Connected TAC: Customer Data Security

Overview

Connected TAC allows customers to use digitized intellectual capital and expertise from Cisco to proactively identify device issues before they become problems that could significantly affect network performance, availability, and security. Customers benefit from faster, automated, proactive problem identification and recommended remediation resulting in improved business continuity and risk management.

This document provides information about the security implemented for the Connected TAC capabilities, including collection of data from Cisco® devices, encryption of the data, communication with the Cisco diagnostic engine, and data retention.

Cisco realizes that data security is a high-priority concerns for its customers and is providing this information to help customers understand Cisco's approach.

TAC Data Security

- Cisco TAC collects and analyzes device data in response to more than 1.8 million service requests a year.
- TAC has developed comprehensive and secure data storage tools and protocols to safeguard customer device data.
- These same practices and protocols are used for Connected TAC.

Cisco Connected TAC service overview

Connected TAC is a new proactive issue detection and remediation service that uses bidirectional, secure connectivity between Cisco and customer devices in order to provide customers with access to Cisco TAC's digitized intellectual capital, which can be used to identify potential issues before they grow into business-affecting problems.

Connected TAC uses the internally developed Diagnostic Bridge to provide connectivity between a customer's devices and Cisco, which enables Cisco to provide automated analysis of potential issues. These issues are shared with customers either using the MyDiagnostics UI or by direct infusion of the identified issues into a customer's incident management system. In addition, Connected TAC provides premium TAC Advisor services, which allow customers to obtain access to specially trained TAC engineers who can provide more in-depth and customized device analysis.

Connected TAC allows customers to effortlessly share device data with Cisco. The data collected is limited to what is needed to perform device diagnostics and does not include any personally identifiable information

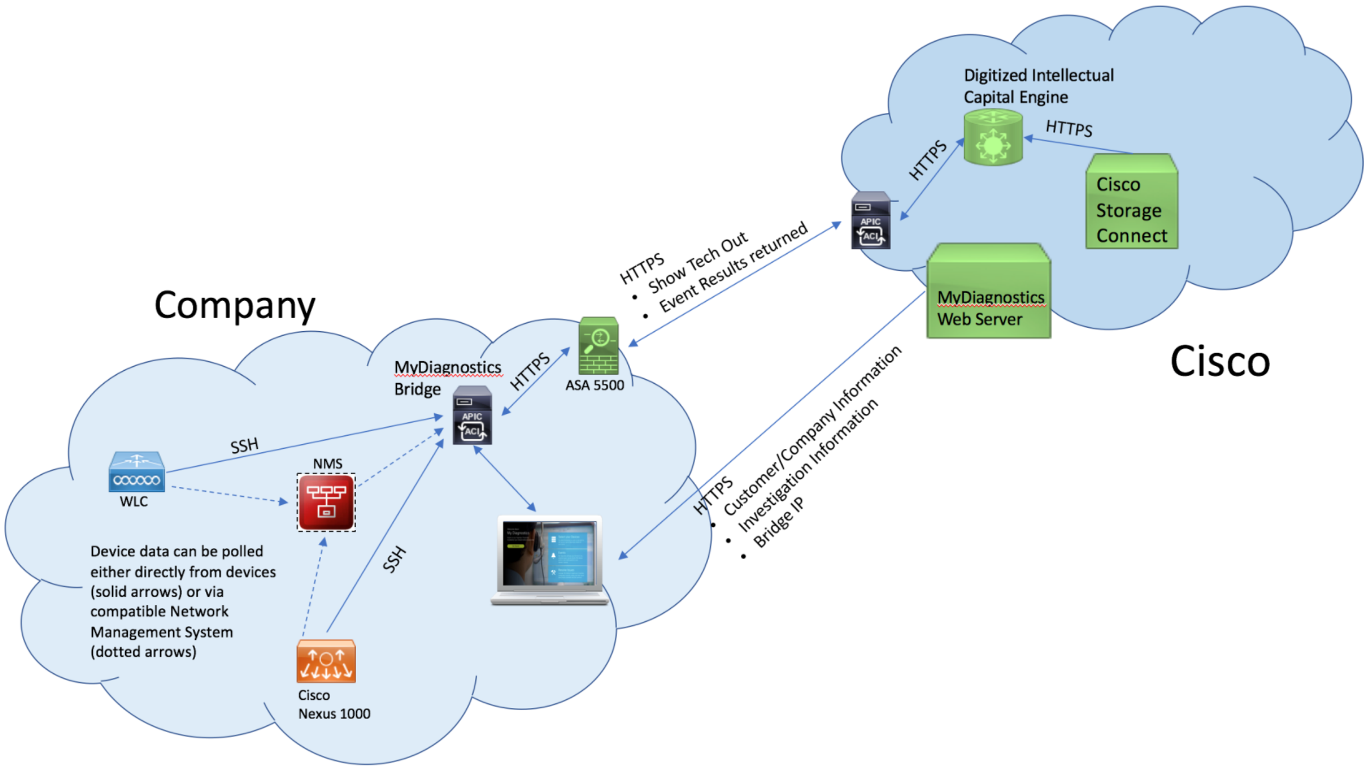
Connected TAC capabilities are organized into a tiered proactive services package that allows customers to choose how they consume our digital and human intellectual capital, while also allowing Cisco to target our proactive service offers to the appropriate market segments.

