Cisco Diagnostic Bridge Release Notes: Version 1.9.3

This document describes changes in major release version 1.9.0 of the Cisco Diagnostic Bridge, as well as changes in minor version releases that have followed.

Changes (1.9.3)

- Changes to infrastructure that require users to upgrade to the latest version of the Cisco Diagnostic Bridge.

Changes (1.9.2)

- An issue was fixed in which the CX collector plugin did not update the scan status message.
- Password requirements have been updated. Passwords must contain at least 8 characters with no white space, and trivial or insecure common passwords are not accepted.

  IMPORTANT: Make sure that all existing passwords comply with the new password policy before you upgrade from version 1.8.0 or older. Otherwise, the upgrade will fail.

Changes (1.9.1)

- There is a new mechanism to facilitate initial configuration of the Diagnostic Bridge.
- A new method is used to create the URL for the CX collector plugin.
- Users can now configure the timeout value for the CSPC source plugin.

Major Changes (1.9.0)

- Compliant with Cisco Secure Development Lifecycle (CSDL); see Security Related Changes below.
- Removal of OVA deployment option.
- New Docker deployment.
- API user settings and outbound connection settings are no longer stored in config files. Automatic migration into database.
- For ServiceNow integration, there is a new certified ServiceNow app for Cisco Diagnostic available, see: https://store.servicenow.com/sn_appstore_store.do#!/store/application/e9c00875db1047406845f9551d96191e

- The WhatsUp Gold Credentials Provider Plugin has been removed from this version. Renewed support for this feature is planned for the future. As a temporary workaround, you can provide fallback credentials on the device group level.
- Support for UCS devices.
- Support for Postgres databases.
- New history-less mode.
- Integration with Insight Engine and Customer Portal.
- New command line setup wizard for all platforms.
- Encryption of sensitive data in config files and in the database.

New Features (1.9.0)

- Opt-in to cloud-storage of scan results.
- Add timing information to SessionLogs and ConnectionLogs.
- Device-Group support for CSPC source plugin.
- Allow static settings to be passed in via environmental variables.
- Improve logging for early startup process.
- Make token lifetime configurable.
- Option to use IP-Address instead of Hostname in DNAC plugins.
- Verify signature of MSI during automatic upgrade process.
- Verify signature of bin archive during upgrade process.
- Make timeout for command collection via CSPC configurable.
- Add timing details to session log for DNAC collector.
- Log level for console output configurable in dynamic settings.
- Source and collector plugin for CX device management interface.
- Create new notification plugin to send scan status to IronBank.
- Include used credentialsProviderType in bridge statistics.
- Introduce delay for request-level retry.
- Print InstanceId and binary path when bridge starts up.

Security Related Changes (1.9.0)

- No longer ship with a self-signed certificate. Instead, provide users the option to create a new one during setup.
- Make supported TLS versions configurable.
- Product does no longer contain any default passwords.
- Hash non-recoverable stored credentials.
- Local UI and Swagger UI can now be disabled.
- More restrictive headers in API responses.
- Configurable limit for failed logins.
- Checking certificate revocation lists for outgoing connections by default.
- Configurable minimum password length enforcement.
- Use good names in certificates (includes using FQDNs).
- Improve logging for security related events.
- Configurable HTTPS redirection and HTTP Strict Transport Security.
- Password generator in MSI installer, setup wizard, and Local UI.

API Changes (1.9.0)

- The /api/Cookie/CookieLogin no longer supports the isPersistent option.
- Improve logging in the case of 500 responses sent to clients.
- New GET /api/Settings/ConnectionInfo endpoint.
- New GET /api/Settings/ApiUsers/PasswordSuggestion endpoint.
- Support hostnames for POST/DELETE /api/Queue/Devices.
- Remove critical device feature.
- Breaking Change: GET/PUT/DELETE /api/Settings/ApiUsers endpoint no longer accept username or userid as part of the URL.
- Queue APIs should return scanId immediately when waitForResult=false.
- Provide a new API for querying the currently active scan requests.
- New externalTransactionId option when enqueueing devices.
- New includeLastResult option for GET /api/Devices and GET /api/DeviceGroups/<id>/Devices endpoints.

Bug Fixes (1.9.0)

- Bug in attempts to delete old results.
- Two unit tests related to streaming currently fail.
- Check status code in CSPC responses.
- Automatic upgrade fails due to missing files.
- Admin is able to delete the super user.
- Attempt to delete devices failed.
- DNAC source plugin returns only first 500 devices.
- Problem with attempt to sync two DNAC device groups.
- Corrupted binaries in MSI installer on Japanese edition of Windows.
- Scans using DNAC collector plugin fail with "Multiple tokens provided".
- New Features (Local UI).
- Fix column names in devices view.
- Allow users to see full exception details.
- Make outbound connection settings configurable from local UI.
- Ability to suppress queue polling.
- Local UI support for API user management.
- Local UI shows commands executed during a scan.
- New search and sort features for devices.
- Summary page for the scan status.
- Bug Fixes (Local UI).
- Hide passwords in text boxes.
- Fix typo.
- LocalUI shows delete button for non-manual device groups.
- Device Group is created with an empty group name.
- Edit device group does not allow you to change Refresh Schedule Profile.
- The login screen does not load properly if the last session timed out.
- In device group settings, profiles cannot be unselected.
- There is a sorting error on the Show All Devices page.
- Management Port does not update.

- The DataCollectionRequests panel on the home page shows wrong data.

Known Issues (1.9.0)

- Passwords can be logged if connection logs or session logs are enabled. These features should be disabled for normal operation.
- The WhatsUp Gold Credentials Provider Plugin has been removed from this version. Renewed support for this feature is planned for the future. As a temporary workaround, you can provide fallback credentials on the device group level.
- Breaking API changes (see above) which could potentially break existing integrations.
- Windows service does not start after automatic upgrade (Port already in use). A manual (re)start of the service is required.
- The ServiceNow apps now use the "caci" application scope instead of "cisit". This might break existing integrations. It is recommended that you upgrade your ServiceNow app to the new certified version from the ServiceNow app store: https://store.servicenow.com/sn_appstore_store.do#!/store/application/e9c00875db1047406845f9551d96191e