

# Horizon DaaS 6.1 – Downloading SSL Certificate for Gold Pattern

A VMware Technical Note

This document describes the procedure for downloading an SSL certificate for a gold pattern.

August 2014



## Revision History

Date	Version	Description
09/04/2014	1.0	Initial release
10/15/2014	1.1	Updated for new DaaS Agent version 6.1.1

© 2014 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Introduction

When you upgrade to DaaS agent version 6.1 or higher, you must manually download the certificate authority's public certificate from Enterprise Center and copy it to the DaaS agent's cert directory. The agent needs to have a copy of the public certificate from the certificate authority in order to verify the signature of the Tenant Appliance certificate.

Note the following:

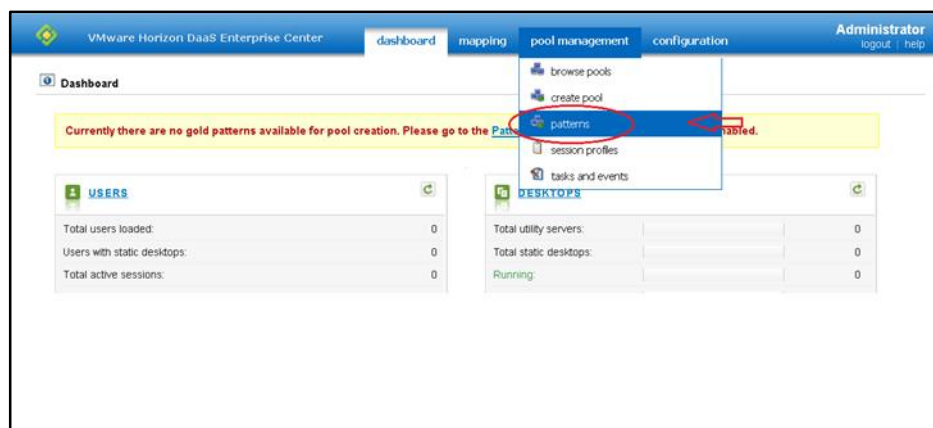
- **Port change** - Beginning in Brighton agents use port 8443 for secure socket communication with the TA. In older releases the agents used port 443. Customer administrators will need to ensure that https traffic on port 8443 is allowed through any firewalls between the agents running on desktop systems and the tenant appliance.
- **Support for older agent versions** - Older agent versions will continue to function, but with no SSL certificate validation when connecting to a Tenant Appliance with the latest version. In a future release that legacy support will be disabled and agents will need to be upgraded or they will be unable to connect to the Tenant Appliance.
- **Future agent upgrades** - This process will not have to be repeated for future agent upgrades, since the the cert direct directory and cacert.pem file will remain after agent uninstallation. On startup of the new agent, it will continue to use the existing cacert.pem file. If uninstalling the DaaS agent, be careful not to unintentionally delete the cert directory containing the cacert.pem file. If you do delete it, you will need to download the cacert.pem file again from Enterprise Center and copy it to the agent's cert directory after installing the new version of the agent.
- **Backup of cacert.pem file** - It is not necessary to back up the cacert.pem file on the DaaS agent system. The cacert.pem file is contained on the service provider and tenant appliances and should be backed up as part of the service provider appliance backups. If the cacert.pem file is lost from the agent system it can be downloaded again from the Enterprise Center.

## Download the Certificate

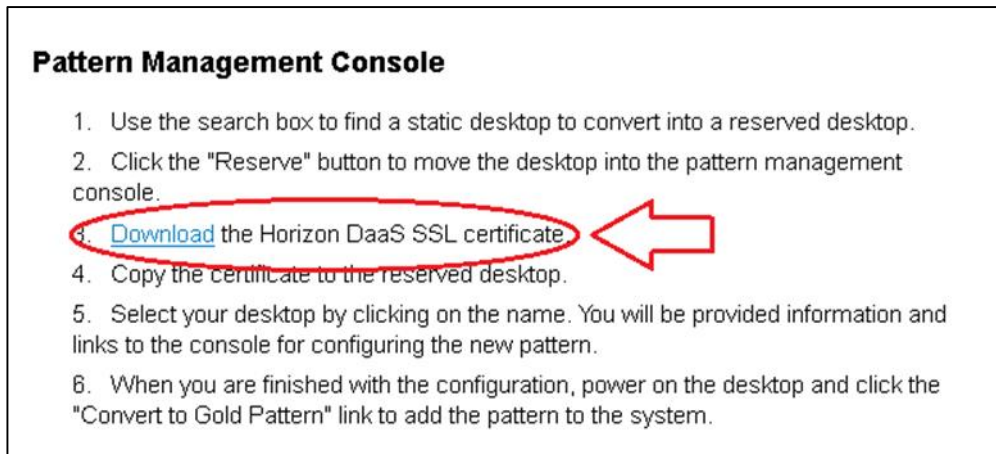
To facilitate this manual step the EC has a page in the UI that allows the enterprise administrator to download the certificate.

