с помощью TLS

Мы рекомендуем задать следующие настройки для снижения риска возникновения уязвимостей.

Местонахождение настройки: [Utility] - [Administrator] - [Security] - [PKI Settings] - [Enable SSL Version] (Утилиты - Администратор - Безопасность - Настройки PKI - Активировать версию SSL)

Параметр настройки	Рекомендуемая настройка
[Mode using SSL/TLS] (Режим использования SSL/TLS)	[Admin. Mode and User Mode] (Режим админ.и режим польз.)
[SSL/TLS Version Setting] (Настройка версии SSL/TLS)	TLS1.2 TLS1.3 (несовместимость с IEEE802.1X)
[Encryption Strength] (Степень шифрования)	AES-256

Начальный сертификат установлен на заводе. При необходимости использования другого сертификата, зарегистрируйте новый сертификат в следующем месте.

Местонахождение настройки: [Utility] - [Administrator] - [Security] - [PKI Settings] - [Device Certificate Setting] (Утилиты - Администратор - Безопасность - Настройки PKI - Настройка сертификата устройства)

Параметр настройки	Рекомендуемая настройка
[Encryption Key Type] (Тип ключа шифрования)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Шифрование с помощью TLS поддерживается для следующих протоколов и сервисов. Подробнее о местонахождении настроек см. в следующих разделах.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP через SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- Сокет TCP

2.1.1 HTTP (Web Connection)

При включении опции [Enable SSL Version] (Активировать версию SSL) режим обмена данными автоматически переключается на обмен данными с шифрованием по TLS (HTTPS).

2.1.2 WebDAVServer

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [WebDAV Settings] - [WebDAV Server Settings] (Утилиты - Администратор - Сеть - Настройки WebDAV - Настройки сервера WebDAV)

Параметр настройки	Рекомендуемая настройка
[SSL Settings] (Настройки SSL)	[SSL Only] (Только SSL)

2.1.3 IPP

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [HTTP Server Settings] (Утилиты - Администратор - Сеть - Настройки сервера HTTP)

Параметр настройки	Рекомендуемая настройка
[IPP-SSL Settings] (Настройки IPP-SSL)	[SSL Only] (Только SSL)

2.1.4 OpenAPI

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [OpenAPI Setting] - [OpenAPI Setting] (Утилиты - Администратор - Сеть - Настройка OpenAPI - Настройка OpenAPI)

Параметр настройки	Рекомендуемая настройка
[SSL/Port Settings] (Настройки SSL/порта)	[SSL Only] (Только SSL)

2.1.5 RemotePanel

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [Remote Panel Settings] - [Remote Panel Server Settings] (Утилиты - Администратор - Сеть - Настройки удаленной панели - Настройки сервера удаленной панели)

Параметр настройки	Рекомендуемая настройка
[Port No.(SSL)] (Номер порта SSL)	[50443]



Советы

При включении опции [Enable SSL Version] (Активировать версию SSL) обмен данными автоматически переключается на режим обмен данными с шифрованием по TLS (HTTPS). Задайте номер порта.

2.1.6 DPWS

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [DPWS Settings] - [DPWS Common Settings] (Утилиты - Администратор - Сеть - Настройки DPWS - Общие настройки DPWS)

Параметр настройки	Рекомендуемая настройка
[SSL Settings] (Настройки SSL)	ON (ВКЛ)

2.1.7 POP

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail RX (POP)] (Утилиты - Администратор - Сеть - Настройки E-mail - Прием E-mail (POP))

Параметр настройки	Рекомендуемая настройка
[Enable SSL] (Включение SSL)	ON (ВКЛ)

2.1.8 SMTP

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail TX (SMTP)] (Утилиты - Администратор - Сеть - Настройки E-mail - Передача E-mail (SMTP))

Параметр настройки	Рекомендуемая настройка
[SSL/TLS Settings] (Настройки SSL/TLS)	[SMTP over SSL] (SMTP через SSL)

2.1.9 IEEE802.1X Auth

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Setting] - [Supplicant Setting] (Утилиты - Администратор - Сеть - Настройки идентификации IEEE802.1X - Настройки идентификации IEEE802.1X - Настройка сапликанта)

Параметр настройки	Рекомендуемая настройка
[EAP-Type] (Тип EAP)	Выберите [EAP-TLS], [EAP-TTLS] или [PEAP].

2.1.10 LDAP

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [LDAP Setting] - [Setting Up LDAP] (Утилиты - Администратор - Сеть - Настройка LDAP - Настройка LDAP)

Параметр настройки	Рекомендуемая настройка
[Enable SSL] (Включение SSL)	ON (ВКЛ)

2.1.11 Сокет TCP

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [TCP Socket Setting] (Утилиты - Администратор - Сеть - Настройка сокета TCP)

Параметр настройки	Рекомендуемая настройка
[Use SSL/TLS] (Использовать SSL/TLS)	ON (ВКЛ)

2.2 Другое шифрование

Мы рекомендуем задать следующие настройки для снижения риска возникновения уязвимостей. Подробнее о настройках для каждой функции см. в следующих разделах.

Функция	Рекомендуемая настройка
SMBServer	Шифрование SMB, Подпись SMB
SMBClient	Идентификация Kerberos
SNMP	SNMPv3
IPSEC	IKEv2
S/MIME	ON (ВКЛ)

2.2.1 SMBServer

Использование шифрования SMB и подписи SMB может снизить следующие риски для безопасности.

- Прослушивание: Злонамеренная третья сторона может перехватывать сообщения и красть личную или конфиденциальную информацию.
- Фальсификация данных: Существует риск фальсификации сообщений с помощью атаки типа "незаконный посредник" (MITM).
- Спуфинг: В случае кражи идентификационных данных третья сторона может выдать себя за легитимного пользователя и получить несанкционированный доступ.
- Утечка данных: Незашифрованные сообщения могут легко перехватываться, в особенности в публичных сетях Wi-Fi, что увеличивает риск утечки личной информации и данных кредитных карт.

Шифрование SMB

Необходимые условия

- Создайте общий ящик пользователя. Также выберите настройку для автоматической передачи файлов из общего ящика пользователя и сохранения их в папке SMB.
- Задайте пароль для ящика пользователя.

Местонахождение настройки: [Utility] - [Administrator] - [Box] - [User Box List] (Утилиты - Администратор - Ящик - Список ящиков пользователя)

Параметр настройки	Рекомендуемая настройка
[SMB Communication Encryption] (Шифрование обмена данными SMB)	[Encrypt] (Шифровать)

Подпись SMB

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [SMB Setting] - [SMB Server Settings] (Утилиты - Администратор - Сеть - Настройка SMB - Настройки сервера SMB)

Параметр настройки	Рекомендуемая настройка
[SMB security Signature Setting] (Настройка подписи для безопасности SMB)	[Required] (Требуемый)

2.2.2 SMBClient

Идентификация Kerberos использует надежную технологию шифрования, что значительно снижает риск кражи регистрационных данных в процессе аутентификации. Кроме того, она обеспечивает целостность данных, предотвращая фальсификацию данных на этапе передачи между отправителем и получателем, а также атаки на ретранслятор NTLM.

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [SMB Setting] - [Client Setting]
(Утилиты - Администратор - Сеть - Настройка SMB - Настройка клиента)

Параметр настройки	Рекомендуемая настройка
[SMB Authentication Setting] (Настройка идентификации SMB)	[Kerberos]

2.2.3 SNMP

Настройте шифрование с использованием SNMPv3. Добавление настройки идентификации способствует дополнительному укреплению безопасности. Риски для безопасности приблизительно те же, что и в случае с SMB.

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [SNMP Setting] (Утилиты - Администратор - Сеть - Настройка SNMP)

Параметр настройки	Рекомендуемая настройка
[SNMP Setting] (Настройка SNMP)	[SNMP v3(IP)]
[Encryption Algorithm] (Алгоритм шифрования)	[AES-128]
[Authentication Method] (Метод идентификации)	Выберите [SHA-256], [SHA-384] или [SHA-512].

2.2.4 IPSEC

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IPsec] - [IPsec Setting] (Утилиты - Администратор - Сеть - Настройка TCP/IP - IPsec - Настройка IPsec)

[IKEv2]

Параметр настройки	Рекомендуемая настройка
[Encryption Algorithm] (Алгоритм шифрования)	[AES-CBC] ([256]/[192 and 256]/[All]) (AES-CBC (256/192 и 256)/Все)
[Authentication Algorithm] (Алгоритм идентификации)	[SHA-2] ([256]/[384]/[512]/[256 and 384]/[384 and 512]/[All]), [AES-XCBC] (SHA-2 (256/384/512/256 и 384/384 и 512/Все), AES-XCBC)
[Diffie-Hellman Group] (Группа Diffie-Hellman)	[Group 14], [Group 19] (Группа 14, Группа 19)

[SA]

Параметр настройки	Рекомендуемая настройка
[Encapsulation Mode] (Режим инкапсуляции)	[Tunnel], [Transport] (Туннелирование, Транспортировка)
[Security Protocol] (Протокол безопасности)	[ESP]
[Key Exchange Method] (Метод обмена ключами)	[IKEv2]
[Authentication Method] (Метод идентификации)	[Digital Signature] (Цифровая подпись)

Параметр настройки	Рекомендуемая настройка
[ESP Encryption Algorithm] (Алгоритм шифрования ESP)	[AES-GCM] ([256]/[192 and 256]/[All]), [AES-GCM-64] ([256]/[192 and 256]/[All]), [ENC_NULL_AES_GMAC] ([256]/[192 and 256]/[All]) (AES-GCM (256/192 и 256/Bce), AES-GCM-64 (256/192 и 256/Bce), ENC_NULL_AES_GMAC (256/192 и 256/Bce))
[Perfect Forward Secrecy] (Совершенная прямая секретность)	ON (ВКЛ)
[Diffie-Hellman Group (IKEv2)] - [Priority1-4] (Группа Diffie-Hellman (IKEv2) - Приоритет 1-4)	[Group 14], [Group 19] (Группа 14, Группа 19)

2.2.5 S/MIME

В случае использования дополнительного протокола S/MIME при отправке электронной почты можно зашифровать содержимое письма, чтобы предотвратить перехват, и проверить личность отправителя с помощью электронной подписи. Это является эффективной мерой против мошенничества со спуфингом и фишингом.

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [S/MIME] (Утилиты - Администратор - Сеть - Настройки E-mail - S/MIME)

Параметр настройки	Рекомендуемая настройка
[Digital Signature] (Цифровая подпись)	[Always add signature] (Всегда добавлять подпись)
[Digital Signature Type] (Тип цифровой подписи)	[SHA-256]
[E-Mail Text Encrypt. Method] (Метод шифр. текста E-mail)	[AES-256]

3 Настройка проверки подлинности сертификата

При использовании обмена данными с шифрованием по TLS для ограничения влияния атак типа "незаконный посредник" мы рекомендуем проводить проверку подлинности сертификата. Для проведения проверки необходимо как минимум включить дату окончания действия сертификата и цепочку.

При попытке подключения к устаревшей среде без функции проверки подлинности сертификатов риск атак типа "незаконный посредник" возрастает. Мы рекомендуем работать в безопасной сетевой среде.

Проверка подлинности сертификата на стороне МФУ рекомендуется в следующих функциях клиента МФУ. Подробнее о местонахождении настроек см. в следующих разделах.

POP, SMTP (Start TLS/SMTP через SSL), IEEE802.1X Auth (ТИП EAP: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel

Советы

Проверка подлинности сертификата на стороне клиента, подключенного к МФУ, рекомендуется в следующих функциях сервера МФУ.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), Сокет TCP

3.1 POP

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail RX (POP)]
(Утилиты - Администратор - Сеть - Настройки E-mail - Прием E-mail (POP))

Параметр настройки	Рекомендуемая настройка
[Certificate Verification Level Settings] (Настройки уровня верификации сертификата)	[Expiration Date] (Дата окончания срока действия): ON (ВКЛ) [Chain] (Цепочка): ON (ВКЛ)

3.2 SMTP

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [E-mail Setting] - [E-mail TX (SMTP)]
(Утилиты - Администратор - Сеть - Настройки E-mail - Передача E-mail (SMTP))

Параметр настройки	Рекомендуемая настройка
[Certificate Verification Level Settings] (Настройки уровня верификации сертификата)	[Expiration Date] (Дата окончания срока действия): ON (ВКЛ) [Chain] (Цепочка): ON (ВКЛ)

3.3 IEEE802.1X Auth

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Setting] - [Supplicant Setting] (Утилиты - Администратор - Сеть - Настройки идентификации IEEE802.1X - Настройки идентификации IEEE802.1X - Настройка сапликанта)

Параметр настройки	Рекомендуемая настройка
[Certificate Verification Level Settings] (Настройки уровня верификации сертификата)	[Expiration Date] (Дата окончания срока действия): ON (ВКЛ) [Chain] (Цепочка): ON (ВКЛ)

3.4 IPSEC

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [TCP/IP Setting] - [IPsec] - [Enable IPsec] (Утилиты - Администратор - Сеть - Настройка TCP/IP - IPsec - Включить IPsec)

Параметр настройки	Рекомендуемая настройка
[Certificate Verification Level Settings] (Настройки уровня верификации сертификата)	[Expiration Date] (Дата окончания срока действия): [Confirm] (Подтвердить) [Chain] (Цепочка): [Confirm] (Подтвердить)

Советы

Предварительно в [IPsec Setting] (Настройка IPsec) зарегистрировать пункты [IKE], [SA], [Peer] (Равноправный узел) и [Protocol Setting] (Настройка протокола).

3.5 WebDAVClient

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [WebDAV Settings] - [WebDAV Client Settings] (Утилиты - Администратор - Сеть - Настройки WebDAV - Настройки клиента WebDAV)

Параметр настройки	Рекомендуемая настройка
[Certificate Verification Level Settings] (Настройки уровня верификации сертификата)	[Expiration Date] (Дата окончания срока действия): ON (ВКЛ) [Chain] (Цепочка): ON (ВКЛ)

3.6 LDAP

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [LDAP Setting] - [Setting Up LDAP] (Утилиты - Администратор - Сеть - Настройка LDAP - Настройка LDAP)

Параметр настройки	Рекомендуемая настройка
[Certificate Verification Level Settings] (Настройки уровня верификации сертификата)	[Expiration Date] (Дата окончания срока действия): ON (ВКЛ) [Chain] (Цепочка): ON (ВКЛ)

3.7 DPWS

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [DPWS Settings] - [DPWS Common Settings] (Утилиты - Администратор - Сеть - Настройки DPWS - Общие настройки DPWS)

Параметр настройки	Рекомендуемая настройка
[Certificate Verification Level Settings] (Настройки уровня верификации сертификата)	[Expiration Date] (Дата окончания срока действия): ON (ВКЛ) [Chain] (Цепочка): ON (ВКЛ)

3.8 OpenAPI

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [OpenAPI Setting] - [OpenAPI Setting]
(Утилиты - Администратор - Сеть - Настройка OpenAPI - Настройка OpenAPI)

Параметр настройки	Рекомендуемая настройка
[Certificate Verification Level Settings] (Настройки уровня верификации сертификата)	[Expiration Date] (Дата окончания срока действия): ON (ВКЛ) [Chain] (Цепочка): ON (ВКЛ)

3.9 RemotePanel

Местонахождение настройки: [Utility] - [Administrator] - [Network] - [Remote Panel Settings] - [Remote Panel Client Settings] (Утилиты - Администратор - Сеть - Настройки удаленной панели - Настройки клиента удаленной панели)

Параметр настройки	Рекомендуемая настройка
[Certificate Verification Level Settings] (Настройки уровня верификации сертификата)	[Expiration Date] (Дата окончания срока действия): ON (ВКЛ) [Chain] (Цепочка): ON (ВКЛ)

4 Дополнительная информация по безопасности

4.1 Рекомендации на основе передовой практики

Мы рекомендуем, чтобы используемые алгоритмы шифрования соответствовали настройкам, разработанным на основе передовой практики и рекомендованным в Руководстве EUCC по криптографии и согласованным SOGIS криптографическим механизмам.

Ниже дан список алгоритмов шифрования и вариантов длины ключей, рекомендованных в Руководстве EUCC по криптографии и согласованным SOGIS криптографическим механизмам.

Пункт	Рекомендуемая настройка
Алгоритмы шифрования	AES (Advanced Encryption Standard (улучшенный стандарт шифрования)) RSA (Rivest-Shamir-Adleman (алгоритм Ривеста-Шамира-Адлемана)) SHA-2 (Secure Hash Algorithm 2 (алгоритм безопасного хэширования)) ECC (Elliptic Curve Cryptography (криптография на основе эллиптических кривых)) HMAC (Hash-based Message Authentication Code (код аутентификации сообщения на основе хеш-функции))
Длина ключа шифрования	RSA: 2048 бит и более ECC: 256 бит и более AES: 256 бит

Советы

Подробнее см. в последней версии Руководства по криптографии EUCC и согласованным SOGIS криптографическим механизмам.

4.2 Меры предосторожности при обмене данными с устаревшими системами

Предполагается, что для обмена данными с устаревшими системами будут использоваться следующие протоколы и версии.

Использование устаревших настроек увеличивает риски безопасности, поэтому следует использовать их в безопасной сетевой среде.

