Security in the Cisco Intersight Platform

Delivering a secure, cloud-hosted management platform.

Built-in security you can trust

When your IT infrastructure resides in an enterprise data center, at the network edge, and in remote and branch offices, the use of separate tools in each location poses management challenges. The Cisco Intersight™ platform unifies and simplifies management for your Cisco Unified Computing System™ (Cisco UCS®) and Cisco HyperFlex™ systems. Using a secure Internet connection, our infrastructure management-as-a-service portal makes it easy to securely deploy, operate, and manage your IT infrastructure wherever it resides.

Contents

Cisco Intersight platform

The Cisco Intersight software-as-a-service (SaaS) platform helps you translate your intent–what you want to accomplish–into infrastructure configuration, ongoing management, and proactive optimization. With this cloud-based, subscription-model solution, all you have to do is claim your servers, hyperconverged infrastructure, and fabric interconnects in the user interface; license the service; place your resources in logical groupings (such as remote- or branch-office locations or virtualization clusters); and use role- and policy-based interfaces to configure and manage your resources wherever they are located.

Built-in security

The Cisco Intersight platform uses a layered security architecture that builds on industry-standard security technologies. It also encrypts data, complies with strict Cisco security and data handling standards, and separates management and IT production network traffic for additional isolation. As a result, you can have confidence that your cloud-based systems management platform offers the strong security you require.

A changing management landscape

Conventional IT infrastructure uses point products with multiple element managers. With the Cisco Unified Computing System™ (Cisco UCS®), Cisco changed the game for both IT infrastructure and the way that systems are managed. Combining converged infrastructure and embedded model-based management, Cisco UCS simplifies and automates computing to make daily operations easier and more efficient. Now we have taken the next step to extend our vision of adaptive management in Cisco UCS and Cisco HyperFlex™ systems through the Cisco Intersight™ cloud-based management platform.

Introducing Cisco Intersight

Hosted by Cisco, Cisco Intersight provides the benefits of cloud-based management that customers have come to appreciate with similar solutions, such as the Cisco Meraki™ platform. Management and automation platforms are enhanced by analytics and machine learning techniques to increase efficiency and continuously evolve to manage the growing complexity of your IT infrastructure.

The software monitors the health and relationships of infrastructure components that use Cisco UCS management. Telemetry and configuration information is collected and stored in accordance with Cisco information security requirements. Your data is isolated and displayed to you through an intuitive user interface. Because the software scales easily and frequent updates are implemented without impact, this simplified and consistent infrastructure management approach removes the difficulties of supporting on-premise tools and appliances (Figure 1).

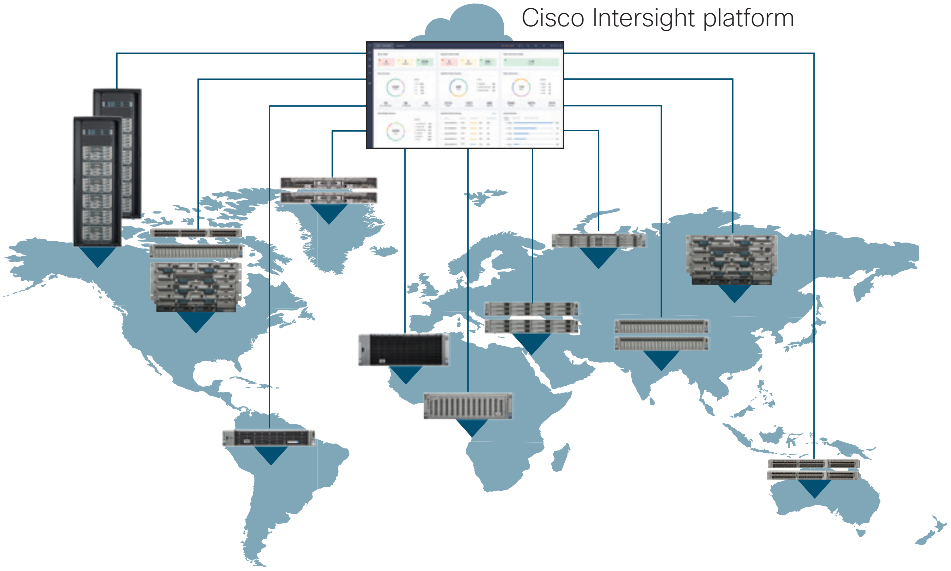


Figure 1 Cisco Intersight eliminates the difficulties of supporting on-premises tools and appliances wherever they are located

> **“Customers expect to be able to consistently monitor workloads, optimize performance, and orchestrate infrastructure operations using integrated, API-driven management solutions supported by customizable graphic user interfaces and big data-enabled IT operations analytics.”**

IDC: Worldwide Cloud Systems Management Software Forecast, 2017–2021, February 2017, #US41374417.

