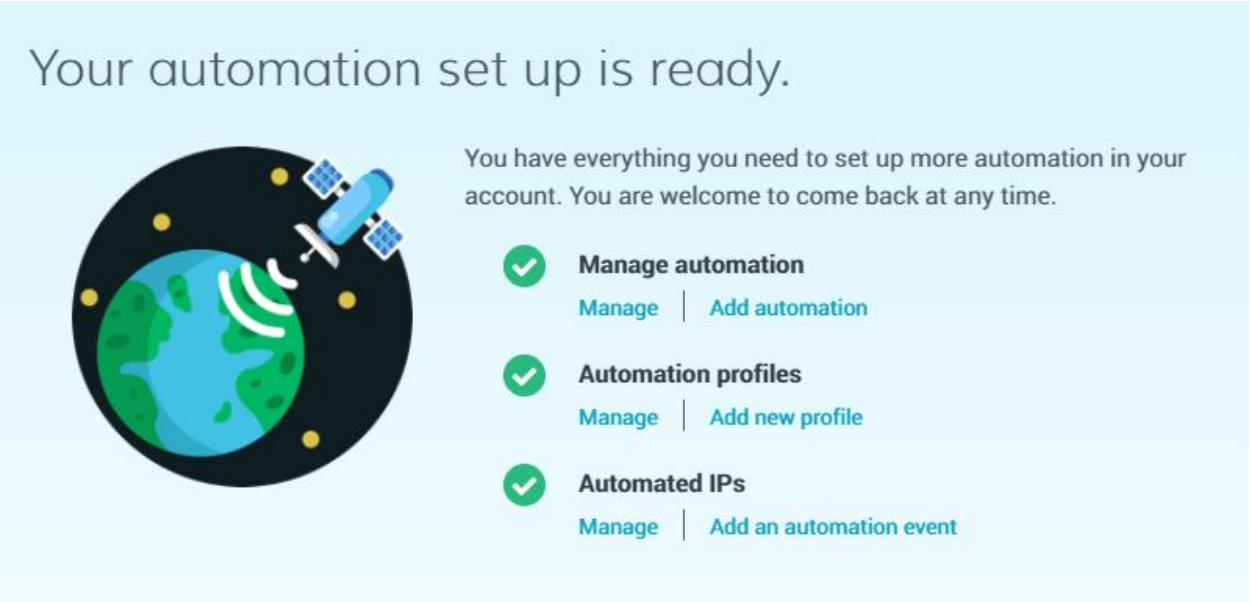
DigiCert® Technical Certifications CertCentral® Automation Expert Study Guide

2021 v1



Contents

List of Acronyms

CA	Certificate Authority
CC	CertCentral
CSR	Certificate Signing Request
FQDN	Fully-qualified Domain Name
O/S	Operating System
RHEL	Red Hat Enterprise Linux

Introduction

This study guide is designed to help you prepare for the **DigiCert Technical Certification: CertCentral Automation Expert** assessment exam. The exam will consist of 50 multiple-choice questions with a maximum time allowed of 1 hour.

The intended audience for this assessment is technical personnel who need to install, configure and troubleshoot the **Discovery** and **Automation** options within DigiCert CertCentral.

Before attempting a certification assessment, you should review the objectives below. If you believe that you are already able to meet all the objectives listed, you are welcome to schedule an assessment. However, if there are any objectives listed where you may need additional preparation, you should plan to research these topics in detail prior to scheduling an assessment.

More information can be found in the **CertCentral Automation Expert Training Guide** which can be downloaded from https://www.digicert.com/tls-ssl/tls-certification-program. Please note – these resources are just a starting point! It is strongly recommended that you do further research in order to be fully prepared for an assessment on all the objectives, including hands-on experience using DigiCert CertCentral Discovery and Automation.

In addition, it may be possible to attend a DigiCert instructor-based workshop which will give in-depth information on many of the assessment objectives. Please contact your DigiCert account manager if you would like to find out more.

Objectives

Before attempting the **DigiCert Technical Certification: CertCentral Automation Expert** assessment exam, you should be able to do the following:

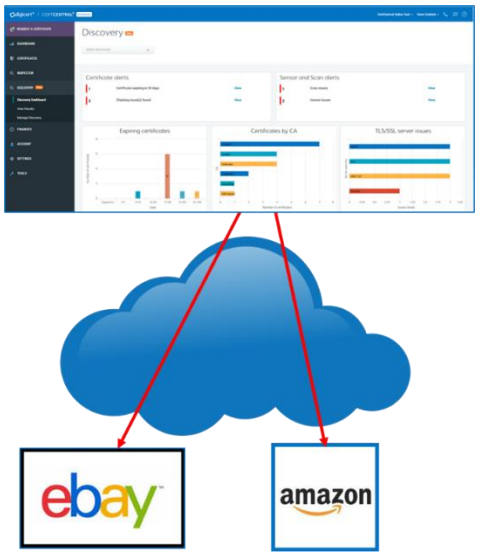
- Describe the benefits of the DigiCert CertCentral Discovery feature.
- Describe the benefits of the DigiCert CertCentral Automation feature.
- List the platforms supporting the DigiCert Discovery sensor.
- List the platforms supporting the DigiCert Automation agent.
- Describe the DigiCert sensor installation process.
- Describe the DigiCert automation agent installation process.
- Describe DigiCert agentless (sensor) automation configuration and operation.
- Create and manage automation profiles in DigiCert CertCentral.
- Create and manage Discovery Scans in DigiCert CertCentral.
- Describe the detailed certificate and end-point information available from Discovery scans in DigiCert CertCentral.
- Describe the differences between Cloud Discovery and Sensor Discovery.
- Configure and manage certificate automation in DigiCert CertCentral.
- Configure and manage ACME directory URLs in DigiCert CertCentral.
- List the API functions available for DigiCert Discovery and Automation functions.
- Perform basic troubleshooting for common sensor and agent configuration problems.

Overview

The DigiCert CertCentral Discovery feature allows you to automatically scan public-facing and internal systems for SSL certificates and SSH keys. This can ensure that you have an up-to-date inventory of all your certificates and are notified about risks such as certificate expirations and other security risks such as weak keys and ciphers.

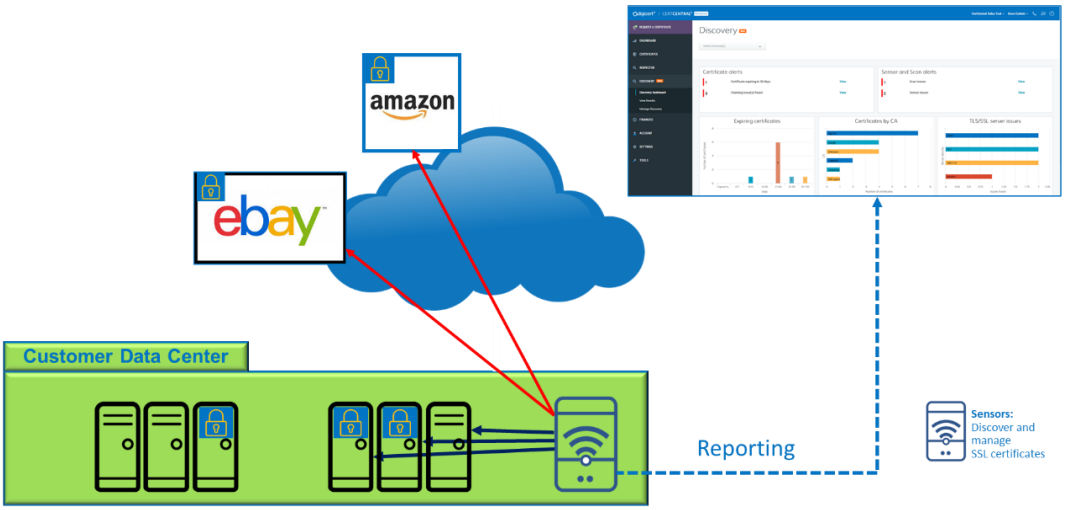
The DigiCert Automation feature allows you to fully automate certificate lifecycle operations, including installation and renewal of SSL certificates on web servers and appliances such as load balancers. To automate a web server certificate, agent software is deployed on the web server. To automate a certificate on a load-balancer, "agentless" (sensor-based) automation is used.

Cloud Discovery



The Discovery cloud scan uses a DigiCert cloud-based scan to find your public-facing TLS/SSL certificates regardless of issuing Certificate Authority (CA). Set up a scan to get the latest information about the certificates found and the endpoints where those certificates are installed.

Sensor Discovery



In addition to the Cloud scan, you can deploy sensors (small software applications) in strategic locations to scan your network. Using these sensors, Discovery can find all your internal and public-facing TLS/SSL certificates regardless of the issuing Certificate Authority (CA) while identifying

problems in certificate configurations and implementations along with certificate-related vulnerabilities or problems in your endpoint configurations.

Discovery sensor scans provide more robust scan configuration options and include the ability to run scans immediately, once – at a specified time, or multiple times – on a set schedule.

Sensors are configured and managed through the CertCentral console.

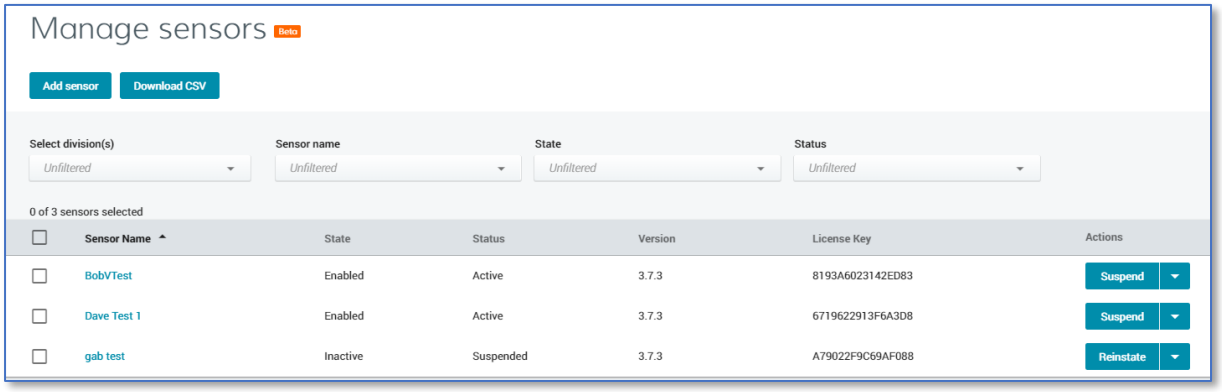
More information: https://docs.digicert.com/certificate-tools/discovery-user-guide/sensor-installation-requirements/

Sensors can be deployed on a number of different platforms, including Windows, Linux and Docker. The latest list of supported sensor platforms is here: https://docs.digicert.com/certificate-tools/discovery-user-guide/sensor-installation-requirements/#hardware-and-software-requirements

Sensor Installation

More information on sensor installation can be found here:

- Linux: https://docs.digicert.com/certificate-tools/discovery-user-guide/activating-sensors/linux-activating-sensor/
- Windows: https://docs.digicert.com/certificate-tools/discovery-user-guide/activating-sensors/microsoft-windows-activating-or-starting-sensor/
- Docker: https://docs.digicert.com/certificate-tools/discovery-user-guide/activating-sensors/docker-activate-or-start-sensor/
- Kubernetes: https://docs.digicert.com/certificate-tools/discovery-user-guide/installing-sensor/kubernetes-install-sensor/



Once a sensor is installed and successfully started, it will appear in the CC console.

