Discovery 2.4
Administration Guide
Document issue: 4.0
Date of issue: June 2017
Entrust Discovery overview ............................................. 7

Entrust Discovery components ......................................... 8
  Entrust Discovery Agent ................................................. 8
    Information collected by an Entrust Discovery scan ........... 8
  Entrust Discovery Manager .......................................... 9
  Entrust Discovery Certificate Scanning Utility ................. 10
Deploying Entrust Discovery ........................................... 11
  Entrust Discovery Manager with one or more Discovery Agents 12
  Entrust Discovery with Certificate Services ...................... 13
  Discovery Agents deployed without a Discovery Manager ...... 14
Licensing ........................................................................ 16

Getting started. ............................................................. 17

Installing Entrust Discovery .............................................. 18
  Installing an Entrust Discovery Agent on Red Hat Enterprise Linux 18
  Installing an Entrust Discovery Agent on Microsoft Windows .... 19
  Installing the Entrust Discovery Manager on Red Hat Enterprise Linux 20
  Installing the Entrust Discovery Manager on Microsoft® Windows 21
  Installing the Entrust Certificate Scanning Utility (Optional) ... 21
Configuring communication .............................................. 22
  Opening the Discovery Manager or Agent Interface ............. 22
    Opening the Discovery Manager interface (from a premises
    installation) ........................................................... 23
    Opening the Discovery Agent interface ......................... 23
  Importing a Discovery Manager certificate license file ........ 23
  Registering Discovery Agents with the Discovery Manager ...... 25
  Configuring communication between the Discovery Manager and Discovery
  Agents ........................................................................ 26
Scanning devices and importing certificate information

- Configuring Discovery Agents to scan for certificates
- Configuring scan parameters
- Creating a preconfigured list of hosts
- Running a scan manually
- Manually uploading a scan to the Discovery Manager or Certificate Services

- Using the Entrust Certificate Scanning Utility
- Uploading the Scan Utility results
- Manually importing certificates and Entrust Security Manager Reports
- Importing a report from Entrust Authority Security Manager

Managing certificates

- Monitoring scan information from the Discovery Agent
- Viewing detailed certificate information
- Assigning a management state to a certificate
- Deleting a certificate
- Configuring management options for an individual certificate
- Changing certificate details and options in bulk
- Configuring email notification and reports
- Configuring reports
- Creating custom fields
- Assigning a friendly name to a Certification Authority (CA)
- Exporting a certificate summary report
- Configuring rules
- Types of rules
- Configuring an issuer rule for certificate management
- Configuring a notice rule
- Configuring a certificate rule

Entrust Discovery administration

- Setting filter, view, and policy options (Premises only)
- Filters
- Policies
Views ........................................... 87
Setting filters ................................. 87
   Editing a saved filter or policy, or creating a policy .......... 91
   Adding an intermediate CA certificate to the list of filters .... 93
   Configuring a view .......................... 93
Creating and using charts (Premises only) ...................... 95
Using organizations to manage certificates (Premises only) ... 101
User account options (Premises only) .......................... 103
   Adding a user account .......................... 103
Using Microsoft Active Directory (Premises only) ............... 108
   Configuring the connection, domain, and search base ....... 108
   Setting caching for credentials ..................... 110
   Login rules for Active Directory ..................... 110
      Base DN ..................................... 112
      Required Entry Properties ..................... 112
      Group ....................................... 112
Changing a user account password (premises only) ............. 114
Adding or editing a Web service account (Premises only) ....... 116
Uninstalling Entrust Discovery (Premises only) .................. 118
   Uninstalling Entrust Discovery from a Microsoft Windows platform 118
   Uninstalling Entrust Discovery from a Red Hat Linux platform 118
Manually stopping and starting the application (Premises only) ... 119
Monitoring the Agent (Premises only) .......................... 120
Viewing the license information (Premises only) ................. 121
Back-up and restoring Discovery (Premises only) ............... 122
Database maintenance (Premises only) .......................... 125
Viewing Discovery logs and System Notices (Premises only) ... 126
Viewing detailed version information (Premises only) ......... 127
Changing the default listen port for the Agent or Manager (Premises only) 128
Using an SSL certificate signed by a CA (Premises only) ....... 130
Listing certificate location by hostname or IP address (Premises only) 132
Configuring the Switch or renew button (Premises only) ....... 133

