



Wildcard SSL Certificate Renewal Process

Virtual Desktop Service

Toby vanRoojen
December 02, 2020

This PDF was generated from https://docs.netapp.com/us-en/virtual-desktop-service/Architectural.Wildcard_SSL_certificate_renewal_process.html on December 10, 2020. Always check docs.netapp.com for the latest.



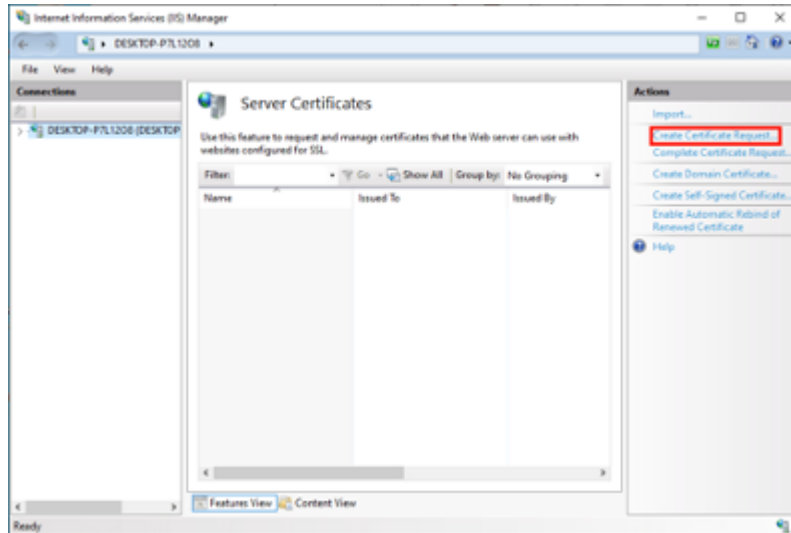
Table of Contents

- Wildcard SSL Certificate Renewal Process 1
 - Create a certificate signing request (CSR): 1
 - Installing and configuring CSR: 3
 - Assigning SSL certificate: 4

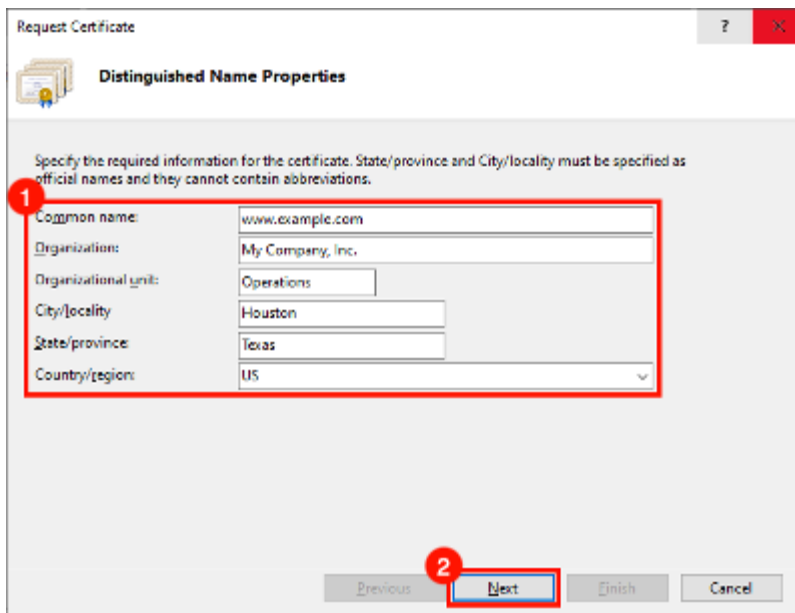
Wildcard SSL Certificate Renewal Process

Create a certificate signing request (CSR):

1. Connect to CWMGR1
2. Open IIS Manager from Administrator Tools
3. Select CWMGR1 and open Server Certificates
4. Click on Create Certificate Request in the Actions pane