Sensor Deployment

Each sensor must be able to access the Internet to communicate with the DigiCert cloud service. The sensor uses HTTPS (port 443). These outbound ports must be open on any intermediate routers or firewalls.

We recommend that you install sensors where they can reach the target IP addresses without going through intermediate devices such as routers and firewalls. If a sensor must scan across a firewall or router, ensure that firewall rules or access control lists allow the sensor to reach the target IP addresses.

How many sensors should I install?

As a general rule, install one sensor for an uninterrupted network segment that can be fully scanned in a reasonable time. For a large network based on multiple data centers, this typically means one sensor per data center to scan each data center's internal network, plus one sensor for each DMZ. However, you may need additional sensors if you plan to scan a large number of IP addresses and ports.

To determine the scanning efficiency of one sensor, install the sensor, configure and run a scan then review the time-to-completion and the results. If needed, you can add more sensors to improve scanning speed, or you may find that you can increase the scanning range of a single sensor.

Increasing the number of sensors will improve the overall time-to-completion for your scans. However, more sensors may increase your network bandwidth usage. You should balance your bandwidth requirements with how quickly you want scan results.

More information: https://docs.digicert.com/certificate-tools/discovery-user-guide/

Proxy Configuration

You can also configure a sensor to communicate with the DigiCert cloud through a proxy server.

On the computer you installed the sensor on, use a text editor (such as vi or Notepad) to edit/create a proxy.properties file, for example:

```
enableProxy=true
httpsHost=125.125.125.125
httpsHostPort=443
httpsAuthUser= system01@Admin
httpsAuthPassword=mypassword
```

Save the proxy.properties file to: install_dir/config/proxy.properties. Restarting the sensor will encrypt the proxy passwords and upload the proxy information.

More information: https://docs.digicert.com/certificate-tools/discovery-user-guide/configuring-sensor-use-proxy-server-communications/

SSL Inspection

The sensor will not communicate successfully via a proxy configured for SSL inspection (i.e. the proxy terminates the SSL connection and then creates a new SSL connection to the target address). The proxy must be configured for "pass-through" in order for the sensor to communicate successfully to the cloud.

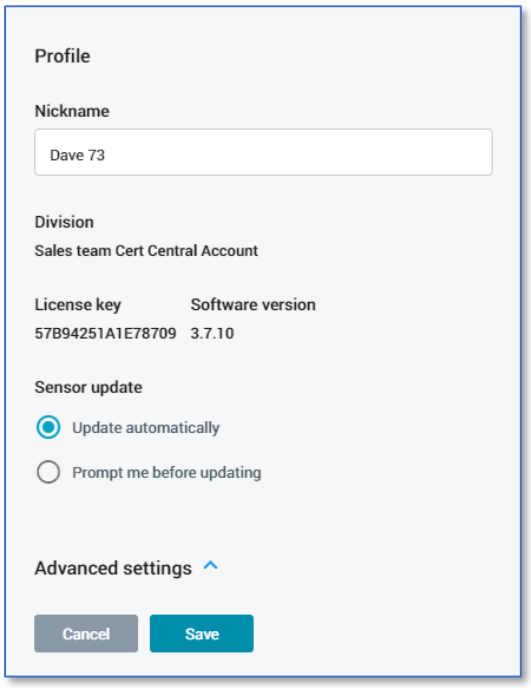
Sensor Restart

The Windows sensor is installed as a Windows service so will automatically restart if the computer they are installed on is rebooted.

On Linux you also have the option to control the sensor using a Linux service. This allows the sensors to operate uninterrupted in the background, even when your machine reboots.

The docker sensor will run if the container is running.

Sensor Maintenance



The Sensor is designed to not require any routine operations. By default, sensor updates are handled automatically by the CC cloud console. Upgrades are initiated remotely from the cloud; no user action is required on the sensor. Only signed code can be loaded and executed. Updates can be either automatic or manually triggered.

Suspending a sensor will cause any scans associated with the sensor to be aborted. Suspended sensors will not discover certificates but can be reinstated at any time.

Voiding a sensor will cause any scans associated with the sensor to be aborted. A voided sensor is permanently disabled and cannot be reinstated.

Sensor Troubleshooting

When a sensor isn't working, the first place to go is the **Manage sensors** page and check the status of the sensor. If the sensor is not listed, check the following possible causes:

- Has the sensor been activated?
- Has the sensor been started?
- Has the sensor been shut down?
- Have you tried restarting the sensor?
- Are there any error messages on the sensor start-up?

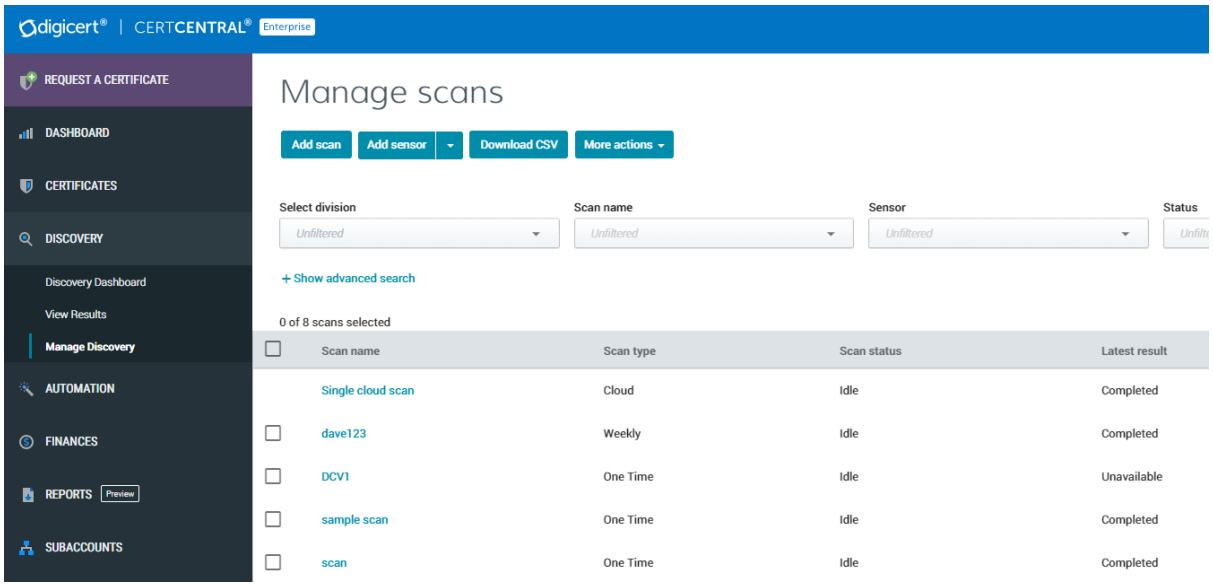
A common issue preventing sensor start-up is network connectivity.

- Can the sensor access the internet?
- Are the cloud URLs reachable from the sensor? Each sensor has a diagnostic tool to check for connectivity to the required URLs (diag.bat or diag.sh).
- Is a proxy server required? if so, configure a sensor to use a proxy server.

If you still haven't pinpointed the problem, check the sensor log. You need a copy of the sensor log to share with DigiCert support if you end up needing help. The sensor logs are located in the logs directory: '<install_dir>/logs'. Sensor logs are available for today and the previous 7 days. Note that the **sensor.log** file is the most recent log.

More information: https://docs.digicert.com/certificate-tools/discovery-user-guide/sensor-troubleshooting/

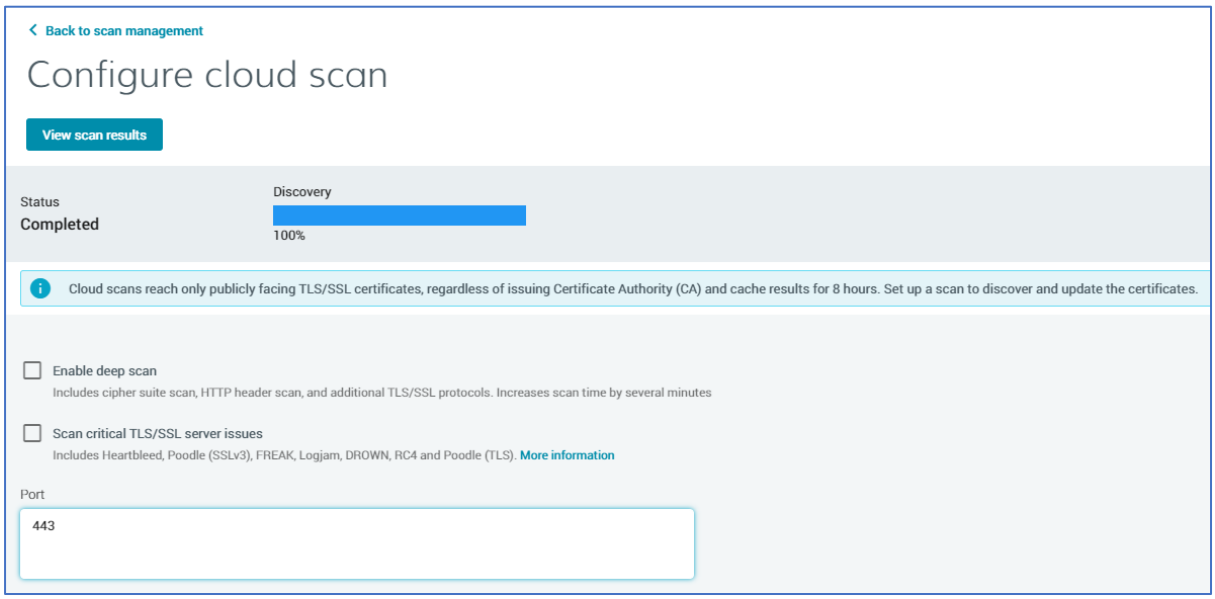
Scan creation and management



You configure scans in the CC console. The main configuration requirement is to set the range of IP addresses and/or FQDNs to scan. When you specify an FQDN, all IP addresses that can be resolved under the domain will be scanned.

