DigiCert® Discovery: Install a sensor and run a scan

Last updated March 13, 2019

DigiCert® Discovery: Install a sensor and run a scan

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Document creation date: March 13, 2019

Legal Notice

DigiCert, Inc.
2801 North Thanksgiving Way Ste. 500
Lehi, Utah, 84043
https://www.digicert.com
Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Table of Contents

Introduction

Discovery uses sensors to scan your network to can find all your internal and public facing SSL/TLS certificates regardless of the issuing CA. These sensors are small software applications that you install in strategic locations.

Each scan is linked to one sensor. Scans are configured to examine specific fully qualified domain names (FQDNs), IP addresses, and port combinations for the presence of SSL/TLS certificates. Scans can be configured to run immediately, once – at a specified time, or multiple times – on a set schedule.

These scans provide detailed information about the certificates on your network:

- Common name
- Expiration date
- Certificate status
- Issuing certificate authority
- Ports and IP addresses of the certificate host
- Certificate security rating
- Server security issues
- TLS/SSL vulnerabilities

Scans can also be used to determine the operating system of your server host, the open IP addresses and ports, and the server host of the IP addresses.

To download a pdf version of the guide, click Discovery: Install a sensor and run a scan.

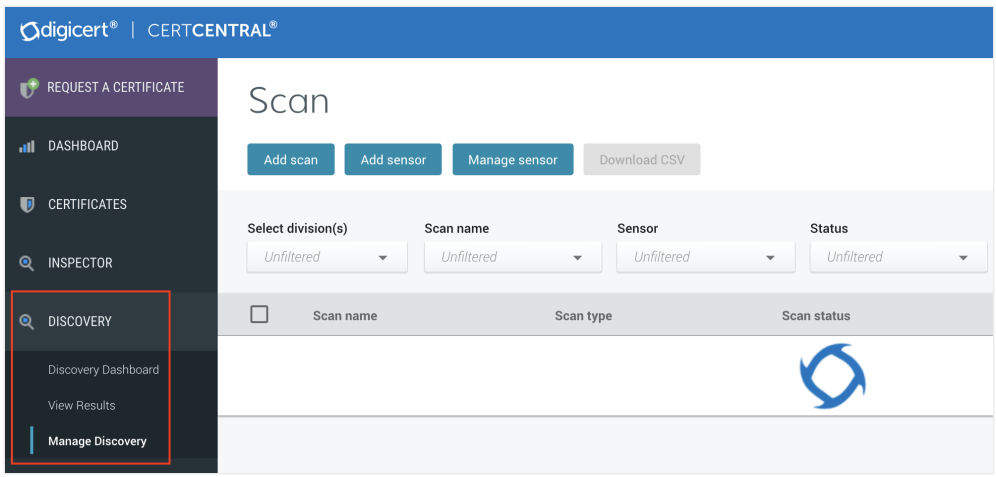
(Source: Discovery Dashboard in CertCental)

Discovery prerequisites

Before you start, make sure you have the required permissions to complete the necessary tasks.

Manage Discovery

To manage Discovery (download a sensor, set up a scan, view a scan's results, etc.) in your CertCentral account, you must be an account **administrator** or **manager**. All other roles lack the permissions to access Discovery.



(Source: Manage Discovery in CertCentral)

Install sensors

To install a sensor on a computer or virtual machine, you only need administrator permissions to the computer (for example, on Linux have sudo access).

Activate sensors

After you've installed the sensor on the computer or virtual machine, you'll need to activate the sensor. To activate a sensor, you'll a CertCentral account with permissions to access the division you want to assign the sensor to.

> **Info:** If you are using divisions in your CertCentral account, you have the ability to restrict users to specific divisions. Make sure the user tasked with activating the sensor can access the division you want to assign the sensor to.

Sensor installation requirements

Before you install a sensor on a computer in your network, verify the computer meets the minimum hardware and software requirements. DigiCert Sensors also have deployment and network requirements that must be met before running your first scan.