INDEX ........................................... 135
Entrust Discovery overview

Entrust Discovery allows an administrator to scan a network, or specific portions of a network, for the most recent information about the certificates protecting servers or in user or computer certificate stores. Using the information collected by Entrust Discovery, the administrator can track:

- the location of each certificate
- details about the type, origin, and expiry date of each certificate

Using the Discovery Manager's advanced reporting system, users can easily determine details about certificates in the network. Discovery also allows users to send standard or custom reports and reminders to specific users using a flexible system of rules and filters.

Note:
The term user (lower case u) is used throughout this guide to refer to any account type (Super Administrator, Administrator, or User). The term User (upper case U) refers specifically to the User account type. The term administrator (lower case a) is used to refer to any administration account (Administrator or Super Administrator).

This chapter discusses the following topics:

- “Entrust Discovery components” on page 8
- “Deploying Entrust Discovery” on page 11
- “Licensing” on page 16
Entrust Discovery overview

Entrust Discovery components

Entrust Discovery is composed of the “Entrust Discovery Agent”, the “Entrust Discovery Manager”, and optionally, the “Entrust Discovery Certificate Scanning Utility”. A Web service is also available.

- Discovery Agents can be obtained free-of-charge from Entrust, and used without a Discovery Manager to scan for certificates. However, only a summary of the data obtained by a scan can be viewed directly from the Agent.

- Discovery Manager
  - Discovery Manager features include full access to detailed information about individual certificates and certificate management capability. Talk to an Entrust Sales agent about obtaining the Discovery Manager and licenses.

- The Certificate Scanning Utility is available without charge to Entrust Discovery Manager users who have purchased certificate management licenses.

- The Entrust Discovery Manager Web Service allows customer applications to interact with Discovery Manager for get, put, and post operations. For detailed information about using the Web service see the Entrust Discovery Manager Web Service Guide.

Entrust Discovery Agent

Discovery Agents use a Web-based interface, allowing remote access by administrators. Scans are configured separately on each Agent. After a scan is created, it can be saved and reused, either on a schedule, or started manually by an administrator.

Discovery Agents can be configured to:

- scan a specific IP address or range of IP addresses
- exclude specific IP addresses or ranges of IP addresses
- scan a specific port or ranges of ports
- run a scan as required (manually) or run a scheduled scan on an hourly, daily, weekly, or monthly basis
- transfer detailed data to the Discovery Manager, either automatically or by packaging it for manual transfer by the administrator
- work with Active Directory to manage users

Information collected by an Entrust Discovery scan

When Entrust Discovery Agent locates a certificate during a scan, it collects detailed information about the certificate. A partial list of the information collected is shown below

- the certificate issuer
• subject DN of the certificate
• key algorithm and length
• creation and expiry date
• host and port (or hosts and ports if it is installed in multiple locations)
• the port state

Note:
Detailed information about individual certificates can only be viewed using the Discovery Manager. The Discovery Agent displays a summary of the information.