Cloud Scan

By default, a cloud scan supports 50,000 IPs/FQDNs per scan (on port 443 only). There is no limit to the number of cloud-based scans you can run. The cloud scan caches scan results for 8 hours, i.e. the scan will not rescan the same site if it was scanned in the last 8 hours. In this case, just the cached results are returned.



The Cloud Scan includes options to enable a deep scan and to scan for critical TLS/SSL server issues:

- **Deep scan**: Includes cipher suite scan, HTTP header scan, and additional TLS/SSL protocols. Increases scan time by several minutes.

- **Critical TLS/SSL server issues**: Includes Heartbleed, Poodle (SSLv3), FREAK, Logjam, DROWN, RC4 and Poodle (TLS).

More information: https://docs.digicert.com/certificate-tools/discovery-cloud-scan-service/

Sensor Scan

In typical deployments, you configure multiple scans so that different subnets or services are scanned at different times. These scans can be periodic (daily, weekly, or monthly) in order to monitor any changes in the SSL environment.

We recommend that you initially scan all IP addresses and ports (1-65,535). This lets you discover which subnets and ports are in use by critical services. Thereafter, you can scan these services more or less frequently by targeted scans.

Default ports

The "default" port list for CC scans includes the 9 ports where SSL certificates are often deployed:

- 443 (HTTPS)
- 389 (LDAP)
- 636 (LDAPS)
- 22 (SSH, SFTP)
- 143 (IMAP)
- 110 (POP3)
- 465 (SMTPS)
- 3389 (RDP)
- 8443 (Apache Tomcat SSL)

SNI Support

Sever Name Indication (SNI) is a mechanism where the same IP:port can host multiple websites that are resolved by name instead of IP.

Discovery scans support an SNI option. If SNI is not enabled, if we scan an IP:Port with multiple certificates we only get the "default" certificate. This can cause issues, especially if the target system is behind a CDN.

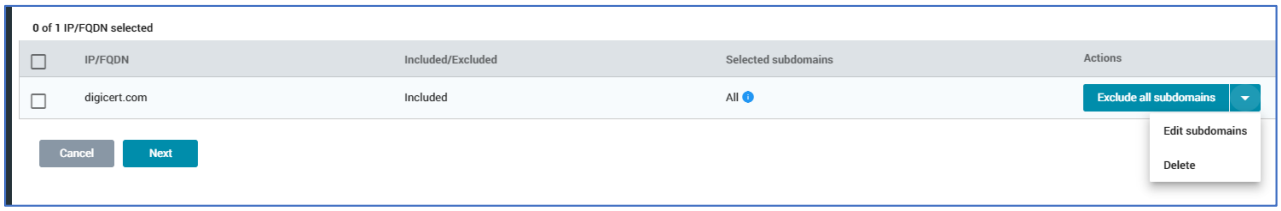
If the SNI option is enabled, if we scan an IP:Port with multiple certificates we get the certificate corresponding to the FQDN specified.

Note:

- An SNI-based discovery may not have IP information as part of the scan.
- SNI Scans are not allowed for large port ranges (limited to 10 ports per server)

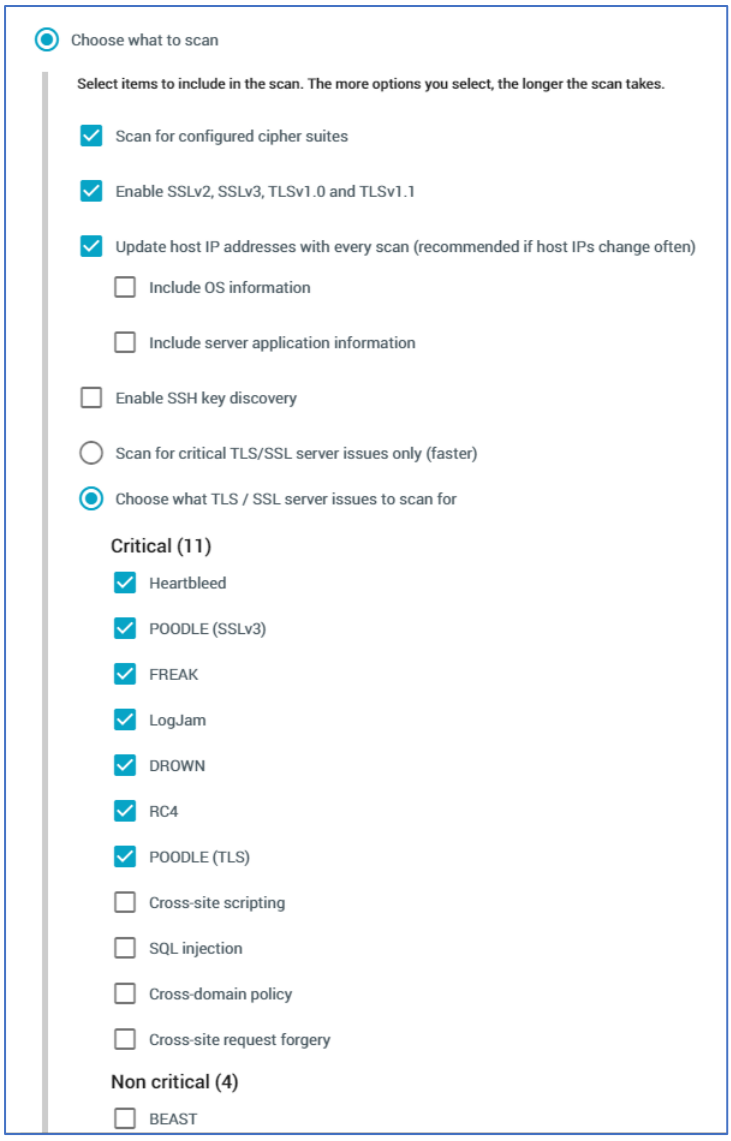
Subdomains

The sensor scan also has the option to include subdomains. The list of subdomains is automatically generated so is not guaranteed to be exhaustive. The list can be edited if required.



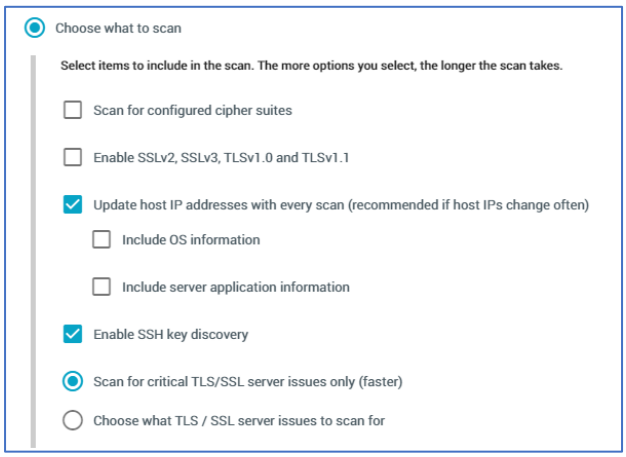
SSL Vulnerability Scans

CC Sensor Discovery includes additional options and flexibility to scan for cipher suites, SSL and website vulnerabilities, SSH keys, operating system information, etc.



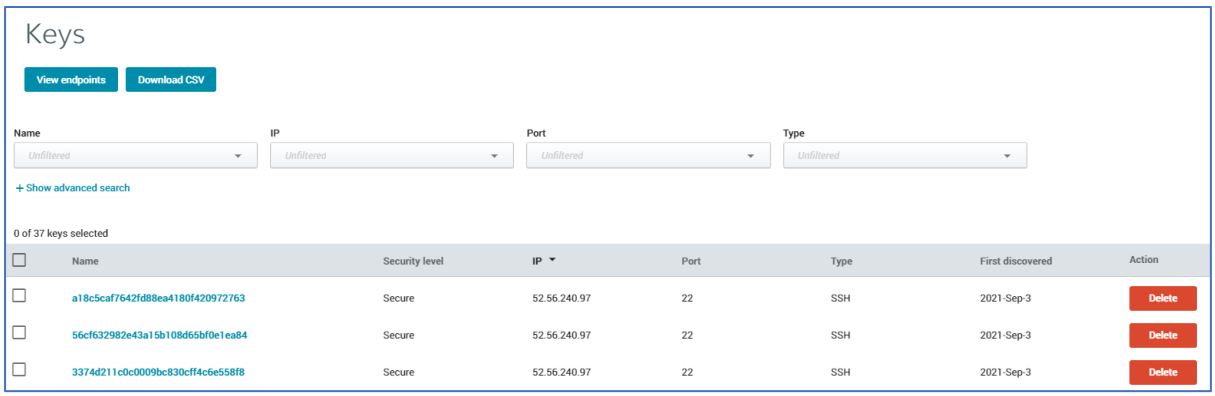
Vulnerability scan options are user-selectable in the scan configuration.