Network requirements

For a sensor to be configured successfully, the host names for the sensor's host device must be resolvable. For example, to resolve the host name on a Red Had Enterprise Linux server, you should add it to /etc/hosts (for non-standard configurations).

The sensor host must have access to:

1. **CertCentral cloud service**
   Sensors must be able to communicate with CertCentral cloud to receive instructions on when to run scans and to send inventory updates when new certificates are discovered.
   1. Outbound HTTP (port 80) and HTTPS (port 443)
      For direct or proxy access communications with the CertCentral cloud service, a sensor host must have access to the outbound HTTP (port 80) and HTTPS (port 443).
   2. CertCentral cloud service IP address
      If you are using a firewall, you need to open the firewall to IP:64.78.193.234 and 45.60.125.229. Failing to do this blocks the sensor from relaying scan information to Discovery in CertCentral.
2. **Targeted IP addresses**
   The firewall rules or Access Control Lists must allow the sensor to reach the target IP addresses you want scanned.

Deployment requirements

Install the sensor where it can access the fully qualified domain names (FQDNs) and IP addresses you want scanned. We recommend installing one sensor per uninterrupted network segment.

You only need additional sensors if your network:

- Is segmented by firewalls or routers
- Has multiple LANs or network segments

Additional sensors may also be useful when scanning a large number of IP addresses and ports. Splitting large IP ranges across multiple scans allows you to decrease the impact of scans on your network resources and to complete scans more quickly.

Hardware and software requirements

Red Hat Enterprise Linux 6.x and 7.x

- Root privileges
- 64-bit version and US locale required
- 2 GB RAM (4GB RAM recommended)
- 2 GB free disk space (minimum)

Microsoft Windows 7, 8, 8.1, 10, Server 2012, and Server 2016

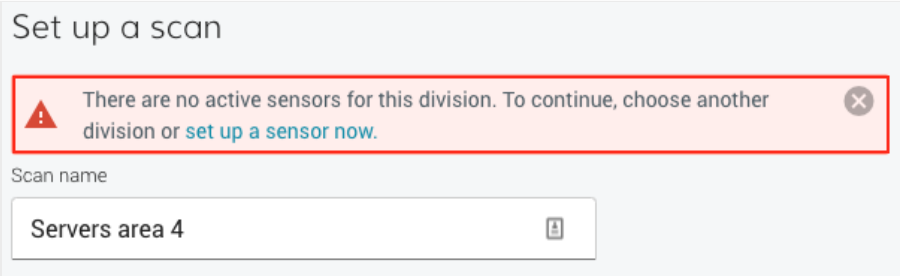
- Run as administrator
- 64-bit version
- Microsoft .NET Framework 4.x
- 2 GB RAM (4GB RAM recommended)
- 2 GB free disk space (minimum)

VMware ESX/ESXi 5.x

- Administrator access
- 2 GB RAM (4GB RAM recommended)
- 30 GB free disk space

Install a sensor

Before you can scan your network and begin using Discovery to manager your SSL/TLS certificates, you must install a sensor. A sensor is required to set up a scan.



(Source: Discovery sensor warning in CertCentral)

Depending on the size of your network and how it's segmented, you may need to install multiple sensors to get an accurate report on all your SSL/TLS certificates.

Info: Are you planning to install the DigiCert Sensor on a computer that requires a proxy server to communicate outside your network?

Verify the sensor will be able to relay its findings back to the CertCentral cloud service. See Configuring a sensor to use a proxy server for communications.

Linux: Install a sensor

Use these instructions to download, install, and activate the sensor on Red Hat Enterprise Linux 6.x and 7.x. These instructions assume you have some experience working with Linux systems.

Info: **Instruction summary:**
Extract the .tar.gz file to a specified folder, run ./start.sh, then follow the prompts to activate the sensor.

1. **Download and install the sensor**
    a. In your CertCentral account, in the sidebar menu, click **Discovery > Manage Discovery**.
    b. On the Scan page, click **Add sensor**.
    c. On the Set up a sensor page, under Download a discovery sensor, in the Linux section, click **Download** to download the installation file (.tar.gz).

