# Cisco Prime Infrastructure 3.10.4 Update 02 Release Notes

**First Published:** 2023-12-22

## Introduction

This is the second update release of Cisco Prime Infrastructure 3.10.4.

You can install Cisco Prime Infrastructure 3.10.4 Update 02 (PI_3_10_4_Update_02_and_PDMT_5.1-1.0.11.ubf) on Cisco Prime Infrastructure 3.10.4 System Patch or Cisco Prime Infrastructure 3.10.4 or 3.10.4 Update 01. Prime Infrastructure PI_3_10_4_Update_02_and_PDMT_5.1-1.0.11.ubf is approximately 713 MB.

**Note** PI 3.10.4 Update 02 ubf includes Prime Data Migration Tool Update 05.01.

You must install the Cisco Prime Infrastructure 3.10.4 Update 02 System Patch (PI_3_10_4_Update_02_SystemPatch-1.0.5.ubf - approximately 2.04 GB) after 3.10.4 Update 02 installation. This includes Oracle October 2023 critical patch update. To install the system patch, see Installing the System Patch from Local Storage.

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 server and wen client requirements, see Understand System Requirements section in the *Cisco Prime Infrastructure 3.10 Quick Start Guide.*

### Installation Guidelines

The following sections explain how to install the maintenance release.

#### Before You Begin Installing the Maintenance Release

You can install Prime Infrastructure 3.10.4 Update 02 on top of Cisco Prime Infrastructure 3.10.4 or Cisco Prime Infrastructure 3.10.4 System Patch or Cisco Prime Infrastructure 3.10.4 Update 01 from Software Download page.

Since the maintenance release is not removable, it is important to have a way to revert your system to the original version in case hardware or software problems cause the maintenance release installation to fail.

To ensure you can do this, take a backup of your system before downloading and installing this UBF maintenance release.

If the backup is a Prime Infrastructure 3.10.4 backup, restore the backup on Prime Infrastructure 3.10.4 server before applying the 3.10.4 update 02 release.

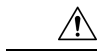
Similarly, if you are running Prime Infrastructure 3.10.4 in a Virtual Machine (VM) and your organization permits taking VM snapshots, stop Prime Infrastructure and use the VMware client to take a VM snapshot before applying this maintenance release. Store the snapshot in an external storage repository, and restore from the snapshot if the maintenance release installation is unsuccessful. For more details, see Restore an Application Backup in the *Cisco Prime Infrastructure 3.10 Administrator Guide*.

To revert to Prime Infrastructure 3.10.4 Update 02 installation (with PI 3.10.x, PI 3.9.x, PI 3.8.x, or PI 3.7.x backup), follow these steps:

1. Reinstall Prime Infrastructure 3.10 from an OVA or ISO distribution
2. Upgrade to Cisco Prime Infrastructure 3.10.2 using tar bundle and install PI 3.10.2 system patch once after upgrade is completed. For more information, see *Cisco Prime Infrastructure 3.10.2 Release Notes*
3. Install Cisco Prime Infrastructure 3.10.4 PI_3_10_4-1.0.24.ubf
4. Install Cisco Prime Infrastructure 3.10.4 System Patch, PI_3_10_4_SystemPatch-1.0.12.ubf
5. Install Cisco Prime Infrastructure 3.10.4 Update 02, PI_3_10_4_Update_02_and_PDMT_5.1-1.0.11.ubf
6. Install Cisco Prime Infrastructure 3.10.4 Update 02 System Patch , PI_3_10_4_Update_02_SystemPatch-1.0.5.ubf
7. If you have a prior 3.10.x, 3.9.x, PI 3.8.x, PI 3.7.x backup - Restore this backup

If you are installing this release as part of a High Availability (HA) implementation, see *Before you Begin Setting Up High Availability* in the Cisco Prime Infrastructure 3.10 Administrator Guide.

## Installing the Release from Local Storage



**Caution** If you have a High Availability (HA) environment, remove the HA setup before proceeding to install this release. For more details, see Installing the Maintenance Release in High Availability Mode, on page 3.

Make sure that you have completed the recommended preparation steps given in Before You Begin Installing the Maintenance Release, on page 1 .