This document provides an overview of the security practices Cisco has implemented as part of Connected TAC with a focus on the security architecture as well as the encryption, communications, and storage practices for device data.

Connected TAC security architecture

Connected TAC provides an end-to-end security architecture for your device data. The security functionality addresses collection, transmission, processing, storage, and viewing. (See Figure 1.)

Figure 1. Connected TAC Security Architecture Overview



Device data can be polled either directly from devices (solid arrows) or via compatible Network Management System (dotted arrows)

The remainder of this document summarizes Cisco's approach to security as it relates to encryption, communications, and storage.

Encryption

Encryption is a primary aspect of maintaining data security. The following is a summary of the Connected TAC approach to data encryption.

In general, the data encryption has the following characteristics:

- A 128-bit AES key is generated dynamically for every data upload to encrypt the data transferred.
- The AES key itself is also encrypted with the public key generated by Cisco.

In addition, the specific encryption practices related to the Connected TAC components are listed in Table 1.

Table 1. Connected TAC encryption summary

Diagnostic Bridge	• Device IP/host name, user ID, and password are stored local to customer's corporate network ○ A database (MySQL) is provided using OVA ○ Network administrator can utilize their own database in place of the one provided • Device information (show tech and so on) is collected using SSH or integrated EMS/NMS and communicated to the Cisco digitized intellectual capital engine using HTTPS. • For the enhanced offer, Cisco diagnostic system creates a container where the device data is loaded and analyzed and deletes container and device information after the analysis is complete. • For the premium offer, Cisco diagnostic systems use the same infrastructure used to store and process device analysis that is used for processing service requests. • Cisco secures your data by providing a unique storage location per bridge, which is isolated from all other uploads. This walled isolation area is wiped clean after the IC engine runs its analysis. In addition, the data can enter, but not leave, this upload area.
MyDiagnostics Web UI	• Web server maintains information regarding webpage usage. • Web server maintains information that maps a user's Cisco.com ID to customer record and bridge IP. • Information stored in the Cisco cloud is associated to a customer record and can only be retrieved with the proper customer record ID. During login a unique token is generated and stored on the web server and associated with the user's customer details. Access back to the web server requires the provided token and customer identifying details are retrieved from the server and used to query the database. • UI loaded into browser talks to Diagnostic Bridge directly while on customer network. **Note:** If you load the UI and your laptop cannot reach the bridge using network routing, no data is returned.
Database	• The database administration and security are delegated to the customer. • Device IP/host name, user ID, and password are not currently stored in the database in an encrypted form. Efforts are under way to allow the customer to configure a password to be used for encryption. The security document will be updated when that enhancement is in place.

Communication

The MyDiagnostics solution uses four components to develop and provide diagnostic results:

- **Diagnostic Bridge**: This bridge is a coordinator that can utilize existing EMS/NMS systems or direct SSH to monitor devices.
- **MyDiagnostics user interface:** The UI is a web application loaded using the customer's browser and communicates with Cisco web servers and the customer-installed Diagnostic Bridge.
- **Cisco Storage System:** This system is used to store attachments to service request and is used to store device data when using the TAC Advisor service.
- **Cisco IC system:** An IC execution engine and library of digitized IC that is used to parse, analyze, and identify issues in device data.

Connecting Diagnostic Bridge to Cisco devices on customer network

The Diagnostic Bridge is installed on a customer's network on a Windows VM using MSI or a virtual machine using OVA.
Diagnostic Bridge communicates with devices in several ways based on how customers decide to integrate the bridge with their EMS/NMS systems:

- Option 1: Connection using Cisco Common Services Platform Collector (CSPC)
  - Diagnostic Bridge can learn of devices and utilize CSPC to communicate with devices to retrieve configuration information.
  - Communication with CSPC uses HTTPS.
  - Diagnostic Bridge does not maintain user IDs or passwords or enable passwords when connected using CSPC.
- Option 2: Connection using WhatsUpGold (WUG)
  - Diagnostic Bridge must be installed on the same Windows VM as WUG.
  - Diagnostic Bridge learns of credentials to use to communicate with devices from the WUG software using DLL, direct connection to WUG database.
- Option 3: Connection using NetBrain and third-party API users
  - Diagnostic Bridge uses NetBrain and third-party vendors to retrieve device configuration information.
  - Diagnostic Bridge communicates with these providers using HTTPS.
- Option 4: Connection using direct SSH
  - Diagnostic Bridge can communicate with devices directly using SSH to retrieve appropriate information.

