

Knowledge Base

KB Home

Knowledge Base Help

Search the Knowledge Base

Search

View by Article ID

View

Products -->

Category -->

Enabling server-certificate verification for Virtual Infrastructure Clients



(0 Ratings)

Details

This article explains how to enable server-certificate verification on Virtual Infrastructure Clients (VI Clients) after installing VirtualCenter 2.0.1 Patch 1 (Build 33643), VirtualCenter 1.4.1 Patch 1 (Build 33425), VirtualCenter 1.3.1 Patch 2 (Build 35640), or subsequent releases.

Note: VMware products use standard X.509 version 3 (X.509v3) certificates. For more information about the usage of Certificates within a VMware environment including certificate specifications, see:

- [Replacing VirtualCenter Server Certificates in Virtual Infrastructure 3](#)
- [Replacing VirtualCenter Server Certificates in vSphere 4](#)

Solution

VirtualCenter 2.0.1 Patch 1, VirtualCenter 1.4.1 Patch 1, VirtualCenter 1.3.1 Patch 2, and subsequent releases resolve an issue with server-certificate verification by VirtualCenter clients during the initial SSL handshake. Specifically, the X.509 certificate presented by a server to a client at the beginning of an SSL session was not verified. VirtualCenter 2.0.1 Patch 1, VirtualCenter 1.4.1 Patch 1, VirtualCenter 1.3.1 Patch 2, and subsequent releases resolve this issue for Windows client hosts.

However, certificate verification is not enabled by default for the clients - you must specifically enable server-certificate verification on the Windows client host systems. Before enabling server-certificate verification, you must confirm that your servers have valid certificates and replace defective server certificates as needed. Depending on the type of server certificate, you may also need to pre-trust certificates or root certificate authorities. The final step is enabling server-certificate verification below. These three basic steps are covered in this KB:

- [Confirming that Server Certificates are Valid](#)
- [Pre-Trust Certificates](#)
- [Enabling Server-Certificate Verification](#)
- [Disabling Certificate Verification](#)

For more information about VirtualCenter server certificates, including information about how to replace them, see Technical Notes in [Replacing VirtualCenter Server Certificates](#).

Confirming that Server Certificates are Valid

For server-certificate verification to succeed, the certificate's *issued-to* hostname must match the current fully-qualified domain name of the host presenting that certificate. If these names do not match, you should not enable SSL server-certificate verification until you have replaced the certificate.

- The default VirtualCenter certificates are defective and must be replaced prior to enabling server-certificate verification.
 - If you replace the default self-signed certificates with signed certificates purchased from a commercial certificate authority (CA), you can enable server-certificate verification on your upgraded Windows hosts, as described in [Enabling Server-Certificate Verification](#). (See Technical Notes in [Replacing VirtualCenter Server Certificates](#) for information about how to create the certificate-signing request (CSR) necessary to obtain a server certificate signed by a commercial CA.)
 - To replace the default VirtualCenter certificates with certificates signed by your own local root CA. (See Technical Notes in [Replacing VirtualCenter Server Certificates](#)) You must also pre-trust the root CA used to sign your certificates, prior to enabling server-certificate verification.
- The ESX host, GSX host, and VMware Server host certificates are valid, so you need not replace them. However, these systems' certificates must be pre-trusted on the Windows client host systems, including the VirtualCenter host, that will connect to them (see [Pre-Trust Certificates](#) for details). Remember that you also replace these certificates with certificates signed by a commercial CA, in which case you will not need to go through the pre-trust step.

Pre-Trust Certificates

Pre-trusting a certificate or a root CA involves installing the certificate into the trusted store of the Windows client system, prior to attempting any connection to a server that presents a certificate (or a certificate signed by the root CA).

For Virtual Infrastructure Client or VirtualCenter Client host systems, you should login to the system using whatever

Actions

- [Bookmark Document](#)
- [Email Document](#)
- [Print Document](#)
- [Subscribe to Document](#)

SHARE [f](#) [t](#) [e](#) ...

