Vulnerability Remediation Plugin Guide

Plugin V 1.0 Doc Rev. 0.139 April 17, 2014

Table of Contents

 © 2014 Venafi Proprietary and Confidential

INTRODUCTION

BACKGROUND

When enterprises discover new risks associated to certificates and private keys, security teams need to be able to detect, protect, and respond quickly and effectively.

PURPOSE

The Venafi TrustAuthority Vulnerability Remediation Plugin allows you to detect SSL certificates that may have been compromised as a result of the Heartbleed bug, weak signing algorithms, or low key strengths. In one bulk action customers can revoke and renew all compromised certificates and keys.

© 2014 Venafi Proprietary and Confidential

PRE-REQUISITES

SUPPORTED VERSIONS OF VENAFI TRUST PROTECTION PLATFORM

The Vulnerability Remediation Plugin requires one of the following versions of the Venafi Trust Protection Platform (formerly known as Venafi Encryption Director):

- 6.1.4
- 7.0.0
- 8.0.3
- 10.0.0
- 11.0.0
- 14.1.0

Although the Plugin may function properly on other versions of Venafi Trust Protection Platform, they have not been tested.

VENAFI UPDATER & SCREEN RESOLUTION

In order to install the Venafi Vulnerability Remediation Plugin, you must have a recent version of the Venafi Updater installed. Any version 2.0.6 and above is suitable for this Venafi Update Package.

The Plugin requires a minimum of 1280x1024 resolution on the screen.

REQUIRED RIGHTS

The Vulnerability Remediation Plugin is designed for Administrators of the Venafi Platform and requires the logged in user to have “Master Admin” rights assigned. Users with less rights may be able to run the Plugin, but they will likely receive errors during work processing. This is expected.

REQUIRED CONFIGURATION

In order for the Vulnerability Remediation Plugin to be able to bulk process the renewal of thousands of certificates at once, Venafi TrustAuthority SSL (formerly known as Venafi Certificate Manager) have the appropriate Certificate Authority Template (CA Template) objects configured and validated for use. Also, if the CA Template that you are using has required vendor specific fields, these fields must be able to be completed via policy so that certificates can be renewed in bulk. For information on configure CA Template objects, please view the section “Managing CA Templates” in the product documentation, available in your product’s help menu, or downloadable for registered customers at https://support.venafi.com/forums/20697646.

Depending upon your version of Venafi Trust Protection Platform, in order to revoke certificates in bulk, certificates must already be configured and linked to the appropriate CA Template object. Venafi TrustAuthority 11 and 14.1 will attempt to determine the appropriate CA Template object from the policy tree, even if the certificate is not explicitly linked to it.

 © 2014 Venafi Proprietary and Confidential

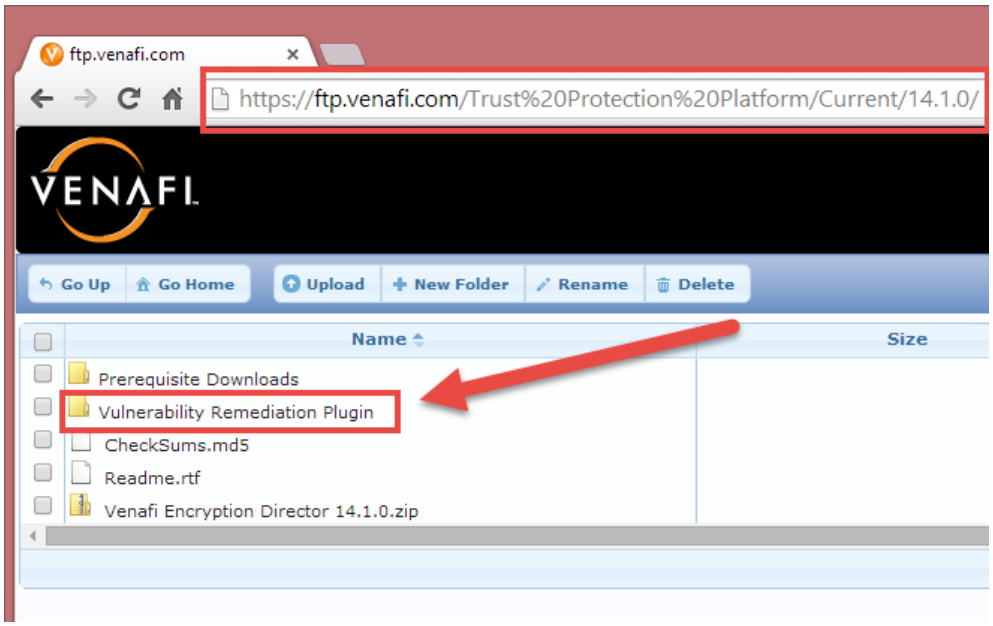
INSTALLATION

DOWNLOADING THE PLUGIN

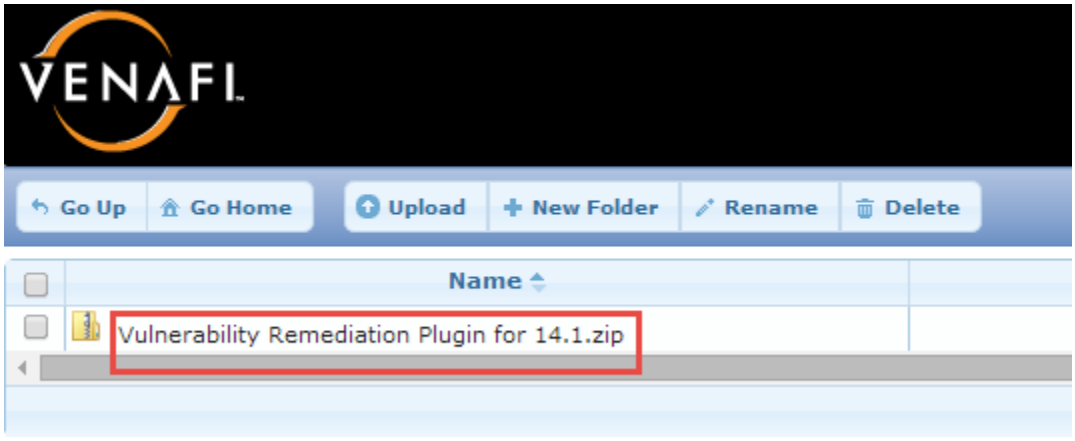
The Vulnerability Remediation Plugin is available to download to all Venafi customers with a current maintenance contract. In order to download, you need to have a valid FTP Account for https://ftp.venafi.com. If you are an authorized Venafi contact for your organization and require an FTP Account, please email support@venafi.com to request a FTP account.