Info: You must have administrator permissions to complete sensor installation.

2. **Create an installation directory to install the sensor**
    a. Log on to your Linux server as a root user
    For example:
    ```
    $ su
    Password: ****************
    #
    ```
    b. Create the installation directory
    For example:
    ```
    mkdir ccsensor
    ```
    c. Navigate to the installation directory and extract the sensor .tar.gz file.
    For example:
    ```
    cd ccsensor
    tar -xzvf <sensor-file>.tar.gz
    ```
    Where **ccsensor** is the sensor installation directory and **<sensor-file>** is the name of the file.

3. **Activate the sensor**

    You can activate the sensor now or later. However, you must activate the sensor before you can use it to set up a scan.

    a. Navigate to the installation directory and run **start.sh**, making sure you have root or admin permissions on the server.
    For example:
    ```
    cd ccsensor
    ./start.sh
    ```
    Where **ccsensor** is the sensor installation directory.

b. When asked to proceed with authentication, type **y** and enter your CertCentral **username** and **password**.
   Once you're authenticated, the installer retrieves the divisions you have access to.
c. Select the division you want to assign the sensor to.

Info: If you don't have any divisions in your account, we will return the name of the organization used to set up your CertCentral account.

Warning: You must select a "division". If you don't, you won't be able to set up a scan using this sensor. If you don't have divisions in your account, select the name of your organization returned after you were authenticated.

4. **(Optional) Rename the sensor**

   When using multiple sensors, you may want to rename the sensors to make tracking/identifying them easier.

   a. In your CertCentral account, in the sidebar menu, click **Discovery > Manage Discovery**.
   b. On the Scan page, click **Manager sensor**.
   c. On the Manage sensors page, in the **Sensor Name** column, click the IP address link of the server you installed the sensor on.
   d. On the sensor details page, in the **Nickname** box, enter a nickname for the sensor and click **Save**.
   e. On the Manage sensors page, use the nickname to locate the sensor.

5. You can now set up a scan using this sensor!

Microsoft Windows: Install a sensor

Use these instructions to download, install, and activate the sensor on Microsoft Windows 7, 8, 8.1, 10, Server 2012, and Server 2016 systems. These instructions assume you have working experience with the Microsoft Windows or Server systems.

1. **Log on to your Windows computer**

Info: You must have administrator permissions to complete sensor installation.

2. **Download the sensor installer file**

   a. In your CertCentral account, in the sidebar menu, click **Discovery > Manage Discovery**.
   b. On the Scan page, click **Add sensor**.
   c. On the Set up a sensor page, under Download a discovery sensor, in the Windows section, click **Download** to download the installation file (.zip).
   d. Save the file to your Windows computer, making sure to note the location.

e. Extract the contents of the zip file so you can run the executable file (.exe).

3. **Install the sensor on you Windows computer**

   a. Run the installer executable file as an administrator.
   Right click on the sensor .exe file and select **Run as administrator**.
   b. The DigiCert Sensor Setup wizard checks your Windows computer verifying that it meets the minimum requirements.
   c. After you accept the **End-User license agreement** terms and select an installation folder, the wizard installs the sensor as a Windows service.

Note: By default, the wizard installs the sensor in `C:\Program File\DigiCert\`.

Info: You can activate the sensor now or later. However, you must activate the sensor before you can set up a scan with it. If you choose to activate the sensor later, see Microsoft Windows: Activating or starting a sensor.

4. **Activate the sensor**

   Now that the sensor is installed on your Windows computer, you are ready to activate it. DigiCert recommends using the wizard to activate the sensor now.

   a. Select **CertCentral** and sign in to your account.
   Note: You must be an administrator or manager in your CertCentral account to activate the sensor.
   b. Once you're authenticated, the installer retrieves the divisions you have access to.
   c. Finally, select the division you want to assign the sensor so the wizard can activate the sensor.

