Self-signed Certificates

https://campus.barracuda.com/doc/96016090/

This article provides the following topics:

- About Self-signed Certificates
- Adding a Certificate from the Software Page
- Adding a Certificate During Backup
- Deleting a Certificate

About Self-signed Certificates

Self-signed certificates are required for running a successful VMware backup without generating certificate-related error messages.

Secure Sockets Layer (SSL) a security protocol that creates an encrypted link between a web server and a web browser.

The ECHOplatform Software page allows you to view and add SSL certificates.

Figure 1 displays an example of SSL certificate options,



Figure 1. SSL Certification Options.

Pre-existent indicates that the server was added from a backup wizard and is stored in the catalog.

Verified indicates either a global or a valid SSL certificate was uploaded.

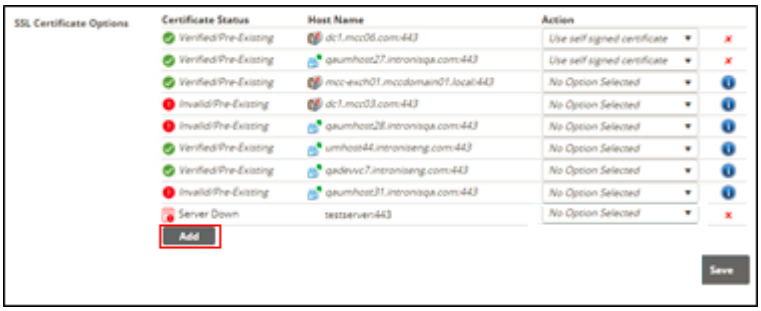
Ignored indicates the user chose to ignore the SSL errors.

Invalid indicates a due to expire certificate or that the user deleted the certificate.

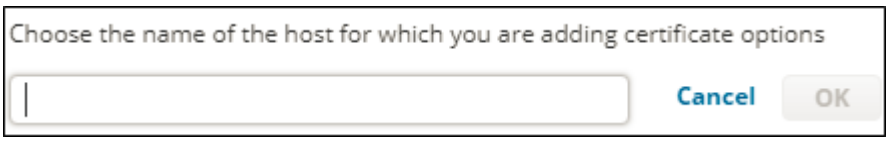
Adding a Certificate from the Software Page

To add a certificate from the Software page, perform the following steps.

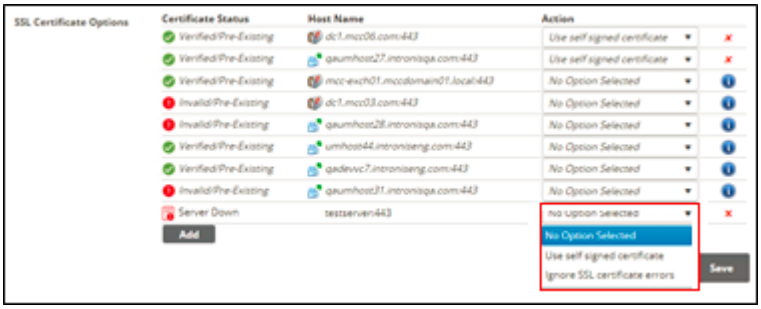
1. At the Software page, click **Edit**.
   The fields that can be edited are displayed.
2. In the SSL Certificates Options section, click the Add button, as shown below.



The Host prompt is displayed.



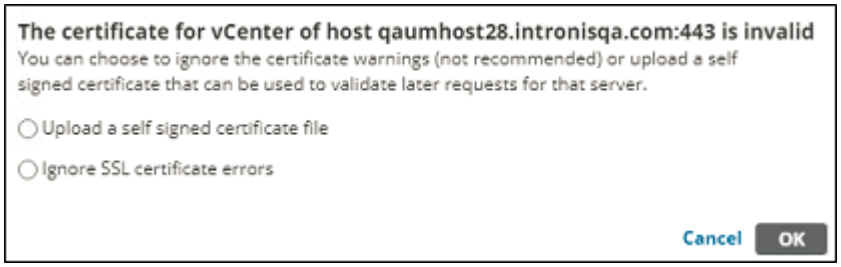
3. At the host prompt, type the name of the host to which you are adding a certificate and then click **OK**.
4. In the Action column, click the down arrow, of the server to which you want to add a certificate, as shown below.
   The Action options menu is displayed.



5. Select **Use self-signed certificate** and then click **Save**.

About Adding a Certificate During Backup

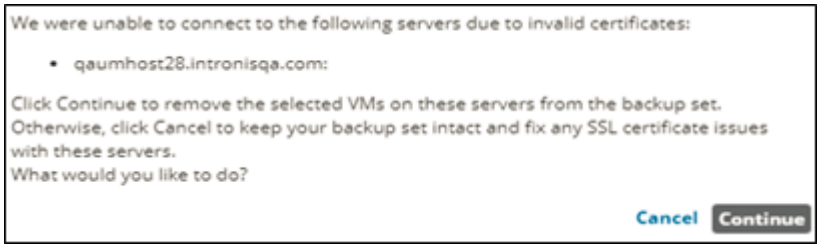
When performing a VMware backup, if a certificate is not assigned to an ESXi host or vCenter, the following error message is displayed.



During the backup procedure, you are provided a step where you can upload a self-signed certificate, by clicking the **Upload a self-signed certificate file** and then clicking **OK**.

The Open dialog is displayed where you can select the certificate.

Also, during backup, In the case where you edited a backup set that contained a VM from a host/vCenter that became invalid after the backup set was created, the following message is displayed.



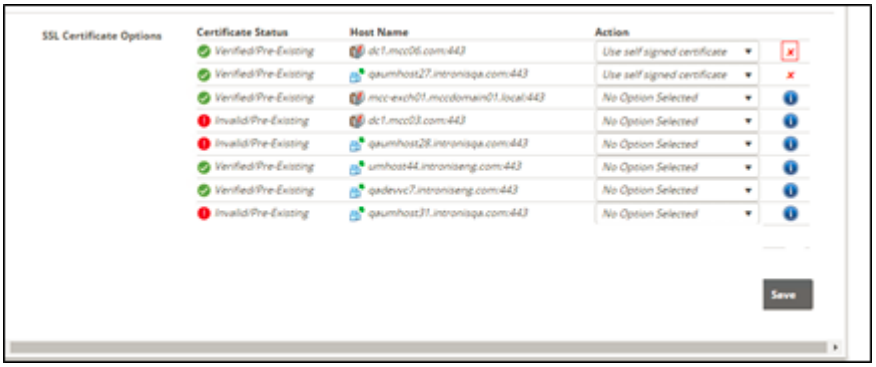
Clicking **Continue** allows you to remove the unsecured VMs from the backup.

Clicking **Cancel** allows you to add a certificate to the respective host/vCenter.

Deleting a Certificate

To delete a certificate, perform the following steps.

1. At the Software page, in the SSL Certificates section, click the **Delete** icon, as shown below.



The Delete confirmation popup is displayed.



2. Click **Yes**, and then click **Save**.

Figures

1. image2021-9-13 12:32:12.png
2. image2021-9-13 12:38:49.png
3. image2021-9-13 12:40:36.png
4. image2021-9-13 12:43:35.png
5. image2021-9-13 12:45:44.png
6. image2021-9-13 12:46:52.png
7. image2021-9-13 12:48:27.png
8. image2021-9-13 12:49:31.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.