The Security Hardening Guide for the AIG-302 Series

Moxa Technical Support Team

support@moxa.com

Contents

Copyright © 2024 Moxa Inc. Released on Jun 4, 2024

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa

Tel: 1-714-528-6777
Fax: 1-714-528-6778

1 Introduction

This document provides guidelines on how to configure and secure the AIG-302 Series. You should consider the recommendations in this document as best practices for securing the AIG-302 in most applications. It is highly recommended that you review and test the configurations thoroughly before implementing them in your production system to ensure that your applications are not negatively impacted.

2 General System Information

2.1 Basic Information About the Device

Model	Operating System	Firmware
AIG-302	Linux Debian 11	v1.0

2.2 Physical Security Measures

The AIG-302 should be safeguarded with physical security measures such as CCTV surveillance, security guards, protective barriers, locks, access control, and perimeter intrusion detection. The appropriate type of physical security should be determined based on the environment and the level of risk of physical attacks.

2.3 Anti-tamper Features

- The AIG-302 is equipped with anti-tamper labels on its enclosures, enabling the administrator to detect any tampering with the device.
- Additionally, security screws are used on the enclosures as a physical tamper-resistance measure, enhancing the difficulty of accessing the internal components in the event of a physical security breach.

2.4 Usage Limitations

The AIG-302 should not be utilized to control mission-critical components. Failure to maintain control of such a device could pose threats to human safety, the environment, or lead to significant financial losses.

2.5 Network Security

- If the AIG-302 needs to be connected to an untrusted network (e.g., Internet) through Ethernet or Wi-Fi, we recommend avoiding direct connections to the network. Set up a firewall between the Ethernet and Wi-Fi connections of the AIG-302 and the untrusted network.
- For security-critical applications, it is highly recommended to use a private APN for cellular networks.

3 Configuration and Hardening Information

3.1 TCP/UDP Port Status and Suggested Settings

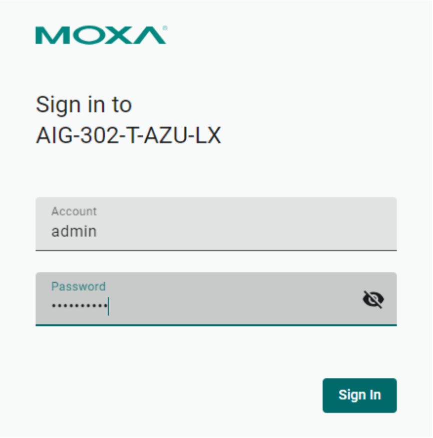
For security reasons, consider disabling unused services and use a higher security level for data-communication services. Refer to the table below for recommended settings.

Process Name	Suggested Settings	Type	Port Number	Description	Security Remark
SSH Server	Enable	TCP	22	SSH console	Encrypted data channel with trusted certificate
HTTP Service	Disable	TCP	80	Web console	Disable HTTP service for transmissions involving plain text
HTTPS Service	Enable	TCP	8443	Secured web console	Encrypted data channel with trusted certificate
Discovery Service	Disable	UDP	5353	For communicating with Moxa utilities	Disable the service if it is not in use
Modbus TCP Server	Disable	TCP	502	For Modbus communication	Disable service if it is not in use
DHCP Server	Disable	UDP	67, 68	For assigning a system IP to DHCP clients	Disable service if it is not in use

3.2 Forcing a Password Change After First Login

For security reasons, account and password protection is enabled by default. Users must provide the correct user account and password to unlock the device to gain access to the web console of the gateway.

The default account and password are **admin** and **admin@123** (both in lowercase letters), respectively.



Sign in to
AIG-302-T-AZU-LX

Account: admin

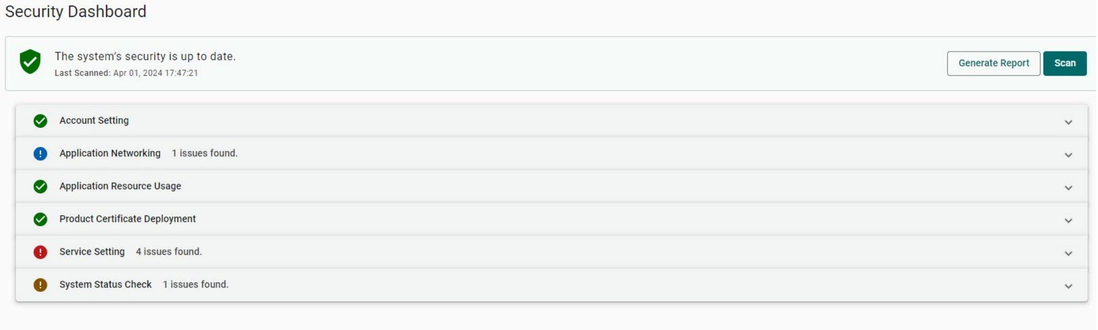
Password: ••••••••••

Copyright © 2024 Moxa Inc.

After the first login, we force a password change to comply with general security policies and practices and to enhance the security of your device.

3.3 Security Dashboard

Once device provisioning is completed, you can log in into the AIG web console, go to **Security Dashboard**, and press **Scan** to check the security status of the device.



Security Dashboard

The system's security is up to date.
Last Scanned: Apr 01, 2024 17:47:21

- Account Setting
- Application Networking 1 issues found.
- Application Resource Usage
- Product Certificate Deployment
- Service Setting 4 issues found.
- System Status Check 1 issues found.

You can utilize the **Security Dashboard** results to fix security issues to enhance the security of your AIG gateway as per the following guidelines:

Category	Security Check Criteria	Threat Mitigation/handling
Account Settings	Password should be changed within the preset interval.	Go to **Account Management** > **Accounts** to change the password.
	An account should only have one active session at any given time.	Go to **Security** > **Session Management** monitor and manage concurrent sessions.
	An account should not have abnormal connections (E.g., more than one session per account from different source IPs).	
Application Networking	System should not have open network ports.	Go to **Security** > **Firewall** and check the allow list.
Application Resource Usage	IoT Edge modules should not utilize system disk's configurable space.	Ensure the IoT Edge modules are deployed in the system storage paths **/var/run/** and **/tmp/**.
	IoT Edge modules should not utilize system disk's non-configurable space.	
	IoT Edge modules should not be granted direct privileges.	To grant permissions to the IoT Edge modules, go to **Cloud Connectivity** > **Azure IoT Edge** > **Module Permission**, create a service account, and grant the required permissions to the IoT Edge module.
Product Certificate Deployment	Production certificate should be configured as an Azure IoT Edge downstream certificate.	For enhanced security robustness, we recommend using your own certificate instead of the default

Copyright © 2024 Moxa Inc.