Info: If you don't have any divisions in your account, we will return the name of the organization used to set up your CertCentral account.

Warning: You must select a "division". If you don't, you won't be able to set up a scan using this sensor. If you don't have divisions in your account, select the name of your organization returned after you were authenticated.

5. **Start the sensor**

   Now that the sensor is installed and activated, you are ready to start it. DigiCert recommends using the wizard to start the sensor now.

   To start the sensor and complete sensor installation, check **Start DigiCert Sensor** and click **Finish**.

Info: You can start the sensor now or later. However, you must start the sensor before you can set up a scan with it. If you choose to start the sensor later, see Microsoft Windows: Activating or starting a sensor.

6. **(Optional) Rename the sensor**

   When using multiple sensors, you may want to rename the sensors to make tracking/identifying them easier.

   a. In your CertCentral account, in the sidebar menu, click **Discovery > Manage Discovery**.
   b. On the Scan page, click **Manager sensor**.
   c. On the Manage sensors page, in the **Sensor Name** column, click the IP address link of the server you installed the sensor on.
   d. On the sensor details page, in the **Nickname** box, enter a nickname for the sensor and click **Save**.
   e. On the Manage sensors page, use the nickname to locate the sensor

7. You can now set up a scan using this sensor!

Virtual appliance: Install a sensor

Use these instructions to download the sensor, deploying the virtual appliance, and configuring the virtual appliance sensor on VMware ESX/ESXi 5.x systems. These instructions assume you have working experience with VMware systems.

1. **Download the sensor installer file**

   a. In your CertCentral account, in the sidebar menu, click **Discovery > Manage Discovery**.
   b. On the Scan page, click **Add sensor**.
   c. On the Set up a sensor page, under **Download a discovery sensor**, in the Virtual appliance section, click **Download** and download the installation .ova file.
   d. Save the .ova file to your VMware computer, making sure to note the location.

Info: You must have administrator permissions to complete sensor installation.

2. **Deploy the virtual appliance**

   The virtual appliance must be a complete VMware image with a Linux operating system.

   a. On your vSphere Client, open the Deploy OVF Template (in the top menu, click **File > Deploy OVF Template**).
   b. Use the Deploy OVF Template wizard to deploy the appliance.
   c. On the Source page, under Deploy from a file or URL, click **Browse** to find the sensor .ova file.
   d. On the OVF Template Details page.
   e. On the End User License Agreement page, read through the agreement and click **Accept**.

f. On the Name and Location page, in the **Name** box enter a name for the deployed image. Under Inventory Location, specify a location for the image.
g. On the Specify a Specific Host page, under Host Name, select the ESX server where you want to deploy the image.
h. On the Storage page, select a storage destination for the virtual machine files.
i. On the Disk Format page, select the format for storing the virtual disks.
j. On the Network Mapping page, select the network you want the deployed image to use.
k. On the Properties page, enter and confirm the password for the **CLI "admin" User Password** and for the **CLI Privilege Mode Password**.
l. On the Ready to Complete page, click **Finish** to deploy the virtual appliance.

3. **Configure the virtual appliance**

a. Select the newly deployed appliance and click Power on the virtual machine.
b. Navigate to the **Console**.
c. If prompted, change the password for the root user and cwsuser.
d. If the virtual appliance can't find a DHCP server, you must run the **assignIpHostname** tool to assign a static IP before you continue to the next step.
Run the assignIpHostname tool
    i. Sign in as ccuser. Then switch to the root user.
    For exmple:
    ```
    [ccuser@localhost]$ su -
    Password: *************
    ```
    ii. Run the **assignIpHostname** command and follow the prompts.
    ```
    [root@localhost]# assignIpHostname
    Enter the network mode (D=DHC{P,S=STATIC): S
    ```
    Note: Make sure to provide the IP address and the hostname.
e. Set up the SSH connection to the virtual appliance as the cwsuser, then switch to the root user.
f. The sensor is installed to **/opt/digicert/.**

4. **Activate the sensor**

You can activate the sensor now or later. However, you must activate the sensor before you can use it to set up a scan.

a. Navigate to the installation directory and run `start.sh`, making sure you have root or admin permissions on the server.
For example:
```
cd ccsensor
./start.sh
```
Where **ccsensor** is the installation directory.
b. When asked to proceed with authentication, type **y** and enter your CertCentral **username** and **password**.
Once you're authenticated, the installer retrieves the divisions you have access to.
c. Select the division you want to assign the sensor to.

d. When sensor activation and startup is complete, you will see a success message letting you know.

