



# Horizon DaaS Platform 6.1.2 Release Notes

VMware Horizon DaaS Platform | 07 NOV 2014

Release notes last updated on 07 NOV 2014

Check for additions and updates to these release notes.

## What's in the Release Notes

The release notes cover the following topics:

- Patch Information
  - Patch Dependencies
  - Affected Horizon DaaS Versions
  - Patch Version
- Resolved Issues
- Installing the Patch
  - Upload the Patch File
  - Install the Patch on All Service Provider Appliances
  - Install the Patch on All Tenant Appliances
  - [Optional] Manually Disable SSLv3 on Org1000 Systems
- Uninstalling the Patch

## Patch Information

### Patch Dependencies

Horizon DaaS Platform 6.1.1 (Build 22355)

### Affected Horizon DaaS Versions

Horizon DaaS Platform 6.1.0 (Build 22210)

Horizon DaaS Platform 6.1.1 (Build 22355)

### Patch Version

Horizon DaaS Platform 6.1.2 (Build 22583)

## Resolved Issues

This patch fixes a security issue related to the use of SSLv3 on appliances. This patch disables

support for SSLv3, which is now considered unsafe due to the POODLE vulnerability. TLSv1 is now considered the minimally safe protocol.

## Installing the Patch

Pushing out software patches to all appliances in one or more Data Centers is a multi-step process:

- Upload the patch. When you upload the patch file, it is automatically replicated to all appliances.
- Install the patch file on all Service Provider appliances.
- Install the patch file on all Tenant appliances.
- [Optional] Manually Disable SSLv3 on Org1000 Systems

These steps are described below.

### Upload the Patch File

1. In the Service Center, select **appliances ► software updates**. The Software Updates screen displays.
2. Click **Browse** to browse for the patch file.
3. Click **Upload**.

The Service Center checks whether the file is the correct file type. The patch file is automatically replicated to all Service Provider appliances in each Data Center. The Replications column in the lower portion of the screen indicates the progress. For example, 2/2 means that the patch file has been replicated to both the primary and secondary Service Provider appliances in a single Data Center and 4/4 means that the patch file has been replicated to the primary and secondary Service Provider appliances in two Data Centers. It can take up to one minute for each appliance. You must wait until the patch file has been replicated to an appliance before installing the patch on that appliance.

### Install the Patch on All Service Provider Appliances

Before you begin the installation, note the following:

- If you have a staggered Horizon DaaS 6.1 environment (that is, with tenant appliances still running Horizon DaaS 6.0 or 6.0.1) it is recommended that you upgrade the tenant appliances to Horizon DaaS 6.1.2 if possible or contact VMware Global Support for instructions on how to apply the 6.0.2 and 6.0.3 patches manually to the 6.0/6.0.1 appliances.
- If you start the installation before the patch file has been replicated to all Service Provider appliances, you are warned that replication is not complete on specific appliances. However, you can begin installation on those appliances where

**replication is complete.**

## Procedure

1. In the Service Center, select **appliances ► software updates**. The Software Updates screen lists the available patches. Each patch name is a link.
2. Click on the name of a patch. The Software Updates screen redisplay to show those organizations that have appliances that have not been patched.
3. Mark the checkbox for organization 1000.
4. To install the patch in a single Data Center, select a Data Center from the drop-down. To install the patch on all appliances in all Data Centers, accept the default value "All".
5. Click **Install**.

## Install the Patch on All Tenant Appliances

1. In the Service Center, select **appliances ► software updates**. The Software Updates screen lists the available patches. Each patch name is a link.
2. Click on the name of a patch. The Software Updates screen redisplay to show those organizations that have appliances that have not been patched.
3. For each Tenant:
  - a. Mark the checkbox for the organizations you need to patch.
  - b. The Data Center drop-down default value is All, which installs the patch on all appliances in all Data Centers. To install in a single Data Center, select that Data Center from the drop-down.
4. Click **Install**.

## [Optional] Manually Disable SSLv3 on Org1000 Systems

**Warning:** Before disabling SSLv3 on Org1000 appliances, you must have applied this patch to all of your Tenant appliances.

If the Service Center is accessible from the public internet, you might want to disable SSLv3 on the Org1000 systems to address the Service Center vulnerability. To do this, perform the steps below on each appliance.

## Procedure

1. Open the server.xml file (/usr/local/jboss-5.1.0.GA-cxf/server/desktop/deploy/jbossweb.sar/server.xml)
2. Insert SSLProtocol="TLSv1" into the Connector element for Ports 443 and 8443, as shown below. New text is in **red**.

```
<Connector  
protocol="HTTP/1.1"
```

```
allowTrace="false"
SSLEnabled="true"
port="443"
maxThreads="500"
scheme="https"
secure="true"
clientAuth="false"
enableLookups="false"
SSLEngine="on"
SSLProtocol="TLSv1"
SSLCertificateFile="/usr/local/desktone/cert/ssl_cert_file"
SSLCertificateKeyFile="/usr/local/desktone/cert/ssl_cert_key_file"
SSLCACertificateFile="/usr/local/desktone/cert/ssl_ca_cert_file"
SSLCipherSuite="ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-ECDSA-AES256-G$
```

```
<Connector
protocol="HTTP/1.1"
allowTrace="false"
SSLEnabled="true"
port="8443"
maxThreads="500"
scheme="https"
secure="true"
clientAuth="false"
enableLookups="false"
SSLEngine="on"
SSLProtocol="TLSv1"
SSLCertificateFile="/usr/local/desktone/cert/appliance_cert_file"
SSLCertificateKeyFile="/usr/local/desktone/cert/appliance_key_file"
SSLCipherSuite="ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-ECDSA-AES256-G$
```

## Uninstalling the Patch

To revert to the previous version, uninstall the patch by executing these commands on all appliances as the root user:

```
sudo apt-get remove dt-platform-6-1-0-patch-2
sudo service dtService restart
```

Copyright © 2021 VMware, Inc. All rights reserved.