Credential handling

Credential handling varies depending on the connection option selected by the customer. In some cases, credentials will be stored on the Diagnostic Bridge, and in others, they will not. As a general practice, Cisco will only store device credentials when it is necessary for the proper functioning of the bridge:

- The bridge will store manually configured device credentials to be used for scans.
- Certain NMS options (for example, CSPC, NetBrain) transport results to the bridge without the need to share device credentials.
- It is also possible to trigger a scan using API and provide temporary credentials, which will be used by the bridge to access the devices. In that case, there are no credentials stored by the bridge.

Connecting Diagnostic Bridge to Cisco IC system

After the Diagnostic Bridge has collected device information, it communicates the collected information to the Cisco IC system using HTTPS. Information uploaded by the Diagnostic Bridge is stored temporarily in the Cisco IC system in an area isolated from every other user or Diagnostic Bridge. The Cisco IC system prevents any other user or Diagnostic Bridge from reaching into another area, which provides a high level of security. Additionally, the Cisco IC system deletes any uploaded data after it is processed. Cisco routinely analyzes and tests the IC system for security vulnerabilities to help protect each customer’s data.

Connecting MyDiagnostics UI to bridge

The MyDiagnostics UI is a website maintained by Cisco to provide a continual improving interface to the customer. This interface provides Diagnostic Bridge configuration screens, update screens, and device and event management. The MyDiagnostics UI relies on Cisco SSO for user login; no user passwords are maintained in the MyDiagnostics UI server. The communication to Cisco web server uses HTTPS. The MyDiagnostics UI also communicates directly with the Diagnostic Bridge on your network using HTTPS. **Note:** You must be able to route traffic to your bridge, or the MyDiagnostics UI will not be able to show you any information. This protects your information by storing it locally to your network.

Additional Communication

1. Diagnostic Bridge API

- Role-based authentication based on local API users. This access method is used by the local UI and by custom on-premises integrations.
- Authentication by CWay-generated token. This access method is used by the MyDiagnostics UI.

  Note: The Cisco back end uses a private key for the Diagnostic Bridge API.

2. Work Items

   The Diagnostic Bridge periodically polls the back end to pick up work that is queued for that particular Bridge instance.

   - Data Collection Request: Allows the back end to trigger a data collection. (The Diagnostic Bridge executes a command and attaches the command output to a case.) There is an approval method for this. The default white list contains only "show..." commands and some helper commands such as "term len 0".
   - Invoke API Request: Allows the back end to trigger (almost arbitrary) calls on the Bridge API. The calls must be authenticated with a CWay-generated token (see above). There is a separate white list for this mechanism, which is empty by default.

Storage

Storage is crucial to the MyDiagnostics solution. Currently there are three storage systems involved to provide you with your experience: bridge DB, MyDiagnostics UI, and Cisco storage system.

Table 2 outlines the Cisco approach to storage security.

Table 2. Connected TAC storage approach summary

Diagnostic Bridge DB	• The OVA provides a prebuilt and installed MySQL database for the bridge to use. Access to the VM is controlled by the network administrator. • The Diagnostic Bridge can also utilize a SQL database provided by the customer. It is the responsibility of the DB administrator to secure access.
MyDiagnostics UI	• The MyDiagnostics UI server stores Cisco.com ID customer information: ○ Bridge IP/host name/port ○ List of Cisco.com IDs that are able to access the account ○ Open/closed investigations and events communicated • The server provides a set of APIs that are security tested and scanned by Cisco API security experts to protect the data. • The database used is encrypted at rest. • All communication between the customer's laptop and the MyDiagnostics UI server uses HTTPS. • All communication between the customer's laptop and the Diagnostic Bridge uses HTTPS.
Cisco storage system	• Cisco provides a storage system used by the Cisco case management system. • All files that are uploaded by customers to the Cisco case management system are encrypted and stored and tied to a specific case. • A user must be authorized to access a case to access stored files. • MyDiagnostics UI utilizes this same system for investigation, diagnostic, and analysis requests.

Summary: Cisco storage of Connected TAC device data

During automated diagnostic scans, device data is housed in a newly created docker (mini-VM) for each scan. After the scan is complete and the diagnostic results are returned to the customer, Cisco deletes the docker and the collected device command output. For customers who use the TAC Advisor capabilities, device data is collected and stored using the same tools and processes Cisco has in place today for the millions of standard TAC service requests that have been processed.

Conclusion

Connected TAC capabilities provide a secure end-to-end architecture for the collection, processing, and transmission of your device data to Cisco's diagnostic resources, which enable data analysis and development of actionable insight into customer device performance.

We take the security of your data very seriously. If you need further details about Connected TAC and how we implement our security architecture, contact your Cisco sales representative or send an email to connectedtac_mt@cisco.com. They will be happy to set up a technical meeting to discuss your questions and provide details about your specific situation.

Additional resources

For more detailed information about how we guard the privacy of customer data, refer to the following. Additional security details are available under nondisclosure agreement.

Cisco Security Vulnerability Policy

Cisco Privacy Portal

Connect TAC Product Support Page (Diagnostic Bridge installation and user guide and related resources)

Cisco Network Data Collection Tools Supplement