Info: If you don't have any divisions in your account, we will return the name of the organization used to set up your CertCentral account.

Warning: You must select a "division". If you don't, you won't be able to set up a scan using this sensor. If you don't have divisions in your account, select the name of your organization returned after you were authenticated.

5. **(Optional) Rename the sensor**

   When using multiple sensors, you may want to rename the sensors to make tracking/identifying them easier.

   a. In your CertCentral account, in the sidebar menu, click **Discovery > Manage Discovery**.
   b. On the Scan page, click **Manager sensor**.
   c. On the Manage sensors page, in the **Sensor Name** column, click the IP address link of the server you installed the sensor on.
   d. On the sensor details page, in the **Nickname** box, enter a nickname for the sensor and click **Save**.
   e. On the Manage sensors page, you will use the nickname to locate the sensor.

6. You can now set up a new scan with the sensor!

Configure a sensor to use a proxy server for communications

Use these instructions to configure a sensor to use a proxy server so it can communicate with the CertCentral cloud service.

For a scan to run successfully, its sensor must be able to communicate with CertCentral cloud service to receive instructions associated with certificate discovery and to report on certificate inventory updates.

Problem

If you installed the DigiCert Sensor on a computer that requires a proxy server to communicate outside your network, the sensor can't relay its findings back to Discovery in your CertCentral account preventing you from seeing the results of the scan.

Solution

You need to configure the DigiCert Sensor to use a proxy server so it can communicate with Discovery in your CertCentral account allowing you to see the results of the scan.

Configure a sensor to use a proxy

1. On the computer you installed the sensor on, use a text editor (such as vi or Notepad) to create a **proxy.properties** file with these configuration settings:

Setting	Description
enableProxy	To enable proxy access: true enables proxy access and false disables proxy access
httpHost	IP address of the proxy server used for HTTP communication
httpHostPort	Port number the proxy server uses for HTTP communications
httpAuthUser	Username required to authenticate the HTTP proxy (Basic Authentication only) – If required
httpAuthPassword	Password required to authenticate to the HTTP proxy (Basic Authentication only) – If required
httpsHost	IP address of the proxy server used for HTTPS communication
httpsHostPort	Port number the proxy server uses for HTTPS communications
httpsAuthUser	Username required to authenticate the HTTPS proxy (Basic Authentication only) – If required
httpsAuthPassword	Password required to authenticate to the HTTPS proxy (Basic Authentication only) – If required

For example

```
enableProxy=true
enableProxy=true
httpHost=123.123.123.123
httpHostPort=80
httpAuthUser=mypassword
httpAuthPassword=system01@Admin
httpsHost=125.125.125.125
httpsHostPort=443
httpsAuthUser=mypassword
httpsAuthPassword=system02@Admin
```

2. Add the configuration file to: `install_dir/config/proxy.properties`
3. Restart the sensor to encrypt the proxy passwords and upload the proxy information.

   Linux

   a. Navigate to `install_dir/cli`.
      Where **install_dir** is the sensor installation directory
   b. Run the command below.
      `./restart.bat`

   Windows

   a. Navigate to `install_dir/cli`.
      Where **install_dir** is the sensor installation directory
   b. Run the command below.
      `restart.bat`

Change proxy settings for a sensor

Use these instructions to change the proxy settings. As an example, we will change the proxy passwords.

