

# Cisco Prime Infrastructure 3.10.2 Release Notes

---

**First Published:** 2022-10-11

## Introduction

This is the second maintenance release of Cisco Prime Infrastructure 3.10.

You can upgrade to Cisco Prime Infrastructure 3.10.2 from Cisco Prime Infrastructure 3.10 or Cisco Prime Infrastructure 3.10 Update 01 or Cisco Prime Infrastructure 3.10.1. Cisco Prime Infrastructure PI-Upgrade-3.10.x\_to\_3.10.2-0.0.90.tar.gz is approximately 2.2GB. The downloading time depends on the available network connection in the enterprise environment. Ensure that you have adequate bandwidth and are not running into high latency issues.

## System Requirements

For more details on the system requirements, see [Understand System Requirements](#) section in the *Cisco Prime Infrastructure 3.10 Quick Start Guide*.

## How to Upgrade From Previous Releases of Prime Infrastructure

While upgrading from Cisco Prime Infrastructure 3.10 or 3.10 Update 01 or 3.10.1 to Cisco Prime Infrastructure 3.10.2, you must install the Cisco Prime Infrastructure 3.10.2 Mandatory System Patch (PI\_3\_10\_2\_SystemPatch-1.0.5.ubf) after Upgrade. This includes Oracle July 2022 critical patch update. To install the system patch, see [Installing the System Patch from Local Storage, on page 3](#).

Before you upgrade from Operations Center Prime Infrastructure 3.10 or 3.10 Update 01 or 3.10.1 to Operations Center Prime Infrastructure 3.10.2, make sure you upgrade any Prime Infrastructure instances that are managed in Operations Center from Prime Infrastructure 3.10 or 3.10 Update 01 or 3.10.1 to Prime Infrastructure 3.10.2.

You can upgrade Prime Infrastructure using either of the following methods:

- Perform an inline upgrade of existing 3.10 or 3.10 Update 01 or 3.10.1 system—See [How to Perform an Inline Upgrade](#).
- Restore data from backup on running system—See *Before You Migrate Your Data* in the *Cisco Prime Infrastructure Quick Start Guide*.

## How to Perform an Inline Upgrade

Use the following procedure to upgrade from primary Prime Infrastructure 3.10 or 3.10 Update 01 or 3.10.1 to Prime Infrastructure 3.10.2.

### Before you begin

Inline upgrade is simpler than system migration, and requires no new hardware. Cisco Prime Infrastructure 3.10.2 supports only inline upgrade from Cisco Prime Infrastructure 3.10 or 3.10 Update 01 or 3.10.1 to 3.10.2 in primary and secondary.

To pair HA deployments in Prime Infrastructure version 3.10.2, you must upgrade from 3.10 or 3.10 Update 01 or 3.10.1 Primary and Secondary to 3.10.2 using the upgrade bundle file. Then Install PI\_3\_10\_2\_SystemPatch-1.0.5.ubf in both primary and secondary 3.10.2 Servers and Pair the servers for high availability. For details, see [Before You Begin Setting Up High Availability](#) in the Cisco Prime Infrastructure 3.10 Administrator Guide.