Download Instructions:

1. On a computer with internet access, open a web browser type https://ftp.venafi.com in your address bar.
   (**Note**: depending upon your web browser the https may need to be typed in manually)
2. Locate the installation files for the version of Venafi Trust Protection Platform (formerly Venafi Encryption Director) where the plugin will be installed.
3. Locate the folder "Vulnerability Remediation Plugin" and click on the folder name



4. Click on the Zip file in the folder to start the download.
   Note: The name of the zip file may vary from the example in the screenshot below

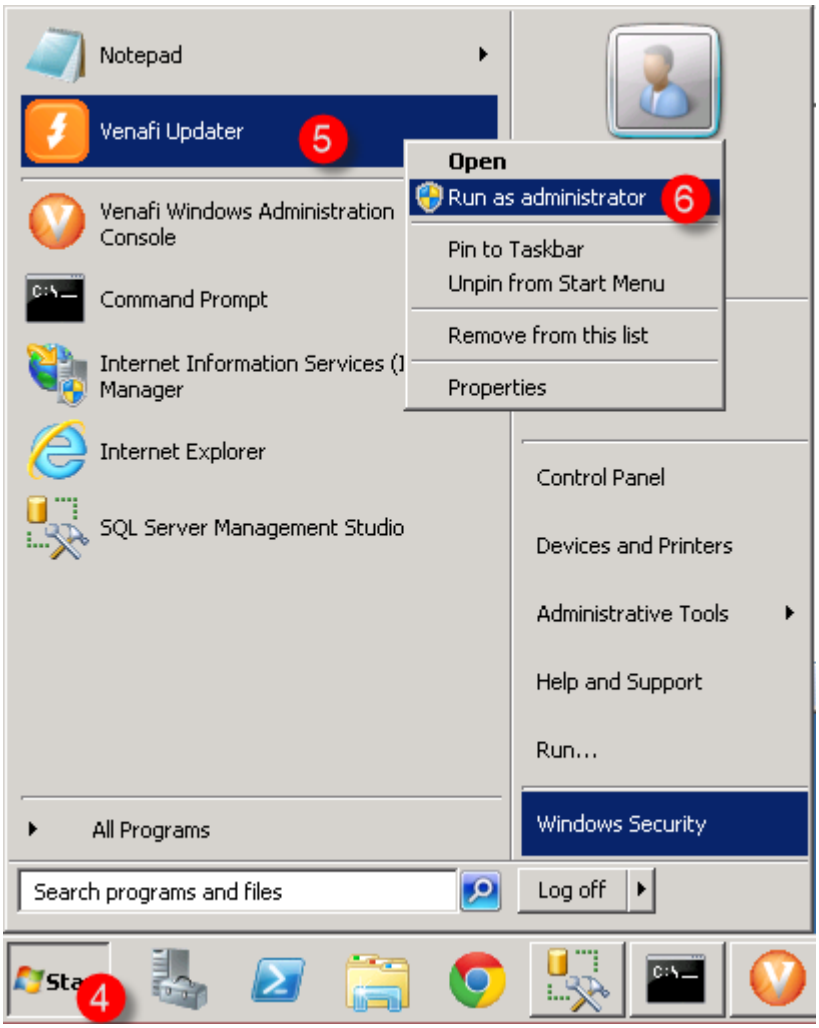


5. Save the downloaded file to the location where you keep other Venafi Update Packages

 © 2014 Venafi Proprietary and Confidential

INSTALLATION INSTRUCTIONS

1. Extract the contents of the *.zip file to the Venafi server on which you are installing the Plugin.
   Note: If your production environment has multiple Venafi servers, it is only necessary to install the Plugin on one server.
2. Locate the *.vupkg file from within the extracted file contents. This is the Venafi Update Package.
3. Copy the *.vupkg file to C:\Program Files\Venafi\Packages.
   Note: the location of "Venafi\Packages" may vary in your environment if you have installed the Venafi Trust Protection Platform to a custom location.
4. Click on the Start Menu.
5. Locate the "Venafi Updater" (formerly known as Director Updater).
6. Right click on Venafi Updater and "Run as administrator".

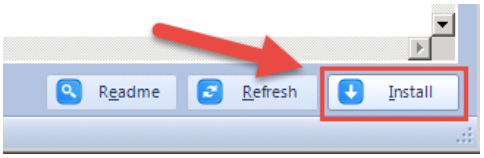


7. Make sure your Windows Administrator Console (Win Admin) is closed.
   Note: it is not necessary to stop IIS or other Venafi services to install this plugin – only WinAdmin.

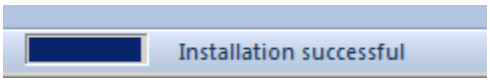
 © 2014 Venafi Proprietary and Confidential

8. Locate and highlight the Venafi Vulnerability Remediation Plugin from the list of installable updates.

9. Click the Install button to start the installation of the plugin. Installation should only take a few seconds.



10. When installation is completed, the status bar in the lower left hand corner will say "Installation successful".



11. Close Venafi Updater.

ACCESSING THE PLUGIN

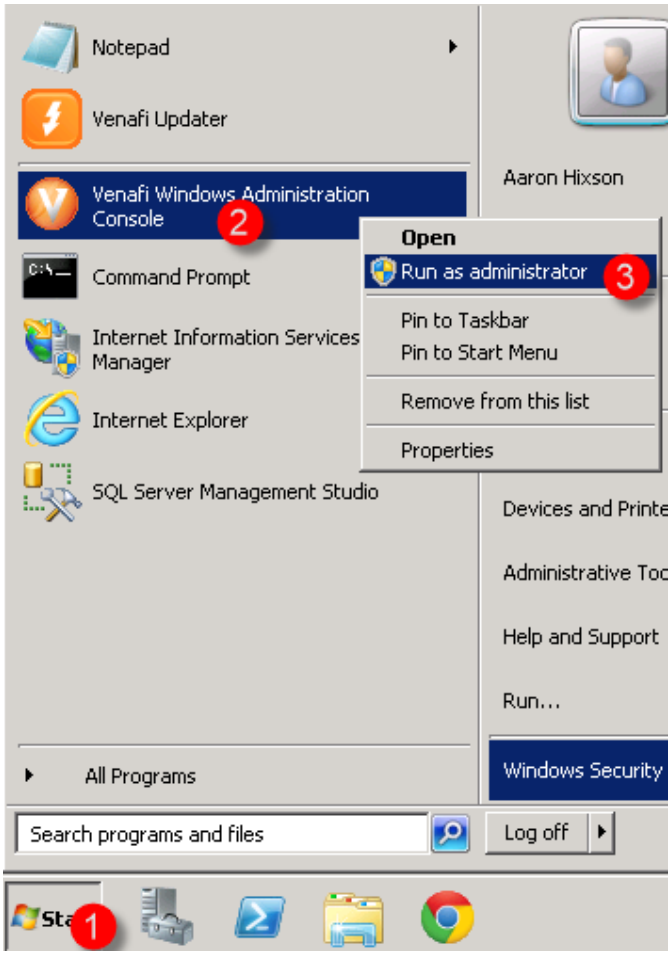
The Venafi Vulnerability Remediation Plugin is only available in the Windows Administration Console (WinAdmin). It is not available in the Web Administration Console (WebAdmin) or in Aperture.

The Plugin requires a minimum of 1280x1024 resolution on the screen. Please adjust your Remote Desktop session settings so that the remote window is in full screen.