5. Fill out the Distinguished Name Properties in the Request Certificate Wizard and click Next:
 - a. Common Name: FQDN of Wildcard - *.domain.com
 - b. Organization: Your company's legally registered name
 - c. Organizational unit: 'IT' works fine
 - d. City: City where company is located
 - e. State: State where company is located
 - f. Country: Country where company is located



The dialog box is titled "Request Certificate" and "Distinguished Name Properties". It contains a text box for "Common name" with the value "www.example.com", a text box for "Organization" with the value "My Company, Inc.", a text box for "Organizational unit" with the value "Operations", a text box for "City/locality" with the value "Houston", a text box for "State/province" with the value "Texas", and a dropdown menu for "Country/region" with the value "US". A red box highlights the entire form area, and a red circle with the number 1 is next to the "Common name" field. At the bottom, there are buttons for "Previous", "Next", "Finish", and "Cancel". A red box highlights the "Next" button, and a red circle with the number 2 is next to it.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

1

Common name: www.example.com

Organization: My Company, Inc.

Organizational unit: Operations

City/locality: Houston

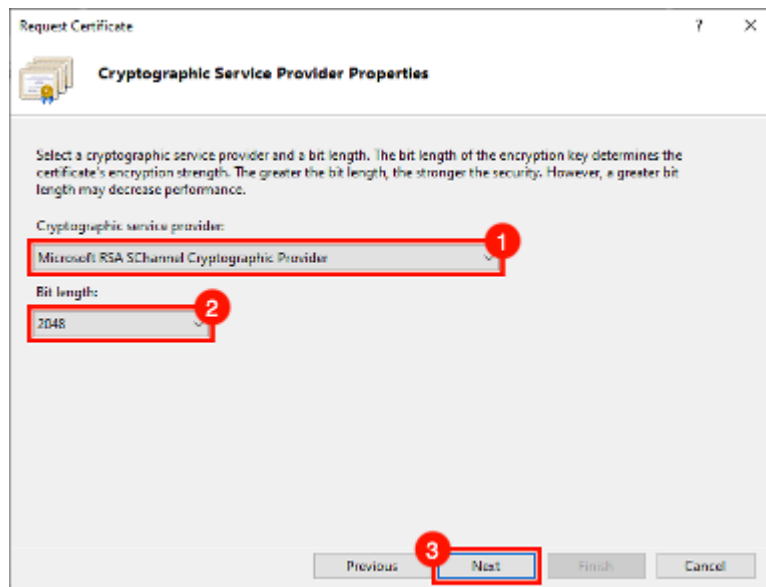
State/province: Texas

Country/region: US

2

Previous Next Finish Cancel

6. On the Cryptographic Service Provider Properties page, verify the below appears and click Next:



The dialog box is titled "Request Certificate" and "Cryptographic Service Provider Properties". It contains a text box for "Cryptographic service provider" with the value "Microsoft RSA SChannel Cryptographic Provider", and a dropdown menu for "Bit length" with the value "2048". A red box highlights the "Cryptographic service provider" field, and a red circle with the number 1 is next to it. Another red box highlights the "Bit length" dropdown, and a red circle with the number 2 is next to it. At the bottom, there are buttons for "Previous", "Next", "Finish", and "Cancel". A red box highlights the "Next" button, and a red circle with the number 3 is next to it.