Entrust Discovery Manager
The Discovery Manager uses a Web-based interface, allowing remote access by administrators. Using the Discovery Manager you can correlate, filter, and view the information from Discovery Agents and, optionally, from Certificate Scanning Utility installations. Additionally, the Discovery Manager can help you to manage your certificates by:
• allowing you to group and manage certificates according to the organization to which they are assigned
• allowing you to assign user roles with different levels of permissions—some options only appear to users with the correct permissions
• allowing you to use rules to automate some management tasks
• consolidating the certificate information acquired by scans from all Discovery Agents and optionally, from the Certificate Scanning Utility and reports from Entrust Authority Security Manager CAs
• manually importing certificates located on machines that cannot be scanned (for network reasons or due to corporate policy, for example)
• displaying either a summary of the data about all certificates, or detailed information about each certificate
• automatically emailing notifications about the status of certificates to designated certificate owners and administrators
• allowing you to specify the default number of days before expiry to begin flagging certificates for alerts
• allowing you to add your own information about the certificate to help you manage it
• allowing you view the certificate
• working with Active Directory to manage users
Detailed information available from Discovery Manager

The Entrust Discovery Manager helps you to manage certificates by allowing you to access or configure the following information:

- a friendly name for the certificate (a meaningful name chosen by the administrator)
- the Distinguished Name (DN) of the Certification Authority (CA) that issued the certificate
- the location of the certificate (for example, the port where an SSL certificate is located)
- the subject DN of the certificate
- the key algorithm and length (for example, RSA-2048)
- the creation and expiry date of the certificate
- the Key usage (for example, digital signature)
- the Extended key usage (object ID of the extended usage)
- the number of subject alternative names in the certificate
- a list of SubjectAltNames (Subject Alternative Names): often used to add the names of hosts protected by the certificate
- the last time and date that the certificate was found by the Discovery Agent
- the trust path and root certificate
- the history (for example, when, and on what host and port, the certificate was first found)
- the contact name, location, and information of the certificate owner (originally specified by an administrator)
- organization that certificates are assigned to

Entrust Discovery Certificate Scanning Utility

Entrust Discovery Certificate Scanning Utility is a self-contained application that scans the certificate stores in Microsoft Windows and exports the results to XML files. The files can be uploaded to the Entrust Discovery Manager either individually or as zipped archives.

The application includes options for scanning a user's or computer's Personal, Other People, Trusted People, Intermediate Certification Authorities, and Trusted Root Certification Authorities certificate stores.

For information about deploying the utility see “Using the Entrust Certificate Scanning Utility” on page 41.
Deploying Entrust Discovery

Entrust Discovery can be deployed in the following configurations:

- an Entrust Discovery Manager with one or more Discovery Agents hosted on machines in your network (premises installation architecture)
- Entrust Discovery with Certificate Services where the discovered certificates can be managed by Certificate Services, a cloud-based service with advanced certificate management capability. Agents are hosted on machines in your network.
- one or more Discovery Agents deployed without a Discovery Manager hosted on machines in your network with no Discovery Manager (Agent only architecture)
**Entrust Discovery overview**

**Entrust Discovery Manager with one or more Discovery Agents**

Using multiple Discovery Agents with a Discovery Manager increases the scope and efficiency of the deployment. In Figure 1, each Discovery Agent monitors a partitioned subnet in the network and transfers the collected information to the Discovery Manager.

**Figure 1:** Distributed Entrust Discovery architecture

Each Discovery Agent finds certificates by scanning IP addresses or host names in a part of the network, using a specific port number or range of port numbers. IP addresses and port numbers are configured by the administrator. All Discovery Agents can be configured to send information from each scan to the Discovery Manager. Optionally, the Certificate Scanning Utility can be installed on computers in the network to obtain information about certificates located in certificate stores.
**Note:**

Discovery Agent and Discovery Manager can be installed on the same host.

**Entrust Discovery with Certificate Services**

If you already use the Entrust Certificate Services to manage the certificates in your network, Agents can collect data about certificates on your network and sent the information directly to Certificate Services. Certificate Services provides management capability for your certificates.
**Discovery Agents deployed without a Discovery Manager**

Entrust Discovery Agents cannot manage certificates without a Discovery Manager or Certificate Services, but they can be used to produce a summary report of the status of certificates in your network. A summary of the findings from each scan is available.
from the Agent that performed it. The summary data is categorized by Certification Authority (CA) and expiry date. Detailed information about the certificates is available only from an Entrust Discovery Manager.