SSH Keys



When configured, the Discovery sensor scans your network (using default SSH port 22) for SSH keys configured on your server. The following information about the discovered keys is available:

- Name (fingerprint)
- Algorithm
- Authentication methods
- First discovered (date)
- Rotation limit
- Protocol (SSH1/SSH2)
- Duplicates
- Security level



The key is regarded as unsecured if it:

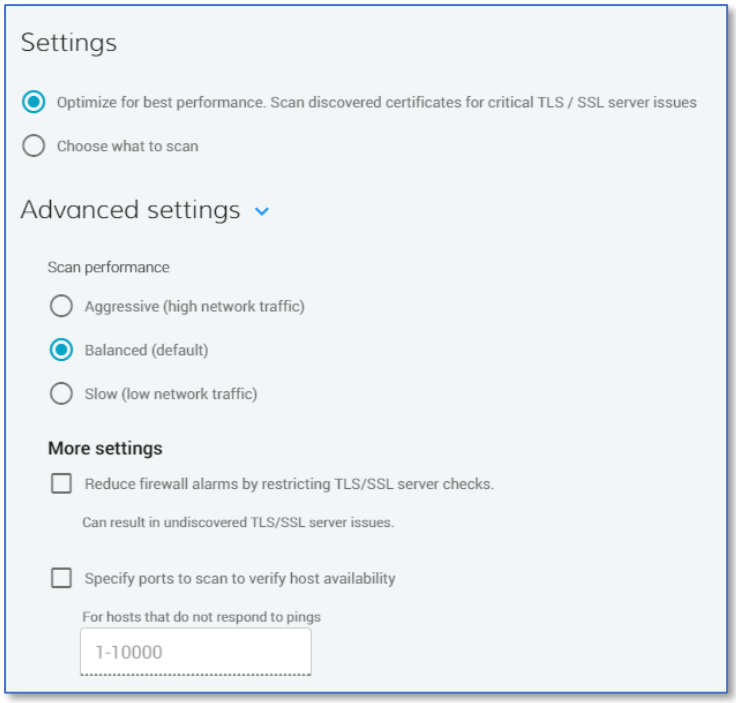
- Has duplicates.
- Reached or is approaching its rotation limit.
- Uses SSH1 protocol to set up the connection.

More information: https://docs.digicert.com/certificate-tools/discovery-user-guide/ssh-keys/

Advanced Settings

Scan performance

Set performance level to control the relative speed of the scan and network bandwidth usage when performing host and certificate discovery scans.



Aggressive (high network traffic) - Sends scan packets at the maximum rate, resulting in a larger number of packets being sent out on the network. The CC service still puts a cap on the number of packets sent at the fast setting to prevent uncontrolled and unintended number of packets. This setting may set off false alarms on Intrusion Detection System or Intrusion Prevention Systems.

Balanced (default) - Balances the speed of the scan and its impact on network resources.

Slow (low network traffic) - Sends a few scan packets at a time, and waits for a response before sending more. This setting will cause the scan to take longer to complete.

CC uses a distributed sensor architecture which can easily scale based on network size. If necessary, discovery performance can be increased by adding more sensors. Each sensor can be configured to work in parallel to achieve the desired performance.

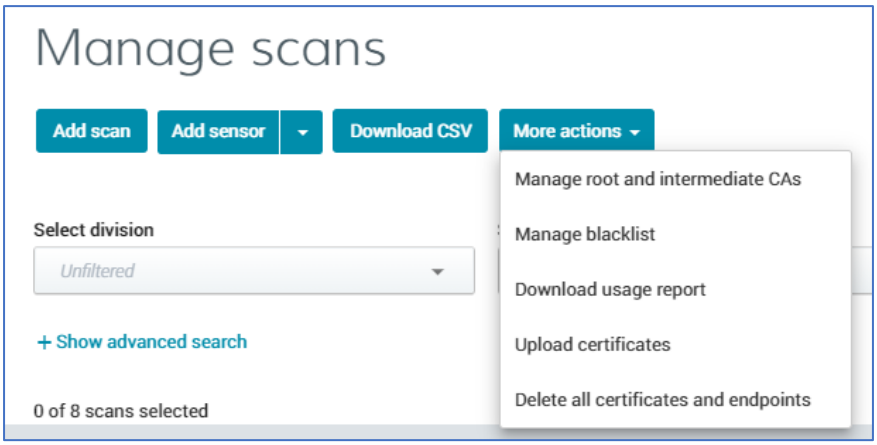
TLS/SSL server checks

In some cases, scans that check for TLS/SSL server issues (such as Heartbleed) must emulate a TLS/SSL server issue to verify that the server is secure. If these scans trigger firewall alarms in your network, you can restrict these checks.

Ping-disabled hosts

If Internet Control Message Protocol (ICMP) pings are disabled on a host, use this setting to specify which ports to scan to verify host availability. The fewer ports you specify, the faster the scan speed. By default, ports 1-10000 are scanned.

The ports you list here are used only for available host discovery (as a first step in the scan process). The ports listed in Add scan, Edit scan are used for certificate discovery.



Blacklist

Under "More actions" you can choose to blacklist specific IPs/FQDNS/hostnames to keep their domain information from appearing in your scan results. For example, you may want to exclude a specific domain in your CDN network. Blacklist settings apply to all scans.

Upload roots and intermediates (ICAs)

You can also upload public and private roots and intermediate certificates.

- Private roots and intermediates become active immediately for your account only.
- Public roots and intermediates will become active for all accounts once reviewed and verified by DigiCert.

More information: https://docs.digicert.com/certificate-tools/discovery-user-guide/add-public-and-private-root-and-intermediate-cas/

Scanning Strategy

Consider the frequency that you want to inventory your SSL certificates. For example, you could run more frequent scans to maintain compliance or to monitor a regularly-changing network. If you need to regularly monitor your network for such purposes, you probably want to consider sensor and scan configurations that enable faster time-to-completion.

In a typical deployment, users will configure a number of different scans.

- All sensors, all ports, medium speed, once per quarter. This scan will answer the question "what do I have on my network?"
- Application scan on targeted ports – every 2 weeks on a test/QA network, every week on a production network. This will test for any changes.
- On demand scans – as required.

Scan data

During SSL discovery scans, the CC sensors collect and then report back selected information to the CC cloud. This includes:

- Data about hosts in the network
- Data about TCP ports on each of the discovered hosts
- Data about SSL server certificates discovered on the open ports (if any are discovered)

The discovered data from scheduled or on-demand scans is temporarily stored on a sensor before being transmitted to the cloud. Two-way SSL server and client authentication using certificates are

used to protect the data during upload from sensor to console. Data is transmitted over HTTPS using a client-authenticated TLS handshake.

Examples of data collected include:

- Common Name
- Port Number
- IP Address
- Expiration Date
- Certificate Status
- Security Rating
- Owner
- Certificate Authority
- Key Length
- Algorithm Type

Certificates discovered

CC scans discover all SSL certificates for the specified IP addresses and ports, on any operating system, and for any CA vendor. CC discovers SSL certificates from any public or internal certificate authority.

The SSL handshaking performed by CC Discovery is based on the target device port number and is not protocol-aware. Therefore all standard certificate-based protocols/services on SSL-based servers are supported (except as noted below).

You can configure CC to detect certificates used by protocols, such as SMTP-TLS, which use the STARTTLS command to upgrade a plain-text connection to an encrypted (TLS or SSL) connection.

Certificate Status

When a scan is done, Discovery performs checks to determine if the certificate is revoked, typically this is done using the CRL/OCSP urls found within the certificate:

Valid	A cert that is not expired and isn't revoked.
Expired	Expired. No revocation check is done for expired certs.
Not Verified	OCSP or CRL status could not be verified when scanning. (This can happen due to multiple reasons, e.g. sensor can't reach the OCSP server or CRL list.)
Unavailable	Not scanned or self-signed or internal CA certs where CRL/OCSP info is missing.
Revoked	Not expired but not valid.

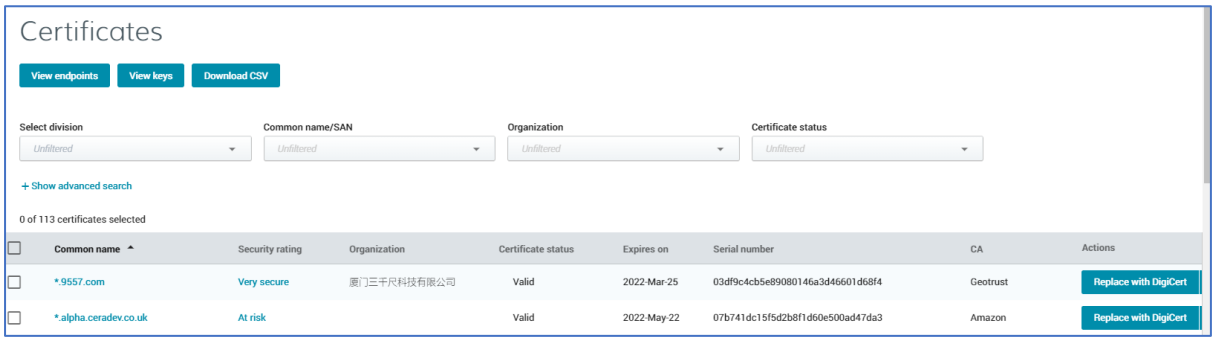
Note: Checks are done daily so these states can change.

Data Views

Scan results can be viewed in 2 ways:

- Certificates View
- Endpoints View

Certificate View

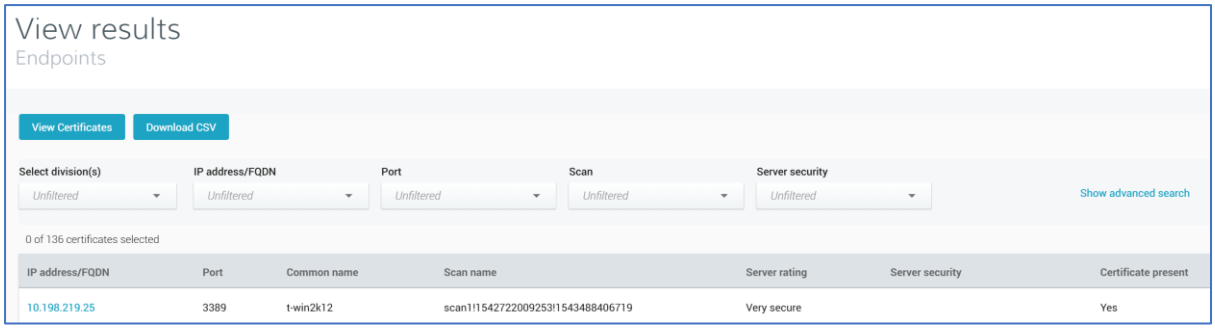


The Certificates view lists discovered certificates. Actions available:

- Replace Certificate
- Delete
- Download Certificate
- Add Tags
- View Certificate Security Details
- View Endpoints containing that certificate
- View SSH keys