Request Certificate

Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

1

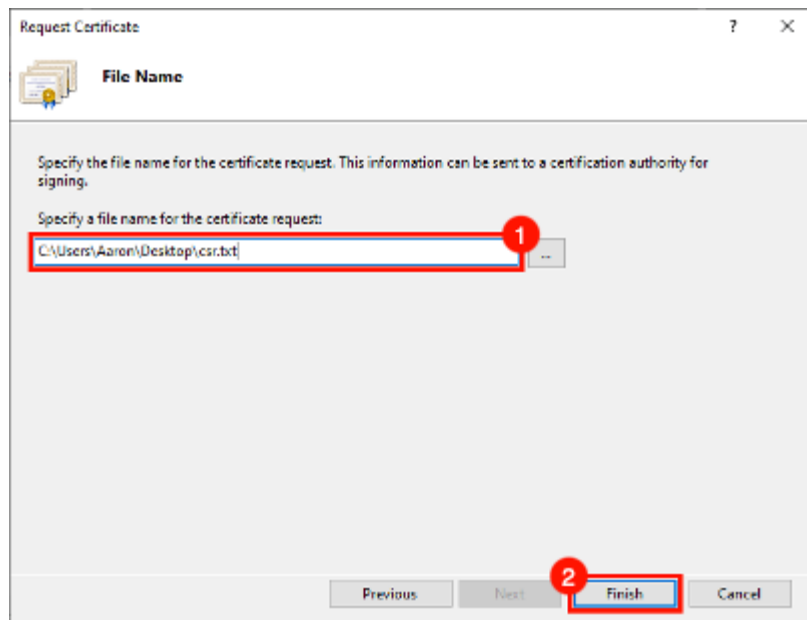
Bit length: 2048

2

3

Previous Next Finish Cancel

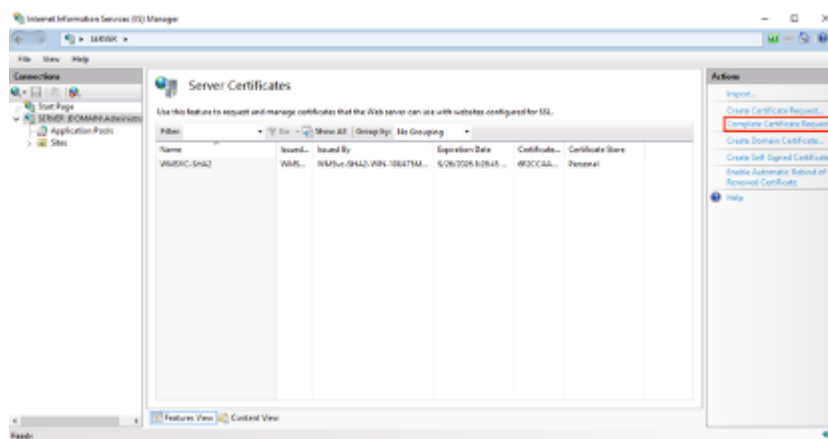
7. Specify a file name and browse to a location where you want to save the CSR. If you do not specify a location, the CSR will be in C:\Windows\System32:



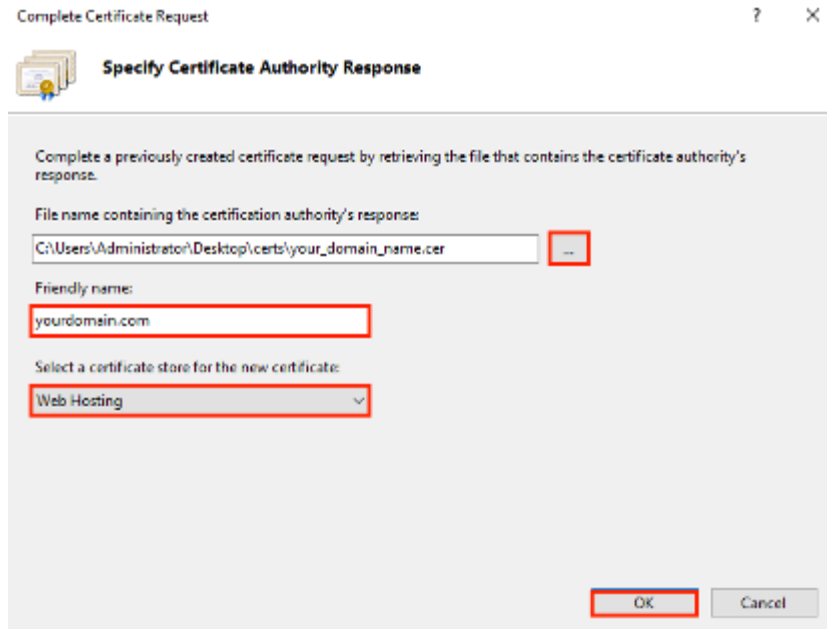
8. Click Finish when completed. You will use this text file to submit your order to certificate registrar
9. Reach out to registrar support to purchase a new Wildcard SSL for your certificate: *.domain.com
10. After receiving your SSL certificate, save the SSL certificate .cer file in a location on CWMGR1 and follow the below steps.

