# Security Architecture

This chapter provides information on the security architecture, feature set, configurations, and practices used by Cisco to ensure that Cisco Optical Network Controller is highly secured and can safely be deployed without any risk or vulnerability. Cisco continuously follows industry-accepted developments and practices, and regularly updates Cisco Optical Network Controller to maintain these standards.

The feature set is described by category, with configurations that reduce risk, a list of supported standards, and explanations of the development and deployment processes. Cisco Optical Network Controller uses a layered security model. Each logical component delivers a distinct security function, and every step in the security process must be completed before moving to the next. For example, user authorization is allowed only after a user is authenticated.

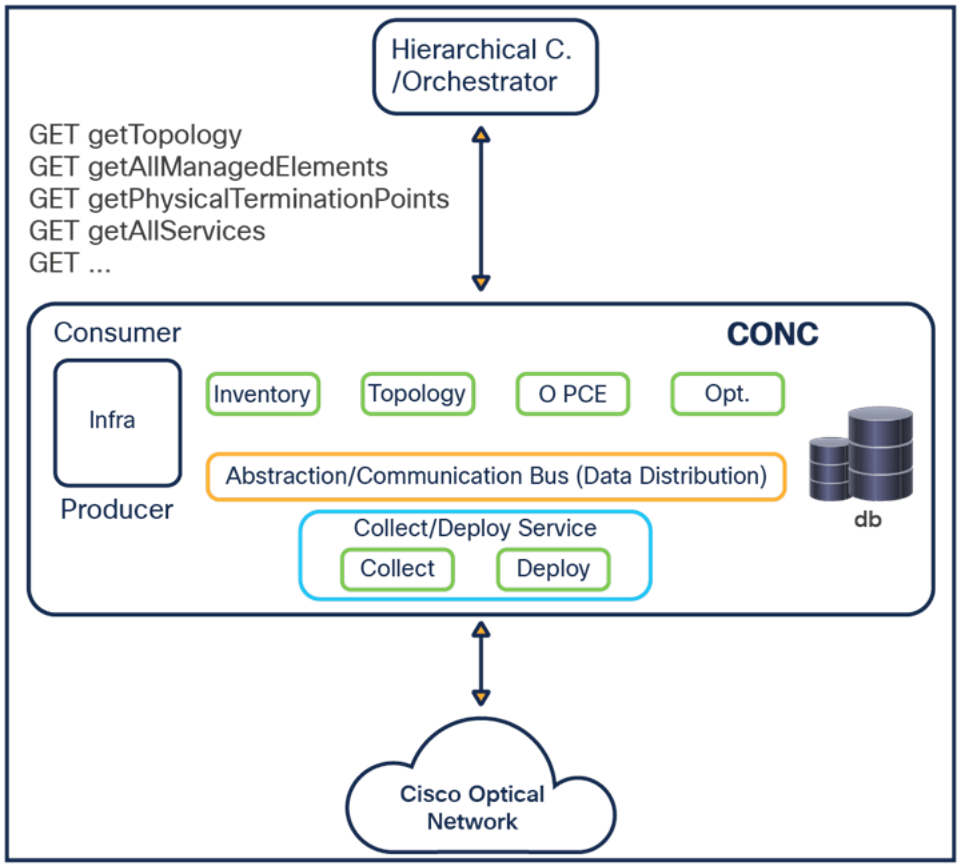


# Cisco Optical Network Controller architecture overview

The Cisco Optical Network Controller (CONC) high-level architecture places CONC between a hierarchical controller or orchestrator and the Cisco optical network. The hierarchical controller or orchestrator uses the northbound interface to request abstracted optical network information and service data from CONC.

The architecture shows example northbound operations such as GET getTopology, GET getAllManagedElements, GET getPhysicalTerminationPoints, and GET getAllServices. These operations allow the higher-level controller to consume topology, managed element, physical termination point, and service information without directly managing optical devices.

*Figure 1: Cisco Optical Network Controller High-Level Architecture*




Inside CONC, consumer and producer functions exchange information through the Abstraction/Communication Bus, which provides data distribution across the controller. The bus separates higher-level consumers from device-specific collection and deployment logic.