KB Article: **4646606**Updated: **Feb 23, 2010**

Category

How to
Troubleshooting

Products:

VMware ESX
VMware Server
VMware VirtualCenter

Product Versions:

VMware VirtualCenter
1.3.x
VMware VirtualCenter
1.4.x
VMware VirtualCenter
2.0.x
VMware VirtualCenter
2.5.x

account and credentials you will use to connect to either VirtualCenter or ESX, and follow the steps below (without using the **Run as...** option). For VirtualCenter Server host systems, the process is as follows:

1. Login to the Windows client host.
2. Launch the Certificates MMC (Microsoft Management Console) snap-in. For the VirtualCenter host system, you must login as a Windows Administrator:
 - a. Locate `%SystemRoot%\System32\certmgr.msc` on the Windows client.
 - b. Right-click on the `certmgr.msc` file.
 - c. Select **Run as...** from the popup menu.
 - d. Enter the Administrator credentials specific to the Windows local Administrator group in the dialog.
 - e. Click **OK** to continue. The Certificates pane displays.
3. Install the server certificate or the appropriate root CA into the Windows certificate store:
 - a. Click the **Trusted Root Certification Authorities** folder in the *Certificate* pane.
 - b. Select **Action > All Tasks > Import...** to launch the Certificate Import Wizard. The Certificate Import Wizard lets you navigate to the location of the certificate file and import it into the Trusted Root Certification Authorities folder.

Enabling Server-Certificate Verification

Assuming all servers have valid certificates and that the VirtualCenter server and client software has been upgraded, you can enable server-certificate verification on Windows hosts as follows:

1. Download the `ssl-reg-files.zip` (see the link under "Attachments," at the bottom of this article).
2. Confirm that the MD5 checksum of the download is `3c1db2b15f5294fbfde4fa58420886eb`.
3. Unpack `ssl-reg-files.zip` to retrieve the two Registry (.reg) Files:
 - `ssl-enable.reg` creates the necessary registry keys and enables SSL server-certificate verification.
 - `ssl-disable.reg` disables SSL server-certificate verification.
4. Run the `ssl-enable.reg` file on each of the upgraded Windows client hosts:
 - a. Double-click `ssl-enable.reg`. A prompt asking, "Are you sure you want to add the information in\ssl-enable.reg to the registry?" appears.
 - b. Click **Yes** to confirm the change to the Windows registry.
5. Run the registry file on the VirtualCenter host system:
 - a. Double-click `ssl-enable.reg`. A prompt asking, "Are you sure you want to add the information in\ssl-enable.reg to the registry?" appears.
 - b. Click **Yes** to confirm the change to the Windows registry.

To ensure that the SSL server-certificate verification works as you expect it to, you can test the process using a non-production Windows client host (either a physical host, or one running as a virtual machine). Doing so before pre-trusting the signing certificate should result in an error message when you attempt to connect to the server. After pre-trusting the signing certificate, you should not see the error message.

Disabling Certificate Verification

If you have problems, use `cto` to disable server-certificate verification temporarily, until the issue can be resolved. To disable server-certificate verification:

1. Double-click `ssl-disable.reg`. A prompt asking, "Are you sure you want to add the information in\ssl-disable.reg to the registry?" appears.
2. Click **Yes** to confirm the change to the Windows registry.

Note: Refer to the VirtualCenter Configuration portion of the [Basic System Administration Guide](#) to enable or disable the *Verify host SSL certifications* option. To change these options in VirtualCenter, click **Administration > VirtualCenter Management Server Configuration > SSL**.

Keywords

4646606; VC201; VC141; VC131; VC201 Patch 1; VC141 Patch 1; VC131 Patch 2; Patch 2 Patch 2; urlz; alertz; filez

Attachments

- [ATssl-reg-files.zip](#)

Request a Product Feature

To request a new product feature or to provide feedback on a VMware product, please visit the [Request a Product Feature](#) page.

Feedback



(0 Ratings)

Did this article help you?

- ☐ This article resolved my issue.
- ☐ This article did not resolve my issue.
- ☐ This article helped but additional information was required to resolve my issue.

What can we do to improve this information? (4000 or fewer characters)

Email address (optional)

Submit

Permalink to: [Enabling server-certificate verification for Virtual Infrastructure Clients](#)



[Read our blog](#)



[Watch KBTv](#)



[Follow us](#)

Download Products

[Visit Download Center](#)
[Download SDKs & APIs](#)
[Download Patches](#)
[Sign Up for Patch Alerts](#)
[Read Downloads Help Guide](#)

Purchase Support

[Review VMware Support Options](#)
[Request Renewal/Upgrade Quote](#)
[Contact VMware Sales](#)
[Locate a VMware Reseller](#)
[View Support Policies](#)

Connect with Experts

[Visit Community Forums](#)
[Join VMware User Groups](#)
[Visit VMworld](#)
[Browse Training](#)
[Register for Support Days](#)

Find Answers

[Visit Product Support Centers](#)
[Read Product Documentation](#)
[Search the Knowledge Base](#)
[Login to Your Account](#)
[Find Support Help Documents](#)

Copyright © 2010 VMware, Inc. All rights reserved. [Contact Us](#) | [Legal](#) | [Privacy](#) | [Accessibility](#) | [Site Index](#) | [Help](#) | [Feedback](#) [+]

[rss feed](#)