### Procedure

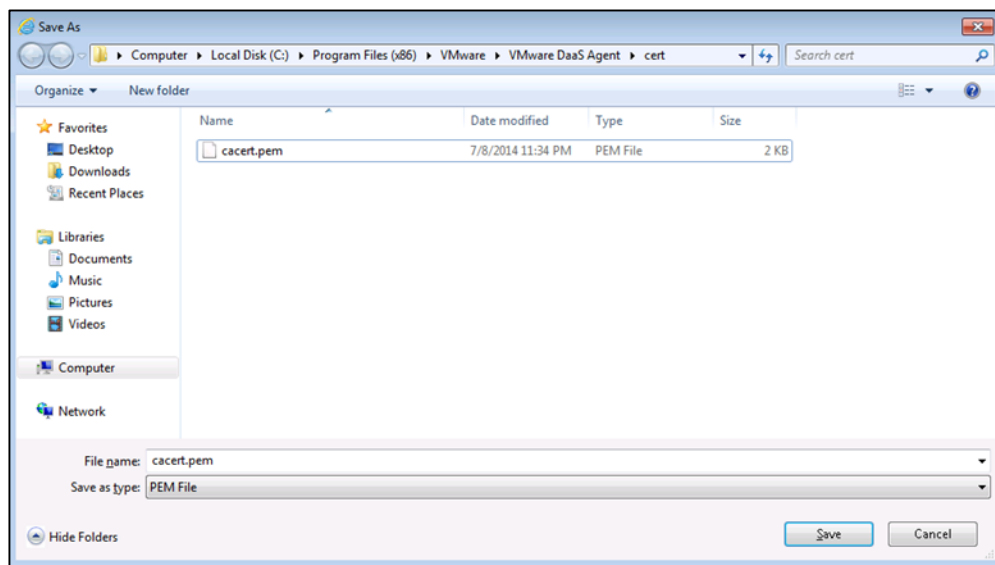
1. In Enterprise Center, select **Pool Management ► Patterns**.



2. On the Pattern Management page, select **Download the Horizon DaaS SSL certificate**.



A dialog box appears prompting you to save the cacert.pem file, which contains the public certificate of the DaaS internal Certificate Authority.



3. Save the file on the gold pattern in the agent's cert directory (typically **C:\Program Files (x86)\VMware\VMware DaaS Agent\cert**) before sealing the gold pattern.
4. Restart the **VMware DaaS Agent** service so that the agent is able to find the file.
5. If you have any desktops that were already deployed before you downloaded the cacert.pem file, copy the cacert.pem file to the agent's cert directory on each of those desktop VMs.
6. If you have any desktops where you have upgraded the agent to version 6.1 or higher from an earlier version, copy the cacert.pm file to the cert directory on those desktop VMs after the agent upgrade is complete.

# Troubleshooting

You can verify that the agent is using the file and that the certificate verification is working by looking in the agent's log in the service\logs directory (C:\Program Files (x86)\VMware\VMware DaaS Agent\service\logs)

- The following log messages show the agent is using SSL validation and properly finding the certificate file:

```
2014-07-10 07:51:49 [INFO ] DaaSAgent - GSoapWithSsl server certificate validation is enabled
```

```
2014-07-10 07:51:49 [INFO ] DaaSAgent - GSoapWithSsl using certificate PEM file: C:/Program Files (x86)/VMware/VMware DaaS Agent/service/./cert/cacert.pem
```

- If the agent is unable to find the cacert.pem file it logs the following warning message:

```
2014-07-10 07:54:31 [WARN ] DaaSAgent - GSoapWithSsl failed to stat certificate PEM file: C:/Program Files (x86)/VMware/VMware DaaS Agent/service/./cert/cacert.pem
```

- Verify that the cacert.pem file exists in the agent's cert directory and has read-only privileges for the Administrator account.

- If the certificate validation is failing messages such as the following may appear:

```
2014-07-08 23:57:01 [ERROR] DaaSAgent - Code: SOAP-ENV:Client; Actor: ; String: SSL_ERROR_SSL
```

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed; Detail: SSL_connect error in tcp_connect()
```

```
2014-07-08 23:57:01 [WARN ] DaaSAgent - DomainHelper: getVmId Failed (2) time(s), will retry after <10> seconds.
```

- Verify that the agent is connecting to the correct Tenant Appliance.