## Procedure

- 
- Step 1** Set up a remote backup repository for the Prime Infrastructure version you are currently running. For details, see the section *Use a Remote Backup Repository* in the latest [Cisco Prime Infrastructure Administrator Guide](#).
- Step 2** Take an application backup of the Prime Infrastructure version you are currently running, and store the backup in the remote repository. For details, see the section *Perform an Immediate Application Backup Using the CLI* in the latest [Cisco Prime Infrastructure Administrator Guide](#).
- Step 3** Verify the integrity of the backup as explained in *Before You Migrate Your Data* in the [Cisco Prime Infrastructure Quick Start Guide](#).
- Step 4** Remove any existing High Availability configuration from your primary Prime Infrastructure server. You can do this using either of the following options:
- Launch Prime Infrastructure, choose **Administration > Settings > High Availability > HA Configuration**, and click **Remove**. Ensure the configuration mode changes to “HA Not Configured.”
  - Ensure the primary server is the active Prime Infrastructure server, go to the admin console on the primary server and run the `ncs ha remove` command.
- Step 5** Move backup files (all files with the tar.gz extension) from the /localdisk directory to another server and ensure that /localdisk has 80% free space. For details, see the sections *copy and delete commands* and *show disks command* in the latest [Command Reference Guide for Cisco Prime Infrastructure](#).
- Please ensure that /tmp folder has 80% free space for the upgrade to complete successfully.
- Step 6** Download the upgrade bundle PI-Upgrade-3.10.x\_to\_3.10.2-0.0.90.tar.gz from Cisco.com and verify the integrity using its checksum listed on Cisco.com.
- Step 7** Copy the verified upgrade file to the default repository:
- Example:**
- ```
admin# copy source
      disk
      :/defaultRepo
```
- Where:
- *source* is the upgrade file’s URL, path and filename (for example: FTP://<YourFTPServer>/PI-Upgrade-3.10.x\_to\_3.10.2-0.0.90.tar.gz)
  - *disk* is the disk and path to the local defaultRepo.
- Step 8** Ensure the current version of Prime Infrastructure is 3.10 or 3.10 Update 01 or 3.10.1.
- Step 9** Ensure the local repository (defaultRepo) contains no backup files.
- Step 10** Stop the Prime Infrastructure server by entering the command `ncs stop`
- Step 11** It is recommended to run the application upgrade from the console. For a virtual appliance, you can run the application upgrade from the VM console. For a physical appliance, you can run the application upgrade from

the KVM, VGA, or serial console. (If you are using the serial console, make sure baud rate is configured to 9600)

**Example:**

```
admin# application upgrade PI-Upgrade-3.10.x_to_3.10.2-0.0.90.tar.gz defaultRepo
```

This step can take several hours to complete, depending on the size of the application database.

**Step 12**

When the upgrade is complete:

- Verify that the application is running by entering the **ncs status** command in the admin console.
- Instruct users to clear the browser cache on all client machines that accessed an older version of Prime Infrastructure before they try to connect to the upgraded Prime Infrastructure server.
- If you were using external AAA (RADIUS or TACACS) before the upgrade, see the section *Renew AAA Settings After Installing a New Prime Infrastructure Version* in the latest [Cisco Prime Infrastructure Administrator Guide](#).
- Synchronize your devices as explained in the section *Synchronize Devices* in the latest [Cisco Prime Infrastructure User Guide](#).

**Note** When you upgrade from Prime Infrastructure version 3.10 or 3.10 Update 01 or 3.10.1 to 3.10.2 that uses two NICs, network outage occurs post the upgrade. This can be avoided by performing the following steps:

You must not add 2 NICs before the first power up of deployment. Also, adding 2 NICs at the same time is not recommended.

- Login to VMware vSphere.
- Choose the Virtual Machine where the Dual NIC has to be configured.
- Power off the Virtual Machine.
- Choose edit settings and then add the second NIC.
- Turn on the Virtual Machine.

**Note** When customer runs Virtual Machine with two network interfaces, after installation of the patch/upgrade, the Prime instance will reboot automatically.

We recommend you to check the network whether the MAC address and network interface match with each other and manually change if there is a mismatch.

## Installing the System Patch from Local Storage

- You can only install Cisco Prime Infrastructure PI\_3\_10\_2\_SystemPatch-1.0.5.ubf by manual download from Cisco.com and upload and install through Cisco Prime Infrastructure UI.
- Cisco Prime Infrastructure PI\_3\_10\_2\_SystemPatch-1.0.5.ubf can be applied only in primary and secondary standalone servers. The server will restart automatically once the installation is complete. The restart typically takes 45 to 60 minutes.