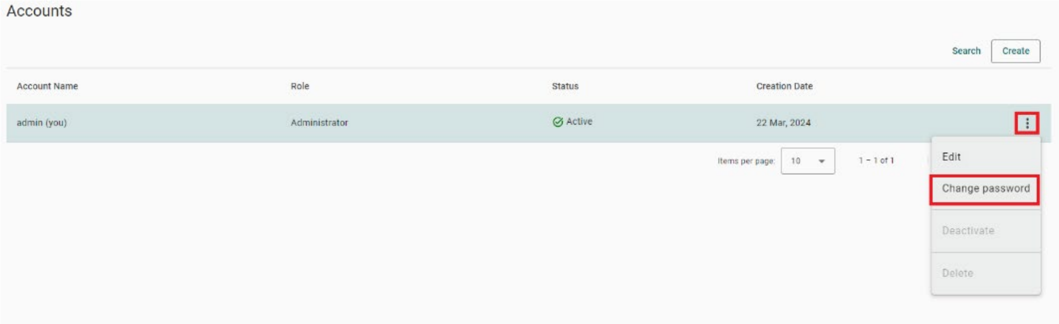
Category	Security Check Criteria	Threat Mitigation/handling
		one. Go to **Cloud Connectivity** > **Azure IoT Edge** > **Downstream Certificate** to upload a certificate.
	Azure IoT Edge should not use a connection string for provisioning.	For enhanced security robustness, we recommend using a TPM or a X.509 certificate.
	All certificates should not expire within the next three months.	Go to **Security** > **Certificate Center** to check the status of each certificate. If you find that a certificate will expire soon or has already expired, go to **Cloud Connectivity** > **Azure IoT Edge/Azure IoT Device/MQTT Client or Security** > **HTTPS** to check and replace the certificates.
	All certificates should have expired.	
Service Settings	Discovery Service should not be enabled.	Go to **Maintenance** > **Service** to disable Discovery Service.
	SSH Service should not be enabled.	Go to **Maintenance** > **Service** to disable the Debug Mode.
	Serial Console Service should not be enabled.	Go to **Security** > **Service** to disable local console.
	Account Lock Service should be enabled.	Go to **Security** > **Login Lockout** to enable the **Login Failure Lockout** option.
	System Use Notification Service should be enabled.	Go to **Security** > **System Use Notification** to enable System Use Notification Service.
System Status Check	Product software package should be up to date.	Go to **Maintenance** > **Software Upgrade** and click **Check for Upgrade** to retrieve the latest upgrade pack information.
	System backup should be performed at least once a year.	Go to **Maintenance** > **Backup & Restore** and click **Manage** to back up the system.

Copyright © 2024 Moxa Inc.

3.3.1 Account Settings

- Security Check Criteria: Password should be changed within the preset interval.

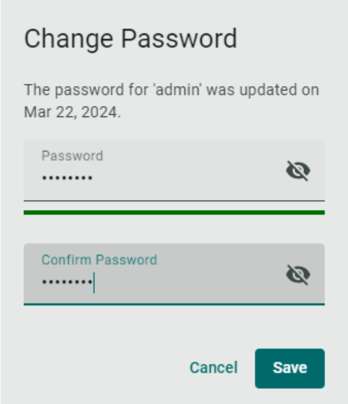
  Go to **Account Management** > **Accounts** to change the password. We recommend changing the password within the preset interval.



Accounts

Account Name	Role	Status	Creation Date
admin (you)	Administrator	✓ Active	22 Mar, 2024

Items per page: 10 1 – 1 of 1



Change Password

The password for 'admin' was updated on Mar 22, 2024.

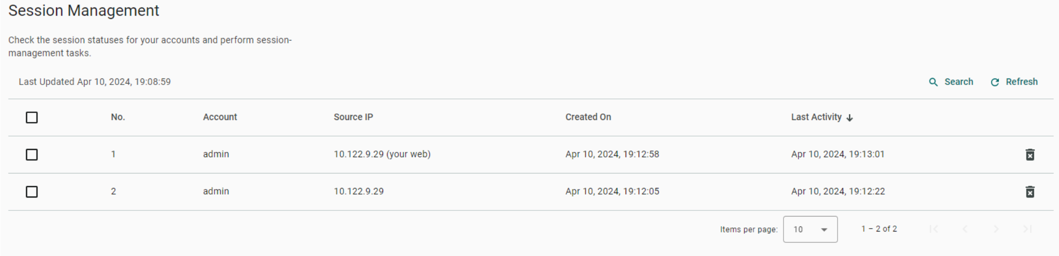
Password: ••••••••

Confirm Password: ••••••••

  To configure a preset interval for changing the password, go to **Account Managements** > **Password Policy** > **Reminder Threshold**.

- Security Check Criteria: An account should have only one active session at any given time.

  Go to **Security** > **Session Management** to identify and manage accounts with more than one session. We recommend deleting connections that you are unaware of, especially in cases where an account has more than one active session.



Session Management

Check the session statuses for your accounts and perform session-management tasks.

Last Updated Apr 10, 2024, 19:08:59

□	No.	Account	Source IP	Created On	Last Activity ↓
□	1	admin	10.122.9.29 (your web)	Apr 10, 2024, 19:12:58	Apr 10, 2024, 19:13:01
□	2	admin	10.122.9.29	Apr 10, 2024, 19:12:05	Apr 10, 2024, 19:12:22

Items per page: 10 1 – 2 of 2

- An account should not have abnormal connections.

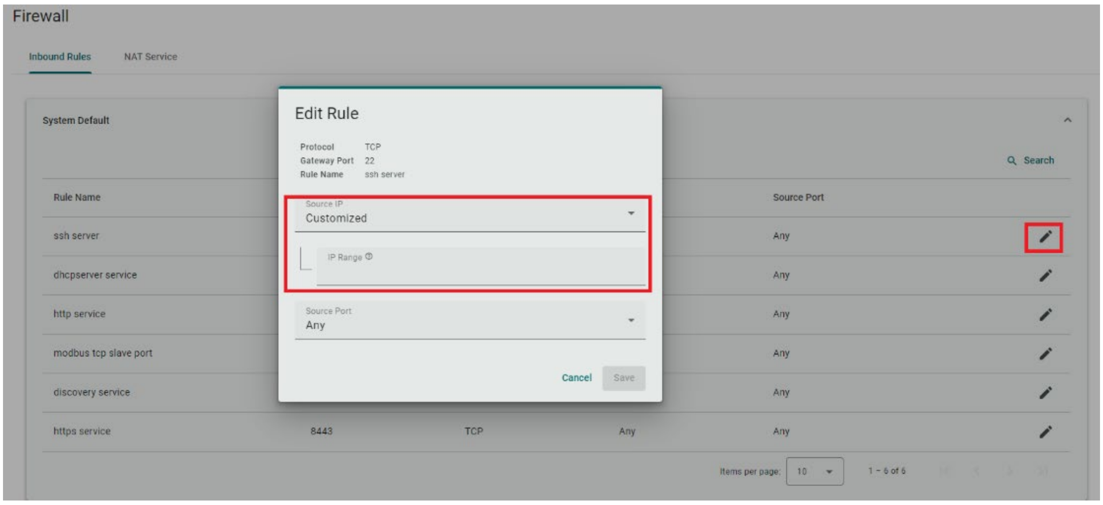
  Go to **Security** > **Session Management** to identify and manage abnormal sessions, such as more than one session per account from different source IPs. We recommend deleting the connections of which you are not aware.