1. Click on the Start Menu
2. Locate "Venafi Windows Administration Console"

© 2014 Venafi Proprietary and Confidential

3. Right click on “Venafi Windows Administration Console” and choose “Run as administrator”

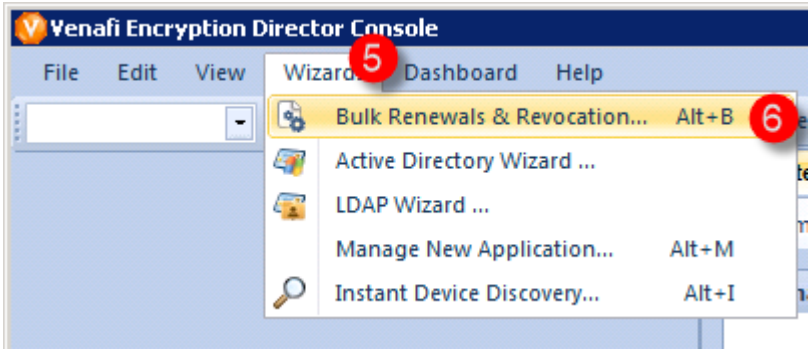


4. Login as a Master Admin with your username and password

5. Once the Windows Administration Console loads, click on the Wizards menu.

© 2014 Venafi Proprietary and Confidential

6. Click on the “Bulk Renewals & Revocation” item from the Wizards menu

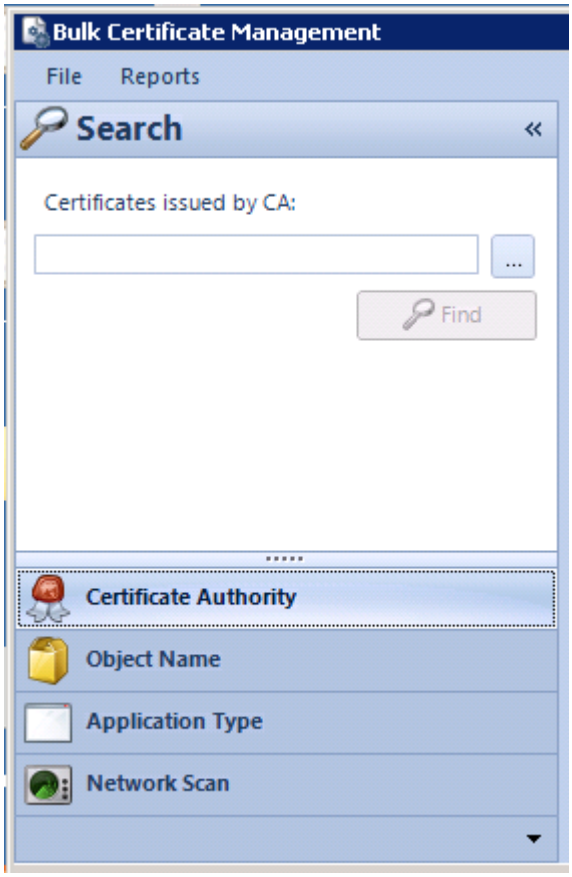


7. The Venafi Vulnerability Remediation Plugin will load. It is recommended that you maximize the Plugin window to take up the full remote session screen.

 © 2014 Venafi Proprietary and Confidential

SEARCHING FOR CERTIFICATES

The left panel of the Plugin is your search configuration panel. It allows you select from building your bulk renewal job in four different ways. You can build your job by searching via Certificate Authority, Object name, Application object type, or by a Network Scan.



Quick Tip: « For small resolution screens, you can collapse the Search panel to allow for more room for reviewing results.

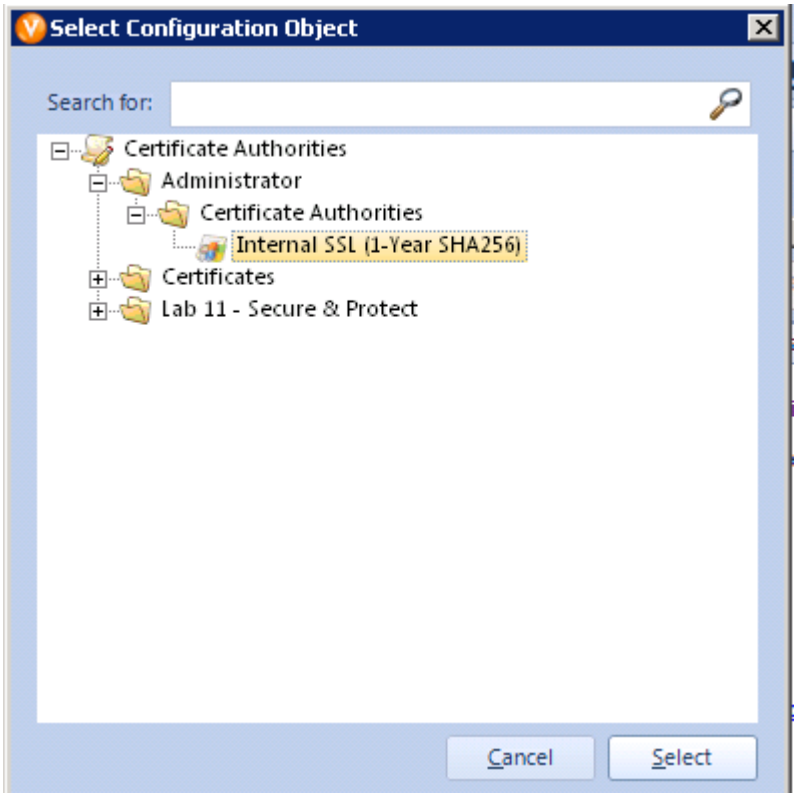
Making changes to search settings will clear your current results. As you perform searches for certificates, results will appear in the middle panel for you to review. Make sure you select your desired certificates from the Results (middle) panel and add them to your Work Queue (left) panel before making changes to your search settings.

CERTIFICATE AUTHORITY

The Certificate Authority search will allow you to locate certificates in your Policy tree by the CA template the certificate is associated with.

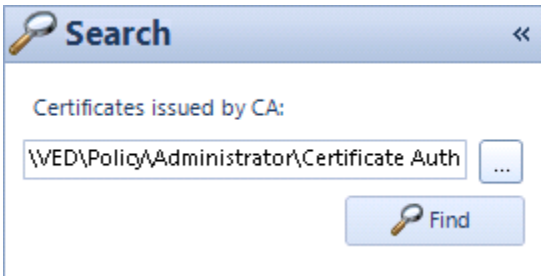
1. Click on the *ellipses* button (picture below)

2. Select the CA Template that you want to use for renewing certificates and click “Select”.



 © 2014 Venafi Proprietary and Confidential

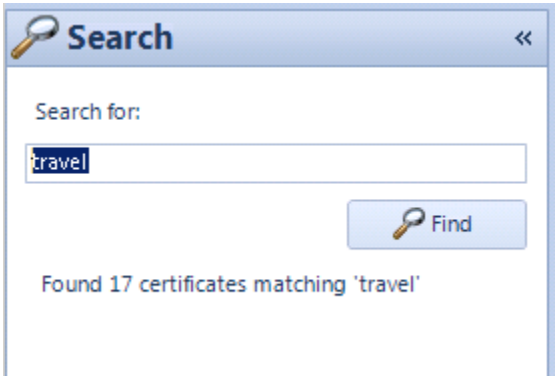
3. Click on the “Find” button to search the Policy tree for all certificates that are linked to the selected CA Template object



OBJECT NAME

Selecting “Object Name” gives you the ability to type in a name and search for certificates by certificate object name, device object name, or application object name.

1. Click on “Object Name”
2. Type in the name of the object you’d like to search for
3. Click the “Find” button



4. The total count of found certificates will appear below the search controls. Results will appear in the middle Results panel.

APPLICATION TYPE

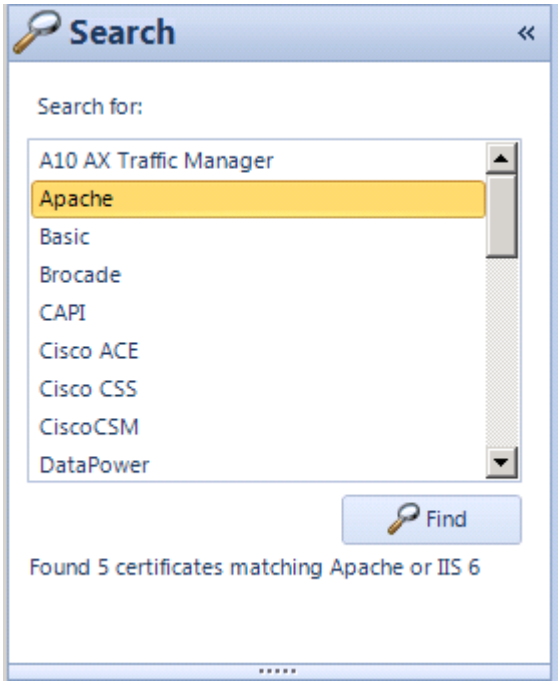
Selecting “Application Type” allows you to search for certificates in the policy tree by the type of associated application object.