To install Cisco Prime Infrastructure PI\_3\_10\_2\_SystemPatch-1.0.5.ubf from the local storage, follow these steps:

### Procedure

- 
- Step 1** Download the Prime Infrastructure PI\_3\_10\_2\_SystemPatch-1.0.5.ubf from [Home > Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions > Prime Infrastructure > Prime Infrastructure 3.10 > Prime Infrastructure Patches - 3.10.2](#) and save the file in your local system.
- Step 2** Log in to Prime Infrastructure **3.10.2** server.
- Step 3** Choose **Administration > Licenses and Software Updates > Software Update**.
- Step 4** Click **Upload** and browse to the location where you have saved the system patch file. Click **OK** to upload the file.
- Step 5** In the **Status of Updates** pane, click the **Files** tab and check whether PI\_3\_10\_2\_SystemPatch-1.0.5.ubf is listed under **FileName** column.
- Step 6** In the **Critical Fixes** pane, click **Install**.
- Step 7** Click **Yes** in the pop-up dialogue box to install Cisco Prime Infrastructure PI\_3\_10\_2\_SystemPatch-1.0.5.ubf. It may take approximately 1 hour for the installation process to complete.
- Note** Do not manually restart the server while the installation is in progress.
- Step 8** You can verify the release installation from Prime Infrastructure Login under **Critical Fixes** by clicking **View Installed Updates** and also by logging into the server and choosing **Administration > Software Update**. You should see a listing for the release in the **Updates** tab, with **Installed** in the Status column.
- 

## New Features and Enhancements

This section provides a brief description of new features and enhancements in Cisco Prime Infrastructure 3.10.2.

### Wired

In **Cisco Prime Infrastructure**, under **Administration > Users > Users, Roles & AAA > TACAS+ Servers > Add TACAS Server** - You can add maximum of five TACAS+ Servers.

### Reports Enhancements

In **Cisco Prime Infrastructure**, under **Reports > Report Launch Pad > Performance > Conversations** report is enhanced to show 300k records in this release.

### Wireless

#### New Access Point Support

Cisco Prime Infrastructure 3.10.2 supports the following Aurora CM6x APs:

- Cisco Catalyst Wireless 9162 Series Unified Access Points
- Cisco Catalyst Wireless 9164 Series Unified Access Points

- Cisco Catalyst Wireless 9166 Series Unified Access Points

## Important Notes

This section contains important notes about Cisco Prime Infrastructure 3.10.2 Upgrade:

- When your system is running with Prime Infrastructure 3.10 or 3.10 Update 01 or 3.10.1 and upgraded to Prime Infrastructure 3.10.2, please do not install the Prime Infrastructure 3.10 - Device Pack 1 separately. By default, the Prime Infrastructure 3.10 - Device Pack 1 is installed during upgrade of Prime Infrastructure 3.10.2.
- When you restore to Cisco Prime Infrastructure 3.10.2 from earlier versions 3.7.x, 3.8.x, 3.9.x, 3.10.x backup, you will be notified with the following warnings in the restore console window:

```
Warning:
<verisignsaca> uses a 1024-bit RSA key which is considered a security risk. This key
size will be disabled in a future update.
<airespace-root> uses a 1536-bit RSA key which is considered a security risk. This key
size will be disabled in a future update.
<verisignclass1ca> uses a 1024-bit RSA key which is considered a security risk. This
key size will be disabled in a future update.
<verisignclass1g2ca> uses a 1024-bit RSA key which is considered a security risk. This
key size will be disabled in a future update.
<verisignclass2g2ca> uses a 1024-bit RSA key which is considered a security risk. This
key size will be disabled in a future update.
<verisignclass3ca> uses a 1024-bit RSA key which is considered a security risk. This
key size will be disabled in a future update.
<verisignclass3g2ca> uses a 1024-bit RSA key which is considered a security risk. This
key size will be disabled in a future update.
<verisignsaca> uses a 1024-bit RSA key which is considered a security risk. This key
size will be disabled in a future update.
Warning:
<airespace-root> uses a 1536-bit RSA key which is considered a security risk. This key
size will be disabled in a future update.
```

These warning messages are displayed due to the recent upgrade of JRE in Prime Infrastructure 3.10.2. For more information, see [JDK-8172404](#).