Installing and configuring CSR:

1. Connect to CWMGR1
2. Open IIS Manager from Administrator Tools
3. Select CWMGR1 and open 'Server Certificates'
4. Click on Complete Certificate Request in the Actions pane



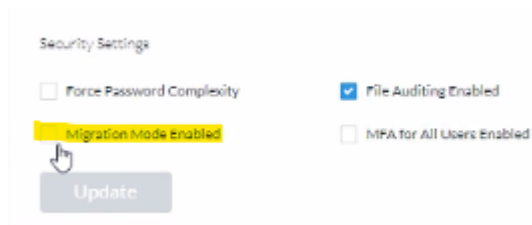
5. Complete the below fields in the Complete Certificate Request and click OK:



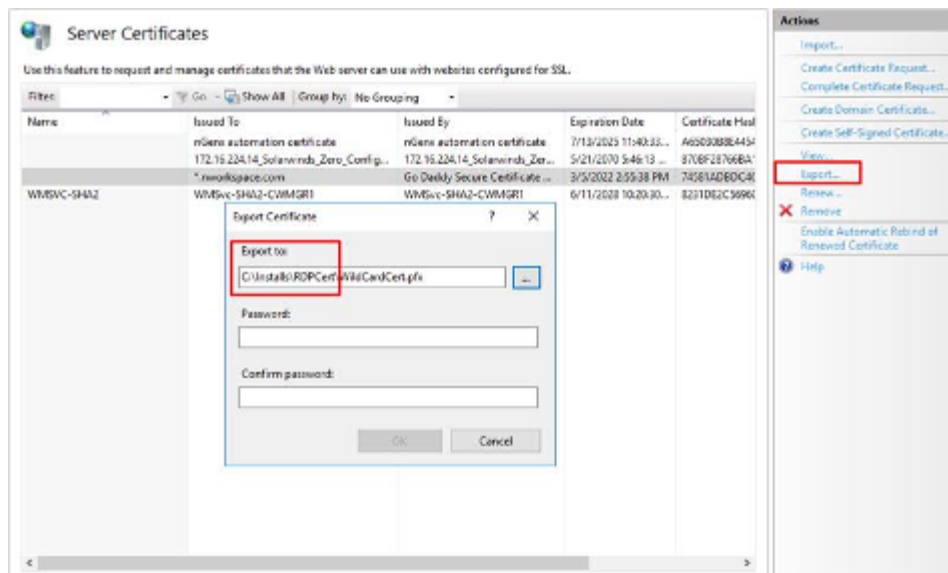
- a. File Name: Select .cer file that was saved previously
- b. Friendly name: *.domain.com
- c. Certificate store: Select either Web Hosting or Personal

Assigning SSL certificate:

