

## Self-signed Certificates

https://campus.barracuda.com/doc/16649/

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,

	different of the second of the	nt on the local computer will behave.	ete mataner		
Temporary Folder	Path: C/Windows/ITEMPIBackupAgent				
Local Vault	Local Vault Disabled Sync the Local Vault folder with the remote servers. Any data backed up to the remote servers while the Local Vault is unavailable will be downloaded to the Local Vault in the background once it is made available.				
	The Local Vault is where local	copies and local-only data are saved.			
Bandwidth Throttling	Do not limit bandwidth use	pe			
Upload Logs	Automatically upload logs f	or online viewing			
	Upload warning and error log entries to enable online viewing.				
	Upiced warning and error log	entries to enable online viewing.			
SSL Certificate Options	Upload warning and error log	entries to enable online viewing. Host Name	Action		
SSL Certificate Options	Upload warning and error log Certificate Status Ø Venified/Pre-Existing	entries to enable online viewing. Host Name Ø dx 1.mcc06.com-443	Action Use self signed certificate ==		
55L Certificate Options	Uplicad warning and error log Certificate Status Venified Pire-Existing	entries to enable online viewing. Host Name Ø dr.Lmoc05.com:443 Ø dr.Lmoc03.com:443	Action Use self signed certificate == Ignore SS, certificate errors ==		
SSL Certificate Options	Upload warning and error log Certificate Status Verified Pre-Existing (gnored Pre-Existing Verified Pre-Existing	entries to enable online viewing, Host Name @ dr.L.mcc08.com.443 @ dr.L.mcc03.com.443 @ quurnhos(27.intronisga.com.443	Action Use self signed certificate = = (gnore SS, certificate errors = Use self signed certificate = =		
SSL Certificate Options	Upibed warning and error log Certificate Status Venified Pre-Existing Venified Pre-Existing Venified Pre-Existing Venified Pre-Existing	entries to enable online viewing, Host Name Ø dct.moct03.com.443 Ø dct.moct03.com.443 Ø dct.moct03.com.443 Ø moc-exch01.mocdomair01.locab.443	Action Use self signed certificate v Ignore SSR certificate errors v Use self signed certificate v Nio Option Selected v		
SSL Certificate Options	Upload warning and error log Certificate Status © Verified One-Existing d (proced-One-Existing © Verified One-Existing © Verified One-Existing © Invalid One-Existing	entries ta enable priline viewing. Hest Name Ø dr.1 moctól.com/443 Ø dr.1.moctól.com/443 Ø aurrhost27.mronisqu.com/443 Ø moc.esth01.mocdoman/01.local/443 Ø aurrhost28.inrondoma.com/443	Action           Use self signed certificate         *           Ignore SSE certificate errors         *           Use self signed certificate         *           Nio Option Selected         *		
SSL Certificate Options	Uplead warning and error log Certificate Status Stronged Stre-Existing Algonored Stre-Existing Stronged Stre-Existing Envelopme-Existing Stronged Stre-Existing Stronged Stre-Existing	entries to enable online viewing. Hest Name Ø dct.mcc0d.com/443 Ø dct.mcc03.com/443 Ø aumhost27.mcc0main01.local/443 Ø mcc=exch01.mcc0omain01.local/443 Ø aumhost28.intronsaga.com/443 Ø aumhost28.intronsaga.com/443	Action         v           Une self signed certificate         v           Ignore SSL certificate errors         v           Une self signed certificate         v           Nio Option Selected         v           Nio Option Selected         v		
SSL Certificate Options	Upload warning and error log Certificate Status Verified/Pre-Existing Verified/Pre-Existing Verified/Pre-Existing Verified/Pre-Existing Verified/Pre-Existing Verified/Pre-Existing Verified/Pre-Existing	entries to enable online viewing. Host Name Ø dr.t.mcc08.com/443 Ø dr.t.mcc03.com/443 Ø dr.t.mcc03.com/443 Ø mor-excH01.mccobmain01.local/443 Ø avamhost28.intronisqu.com/443 Ø avamhost28.intronisqu.com/443 Ø avamhost28.intronisqu.com/443	Action         v           Use self signed certificate         v           Ignore SSL certificate errors         v           Use self signed certificate         v           Use self signed certificate         v           Nio Option Selected         v           Nio Option Selected         v           Nio Option Selected         v		

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.

SSL Certificate Options	Certificate Status	Host Name	Action		
	Verified/Pre-Existing	💕 dc1.mcc06.com/443	Use self signed certificate		*
	O Verified/Pre-Existing	👩 geumhost27.intronisge.com:443	Use self signed certificate	•	*
	S Verified/Pre-Existing	💕 mcc-exch01.mccdomain01.local:443	No Option Selected		0
	Invalid/Pre-Existing	💕 dc1.mcc03.comv443	No Option Selected		0
	Invalid/Pre-Existing	💣 qaumhost28.intronisqa.com:443	No Option Selected		0
	O Verified/Pre-Existing	💣 umhost44.introniseng.com:443	No Option Selected	٠	0
	O Verified/Pre-Existing	andervc7.intraniaeng.comv443	No Option Selected		0
	Invalid/Pre-Existing	asumhost.31.intronisiga.com:443	No Option Selected		0
	Server Down	testerven443	No Option Selected		×
	Add				
	Add				1.

The Host prompt is displayed.

Choose the name of the host for which you are adding certificate options			
	Cancel	ОК	

- 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.

SSL Certificate Options	Certificate Status	Host Name	Action		
	Verified/Pre-Existing	💕 dc1.mcc06.comv443	Use self signed certificate	٠	
	Verified/Pre-Existing	👩 gaumhost27.intronisga.com/443	Use self signed certificate	•	*
	S Verified/Pre-Existing	💕 mcc-exch01.mccdomain01.local:443	No Option Selected	٠	0
	Invalid/Pre-Existing	💕 dc1.mcc03.comv443	No Option Selected	٠	0
	Invalid/Pre-Existing	👩 gaumhost28.intronisga.com/443	No Option Selected	•	
	O Verified/Pre-Existing	💣 umhoss44.introniseng.com:443	No Option Selected	٠	
	O Verified/Pre-Existing	andevvc7.intronioeng.com/443	No Option Selected		
	Invalid/Pre-Existing	💣 gaumhost.)1.intronisga.com;443	No Option Selected		
	🔓 Server Down	testaerven443	No Uption Selected	•	,
	Add		No Option Selected		
			Use self signed certificate		
			Ignore SSL certificate errors		Ser

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.

# Barracuda Intronis Backup



f signed certificate   f signed certificate  f signed certificate	*
f signed certificate	*
ing Colormad	
•	0
ion Selected	0
	Save
	Ion Selected   ion Se

The Delete confirmation popup is displayed.

	No Yes	
Are you sure you want to delete the certificate for qaumhost28.in	tronisqa.com:443	

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

r



#### 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., 2025 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.