

Upgrade the Cisco Diagnostic Bridge to Version 1.9

Version 1.9 of the Cisco Diagnostic Bridge contains many changes, some of which are related to security. This document provides important information about the upgrade process.

Passwords

Version 1.9 of the Cisco Diagnostic Bridge implements a stricter password policy.

Before you upgrade to version 1.9, make sure that all existing passwords comply with these new requirements:

- Length must be at least 8 characters
- No white space
- Trivial passwords like “12345678” are blacklisted

If the file `/etc/api-users.json` contains passwords that do not comply with the new policy, the version 1.9 upgrade process will not start.

Additionally, previous versions of the Diagnostic Bridge stored user passwords as clear-text in `/etc/api-users.json`. In version 1.9 and future versions, those credentials will be imported to the database, and the file `/etc/api-users.json` will be deleted. During the import process, passwords are hashed, so ***it will no longer be possible to obtain the clear-text passwords.***

Existing OVA Deployments

Cisco no longer ships OVA images for the Diagnostic Bridge. You can continue to use your existing Cisco-provided OVA, but it is your responsibility to keep the OVA up-to-date and secure with applicable security fixes for your operating system.