



Common Industrial Protocol

- [Information about CIP, on page 1](#)
- [CIP restrictions, on page 1](#)
- [Enabling CIP, on page 1](#)
- [CIP password encryption, on page 2](#)
- [Additional references, on page 4](#)

Information about CIP

The Common Industrial Protocol (CIP) is an industrial protocol for industrial automation applications. Previously known as Control and Information Protocol, CIP encompasses a comprehensive suite of messages and services for the collection of manufacturing automation applications - control, safety, synchronization, motion, configuration and information.

It is supported by Open DeviceNet Vendors Association (ODVA), an organization that supports network technologies based upon CIP such as DeviceNet, EtherNet/IP, CIP Safety and CIP Sync. CIP allows users to integrate these manufacturing applications with enterprise-level Ethernet networks and the Internet.

CIP restrictions

CIP can be enabled on only one VLAN on the switch.

Enabling CIP

Before you begin

By default, CIP is not enabled

Procedure

Step 1 Enters global configuration mode.

Configure Terminal

- Step 2** Sets CIP security options on the switch.
- ```
cip security { password password | window timeout value }
```
- Step 3** Enters interface configuration mode.
- ```
interface vlan 20
```
- Step 4** Enables CIP on a VLAN.
- ```
cip enable
```
- Step 5** Returns to privileged EXEC mode.
- ```
end
```
- Step 6** Verifies your entries.
- ```
show running-config
```
- Step 7** (Optional) Saves your entries in the configuration file.
- ```
copy running-config startup-config
```
- Step 8** (Optional) Displays information about the CIP subsystem.
- ```
show cip { connection | faults | file | miscellaneous |
object | security | session | status }
```
- Step 9** (Optional) Enables debugging of the CIP subsystem.
- ```
debug cip {assembly | connection manager | dlr | errors  
| event | file | io | packet | infra | security | session | socket}
```
-

CIP password encryption

Common Industrial Protocol (CIP) password encryption is a security feature for industrial environments that

- protects CIP credentials within device configuration files,
- uses the Type 8 (SHA256) hashing algorithm to meet modern security standards, and
- ensures that stored credentials are irreversible and resistant to cryptographic attacks.

Type 8 encryption is a strong, irreversible hashing method that replaces the legacy Type 7 encryption to improve the security posture of industrial deployments.

Table 1: Feature history table

Feature name	Release information	Description
CIP password encryption	26.2.1	This feature provides enhanced security by converting legacy CIP passwords to the irreversible Type 8 (SHA256) algorithm to resist cryptographic attacks. It ensures credential integrity and uninterrupted authentication across industrial deployments.

Type 8 password encryption advantages

Type 8 password encryption provides security and operational advantages by automatically converting legacy passwords during the Cisco IOS XE software upgrade. This irreversible method reinforces credential security by preventing the system from converting passwords back to plaintext. During migration, the system handles invalid or corrupted data gracefully to ensure data integrity. By storing these passwords in the configuration file, the system maintains consistency across reboots and device transfers. It also integrates with the CIP module to provide uninterrupted authentication and communication.

CIP password encryption transitions

When you upgrade the software image to release 26.2.1 or later, the system automatically detects existing CIP passwords stored with Type 7 encryption. The system converts these passwords to the strong, irreversible Type 8 hashing algorithm and saves them into the device configuration file.

Guidelines and restrictions of CIP

Guidelines

- Downgrading to a software version earlier than 26.2.1 removes the CIP password from the configuration.
- Plaintext passwords must be stored externally as they cannot be retrieved once encrypted.
- Manual configuration transfers preserve CIP password.

Restrictions

Type 8 encryption is irreversible, and the original plaintext password cannot be recovered from the device.

Configure CIP password encryption

Set a password to secure CIP communications.

You can enter a plaintext password, which the system automatically converts to Type 8 encryption in the configuration file, or you can manually enter a pre-encrypted Type 8 (SHA256) hash.

Before you begin

Ensure the device is running release 26.2.1 or later to support Type 8 encryption.

Procedure

- Step 1** Use the `configure terminal` command to enter global configuration mode.
- Example:**
- ```
Switch# configure terminal
```
- Step 2** Use the `cip security { password <pass_word> | password 8 <SHA256-encrypted-password> }` command to configure the password based on your available credential format.
- Example:**
- ```
Switch(config)# cip security password cisco
```
- Use the `cip security password 8 <SHA256-encrypted-password>` command to enter a pre-encrypted Type 8 hash.
- Step 3** Use the `exit` command to return to privileged EXEC mode.
- Example:**
- ```
Switch(config)# exit
```
- Step 4** Use the `copy running-config startup-config` command to copy the running configuration to NVRAM.
- Example:**
- ```
Switch# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Additional references

Related documents

Related Topic	Document Title
Cisco IOSbasic commands	Cisco IOS Configuration Fundamentals Command Reference

Standards and RFCs

Standard/RFC
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.

Technical Assistance

Standard/RFC	Title
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	https://www.cisco.com/support

Additional references