Пункт	Устаревшие настройки
Протокол	SLP FTP SMB (3.0 или более ранняя версия, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (ТИП EAP: В зависимости от сервера/ВыКЛ) DPWS Сокет TCP
Алгоритмы шифрования	SHA-1 (Secure Hash Algorithm 1 (алгоритм безопасного хэширования 1)) DES (Data Encryption Standard = стандарт шифрования данных) 3DES (Triple Data Encryption Standard = стандарт тройного шифрования данных) RC2-40 (шифр D51Rivest) RC2-64 (шифр D51Rivest) RC2-128 (шифр D51Rivest)
Длина ключа шифрования	RSA: 1024 бит и менее ECC: 160 бит и менее AES: 128 бит и менее DES: 56 бит 3DES: 112 бит

Устаревшие настройки IPsec

[IKEv1]

Параметр настройки	Устаревшие настройки
[Encryption Algorithm] (Алгоритм шифрования)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192]) (AES-CBC (128/192/128 и 192))
[Authentication Algorithm] (Алгоритм идентификации)	Не используется
[Diffie-Hellman Group] (Группа Diffie-Hellman)	[Group 1], [Group 2], [Group 5] (Группа 1, Группа 2, Группа 5)

[IKEv2]

Параметр настройки	Устаревшие настройки
[Encryption Algorithm] (Алгоритм шифрования)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192]) (AES-CBC (128/192/128 и 192))
[Authentication Algorithm] (Алгоритм идентификации)	Не используется
[Diffie-Hellman Group] (Группа Diffie-Hellman)	[Group 1], [Group 2], [Group 5] (Группа 1, Группа 2, Группа 5)

[SA]

Параметр настройки	Устаревшие настройки
[Key Exchange Method] (Метод обмена ключами)	[IKEv1]
[Authentication Method] (Метод идентификации)	[Digital Signature] (Цифровая подпись)
[ESP Encryption Algorithm] (Алгоритм шифрования ESP)	[3DES-CBC] ([128]/[192]/[128 and 192]) (3DES-CBC (128/192/128 и 192)) [AES-CTR] ([128]/[192]/[128 and 192]) (AES-CTR (128/192/128 и 192)) [AES-GCM] ([128]/[192]/[128 and 192]) (AES-GCM (128/192/128 и 192)) [AES-GCM-64] ([128]/[192]/[128 and 192]) (AES-GCM-64 (128/192/128 и 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192]) (ENC_NULL_AES_GMAC (128/192/128 и 192))
[Perfect Forward Secrecy] (Совершенная прямая секретность)	ON (ВКЛ)
[Diffie-Hellman Group(IKEv1)] (Группа Diffie-Hellman (IKEv1))	[Group 1], [Group 2], [Group 5] (Группа 1, Группа 2, Группа 5)

4.3 Сетевые интерфейсы и сервисы, доступные при поставке с завода

Тип сервиса	Протокол	Номер порта
DHCP	UDP	68
Сервер HTTP	TCP	80
Сервис имен NETBIOS	UDP	137
Сервис дейтаграмм NETBIOS	UDP	138
SNMP	UDP	161
Сервер HTTP через SSL / IPP через SSL	TCP	443
Печать LPD	TCP	515
Клиент DHCPv6	UDP	546
Печать IPP	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-инструмент)	TCP	8091
Печать RAW	TCP	9100
Печать RAW	TCP	9112
Печать RAW	TCP	9113
Печать RAW	TCP	9114
Печать RAW	TCP	9115
Печать RAW	TCP	9116
OpenAPI	TCP	50001

4.4 Проверка вводимых данных

Количество символов, которое необходимо ввести для сетевых настроек и т. д., указано в соответствующих параметрах настройки в Руководстве пользователя.

В зависимости от кодировки языка максимально допустимый объем вводимых данных (данных, сохраненных в МФУ) для параметров, поддерживающих многобайтовые символы, может в три раза превышать количество символов.

Odporúčania pre zabezpečené sieťové zariadenia

Obsah

1 Nastavenie filtrovania IP adries

1.1	Filtrovanie IP adries	1-3
1.2	Rýchle filtrov. adries IP.....	1-3

2 Nastavenie šifrovanej komunikácie

2.1	Šifrovanie TLS	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel (Vzdialený panel).....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP Socket.....	2-6
2.2	Iné šifrovanie	2-7
2.2.1	SMBServer.....	2-7
	SMB Encryption (Šifrovanie priečinka SMB).....	2-7
	SMB Signature (Podpis SMB).....	2-7
2.2.2	SMBClient.....	2-8
2.2.3	SNMP	2-8
2.2.4	IPSEC.....	2-8
2.2.5	S/MIME	2-9

3 Nastavenie platnosti certifikátu

3.1	POP.....	3-10
3.2	SMTP	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPSEC	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	RemotePanel (Vzdialený panel)	3-12

4 Ďalšie informácie zabezpečenia

4.1	Odporúčanie osvedčených postupov	4-13
4.2	Bezpečnostné opatrenia pre komunikáciu so staršími systémami	4-14
	Staršie nastavenia IPsec.....	4-14
4.3	Sieťové rozhrania a služby dostupné od výroby	4-15
4.4	Informácie o overovaní platnosti vstupu	4-16



Informácie o návode

Tento návod opisuje informácie a nastavenia, ktoré umožňujú bezpečné používanie zariadení.

Pri pripojení tejto hlavnej jednotky k sieti ju využívajte v prostredí chránenom bránou firewall. Ako IP adresu hlavnej jednotky tiež odporúčame nastaviť súkromnú IP adresu.

Nastavenie súkromnej IP adresy umožňuje prístup k hlavnej jednotke iba používateľom v lokálnej sieti, napríklad v internej LAN sieti, čím sa zabráni neoprávnenému prístupu z vonkajšieho prostredia.

Ak je nutné použiť globálnu IP adresu, nainštalujte hlavnú jednotku za bránu firewall (ochrana bránou).

1 Nastavenie filtrovania IP adries

Filtrovanie IP adresy je funkcia, ktorá obmedzuje prístup k hlavnej jednotke na báze IP adries. Správnym nastavením tejto funkcie môžete obmedziť prístup z neoprávnených zariadení.

Funkciu filtrovania IP adries je v hlavnej jednotke možné nastaviť dvomi spôsobmi.

1.1 Filtrovanie IP adries

Manuálne nastavte interval IP adries, ktorým chcete umožniť alebo zakázať prístup.

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [TCP/IP Setting] (Nastavenie TCP/IP) - [IP Address Filtering] (Filtrovanie IP)



Tipy

Nastavte IP adresy tak, aby boli povolené alebo zakázané, podľa vášho prostredia.

1.2 Rýchle filtrov. adries IP

Interval IP adries, ktoré majú povolený prístup, sa automaticky nastaví podľa IP adresy a masky podsiete nastavenej v hlavnej jednotke.

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [TCP/IP Setting] (Nastavenie TCP/IP) - [Quick IP Filtering] (Rýchle filtrovanie IP)

Odporúčané nastavenia: [Synchronize IP Address] (Synchronizovať adresu IP)/[Synchronize Subnet Mask] (Synchronizovať masku podsiete) *

* Vyberte jednu z možností, ktorá vyhovuje vášmu prostrediu.

2 Nastavenie šifrovanej komunikácie

Odporúčame používať nasledujúcu šifrovanú komunikáciu na zabránenie odpočúvaniu údajov, manipulácii s údajmi a prevzatiu relácie.

2.1 Šifrovanie TLS

Odporúčame nakonfigurovať nasledujúce nastavenia na zníženie rizika zraniteľnosti/narušení.

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Security] (Zabezpečenie) - [PKI Settings] (Nastavenia PKI) - [Enable SSL Version] (Povoliť verziu SSL)

Nastavovaná položka	Odporúčané nastavenie
[Mode using SSL/TLS] (Režim s použitím SSL/TLS)	[Admin. Mode and User Mode] (Režim správcu a režim používateľa)
[SSL/TLS Version Setting] (Nastavenie verzie SSL/TLS)	TLS1.2 TLS1.3 (IEEE802.1X nekompatibilné)
[Encryption Strength] (Stupeň šifrovania)	AES-256

Počiatkový certifikát je nainštalovaný z výroby. Ak potrebujete iný certifikát, zaregistrujte nový v nasledujúcej oblasti.

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Security] (Zabezpečenie) - [PKI Settings] (Nastavenia PKI) - [Device Certificate Setting] (Nastavenie certifikátu zariadenia)

Nastavovaná položka	Odporúčané nastavenie
[Encryption Key Type] (Typ šifrovacieho kľúča)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Šifrovanie TLS je podporované pre nasledujúce protokoly a služby. Podrobnejšie informácie o nastavovaných oblastiach pozri v nasledujúcich častiach.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel (Vzdialený panel))
- DPWS
- POP
- SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP Socket

2.1.1 HTTP (Web Connection)

Ak povolíte [Enable SSL Version] (Povoliť verziu SSL), komunikačný režim sa automaticky prepne na šifrovanú komunikáciu TLS (HTTPS).

2.1.2 WebDAVServer

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [WebDAV Settings] (Nastavenia WebDAV) - [WebDAV Server Settings] (Nastavenia servera WebDAV)

Nastavovaná položka	Odporúčané nastavenie
[Nastavenie SSL]	[SSL Only] (Iba SSL)

2.1.3 IPP

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [HTTP Server Settings] (Nastavenia servera HTTP)

Nastavovaná položka	Odporúčané nastavenie
[IPP-SSL Settings] (Nastavenia IPP-SSL)	[SSL Only] (Iba SSL)

2.1.4 OpenAPI

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [OpenAPI Setting] (Nastavenie OpenAPI) - [OpenAPI Setting] (Nastavenie OpenAPI)

Nastavovaná položka	Odporúčané nastavenie
[Nastavenia SSL/portu]	[SSL Only] (Iba SSL)

2.1.5 RemotePanel (Vzdialený panel)

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [Remote Panel Settings] (Nastavenia vzdialeného panela) - [Remote Panel Server Settings] (Nastavenia servera vzdialeného panela)

Nastavovaná položka	Odporúčané nastavenie
[Port No.(SSL)] (Č. portu (SSL))	[50443]



Tipy

Ak povolíte [Enable SSL Version] (Povoliť verziu SSL), komunikačný režim sa automaticky prepne do režimu šifrovanej komunikácie TLS. Zadať číslo portu.

2.1.6 DPWS

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [DPWS Settings] (Nastavenia DPWS) - [DPWS Common Settings] (Všeobecné nastavenia DPWS)

Nastavovaná položka	Odporúčané nastavenie
[Nastavenie SSL]	ON (Zap.)

2.1.7 POP

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [E-mail Setting] (Nastavenie e-mailu) [E-mail RX (POP)] (Príjem e-mailu (POP))

Nastavovaná položka	Odporúčané nastavenie
[Povoliť SSL]	ON (Zap.)

2.1.8 SMTP

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [E-mail Setting] (Nastavenie e-mailu) [E-mail RX (POP)] (Odos. e-mailu (SMTP))

Nastavovaná položka	Odporúčané nastavenie
[Nastavenie SSL/TLS]	[SMTP cez SSL]

2.1.9 IEEE802.1X Auth

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [IEEE802.1X Authentication Setting] (Nastavenie overenia IEEE802.1X) - [IEEE802.1X Authentication Setting] (Nastavenie overenia IEEE802.1X) - [Supplicant Setting] (Nastavenie žiadateľa)

Nastavovaná položka	Odporúčané nastavenie
[EAP-Type]	Vyberte [EAP-TLS], [EAP-TTLS] alebo [PEAP].

2.1.10 LDAP

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [LDAP Setting] (Nastavenie LDAP) - [Setting Up LDAP] (Nastaviť LDAP)

Nastavovaná položka	Odporúčané nastavenie
[Povoliť SSL]	ON (Zap.)

2.1.11 TCP Socket

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [TCP Socket Setting] (Nastavenie TCP Socket)

Nastavovaná položka	Odporúčané nastavenie
[Use SSL/TLS] (Použiť SSL/TLS)	ON (Zap.)

2.2 Iné šifrovanie

Odporúčame nakonfigurovať nasledujúce nastavenia na zníženie rizika zraniteľnosti/narušení. Podrobnejšie informácie o nastaveniach jednotlivých funkcií pozri v nasledujúcich častiach.

Funkcia	Odporúčané nastavenie
SMBServer	SMB Encryption, (Šifrovanie priečinka SMB), SMB Signature (Podpis SMB)
SMBClient	Kerberos Authentication (Overenie Kerberos)
SNMP	SNMPv3
IPSEC	IKEv2
S/MIME	ON (Zap.)

2.2.1 SMBServer

Používanie šifrovania priečinka SMB a podpisu SMB môže znížiť nasledujúce bezpečnostné riziká.

- Odpočúvanie: Nekalá tretia strana môže zachytiť komunikáciu a ukradnúť osobné údaje alebo dôverné informácie.
- Manipulácia s údajmi: Existuje riziko, že obsah komunikácie môže byť manipulovaný útokom MITM (Man-In-The-Middle).
- Falšovanie údajov: Ak je overovacia informácia odcudzená, tretia strana sa môže vydávať za legitímneho používateľa na získanie neoprávneného prístupu.
- Únik informácií: Nešifrovaná komunikácia sa dá ľahko zachytiť, najmä vo verejných sieťach Wi-Fi, čo zvyšuje riziko úniku osobných údajov a informácií o kreditných kartách.

SMB Encryption (Šifrovanie priečinka SMB)

Nevyhnutné podmienky

- Vytvorte verejnú používateľskú schránku. Nakonfigurujte tiež nastavenie automatického prenosu súborov z verejnej používateľskej schránky a ich ukladania do priečinka SMB.
- Zadajte heslo pre používateľskú schránku.

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Box] (Schránka) - [User Box List] (Zoznam používateľských schránok)

Nastavovaná položka	Odporúčané nastavenie
[SMB Communication Encryption] (Šifrovanie komunikácie SMB)	[Kódovať]

SMB Signature (Podpis SMB)

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [SMB Setting] (Nastavenie SMB) - [SMB Server Settings] (Nastavenia servera SMB)

Nastavovaná položka	Odporúčané nastavenie
[SMB security Signature Setting] (Nastavenie podpisu zabezpečenia SMB)	[Vyžaduje sa]

2.2.2 SMBClient

Overovanie Kerberos používa silnú šifrovaciu technológiu, ktorá výrazne znižuje riziko odcudzenia prihlasovacích údajov počas procesu overovania. Zaisťuje tiež integritu údajov, zabraňuje manipulácii s údajmi medzi odosielateľom a príjemcom, ako aj útokom NTLM Relay.

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [SMB Setting] (Nastavenie SMB) - [Client Setting] (Nastavenie klienta)

Nastavovaná položka	Odporúčané nastavenie
[SMB Authentication Setting] (Nastavenie overenia SMB)	[Kerberos]

2.2.3 SNMP

Nastavte šifrovanie pomocou SNMPv3. Ak pridáte aj nastavenie overenia, môžete ďalej zvýšiť zabezpečenie. Bezpečnostné riziká sú približne rovnaké ako pri SMB.

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [SNMP Setting] (Nastavenie SNMP)

Nastavovaná položka	Odporúčané nastavenie
[Nastavenie SNMP]	[SNMP v3(IP)]
[Kódovací algoritmus]	[AES-128]
[Authentication Method] (Spôsob overenia)	Vyberte [SHA-256], [SHA-384] alebo [SHA-512].

2.2.4 IPSEC

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [TCP/IP Setting] (Nastavenie TCP/IP) - [IPsec] - [IPsec Setting] (Nastavenie IPsec)

[IKEv2]

Nastavovaná položka	Odporúčané nastavenie
[Kódovací algoritmus]	[AES-CBC] ([256]/[192 and 256] (192 a 256))/[All] (Všetky)
[Autorizačný algoritmus]	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 a 384)/[384 and 512] (384 a 512))/[All] (Všetky), [AES-XCBC]
[Skupina Diffie-Hellman]	[Group 14] (Skupina 14), [Group 19] (Skupina 19)

[SA]

Nastavovaná položka	Odporúčané nastavenie
[Režim zapuzdrenia]	[Tunnel] (Tunel), [Transport] (Dopravník)
[Bezpečnostný protokol]	[ESP]
[Spôsob výmeny hesla]	[IKEv2]
[Authentication Method] (Spôsob overenia)	[Digitálny podpis]
[Kódovací algoritmus ESP]	[AES-GCM] ([256]/[192 and 256] (192 a 256))/[All] (Všetky), [AES-GCM-64] ([256]/[192 and 256] (192 a 256))/[All] (Všetky), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 a 256))/[All] (Všetky)
[Diskrétnosť preposlania]	ON (Zap.)
[Diffie-Hellman Group(IKEv2)] (Skupina Diffie-Hellman (IKEv2)) - [Priority1-4] (Priorita 1 - 4)	[Group 14] (Skupina 14), [Group 19] (Skupina 19)

2.2.5 S/MIME

Ak pri odosielaní e-mailov používate voliteľný protokol S/MIME, môžete zašifrovať obsah e-mailu, aby ste zabránili odpočúvaniu a overili identitu odosielateľa elektronickým podpisom. Toto je účinné opatrenie proti podvodom falšovania údajov (Spoofing) a podvodného získavania citlivých informácií (Phishing).