**Figure 3:** No Manager—summary information available at each Agent
Licensing

To use the Discovery Manager to manage certificates, you must purchase certificate management licenses from Entrust. Contact your Entrust representative for information about purchasing licenses.

Entrust offers several types of licenses for managing certificates:

- **Premises subscription**
  - designed for use with a Discovery Manager hosted on a machine in your network
  - includes an expiry date based on your subscription.
  - software support is included in the price

- **Premises perpetual**
  - designed for use with a Discovery Manager hosted on a machine in your network
  - no expiry date

For information about using Entrust Certificate Services, see: [https://www.entrust.com/solutions/certificate-services/](https://www.entrust.com/solutions/certificate-services/) or contact your Entrust representative.

---

**Note:**

The functionality available in the user interface depends on licensing. This guide includes information about features that do not work as documented if you do not have valid licenses.
Getting started

To start using Entrust Discovery:

• Install the Discovery Agent software (all architectures) and the Discovery Manager software (premises architecture users only) on a compatible host. Discovery Agent and Manager servers can be installed on a Microsoft or Red Hat operating system. For details see the section “Installing Entrust Discovery” on page 18.

• Configure secure communication between the Discovery Agent and the Discovery Manager (Certificate Services and premises architecture users). For details see the section “Configuring communication” on page 22.
Installing Entrust Discovery

Entrust Discovery components (Agent, Manager, or both) is available for a Linux or Microsoft® Windows OS. See the product release notes for specific platform version information. Users with Entrust Support Web access will find the most up-to-date information about supported platforms on the Entrust TrustedCare Web pages.

Certificate Services users do not need to install Discovery Manager. For information about this architecture, see “Entrust Discovery with Certificate Services” on page 13.

In general, the Entrust Discovery Manager and Agents are accessed remotely so access to the server host can be limited to specific users. To help secure your data, administrator access to a machine hosting Discovery should be limited to Discovery Super Administrators. For information about roles, see “User account options” on page 102.

Note:

By default, Discovery Manager uses port 27535 and Discovery Agent uses port 27534. These ports can be changed after the software is installed. For information about changing the port used to contact an Agent or Manager, see “Changing the default listen port for the Agent or Manager” on page 124. If you change the port used to contact the Manager Agent or Manager substitute the new port number in the procedures in this guide.

Topics in this section include:

- “Installing an Entrust Discovery Agent on Red Hat Enterprise Linux” on page 18
- “Installing an Entrust Discovery Agent on Microsoft Windows” on page 19
- “Installing the Entrust Discovery Manager on Red Hat Enterprise Linux” on page 20
- “Installing the Entrust Discovery Manager on Microsoft® Windows” on page 21

Attention:

Discovery upgrades (both Agent and Manager) cannot be installed over existing Discovery installations. Uninstall any pre-existing Discovery software before installation. Your data will be preserved.

Installing an Entrust Discovery Agent on Red Hat Enterprise Linux
Before installing the Discovery Agent software, add the `compat-libstdc++-33` library to your installation. This library is not included in the default Red Hat installation but can be obtained from the Red Hat Enterprise Linux installation disk.

For example, in the Red Hat version 6.2 this library is named `compat-libstdc++-33-3.2.3-69.el6.i686.rpm` (or `compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm` for the 64 bit version of the OS).

For information about changing the port after installation, see “Changing the default listen port for the Agent or Manager” on page 124.

**To install an Entrust Discovery Agent**

1. Download the Discovery Agent software bundle to your machine and extract the contents.

2. Either:
   - Double-click the Discovery Agent RPM file and follow the instructions in the wizard.
   Or:
   - Open a terminal window on your Linux machine.
   - Change directory to the location of the Discovery Agent installation file.
   - Type the command:
     ```
     rpm -ivh <name of installation file>
     ```
     For example:
     ```
     rpm -ivh discovery-agent-2.4-0.i386.rpm
     ```
     The Discovery Agent software is installed in the file system under `/opt`.