Copyright © 2024 Moxa Inc.

3.3.2 Application Networking

Security Check Criteria: System should not have open network ports.

Understanding which network ports are open is crucial for improving security, preventing vulnerabilities, safeguarding data, staying compliant, and optimizing system resources. We advise minimizing open network ports to reduce cybersecurity risks. To check for open ports in the system, navigate to **Security** > **Firewall**. If there are open ports that are not in use, we strongly recommend disabling them. For the essential open ports, we recommend adding rules to limit access.



Protocol TCP
Gateway Port 22
Rule Name ssh server

Source IP: Customized

IP Range

Source Port: Any

Rule Name				Source Port
ssh server				Any
dhcpserver service				Any
http service				Any
modbus tcp slave port				Any
discovery service				Any
https service	8443	TCP	Any	Any

Items per page: 10 1 – 6 of 6

3.3.3 Application Resource Usage

- Security Check Criteria: IoT Edge modules should not utilize system disk's configurable space.

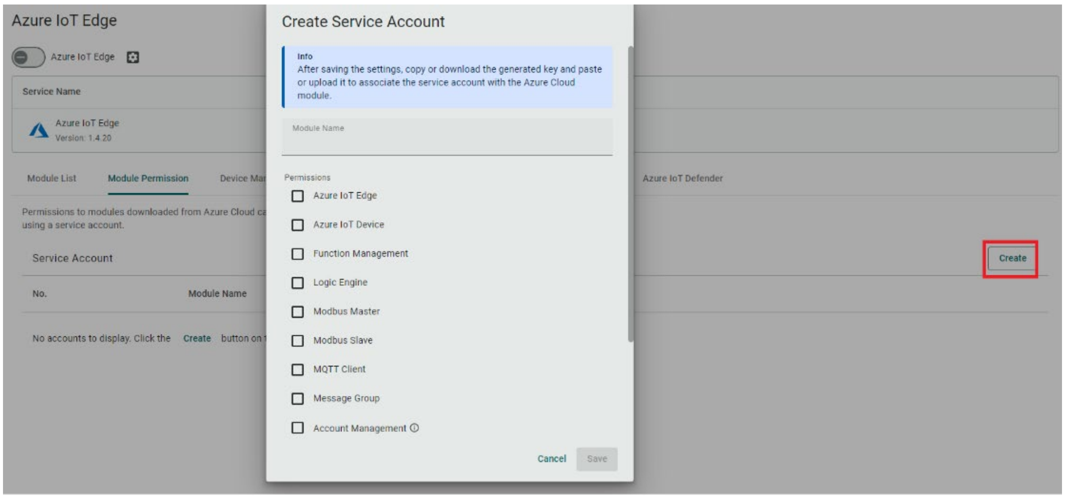
  Our recommendation is for the IoT Edge modules to be deployed only in specific system storage directories/paths such as **/var/run/** and **/tmp/**.

- Security Check Criteria: IoT Edge modules should not utilize system disk's non-configurable space.

  Our recommendation is for the IoT Edge modules to be deployed only in specific system storage directories/paths such as **/var/run/** and **/tmp/**.

- Security Check Criteria: IoT Edge modules should not granted direct privileges.

  Granting permissions to IoT Edge modules in a controlled manner is important for cybersecurity because it reduces the risk of unauthorized access, protects sensitive data, and ensures that each module has access only to what it needs to function properly. To grant permissions to IoT Edges, go to **Cloud Connectivity** > **Azure IoT Edge** > **Module Permission**, create a service account, and grant permission to the IoT Edge module.



Permissions to modules downloaded from Azure Cloud ca using a service account.

No accounts to display. Click the Create button on t

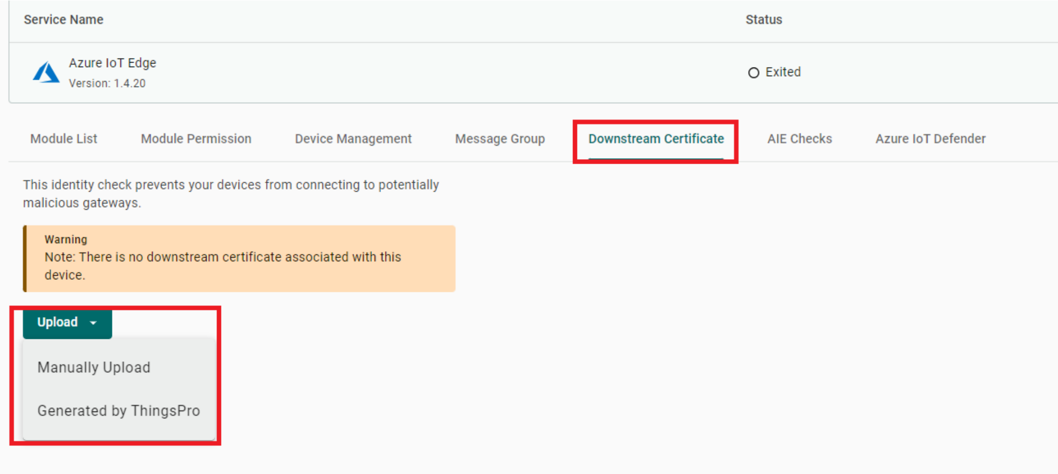
Info
After saving the settings, copy or download the generated key and paste or upload it to associate the service account with the Azure Cloud module.

□ Azure IoT Edge
□ Azure IoT Device
□ Function Management
□ Logic Engine
□ Modbus Master
□ Modbus Slave
□ MQTT Client
□ Message Group
□ Account Management ⓘ

3.3.4 Product Certificate Deployment

- Security Check Criteria: Production Certificate should be configured as an Azure IoT Edge downstream certificate.

  For enhanced security robustness, we recommend using your own certificate instead of the default one. Go to **Cloud Connectivity** > **Azure IoT Edge** > **Downstream Certificate** to upload a certificate.