1. Click on “Application Type”

2. Use the CTRL or SHIFT key to select multiple application objects.
   Quick Tip: Click the top application object and use the SHIFT key to select the last application object to select all available options.

 © 2014 Venafi Proprietary and Confidential

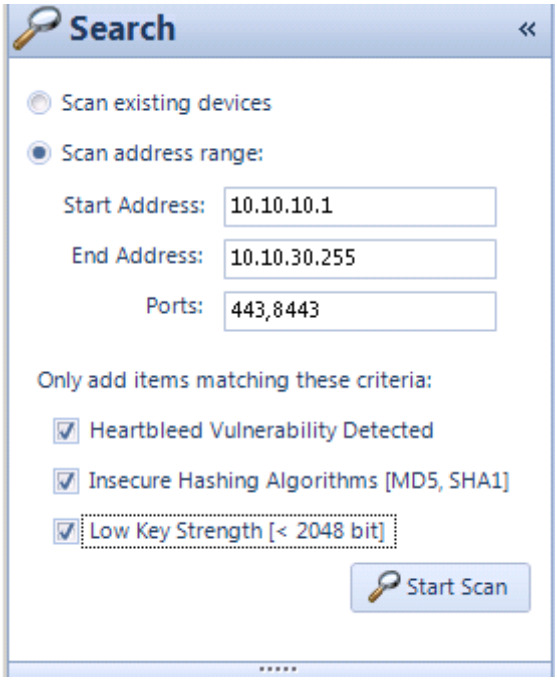
3. Click the “Find” button



4. The total count of found certificates will appear below the search controls. Results will appear in the middle Results panel.
   Note: If certificates are associated to multiple application objects (one-to-many) than the certificates may be counted more than once. The list of unique certificates, however will appear in the middle Results pane.

NETWORK SCAN

The Venafi Vulnerability Remediation Plugin has the ability to scan the network for Heartbleed vulnerabilities, insecure hashing algorithms, and low key strengths to discover where security vulnerabilities may lie both in your internal and public networks.



Scan Existing Devices

Choosing “Scan existing devices” will utilize the host address on application objects and network validation settings on application and certificate objects to provide a list of IP Addresses and ports to scan to detect vulnerable private keys and certificates.

Note: Certificate objects that have network validation settings to “Use Subject Common Name” will not be included in the discovery job when “Scan existing devices” is selected.

 © 2014 Venafi Proprietary and Confidential

Scan Address Range

If you select “Scan address range” you can provide one IP address as well as list the ports to scan.

Note: Ports need to be in a comma separated format. Separating ports by semicolons will not work.

Vulnerability Criteria

Heartbleed vulnerability: This will detect servers that have not been patched and still have an affected version of OpenSSL providing TLS sessions.

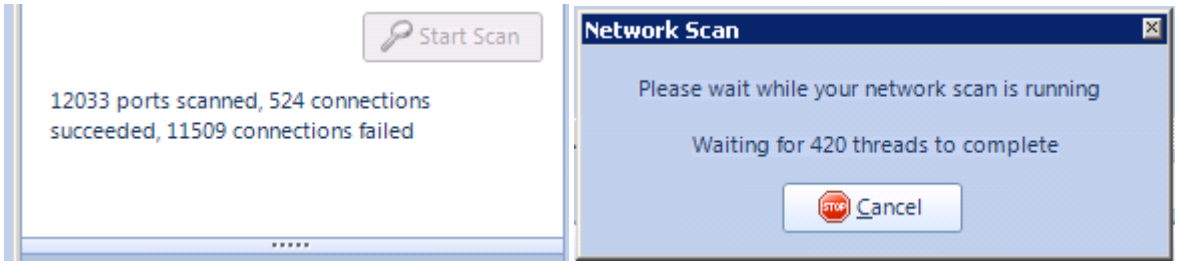
Insecure Hashing Algorithms: This will detect certificates that are using SHA1 or MD5 as their signing algorithm.

Low Key Strength: This will find certificates that have a private key less than 2048-bits

If none of these three vulnerabilities are checked, then the middle Results panel will be populated with any certificate found during the network scan.

Running the Scan

While the scan is running, there is a detailed status of its progress.



Scan Report

Network Scan results can be exported so that vulnerable servers can be patched prior to rotating the certificate and private key. See the Reports section for more information on the Scan Report.

© 2014 Venafi Proprietary and Confidential

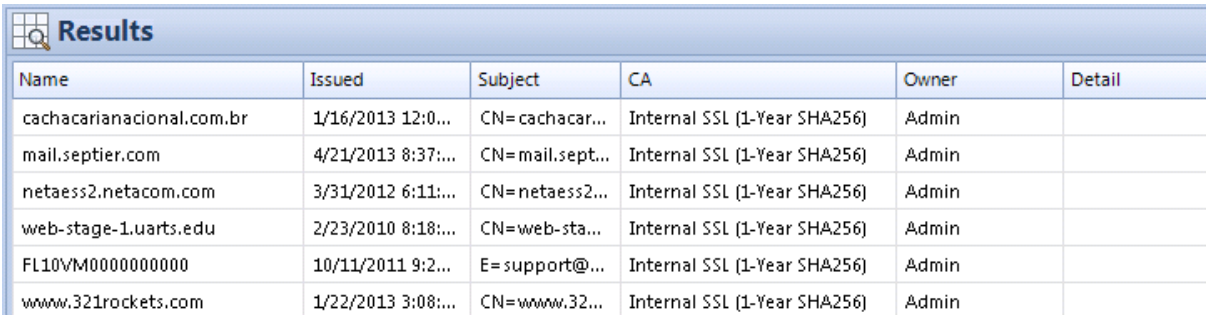
MANAGING CERTIFICATE RESULTS

REVIEWING RESULT DETAILS

The Results pane is the middle pane. It has two sections, a Results grid and a Details window.

The results grid has the following information:

- Name – the name of the Certificate object. This field is blank if the Plugin finds a certificate from a Network scan that isn't currently in the Policy Tree.
- Issued – Shows when the certificate was issued. Demonstrates that the certificate has been issued after the date of the vulnerability.
- Subject – Subject DN of the discovered certificate.
- CA – the associated Certificate Authority. Will be blank if the Certificate is not in the Policy Tree or if the certificate is not associated to a Certificate Authority.
- Owner –Name of the contact/owner for the certificate.
- Details – If a network scan detected a security problem, the most important issue is listed. Otherwise it will list the IP:port that where the certificate was found.