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [E-mail Setting] (Nastavenie e-mailu) - [S/MIME]

Nastavovaná položka	Odporúčané nastavenie
[Digitálny podpis]	[Always add signature] (Vždy pridať podpis)
[Typ digitálneho podpisu]	[SHA-256]
[E-Mail Text Encrypt. Method] (Metóda šifrovania textu e-mailu)	[AES-256]

3 Nastavenie platnosti certifikátu

Pri používaní komunikácie šifrovanej protokolom TLS na zníženie vplyvu útokov typu "MITM" (Man-in-the-middle) odporúčame použiť overenie platnosti certifikátu. Pre položky overenia platnosti odporúčame minimálne povoliť dátum uplynutia platnosti certifikátu a reťazec.

Ak sa pokúsite pripojiť k staršiemu prostrediu, ktoré nemá certifikovanú funkciu overovania platnosti, zvyšuje sa riziko útokov typu "MITM". Odporúčame ho používať v zabezpečenom sieťovom prostredí.

Overenie platnosti certifikátu na strane MFP sa odporúča v nasledujúcich funkciách klienta MFP. Podrobnejšie informácie o nastavovaných oblastiach pozri v nasledujúcich častiach.

POP, SMTP (Start TLS/SMTP over SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel (Vzdialený panel)

Tipy

Overenie platnosti certifikátu na strane klienta pripojeného k MFP sa odporúča v nasledujúcich funkciách MFP servera.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel (Vzdialený panel)), TCP Socket

3.1 POP

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [E-mail Setting] (Nastavenie e-mailu) [E-mail RX (POP)] (Príjem e-mailu (POP))

Nastavovaná položka	Odporúčané nastavenie
[Certificate Verification Level Settings] (Nastavenia úrovne overovania certifikátu)	[Expiration Date] (Dátum uplynutia platnosti): ON (Zap.) [Chain] (Reťazec): ON (Zap.)

3.2 SMTP

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [E-mail Setting] (Nastavenie e-mailu) [E-mail RX (POP)] (Odos. e-mailu (SMTP))

Nastavovaná položka	Odporúčané nastavenie
[Certificate Verification Level Settings] (Nastavenia úrovne overovania certifikátu)	[Expiration Date] (Dátum uplynutia platnosti): ON (Zap.) [Chain] (Reťazec): ON (Zap.)

3.3 IEEE802.1X Auth

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [IEEE802.1X Authentication Setting] (Nastavenie overenia IEEE802.1X) - [IEEE802.1X Authentication Setting] (Nastavenie overenia IEEE802.1X) - [Supplicant Setting] (Nastavenie žiadateľa)

Nastavovaná položka	Odporúčané nastavenie
[Certificate Verification Level Settings] (Nastavenia úrovne overovania certifikátu)	[Expiration Date] (Dátum uplynutia platnosti): ON (Zap.) [Chain] (Reťazec): ON (Zap.)

3.4 IPSEC

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [TCP/IP Setting] (Nastavenie TCP/IP) - [IPsec] - [Enable IPsec] (Povoliť IPsec)

Nastavovaná položka	Odporúčané nastavenie
[Certificate Verification Level Settings] (Nastavenia úrovne overovania certifikátu)	[Expiration Date] (Dátum uplynutia platnosti): [Potvrdiť] [Chain] (Reťazec): [Potvrdiť]



Tipy

V nastavení [IPsec Setting] (Nastavenie IPsec) vopred zaregistrujte položky [IKE], [SA], [Peer] (Partnerské zariadenie) a [Protocol Setting] (Nastavenie protokolu).

3.5 WebDAVClient

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [WebDAV Settings] (Nastavenia WebDAV) - [WebDAV Client Settings] (Nastavenia klienta WebDAV)

Nastavovaná položka	Odporúčané nastavenie
[Certificate Verification Level Settings] (Nastavenia úrovne overovania certifikátu)	[Expiration Date] (Dátum uplynutia platnosti): ON (Zap.) [Chain] (Reťazec): ON (Zap.)

3.6 LDAP

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [LDAP Setting] (Nastavenie LDAP) - [Setting Up LDAP] (Nastaviť LDAP)

Nastavovaná položka	Odporúčané nastavenie
[Certificate Verification Level Settings] (Nastavenia úrovne overovania certifikátu)	[Expiration Date] (Dátum uplynutia platnosti): ON (Zap.) [Chain] (Reťazec): ON (Zap.)

3.7 DPWS

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [DPWS Settings] (Nastavenia DPWS) - [DPWS Common Settings] (Všeobecné nastavenia DPWS)

Nastavovaná položka	Odporúčané nastavenie
[Certificate Verification Level Settings] (Nastavenia úrovne overovania certifikátu)	[Expiration Date] (Dátum uplynutia platnosti): ON (Zap.) [Chain] (Reťazec): ON (Zap.)

3.8 OpenAPI

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [OpenAPI Setting] (Nastavenie OpenAPI) - [OpenAPI Setting] (Nastavenie OpenAPI)

Nastavovaná položka	Odporúčané nastavenie
[Certificate Verification Level Settings] (Nastavenia úrovne overovania certifikátu)	[Expiration Date] (Dátum uplynutia platnosti): ON (Zap.) [Chain] (Reťazec): ON (Zap.)

3.9 RemotePanel (Vzdialený panel)

Oblasť nastavenia: [Utility] (Nástroje) - [Administrator] (Správca) - [Network] (Sieť) - [Remote Panel Settings] (Nastavenia vzdialeného panela) - [Remote Panel Client Settings] (Nastavenia klienta vzdialeného panela)

Nastavovaná položka	Odporúčané nastavenie
[Certificate Verification Level Settings] (Nastavenia úrovne overovania certifikátu)	[Expiration Date] (Dátum uplynutia platnosti): ON (Zap.) [Chain] (Reťazec): ON (Zap.)

4 Ďalšie informácie zabezpečenia

4.1 Odporúčanie osvedčených postupov

Odporúčame, aby používané šifrovacie algoritmy boli v súlade s nastaveniami osvedčených postupov odporúčanými v usmerneniach EUCC o kryptografii a kryptografických mechanizmoch odsúhlasených SOGIS.

Nižšie je uvedený zoznam šifrovacích algoritmov a dĺžok kľúčov odporúčaných v usmerneniach EUCC o kryptografii a kryptografických mechanizmoch odsúhlasených SOGIS.

Položka	Odporúčané nastavenie
Šifrovacie algoritmy	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Dĺžka šifrovacieho kľúča	RSA: 2 048 bitov alebo viac ECC: 256 bitov alebo viac AES: 256 bitov



Tipy

Podrobnosti nájdete v najnovších usmerneniach EUCC o kryptografii a kryptografických mechanizmoch odsúhlasených SOGIS.

4.2 Bezpečnostné opatrenia pre komunikáciu so staršími systémami

Na komunikáciu so staršími systémami sa predpokladá používanie nasledujúcich protokolov a verzií.

Používanie starších nastavení zvyšuje bezpečnostné riziká, preto ich používajte v zabezpečenom sieťovom prostredí.

Položka	Staršie nastavenia
Protokol	SLP FTP SMB (3.0 alebo staršia verzia, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYP: Závisí od servera/OFF (Vyp.)) DPWS TCPsocket
Šifrovacie algoritmy	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Trojitý Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Dĺžka šifrovacieho kľúča	RSA: 1 024 bitov alebo menej ECC: 160 bitov alebo menej AES: 128 bitov alebo menej DES: 56 bitov 3DES: 112 bitov

Staršie nastavenia IPsec

[IKEv1]

Nastavovaná položka	Staršie nastavenia
[Kódovací algoritmus]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 a 192))
[Autorizačný algoritmus]	Nepoužíva sa
[Skupina Diffie-Hellman]	[Group 1], (Skupina 1) [Group 2] (Skupina 2), [Group 5] (Skupina 5)

[IKEv2]

Nastavovaná položka	Staršie nastavenia
[Kódovací algoritmus]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 a 192))
[Autorizačný algoritmus]	Nepoužíva sa
[Skupina Diffie-Hellman]	[Group 1], (Skupina 1) [Group 2] (Skupina 2), [Group 5] (Skupina 5)

[SA]

Nastavovaná položka	Staršie nastavenia
[Spôsob výmeny hesla]	[IKEv1]
[Authentication Method] (Spôsob overenia)	[Digitálny podpis]
[Kódovací algoritmus ESP]	[3DES-CBC] ([128]/[192]/[128 and 192] (128 a 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 a 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 a 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 a 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 a 192))
[Diskrétnosť preposlania]	ON (Zap.)
[Skupina Diffie-Hellman (IKEv1)]	[Group 1], (Skupina 1) [Group 2] (Skupina 2), [Group 5] (Skupina 5)

4.3 Sieťové rozhrania a služby dostupné od výroby

Typ služby	Protokol	Číslo portu
DHCP	UDP	68
HTTP Server	TCP	80
NETBIOS Name Service	UDP	137
NETBIOS Datagram Service	UDP	138
SNMP	UDP	161
HTTP Server over SSL / IPP over SSL	TCP	443
LPD Print	TCP	515
DHCPv6 Client	UDP	546
IPP Print	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-tool)	TCP	8091
RAW Print	TCP	9100
RAW Print	TCP	9112
RAW Print	TCP	9113
RAW Print	TCP	9114
RAW Print	TCP	9115
RAW Print	TCP	9116
OpenAPI	TCP	50001

4.4 Informácie o overovaní platnosti vstupu

Počet znakov, ktoré sa majú zadať pre sieťové nastavenia atď., pozri v každej nastavovanej položke v návode na používanie.

V závislosti od kódovania jazyka môže byť maximálny povolený vstup (údaje uložené v MFP) pre položky, ktoré podporujú multibajtové znaky, trojnásobok počtu znakov.

Priporočila za naprave v varnem omrežju

Preglednica vsebine

1 Nastavitev filtriranja naslovov IP

1.1	Filtriranje naslovov IP	1-3
1.2	Hitro filtriranje po IP.....	1-3

2 Nastavitev šifrirane komunikacije

2.1	Šifriranje prek protokola TLS.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	Prev. pristnosti IEEE802.1X	2-6
2.1.10	LDAP	2-6
2.1.11	TCPsocket.....	2-6
2.2	Drugo šifriranje.....	2-7
2.2.1	SMBServer	2-7
	Šifriranje prek protokola SMB	2-7
	Podpis SMB	2-7
2.2.2	SMBCClient	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Nastavitev preverjanja certifikata

3.1	POP.....	3-10
3.2	SMTP	3-10
3.3	Prev. pristnosti IEEE802.1X.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	RemotePanel	3-12

4 Dodatne varnostne informacije

4.1	Priporočilo za najboljšo prakso.....	4-13
4.2	Previdnostni ukrepi za komunikacijo z zastarelimi sistemi	4-14
	Zastarele nastavitve zbirke IPsec	4-14
4.3	Tovarniško dobavljeni omrežni vmesniki in storitve.....	4-16
4.4	O vnosu preverjanja.....	4-17



O tem priročniku za uporabo

V tem priročniku za uporabo najdete informacije in opis nastavitv, ki omogočajo varno uporabo naprav.

Napravo priključite v omrežje, ki je zaščiteno s požarnim zidom. Priporočamo tudi, da za naslov IP naprave nastavite zasebni naslov IP.

Če je nastavljen zasebni naslov IP, lahko do naprave dostopajo samo uporabniki v lokalnem omrežju, na primer v notranjem omrežju LAN, kar preprečuje nepooblaščen dostop od zunaj.

Če morate uporabiti globalni naslov IP, za to napravo namestite požarni zid.

1 Nastavitev filtriranja naslovov IP

Filtriranje naslovov IP je funkcija, ki omejuje naprave, ki lahko dostopajo do te naprave z naslovom IP. S pravilno nastavitvijo te funkcije lahko omejite dostop nepooblaščenih naprav.

Funkcijo filtriranja naslovov IP te naprave lahko nastavite na enega od naslednjih dveh načinov.

1.1 Filtriranje naslovov IP

Ročno določite območje naslovov IP.

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [TCP/IP Setting] (Nastavitev zbirke TCP/IP) - [IP Address Filtering] (Filtriranje naslovov IP)



Nasveti

Določite naslove IP, ki naj bodo dovoljeni ali zavrnjeni, da bodo ustrezali vašemu okolju.

1.2 Hitro filtriranje po IP

Razpon naslovov IP, ki jim je omogočen dostop, se samodejno nastavi na podlagi naslova IP in maske podomrežja, nastavljene v tej napravi.

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [TCP/IP Setting] (Nastavitev zbirke TCP/IP) - [Quick IP Filtering] (Hitro filtriranje po IP)

Priporočene nastavitve: [Synchronize IP Address] (Sinhroniziraj naslov IP)/[Synchronize Subnet Mask] (Sinhroniziraj masko podomrežja) *

*Izberite tisto, ki ustreza vašemu okolju.

2 Nastavitev šifrirane komunikacije

Priporočamo, da za preprečevanje prisluškovanja, poseganja v podatke in vdora v sejo uporabljate naslednjo šifrirano komunikacijo.

2.1 Šifriranje prek protokola TLS

Priporočamo, da konfigurirate naslednje nastavitve, da zmanjšate tveganje za ranljivosti.

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Security] (Varnost) - [PKI Settings] (Nastavitve ogrodja PKI) - [Enable SSL Version] (Omogoči različico protokola SSL)

Element nastavitve	Priporočena nastavitev
[Mode using SSL/TLS] (Način z uporabo protokola SSL/TLS)	[Admin. Mode and User Mode] (Skrbn. način in uporab. način)
[SSL/TLS Version Setting] (Različica nastavitve protokola SSL/TLS)	TLS 1.2 TLS 1.3 (nezdružljiv z IEEE802.1X)
[Encryption Strength] (Moč šifriranja)	AES-256

Začetni certifikat je nameščen v tovarni. Če potrebujete drug certifikat, novi certifikat registrirajte na eni izmed sledečih lokacij.

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Security] (Varnost) - [PKI Settings] (Nastavitve ogrodja PKI) - [Device Certificate Setting] (Nastavitev certifikata naprave)

Element nastavitve	Priporočena nastavitev
[Encryption Key Type] (Vrsta šifrirnega ključa)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Šifriranje prek protokola TLS podpirajo sledeči protokoli in storitve. Podrobnosti o nastavitvi lokacije so na voljo v naslednjih poglavjih.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Začetek TLS, SMTP prek SSL)
- Prev. pristnosti IEEE802.1X (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCPSocket

2.1.1 HTTP (Web Connection)

Če izberete [Enable SSL Version] (Omogoči različico protokola SSL), se način komunikacije samodejno preklopi na šifrirano komunikacijo prek protokola TLS (HTTPS).

2.1.2 WebDAVServer

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [WebDAV Settings] (Nastavitve protokola WebDAV) - [WebDAVServer Settings] (Nastavitve strežnika WebDAVServer)

Element nastavitve	Priporočena nastavitev
[SSL Settings] (Nastavitve protokola SSL)	[SSL Only] (Samo protokol SSL)

2.1.3 IPP

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [HTTP Server Settings] (Nastavitve strežnika HTTP)

Element nastavitve	Priporočena nastavitev
[IPP-SSL Settings] (Nastavitve protokola IPP-SSL)	[SSL Only] (Samo protokol SSL)

2.1.4 OpenAPI

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [OpenAPI Setting] (Nastavitev standarda OpenAPI) - [OpenAPI Setting] (Nastavitev standarda OpenAPI)

Element nastavitve	Priporočena nastavitev
[SSL/Port Settings] (Nastavitve protokola SSL/vrat)	[SSL Only] (Samo protokol SSL)

2.1.5 RemotePanel

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [Remote Panel Settings] (Nastavitve oddaljene plošče) - [Remote Panel Server Settings] (Nastavitve strežnika RemotePanel)

Element nastavitve	Priporočena nastavitev
[Port No.(SSL)] (Št. vrat (SSL))	[50443]



Nasveti

Če izberete [Enable SSL Version] (Omogoči različico protokola SSL), se način komunikacije samodejno preklopi na šifrirano komunikacijo protokola TLS (HTTPS). Določite številko vrat.

2.1.6 DPWS

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [DPWS Settings] (Nastavitve protokola DPWS) - [DPWS Common Settings] (Skupne nastavitve protokola DPWS)

Element nastavitve	Priporočena nastavitev
[SSL Settings] (Nastavitve protokola SSL)	VKLOP

2.1.7 POP

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [E-mail Setting] (Nastavitev e-pošte) - [E-mail RX (POP)] (Prejem e-pošte (POP))

Element nastavitve	Priporočena nastavitev
[Enable SSL] (Omogoči protokol SSL)	VKLOP

2.1.8 SMTP

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [E-mail Setting] (Nastavitev e-pošte) - [E-mail TX (SMTP)] (Pošiljanje e-pošte (SMTP))

Element nastavitve	Priporočena nastavitev
[SSL/TLS Settings] (Nastavitve protokola SSL/TLS)	[SMTP over SSL] (SMTP prek SSL)

2.1.9 Prev. pristnosti IEEE802.1X

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [IEEE802.1X Authentication Setting] (Nastavitev preverjanja pristnosti IEEE802.1X) - [IEEE802.1X Authentication Setting] (Nastavitev preverjanja pristnosti IEEE802.1X) - [Supplicant Setting] (Nastavitev prosilca)

Element nastavitve	Priporočena nastavitev
[EAP-Type]	Izberite [EAP-TLS], [EAP-TTLS] ali [PEAP].