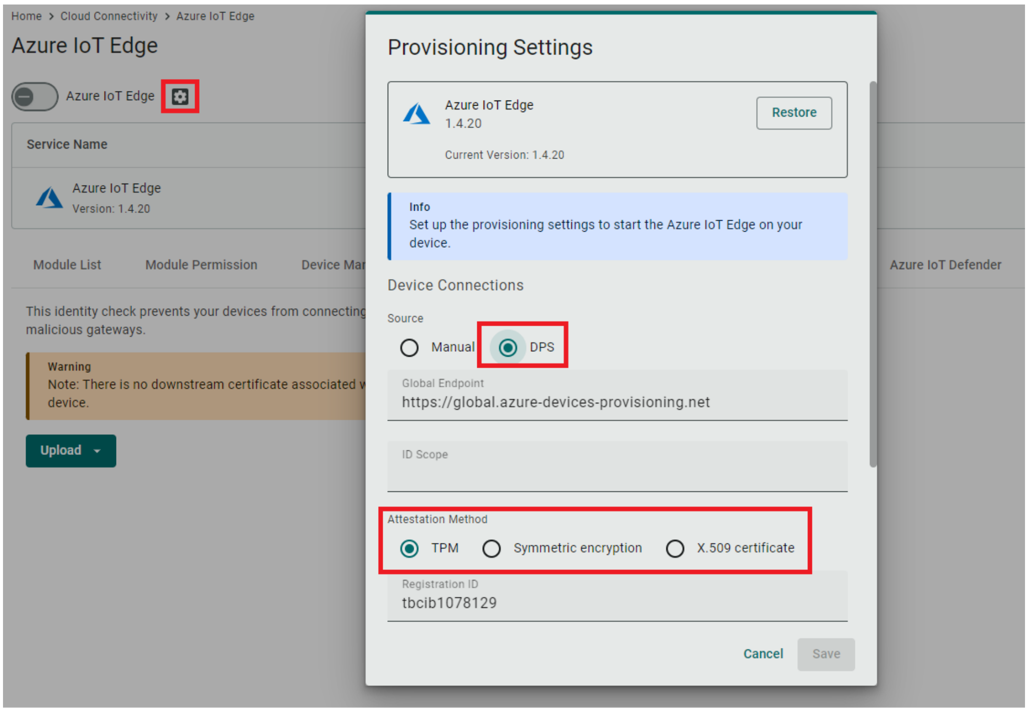
Service Name	Status
Azure IoT Edge Version: 1.4.20	○ Exited

This identity check prevents your devices from connecting to potentially malicious gateways.

Warning
Note: There is no downstream certificate associated with this device.

- Security Check Criteria: Azure IoT Edge should not use connection string for provisioning.

  We recommend an attestation method, which uses a TPM or a X.509 certificate, instead of a manual confirmation using a connection string. You can configure this at **Cloud Connectivity** > **Provisioning Settings** > **DPS**.



This identity check prevents your devices from connecting malicious gateways.

Warning
Note: There is no downstream certificate associated v device.

Provisioning Settings

Azure IoT Edge
1.4.20
Current Version: 1.4.20

Info
Set up the provisioning settings to start the Azure IoT Edge on your device.

Device Connections

Source: ○ Manual ● DPS

Global Endpoint: https://global.azure-devices-provisioning.net

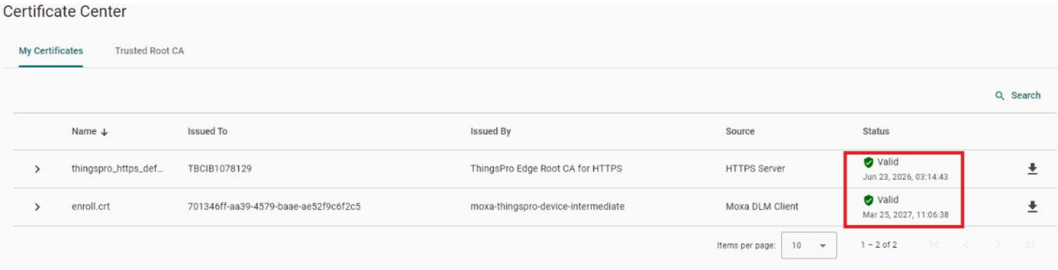
ID Scope:

Attestation Method: ● TPM ○ Symmetric encryption ○ X.509 certificate

Registration ID: tbcib1078129

- Security Check Criteria: All certificates should not expire within the next three months.

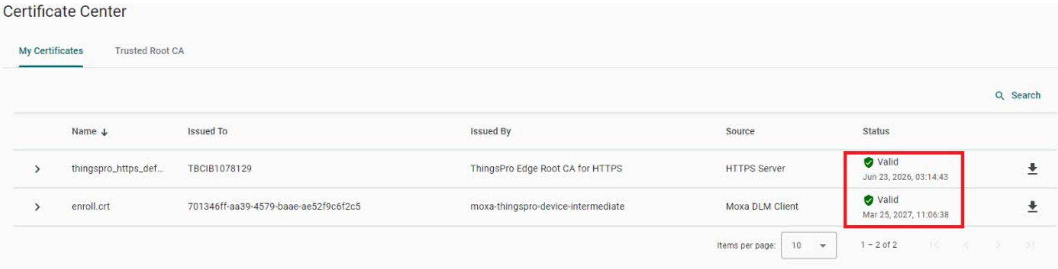
  You can check the status of all the certificates being used by the AIG at **Security** > **Certificate Center**. We recommend regular inspection of the status of the certificates and importing new certificates to replace the ones that are about to expire.



	Name ↓	Issued To	Issued By	Source	Status	
>	thingspro_https_def...	TBCIB1078129	ThingsPro Edge Root CA for HTTPS	HTTPS Server	✓ Valid Jun 23, 2026, 03:14:43	⬇
>	enroll.crt	701346ff-aa39-4579-baae-ae52f9c6f2c5	moxa-thingspro-device-intermediate	Moxa DLM Client	✓ Valid Mar 25, 2027, 11:06:38	⬇

- Security Check Criteria: All certificates should not have expired.

  You can check the status of all the certificates being used by the AIG at **Security** > **Certificate Center**. We recommend regular inspection of the status of the certificates and importing new certificates to replace the ones that are about to expire.