1. On the computer you installed the sensor on, navigate to `install_dir/config/`.

   Where **install_dir** is the installation sensor installation directory

2. Open the proxy.properties file and make these modifications to change the proxy passwords:
   a. Replace httpAuthPasswordEncrypted with httpAuthPassword.
   b. Replace httpsAuthPasswordEncrypted with httpsAuthPassword.
   c. Add the proxy password values for these settings.
   d. Navigate to `install_dir/cli`.
      Where **install_dir** is the sensor installation directory
   e. Run the applyproxysettings command.
      Where **input_file** is the path and file name containing the proxy settings
      i. **Linux**
         `./applyproxysettings.sh -file input_file`
      ii. **Windows**
         `applyproxysettings.bat -file input_file`
   f. Restart the sensor to encrypt the proxy passwords and upload the proxy information.
      i. **Linux**
         - Navigate to `install_dir/cli`.
           Where **install_dir** is the sensor installation directory.
         - Run the command below
           `./restart.bat`
      ii. **Windows**
         - Navigate to `install_dir/cli`.
           Where **install_dir** is the sensor installation directory.
         - Run the command below
           `restart.bat`

Retrieve proxy settings for a sensor

Use these instructions to retrieve the proxy settings for a sensor.

Use the `getproxysettings` command to retrieve the existing proxy settings of a sensor. Then, you can save the settings in a separate file for future references.

1. On the computer you installed the sensor on, navigate to `install_dir/cli`.

   Where **install_dir** is the sensor installation directory

2. Run the `getproxysettings` command.

Linux

```
./getproxysettings.sh
```

Windows

```
getproxysettings.bat
```

Activate a sensor

Did you activate the sensor as part of the installation process? You can manually start the sensor on Linux and Microsoft Windows systems.

Info: Before you can use a sensor in a scan, that sensor must be activated.

Linux: Activate a sensor

Use these instructions to activate a sensor on Linux.

1. Navigate to the installation directory and run `start.sh`, making sure you have root or admin permissions to the server where the sensor is installed.

   For example:

   ```
   cd ccsensor
   ./start.sh
   ```

   Where **ccsensor** is the sensor installation directory.

2. When asked to proceed with authentication, type **y** and enter your CertCentral **username** and **password**.

   Once you're authenticated, the installer retrieves the divisions you have access to.

> **Info:** If you don't have any divisions in your account, we will return the name of the organization used to set up your CertCentral account.

3. Enter the division you want to assign the sensor to.

> **Warning:** You must select a "division". If you don't, you won't be able to set up a scan using this sensor. If you don't have divisions in your account, select the name of your organization returned after you were authenticated.

5. When sensor activation and startup is complete, you should see a success message letting you know.

Microsoft Windows: Activate or start a sensor

Use these instructions to activate or start a sensor on your Windows computer. The `start.bat` command can be used to activate and start the sensor or to just start the sensor.

1. Navigate to the `install_dir/cli`.

   Where **install_dir** is the sensor installation directory.

> **Info:** You must have administrator permissions to activate the sensor.

2. Run the command below.

   ```
   start.bat
   ```

3. When prompted, enter your CertCentral username and password.

   Once you're authenticated, the installer retrieves the divisions you have access to.

Info: If you don't have any divisions in your account, we will return the name of the organization used to set up your CertCentral account.

4. Enter the division you want to assign the sensor to.

Warning: You must select a "division". If you don't, you won't be able to set up a scan using this sensor. If you don't have divisions in your account, select the name of your organization returned after you were authenticated.

5. When sensor activation and startup is complete, you should see a success message letting you know.

Restart a sensor

If a sensor has technical problems, you can stop and restart a sensor to resolve any technical problems. The **restart** command stops the sensor and then immediately restarts it. The sensor then immediately resumes any scans or other activities that were in progress.

Linux: Restart a sensor

Use these instructions to restart a sensor on Linux.

1. Navigate to the installation directory and run `restart.sh`, making sure you have root or admin permissions to the server where the sensor is installed.