2.1.10 LDAP

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [LDAP Setting] (Nastavitev protokola LDAP) - [Setting Up LDAP] (Namestitev protokola LDAP)

Element nastavitve	Priporočena nastavitev
[Enable SSL] (Omogoči protokol SSL)	VKLOP

2.1.11 TCPSocket

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [TCP Socket Setting] (Nastavitev vtičnice TCPSocket)

Element nastavitve	Priporočena nastavitev
[Use SSL/TLS] (Uporabite protokol SSL/TLS)	VKLOP

2.2 Drugo šifriranje

Priporočamo, da konfigurirate naslednje nastavitve, da zmanjšate tveganje za ranljivosti. Podrobnosti o vseh nastavitvah funkcij so na voljo v naslednjih poglavjih.

Funkcija	Priporočena nastavitvev
SMBServer	Šifriranje prek protokola SMB, Podpis SMB
SMBCClient	Preverjanje pristnosti Kerberos
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	VKLOP

2.2.1 SMBServer

Z uporabo šifriranja prek protokola SMB in podpisa SMB lahko zmanjšate naslednja varnostna tveganja.

- Prisluškovanje: Zlonamerna tretja stran lahko prestreže komunikacijo in ukrade osebne podatke ali zaupne informacije.
- Poseganje v podatke: Obstaja tveganje za napad vrinjenega napadalca (MITM) in poseganje v podatke.
- Slepjenje: Če so podatki za preverjanje pristnosti ukradeni, se lahko tretja stran izda za legitimnega uporabnika in pridobi nepoblaščen dostop.
- Uhajanje informacij: Nešifrirano komunikacijo je mogoče zlahka presteči, zlasti v javnih brezžičnih omrežjih, kar povečuje tveganje za uhajanje osebnih podatkov in podatkov o kreditnih karticah.

Šifriranje prek protokola SMB

Zahteve

- Ustvarite javni uporabniški predal. Poleg tega konfigurirajte nastavitve na samodejni prenos datotek iz javnega uporabniškega predala in shranjevanje teh datotek v protokol SMB.
- Določite geslo za uporabniški predal.

Nastavitve lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Box] (Predal) - [User Box List] (Seznam uporabniških predalov)

Element nastavitve	Priporočena nastavitvev
[SMB Communication Encryption] (Šifriranje komunikacije prek protokola SMB)	[Encrypt] (Šifriraj)

Podpis SMB

Nastavitve lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [SMB Setting] (Nastavitve protokola SMB) - [SMB Server Settings] (Nastavitve strežnika SMB)

Element nastavitve	Priporočena nastavitvev
[SMB security Signature Setting] (Nastavitve varnostnega podpisa SMB)	[Obvezno]

2.2.2 SMBClient

Preverjanje pristnosti Kerberos uporablja močno tehnologijo šifriranja, ki med postopkom preverjanja pristnosti znatno zmanjša tveganje za krajo poverilnic. Zagotavlja tudi neokrnjenost podatkov, saj preprečuje poseganje v podatke med pošiljateljem in prejemnikom ter napade s posredovanjem NTLM.

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [SMB Setting] (Nastavitev protokola SMB) - [Client Setting] (Nastavitve odjemalca)

Element nastavitve	Priporočena nastavitev
[SMB Authentication Setting] (Nastavitev preverjanja pristnosti protokola SMB)	[Kerberos]

2.2.3 SNMP

Nastavite šifriranje prek protokola SNMPv3. Varnost lahko povečate tudi z nastavitvijo preverjanja pristnosti. Varnostna tveganja so približno enaka kot pri protokolu SMB.

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [SNMP Setting] (Nastavitev protokola SNMP)

Element nastavitve	Priporočena nastavitev
[SNMP Setting] (Nastavitev protokola SNMP)	[SNMP v3(IP)]
[Encryption Algorithm] (Algoritem šifriranja)	[AES-128]
[Authentication Method] (Metoda preverjanja pristnosti)	Izberite [SHA-256], [SHA-384] ali [SHA-512].

2.2.4 IPsec

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [TCP/IP Setting] (Nastavitev zbirke TCP/IP) - [IPsec] - [IPsec Setting] (Nastavitev zbirke IPsec)

[IKEv2]

Element nastavitve	Priporočena nastavitev
[Encryption Algorithm] (Algoritem šifriranja)	[AES-CBC] ([256]/[192 and 256] (192 in 256)/[All] (Vse))
[Authentication Algorithm] (Algor. prever. pristnosti)	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 in 384)/[384 and 512] (384 in 512)/[All] (Vse)), [AES-XCBC]
[Diffie-Hellman Group] (Skupina Diffie-Hellman)	[Group 14] (Skupina 14), [Group 19] (Skupina 19)

[SA]

Element nastavitve	Priporočena nastavitev
[Encapsulation Mode] (Način za inkapsulacijo)	[Tunnel] (Tunel), [Transport]
[Security Protocol] (Varnostni protokol)	[ESP]
[Key Exchange Method] (Način izmenjave ključa)	[IKEv2]
[Authentication Method] (Metoda preverjanja pristnosti)	[Digital Signature] (Digitalni podpis)

Element nastavitve	Priporočena nastavitev
[ESP Encryption Algorithm] (Algoritem šifriranja prek protokola ESP)	[AES-GCM] ([256]/[192 and 256] (192 in 256)/[All] (Vse)), [AES-GCM-64] ([256]/[192 and 256] (192 in 256)/[All] (Vse)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 in 256)/[All] (Vse))
[Perfect Forward Secrecy] (Popolna tajnost posredovanja)	VKLOP
[Diffie-Hellman Group(IKEv2)] (Skupina Diffie-Hellman (IKEv2)) - [Priority1-4] (Prioriteta 1-4)	[Group 14] (Skupina 14), [Group 19] (Skupina 19)

2.2.5 S/MIME

Če pri pošiljanju e-poštnih sporočil uporabljate izbirni protokol S/MIME, lahko vsebino e-poštnega sporočila šifirate in tako preprečite prisluškovanje, identiteto pošiljatelja pa lahko preverite z digitalnim podpisom. To je učinkovit ukrep za preprečevanje spleljenja in prevar lažnega predstavljanja.

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [E-mail Setting] (Nastavitve e-pošte) - [S/MIME]

Element nastavitve	Priporočena nastavitev
[Digital Signature] (Digitalni podpis)	[Always add signature] (Vedno dodaj podpis)
[Digital Signature Type] (Vrsta digitalnega podpisa)	[SHA-256]
[E-Mail Text Encrypt. Method] (Način šifriranja e-poštnega besedila)	[AES-256]

3 Nastavitev preverjanja certifikata

Pri uporabi šifrirane komunikacije prek protokola TLS priporočamo uporabo preverjanje certifikata, saj boste tako zmanjšali vpliv napadov vrinenega napadalca. Priporočamo, da za veljaven dokaz preverjanja nastavite vsaj datum poteka in verigo certifikata.

Povezovanje z zastarelim okoljem, ki nima funkcije preverjanja certifikata, predstavlja večje tveganje za napade vrinenega napadalca. Priporočamo uporabo v varnem omrežnem okolju.

Preverjanje certifikata naprave VFT je priporočljivo pri naslednjih funkcijah odjemalca naprave VFT. Podrobnosti o nastavitvi lokacije so na voljo v naslednjih poglavjih.

POP, SMTP (Začetek TLS/SMTP prek SSL), Prev. pristnosti IEEE802.1X (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel



Nasveti

Preverjanje certifikata odjemalca, ki je priključen na napravo VFT, je priporočljivo v naslednjih funkcijah strežnika VFT.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCPSocket

3.1 POP

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [E-mail Setting] (Nastavitev e-pošte) - [E-mail RX (POP)] (Prejem e-pošte (POP))

Element nastavitve	Priporočena nastavitev
[Certificate Verification Level Settings] (Nastavitve stopnje preverjanja certifikata)	[Expiration Date] (Datum poteka): VKLOP [Chain] (Veriga): VKLOP

3.2 SMTP

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [E-mail Setting] (Nastavitev e-pošte) - [E-mail TX (SMTP)] (Pošiljanje e-pošte (SMTP))

Element nastavitve	Priporočena nastavitev
[Certificate Verification Level Settings] (Nastavitve stopnje preverjanja certifikata)	[Expiration Date] (Datum poteka): VKLOP [Chain] (Veriga): VKLOP

3.3 Prev. pristnosti IEEE802.1X

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [IEEE802.1X Authentication Setting] (Nastavitev preverjanja pristnosti IEEE802.1X) - [IEEE802.1X Authentication Setting] (Nastavitev preverjanja pristnosti IEEE802.1X) - [Supplicant Setting] (Nastavitev prosilca)

Element nastavitve	Priporočena nastavitev
[Certificate Verification Level Settings] (Nastavitve stopnje preverjanja certifikata)	[Expiration Date] (Datum poteka): VKLOP [Chain] (Veriga): VKLOP

3.4 IPsec

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [TCP/IP Setting] (Nastavitev zbirke TCP/IP) - [IPsec] - [Enable IPsec] (Omogoči zbirko IPsec)

Element nastavitve	Priporočena nastavitev
[Certificate Verification Level Settings] (Nastavitve stopnje preverjanja certifikata)	[Expiration Date] (Datum poteka): [Confirm] (Potrdi) [Chain] (Veriga): [Confirm] (Potrdi)



Nasveti

V možnosti [IPsec Setting] (Nastavitev zbirke IPsec) vnaprej shranite možnosti [IKE], [SA], [Peer] (Vrstnik) in [Protocol Setting] (Nastavitev protokola).

3.5 WebDAVClient

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [WebDAV Settings] (Nastavitve protokola WebDAV) - [WebDAVClient Settings] (Nastavitve aplikacije WebDAVClient)

Element nastavitve	Priporočena nastavitev
[Certificate Verification Level Settings] (Nastavitve stopnje preverjanja certifikata)	[Expiration Date] (Datum poteka): VKLOP [Chain] (Veriga): VKLOP

3.6 LDAP

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [LDAP Setting] (Nastavitev protokola LDAP) - [Setting Up LDAP] (Namestitev protokola LDAP)

Element nastavitve	Priporočena nastavitev
[Certificate Verification Level Settings] (Nastavitve stopnje preverjanja certifikata)	[Expiration Date] (Datum poteka): VKLOP [Chain] (Veriga): VKLOP

3.7 DPWS

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [DPWS Settings] (Nastavitve protokola DPWS) - [DPWS Common Settings] (Skupne nastavitve protokola DPWS)

Element nastavitve	Priporočena nastavitev
[Certificate Verification Level Settings] (Nastavitve stopnje preverjanja certifikata)	[Expiration Date] (Datum poteka): VKLOP [Chain] (Veriga): VKLOP

3.8 OpenAPI

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [OpenAPI Setting] (Nastavitev standarda OpenAPI) - [OpenAPI Setting] (Nastavitev standarda OpenAPI)

Element nastavitve	Priporočena nastavitev
[Certificate Verification Level Settings] (Nastavitve stopnje preverjanja certifikata)	[Expiration Date] (Datum poteka): VKLOP [Chain] (Veriga): VKLOP

3.9 RemotePanel

Nastavitev lokacije: [Utility] (Nastavitve) - [Administrator] (Skrbnik) - [Network] (Omrežje) - [Remote Panel Settings] (Nastavitve oddaljene plošče) - [Remote Panel Client Settings] (Nastavitve odjemalca RemotePanel)

Element nastavitve	Priporočena nastavitev
[Certificate Verification Level Settings] (Nastavitve stopnje preverjanja certifikata)	[Expiration Date] (Datum poteka): VKLOP [Chain] (Veriga): VKLOP

4 Dodatne varnostne informacije

4.1 Priporočilo za najboljšo prakso

Priporočamo uporabo algoritmov šifriranja, ki so skladni z nastavitvami najboljše prakse, priporočenimi v smernicah za kriptografijo EUCC in so sprejeti kot mehanizmi šifriranja v sporazumu SOGIS.

Spodaj je seznam algoritmov šifriranja in dolžin ključev, ki so priporočeni v smernicah za kriptografijo EUCC in so sprejeti kot mehanizmi šifriranja v sporazumu SOGIS.

Element	Priporočena nastavitvev
Algoritmi šifriranja	AES (napredni standard šifriranja) RSA (Rivest-Shamir-Adleman) SHA-2 (algoritem varnega razprševanja 2) ECC (kriptografija eliptičnih krivulj) HMAC (koda za preverjanje pristnosti sporočila na podlagi razprševanja)
Dolžina šifrirnega ključa	RSA: 2048 bitov ali več ECC: 256 bitov ali več AES: 256 bitov

Nasveti

Podrobnosti so na voljo v najnovejših smernicah za kriptografijo EUCC in v sporazumu SOGIS.

4.2 Previdnostni ukrepi za komunikacijo z zastarelimi sistemi

Za komunikacijo z zastarelimi sistemi se predvidoma uporabljajo naslednji protokoli in različice.

Z uporabo zastarelih nastavitev je večje tveganje za varnost, zato naprave uporabljajte v varnem omrežnem okolju.

Element	Zastarele nastavitve
Protokol	SLP FTP SMB (različica 3.0 ali starejša, NTLMv1/v2) SNMPv1/v2 Prev. pristnosti IEEE802.1X (EAP-TYPE: Odvisno od strežnika/IZKLOP) DPWS TCPsocket
Algoritmi šifriranja	SHA-1 (algoritem varnega razprševanja 1) DES (standard šifriranja podatkov) 3DES (standard trojnega šifriranja podatkov) RC2-40 (šifra D51Rivest) RC2-64 (šifra D51Rivest) RC2-128 (šifra D51Rivest)
Dolžina šifrirnega ključa	RSA: 1024 bitov ali manj ECC: 160 bitov ali manj AES: 128 bitov ali manj DES: 56 bitov 3DES: 112 bitov

Zastarele nastavitve zbirke IPsec

[IKEv1]

Element nastavitve	Zastarele nastavitve
[Encryption Algorithm] Algoritem šifriranja	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 in 192))
[Authentication Algorithm] (Algor. prever.pristnosti)	Ni v uporabi
[Diffie-Hellman Group] (Skupina Diffie-Hellman)	[Group 1] (Skupina 1), [Group 2] (Skupina 2), [Group 5] (Skupina 5)

[IKEv2]

Element nastavitve	Zastarele nastavitve
[Encryption Algorithm] (Algoritem šifriranja)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 in 192))
[Authentication Algorithm] (Algor. prever.pristnosti)	Ni v uporabi
[Diffie-Hellman Group] (Skupina Diffie-Hellman)	[Group 1] (Skupina 1), [Group 2] (Skupina 2), [Group 5] (Skupina 5)

[SA]

Element nastavitve	Zastarele nastavitve
[Key Exchange Method] (Način izmenjave ključa)	[IKEv1]
[Authentication Method] (Metoda preverjanja pristnosti)	[Digital Signature] (Digitalni podpis)

Element nastavitve	Zastarele nastavitve
[ESP Encryption Algorithm] (Algoritem šifriranja prek protokola ESP)	[3DES-CBC] ([128]/[192]/[128 and 192] (128 in 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 in 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 in 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 in 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 in 192))
[Perfect Forward Secrecy] (Popolna tajnost posredovanja)	VKLOP
[Diffie-Hellman Group(IKEv1)] (Skupina Diffie-Hellman (IKEv1))	[Group 1] (Skupina 1), [Group 2] (Skupina 2), [Group 5] (Skupina 5)

4.3 Tovarniško dobavljeni omrežni vmesniki in storitve

Vrsta storitve	Protokol	Številka vrat
DHCP	UDP	68
Strežnik HTTP	TCP	80
Storitev imena NETBIOS	UDP	137
Storitev datagrama NETBIOS	UDP	138
SNMP	UDP	161
Strežnik HTTP prek SSL/IPP prek SSL	TCP	443
Tiskanje LPD	TCP	515
DHCPv6 Client	UDP	546
Tiskanje IPP	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (orodje IWS)	TCP	8091
Tiskanje RAW	TCP	9100
Tiskanje RAW	TCP	9112
Tiskanje RAW	TCP	9113
Tiskanje RAW	TCP	9114
Tiskanje RAW	TCP	9115
Tiskanje RAW	TCP	9116
OpenAPI	TCP	50001

4.4 O vnosu preverjanja

Za podatke o številu znakov, ki jih je treba navesti za omrežne nastavitve itd., glejte elemente za nastavitve v priročniku za uporabo.

Največji dovoljeni vnos za elemente, ki podpirajo večbitne znake (podatki, shranjeni v napravi VFT) je odvisen od kodiranja jezika in je lahko do trikratno število znakov.