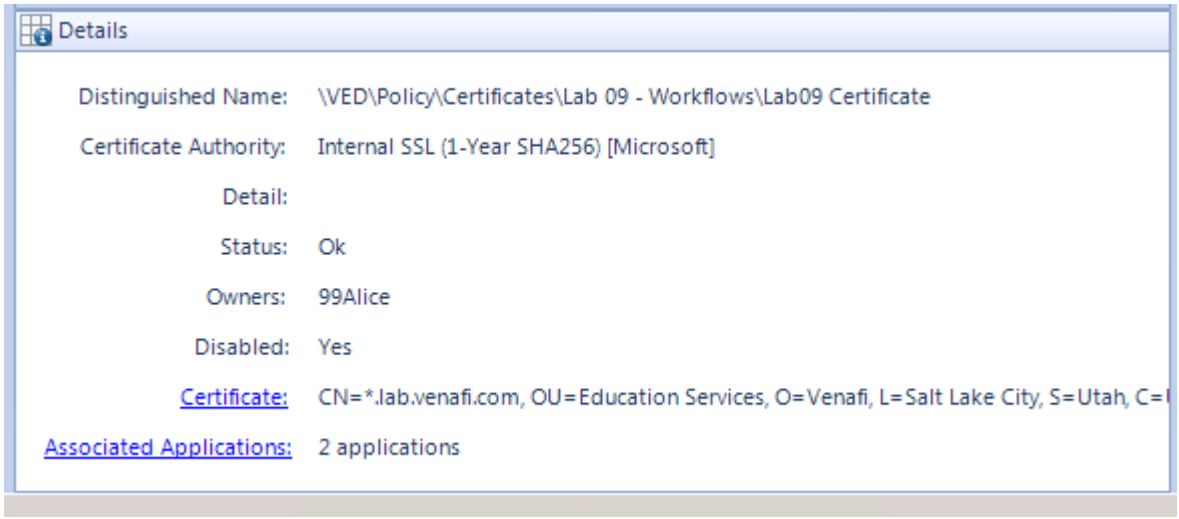


Name	Issued	Subject	CA	Owner	Detail
cachacarianacional.com.br	1/16/2013 12:0...	CN=cachacar...	Internal SSL (1-Year SHA256)	Admin	
mail.septier.com	4/21/2013 8:37:...	CN=mail.sept...	Internal SSL (1-Year SHA256)	Admin	
netaess2.netacom.com	3/31/2012 6:11:...	CN=netaess2...	Internal SSL (1-Year SHA256)	Admin	
web-stage-1.uarts.edu	2/23/2010 8:18:...	CN=web-sta...	Internal SSL (1-Year SHA256)	Admin	
FL10VM0000000000	10/11/2011 9:2...	E=support@...	Internal SSL (1-Year SHA256)	Admin	
www.321rockets.com	1/22/2013 3:08:...	CN=www.32...	Internal SSL (1-Year SHA256)	Admin	

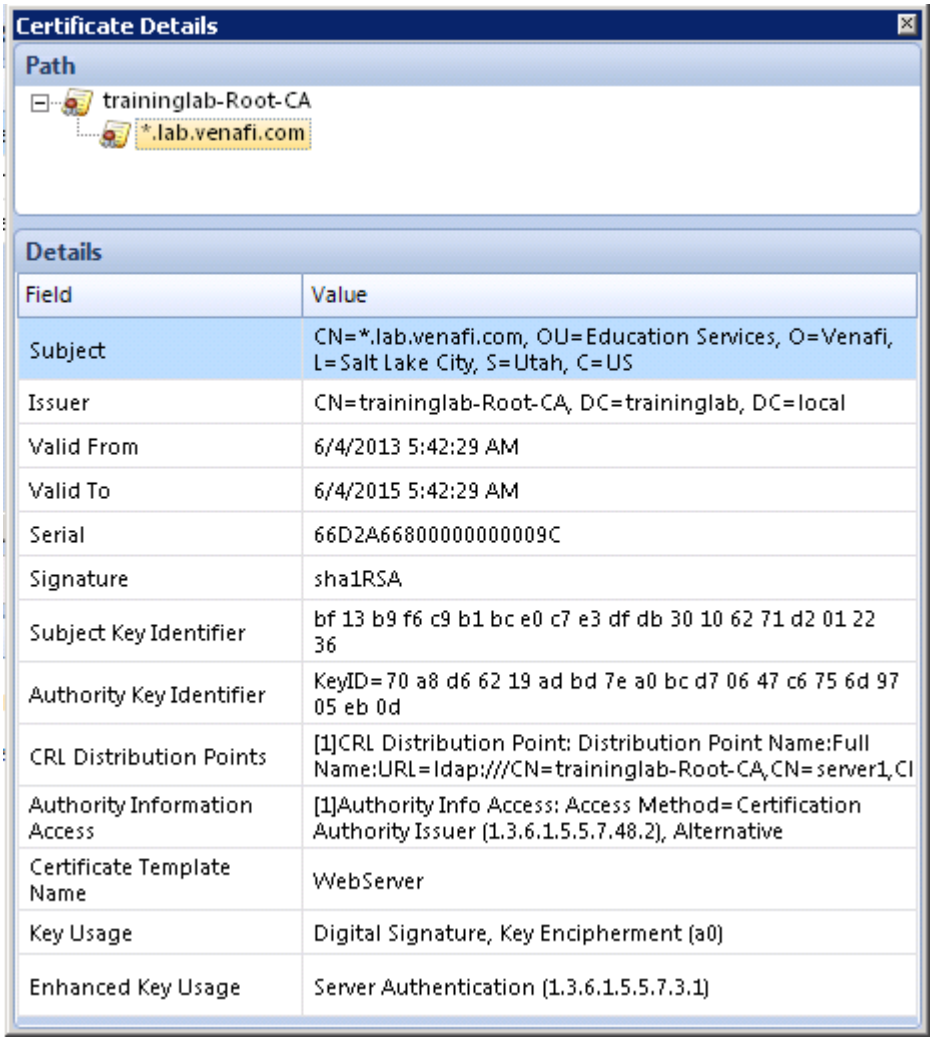
When an individual certificate is selected from the results grid, its details are populated in the Details window. The following information is available in the Details window:

- Distinguished Name – the full path of the certificate in the Policy Tree
- Certificate Authority – the CA template name and type of certificate authority object linked to the certificate
- Details – If a network scan detected a security problem, the most important issue is listed here. Otherwise it will list the IP:port where the certificate was found.
- Status – Current processing status of the certificate
- Owner – Name of the current contact/owner of the certificate
- Disabled – Whether the certificate object is currently disabled
- Certificate – the full Subject DN (Distinguished Name) of the certificate
- Associated Applications – Total number of applications associated to the certificate

 © 2014 Venafi Proprietary and Confidential

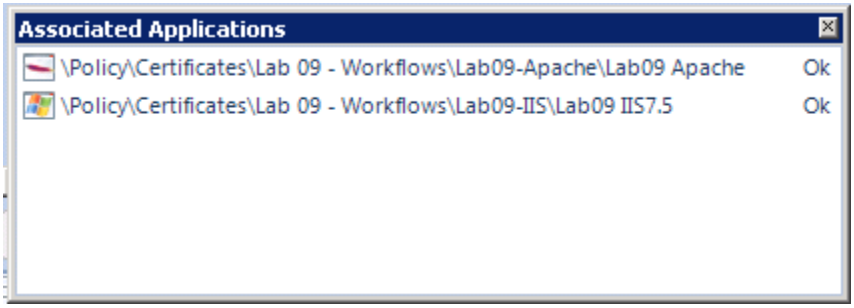


If you click on the “Certificate:” link then you will see a pop-up window with the full certificate details:



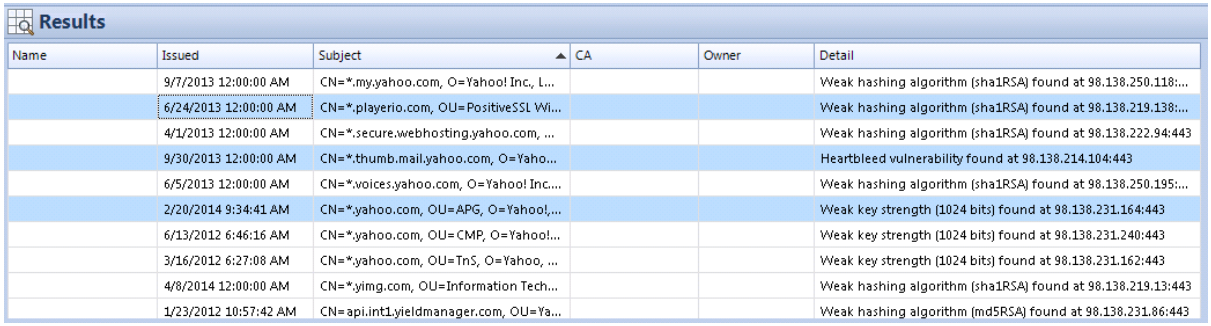
 © 2014 Venafi Proprietary and Confidential

If you click on the “Associated Applications:” link you will see a list of the Associated Applications and their corresponding status:

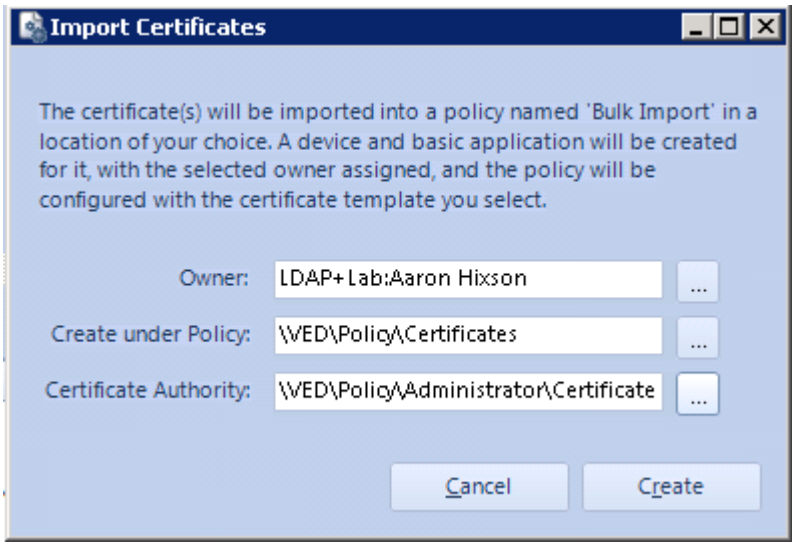


IMPORTING RESULTS INTO POLICY TREE FROM NETWORK SCAN

Certificate results cannot be added to the Work Queue unless the certificate exists in the policy tree. New certificates that are found during a network scan can be imported into the Policy Tree so that the certificates can be protected.



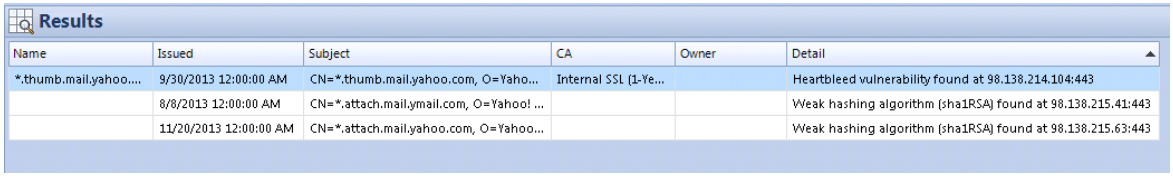
1. Select a certificate from the Results grid
2. Click the “Import” button
3. Select the Owner, Policy, and Certificate Authority template and click “Create”



Note: the certificates will be created in a “Batch Import” policy within the policy you selected.

 © 2014 Venafi Proprietary and Confidential

4. The results column will update with the new object name from the policy tree.



ADDING RESULTS TO THE WORK QUEUE

As you review results from various search types, you can select certificates individually or in groups to be added to the Work Queue. You can use CTRL + A to select all results from the Results grid.

Things to check for before adding to the Work Queue

Certificates in certain circumstances can get you into to trouble. Be sure to check your certificates before you add them to the Work Queue for bulk revocation/renewing

- Make sure the certificate is enabled
- Make sure the certificate is set to enrollment or provisioning
- Make sure the certificate has an associated Certificate Authority if you plan to revoke
- Make sure the certificate is not currently processing or in an error state
- Make sure your policies are configured so that TrustAuthority generates the private key and CSR
- If the Certificate Authority has required vendor specific fields, make sure the fields are completed via policy.

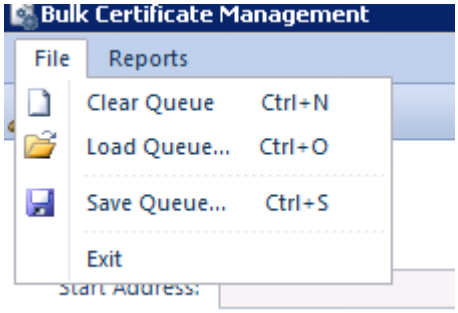
After you feel comfortable with the certificates in your results grid, select the certificates and click “Select” to add them to the Work Queue in the third (left) panel.

 © 2014 Venafi Proprietary and Confidential

THE WORK QUEUE

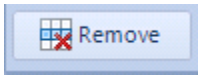
REVIEWING QUEUE DETAILS

Unlike the Results panel, the Work Queue panel is persistent and attempts to auto save your progress as you build your work queue. If you need to exit the Venafi Vulnerability Remediation Plugin, it is recommended that you save the queue so that you do not lose your work. Work queues can be cleared, saved, and loaded from the File menu.



REMOVING CERTIFICATES FROM THE QUEUE

If you decide you'd like to remove selected certificates from the Work Queue in the third (left) panel, you can highlight those certificates and click the "Remove" button.



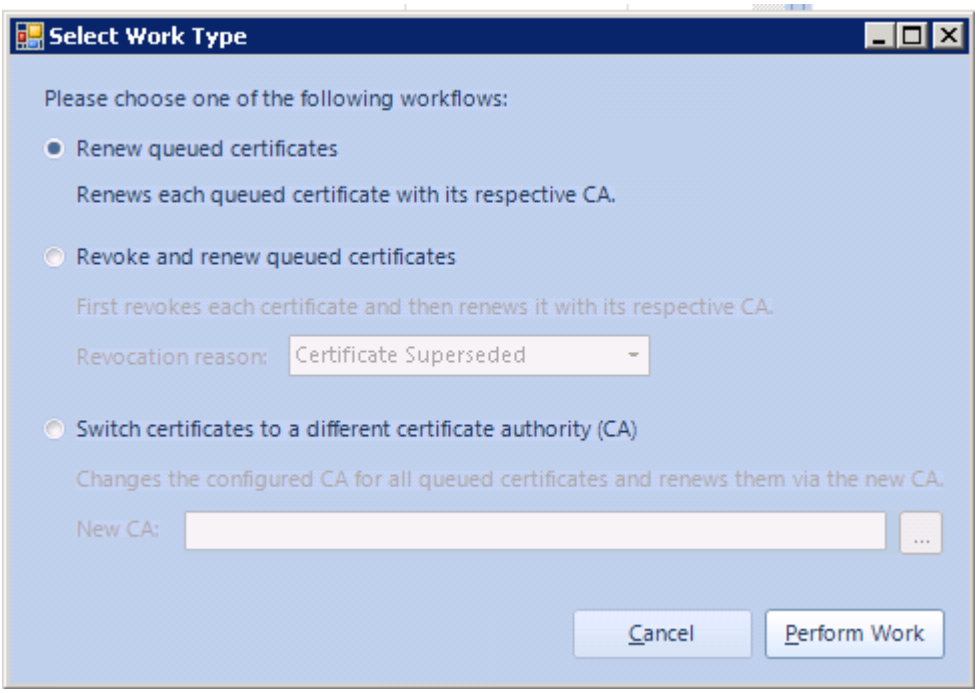
STARTING WORK

After you feel comfortable with the current Work Queue, click the "Start Work" button.