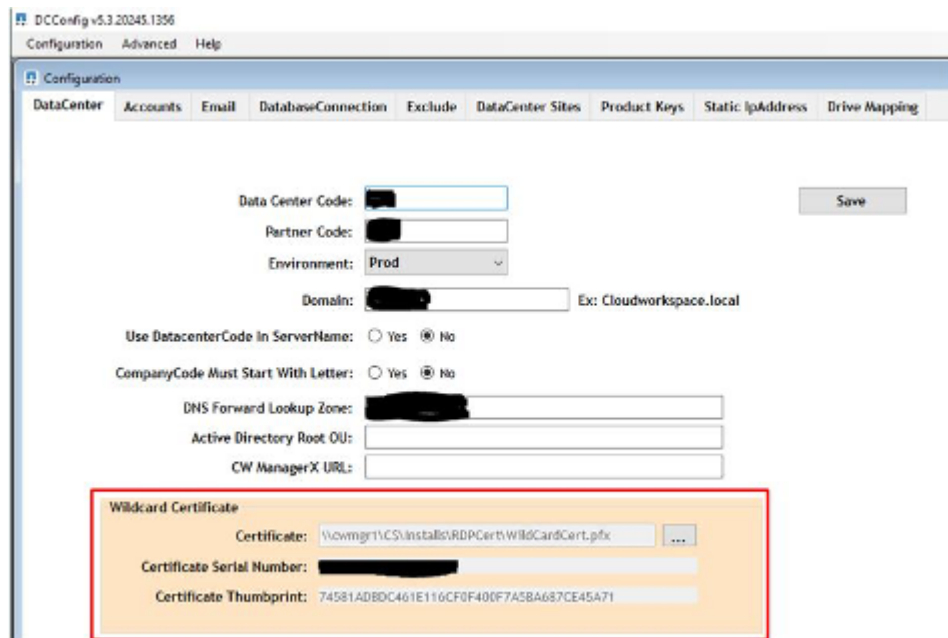
1. Verify that Migration Mode is not enabled. This can be found on the Workspace Overview page under Security Settings in VDS.



2. Connect to CWMGR1
3. Open IIS Manager from Administrator Tools
4. Select CWMGR1 and open 'Server Certificates'
5. Click on Export in the Actions pane
6. Export the certificate in .pfx format
7. Create a password. Store password as it will be needed to import or re-use .pfx file in the future
8. Save .pfx file to the C:\installs\RDPcert directory
9. Click OK and close IIS Manager

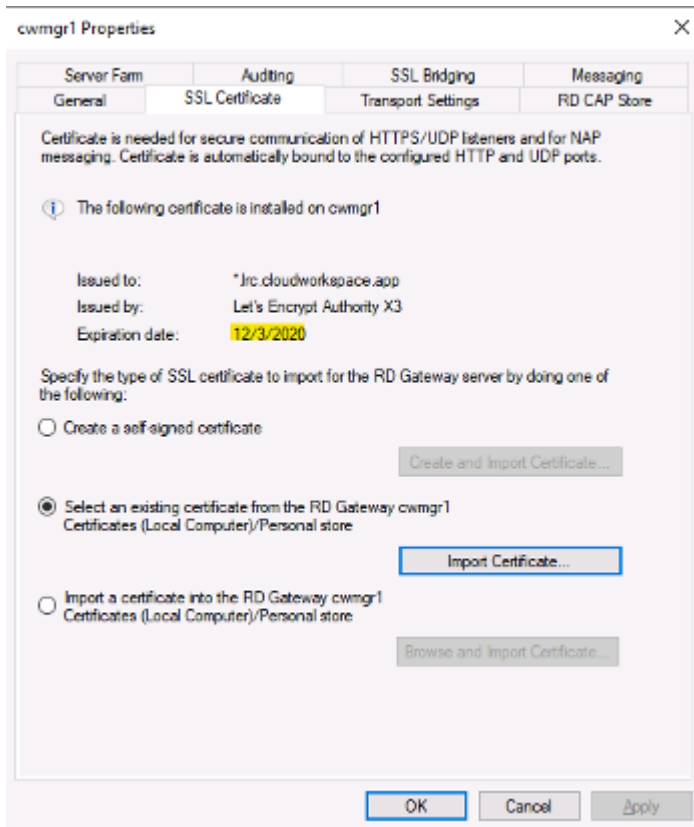


10. Open DCConfig
11. Under Wildcard Certificate, update the Certificate path to new .pfx file
12. Enter .pfx password when prompted
13. Click Save