To install Cisco Prime Infrastructure 3.10.4 Update 02 from the local storage, follow these steps:

### Procedure

**Step 1** Download the Prime Infrastructure PI_3_10_4_Update_02_and_PDMT_5.1-1.0.11.ubf from Home > Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions > Prime Infrastructure > Prime Infrastructure 3.10 > Prime Infrastructure Patches - 3.10.4 and save the file in your local system.

**Step 2** Log in to Prime Infrastructure 3.10.4 System Patch or Prime Infrastructure **3.10.4** 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 maintenance release 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_4_Update_02_and_PDMT_5.1-1.0.11.ubf is listed under **FileName** column.

**Step 6** In the **Critical Fixes** pane, click **Install**.

**Note** Do not manually restart the server while the installation is in progress.

**Step 7** Click **Yes** in the pop-up dialogue box to install Cisco Prime Infrastructure **PI_3_10_4_Update_02_and_PDMT_5.1-1.0.11.ubf**. It may take approximately 1 hour for the installation process to complete.

**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.

## Installing the Maintenance Release in High Availability Mode

Download PI_3_10_4_Update_02_and_PDMT_5.1-1.0.11.ubf from Home > Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions > Prime Infrastructure > Prime Infrastructure 3.10 > Prime Infrastructure Patches - 3.10.4 and save the file in your local system.

To install the downloaded PI_3_10_4_Update_02_and_PDMT_5.1-1.0.11.ubf in High Availability mode follow the below prerequisites:

- Make sure that you have completed the recommended preparation steps given in Before You Begin Installing the Maintenance Release, on page 1.

**Note** Prime Infrastructure **3.10.4 Update 02** can be applied only in primary and secondary standalone servers. The server will restart automatically once the installation is complete. The restart typically takes more than 60 minutes. You cannot apply Prime Infrastructure **3.10.4 Update 02** when HA is enabled.

- If you are installing Cisco Prime Infrastructure 3.10.4 Update 02 on High Availability (HA) paired servers, you will get an error message.

For more details, see Remove HA Via the GUI in the *Cisco Prime Infrastructure 3.10 Administrator Guide*.

- Continue the patching once HA removed completely. For more details, see the How to Patch New HA Servers section in the *Cisco Prime Infrastructure 3.10 Administrator Guide* .

### Troubleshooting Maintenance Release Installs in High Availability Implementations

If you are unable to apply this maintenance release in a High Availability (HA) implementation, check whether your network bandwidth, throughput and latency meets the network requirements recommended in Network Throughput Restrictions on HA section in the *Cisco Prime Infrastructure 3.10 Administrator Guide.* In a few cases, continued or intermittent throughput problems can cause a complete failure. If you believe this has occurred, contact Cisco TAC for support.

If you are unable to verify that this maintenance release has been successfully installed on a Prime Infrastructure server, or one or both of the servers fails to restart properly after installing the maintenance release, you may need to re-image the server as explained in Before You Begin Installing the Maintenance Release, on page 1 before continuing.

In all cases, you can use the backup-logs command on one or both servers to get information on the source of the failure. For more information, see the backup-logs section in the *Cisco Prime Infrastructure 3.10 Command Reference Guide* .

### Installing the System Patch from Local Storage

- You can only install Cisco Prime Infrastructure PI_3_10_4_Update_02_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_4_Update_02_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 more than 60 minutes.

To install Cisco Prime Infrastructure PI_3_10_4_Update_02_SystemPatch-1.0.5.ubf from the local storage, follow these steps:

**Procedure**

**Step 1** Download the Prime Infrastructure from PI_3_10_4_SystemPatch-1.0.12.ubf Home > Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions > Prime Infrastructure > Prime Infrastructure 3.10 > Prime Infrastructure Patches - 3.10.4 and save the file in your local system.

**Step 2** Log in to Prime Infrastructure **3.10.4 Update 02** 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_4_Update_02_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_4_Update_02_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 3.10.4 Update 02.

### Wired

Starting from Prime Infrastructure 3.10.4 Update 02, the registration URL for Smart Software Licensing has been modified to https://smartreceiver.cisco.com/licservice/license. Ensure that you need to re-register the Prime Infrastructure using the provided token.