When you click "Start Work" the "Select Work Type" dialog appears asking what type of work you'd like to do:

- Renew queued certificates – This will renew each certificate in the Work Queue list with its respective Certificate Authorities
  Note: Certificates using the VeriSign VICE 2 certificate will automatically be renewed using the "Replace" enrollment mode.
- Revoke and renew queued certificates – First revokes each certificate and then renews it with its respective Certificate Authority.
- Switch certificates to a different certificate authority – Changes the configured CA template for all queued certificate and renews them via the new CA template object.

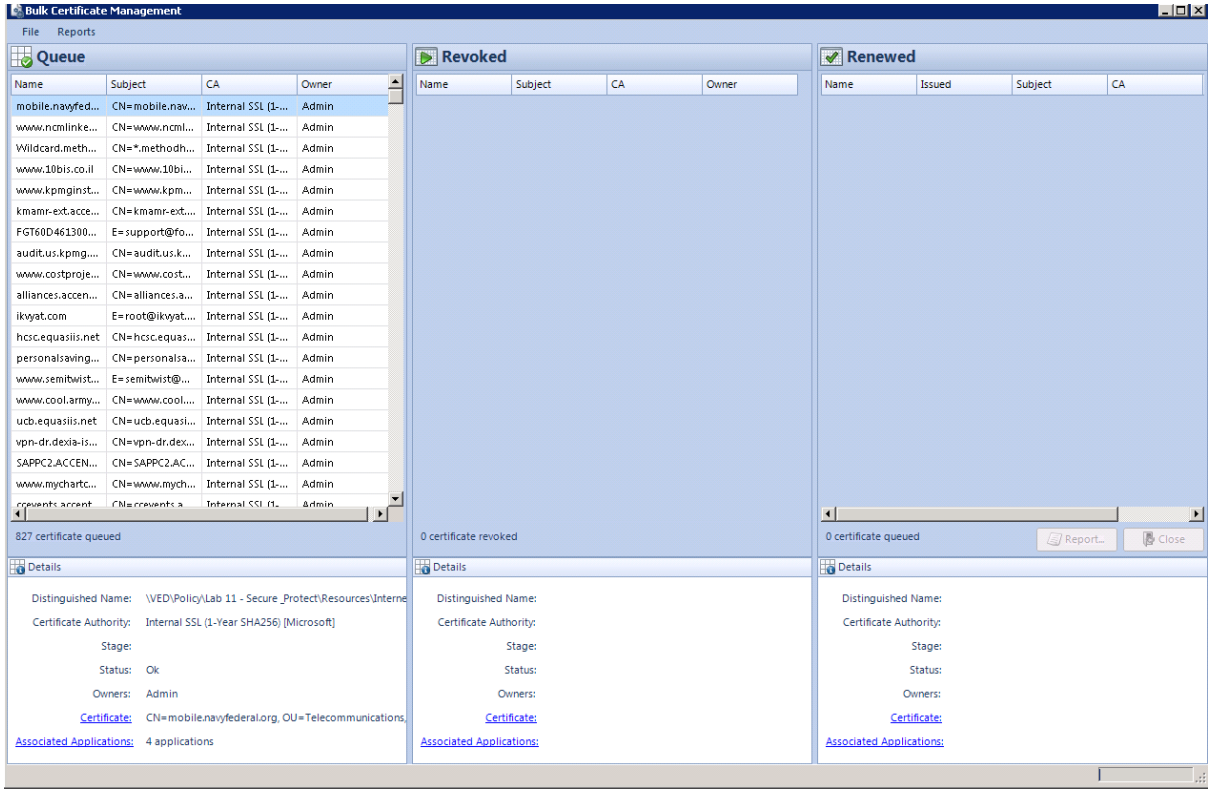
© 2014 Venafi Proprietary and Confidential



Click the “Perform Work” can you have completed your selection on the “Select Work Type” dialog. Clicking “Perform Work” will immediately queue up all renewals and revocations (if applicable) in bulk.

 © 2014 Venafi Proprietary and Confidential

THE PROCESSING WINDOW



INTRODUCTION

After the bulk work begins, the three windows are replaced with a new view called the processing window. This view shows you the progress of your certificates as they are revoked (if applicable) and renewed. The screen automatically refreshes as certificate work is done.

On this screen, you have the ability to click on the “Certificates” and “Associated Application” link to see further details for a highlighted certificate (similar to the information on the Results and Work Queue screen).

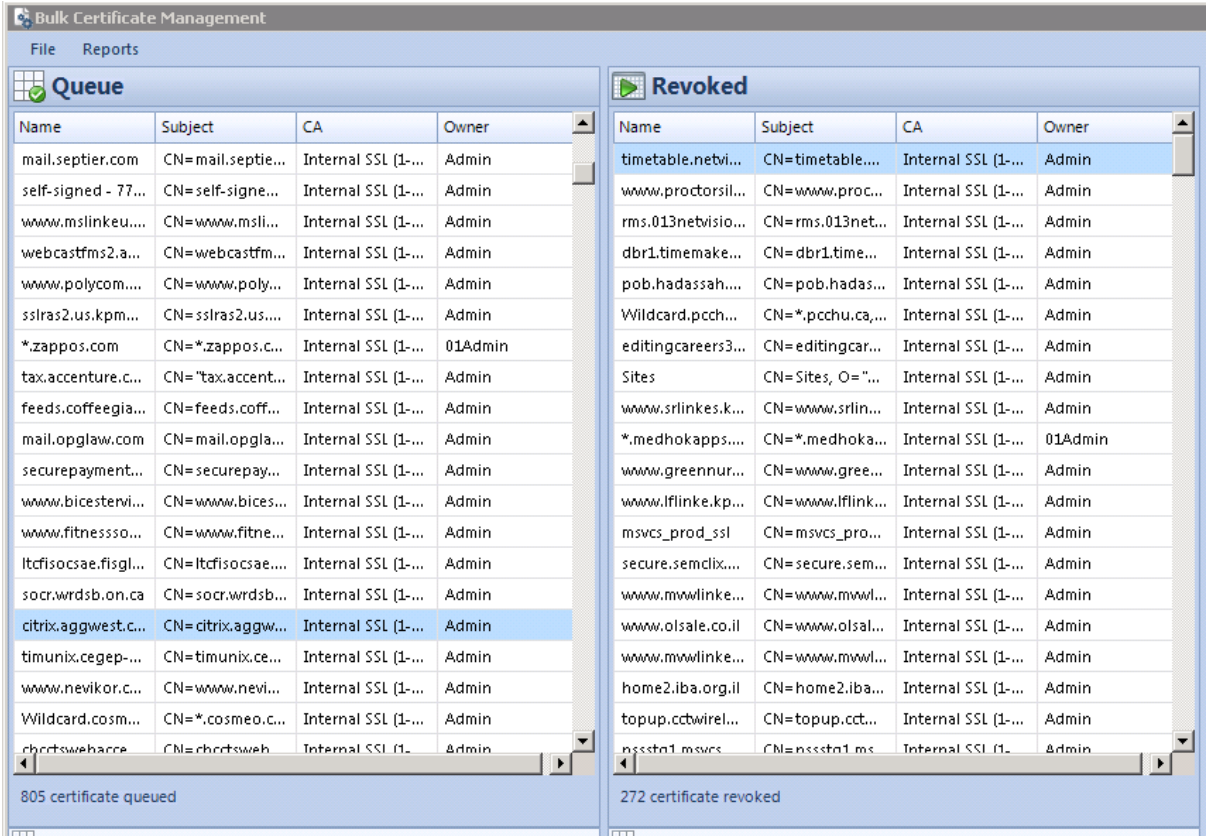
QUEUE

The queue pane on the left shows the work that needs to be done.