Designed to support continuous integration and continuous delivery (CI/CD) processes, Cisco Intersight offers adaptive systems management. The software gathers data from the entire installed base and learns from all customer environments. The data points are correlated to create models that recognize indications of problems. This data is combined with practical knowledge to help Cisco Intersight evolve and become smarter. As the Cisco Intersight knowledge base increases, trends are revealed, and insights and information are provided to you through a recommendation engine.

The knowledge base is tightly integrated with Cisco Technical Assistance Center (TAC) support and supplemented by the expertise of the Cisco UCS community. When used with the TAC’s vast knowledge base, Cisco Intersight helps prevent problems by delivering new levels of proactive systems support. The information is synthesized and provided to you in an easily consumable, actionable format through the Cisco Insight recommendation engine. By combining these insights and recommendations with automated actions, you can significantly increase efficiency, reduce costs, and accelerate time to resolution.

The importance of security

Your organization must respond to a rapidly changing cybersecurity landscape in which attacks are continually becoming more sophisticated and frequent. When we started designing the Cisco Intersight platform, we knew that security would be of paramount importance. Cisco Intersight builds in protection mechanisms so that you can feel confident that your cloud-based systems management platform offers the strong security you require.

Security in the Cisco Intersight platform

Both the Cisco UCS and Cisco Intersight platforms use Cisco’s built-in protection approach to provide device, system, infrastructure, and services security. Using a layered security architecture, Cisco Intersight builds on the same industry-standard security technologies that are used widely in Internet e-commerce. It also encrypts data, complies with strict Cisco security and data handling standards, and separates management and IT production network traffic for additional isolation.

Role-based access control

The Cisco Intersight framework uses a granular access control system with permissions managed per resource (user actions, views, and objects). Common roles are implemented, such as administrator, user, and user with read-only access. The system also provides users with a flexible system to create custom roles to manage resources and resource groups.

The Cisco Intersight rroadmap includes support for multifactor authentication (MFA) and integration with external identity management systems (IMSs) to meet existing customer authentication requirements.

Device connection

Cisco UCS and Cisco HyperFlex systems are connected to the Cisco Intersight portal through a device connector that is embedded in the management controller of each system (Figure 2). The device connector provides a secure way for connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure Internet connection.

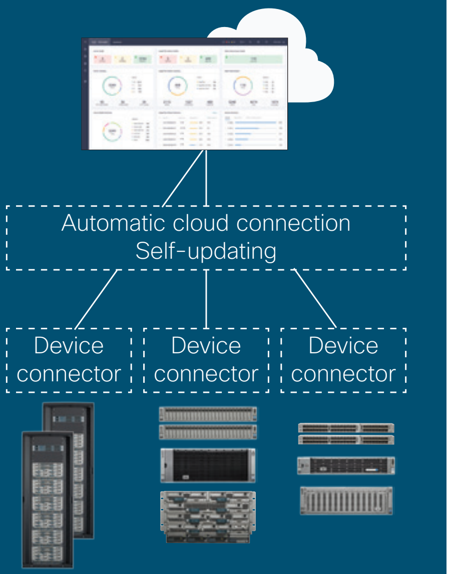


Figure 2 Device connection

Secure device claiming with two-factor authentication

The first step is to claim a device for use with the Cisco Intersight platform. Using a browser, go to the portal and click on the “Claim Devices” tab. Enter the device ID and claim code, both of which are unique to the device and retrieved from the device. You can find the device ID by opening the Admin tab. The claim code is refreshed every 10 minutes as an additional safeguard.

Two-factor authentication is used to verify the identity and authenticity of each device being claimed. This authentication mechanism adds another layer of security to the device-claiming process. It requires access to the device as well as device identification information that is validated against your Cisco Intersight account. In the event that an unauthorized user guesses or learns device information, the user cannot claim a device without physical access to the device.

Devices also can be unclaimed, or removed from your list, through the portal.