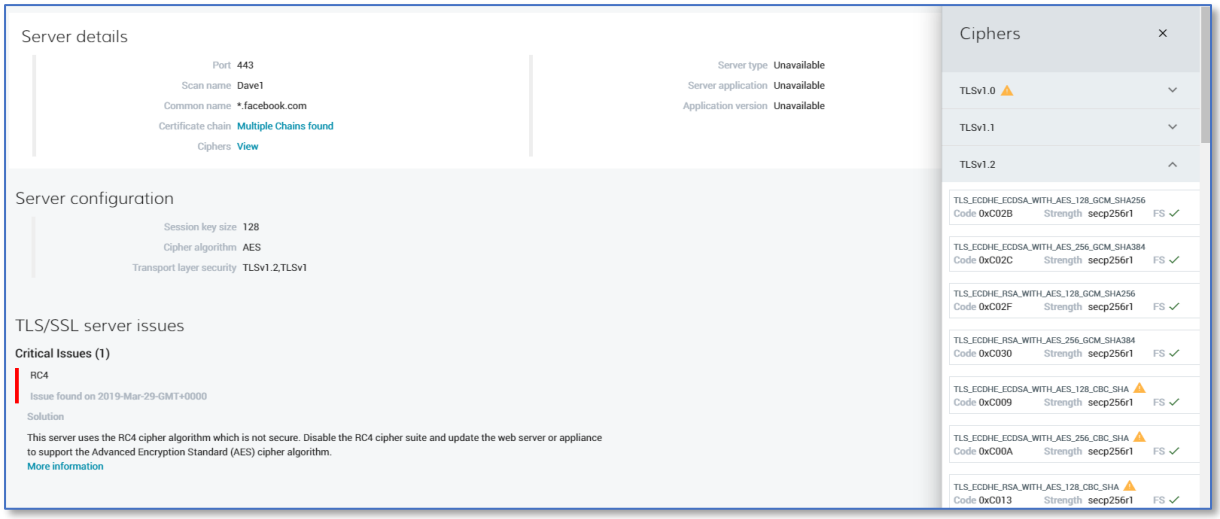
The **Replace Certificate** option allows the user to request a replacement certificate through CertCentral.

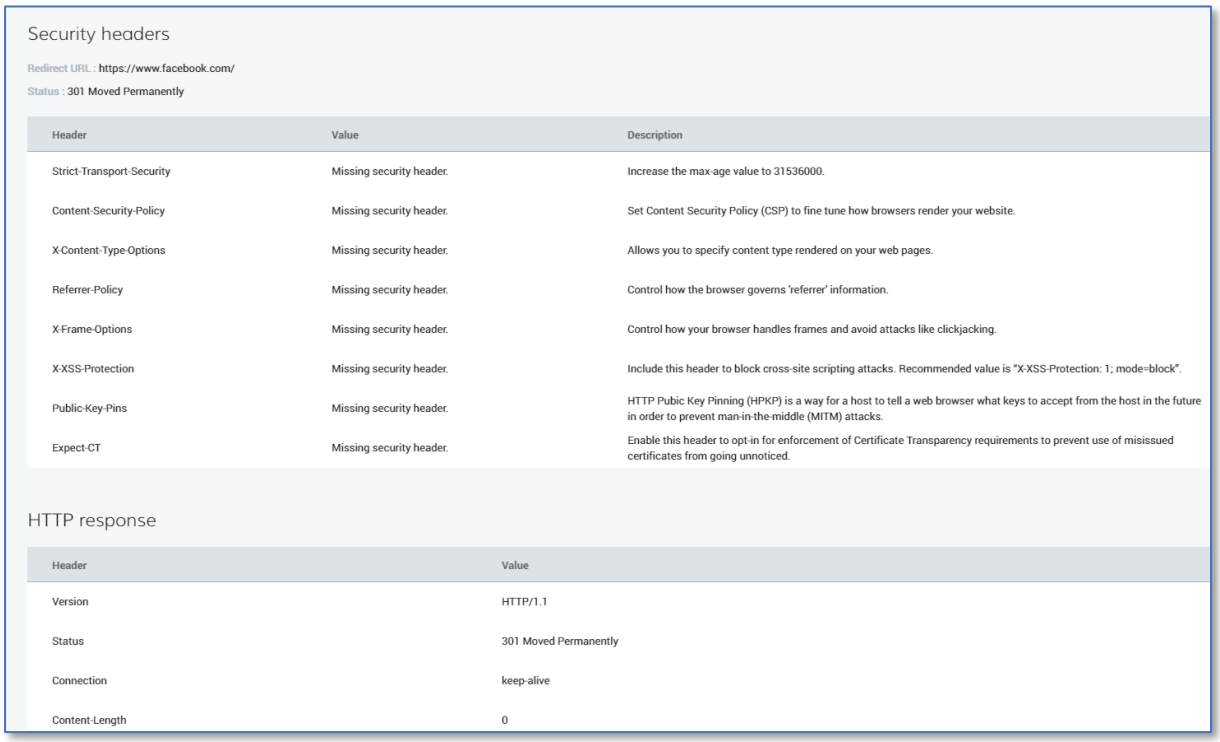
Endpoint View



The Endpoints view lists listening IP:port combinations which have been scanned and shows what certificates (if any) were discovered. Actions available:

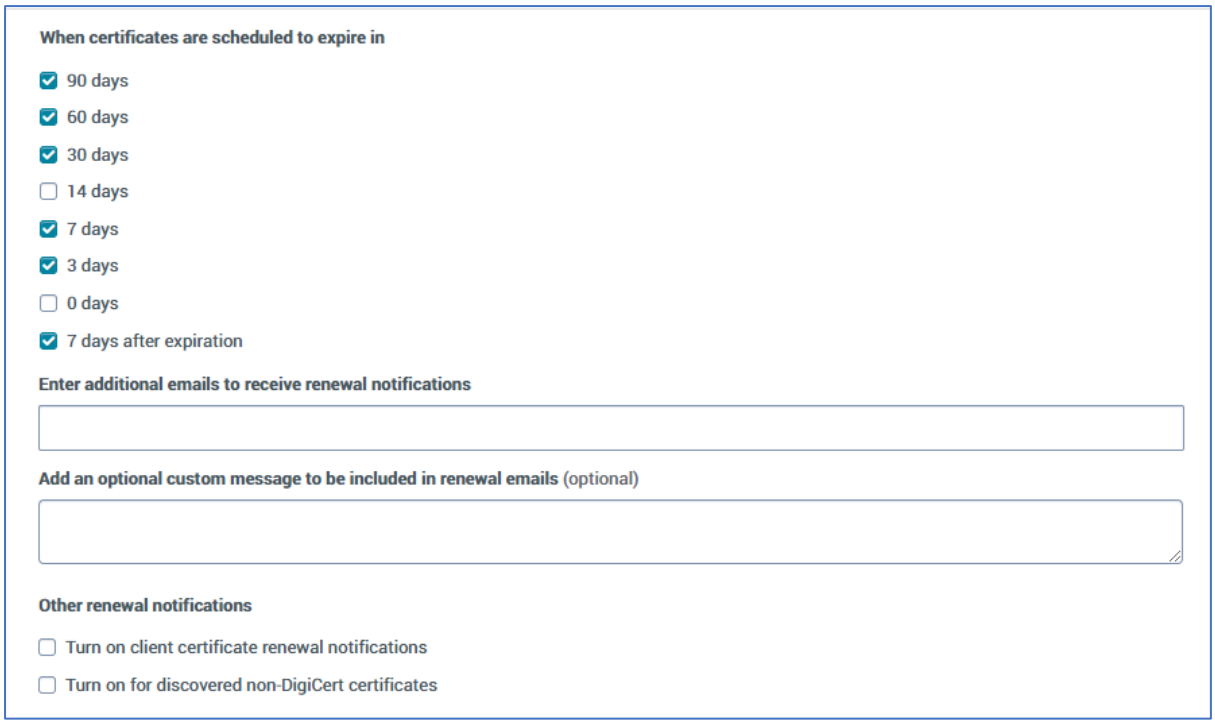
- View server details
- View certificate details
- View SSL chain information
- View TLS/SSL server issues
- View Security headers
- View HTTP response
- View supported ciphers



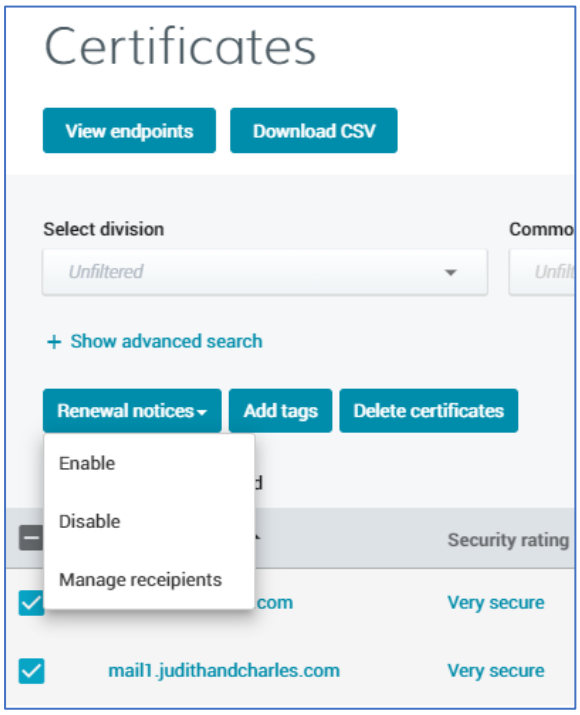


Notifications

CertCentral can send renewal notices for discovered (non-Digicert-issued) certificates if configured. The frequency will honour existing CertCentral preferences (under SETTINGS -> Notifications -> Advanced notification settings).



There is also an option to enable/disable notifications per certificates or certificate group.