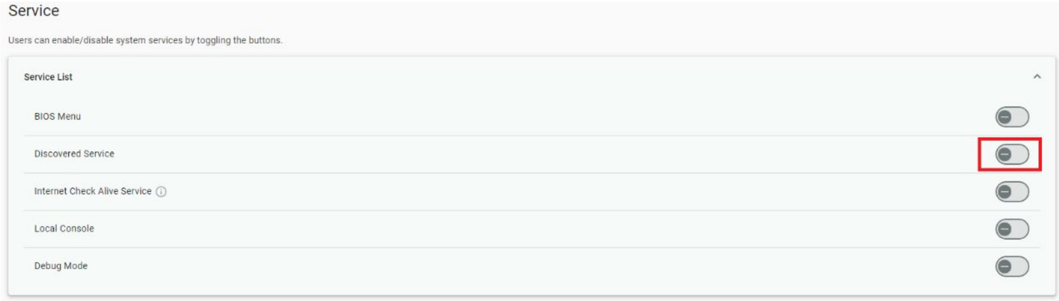
	Name ↓	Issued To	Issued By	Source	Status	
>	thingspro_https_def...	TBCIB1078129	ThingsPro Edge Root CA for HTTPS	HTTPS Server	✓ Valid Jun 23, 2026, 03:14:43	⬇
>	enroll.crt	701346ff-aa39-4579-baae-ae52f9c6f2c5	moxa-thingspro-device-intermediate	Moxa DLM Client	✓ Valid Mar 25, 2027, 11:06:38	⬇

Copyright © 2024 Moxa Inc.

3.3.5 Service Setting

- Security Check Criteria: Discovery Service should not be enabled.

  We recommend disabling the **Discovery Service** in the commissioning stage. Go to **Maintenance** > **Service** to disable the service.



Service

Users can enable/disable system services by toggling the buttons.

Service List

BIOS Menu

Discovered Service

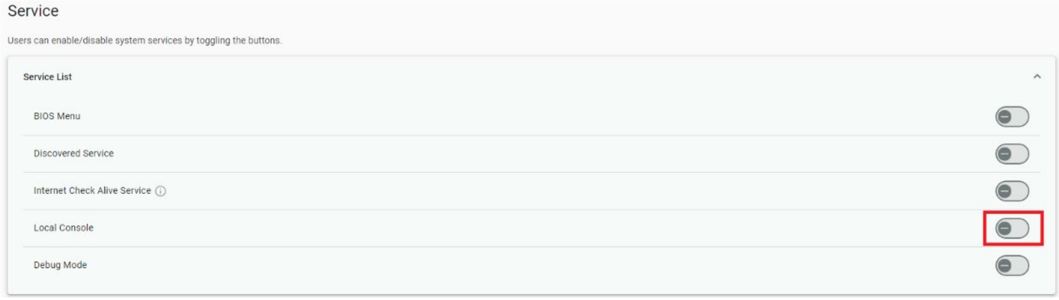
Internet Check Alive Service

Local Console

Debug Mode

- Security Check Criteria: SSH Service should not be enabled.

  We recommend disabling the SSH Service in the commissioning stage. Go to **Maintenance** > **Service** to disable Debug Mode.



Service

Users can enable/disable system services by toggling the buttons.

Service List

BIOS Menu

Discovered Service

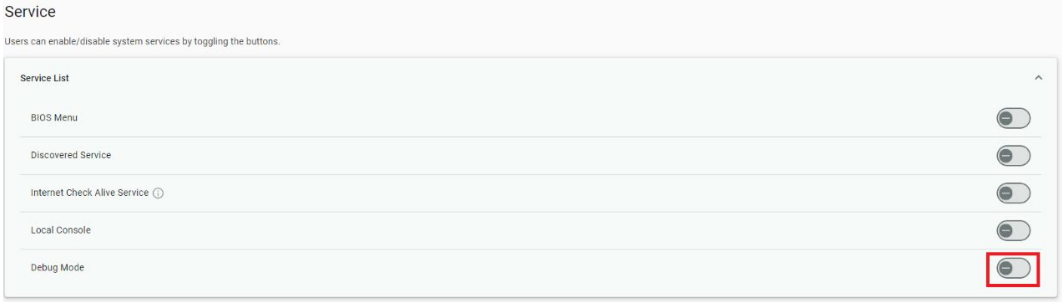
Internet Check Alive Service

Local Console

Debug Mode

- Security Check Criteria: Serial Console Service should not be enabled.

  We recommend disabling Serial Console Service in commissioning stage. Go to **Maintenance** > **Service** to disable the Local Console.



Service

Users can enable/disable system services by toggling the buttons.

Service List

BIOS Menu

Discovered Service

Internet Check Alive Service

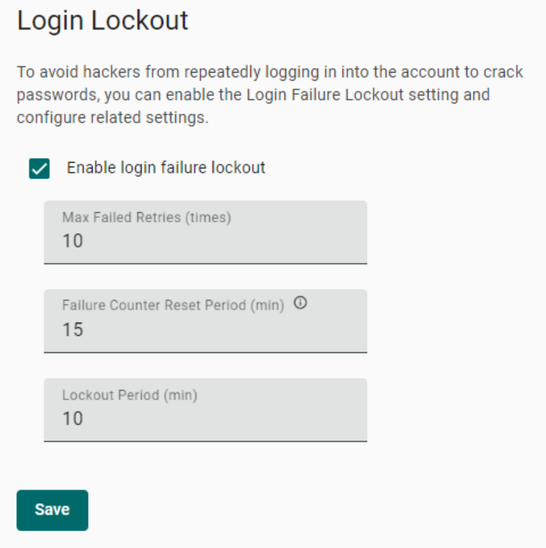
Local Console

Debug Mode

Copyright © 2024 Moxa Inc.

- Security Check Criteria: Account Lock Service should be enabled.

  To thwart brute-force attacks, we recommend activating the Account Lock Service. When AIG detects multiple failed login attempts surpassing the set threshold, it will automatically lock the account for the specified duration. Go to **Security** > **Login Lockout** to enable and configure parameters for this service.



Login Lockout

To avoid hackers from repeatedly logging in into the account to crack passwords, you can enable the Login Failure Lockout setting and configure related settings.

☑ Enable login failure lockout

Max Failed Retries (times): 10

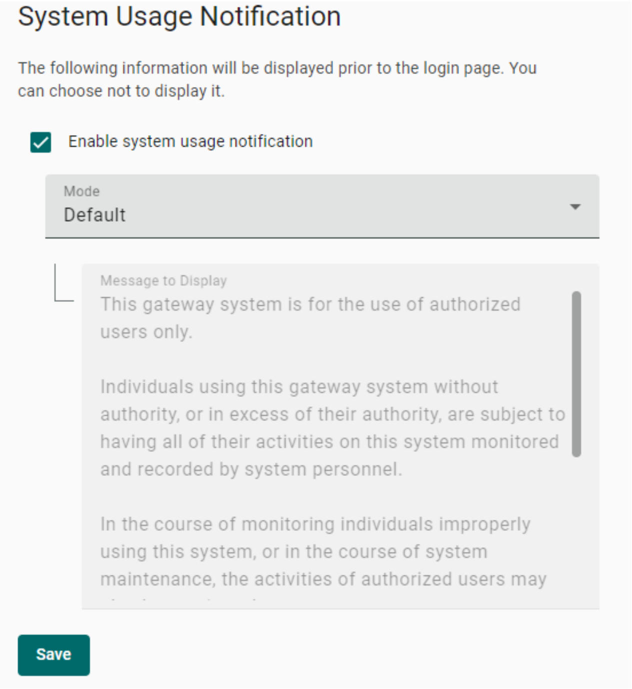
Failure Counter Reset Period (min): 15

Lockout Period (min): 10

- Security Check Criteria: System Use Notification Service should be enabled.