The CONC architecture includes these components:

- Infra, which provides the infrastructure function shown on the consumer and producer side of the CONC boundary.
- Inventory, which maintains managed element and resource information for the optical domain.
- Topology, which maintains the abstracted network topology made available to the hierarchical controller or orchestrator.
- O-PCE, which supports optical path computation for the services and topology managed by CONC.
- Optimization (Opt.), which represents optimization functions operating on network and service data.
- Database (db), which stores controller data used by CONC functions.
- Collect/Deploy Service, which contains Collect and Deploy functions for interaction with the Cisco optical network.
- Collect, which gathers network data from the Cisco optical network and feeds it into CONC.
- Deploy, which sends service or configuration changes from CONC to the Cisco optical network.

The southbound side of the architecture connects CONC to the Cisco optical network. CONC collects network state from the optical domain, distributes that data internally, and exposes the resulting abstracted view to the hierarchical controller or orchestrator.

# Crosswork framework services

Cisco Optical Network Controller (CONC) runs on the Crosswork framework. The framework provides common platform services used by CONC applications and controller functions.

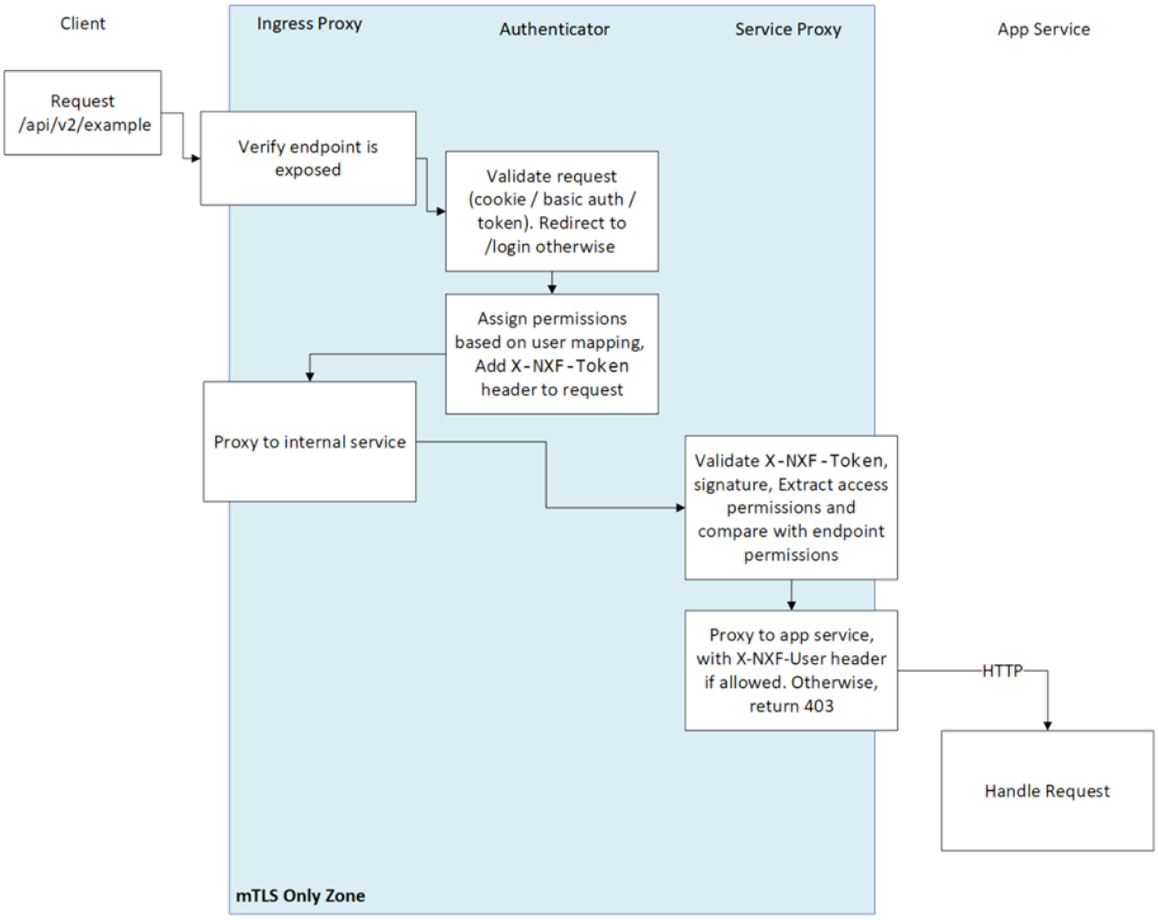
The Crosswork framework provides the following supporting services for CONC:

- User management for controlling access to CONC applications and services.
- Logging and monitoring services for controller operation and troubleshooting.
- A common Kafka bus for message exchange and data distribution across CONC functions.
- Underlying platform support for high availability (HA).
- Underlying platform support for scale.