© 2014 Venafi Proprietary and Confidential

REVOKED

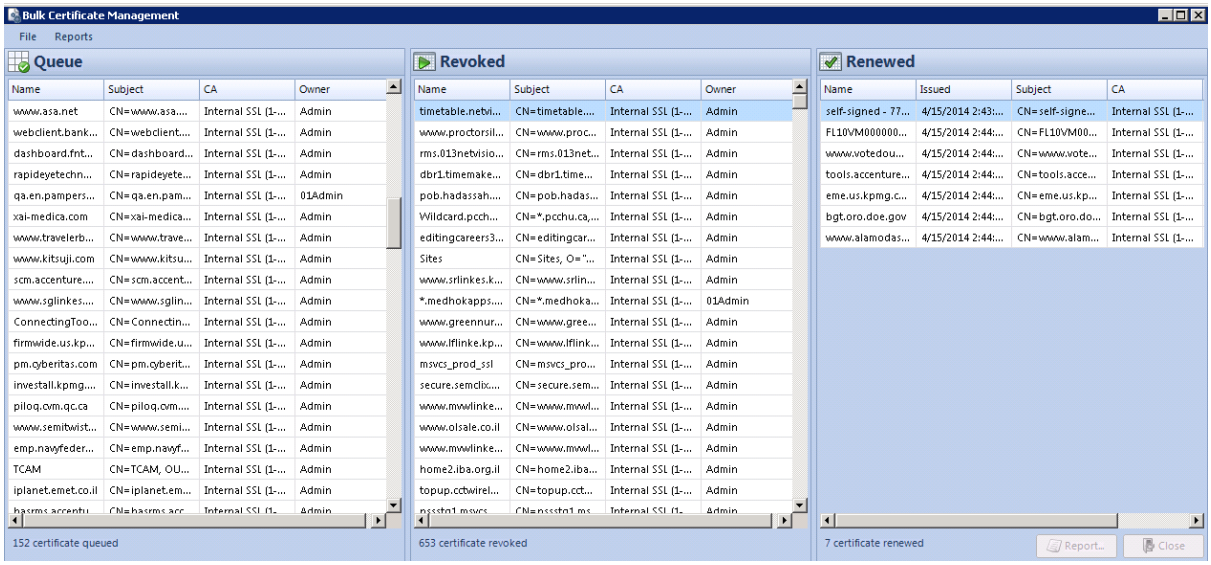
Certificates will show up in the Revoked pane after they have successfully been revoked and are waiting on being renewed



RENEWED

Certificates will show up in the Renewed pane after renewal is complete and all processing has been done.

Note: the “Done” button has an approximate 30-second delay after all work is complete before it can be selected.



 © 2014 Venafi Proprietary and Confidential

REPORTS

WORK REPORT

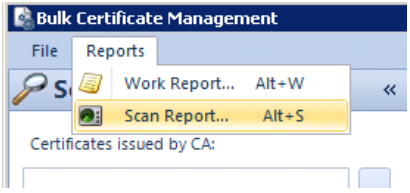
After work is done an all certificates appear in the 'Renewed panel, the 'Report' button becomes available. Selecting 'Report' will generate a CSV file of all work that was performed.

Items included in the report:

- Full path in the policy tree of the certificate object
- Timestamp for revocation (if applicable)
- Timestamp for certificate renewal
- Name of new Certificate Authority template (if applicable)
- Certificate DN
- Certificate start validity timestamp
- Scan details (if applicable)

Certificate DN	Revoked	Renewed	New CA	Certificate	Certificate Valid From	Detail
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\timetable.net	4/15/2014 14:53	4/15/2014 15:07		CN=timet	4/15/2014 14:57	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\www.proctors	4/15/2014 14:53	4/15/2014 15:09		CN=www.	4/15/2014 14:53	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\rms.013netvis	4/15/2014 14:53	4/15/2014 14:56		CN=rms.0	4/15/2014 14:43	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\dbr1.timemak	4/15/2014 14:53	4/15/2014 15:12		CN=dbr1.t	4/15/2014 15:01	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\pob.hadassah.	4/15/2014 14:53	4/15/2014 15:00		CN=pob.h	4/15/2014 14:50	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\Wildcard.pcch	4/15/2014 14:53	4/15/2014 15:14		CN=*.pcch	4/15/2014 15:04	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\editingcareers	4/15/2014 14:53	4/15/2014 15:08		CN=editin	4/15/2014 14:45	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\Sites	4/15/2014 14:53	4/15/2014 15:13		CN=Sites,	4/15/2014 14:59	

SCAN REPORT



After a network scan is performed, the results of the scan from the middle Results panel can be exported to a Scan report so that if vulnerabilities require patching any server software (eg. Heartbleed) than you can address those issues with the report before continuing with the key rotation and certificate renewal.

Items included in the report:

- Severity – What is the severity of the vulnerability that was detected by the scan
- Host – IP address of certificate find
- Port – Listening port of certificate found
- Issue – Lists the vulnerability found (Heartbleed, SHA1/MD5, Key length)

Severity	Host	Port	Issue	Certificate Subject
Critical	10.10.11.5	443	Heartbleed vulnerability found a	C=US, S=New York, L=New York, O=A Fine
Important	10.10.10.4	443	Weak hashing algorithm (sha1RS	CN=*.zappos.com, OU=Systems Administr
Important	10.10.10.2	443	Weak hashing algorithm (sha1RS	CN=qa.en.pampersrewards.pampers.com
Important	10.10.15.1	443	Weak hashing algorithm (sha1RS	CN=*.medhokapps.com, OU=Domain Cont
Important	10.10.17.4	443	Weak hashing algorithm (sha1RS	CN=SUBWAY, OU=EDI, O=IT, L=MILFORD, S

© 2014 Venafi Proprietary and Confidential

TROUBLESHOOTING

Certificate processing typically runs into problems when the certificate is in a state where it can't be renewed, such as:

- Wrong management type
- Missing required fields (CA Template or Vendor specific required fields)
- Certificate was already in error

Workflow

Workflows still need to be approved for when bulk renewals and revocations are performed. These are not bypassed by the Plugin.

Source File

There is a file called WinAdminBulkCertSelected.txt stored in %AppData%\Venafi, Inc\Venafi Encryption Director\{Version}\. This file is what keeps track of the work currently being done and attempts to automatically save progress in case the Plugin is closed.

Certificates Stuck in Processing

Certificates will stay in the "Queued" window if they encounter errors during revocation or renewal. Clicking on individual certificates will show the stage and status of the certificate in the detail window. Login to Web Admin to address the issue for each certificate. The Processing Window will automatically refresh as certificates continue to process. If fixing the issues are not available, close the Plugin and move the Plugin source file to a new location.

Known Issue

- Scanned certificates will always show that they are being Monitored, even if they do not exist in the Policy Tree
- Using the feature "Scan Existing Devices" will not work if any device objects in the policy tree have the hostname of "localhost"

LOGGING

When the Venafi Vulnerability Remediation Plugin is used, much of the same logging from automated renewals that happens in the platform is still logged. The primary items that are not currently logged by the Plugin are the action items that the Plugin automates like the clicking of "Revoke" or "Renew Now". The logs continue to be extremely valuable for troubleshooting purposes.

© 2014 Venafi Proprietary and Confidential