  It is important to display system usage notifications prior to the login page so users know the rules and risks involved in using the system. This helps meet legal requirements, reduces risks, and holds users accountable for their actions.

  Go to **Security** > **System Usage Notification** to enable this function.



System Usage Notification

The following information will be displayed prior to the login page. You can choose not to display it.

☑ Enable system usage notification

Mode: Default

Message to Display:

This gateway system is for the use of authorized users only.

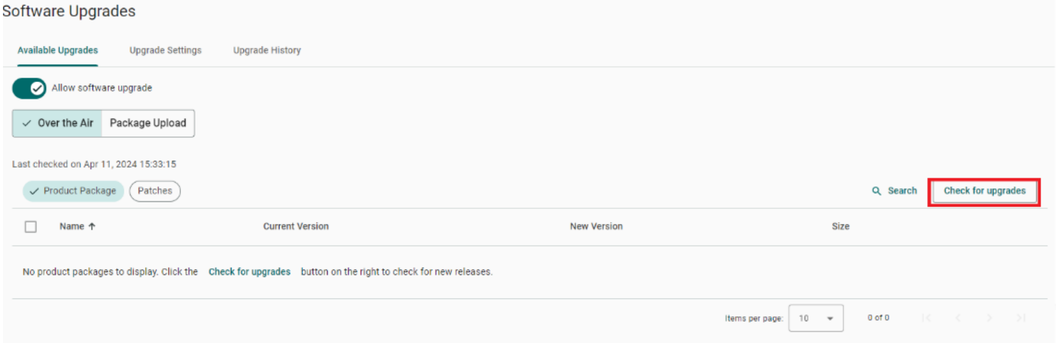
Individuals using this gateway system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.

In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may

3.3.6 System Status Check

- Security Check Criteria: Product software package should be up to date.

  The importance of security cannot be overstated when it comes to keeping your product software up to date. Regular updates help patch vulnerabilities, reduce the risk of cyberattacks, and protect sensitive data, safeguarding your system and users from potential security threats. Go to **Maintenance** > **Software Upgrades** to retrieve up-to-date software for your AIG.

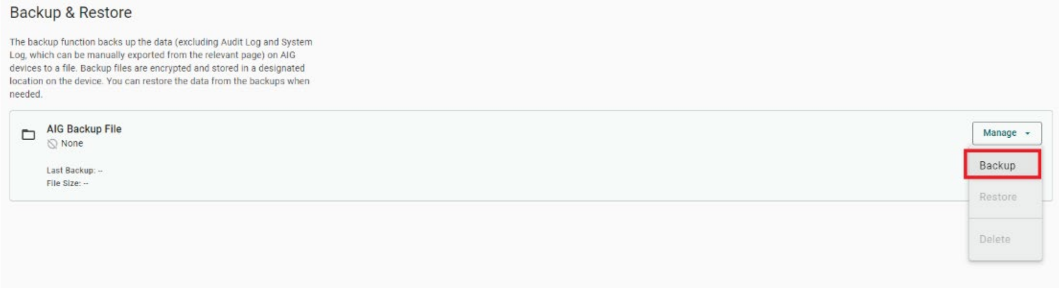


Last checked on Apr 11, 2024 15:33:15

No product packages to display. Click the Check for upgrades button on the right to check for new releases.

- Security Check Criteria: System backup should be performed at least once a year.

  Performing a system backup annually is important to protect your data in case of system failures, cyberattacks, or disasters. It ensures you can quickly recover your information, stay compliant with regulations, and maintain business continuity. Go to **Maintenance** > **Backup & Restore** to back up your system.



The backup function backs up the data (excluding Audit Log and System Log, which can be manually exported from the relevant page) on AIG devices to a file. Backup files are encrypted and stored in a designated location on the device. You can restore the data from the backups when needed.

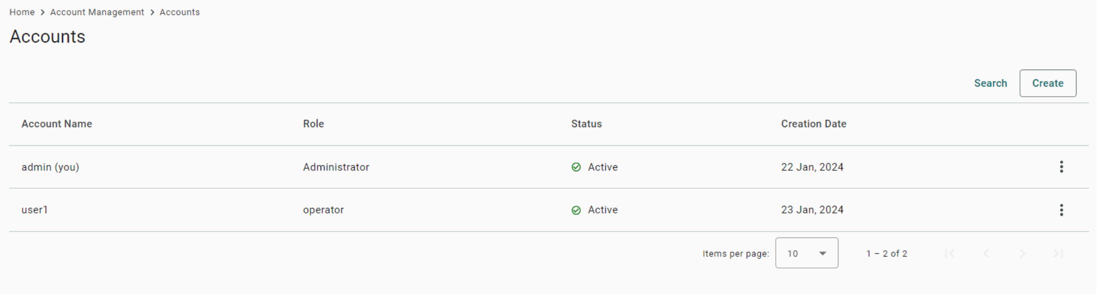
Last Backup: --
File Size: --

3.4 Account Management

You can maintain user accounts and assign a role with specific permissions to each account. These functions allow you to track and control the access to the device.

3.4.1 Accounts

You can **View**, **Create**, **Edit**, **Deactivate**, and **Delete** user accounts. In the main menu, go to **Account Management** > **Accounts** to manage user accounts.