Rekommendationer för säkra nätverksanslutna enheter

Innehållsförteckning

1 Setting the IP Address Filtering

1.1	IP Address Filtering.....	3
1.2	Quick IP Filtering.....	3

2 Setting the Encrypted Communication

2.1	TLS encryption	4
2.1.1	HTTP (Web Connection)	4
2.1.2	WebDAVServer	4
2.1.3	IPP.....	5
2.1.4	OpenAPI.....	5
2.1.5	RemotePanel.....	5
2.1.6	DPWS.....	5
2.1.7	POP.....	5
2.1.8	SMTP	5
2.1.9	IEEE802.1X Auth	5
2.1.10	LDAP	6
2.1.11	TCP Socket.....	6
2.2	Other encryption	7
2.2.1	SMBServer.....	7
	SMB Encryption.....	7
	SMB Signature.....	7
2.2.2	SMBClient.....	8
2.2.3	SNMP	8
2.2.4	IPsec	8
2.2.5	S/MIME	9

3 Setting the Certificate Validation

3.1	POP.....	10
3.2	SMTP.....	10
3.3	IEEE802.1X Auth.....	10
3.4	IPsec.....	10
3.5	WebDAVClient	11
3.6	LDAP.....	11
3.7	DPWS	11
3.8	OpenAPI	11
3.9	RemotePanel	11

4 Additional Security Information

4.1	Recommendation of best practice.....	12
4.2	Precautions for communicating with legacy systems	13
	IPsec legacy settings	13
4.3	Network interfaces and services available from factory shipment.....	14
4.4	About input validation.....	15



Om denna handbok

Denna handbok innehåller information och inställningar som möjliggör säker användning av enheter.

Om basenheten är ansluten till ett nätverk ska miljön skyddas av en brandvägg. Vi rekommenderar även att ställa in en privat IP-adress för basenhetens IP-adress.

Med en privat IP-adress får endast användare i ett lokalt nätverk, som internt LAN, åtkomst till basenheten, vilket förhindrar obehörig åtkomst utifrån.

Om du måste använda en global IP-adress ska basenheten installeras bakom en brandvägg.

1 Inställning av IP-filtrering

IP-filtrering är en funktion som begränsar vilka enheter som har åtkomst till basenheten via IP-adressen. När denna funktion är korrekt inställd kan du begränsa åtkomst från obehöriga enheter.

IP-filtreringsfunktionen kan ställas in på två sätt.

1.1 IP-filtrering

Ange ett IP-adressintervall för IP-adresser som ska nekas eller tillåtas åtkomst.

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [TCP/IP Setting] (TCP/IP-inställning) - [IP Address Filtering] (IP-filtrering)



Tips

Ställ in IP-adresserna som ska tillåtas eller nekas för att passa din miljö.

1.2 Snabb IP-filtrering

Intervallet av IP-adresser som medges åtkomst konfigureras automatiskt utifrån den IP-adress och nätmask som har ställts in i basenheten.

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [TCP/IP Setting] (TCP/IP-inställning) - [Quick IP Filtering] (Snabb IP-filtrering)

Rekommenderade inställningar: [Synchronize IP Address] (Synkronisera IP-adress)/[Synchronize Subnet Mask] (Synkronisera delnätmask)*

*Välj den som passar din miljö.

2 Inställning av krypterad kommunikation

Vi rekommenderar att du använder följande krypterade kommunikation för att förhindra att data avlyssnas, data manipuleras och sessioner kapas.

2.1 TLS-kryptering

Vi rekommenderar att du konfigurerar följande inställningar för att minska sårbarheten.

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Security] (Säkerhet) - [PKI Settings] (PKI-inställningar) - [Enable SSL Version] (Aktivera SSL-version)

Inställningspost	Rekommenderad inställning
[Mode using SSL/TLS]	[Admin. Mode and User Mode] (Administratörsläge och användarläge)
[SSL/TLS Version Setting] (Inställning av SSL/TLS-version)	TLS1.2 TLS1.3 (IEEE802.1X inkompatibel)
[Encryption Strength] (Krypteringsstyrka)	AES-256

Det första certifikatet installeras på fabriken. Om du behöver ett annat certifikat, registrera det nya på följande plats.

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Security] (Säkerhet) - [PKI Settings] (PKI-inställningar) - [Device Certificate Setting] (Enhetscertifikatsinställning)

Inställningspost	Rekommenderad inställning
[Encryption Key Type] (Typ av krypteringsnyckel)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

TLS-krypteringen är kompatibel med följande protokoll och tjänster. För mer information om inställningens sökväg, se följande avsnitt.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP via SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP Socket

2.1.1 HTTP (Web Connection)

Om du aktiverar [Enable SSL Version] (Aktivera SSL-version) kommer kommunikationsläget automatiskt växla till TLS-krypterad kommunikation (HTTPS).

2.1.2 WebDAVServer

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [WebDAV Settings] (WebDAV-inställningar) - [WebDAV Server Settings] (WebDAV-serverinställningar)

Inställningspost	Rekommenderad inställning
[SSL Settings] (SSL-inställningar)	[Endast SSL]

2.1.3 IPP

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [HTTP Server Settings] (HTTP-serverinställningar)

Inställningspost	Rekommenderad inställning
[IPP-SSL Settings] (IPP-SSL-inställningar)	[Endast SSL]

2.1.4 OpenAPI

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [OpenAPI Setting] (OpenAPI-inställning) - [OpenAPI Setting] (OpenAPI-inställning)

Inställningspost	Rekommenderad inställning
[SSL/Port Settings] (SSL/portinställningar)	[Endast SSL]

2.1.5 RemotePanel

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [Remote Panel Settings] (Fjärrpanelsinställningar) - [Remote Panel Server Settings] (Fjärrpanelsserverinställningar)

Inställningspost	Rekommenderad inställning
[Port No.(SSL)] (Portnummer (SSL))	[50443]



Tips

Om du aktiverar [Enable SSL Version] (Aktivera SSL-version) kommer kommunikationen automatiskt växla till TLS-krypterat läge. Ange ett portnummer.

2.1.6 DPWS

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [DPWS Settings] (DPWS-inställningar) - [DPWS Common Settings] (DPWS-grundinställningar)

Inställningspost	Rekommenderad inställning
[SSL Settings] (SSL-inställningar)	PÅ

2.1.7 POP

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [E-mail Setting] (E-postinställning) - [E-mail RX (POP)] (E-postmottagning (POP))

Inställningspost	Rekommenderad inställning
[Aktivera SSL]	PÅ

2.1.8 SMTP

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [E-mail Setting] (E-postinställning) - [E-mail TX (SMTP)] (E-postsändning (SMTP))

Inställningspost	Rekommenderad inställning
[SSL/TLS-inställningar]	[SMTP via SSL]

2.1.9 IEEE802.1X Auth

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentiseringsinställning) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentiseringsinställning) - [Supplicant Setting] (Supplikantinställning)

Inställningspost	Rekommenderad inställning
[EAP-Type]	Välj [EAP-TLS], [EAP-TTLS] eller [PEAP].

2.1.10 LDAP

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [LDAP Setting] (LDAP-inställning) - [Setting Up LDAP] (Ange LDAP)

Inställningspost	Rekommenderad inställning
[Aktivera SSL]	PÅ

2.1.11 TCP Socket

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [TCP Socket Setting] (TCP-socketinställning)

Inställningspost	Rekommenderad inställning
[Use SSL/TLS]	PÅ

2.2 Annan kryptering

Vi rekommenderar att du konfigurerar följande inställningar för att minska sårbarheten. För mer information om varje funktions inställningar, se följande avsnitt.

Funktion	Rekommenderad inställning
SMBServer	SMB-mappkryptering, SMB-signatur
SMBClient	Kerberos-autentisering
SNMP	SNMPv3
IPSEC	IKEv2
S/MIME	PÅ

2.2.1 SMBServer

Att använda SMB-mappkryptering och SMB-signatur kan reducera följande säkerhetsrisker.

- Avlyssning: En fientlig tredje part kan fånga upp kommunikation och stjäla personlig eller sekretessbelagd information.
- Manipulering av data: Det finns en risk att innehållet i kommunikationen kan manipuleras med en Man-In-The-Middle Attack (MITM).
- Förfalskade identiteter: Om autentiseringsinformation blir stulen kan en tredje part använda uppgifterna för en godkänd användare för att få obehörig åtkomst.
- Informationsläckor: Okrypterad information kan lätt fångas upp, särskilt i öppna WiFi-nätverk, vilket ökar risken för läckor av personlig information och kreditkortsinformation.

SMB-mappkryptering

Förutsättningar

- Skapa en offentlig användarbox. Konfigurera även inställningen så att den automatiskt överför filer från den offentliga användarboxen och sparar dem i SMB-mappen.
- Ange lösenordet för användarboxen.

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Box] (Användarbox) - [User Box List] (Användarboxlista)

Inställningspost	Rekommenderad inställning
[SMB Communication Encryption] (SMB-kommunikationskryptering)	[Kryptera]

SMB-signatur

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [SMB Setting] (SMB-inställning) - [SMB Server Settings] (SMB-serverinställning)

Inställningspost	Rekommenderad inställning
[SMB security Signature Setting] (SMB-säkerhets-signaturinställning)	[Obligatoriskt]

2.2.2 SMBClient

Kerberos-autentiseringen använder stark krypteringsteknik som markant reducerar risken för behörighetsstöld under autentiseringsprocessen. Den säkerställer även datasekretess och förhindrar att data manipuleras mellan sändaren och mottagaren samt NTLM-reläattacker.

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [SMB Setting] (SMB-inställning) - [Client Setting] (Klientinställning)

Inställningspost	Rekommenderad inställning
[SMB Authentication Setting] (SMB-autentiseringsinställning)	[Kerberos]

2.2.3 SNMP

Ställ in krypteringen med SNMPv3. Om även autentiseringsinställningen läggs till kan du öka säkerheten ytterligare. Säkerhetsriskerna är ungefär de samma som med SMB.

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [SNMP Setting] (SNMP-inställning)

Inställningspost	Rekommenderad inställning
[SNMP Setting] (SNMP-inställning)	[SNMP v3(IP)]
[Krypteringsalgoritm]	[AES-128]
[Authentication Method] (Autentiseringsmetod)	Välj [SHA-256], [SHA-384] eller [SHA-512].

2.2.4 IPSEC

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [TCP/IP Setting] (TCP/IP-inställning) - [IPsec] - [IPsec Setting] (IPsec-inställning)

[IKEv2]

Inställningspost	Rekommenderad inställning
[Krypteringsalgoritm]	[AES-CBC] ([256]/[192 and 256] (192 och 256)/[All] (Alla))
[Verifieringsalgoritm]	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 och 384)/[384 and 512] (384 och 512)/[All] (Alla)), [AES-XCBC]
[Diffie-Hellman-grupp]	[Group 14] (Grupp 14), [Group 19] (Grupp 19)

[SA]

Inställningspost	Rekommenderad inställning
[Inkapslingsläge]	[Tunnel], [Transport]
[Säkerhetsprotokoll]	[ESP]
[Metod för nyckelutbyte]	[IKEv2]
[Authentication Method] (Autentiseringsmetod)	[Digital signatur]
[ESP Krypteringsalgoritm]	[AES-GCM] ([256]/[192 and 256] (192 och 256)/[All] (Alla)), [AES-GCM-64] ([256]/[192 and 256] (192 och 256)/[All] (Alla)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 och 256)/[All] (Alla))
[Perfekt fram. sekretess]	PÅ

Inställningspost	Rekommenderad inställning
[Diffie-Hellman Group(IKEv2)] (Diffie-Hellman-grupp(IKEv2) - [Priority1-4] (Prioritet 1-4)	[Group 14] (Grupp 14), [Group 19] (Grupp 19)

2.2.5 S/MIME

Om du använder alternativet S/MIME när du skickar e-post kan du kryptera innehållet i e-posten för att förhindra avlyssning och för att kontrollera avsändarens identitet med en elektronisk signatur. Detta är en effektiv åtgärd mot förfälskade identiteter och nätfiske.

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [E-mail Setting] (E-postinställning) - [S/MIME] (S/MIME)

Inställningspost	Rekommenderad inställning
[Digital signatur]	[Always add signature] (Lägg alltid till signatur)
[Digital Signature Type] (Digital signaturtyp)	[SHA-256]
[E-Mail Text Encrypt. Method] (Krypteringsmetod för e-posttext)	[AES-256]

3 Inställning av certifikatvalidering

När TLS-krypterad kommunikation används för att reducera påverkan från man-in-the-middle-attacker rekommenderar vi att du använder certifikatvalidering. För valideringsposter rekommenderar vi att du aktiverar certifikatets utgångsdatum och certifikatkedjan som minimum.

Vid ett försök att ansluta till en föråldrad miljö som inte har någon certifikatvalideringsfunktion ökar risken för man-in-the-middle-attacker. Vi rekommenderar att du använder den i en säker nätverksmiljö.

Certifikatvalidering på MFP-sidan rekommenderas i följande MFP-klientfunktioner. För mer information om inställningens sökväg, se följande avsnitt.

POP, SMTP (Start TLS/SMTP via SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel



Tips

Certifikatvalidering på klientsidan som är ansluten till MFP rekommenderas i följande MFP-serverfunktioner. HTTP (Web Connection/WebDAV/IPP/DPWS/OpenAPI/RemotePanel), TCP Socket

3.1 POP

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [E-mail Setting] (E-postinställning) - [E-mail RX (POP)] (E-postmottagning (POP))

Inställningspost	Rekommenderad inställning
[Certificate Verification Level Settings] (Inställning för certifikatverifieringsnivå)	[Expiration Date] (Utgångsdatum): PÅ [Chain] (Kedja): PÅ

3.2 SMTP

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [E-mail Setting] (E-postinställning) - [E-mail TX (SMTP)] (E-postsändning (SMTP))

Inställningspost	Rekommenderad inställning
[Certificate Verification Level Settings] (Inställning för certifikatverifieringsnivå)	[Expiration Date] (Utgångsdatum): PÅ [Chain] (Kedja): PÅ

3.3 IEEE802.1X Auth

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentiseringsinställning) - [IEEE802.1X Authentication Setting] (IEEE802.1X autentiseringsinställning) - [Supplicant Setting] (Supplikantinställning)

Inställningspost	Rekommenderad inställning
[Certificate Verification Level Settings] (Inställning för certifikatverifieringsnivå)	[Expiration Date] (Utgångsdatum): PÅ [Chain] (Kedja): PÅ

3.4 IPSEC

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [TCP/IP Setting] (TCP/IP-inställning) - [IPsec] (IPsec) - [Enable IPsec] (Aktivera IPsec)

Inställningspost	Rekommenderad inställning
[Certificate Verification Level Settings] (Inställning för certifikat-verifieringsnivå)	[Expiration Date] (Utgångsdatum): [Bekräfta] [Chain] (Kedja): [Bekräfta]



Tips

I [IPsec Setting] (IPsec-inställning), registrera posterna [IKE], [SA], [Peer] (P2P-nod) och [Protocol Setting] (Protokollinställning) i förväg.

3.5 WebDAVClient

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [WebDAV Settings] (WebDAV-inställningar) - [WebDAV Client Settings] (WebDAV-klientinställningar)

Inställningspost	Rekommenderad inställning
[Certificate Verification Level Settings] (Inställning för certifikat-verifieringsnivå)	[Expiration Date] (Utgångsdatum): PÅ [Chain] (Kedja): PÅ

3.6 LDAP

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [LDAP Setting] (LDAP-inställning) - [Setting Up LDAP] (Ange LDAP)

Inställningspost	Rekommenderad inställning
[Certificate Verification Level Settings] (Inställning för certifikat-verifieringsnivå)	[Expiration Date] (Utgångsdatum): PÅ [Chain] (Kedja): PÅ

3.7 DPWS

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [DPWS Settings] (DPWS-inställningar) - [DPWS Common Settings] (DPWS-grundinställningar)

Inställningspost	Rekommenderad inställning
[Certificate Verification Level Settings] (Inställning för certifikat-verifieringsnivå)	[Expiration Date] (Utgångsdatum): PÅ [Chain] (Kedja): PÅ

3.8 OpenAPI

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [OpenAPI Setting] (OpenAPI-inställning) - [OpenAPI Setting] (OpenAPI-inställning)

Inställningspost	Rekommenderad inställning
[Certificate Verification Level Settings] (Inställning för certifikat-verifieringsnivå)	[Expiration Date] (Utgångsdatum): PÅ [Chain] (Kedja): PÅ

3.9 RemotePanel

Inställningens sökväg: [Utility] (Hjälp) - [Administrator] (Administratör) - [Network] (Nätverk) - [Remote Panel Settings] (Fjärrpanelsinställningar) - [Remote Panel Client Settings] (Fjärrpanelsklientinställningar)

Inställningspost	Rekommenderad inställning
[Certificate Verification Level Settings] (Inställning för certifikatverifieringsnivå)	[Expiration Date] (Utgångsdatum): PÅ [Chain] (Kedja): PÅ

4 Ytterligare säkerhetsinformation

4.1 Rekommenderade bästa metoder

Vi rekommenderar att krypteringsalgoritmerna används i enlighet med inställningarna som rekommenderas som bästa metoder i EUCC:s riktlinjer för kryptografi och SOGIS godkända kryptografiska mekanismer.

Nedan finns en lista över krypteringsalgoritmer och nyckellängder som rekommenderas av EUCC:s riktlinjer för kryptografi och SOGIS godkända kryptografiska mekanismer.