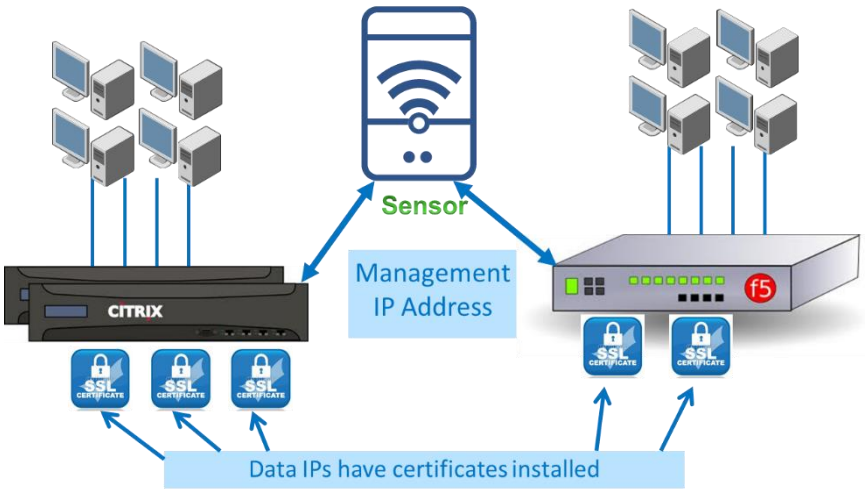


Discovery Dashboard

The Discovery Dashboard gives a high-level view of any critical alerts, as well as a graphical overview of the discovered certificates.

Agentless automation

Automating certificate requests on a load balancer or similar device is performed through a CertCentral sensor, the software that also manages and performs discovery scans.



The sensor talks to the management IP address on the target system. The sensor maintains login credentials for the target system in encrypted form and communications are encrypted (either HTTPS or SSH, depending on device).

The sensor controls the load balancers via remote API calls. No extra software is installed on the target system. Agentless modules are installed as part of sensor installation.

The current list of supported appliances can be found here: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/automation-user-guide/automation-getting-started/#sensor-agentless-automation-for-load-balancers

Setup and configuration

To configure agentless automation for a supported appliance, run the ***addagentless*** CLI command on any sensor which can access the management IP address of the appliance, and supply the necessary information when prompted. (Alternatively, a text file can be used to supply the information.)

More information: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/automation-user-guide/install-automation-agentless-loadbalancer/configuring-your-sensor-agentless-automation/

Below is an example of adding automation for an F5 BIG-IP on a Linux sensor:

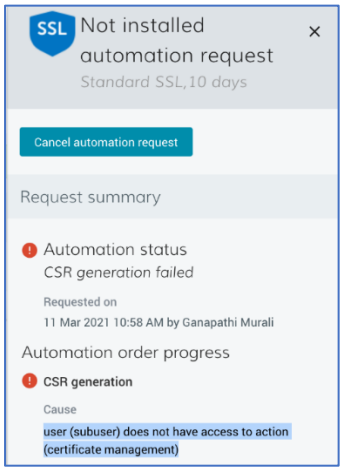
```
[root@cc-sensor cli]# ./addagentless.sh -type BIGIP
Sensor CLI. Copyright 2021, DigiCert Inc.
Add or change login credentials and specify data IP addresses for certificate
automation.
Enter management IP address: 62.116.156.91
Enter management Port: 443
Enter web service username: admin
Enter web service password:
Confirm web service password:
To activate data IP addresses for certificate automation, enter each IP address
separately below, or run the standalone activateips.sh command.
Data IP addresses found
62.116.156.92
To finish the list, press Return at the prompt (blank input). To enable all IP
addresses found, enter a (for all).
Enter data IP address: a

Successfully added or changed the agentless automation.
```

More information on configuring agentless automation for specific platforms can be found here:

- AWS: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/automation-user-guide/install-automation-agentless-loadbalancer/configuring-your-sensor-agentless-automation/configure-sensor-agentless-automation-settings-aws-load-balancer/
- F5 BIG-IP: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/automation-user-guide/install-automation-agentless-loadbalancer/configuring-your-sensor-agentless-automation/configure-sensor-agentless-automation-settings-f5-big-ip-load-balancer/
- Citrix NetScaler: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/automation-user-guide/install-automation-agentless-loadbalancer/configuring-your-sensor-agentless-automation/configure-sensor-agentless-automation-settings-citrix-netscaler-load-balancer/
- A10: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/automation-user-guide/install-automation-agentless-loadbalancer/configuring-your-

sensor-agentless-automation/configure-sensor-agentless-automation-settings-a10-load-balancer/



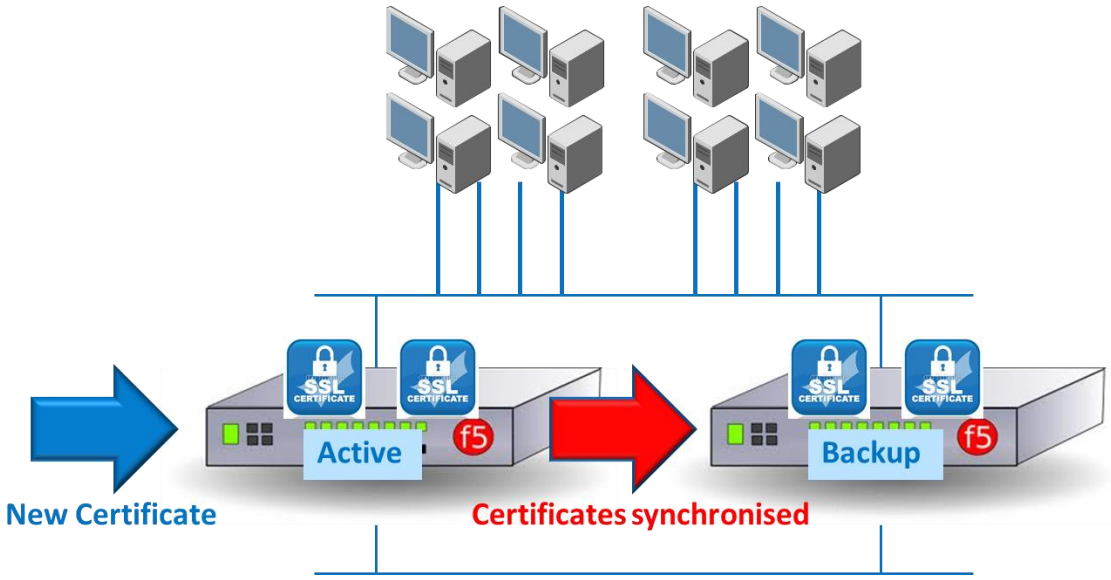
The login credentials must have sufficient privilege for automation to succeed. For example, automation on F5 BIG-IP is successful only with *Administrator* and *Resource Administrator* roles.

HA Configurations

Load balancers such as F5 and Citrix support HA configurations, i.e. an active system has one or more backups which take over in case of failure.

You can choose to automate any load balancer in a cluster or HA configuration. But it's up to you to decide (and configure) how the cluster synchronizes settings (including certificates).

When configuring an HA configuration, just add one IP address – if you try to add a second (e.g. backup) it will fail (it's already discovered).



When working with F5:

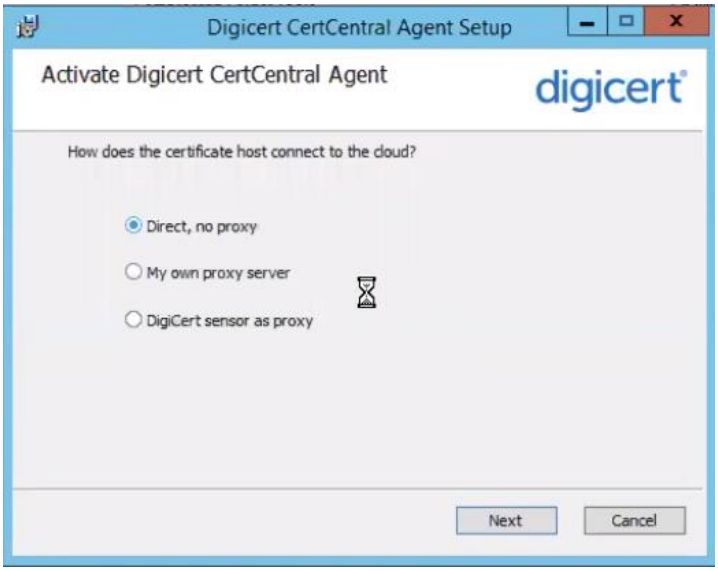
- Add management IP address of either F5 (not both) or the "Floating" (shared) IP address
- The HA pair will be discovered
- The active device is updated with new certificates
- F5s synchronise manually or automatically

More information: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/automation-user-guide/install-automation-agentless-loadbalancer/high-availability-f5-big-ip-load-balancer/

Agent setup and configuration

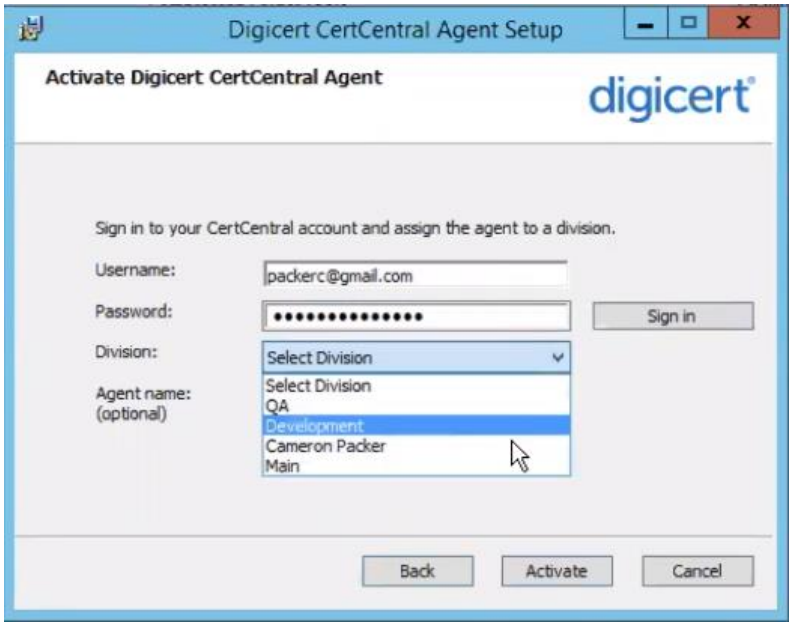
Automating certificate requests on dedicated hosts such as web servers requires a CertCentral automation agent on the host.

Details on supported applications can be found here: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/automation-user-guide/get-started-with-automation/



Agents can be configured to communicate directly with CertCentral, via a proxy, or via a sensor.