To re-register the Smart Software Licensing after installing the Prime Infrastucture 3.10.4 update 02, do the following:

**Note** Ensure that proxy is enabled before registering the Smart Software Licensing.

- De-register the existing Smart Software Licensing registration.
- Disable Smart Software Licensing and Enable Smart Software Licensing.
- Register the Smart Software Licensing using the provided token.

## Important Notes

- Cisco announced the End-of-Life and End-of-Sale for all versions of Prime Infrastructure. Please use the PDMT to migrate data to Cisco DNA Center or use Cisco Networking Bot for self-help migration. For more information reach out to the migration team at **primetodnacmigration@external.cisco.com**.
- The EOL/EOS message always appears on the Login Page of Prime Infrastructure.
- The EOL/EOS message appears in a pop-up notification window every time the user login to the Prime Infrastructure. However, after restart of the Prime Infrastructure services, the pop-up message will not be notified in the future.
- For all the versions of Prime Infrastructure, Prime XWT Widgets are not compatible with the latest versions of Chrome and Edge browsers. This impacts the prime xwt actions such as add, update, delete, duplicate, and so on.
  - **Edge**:
    - 114.0.1823.51
    - 114.0.1823.43
  - **Chrome**:
    - 114.0.5735.133
- It is recommended to use Firefox or lower versions of Chrome and Edge browsers to carry out the Prime XWT widget actions in the Prime Infrastructure.
- When you restore to Cisco Prime Infrastructure 3.10.4 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:
<verisigntsaca> 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.
<verisigntsaca> 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 Prime Infrastructure Release 3.10.4 Update 02.

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 |
|---|---|
| CSCwf79556 | CSCvs32965 - defect not fixed in the latest version of Prime Infrastructure |
| CSCwh47648 | Copy and replace APs from 9800 WLC may not copy the correct tag source |
| CSCwi08182 | Unable to generate reports - Wireless utilization and AP RF Quality history |
| CSCwi24936 | Peak throughput value retrieved is incorrect in report-AP Utilization |
| CSCwi28067 | Cisco Prime Infrastructure not setting source VRF and source address in telemetry subscriptions |
| CSCwi36513 | Operations Center may show incorrect redunancy status for wireless controllers |
| CSCwi39231 | \"Distribution operation failed\" error is received using Smart Delete option in SWIM to Catalyst 9200 |
| CSCwi40878 | Dot1x authenticated client is discovered on another switch randomly |
| CSCwi41164 | Prime operaation center's AP inventory report fails when choosing the Report View as tabular column or both |
| CSCwi51801 | 500 Internal error occurs intermittently while running Client Details in REST API |
| CSCwi54771 | Different report data received from Prime Infrastructure 3.4 than PI 3.10 with the same wireless conteroller 5508 |
| CSCwi57090 | PDMT 5.1 update 02: PDMT Launch UI page kept on loading in loop |

# Resolved Caveats

The following caveats were resolved in Prime Infrastructure Release 3.10.4 Update 02.

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 2: Resolved Caveats***

| Identifier | Description |
|---|---|
| CSCwe84738 | Cisco Prime Infrastructure 3.10 High Availability failed to create standby database with Cisco DNA Center appliance (250GB RAM) |
| CSCwf32195 | Export or import of BULK AP report fails when building or floor name contains double-byte characters or comma (,) in the BULK |
| CSCwf32545 | When two protocols are selected, Air Quality vs Time report shows an error |
| CSCwf42327 | Inspect Voice Readiness may not work for floors with high AP counts |
| CSCwf52364 | Prime Infrastucture 3.10.3 operation center may intermittently break reachability with instances |
| CSCwf62199 | Critical CVE in component axis. Upgrade to latest version |
| CSCwf70606 | CGS2520 Switch software image distribution job returns false negative result |
| CSCwf71714 | Prime Infrastucture 3.10.3 - C9200 Devices collection failure |
| CSCwf77474 | Unable to export Unified AP from **Dashboard > Overview > Unified AP status** returns page error: 404 |
| CSCwf79753 | Syslog forward related functionality - not updated in the documentation accurately from PI 3.8 |
| CSCwf81859 | Cisco Prime Infrastructure Java Deserialization Vulnerability |
| CSCwf81862 | PI and EPNM SQL Injection Vulnerability |
| CSCwf81865 | Prime Infrastructure Privilege Escalation Vulnerability |
| CSCwf81870 | Cisco Prime Infrastructure Cross-Site Scripting Vulnerability |