Accounts

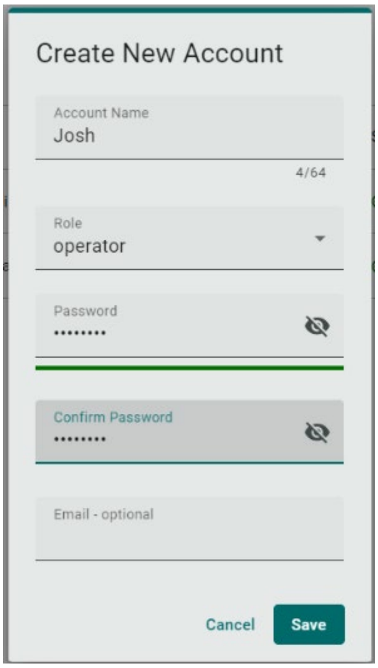
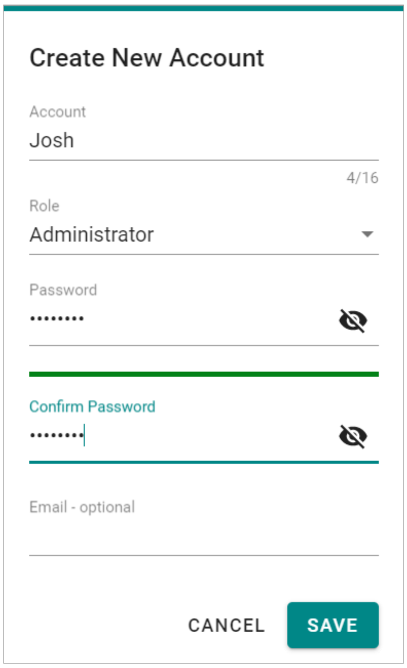
Account Name	Role	Status	Creation Date
admin (you)	Administrator	Active	22 Jan, 2024
user1	operator	Active	23 Jan, 2024

Items per page: 10 1 – 2 of 2

Creating a New User Account

Click **+ Create** to create a new user account. In the dialogue box that is displayed, fill in the fields and click **SAVE**.

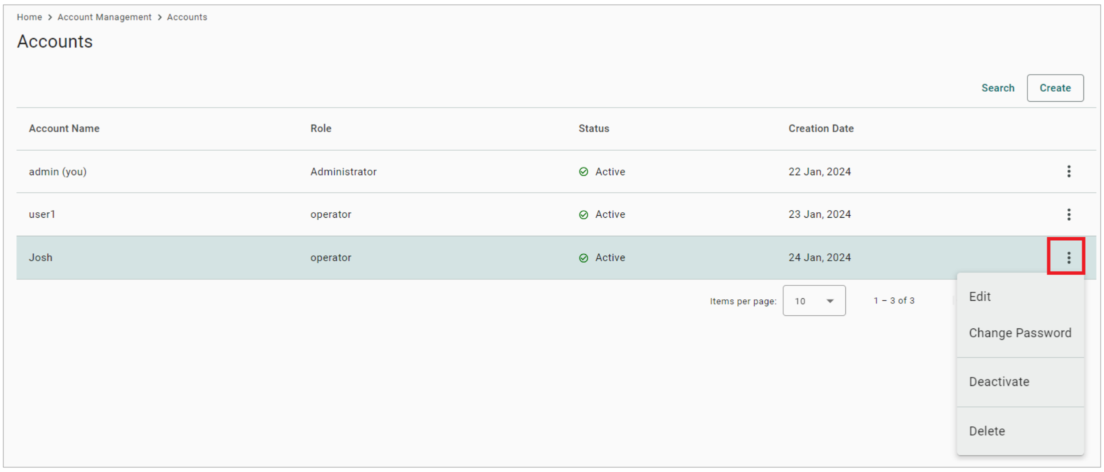
Note To comply with security policy and best practices, specify a strong password that is at least eight characters long, consisting of at least one number and at least one special character.

Password Policy	Valid Password
 Create New Account Account Name: Josh (4/64) Role: operator Password: •••••••• Confirm Password: •••••••• Email - optional Cancel Save	 Create New Account Account: Josh (4/16) Role: Administrator Password: •••••••• Confirm Password: •••••••• Email - optional CANCEL SAVE

Copyright © 2024 Moxa Inc.

Managing Existing User Accounts

To manage an account, click on the pop-up menu icon for the account.



Home > Account Management > Accounts

Accounts

Account Name	Role	Status	Creation Date
admin (you)	Administrator	✓ Active	22 Jan, 2024
user1	operator	✓ Active	23 Jan, 2024
Josh	operator	✓ Active	24 Jan, 2024

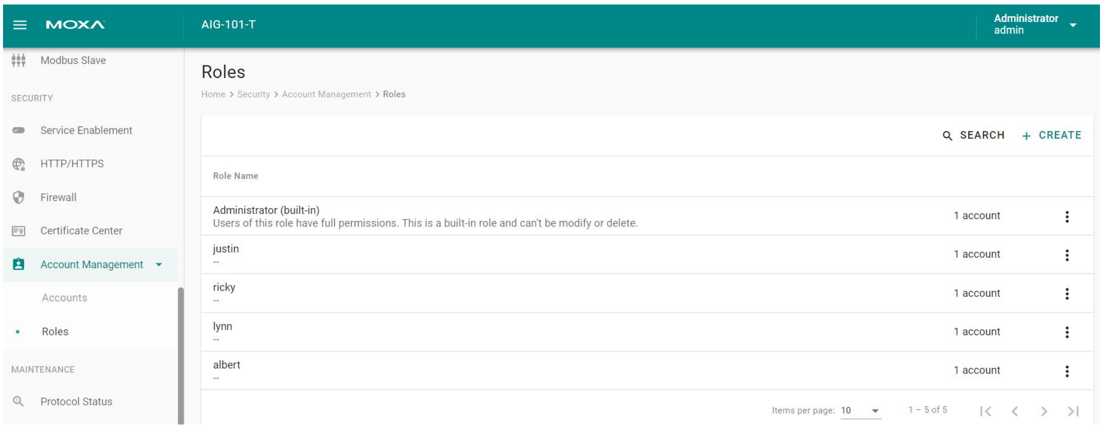
Items per page: 10 1 – 3 of 3

Function	Description
Edit	Change the role, email, or password of an existing account
Deactivate	Does not allow the user to log in to the device
Delete	Delete the user account (**NOTE:** This operation is irreversible.)

Note You cannot **Deactivate** or **Delete** the last remaining account with an Administrator role. This is to prevent an unauthorized account from fully managing the system. When the system detects only one active account when selecting the Administrator role, all items in the pop-up menu are grayed out.

3.4.2 Roles

You can **View**, **Create**, **Edit**, and **Delete** user roles for your AIG device here.