Data encryption and connection security

All data exchanged between Cisco UCS devices and the Cisco Intersight platform uses industry-standard encryption and security protocols (Figure 3). Connected devices communicate with Cisco Intersight exclusively using Transport Layer Security (TLS) with restricted ciphers and HTTPS on the standard HTTPS port 443. All data sent to Cisco Intersight is encrypted, and all connections are initiated outbound from the device. Firewalls can block all incoming connection requests; only HTTPS port 443 needs to be enabled for outbound connections. As a result, firewalls do not need any other special configuration to enable Cisco Intersight connectivity. Devices can be configured to use HTTPS proxy servers so that devices are not directly accessible from the Internet.

To help ensure connection security and prevent man-in-the-middle attacks, Cisco UCS and Cisco HyperFlex devices connect only to the Cisco Intersight portal: a single-destination HTTPS URL. The portal presents a certificate signed by a certificate authority (CA). If an unsigned certificate is presented, the devices will not connect to the portal. Cisco Intersight software and the device connector create a secure management framework that provides real-time information related to device security. This approach also allows connected devices and Cisco Intersight to stay synchronized with the latest connection security updates.

Portal infrastructure

The Cisco Intersight portal is a SaaS management solution delivered through the Cisco Intersight portal. Cisco personnel are available 24 hours a day, 7 days a week, for logistical security, operational, and change-management support. All services are replicated across multiple independent datacenters so that user services fail over rapidly in the event of a datacenter failure.

Data center reliability and availability

- Rapid escalation procedures across multiple operations teams
- Independent outage alert system
- Replication of all data (including metrics and device configurations) across data centers
- Real-time replication of data between data centers
- Rapid failover of Cisco Intersight services in the event of a hardware failure or other data center outage
- Preservation of end-user network functions, even if portal connectivity is interrupted, through an out-of-band architecture
- Regular testing of failover procedures

Secure, out-of-band architecture

- No disruption of your IT production or management network if the connection is interrupted
- Storage of only management network data
- Encryption of sensitive data when it is stored
- Regular penetration testing of data centers

Datacenter certification and compliance

Contact the Cisco Intersight Security and Data Privacy team for specific questions about data center certifications and compliance reports.

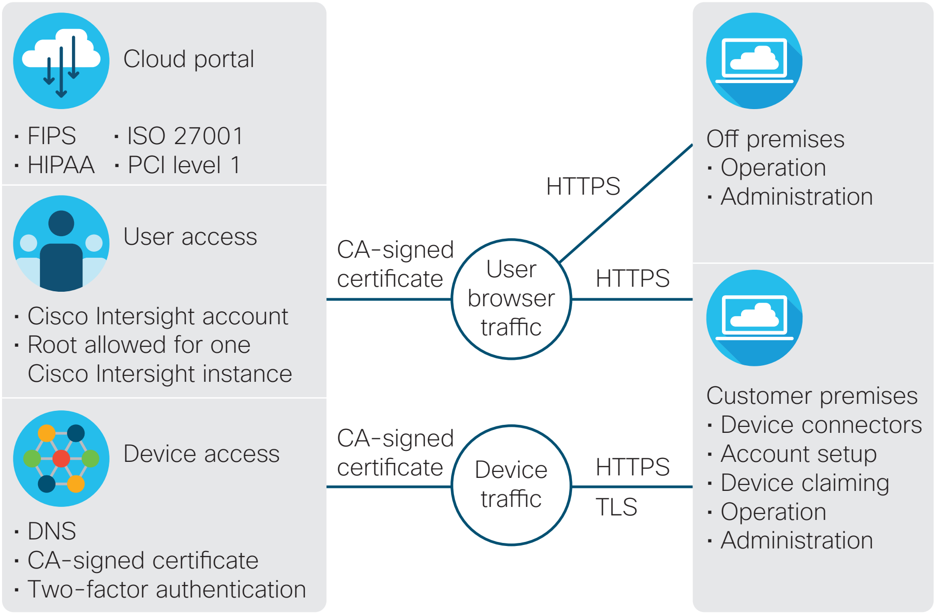


Figure 3 The Cisco Intersight platform separates user and device traffic and communicates using industry-standard protocols

Compliance with industry-security standards

The Cisco Intersight platform meets or exceeds information security requirements by using several industry-standard security protocols:

- The Payment Card Industry Data Security Standard (PCI DSS) protects the security of payment and credit card information. Cisco Intersight management is out of band: customer traffic (including cardholder data) does not flow through the Cisco Intersight platform. Even though Cisco Intersight data centers are considered out of scope for PCI audits, Cisco has taken the additional step of obtaining PCI certification for these data centers.
- The Health Insurance Portability and Accountability Act (HIPAA) safeguards medical information. No individually identifiable health information (IIHI) on the network is ever sent to the Cisco Intersight portal. Even though Cisco Intersight data centers are considered out of scope for HIPAA audits, Cisco has obtained HIPAA certification for these data centers.
- ISO 27001, an information-security standard published by the International Organization for Standardization (ISO), provides best-practice recommendations for creating an information-security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, administrative, physical, and technical controls involved in an organization’s information risk-management processes.
- Federal Information Processing Standard (FIPS) 140-2 validates cryptographic functions used in hardware, software, and firmware solutions.