# Authentication flow

All HTTP(s) requests are authenticated throughout the system, both inside and outside the cluster.

*Figure 2: Cisco Optical Network Controller Authentication Flow*




Every request MUST have an X-NXF-Token header, which is an ES256 signed JWT header issued by either Authenticator - for exposed endpoints, or NextFusion Controller - for internal endpoints.

Whenever a service starts, the NextFusion Controller issues a short-lived token which gets pushed to the service proxy. This token contains the permissions that were declared in the service access field in the CRD.

When trying to access some service endpoint, Service Proxy checks the X-NXF-Token of the request with the allowed permission field of this endpoint. If the user is authorized for this action, Service Proxy proxies the request to the app service, including an X-NXF-User header, which contains the decoded user profile.

The Ingress Proxy Server is configured as a reverse proxy server, intercepts all requests to the Cisco Optical Network Controller, and acts as the first line of defense against security attacks. The Ingress Proxy Server only accepts HTTPS packets on port 8443. The Ingress Proxy Server uses the NextFusion Authenticator to perform client authorization and authentication for Cisco Optical Network Controller. The Ingress Proxy Server is the only component that is accessible from outside the device on which Cisco Optical Network Controller is installed. The HTTP and SQL connections are internal connections that are bound to local interfaces and are not accessible from outside.

## Password storage

Password storage uses secure, salted password hashing for local authentication. A salt is random data used as input to a hashing function, preventing dictionary attacks. This significantly increases security by protecting passwords even if the password file is compromised. The hashing function used is bcrypt, based on the Blowfish cipher. Bcrypt incorporates a salt to protect against rainbow table attacks and is an adaptive function that ensures Cisco Optical Network Controller remains resistant to brute-force search attacks even with increasing computation power.

## Containers

Cisco Optical Network Controller (CONC) components are designed as microservices. These components are packaged as Docker images and launched in Kubernetes (K8s) pods.

This container-based architecture supports scale and alignment with Cisco automation products and platforms.

## Database

Cisco Optical Network Controller uses Postgres as the database. Access to the database is restricted per service by mutual TLS. Tables of sensitive data, such as network element details and user credentials, are all encrypted (encryption is by AES256 GCM).

# User access and authentication

Cisco Optical Network Controller authenticates users by communicating with an external LDAP server or locally for users defined in Cisco Optical Network Controller. Each user accessing the system is uniquely authenticated. Each user can open multiple sessions concurrently. Cisco Optical Network Controller users can only interact with the platform resources and cannot gain underlying OS access from the platform. Access management for the host OS and the Cisco Optical Network Controller platform are managed separately.

## User groups

User groups can be defined in the LDAP server, which passes them to Cisco Optical Network Controller. These groups are mapped to user roles (see more in Authentication).

## Local users

Cisco Optical Network Controller allows the creation of local users. As a best practice, locally defined users should be limited to admin users only.

## Password policy settings

The password strength forced for local users can be enabled or disabled and can be set in scores of 1 to 5 (weak to strong). The password is checked against several dictionaries and common passwords lists, to ensure its complexity according to the selected score.

# Role-based access control

Cisco Optical Network Controller supports role-based access control (RBAC), which allows you to assign each user (either locally defined or an LDAP user) to a role individually. Each role has its own set of permissions and inherits permissions of the lower-level roles. There are four pre-defined user roles: read-only, user, support, and admin.

| Cisco Optical Network Controller Role | Permissions |
|---|---|
| read-only | Read-only access to Cisco Optical Network Controller Explorer UI. |
| user | Access to Cisco Optical Network Controller Explorer UI and all apps, some of which can change the network. |
| support | Same permissions as the User role with the addition of access to Cisco Optical Network Controller diagnostic tools for the Cisco Support Team. |
| admin | Full control over configuration and all users.<br>Access to Configuration UI, Cisco Optical Network Controller Explorer UI, and all apps. |

# Communication with LDAP server

The LDAP application protocol is an open, vendor-neutral industry standard for accessing and maintaining distributed directory information services. LDAP authentication is similar, but its communication occurs over an encrypted transport connection. Local authentication is encrypted over HTTPS.