| Identifier | Description |
|---|---|
| CSCwf88943 | Client count differs between Prime Infrastructure and eWLC 9800 |
| CSCwf90656 | Documentation should be clearer on the compatibility between PI 3.10 and MSE 8.0.150.x |
| CSCwf92234 | Need to document that Map Editor cannot be launched from Planning Mode |
| CSCwf93363 | Alarm policy isn't created from Alarms & Events page |
| CSCwf93551 | Prime Infrastructure 3.10.5 - Apache Tomcat 9.0.0 < 9.0.75 |
| CSCwf93565 | RHEL 7 : c-ares (RHSA-2023:3741) , open-vm-tools (RHSA-2023:3944) , emacs (RHSA-2023:3481) |
| CSCwf96729 | Prime 3.10.4 PSIRT and EOX compliance “PAS bundle” updation |
| CSCwf97489 | Critical CVE in component python. Upgrade to latest version |
| CSCwf97496 | Critical CVE in component activemq. Upgrade to latest version |
| CSCwh00530 | Data may be missing from Report Criteria after running or saving the Client Count report |
| CSCwh02008 | RHEL 7 : kernel (RHSA-2023:4151) , bind (RHSA-2023:4152) |
| CSCwh02023 | Oracle Database Server (Jul 2023 CPU),Oracle Java SE Multiple Vulnerabilities (July 2023 CPU) |
| CSCwh07826 | The number of unified APs mismatch under unifiedAP view. |
| CSCwh09288 | Controller Inventory Report is missing data in the Peer Controller Serial Number Field |
| CSCwh09619 | PI 3.10.3 - Software Image Activation fails for C3560CX device |
| CSCwh18401 | OpenSSL 1.0.2 < 1.0.2zg & 1.0.2 < 1.0.2zh & 1.0.2 < 1.0.2zi Multiple Vulnerabilities |
| CSCwh19702 | Send file to this SFTP software using CLI copy command or automated backup process fails |
| CSCwh21400 | If devices are managed with FQDN/DNS name then the Compliance Audit job may fail |

| Identifier | Description |
|---|---|
| CSCwh28995 | There are 1841 Devices in partial collection failure |
| CSCwh40535 | SWIM distribution with activation job fails for Catalyst 3850 devices in Prime Infrastructure 3.10.4 |
| CSCwh44796 | RHEL 7 : kernel (RHSA-2023:4819) & RHEL 7 : cups (RHSA-2023:4766) |
| CSCwh44802 | Apache Tomcat 9.0.0.M1 < 9.0.80 |
| CSCwh54086 | PI 3.10.4 - Device Discovery page may not load |
| CSCwh55122 | Unable to export the violation details in Excel format in Compliance dashboard |
| CSCwh57823 | Prime Infrastructure do not set source-VRF for telemetry |
| CSCwh57882 | PI 3.7 - REST API for C9800 returns 500 error code |
| CSCwh61703 | PI 3.10.2 - Association time for clients may show up with future dates |
| CSCwh63298 | RHEL 7 : open-vm-tools (RHSA-2023:5217) |
| CSCwh84581 | HTTP/2 Rapid Reset Attack Affecting Cisco Products: October 2023 |
| CSCwh84591 | RHEL 7 : kernel (RHSA-2023:5622) , libssh2 (RHSA-2023:5615) |
| CSCwh84595 | Apache Shiro < 1.11.0 Authentication Bypass |
| CSCwh88008 | RHEL7 : bind (RHSA-2023:5691) |
| CSCwh90825 | Active or scheduled guest users status change to expired |
| CSCwh93435 | Oracle Java SE Multiple Vulnerabilities (October 2023 CPU),Oracle Database Server (October 2023 CPU) |
| CSCwh97250 | Apache 2.4.x < 2.4.58 Multiple Vulnerabilities |
| CSCwi02407 | RHEL 7 : kernel (RHSA-2023:5622) |

## 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

## 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.