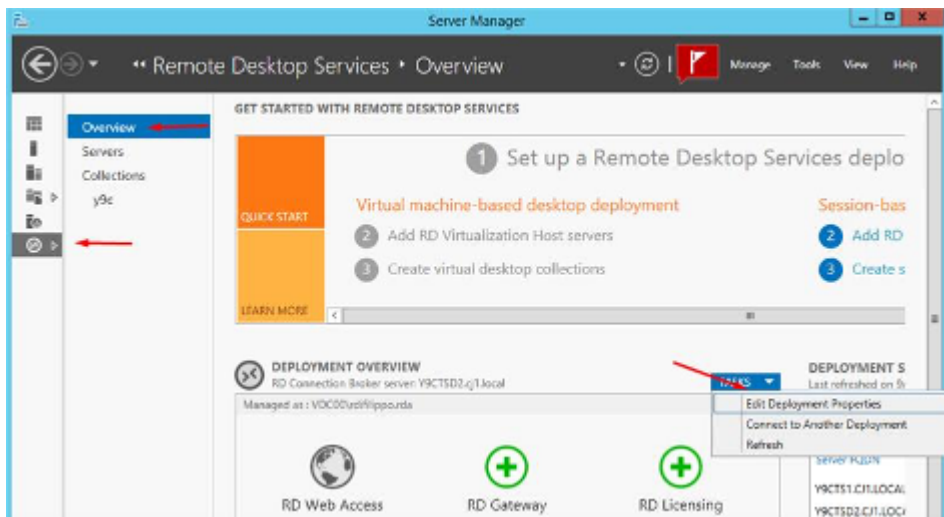
14. If the certificate is valid for 30 more days, allow automation to apply the new certificate during the morning Daily Actions task throughout the week
15. Periodically check the Platform servers to verify that the new certificate has propagated. Validate and test user connectivity to confirm.
 - a. On the server, go to Admin Tools
 - b. Select Remote Desktop Services > Remote Desktop Gateway Manager

- c. Right click on gateway server name, select Properties. Click on the SSL Certificate tab to review expiration date

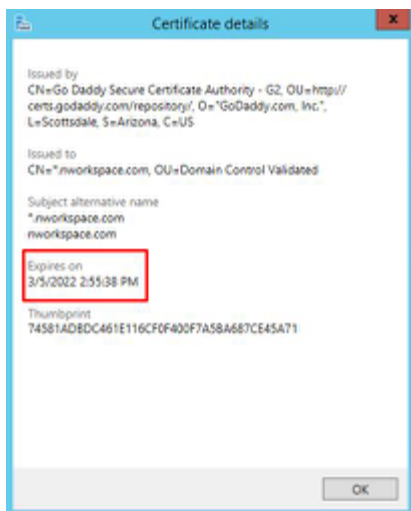
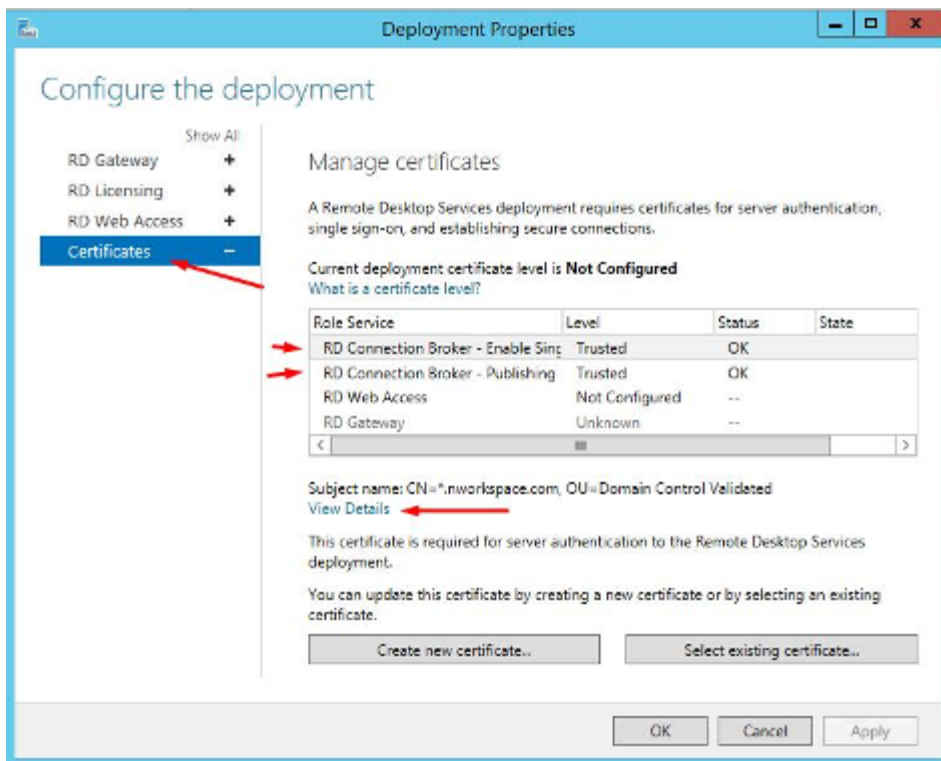