> **“We strive to be trustworthy, transparent, and accountable. That means leaving no stone unturned in our search for threats to our infrastructure or data.”**
>
> **Michele Guel, distinguished engineer and chief security architect, Cisco**

Encryption of all data

All data is transported from a device to the Cisco Intersight platform using 128-bit Secure Sockets Layer (SSL) security. All data moving between devices and the portal is encrypted using the Advanced Encryption Standard (AES) with a 256-bit, randomly generated key and distributed with a public-key mechanism. In addition, every device connection to the portal is authenticated with a cryptographic token so that only legitimate devices can be managed.

Compliance with Cisco security and data handling standards

Protecting infrastructure and data requires a close partnership between the Cisco IT and Information Security (InfoSec) organizations. Part of Cisco’s Security and Trust Organization (STO), InfoSec works with Cisco IT to help ensure that the products we build and the infrastructure we operate are secure. These groups work together to support business productivity while protecting our systems and data from internal and external threats. Instead of focusing on security hardware and software alone, we take a holistic, pervasive approach to security by:

- Fostering a security-conscious culture to reduce the attack surface and provide a robust security posture
- Implementing security-focused policies and processes
- Embedding security throughout our infrastructure

In conjunction with our emphasis on people and processes, we enforce security-focused policies:

- Access management: We enforce requirements for managing user and administrative access to information assets and information systems through proper controls for authentication, authorization, and auditing.
- Auditing and risk assessments: We enforce compliance with security and data integrity policies and investigate incidents and monitor user and system activity as appropriate.
- Cloud security: We set minimum security requirements for the clouds we use and the clouds we build for hosted services.
- Cryptographic controls: We explain how to use cryptographic controls to protect the confidentiality, integrity, and availability of information assets.