Activating an agent is similar to activating a sensor:

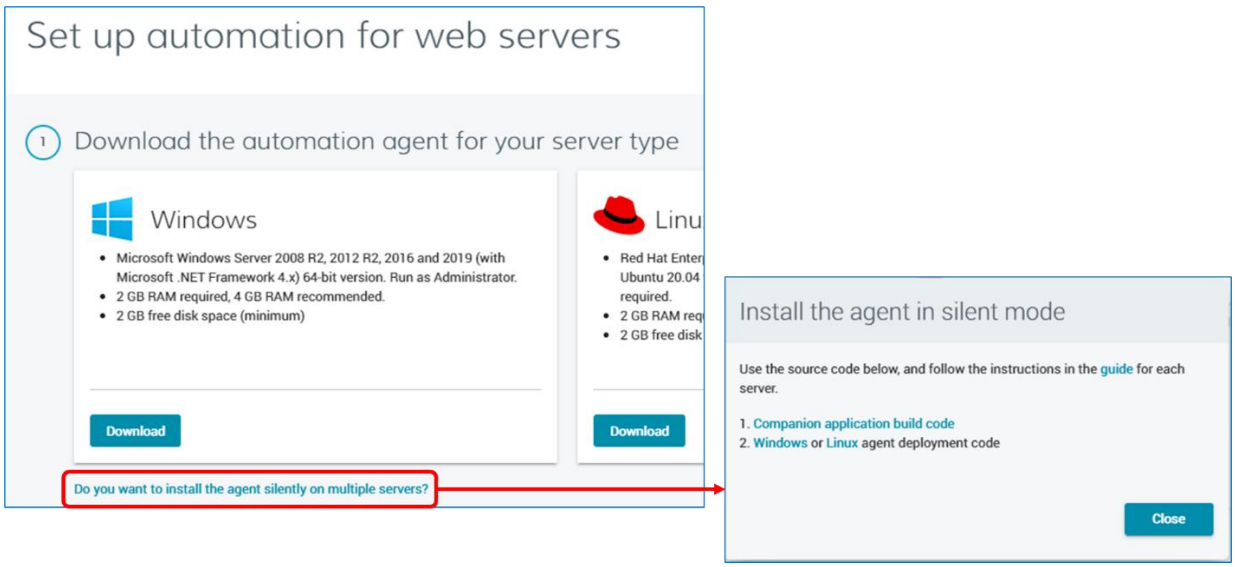


1. Sign into your CertCentral account with your usual credentials;

2. Select an appropriate division.

The standard agent includes a standard ACME client, currently either certbot (Linux) or win-acme (Windows). Note: The ACME client will automatically restart the web server (e.g. Apache, Nginx) if necessary.

Silent Install



With the April 2021 release we are enabling customers to download code and instructions to build an agent companion tool that can then be distributed to multiple machines to install the agent silently. The distribution can be done using popular methods like GPO push on Windows, an Ansible playbook on Linux, or any other method that customers may be using. This will help customers install and provision agents on large number of servers remotely, to get up and running with webserver automation quicker. Detailed instructions in the guide.

Failover

Agents configured to communicate via a sensor can take advantage of failover in case the sensor becomes unavailable. For failover to work, the account must have more than 1 sensor configured and contactable by the agent.

During initial setup and provisioning of the agent with the sensor as proxy, one sensor (the proxy given during provision) will be configured on the agent. Once provisioning is complete, a list of all sensors in the account will be sent to agent from the cloud and stored in the agent's database.

Whenever the primary sensor goes down, the agent will start to test connectivity with other sensors and connect through the first available sensor.

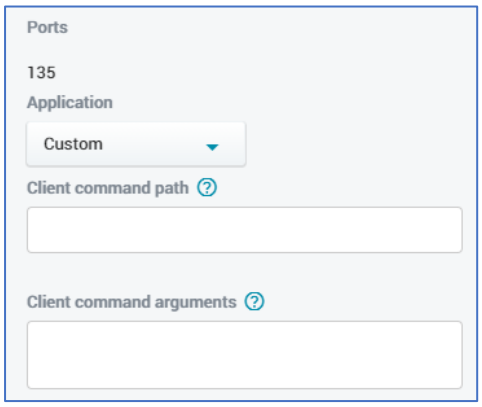
Whenever a sensor gets added or removed from cloud for the account, the updated list of sensors is sent to the agents.

Maintenance

The agent has a capability to update all its modules which are pushed from the cloud. It also does auto-upgrade of certbot/win-acme clients whenever there is a change pushed from the cloud.

The provisioning cert used by the agent is valid for 3 years and auto-renews when close to expiry, so the agent can keep running without user intervention.

Custom Agents



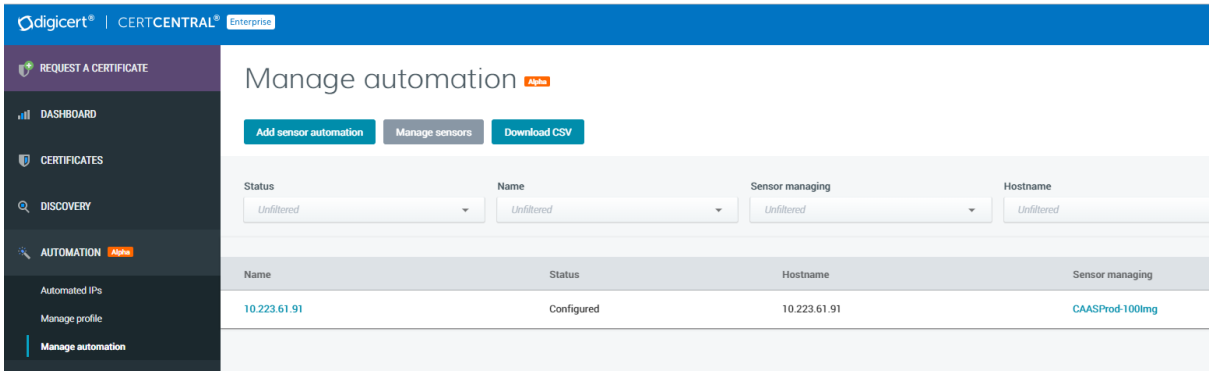
With managed automation, you can use a DigiCert provided agent, or you can configure the agent to use another ACME client. To use a custom ACME client, you need to specify the client command path and arguments when configuring the automation agent.

The process is:

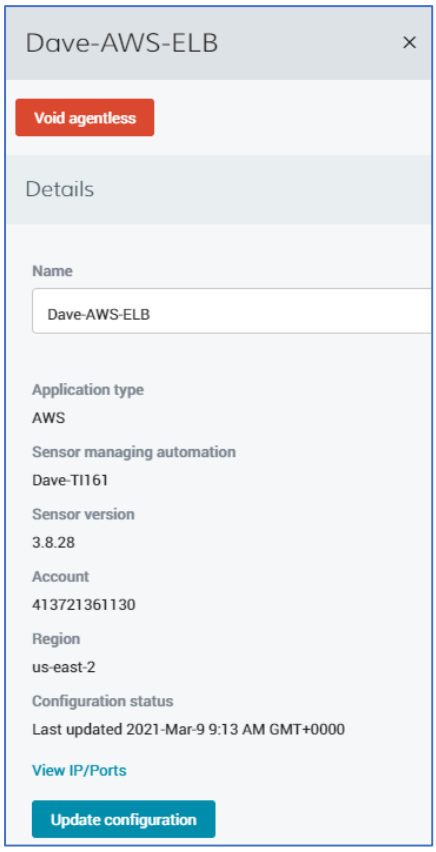
1. Download, install and start linux/windows agent on platform.
2. Configure agent ports as “custom” in CertCentral and specify command path and arguments.

More information: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/acme-user-guide/configure-automation-agent-use-custom-acme-client/

Automation management in CertCentral

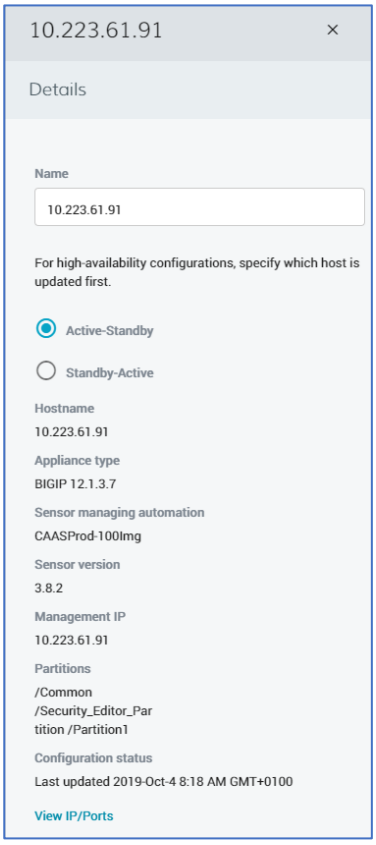


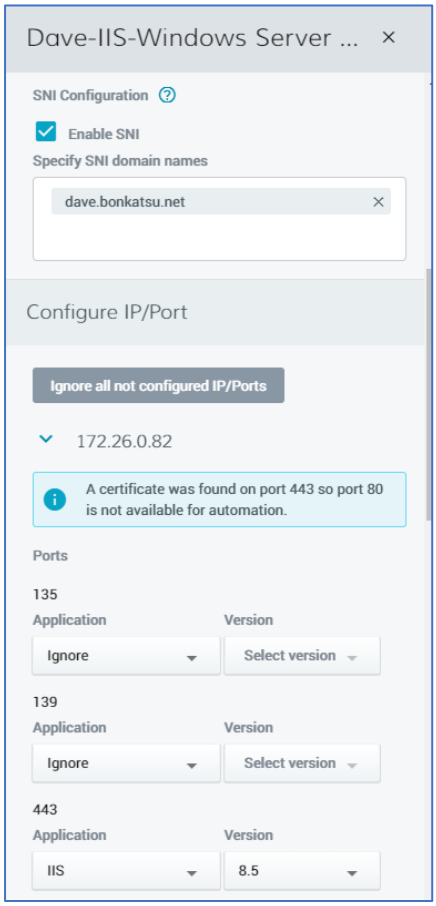
All agent and agentless configurations are listed in the **Manage automation** page. Click on the name to see more details.