# Administrator options

The administrator can set the login banner, lock users and unlock users (preventing them from logging in), and set the idle session expiration time.

# SSO server communication

If you use the same SSO server (SAML 2.0) for several of the Crosswork platform applications, you only need to log in once.

# User lockout policy

After a configurable number of unsuccessful login attempts, the system block the IP. The blocking period starts with a short duration and increases with each failed login attempt. The default number of login attempts is 8. The system does not handle login attempts from the IP address during this period. For more information, see the Session Login Limiter section.

## Role assignment to user

A Cisco Optical Network Controller administrator provides Cisco Optical Network Controller a Bind DN and password that Cisco Optical Network Controller then uses to connect and query the LDAP server. The administrator also configures the search base, search filter, and mapping between LDAP groups and Cisco Optical Network Controller roles. This mapping policy identifies who can log in to the Cisco Optical Network Controller Explorer UI and what role they have. All users who meet both the search base and the search filter criteria can log in with the roles (access privileges) assigned to their group. If the user is not a member of any group mapped to a Cisco Optical Network Controller role, the system rejects the login attempt. The Cisco Optical Network Controller administrator also assigns roles to local users not handled by LDAP. You can disable both local users and access to the LDAP server so that one or the other method can be used for authentication and authorization.

# Access to VM and containers

For more information on the control plane and Virtual Management networks installation requirements and ports, see the *Cisco Optical Network Controller Installation Guide*.

# HTTP access in northbound interface

The Cisco Optical Network Controller management interface uses secure interfaces. HTTPS/Secure WebSocket is used on the management interface for application-level management for both the GUI and NBI. Web access to Cisco Optical Network Controller UI and Web services (REST commands) is protected with TLS v1.2/1.3. The URL does not include user credentials or device-sensitive information.

# Access in southbound interface

All control traffic between Cisco Optical Network Controller and NEs/NMSs is encrypted if the NE/NMS provides an encrypted interface. As a best practice policy, Cisco chooses the most secure interface/protocol the NE/NMS offers.

# Audit trail log (accounting)

The system audits and logs all user login/logout and operations activities in applications. You can export these to external systems. The audit log contains the username, hostname, time, operation, specific information, and results.

# Events and notifications

Cisco Optical Network Controller database stores the system events. You can access these events using SHQL commands. These events include:

- Applications activities
- Updates in network inventory and topology

# EU data protection directive

As a network controller, Cisco Optical Network Controller deals with network data. It does not deal with data associated with a ‘natural person’ as defined within GDPR and outlined by the EU data protection directive. Cisco acts as the data processor when addressing support tickets. The Service Provider customer remains the data controller, and data processor, using Cisco Optical Network Controller. There is no personal data associated with a ‘natural person’.

# Development security procedures

Cisco’s continuous integration build process runs a static check, which includes security checks. Static analysis does not allow the build to continue if there are high-severity warnings, such as security warnings. The continuous integration process also runs a Web Server scanner on an instance of Cisco Optical Network Controller that is automatically deployed for integration test purposes.

The security tools, which are referenced by OWASP, are FindBugs, Find Security Bugs plug-in and Test-ssl which verifies SSL configuration.

- FindBugs is an open-source tool that uses static analysis to detect bug patterns in Java code. Potential errors are ranked, enabling developers to readily understand the possible impact or severity. One of the main techniques FindBugs uses is syntactically matching source code to known suspicious programming practices.
- Find Security Bugs is a FindBugs plugin for security audits of Java Web applications. It can detect dozens of vulnerability types with hundreds of unique signatures. The tool provides extensive references for each bug pattern with references to OWASP Top 10 and CWE. The tool is constantly updated to identify newly discovered vulnerabilities.
- Test-ssl is a command line tool that checks a server's service on any port for the support of TLS/SSL ciphers, protocols, recent cryptographic flaws and more.

# Security patches update policy

Cisco Optical Network Controller is compliant with Cisco’s security patch update policy.

# Security vulnerabilities

Cisco Optical Network Controller follows the standard Cisco process for discovering, addressing, and reporting security vulnerabilities. This process is well documented, and this customer portal provides policies and documentation: Cisco Security.