Alternativ	Rekommenderad inställning
Krypteringsalgoritmer	AES (Advanced Encryption Standard) RSA (Rivest-Shamir-Adleman) SHA-2 (Secure Hash Algorithm 2) ECC (Elliptic Curve Cryptography) HMAC (Hash-based Message Authentication Code)
Krypteringsnyckellängd	RSA: 2048 bitar eller mer ECC: 256 bitar eller mer AES: 256 bitar

Tips

För mer information, se senaste EUCC:s riktlinjer för kryptografi och SOGIS godkända kryptografiska mekanismer.

4.2 Försiktighetsåtgärder för kommunikation med föråldrade system

Följande protokoll och versioner förmodas användas för kommunikation med föråldrade system.

Att använda föråldrade system ökar säkerhetsriskerna, använd dem därför i en säker nätverksmiljö.

Alternativ	Inställningar för föråldrade system
Protokoll	SLP FTP SMB (3.0 eller äldre version, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Beroende på server/OFF) DPWS TCPsocket
Krypteringsalgoritmer	SHA-1 (Secure Hash Algorithm 1) DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Krypteringsnyckellängd	RSA: 1024 bitar eller mindre ECC: 160 bitar eller mindre AES: 128 bitar eller mindre DES: 56 bitar 3DES: 112 bitar

IPsec-inställningar för föråldrade system

[IKEv1]

Inställningspost	Inställningar för föråldrade system
[Krypteringsalgoritm]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 och 192))
[Verifieringsalgoritm]	Används inte
[Diffie-Hellman-grupp]	[Group 1] (Grupp 1), [Group 2] (Grupp 2), [Group 5] (Grupp 5)

[IKEv2]

Inställningspost	Inställningar för föråldrade system
[Krypteringsalgoritm]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 och 192))
[Verifieringsalgoritm]	Används inte
[Diffie-Hellman-grupp]	[Group 1] (Grupp 1), [Group 2] (Grupp 2), [Group 5] (Grupp 5)

[SA]

Inställningspost	Inställningar för föråldrade system
[Metod för nyckelutbyte]	[IKEv1]
[Authentication Method] (Autentiseringsmetod)	[Digital signatur]
[ESP Krypteringsalgoritm]	[3DES-CBC] ([128]/[192]/[128 and 192] (128 och 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 och 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 och 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 och 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 och 192))
[Perfekt fram. sekretess]	PÅ
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellman-grupp(IKEv1))	[Group 1] (Grupp 1), [Group 2] (Grupp 2), [Group 5] (Grupp 5)

4.3 Nätverksgränssnitt och tjänster som är tillgängliga från leverans från fabrik

Typ av tjänst	Protokoll	Portnummer
DHCP	UDP	68
HTTP-server	TCP	80
NetBIOS-namntjänst	UDP	137
NetBIOS-datagramtjänst	UDP	138
SNMP	UDP	161
HTTP-server via SSL/IPP via SSL	TCP	443
LPD-utskrift	TCP	515
DHCPv6-klient	UDP	546
IPP Print	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-verktyg)	TCP	8091
RAW-utskrift	TCP	9100
RAW-utskrift	TCP	9112
RAW-utskrift	TCP	9113
RAW-utskrift	TCP	9114
RAW-utskrift	TCP	9115
RAW-utskrift	TCP	9116
OpenAPI	TCP	50001

4.4 Om validering av inmatning

För antalet tecken som ska matas in för nätverksinställning med mera, se respektive inställningspost i användarhandboken.

Beroende på språkets kodning kan maximalt tillåten inmatning (data som sparas i MFP) för poster som stödjer tecken med flera bytes vara tre gånger antalet tecken.

Güvenli ağ bağlantılı cihazlar için öneriler

İçindekiler

1 IP Filtreleme Ayarları

1.1	IP filtreleme.....	1-3
1.2	Hızlı IP Filtreleme	1-3

2 Şifreli İletişimi Ayarlama

2.1	TLS şifreleme.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-4
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	UzaktanKumandaPaneli.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-5
2.1.8	SMTP	2-5
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP Soketi	2-6
2.2	Diğer şifreleme	2-7
2.2.1	SMBSunucusu	2-7
	SMB Klasörü Şifreleme	2-7
	SMB İmza.....	2-7
2.2.2	SMBİstemcisi	2-8
2.2.3	SNMP	2-8
2.2.4	IPSEC.....	2-8
2.2.5	S/MIME	2-9

3 Sertifika Doğrulamasını Ayarlama

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPSEC	3-11
3.5	WebDAVİstemcisi.....	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-11
3.9	UzaktanKumandaPaneli	3-12

4 Ek Güvenlik Bilgileri

4.1	En iyi uygulama önerisi.....	4-13
4.2	Eski sistemlerle iletişim kurarken alınması gereken önlemler	4-14
	IPsec eski ayarları	4-14
4.3	Fabrika sevkiyatında mevcut ağ arayüzleri ve hizmetleri.....	4-16
4.4	Giriş doğrulaması hakkında	4-17

Bu kılavuz hakkında

Bu kılavuz, cihazların güvenli kullanımını saęlayan bilgileri ve ayarları açıklamaktadır.

Makineyi aęa baęlarken, güvenlik duvarı ile korunan bir ortamda kullanın. Ayrıca, makinenin IP adresi için özel bir IP adresi ayarlamayı öneririz.

Özel bir IP adresi ayarlamak, yalnızca yerel alan aęı (örneğin, dahili LAN) üzerindeki kullanıcıların makineye erişmesine izin vererek, dışarıdan yetkisiz erişimi engeller.

Global IP adresi kullanmanız gerekiyorsa, makineyi mutlaka bir güvenlik duvarı içine kurun.

1 IP Filtreleme Ayarları

IP filtreleme, makineye erişebilen cihazları IP adresine göre sınırlayan bir işlemdir. Bu işlevi doğru şekilde ayarlamak, yetkisiz cihazların erişimini sınırlamanıza olanak sağlar.

Makinenin IP filtreleme işlevi aşağıdaki iki yöntemle ayarlanabilir.

1.1 IP filtreleme

Erişime izin veren veya engelleyen IP adreslerinin aralığını manuel olarak belirtin.

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [TCP/IP Setting] (TCP/IP Ayarı) - [IP Address Filtering] (IP Filtreleme)



Tavsiyeler

Ortaminıza uygun olarak izin verilecek veya engellenecek IP adreslerini ayarlayın.

1.2 Hızlı IP Filtreleme

Erişime izin verilecek IP adresleri aralığı, makinede ayarlanan IP adresi ve alt ağ maskesine göre otomatik olarak belirlenir.

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [TCP/IP Setting] (TCP/IP Ayarı) - [Quick IP Filtering] (Hızlı IP Filtreleme)

Önerilen ayarlar: [Synchronize IP Address] (IP Adresi Senkronize Et)/[Synchronize Subnet Mask] (Alt Ağ Maskesini Senkronize Et) *

* Ortaminıza uygun olanı seçin.

2 Şifreli İletişimi Ayarlama

Veri dinleme, veri tahrifatı ve oturum ele geçirmeyi önlemek için aşağıdaki şifreli iletişimi kullanmanızı öneririz.

2.1 TLS şifreleme

Güvenlik açıkları riskini azaltmak için aşağıdaki ayarları yapılandırmanızı öneririz.

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Security] (Güvenlik) - [PKI Settings] (PKI Ayarları) - [Enable SSL Version] (SSL Sürümünü Etkinleştir)

Ayar öğesi	Önerilen ayar
[Mode using SSL/TLS]	[Admin. Mode and User Mode] (Yönetici Modu ve Kullanıcı Modu)
[SSL/TLS Version Setting] (SSL/TLS Sürüm Ayarı)	TLS1.2 TLS1.3 (IEEE802.1X uyumsuz)
[Encryption Strength] (Şifreleme Güvenlik Düzeyi)	AES-256

İlk sertifika fabrikada yüklenir. Farklı bir sertifikaya ihtiyacınız varsa, aşağıdaki yerden yeni bir sertifika kaydedin.

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Security] (Güvenlik) - [PKI Settings] (PKI Ayarları) - [Device Certificate Setting] (Cihaz Sertifika Ayarı)

Ayar öğesi	Önerilen ayar
[Encryption Key Type] (Şifreleme Anahtarı Türü)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

TLS şifreleme, aşağıdaki protokoller ve hizmetler için desteklenmektedir. Ayar konuları hakkında detaylı bilgi için aşağıdaki bölümlere bakın.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, UzaktanKumandaPaneli)
- DPWS
- POP
- SMTP (TLS'yi başlat, SSL üzerinden SMTP)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP Soketi

2.1.1 HTTP (Web Connection)

[Enable SSL Version] (SSL Sürümünü Etkinleştir) seçeneğini etkinleştirirseniz, iletişim modu otomatik olarak TLS şifreli iletişime (HTTPS) geçer.

2.1.2 WebDAVServer

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [WebDAV Settings] (WebDAV Ayarları) - [WebDAV Server Settings] (WebDAV Sunucu Ayarları)

Ayar öğesi	Önerilen ayar
[SSL Ayarları]	[Sadece SSL]

2.1.3 IPP

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [HTTP Server Settings] (HTTP Sunucu Ayarları)

Ayar öğesi	Önerilen ayar
[IPP-SSL Settings] (IPP-SSL Ayarları)	[Sadece SSL]

2.1.4 OpenAPI

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [OpenAPI Setting] (OpenAPI Ayarı) - [OpenAPI Setting] (OpenAPI Ayarı)

Ayar öğesi	Önerilen ayar
[SSL/Port Settings] (SSL/Port Ayarları)	[Sadece SSL]

2.1.5 UzaktanKumandaPaneli

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [Remote Panel Settings] (Uzaktan Kumanda Paneli Ayarları) - [Remote Panel Server Settings] (Uzaktan Kumanda Sunucu Ayarları)

Ayar öğesi	Önerilen ayar
[Port No.(SSL)] (Port Numarası (SSL))	[50443]



Tavsiyeler

[Enable SSL Version] (SSL Sürümünü Etkinleştir) seçeneğini etkinleştirirseniz, iletişim otomatik olarak TLS şifreli moda geçer. Bir port numarası belirtin.

2.1.6 DPWS

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [DPWS Settings] (DPWS Ayarları) - [DPWS Common Settings] (DPWS Ortak Ayarları)

Ayar öğesi	Önerilen ayar
[SSL Ayarları]	AÇIK

2.1.7 POP

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [E-mail Setting] (E-posta Ayarı) - [E-mail RX (POP)] (E-posta alımı (POP))

Ayar öğesi	Önerilen ayar
[SSL Geç. Kıl]	AÇIK

2.1.8 SMTP

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [E-mail Setting] (E-posta Ayarı) - [E-mail TX (SMTP)] (E-posta TX (SMTP))

Ayar öğesi	Önerilen ayar
[SSL/TLS Settings] (SSL/TLS Ayarları)	[SSL üzerinden SMTP]

2.1.9 IEEE802.1X Auth

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [IEEE802.1X Authentication Setting] (IEEE802.1X Doğrulama Ayarı) - [IEEE802.1X Authentication Setting] (IEEE802.1X Doğrulama Ayarı) - [Supplicant Setting] (Doğrulama İsteyen Ayar)

Ayar öğesi	Önerilen ayar
[EAP-Type] (EAP Tipi)	[EAP-TLS], [EAP-TTLS], veya [PEAP] seçin.

2.1.10 LDAP

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [LDAP Setting] (LDAP Ayarı) - [Setting Up LDAP] (LDAP Kurulumunu Yap)

Ayar öğesi	Önerilen ayar
[SSL Geç. Kılı]	AÇIK

2.1.11 TCP Soketi

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [TCP Socket Setting] (TCP Soket Ayarı)

Ayar öğesi	Önerilen ayar
[Use SSL/TLS]	AÇIK

2.2 Diğer şifreleme

Güvenlik açıkları riskini azaltmak için aşağıdaki ayarları yapılandırmanızı öneririz. Her bir işlevin ayarları hakkında detaylı bilgi için aşağıdaki bölümlere bakın.

Fonksiyon	Önerilen ayar
SMBSunucusu	SMB Klasörü Şifreleme, SMB İmza
SMBİstemcisi	Kerberos Doğrulama
SNMP	SNMPv3
IPSEC	IKEv2
S/MIME	AÇIK

2.2.1 SMBSunucusu

SMB klasörü şifreleme ve SMB imzası kullanmak aşağıdaki güvenlik risklerini azaltabilir.

- Gizlice dinleme: Kötü niyetli üçüncü şahıslar iletişimi ele geçirebilir ve kişisel veya gizli bilgileri çalabilir.
- Veri tahrifatı: İletişim içeriğinin Aradaki Adam Saldırısı (MITM) ile tahrif edilme riski vardır.
- Sahte e-posta: Doğrulama bilgisi çalınırsa, üçüncü bir taraf meşru bir kullanıcı gibi davranarak yetkisiz erişim sağlayabilir.
- Bilgi sızıntısı: Şifrelenmemiş iletişim, özellikle halka açık Wi-Fi ağlarında kolayca ele geçirilebilir ve bu da kişisel bilgilerin ve kredi kartı bilgilerinin sızdırılma riskini artırır.

SMB Klasörü Şifreleme

Ön Koşullar

- Ortak Kullanıcı Kutusu oluşturun. Ayrıca, dosyaları Ortak Kullanıcı Kutusundan otomatik olarak aktarmak ve SMB klasörüne kaydetmek için ayarı yapılandırın.
- Kullanıcı Kutusu için şifreyi belirtin.

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Box] (Kutu) - [User Box List] (Kullanıcı Kutusu Listesi)

Ayar öğesi	Önerilen ayar
[SMB Communication Encryption] (SMB İletişim Şifreleme)	[Encrypt] (Şifrele)

SMB İmza

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [SMB Setting] (SMB Ayarı) - [SMB Server Settings] (SMB Sunucu Ayarları)

Ayar öğesi	Önerilen ayar
[SMB security Signature Setting] (SMB güvenliği İmza Ayarı)	[Gerekli]

2.2.2 SMBİstemcisi

Kerberos doğrulama, güçlü şifreleme teknolojisi kullanır ve kimlik doğrulama işlemi sırasında kimlik bilgilerinin çalınma riskini önemli ölçüde azaltır. Ayrıca veri bütünlüğünü sağlar, gönderen ve alıcı arasında veri tahrifatını ve NTLM aktarım saldırılarını önler.

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [SMB Setting] (SMB Ayarı) - [Client Setting] (İstemci Ayarı)

Ayar öğesi	Önerilen ayar
[SMB Authentication Setting] (SMB Doğrulama Ayarı)	[Kerberos]

2.2.3 SNMP

SNMPv3 kullanarak şifrelemeyi ayarlayın. Doğrulama ayarı da eklenirse, güvenliği daha da artırabilirsiniz. Güvenlik riskleri SMB ile hemen hemen aynıdır.

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [SNMP Setting] (SNMP Ayarı)

Ayar öğesi	Önerilen ayar
[SNMP Ayarı]	[SNMP v3(IP)]
[Şifreleme Algoritması]	[AES-128]
[Doğrulama metodu]	[SHA-256], [SHA-384], veya [SHA-512] seçin.

2.2.4 IPSEC

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [TCP/IP Setting] (TCP/IP Ayarı) - [IPsec] - [IPsec Setting] (IPsec Ayarı)

[IKEv2]

Ayar öğesi	Önerilen ayar
[Şifreleme Algoritması]	[AES-CBC] ([256]/[192 and 256] (192 ve 256)/[All] (Tümü))
[Doğrulama Algoritması]	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 ve 384)/[384 and 512] (384 ve 512)/[All] (Tümü)), [AES-XCBC]
[Diffie-Hellman Grubu]	[Group 14] (Grup 14), [Group 19] (Grup 19)

[SA]

Ayar öğesi	Önerilen ayar
[Sarma Modu]	[Tunnel] (Tünel), [Transport] (Taşıma)
[Güvenlik Protokolü]	[ESP]
[Key Exchange Method] (Anahtar Değişim Yöntemi)	[IKEv2]
[Doğrulama metodu]	[Dijital İmza]
[ESP Şifrel. Algoritması]	[AES-GCM] ([256]/[192 and 256] (192 ve 256)/[All] (Tümü)), [AES-GCM-64] ([256]/[192 and 256] (192 ve 256)/[All] (Tümü)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 ve 256)/[All] (Tümü))
[Mükemmel İleti Gizliliği]	AÇIK
[Diffie-Hellman Group(IKEv2)] (Diffie-Hellman Grubu(IKEv2)) - [Priority1-4] (Öncelik1-4)	[Group 14] (Grup 14), [Group 19] (Grup 19)

2.2.5 S/MIME

E-posta gönderirken isteğe bağlı S/MIME kullanırsanız, e-posta içeriğini dinlemeye karşı şifreleyebilir ve elektronik imza ile gönderenin kimliğini doğrulayabilirsiniz. Bu, sahtecilik ve kimlik hırsızlığı dolandırıcılığına karşı etkili bir önlemdir.

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [E-mail Setting] (E-posta Ayarı) - [S/MIME]

Ayar öğesi	Önerilen ayar
[Dijital İmza]	[Always add signature] (Her zaman imza ekleyin)
[Digital Signature Type] (Dijital İmza Tipi)	[SHA-256]
[E-Mail Text Encrypt. Method] (E-Posta Metin Şifreleme Yöntemi)	[AES-256]

3 Sertifika Doğrulamasını Ayarlama

TLS ile şifrelenmiş iletişimi kullanırken Aradaki Adam (MITM) saldırılarının etkisini azaltmak için sertifika doğrulamasını kullanmanızı öneririz. Doğrulama öğeleri için, en azından sertifika son kullanma tarihini ve zincirini etkinleştirmenizi öneririz.