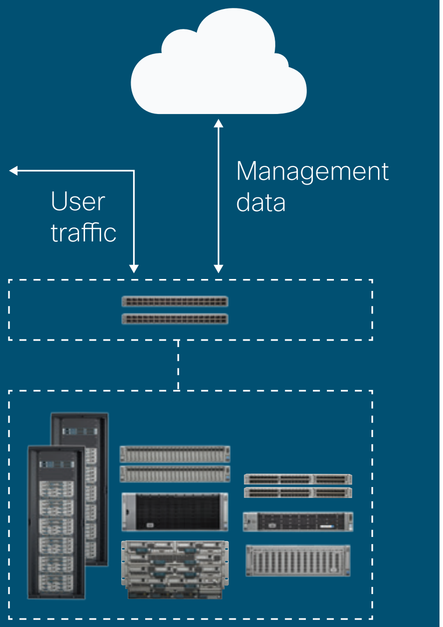


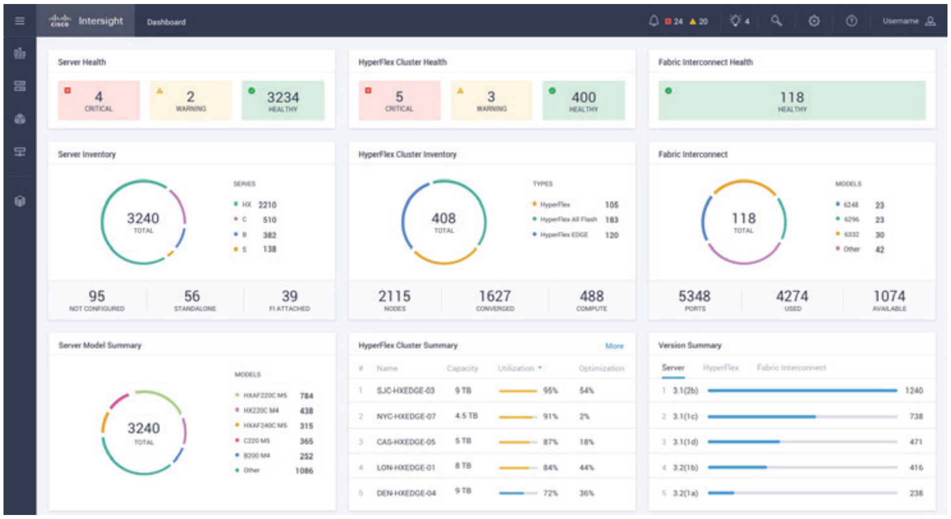
Figure 4 Traffic separation

- **Data protection:** We specify requirements for classifying, labeling, and protecting data. These policies define the relative sensitivity of information and determine how this information is treated and disclosed to Cisco employees and other parties.
- **Information security:** We enforce policies specifying the confidentiality, integrity, and availability of information assets.
- **Network access:** We identify authorized users and devices that can access our networks.

Separation of the management network

The out-of-band control plane in the Cisco Intersight platform separates management data from IT production and application data (Figure 4). Management data, such as configuration and monitoring information and statistics, flows from the devices to the Cisco Intersight portal (Figure 5). IT production and application data is sent directly to its destination on your production data network.

The use of an out-of-band architecture means that your users are not affected if devices are unable to communicate with Cisco Intersight due to Internet or other service disruptions. Users can still access local management and production networks, and all Cisco UCS and Cisco HyperFlex policies and settings continue to be enforced. In addition, local user authentication is unaffected, and local configuration tools such as Cisco UCS Manager remain available.



Server Health
4 CRITICAL
2 WARNING
3234 HEALTHY

HyperFlex Cluster Health
5 CRITICAL
3 WARNING
400 HEALTHY

Fabric Interconnect Health
118 HEALTHY

Server Inventory
3240 TOTAL

SERIES	
HX	2210
C	510
B	382
S	138

95 NOT CONFIGURED
56 STANDALONE
39 FI ATTACHED

HyperFlex Cluster Inventory
408 TOTAL

TYPES	
HyperFlex	105
HyperFlex All Flash	183
HyperFlex EDGE	120

2115 NODES
1627 CONVERGED
488 COMPUTE

Fabric Interconnect
118 TOTAL

MODELS	
6248	23
6296	23
6332	30
Other	42

5348 PORTS
4274 USED
1074 AVAILABLE

Server Model Summary
3240 TOTAL

MODELS	
HXAF220C M5	784
HX220C M4	438
HXAF240C M5	315
C220 M5	365
B200 M4	252
Other	1086

HyperFlex Cluster Summary
More

#	Name	Capacity	Utilization	Optimization
1	SJC-HXEDGE-03	9 TB	95%	54%
2	NYC-HXEDGE-07	4.5 TB	91%	2%
3	CAS-HXEDGE-05	5 TB	87%	18%
4	LON-HXEDGE-01	8 TB	84%	44%
5	DEN-HXEDGE-04	9 TB	72%	36%

Version Summary
Server HyperFlex Fabric Interconnect

1	3.1(2b)	1240
2	3.1(1c)	738
3	3.1(1d)	471
4	3.2(1b)	416
5	3.2(1a)	238

Figure 5 Cisco Intersight dashboard

For more information

To learn more about the Cisco Intersight platform, visit http://www.cisco.com/go/intersight.

To learn more about Cisco's approach to operational security, visit http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/cs-sec-03232016-operational-security.html.

To learn more about Cisco UCS, visit http://www.cisco.com/go/ucs.

To learn more about Cisco HyperFlex systems, visit http://www.cisco.com/go/hyperflex.

Delivering security advantages

The SaaS management approach of the Cisco Intersight platform offers many security advantages compared to local and agent-based monitoring and management tools:

- Simplicity: The Cisco Intersight portal offloads the responsibility of platform management, allowing IT staff to focus on other tasks and priorities.
- Device connectivity: Devices that are managed by Cisco Intersight automatically connect and report their configuration and operation status, including their active firmware and software versions.
- Autonomy: User interaction is not required on the device after initial connection. There is no agent or other software to install or maintain.
- Synchronization: With self-updating device connectors, each device automatically synchronizes with Cisco Intersight. Patches and security updates can be pushed to the device connector as needed with no user action required.
- Analysis: Based on data that is automatically collected, Cisco Intersight provides recommendations for infrastructure updates that are needed to keep your hardware, firmware, and software compliant with Cisco's latest tested combinations.
- Simplicity: Cisco Intersight provides a single location for tracking and reporting endpoint security and compliance.