Roles

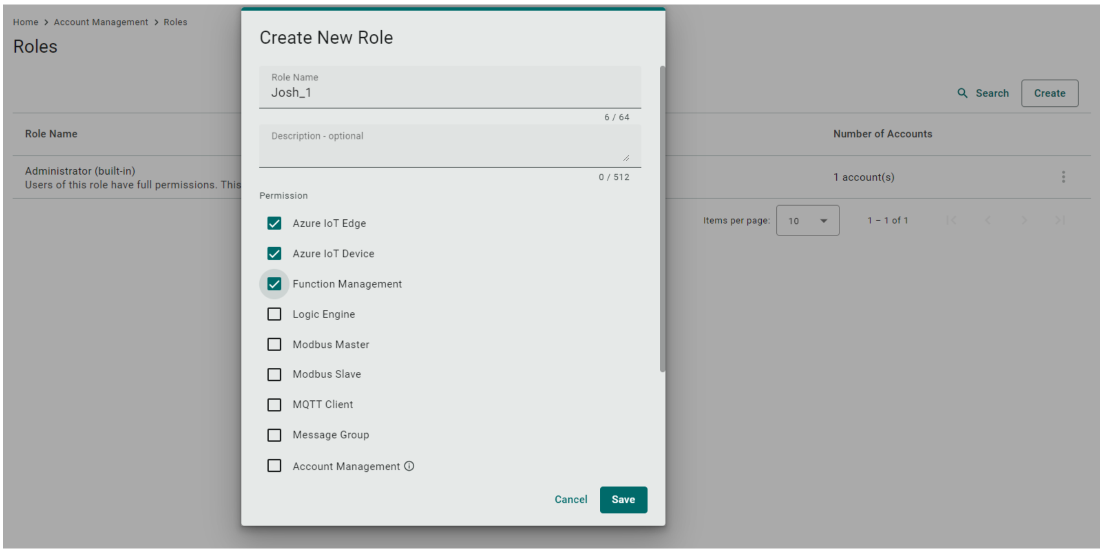
Home > Security > Account Management > Roles

Role Name		
Administrator (built-in) Users of this role have full permissions. This is a built-in role and can't be modify or delete.	1 account	⋮
justin --	1 account	⋮
ricky --	1 account	⋮
lynn --	1 account	⋮
albert --	1 account	⋮

Items per page: 10 1 – 5 of 5

Click **+ Create** to set up a new user role. Specify a unique name for the role and assign the appropriate permissions and click **Save** to create the role in the system.

Copyright © 2024 Moxa Inc.


Home > Account Management > Roles

Roles

Create New Role

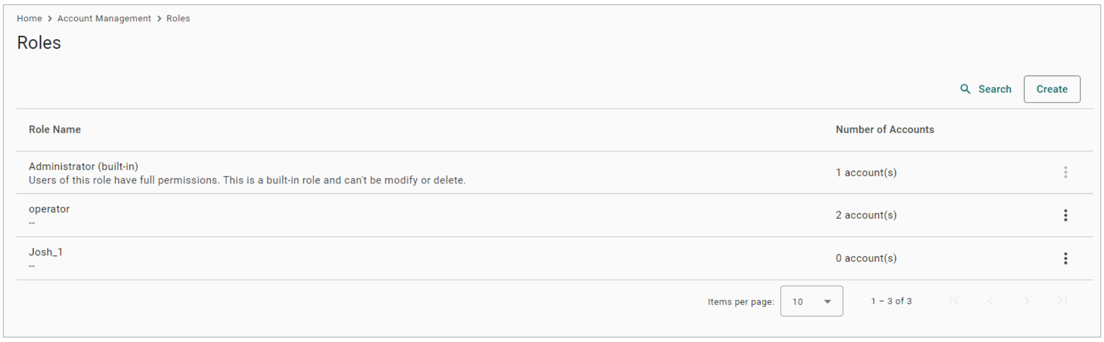
Role Name: Josh_1 (6 / 64)

Description - optional (0 / 512)

Permission

☑ Azure IoT Edge
☑ Azure IoT Device
☑ Function Management
☐ Logic Engine
☐ Modbus Master
☐ Modbus Slave
☐ MQTT Client
☐ Message Group
☐ Account Management ⓘ

You can **edit** the settings or **delete** an existing role by clicking on the pop-up menu icon next to the role.

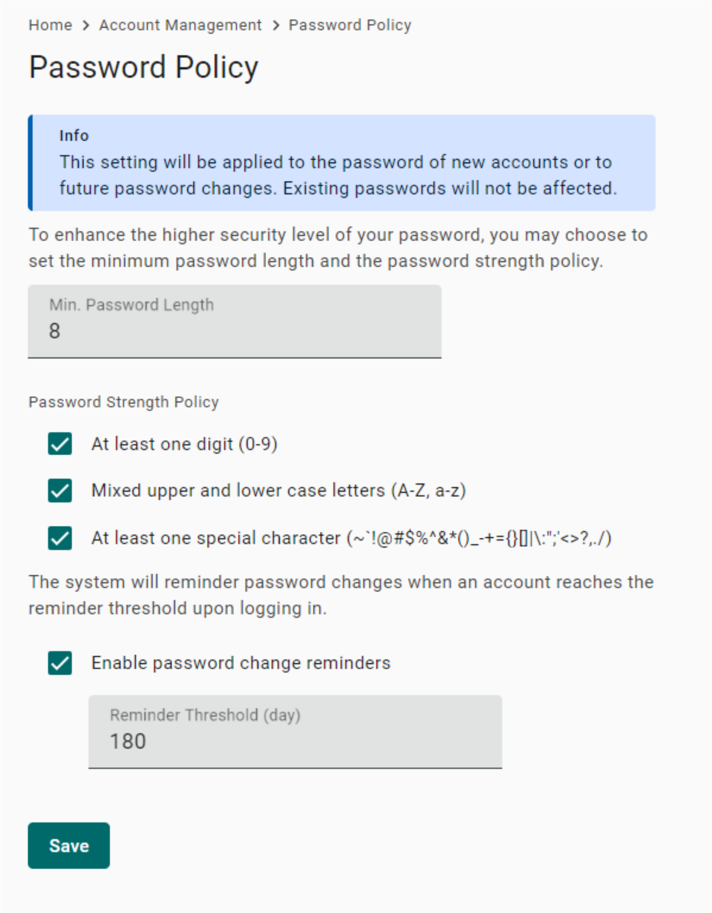

Home > Account Management > Roles

Roles

Role Name	Number of Accounts
Administrator (built-in) Users of this role have full permissions. This is a built-in role and can't be modify or delete.	1 account(s)
operator --	2 account(s)
Josh_1 --	0 account(s)

When the role has been set up, it is available for selection by accounts.

3.4.3 Password Policy



Password Policy

Info
This setting will be applied to the password of new accounts or to future password changes. Existing passwords will not be affected.

To enhance the higher security level of your password, you may choose to set the minimum password length and the password strength policy.

Min. Password Length
8

Password Strength Policy

☑ At least one digit (0-9)

☑ Mixed upper and lower case letters (A-Z, a-z)

☑ At least one special character (~`!@#$%^&*()_-+={}[]|\:";'<>?,./)

The system will reminder password changes when an account reaches the reminder threshold upon logging in.

☑ Enable password change reminders

Reminder Threshold (day)
180

Parameter	Value	Description
Min. Password Length	8 to 256	The minimum password length
Password Strength Policy		To define how the AIG checks the password strength
Password Change Reminders	10 to 360 days	Notify user to change the password

Copyright © 2024 Moxa Inc.