Sertifika doğrulama işlevi olmayan eski bir ortama bağlanmaya çalışılırsa, aradaki adam saldırılarının riski artar. Güvenli bir ağ ortamında kullanmanızı öneririz.

Aşağıdaki MFP istemci işlevlerinde MFP tarafında sertifika doğrulaması önerilir. Ayar konumları hakkında detaylı bilgi için aşağıdaki bölümlere bakın.

POP, SMTP (SSL üzerinden TLS/SMTP'yi başlatın), IEEE802.1X Auth (EAP-TİPİ: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, UzaktanKumandaPaneli



Tavsiyeler

MFP'ye bağlı istemci tarafında sertifika doğrulaması, aşağıdaki MFP sunucu işlevlerinde önerilir.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / UzaktanKumandaPaneli), TCP Soketi

3.1 POP

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [E-mail Setting] (E-posta Ayarı) - [E-mail RX (POP)] (E-posta alımı (POP))

Ayar öğesi	Önerilen ayar
[Sertifika Doğrulama Seviyesi Ayarları]	[Expiration Date] (Son Kullanma Tarihi): AÇIK [Chain] (Zincir): AÇIK

3.2 SMTP

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [E-mail Setting] (E-posta Ayarı) - [E-mail TX (SMTP)] (E-posta TX (SMTP))

Ayar öğesi	Önerilen ayar
[Sertifika Doğrulama Seviyesi Ayarları]	[Expiration Date] (Son Kullanma Tarihi): AÇIK [Chain] (Zincir): AÇIK

3.3 IEEE802.1X Auth

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [IEEE802.1X Authentication Setting] (IEEE802.1X Doğrulama Ayarı) - [IEEE802.1X Authentication Setting] (IEEE802.1X Doğrulama Ayarı) - [Supplicant Setting] (Doğrulama İsteyen Ayar)

Ayar öğesi	Önerilen ayar
[Sertifika Doğrulama Seviyesi Ayarları]	[Expiration Date] (Son Kullanma Tarihi): AÇIK [Chain] (Zincir): AÇIK

3.4 IPSEC

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [TCP/IP Setting] (TCP/IP Ayarı) - [IPsec] - [Enable IPsec] (IPsec Devreye Al)

Ayar öğesi	Önerilen ayar
[Sertifika Doğrulama Seviyesi Ayarları]	[Expiration Date] (Son Kullanma Tarihi): [Onay] [Chain] (Zincir): [Onay]



Tavsiyeler

[IPsec Setting]'de (IPsec Ayarı), [IKE], [SA], [Peer] (Eş), ve [Protocol Setting] (Protokol Ayarı) öğelerini önceden kaydedin.

3.5 WebDAVİstemcisi

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [WebDAV Settings] (WebDAV Ayarları) - [WebDAV Client Settings] (WebDAV İstemci Ayarları)

Ayar öğesi	Önerilen ayar
[Sertifika Doğrulama Seviyesi Ayarları]	[Expiration Date] (Son Kullanma Tarihi): AÇIK [Chain] (Zincir): AÇIK

3.6 LDAP

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [LDAP Setting] (LDAP Ayarı) - [Setting Up LDAP] (LDAP Kurulumunu Yap)

Ayar öğesi	Önerilen ayar
[Sertifika Doğrulama Seviyesi Ayarları]	[Expiration Date] (Son Kullanma Tarihi): AÇIK [Chain] (Zincir): AÇIK

3.7 DPWS

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [DPWS Settings] (DPWS Ayarları) - [DPWS Common Settings] (DPWS Ortak Ayarları)

Ayar öğesi	Önerilen ayar
[Sertifika Doğrulama Seviyesi Ayarları]	[Expiration Date] (Son Kullanma Tarihi): AÇIK [Chain] (Zincir): AÇIK

3.8 OpenAPI

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [OpenAPI Setting] (OpenAPI Ayarı) - [OpenAPI Setting] (OpenAPI Ayarı)

Ayar öğesi	Önerilen ayar
[Sertifika Doğrulama Seviyesi Ayarları]	[Expiration Date] (Son Kullanma Tarihi): AÇIK [Chain] (Zincir): AÇIK

3.9 Uzaktan Kumanda Paneli

Konum ayarı: [Utility] (Uygulama) - [Administrator] (Yönetici) - [Network] (Ağ) - [Remote Panel Settings] (Uzaktan Kumanda Paneli Ayarları) - [Remote Panel Client Settings] (Uzaktan Kumanda Paneli İstemci Ayarları)

Ayar öğesi	Önerilen ayar
[Sertifika Doğrulama Seviyesi Ayarları]	[Expiration Date] (Son Kullanma Tarihi): AÇIK [Chain] (Zincir): AÇIK

4 Ek Güvenlik Bilgileri

4.1 En iyi uygulama önerisi

Kullanılacak şifreleme algoritmalarının, EUCC Kriptografi Kılavuzları ve SOGIS-Onaylı-Kriptografik-Mekanizmalarında önerilen en iyi uygulama ayarlarına uygun olmasını tavsiye ederiz.

Aşağıda, EUCC Kriptografi Kılavuzları ve SOGIS-Onaylı-Kriptografik-Mekanizmalar tarafından önerilen şifreleme algoritmaları ve anahtar uzunluklarının bir listesi bulunmaktadır.

Öge	Önerilen ayar
Şifreleme algoritmaları	AES (Gelişmiş Şifreleme Standardı) RSA (Rivest-Şamir-Adleman) SHA-2 (Güvenli Karma Algoritması 2) ECC (Eliptik Eğri Kriptografisi) HMAC (Karma tabanlı Mesaj Doğrulama Kodu)
Şifreleme anahtarı uzunluğu	RSA: 2048 bit veya daha fazla ECC: 256 bit veya daha fazla AES: 256 bit



Tavsiyeler

Detaylar için, en son EUCC Kriptografi Kılavuzları ve SOGIS-Onaylı-Kriptografik-Mekanizmalara bakınız.

4.2 Eski sistemlerle iletişim kurarken alınması gereken önlemler

Aşağıdaki protokoller ve sürümlerin eski sistemlerle iletişim için kullanıldığı varsayılmaktadır.

Eski ayarları kullanmak güvenlik risklerini artırır, bu nedenle lütfen bunları güvenli bir ağ ortamında kullanın.

Öğe	Eski ayarlar
Protokol	SLP FTP SMB (3.0 veya önceki sürüm, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TiPi: Sunucuya Bağlı/KAPALI) DPWS TCPSoketi
Şifreleme algoritmaları	SHA-1 (Güvenli Karma Algoritması 1) DES (Veri Şifreleme Standardı) 3DES (Üçlü Veri Şifreleme Standardı) RC2-40 (D51Rivest Şifre) RC2-64 (D51Rivest Şifre) RC2-128 (D51Rivest Şifre)
Şifreleme anahtarı uzunluğu	RSA: 1024 bit veya daha az ECC: 160 bit veya daha az AES: 128 bit veya daha az DES: 56 bit 3DES: 112 bit

IPsec eski ayarları

[IKEv1]

Ayar ögesi	Eski ayarlar
[Şifreleme Algoritması]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 ve 192))
[Doğrulama Algoritması]	Kullanılmıyor
[Diffie-Hellman Grubu]	[Group 1] (Grup 1), [Group 2] (Grup 2), [Group 5] (Grup 5)

[IKEv2]

Ayar ögesi	Eski ayarlar
[Şifreleme Algoritması]	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 ve 192))
[Doğrulama Algoritması]	Kullanılmıyor
[Diffie-Hellman Grubu]	[Group 1] (Grup 1), [Group 2] (Grup 2), [Group 5] (Grup 5)

[SA]

Ayar ögesi	Eski ayarlar
[Key Exchange Method] (Anahtar Değişim Yöntemi)	[IKEv1]
[Doğrulama metodu]	[Dijital İmza]
[ESP Şifrel. Algoritması]	[3DES-CBC] ([128]/[192]/[128 and 192] (128 ve 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 ve 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 ve 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 ve 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 ve 192))
[Mükemmel İleti Gizliliği]	AÇIK

Ayar ögesi	Eski ayarlar
[Diffie-Hellman Group(IKEv1)] (Diffie-Hellman Grubu(IKEv1))	[Group 1] (Grup 1), [Group 2] (Grup 2), [Group 5] (Grup 5)

4.3 Fabrika sevkiyatında mevcut ađ arayüzleri ve hizmetleri

Hizmet Türü	Protokol	Port Numarası
DHCP	UDP	68
HTTP sunucu	TCP	80
NETBIOS Ad Hizmeti	UDP	137
NETBIOS Datagram Hizmeti	UDP	138
SNMP	UDP	161
SSL üzerinden HTTP Sunucusu / SSL üzerinden IPP	TCP	443
LPD Yazdır	TCP	515
DHCPv6 İstemci	UDP	546
IPP Yazdır	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS aracı)	TCP	8091
RAW Baskı	TCP	9100
RAW Baskı	TCP	9112
RAW Baskı	TCP	9113
RAW Baskı	TCP	9114
RAW Baskı	TCP	9115
RAW Baskı	TCP	9116
OpenAPI	TCP	50001

4.4 Giriş dođrulaması hakkında

Ađ ayarları vb. için girilecek karakter sayısı hakkında bilgi için, Kullanım Kılavuzu'ndaki her bir ayar öđesine bakın.

Dilin kodlamasına bađlı olarak, çok baytlı karakterleri destekleyen öđeler için izin verilen maksimum giriş (MFP'de kaydedilen veriler) karakter sayısının üç katı olabilir.

Рекомендації для приладів, об'єднаних у безпечну мережу

Зміст

1 Налаштування фільтрування IP-адрес

1.1	Фільтрування IP-адрес	1-3
1.2	Швидке фільтрування IP-адрес.....	1-3

2 Налаштування зашифрованого зв'язку

2.1	Шифрування TLS.....	2-4
2.1.1	HTTP (Web Connection)	2-4
2.1.2	WebDAVServer	2-5
2.1.3	IPP.....	2-5
2.1.4	OpenAPI.....	2-5
2.1.5	RemotePanel.....	2-5
2.1.6	DPWS.....	2-5
2.1.7	POP.....	2-6
2.1.8	SMTP	2-6
2.1.9	IEEE802.1X Auth	2-6
2.1.10	LDAP	2-6
2.1.11	TCP Socket.....	2-6
2.2	Інше шифрування	2-7
2.2.1	SMBServer.....	2-7
	Шифрування SMB.....	2-7
	Підпис SMB.....	2-7
2.2.2	SMBClient.....	2-8
2.2.3	SNMP	2-8
2.2.4	IPsec	2-8
2.2.5	S/MIME	2-9

3 Налаштування підтвердження сертифіката

3.1	POP.....	3-10
3.2	SMTP.....	3-10
3.3	IEEE802.1X Auth.....	3-10
3.4	IPsec.....	3-11
3.5	WebDAVClient	3-11
3.6	LDAP.....	3-11
3.7	DPWS	3-11
3.8	OpenAPI	3-12
3.9	RemotePanel	3-12

4 Додаткова інформація безпеки

4.1	Рекомендації щодо найкращих методів роботи	4-13
4.2	Запобіжні заходи щодо обміну даними із застарілими системами	4-14
	Застарілі налаштування IPsec.....	4-14
4.3	Інтерфейси мережі і служби, доступні при постачанні з заводу.....	4-16
4.4	Про перевірку даних введення	4-17



Про цей посібник

У цьому посібнику описана інформація та налаштування, що забезпечують безпечне використання приладів.

Підключаючи цей апарат до мережі, використовуйте його в середовищі, захищеному брандмауером. Також рекомендуємо налаштувати приватну IP-адресу для IP-адреси апарата.

Лише налаштування приватної IP-адреси дає можливість користувачам локальної мережі, як-от внутрішня LAN, мати доступ до апарата, запобігаючи несанкціонованому доступу ззовні.

Якщо вам потрібно використовувати глобальну IP-адресу, обов'язково захистіть цей апарат за допомогою брандмауера.

1 Налаштування фільтрування IP-адрес

Фільтрування IP-адрес — це функція, яка обмежує кількість приладів, що можуть отримати доступ до цього апарата, за IP-адресою. Правильне налаштування цієї функції дає змогу обмежити доступ із несанкціонованих приладів.

Функцію фільтрування IP-адрес на цьому апараті можна встановити одним із двох наведених нижче методів.

1.1 Фільтрування IP-адрес

Задати вручну діапазон IP-адрес, яким потрібно дозволити або заборонити доступ.

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [TCP/IP Setting] (Налаштування TCP/IP) - [IP Address Filtering] (Фільтрування IP-адрес)



Налаштуйте IP-адреси, які буде дозволено або заборонено відповідно до вашого середовища.

1.2 Швидке фільтрування IP-адрес

Діапазон IP-адрес із дозволеним доступом встановлюється автоматично на основі IP-адреси та маски підмережі, встановлених у цьому апараті.

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [TCP/IP Setting] (Налаштування TCP/IP) - [Quick IP Filtering] (Швидке фільтрування IP)

Рекомендовані налаштування: [Synchronize IP Address] (Синхронізувати IP-адресу)/[Synchronize Subnet Mask] (Синхронізувати маску мережі) *

* Оберіть одне відповідно до середовища.

2 Налаштування зашифрованого зв'язку

Рекомендуємо використовувати наступний зашифрований зв'язок, щоб уникнути перехоплення даних, незаконної зміни даних та перехоплення сеансу зв'язку.

2.1 Шифрування TLS

Рекомендуємо виконати наступні налаштування, щоб зменшити ризик вразливості.

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Security] (Безпека) - [PKI Settings] (Налаштування інфраструктури відкритих ключів) - [Enable SSL Version] (Увімкнути версію SSL)

Налаштовуваний елемент	Рекомендоване налаштування
[Mode using SSL/TLS] (Режим використання SSL/TLS)	[Admin. Mode and User Mode] (Режим адміністратора і режим користувача)
[SSL/TLS Version Setting] (Налаштування версії SSL/TLS)	TLS1.2 TLS1.3 (IEEE802.1X несумісно)
[Encryption Strength] (Стойкість шифрування)	AES-256

Початковий сертифікат встановлений на заводі. Якщо потрібен інший сертифікат, зареєструйте новий за наступним місцезнаходженням.

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Security] (Безпека) - [PKI Settings] (Налаштування інфраструктури відкритих ключів) - [Device Certificate Setting] (Налаштування сертифіката приладу)

Налаштовуваний елемент	Рекомендоване налаштування
[Encryption Key Type] (Тип ключа шифрування)	RSA-2048_SHA-256 ECDSA-256_SHA-256 ECDSA-384_SHA-384 ECDSA-521_SHA-384

Шифрування TLS підтримується для наступних протоколів та служб. Подробиці про місце знаходження налаштування локації див. у наступних розділах.

- HTTP (Web Connection, WebDAVServer, IPP, OpenAPI, RemotePanel)
- DPWS
- POP
- SMTP (Start TLS, SMTP over SSL)
- IEEE802.1X Auth (EAP-TLS, EAP-TTLS, PEAP)
- LDAP
- TCP Socket

2.1.1 HTTP (Web Connection)

Якщо увімкнути [Enable SSL Version] (Увімкнути версію SSL), режим обміну даними автоматично перемикається на обмін даними, зашифрованими TLS (HTTPS).

2.1.2 WebDAVServer

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [WebDAV Settings] (Налаштування WebDAV) - [WebDAV Server Settings] (Налаштування сервера WebDAV)

Налаштовуваний елемент	Рекомендоване налаштування
[SSL Settings] (Налаштування SSL)	[SSL Only] (Тільки SSL)

2.1.3 IPP

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [HTTP Server Settings] (Налаштування сервера HTTP)

Налаштовуваний елемент	Рекомендоване налаштування
[IPP-SSL Settings] (Налаштування IPP-SSL)	[SSL Only] (Тільки SSL)

2.1.4 OpenAPI

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [OpenAPI Setting] (Налаштування OpenAPI) - [OpenAPI Setting] (Налаштування OpenAPI)

Налаштовуваний елемент	Рекомендоване налаштування
[SSL/Port Settings] (Налаштування SSL/Port)	[SSL Only] (Тільки SSL)

2.1.5 RemotePanel

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [Remote Panel Settings] (Налаштування дистанційної панелі) - [Remote Panel Server Settings] (Налаштування сервера дистанційної панелі)

Налаштовуваний елемент	Рекомендоване налаштування
[Port No.(SSL)] (Порт № (SSL))	[50443]

Поради

Якщо увімкнути [Enable SSL Version] (Увімкнути версію SSL), обмін даними автоматично перемикається на зашифрований режим TLS. Уточніть номер порту.