   For example:

   ```
   cd sensor
   ./restart.sh
   ```

   Where **ccsensor** is the sensor installation directory.

2. When sensor shutdown and restart are complete, you should see a success message letting you know.

Microsoft Windows: Restart a sensor

Use these instructions to restart a sensor on Windows.

Complete one of the tasks below to restart the sensor on your Window system.

Options 1: restart.bat command

1. Navigate to `install_dir/cli`.

   Where **install_dir** is the sensor installation directory

2. Run the command below.

   ```
   restart.bat
   ```

3. When sensor shutdown and restart are complete, you should see a success message letting you know.

Option 2: Windows Services manager

1. Open the Windows Services manager (services.msc).

   As an example, in Windows 10:

   a. Right-click on the start icon (Windows logo) and select run.
   b. In the Run window in the **Open** box, type ***services.msc*** and click **OK**.

2. In the Services window, locate and right-click on **DigiCert Sensor** and select **Restart**.

3. When sensor shutdown and restart are complete, you should see a success message letting you know.

Option 3: DigiCert app

1. Open the start menu and locate the DigiCert app.
2. In the app's menu, right-click on **Restart Sensor** and select **Run as Administrator**.
3. When sensor shutdown and restart are complete, you should see a success message letting you know.

Options 4: DigiCert Sensor

1. Open the Start menu and click **All Programs > DigiCert > DigiCert Sensor**.
2. In the sensor menu, right-click on **Restart Sensor** and select **Run as Administrator**.
3. When sensor shutdown and restart are complete, you should see a success message letting you know.

Set up a scan

Use these instructions to set up a scan.

Before you begin

Before you set up a scan, make sure all prerequisites are met. See Discovery prerequisites.

Additionally, you'll want to gather some information:

- The name of the sensor to use for the scan
- The division the sensor is assigned to (if you are using divisions in your account)
- The ports you want to use to scan your network
- The FQDNs and IP addresses you want to include in the scan
- If you're using Server Name Indication (SNI) to serve multiple domains from a single IP address

Run a scan now, schedule a scan to run once, or schedule the scan to run daily, weekly, or monthly.

1. **Go to the Add a scan page**
    a. In your CertCentral account, in the sidebar menu, click **Discovery > Manage Discovery**.
    b. On the Scan page, click **Add scan**.

2. **Set up your scan**

    On the Add a scan page, under Set up scan, provide the necessary scan information.

    a. **Scan name**
    Name your scan so you can easily identify it (names becomes more important when you have multiple scans).
    b. **Division**
    In the dropdown, choose the division with the sensor you want to use for the scan. Sensors are assigned to divisions. In the **Sensors** dropdown, you can only see the sensors assigned to the selected division.
    Note: If you aren't using divisions in your account, you won't see the drop-down list. You will see your organization name.

c. **Ports**
Specify which ports you want to use to scan your network for SSL/TLS certificates.
   i. Click **All** to include all ports in a specified range
   ii. Click **Default** to include ports commonly used for SSL/TLS certificates: 80, 443, 389, 636, 22, 143, 110, 465, 8443, 3389

d. **Enable SNI**
Are you using Server Name Indication (SNI) to serve multiple domains from .a single IP address?
Check this box to enable SNI scanning for the scan (limited to max 10 ports per server).
Note: An SNI scan may not have IP information as part of the results.

e. **Sensor**
In the dropdown, select the sensor you want to use for the scan.
Note: Because sensors are assigned to divisions, you can only see the sensors assigned to the division you selected in the **Division** dropdown. If you aren't using divisions in your account, you will see the sensors assigned to your organization.

f. **FQDNs / IP to scan**
Use the options below to add the FQDNs and IP addresses you want included in the scan.
   i. Enter the FQDNs and IP addresses you want to include in the scan and click **Include**
   You can include single IP addresses (10.0.0.1), a range of IP addresses (10.0.0.1-10.0.0.255), or an IP range in CIDR format (10.0.0.0/24).
   ii. Enter the IP address you want to exclude from a range of IP address (10.0.0.5, 10.0.0.150 , 10.0.0.20 -10.0.0.254) and click **Exclude**
   iii. To import the FQDNs and IP address from a .csv file, click **Import** from CSV.

g. When you are finished, click **Next**.