Left: AWS ELB configuration example

Right: F5 Big-IP HA configuration example



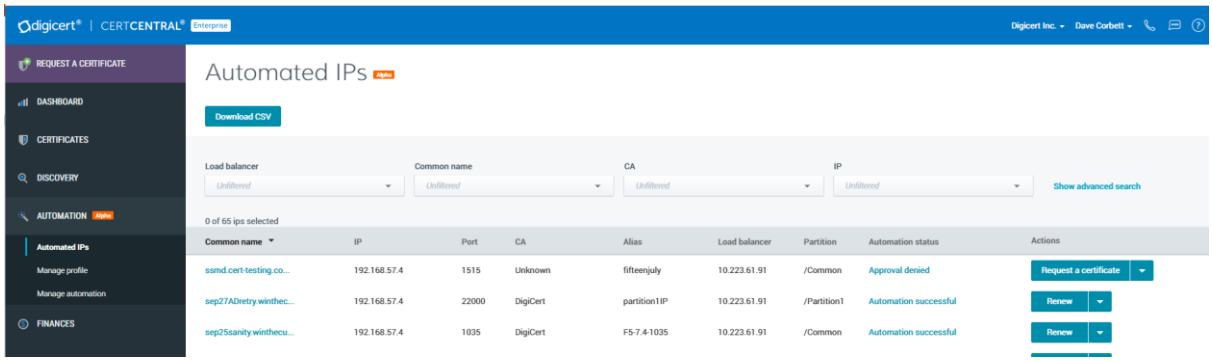


For agent-based automation, it is necessary to configure in CertCentral the correct application for each TCP port where automation is required. The “ignore” option should be set for other available ports.

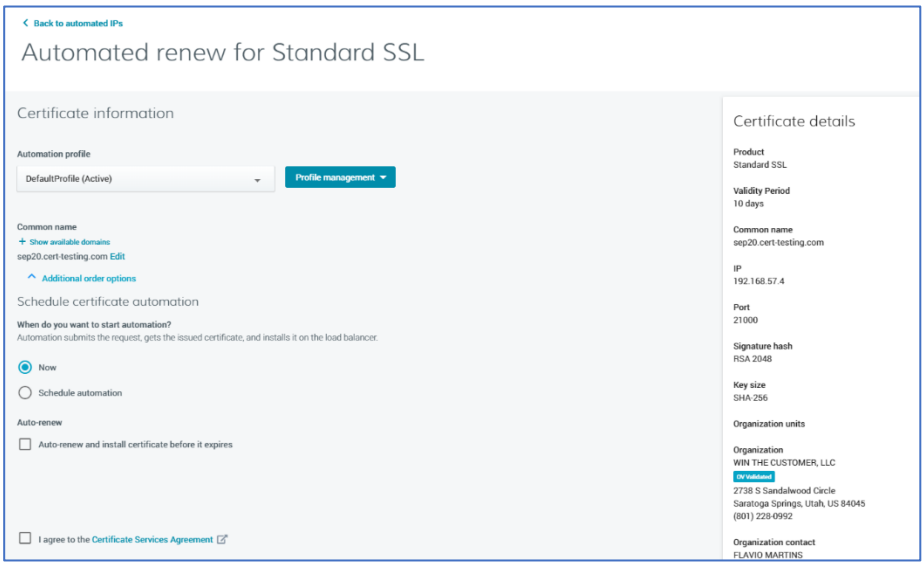
For a web server using SNI, check the “Enable SNI” option and specify the domain names you want to automate. (Note: the SNI option assumes a pre-existing SNI configuration on the web server. Automation cannot create a new SNI configuration.)

Automated IPs

To schedule an automation event, go to the Automated IPs screen. Locate the certificate and choose the appropriate action.



- Request a certificate: Request a certificate when there is no certificate configured to IP/Port.
- Switch to DigiCert: When you want to replace a certificate issued from a different Certificate Authority (CA) with a DigiCert certificate.
- Renew:
  - For non-Multi-year Plans: When a certificate expired or is about to expire in less than 90 days.
  - For Multi-year Plans: When a certificate and/or Multi-year Plan expired or is about to expire in less than 90 days.
- Reissue:
  - For non-Multi-year Plans: When an active certificate is revoked or missing. Note: The certificate will be reissued with the remaining validity of the original certificate.
  - For Multi-year Plans: When an active certificate for a Multi-year Plan is about to expire.
- Get your next certificate: Applicable only for Multi-year Plans, when an active certificate for a Multi-year Plan is about to expire in less than 30 days. Note: Until the Multi-year Plan expires, you can reissue or get your next certificate at no cost each time it reaches the end of its validity period.
- Submit manual request: When you want to request a certificate manually.



On the next screen, you can make changes if necessary before confirming:

- Choose or create an automation profile for this event.
- Enter the Common name and Subject Alternative Name (optional) you want to request the certificate for.

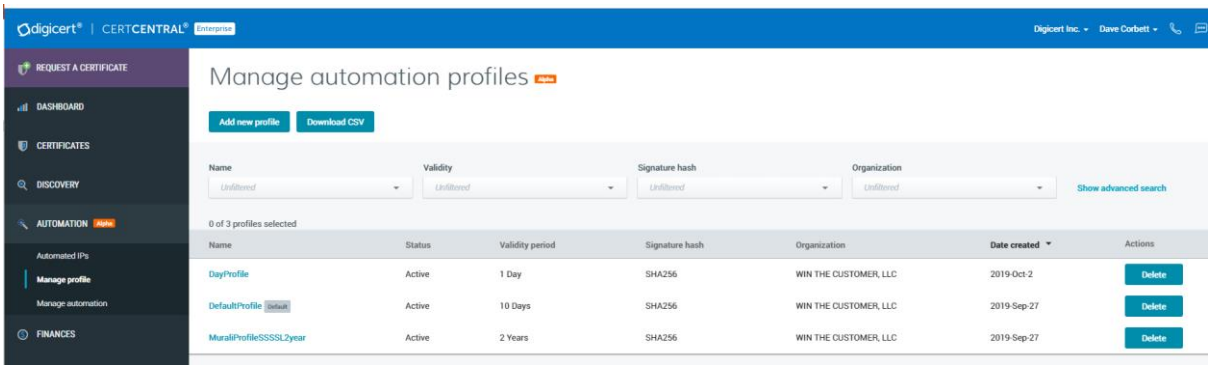
- Set the time for automation to begin—immediately or scheduled in advance.
- (Optional) Set the certificate to renew and install automatically near the end of its validity period.

More information: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/automation-user-guide/schedule-automation-event/

Automation Profiles

An automation profile is a template for SSL/TLS certificate deployment. A profile defines certificate properties, such as product type and validity, so you can maintain SSL/TLS uniformity across your environment.

When you schedule automation, you choose a profile. The agent then requests and installs a certificate with those pre-determined settings. You can define multiple profiles and choose the right one depending on the host device.

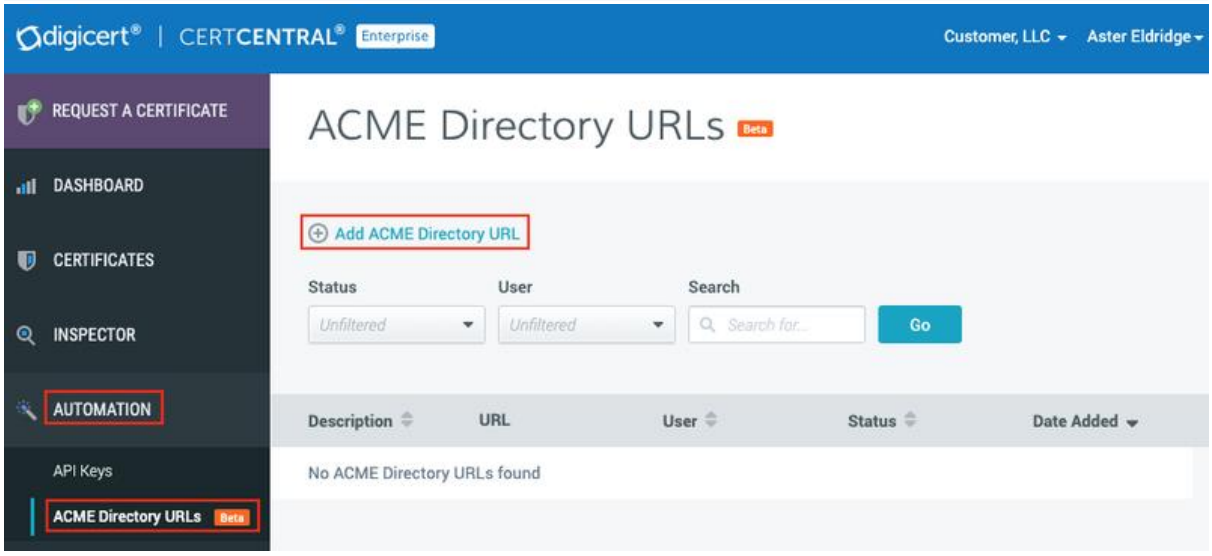


More information: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/automation-user-guide/automation-profiles/

ACME Directory URLs

If you have already deployed an ACME client such as CertBot to automate certificate installation and renewal, with CertCentral, you can use your existing ACME client to automate your SSL/TLS certificate deployments using certificates from your CertCentral account.

CertCentral ACME protocol support allows you to automate private SSL certificates and public OV and EV SSL/TLS 1-year and custom validity certificate deployments. Our ACME protocol also supports the Signed HTTP Exchange certificate profile option, enabling you to automate your Signed HTTP Exchange certificate deployments.



To begin, generate a unique ACME Directory URL in your CertCentral account. You'll need to include your ACME Directory URL with External account binding (EAB) in your ACME client certificate request command. Below is an example using CertBot:

```
sudo certbot --apache --register-unsafely-without-email --eab-kid "YOUR-KEY-IDENTIFIER" --eab-hmac-key "YOUR-HMAC-KEY" --server "YOUR-ACME-URL" -d FQDN
```

More information: https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/acme-user-guide/

Discovery and Automation API

Discovery API is a powerful API that allows you to scan your network using sensors and find all your internal and public facing SSL/TLS certificates regardless of the issuing Certificate Authority (CA). More information: https://dev.digicert.com/discovery-api/

The DigiCert Automation API is a powerful API that allows you to automate certificate enrollment and installation on your devices. The Automation API gives you complete control to configure automation profiles and manage automation activities. Use it to access all of the features of automation that are available in CertCentral, without needing to log in to the platform.

Depending on the host where your certificate is installed, you can use the Automation API to set up agent-based or sensor-based (agentless) automation.

More information: https://dev.digicert.com/automation-api/