2.1.6 DPWS

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [DPWS Settings] (Налаштування DPWS) - [DPWS Common Settings] (Загальні налаштування DPWS)

Налаштовуваний елемент	Рекомендоване налаштування
[SSL Settings] (Налаштування SSL)	УВІМКН

2.1.7 POP

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [E-mail Setting] (Налаштування ел. пошти) - [E-mail RX (POP)] (RX (POP) ел. пошти)

Налаштовуваний елемент	Рекомендоване налаштування
[Enable SSL] (Увімкнути SSL)	УВІМКН

2.1.8 SMTP

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [E-mail Setting] (Налаштування ел. пошти) - [E-mail TX (SMTP)] (TX (SMTP) ел. пошти)

Налаштовуваний елемент	Рекомендоване налаштування
[SSL/TLS Settings] (Налаштування SSL/TLS)	[SMTP over SSL] (SMTP через SSL)

2.1.9 IEEE802.1X Auth

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [IEEE802.1X Authentication Setting] (Налаштування автентифікації IEEE802.1X) - [IEEE802.1X Authentication Setting] (Налаштування автентифікації IEEE802.1X) - [Supplicant Setting] (Налаштування запитувача)

Налаштовуваний елемент	Рекомендоване налаштування
[EAP-Type] (Тип EAP)	Оберіть [EAP-TLS], [EAP-TTLS] або [PEAP].

2.1.10 LDAP

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [LDAP Setting] (Налаштування LDAP) - [Setting Up LDAP] (Налаштування LDAP)

Налаштовуваний елемент	Рекомендоване налаштування
[Enable SSL] (Увімкнути SSL)	УВІМКН

2.1.11 TCP Socket

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [TCP Socket Setting] (Налаштування TCP-сокета)

Налаштовуваний елемент	Рекомендоване налаштування
[Use SSL/TLS] (Використання SSL/TLS)	УВІМКН

2.2 Інше шифрування

Рекомендуємо виконати наступні налаштування, щоб зменшити ризик вразливості. Подробиці про налаштування кожної функції див. у наступних розділах.

Функція	Рекомендоване налаштування
SMBServer	SMB шифрування, SMB підпис
SMBClient	Протокол Цербер
SNMP	SNMPv3
IPsec	IKEv2
S/MIME	УВІМКН

2.2.1 SMBServer

Використання шифрування SMB і підпису SMB може зменшити наступні ризики безпеки.

- Перехоплення: зловмисна третя сторона може перехопити повідомлення та викрасти особисту або конфіденційну інформацію.
- Незаконна зміна даних: існує ризик, що зміст обміну даними може бути змінений у ході атаки через посередника (MITM).
- Підробка: якщо інформація автентифікації вкрадена, третя сторона може представитися законним користувачем, щоб отримати неуповноважений доступ.
- Витік інформації: незашифрований обмін даними може легко бути перехоплений, особливо в громадських мережах Wi-Fi, що збільшує ризик витоку персональної інформації та інформації кредитної картки.

Шифрування SMB

Передумови

- Створіть спільну скриньку користувача. Також налаштуйте автоматичну передачу файлів зі спільної скриньки користувача і збереження їх у папці SMB.
- Вкажіть пароль для скриньки користувача.

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Box] (Скринька) - [User Box List] (Перелік скриньки користувача)

Налаштовуваний елемент	Рекомендоване налаштування
[SMB Communication Encryption] (Шифрування обміну даними SMB)	[Encrypt] (Шифрувати)

Підпис SMB

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [SMB Setting] (Налаштування SMB) - [SMB Server Settings] (Налаштування сервера SMB)

Налаштовуваний елемент	Рекомендоване налаштування
[SMB security Signature Setting] (Налаштування підпису безпеки SMB)	[Required] (Обов'язково)

2.2.2 SMBClient

Протокол Цербер використовує стійку технологію шифрування, значно зменшуючи ризик викрадення облікових даних під час процесу автентифікації. Це також забезпечує цілісність, запобігаючи незаконній зміні даних між відправником та отримувачем, а також атакам ретрансляції NTLM.

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [SMB Setting] (Налаштування SMB) - [Client Setting] (Налаштування клієнта)

Налаштовуваний елемент	Рекомендоване налаштування
[SMB Authentication Setting] (Налаштування автентифікації SMB)	[Kerberos] (Протокол Цербер)

2.2.3 SNMP

Налаштуйте шифрування за допомогою SNMPv3. Якщо також додається налаштування автентифікації, можете ще більше підвищити безпеку. Ризики безпеки приблизно однакові, як з SMB.

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [SNMP Setting] (Налаштування SNMP)

Налаштовуваний елемент	Рекомендоване налаштування
[SNMP Setting] (Налаштування SNMP)	[SNMP v3(IP)]
[Encryption Algorithm] (Алгоритм шифрування)	[AES-128]
[Authentication Method] (Метод автентифікації)	Оберіть [SHA-256], [SHA-384] або [SHA-512].

2.2.4 IPsec

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [TCP/IP Setting] (Налаштування TCP/IP) - [IPsec] (IPsec) - [IPsec Setting] (Налаштування IPsec) [IKEv2]

Налаштовуваний елемент	Рекомендоване налаштування
[Encryption Algorithm] (Алгоритм шифрування)	[AES-CBC] ([256]/[192 and 256] (192 і 256)/[All] (Всі))
[Authentication Algorithm] (Алгоритм автентифікації)	[SHA-2] ([256]/[384]/[512]/[256 and 384] (256 і 384)/[384 and 512] (384 і 512) /[All] (Всі)), [AES-XCBC]
[Diffie-Hellman Group]	[Group 14] (Група 14), [Group 19] (Група 19)

[SA]

Налаштовуваний елемент	Рекомендоване налаштування
[Encapsulation Mode] (Метод пакетування)	[Tunnel] (Тунель), [Transport] (Транспорт)
[Security Protocol] (Протокол безпеки)	[ESP]
[Key Exchange Method] (Основний метод обміну)	[IKEv2]
[Authentication Method] (Метод автентифікації)	[Digital Signature] (Цифровий підпис)

Налаштовуваний елемент	Рекомендоване налаштування
[ESP Encryption Algorithm] (Алгоритм шифрування ESP)	[AES-GCM] ([256]/[192 and 256] (192 і 256)/[All] (Всі)), [AES-GCM-64] ([256]/[192 and 256] (192 і 256)/[All] (Всі)), [ENC_NULL_AES_GMAC] ([256]/[192 and 256] (192 і 256)/[All] (Всі))
[Perfect Forward Secrecy] (Ідеальна пряма секретність)	УВІМКН
[Diffie-Hellman Group(IKEv2)] - [Priority1-4] (Пріоритет 1-4)	[Group 14] (Група 14), [Group 19] (Група 19)

2.2.5 S/MIME

Якщо ви використовуєте додатковий S/MIME при надсиланні електронної пошти, можете шифрувати вміст електронного листа, щоб запобігти перехопленню та перевірити особу відправника з електронним підписом. Це ефективний спосіб захисту від підробок та фішингу.

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [E-mail Setting] (Налаштування ел. пошти) - [S/MIME]

Налаштовуваний елемент	Рекомендоване налаштування
[Digital Signature] (Цифровий підпис)	[Always add signature] (Завжди додавати підпис)
[Digital Signature Type] (Тип цифрового підпису)	[SHA-256]
[E-Mail Text Encrypt. Method] (Метод шифрування тексту електронного листа)	[AES-256]

3 Налаштування підтвердження сертифіката

При використанні обміну даними з шифруванням TLS, щоб зменшити вплив атак через посередника, рекомендуємо використовувати підтвердження сертифіката. Для підтверджуваних елементів рекомендуємо як мінімум увімкнути дату завершення дії сертифіката та ланцюжок.

Якщо здійснюється спроба підключення до застарілого середовища, яке не має функції підтвердження сертифіката, збільшується ризик атак через посередника. Рекомендуємо використовувати у середовищі безпечної мережі.

Підтвердження сертифіката на стороні MFP рекомендоване у наступних функціях клієнта MFP. Подробиці про місце знаходження налаштування локації див. у наступних розділах. POP, SMTP (Start TLS/SMTP over SSL), IEEE802.1X Auth (EAP-TYPE: EAP-TLS/EAP-TTLS/PEAP), IPSec, WebDAV, LDAP, DPWS, RemotePanel

Поради

Підтвердження сертифіката на стороні клієнта, підключеного до MFP, рекомендоване у наступних функціях сервера MFP.

HTTP (Web Connection / WebDAV / IPP / DPWS / OpenAPI / RemotePanel), TCP Socket

3.1 POP

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [E-mail Setting] (Налаштування ел. пошти) - [E-mail RX (POP)] (RX (POP) ел. пошти)

Налаштовуваний елемент	Рекомендоване налаштування
[Certificate Verification Level Settings] (Налаштування рівня перевірки сертифіката)	[Expiration Date] (Дата завершення дії): УВІМКН [Chain] (Ланцюжок): УВІМКН

3.2 SMTP

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [E-mail Setting] (Налаштування ел. пошти) - [E-mail TX (SMTP)] (TX (SMTP) ел. пошти)

Налаштовуваний елемент	Рекомендоване налаштування
[Certificate Verification Level Settings] (Налаштування рівня перевірки сертифіката)	[Expiration Date] (Дата завершення дії): УВІМКН [Chain] (Ланцюжок): УВІМКН

3.3 IEEE802.1X Auth

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [IEEE802.1X Authentication Setting] (Налаштування автентифікації IEEE802.1X) - [IEEE802.1X Authentication Setting] (Налаштування автентифікації IEEE802.1X) - [Supplicant Setting] (Налаштування запитувача)

Налаштовуваний елемент	Рекомендоване налаштування
[Certificate Verification Level Settings] (Налаштування рівня перевірки сертифіката)	[Expiration Date] (Дата завершення дії): УВІМКН [Chain] (Ланцюжок): УВІМКН

3.4 IPsec

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [TCP/IP Setting] (Налаштування TCP/IP) - [IPsec] (IPsec) - [IPsec Setting] (Налаштування IPsec)

Налаштовуваний елемент	Рекомендоване налаштування
[Certificate Verification Level Settings] (Налаштування рівня перевірки сертифіката)	[Expiration Date] (Дата завершення дії): [Confirm] (Підтвердити) [Chain] (Ланцюжок): [Confirm] (Підтвердити)

Поради

У [IPsec Setting] (Налаштування IPsec) зареєструйте елементи [IKE], [SA], [Peer] (Рівноправний) і [Protocol Setting] (Налаштування протоколу) заздалегідь.

3.5 WebDAVClient

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [WebDAV Settings] (Налаштування WebDAV) - [WebDAV Client Settings] (Налаштування клієнта WebDAV)

Налаштовуваний елемент	Рекомендоване налаштування
[Certificate Verification Level Settings] (Налаштування рівня перевірки сертифіката)	[Expiration Date] (Дата завершення дії): УВІМКН [Chain] (Ланцюжок): УВІМКН

3.6 LDAP

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [LDAP Setting] (Налаштування LDAP) - [Setting Up LDAP] (Налаштовування LDAP)

Налаштовуваний елемент	Рекомендоване налаштування
[Certificate Verification Level Settings] (Налаштування рівня перевірки сертифіката)	[Expiration Date] (Дата завершення дії): УВІМКН [Chain] (Ланцюжок): УВІМКН

3.7 DPWS

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [DPWS Settings] (Налаштування DPWS) - [DPWS Common Settings] (Загальні налаштування DPWS)

Налаштовуваний елемент	Рекомендоване налаштування
[Certificate Verification Level Settings] (Налаштування рівня перевірки сертифіката)	[Expiration Date] (Дата завершення дії): УВІМКН [Chain] (Ланцюжок): УВІМКН

3.8 OpenAPI

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [OpenAPI Setting] (Налаштування OpenAPI) - [OpenAPI Setting] (Налаштування OpenAPI)

Налаштовуваний елемент	Рекомендоване налаштування
[Certificate Verification Level Settings] (Налаштування рівня перевірки сертифіката)	[Expiration Date] (Дата завершення дії): УВІМКН [Chain] (Ланцюжок): УВІМКН

3.9 RemotePanel

Місце знаходження налаштування: [Utility] (Утиліта) - [Administrator] (Адміністратор) - [Network] (Мережа) - [Remote Panel Settings] (Налаштування дистанційної панелі) - [Remote Panel Server Settings] (Налаштування сервера дистанційної панелі)

Налаштовуваний елемент	Рекомендоване налаштування
[Certificate Verification Level Settings] (Налаштування рівня перевірки сертифіката)	[Expiration Date] (Дата завершення дії): УВІМКН [Chain] (Ланцюжок): УВІМКН

4 Додаткова інформація безпеки

4.1 Рекомендації щодо найкращих методів роботи

Рекомендуємо, щоб алгоритми шифрування відповідали налаштуванням найкращих методів, рекомендованих в інструкціях EUCC щодо шифрування та узгоджених механізмах шифрування SOGIS.

Нижче подано перелік алгоритмів шифрування та довжини ключів, рекомендованих в інструкціях EUCC щодо шифрування та узгоджених механізмах шифрування SOGIS.

Елемент	Рекомендоване налаштування
Алгоритми шифрування	AES (Розширений стандарт шифрування) RSA (Rivest-Shamir-Adleman) SHA-2 (Захищений алгоритм хешування 2) ECC (Еліптична криптографія) HMAC (Хеш-код автентифікації повідомлень)
Довжина ключа шифрування	RSA: 2048 біт або більше ECC: 256 біт або більше AES: 256 біт

Поради

Подробиці див. в останніх Інструкціях EUCC та узгоджених механізмах шифрування SOGIS.

4.2 Запобіжні заходи щодо обміну даними із застарілими системами

Наступні протоколи та версії вважаються використовуваними для обміну даними із застарілими системами.

Використання застарілих налаштувань збільшує ризики безпеки, тому прохання використовувати їх у середовищі безпечної мережі.

Елемент	Застарілі налаштування
Протокол	SLP FTP SMB (3.0 або раніша версія, NTLMv1/v2) SNMPv1/v2 IEEE802.1X Auth (EAP-TYPE: Depend on Server/OFF) DPWS TCPSocket
Алгоритми шифрування	SHA-1 (Захищений алгоритм хешування 1) DES (Стандарт шифрування даних) 3DES (Потрійний стандарт шифрування даних) RC2-40 (D51Rivest Cipher) RC2-64 (D51Rivest Cipher) RC2-128 (D51Rivest Cipher)
Довжина ключа шифрування	RSA: 1024 біт або менше ECC: 160 біт або менше AES: 128 біт або менше DES: 56 біт 3DES: 112 біт

Застарілі налаштування IPsec

[IKEv1]

Налаштовуваний елемент	Застарілі налаштування
[Encryption Algorithm] (Алгоритм шифрування)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 і 192))
[Authentication Algorithm] (Алгоритм автентифікації)	Не використовується
[Diffie-Hellman Group]	[Group 1] (Група 1), [Group 2] (Група 2), [Group 5] (Група 5)

[IKEv2]

Налаштовуваний елемент	Застарілі налаштування
[Encryption Algorithm] (Алгоритм шифрування)	[DES-CBC] [3DES-CBC] [AES-CBC] ([128]/[192]/[128 and 192] (128 і 192))
[Authentication Algorithm] (Алгоритм автентифікації)	Не використовується
[Diffie-Hellman Group]	[Group 1] (Група 1), [Group 2] (Група 2), [Group 5] (Група 5)

[SA]

Налаштовуваний елемент	Застарілі налаштування
[Key Exchange Method] (Основний метод обміну)	[IKEv1]
[Authentication Method] (Метод автентифікації)	[Digital Signature] (Цифровий підпис)

Налаштовуваний елемент	Застарілі налаштування
[ESP Encryption Algorithm] (Алгоритм шифрування ESP)	[3DES-CBC] ([128]/[192]/[128 and 192] (128 i 192)) [AES-CTR] ([128]/[192]/[128 and 192] (128 i 192)) [AES-GCM] ([128]/[192]/[128 and 192] (128 i 192)) [AES-GCM-64] ([128]/[192]/[128 and 192] (128 i 192)) [ENC_NULL_AES_GMAC] ([128]/[192]/[128 and 192] (128 i 192))
[Perfect Forward Secrecy] (Ідеальна пряма секретність)	УВІМКН
[Diffie-Hellman Group(IKEv1)]	[Group 1] (Група 1), [Group 2] (Група 2), [Group 5] (Група 5)

4.3 Інтерфейси мережі і служби, доступні при постачанні з заводу

Тип служби	Протокол	Номер порту
DHCP	UDP	68
Сервер HTTP	TCP	80
NETBIOS Name Service	UDP	137
NETBIOS Datagram Service	UDP	138
SNMP	UDP	161
HTTP Server over SSL / IPP over SSL	TCP	443
Друк LPD	TCP	515
Клієнт DHCPv6	UDP	546
Друк IPP	TCP	631
MFPIF	UDP	1900
WebService	UDP	3702
LLMNR	UDP	5355
HTTP (IWS-tool)	TCP	8091
Друк RAW	TCP	9100
Друк RAW	TCP	9112
Друк RAW	TCP	9113
Друк RAW	TCP	9114
Друк RAW	TCP	9115
Друк RAW	TCP	9116
OpenAPI	TCP	50001

4.4 Про перевірку даних введення

Кількість символів введення для налаштувань мережі тощо див. по кожному елементу налаштування у Посібнику користувача.

Залежно від шифрування мови, максимально припустимий ввід (дані, збережені в MFP) для елементів, що підтримують багатобітні символи, можуть втричі перевищувати кількість символів.