16. Periodically check the client VMs that are running the Connection Broker role

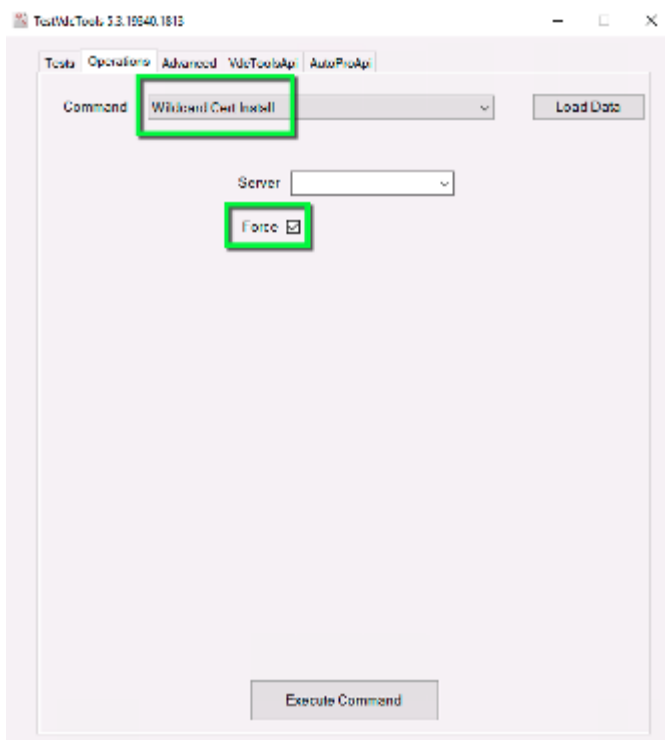
- a. Go to Server Manager > Remote Desktop Services
- b. Under Deployment Overview, select Tasks dropdown and choose Edit Deployment Properties



- c. Click on Certificates, select certificate and click View Details. Expiration date will be listed.



17. If less than 30 days or you prefer to push out the new certificate immediately, force the update with TestVdcTools. This should be done during a maintenance window as connectivity for any users logged in and your connection to CWMGR1 will be lost.
 - a. Go to C:\Program Files\CloudWorkspace\TestVdcTools, click the Operations tab and select the Wildcard Cert-Install command
 - b. Leave the server field blank
 - c. Check the Force box
 - d. Click Execute Command
 - e. Verify certificate propagates using the steps listed above



Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.