3. **When to scan**

   On the Add a scan page, under When to scan, configure you scan to run now or schedule it to run once, daily, weekly, or monthly.

   Note: Scans configure to run now start when you click **Save**.

   To set a limit for how long an unfinished scan should run before you stop it, check **Stop of scan time exceeds**.

4. **Settings**

   On the Add a scan page, under Settings, configure what you want to scan for.

   - **Optimize for best performance**
   This scan provides basic SSL/TLS certificate and server information along with any discovered critical TLS/SSL server issues. (Heartbleed, Poodle [SSLv3], FREAK, Logjam, DROWN, RC4, and POODLE [TLS]).
   This option is the default scan setting. Before you start customizing scans, we recommend running this scan first. After reviewing the results of the default scan setting, you can better determine what information you want included in your scans.

- **Choose what to scan**
  This option allows you to choose what to include in your scan (OS information, server application information, and critical and non-critical TLS/SSL server issues). Adding more options increases the scan's impact on network resources as well has how long it takes to complete it.

5. **Advanced settings**

   Scan performance

   Use the Scan performance options to configure how quickly the scan is completed or to limit the scans impact on network resources.
   Note: If a scan triggers a false alarm in intrusion detection systems (IDS) or intrusion protection systems (IPS), make sure to whitelist your scans in your IDS/IPS utilities. Also, configure your scan to run **Slow**, as slower scans are less likely to trigger false alarms. You may also need to whitelist the sensor from your firewall to allow communication to Digicert.com.

   - **Aggressive (complete scan quickly when network traffic is low)**
     Use this option to complete the scan quickly. Note that the scan will have a higher impact on network resources. The scan sends out a large number of scan packets to the network. However, Discovery caps how many packets are sent to prevent an unintended number of packets from being sent.
     Note: Using the aggressive setting may set off false alarms on Intrusion Detection System (IDS) or Intrusion Prevention Systems (IPS).
   - **Balanced (default)**
     Use this option to balance the speed of the scan and its effects on network resources.
   - **Slow (complete scan slowly with minimal impact on network resources)**
     Use this option to limit the impact of the scan on network resources and to reduce the number of IDS or IPS false alarms. The scan sends a few scan packets at a time and waits for a response before sending more packets.

   More settings

   - **Reduce firewall alarms by restricting TLS/SSL server checks**
     To identify TLS/SSL server issues (for example, Heartbleed), scans sometimes emulate a TLS/SSL server issue to make sure that the server is secure. Such emulations might trigger false firewall alarms on your network. To avoid such alarms, you can restrict the TLS/SSL server checks.
     Note: Use this option with the understanding that it may limit the effectiveness of your scan, as it may result in missed TLS/SSL server issues.
   - **Specify ports to scan to verify host availability**
     The first step in the scan process is to the ping the host to verify its availability.
     If Internet Control Message Protocol (ICMP) pings are disabled on a host, use this setting to specify the ports that can be scanned to verify host availability. The fewer ports specified, the faster your scan.

Note: The ports specified here are only used to verify the host availability. The ports specified while setting up or editing the scan are used for certificate discovery.

6. When you are finished, click **Save.**

   Scans set to run now start when you click **Save**.

Congratulations! You've successfully set up a scan. Your scan will now run as scheduled. Scan completion time depends on network size, and the scan performance setting selected during set up.

To manage your scans, go to the **Scan** page (in the sidebar menu, click **Discovery > Manage Discovery**).

To view scan details or to modify scan settings, go to the scan's details page, (on the Scans page, click the scan name link).

- On the **Discovery location** and **Scan settings** tabs, view or modify scan settings.
- On the **Scan activity** tab, view current and past scan details such as start time, duration, scan status, and actions.