## Open Caveats

The following table lists the open caveats in Cisco Prime Infrastructure Release 3.10.2

Click the identifier to view the impact and workaround for the caveat. This information is displayed in the Bug Search Tool. You can track the status of the open caveats using the [Bug Search Tool](#).

**Table 1: Open Caveats**

| Identifier                 | Description                                                                              |
|----------------------------|------------------------------------------------------------------------------------------|
| <a href="#">CSCwb01957</a> | Unified AP count is wrong from Cisco Prime Infrastructure Operations Center.             |
| <a href="#">CSCwb87973</a> | Cisco Prime Infrastructure Smart Licensing registration through Transport Gateway fails. |
| <a href="#">CSCwc30308</a> | Floor image is not displayed on the floor when sitemaps are opened in Planning Mode.     |

| Identifier                 | Description                                                                   |
|----------------------------|-------------------------------------------------------------------------------|
| <a href="#">CSCwc48125</a> | Reports not getting in Interface Utilization and Interface Utilization Trend. |
| <a href="#">CSCwc53613</a> | Duplicate data in AP Summary Report.                                          |

## Resolved Caveats

The following caveats were resolved in Cisco Prime Infrastructure Release 3.10.2. You can view additional information about these caveats in the [Bug Search Tool](#).

**Table 2: Resolved Caveats**

| Identifier                 | Description                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------|
| <a href="#">CSCwc00879</a> | Cisco Prime Infrastructure 3.10 server slowness and degraded performance.                                           |
| <a href="#">CSCwa95488</a> | /var/log/audit log pilling and hitting 100% crashes the server.                                                     |
| <a href="#">CSCvy86201</a> | Cisco Prime Infrastructure PSIRT incorrectly reports vulnerabilities as non-vulnerable for multiple devices.        |
| <a href="#">CSCvz76428</a> | Backup file transfer operation doesn't resume back when it is interrupted during file transfer.                     |
| <a href="#">CSCvz79440</a> | Intermittently AP Radio Downtime Report has inconsistent uptime and downtime.                                       |
| <a href="#">CSCvz91745</a> | Cisco Prime Infrastructure 3.8 affected by Vulnerabilities CVE-2021-39275 CVE-2021-34798.                           |
| <a href="#">CSCvz93377</a> | Compliance report fails to generate data, if a device is deleted that is mapped to a compliance job.                |
| <a href="#">CSCvz93390</a> | Duplicate hostname in the database, causes fail to generate compliance report data.                                 |
| <a href="#">CSCwa23046</a> | Prime Infrastructure 3.9.1 Backup failure: Directory appcomponent/DB/WCS/fast_recovery_area/WCS not empty.          |
| <a href="#">CSCwa26095</a> | Cisco Prime Infrastructure 3.9 export without credentials is not working for some filtering criteria.               |
| <a href="#">CSCwa33627</a> | Client Count report on every floor to select SSID style is changed from Prime Infrastructure 3.5.                   |
| <a href="#">CSCwa36320</a> | Cisco Prime Infrastructure 3.9 Custom Reports saved templates, the export to CSV generates a blank or partial file. |

| Identifier                 | Description                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------|
| <a href="#">CSCwa42051</a> | Misspelled word in "ncs certvalidation" error message.                                                              |
| <a href="#">CSCwa45650</a> | RPM Vulnerabilities- kernel, libxml2, krb5, nss, bind, libx11                                                       |
| <a href="#">CSCwa48391</a> | Update the vulnerabilities details in 3.8 3.7 & other relevant versions or Prime Infra release notes                |
| <a href="#">CSCwa57114</a> | Cisco Prime Infrastructure 3.10 the "ON/OFF" switch labels on Site Map (New) is incomplete when logged in Japanese. |
| <a href="#">CSCwa61084</a> | Validation for Exported Map archive doesn't work when the file name contains a comma.                               |
| <a href="#">CSCwa73474</a> | MAPS imports fails, when the user had imported the groups earlier into Prime.                                       |
| <a href="#">CSCwa81173</a> | CDP AP Neighbor records are not getting updated automatically in Prime Infrastructure.                              |
| <a href="#">CSCwa99921</a> | Password-lock-enabled command locks out tacacs+ user from Prime Infrastructure CLI.                                 |
| <a href="#">CSCwb00243</a> | Rogue APs list will not be shown from Alarm Summary.                                                                |
| <a href="#">CSCwb18109</a> | Clients not discovered properly in Prime Infrastructure when it roams between AireOS and 9800.                      |
| <a href="#">CSCwb21197</a> | Validate images REST API pairs incorrect kickstart with system image of the same release version                    |
| <a href="#">CSCwb23834</a> | Wireless Network Executive Summary failed to run report with error message -1.                                      |
| <a href="#">CSCwb25202</a> | Prime 3.10 PSIRT and EOX compliance "PAS and RBML bundle" update.                                                   |
| <a href="#">CSCwb34815</a> | Heatmaps for a/n/ac protocol are not getting colored up in planning mode.                                           |
| <a href="#">CSCwb57097</a> | Cisco Prime Infrastructure 3.9 Site Membership column in Config Archive page is showing incorrect location.         |
| <a href="#">CSCwb68584</a> | Device/interface auto monitoring policy not collecting the data when SNMPv1 disabled.                               |
| <a href="#">CSCwb71299</a> | Cisco Prime Infrastructure may fail to prune job entries.                                                           |

| Identifier                 | Description                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------|
| <a href="#">CSCwb86927</a> | When we remove client from prime exclusion list, its not removing automatically from WLC exclusion.             |
| <a href="#">CSCwb93262</a> | snmpmonitor.sh cannot restart snmpservice                                                                       |
| <a href="#">CSCwb93504</a> | Last backupTime column in wireless inventory page is showing NA for 9800 devices.                               |
| <a href="#">CSCwc00746</a> | Client Traffic shown as 0 for 9800 WLC in Prime Infrastructure 3.10.1.                                          |
| <a href="#">CSCwc23733</a> | Cisco Prime Infrastructure 3.10.1 - Apache version 2.4.53 affected by CVE-2022-26377.                           |
| <a href="#">CSCwc27850</a> | Cisco Prime Infrastructure 3.10.2 - Multiple RPM vulnerabilities.                                               |
| <a href="#">CSCwc56869</a> | Heatmaps are not shown correctly for C9120AXE-E with AIR-ANT2566P4W-RS.                                         |
| <a href="#">CSCwc62594</a> | Stopping NCS services may unmount required /dev/shm disk partition.                                             |
| <a href="#">CSCwc74839</a> | Cisco Prime Infrastructure does not allow adding ISE server when the username contains more than 15 characters. |

## Submitting Feedback

Your feedback will help us improve the quality of our product. You must configure the email server and then enable data collection to configure the feedback tool. To send your feedback, follow these steps:

### Procedure

- 
- Step 1** If you have configured your mail server, go to Step 4.
  - Step 2** Choose **Administration > Settings > System Settings > Mail and Notification > Mail Server Configuration**.
  - Step 3** In the Mail Server Configuration page, enter the mail server details, then click **Save** to save the configuration settings.
  - Step 4** Choose **Administration > Settings > System Settings > General > Help Us Improve**.
  - Step 5** In the Help Us Improve Cisco Products page, select **Yes, collect data periodically**, then click **Save**.
  - Step 6** Click the Settings icon, then select **Feedback > I wish this page would**.
  - Step 7** Enter your feedback, then click **OK**.
- 

## Related Documentation

You can access additional Cisco Prime Infrastructure documentation at:



[http://www.cisco.com/en/US/products/ps12239/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps12239/tsd_products_support_series_home.html)

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html> .

Subscribe to *What's New in Cisco Product Documentation* , which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