To open the application Web interface and begin configuring the software, see the section “Configuring communication” on page 22.

**Installing an Entrust Discovery Agent on Microsoft Windows**

Entrust Discovery Agent for the Windows platform is installed from the executable file `eed_agent_<version>_setup_win32.exe`.

By default the Entrust Discovery Agent uses port 27534. During the installation, the installer checks to see if this port is in use, and issues a warning if it is not available. The warning does not result in an installation failure, however until the port is released for use by the Discovery Agent or the port is changed, the software will not work correctly. For information about changing the port after installation, see “Changing the default listen port for the Agent or Manager” on page 124.
To install Entrust Discovery Agent
1. Download the Discovery Agent software bundle to your machine and extract the contents.
2. Double-click the Discovery Agent executable.
3. Page through the installation wizard. Accept the defaults or choose a different destination folder for the software.
4. In the Pre-Installation summary page, click Install.
5. In the Install complete page, click Done.

To open the application Web interface and begin configuring the software, see the section “Configuring communication” on page 22.

Installing the Entrust Discovery Manager on Red Hat Enterprise Linux

Before installing the Discovery Manager software, add the compat-libstdc++-33 library to your installation. This library is not included in the default Red Hat installation, but can be obtained from the Red Hat Enterprise Linux installation disk.

For example, in the Red Hat version 6.2 this library is named compat-libstdc++-33-3.2.3-69.el6.i686.rpm (compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm for the 64 bit version of the OS).

For information about changing the port after installation, see “Changing the default listen port for the Agent or Manager” on page 124.

To install Entrust Discovery Manager
1. Download the Discovery Manager software bundle to your machine and extract the contents.
2. Either
   a. Double-click the Discovery Manager RPM file and follow the instructions in the wizard. The installer will complete the installation.
   Or
   a. Open a terminal window on your Linux machine.
   b. Change directory to the location of the Discovery Manager installation file.
   c. Type the command:
      
      rpm -ivh <name of installation file>
      
      For example:
      
      rpm -ivh discovery-manager-2.4-0.i386.rpm
The Discovery Manager software is installed in the file system under `/opt`.
To open the application Web interface and begin configuring the software, see the section “Configuring communication” on page 22.

Installing the Entrust Discovery Manager on Microsoft® Windows

Entrust Discovery Manager for the Windows platform is installed from the executable file `eed_manager_setup_win32.exe`.

The Entrust Discovery Manager uses port 27535. During the installation, the installer checks to see if the port is in use and will issue a warning if it is not available. The warning does not result in an installation failure, however until the port is released for use by the Discovery Manager or the port is changed, the software will not work correctly.

For information about changing the port after installation, see “Changing the default listen port for the Agent or Manager” on page 124.

To install Entrust Discovery Manager
1. Download the Discovery Manager software bundle to your machine and extract the contents.
2. Double-click the Discovery Manager executable.
3. Page through the installation Wizard, you can accept the defaults or choose a different destination folder for the software.
4. In the Pre-Installation Summary page, click Install.
5. In the Install complete page, click Done.

To open the application Web interface and begin configuring the software, see the section “Configuring communication” on page 22.

Installing the Entrust Certificate Scanning Utility (Optional)

The scanning utility is installed on individual computers in the network. It is a command line utility.

To install the Certificate Scanning Utility
1. Download the scanning utility software ZIP file to your machine and extract the contents.
2. Save the executable to a convenient folder on the computer to be scanned (where the certificate store is located).

For information about using the utility see the section “Using the Entrust Certificate Scanning Utility” on page 41.
Getting started

Configuring communication

The section explains how to configure communication between the Discovery Manager and your Discovery Agent or Agents. If you are using multiple Discovery Agents, you must configure each Agent separately.

- If you are configuring Discovery Agents and a Discovery Manager complete all sections in order.
- If you are configuring Discovery Agents with no Discovery Manager go to the section “Opening the Discovery Agent interface” on page 23.

Note:
For more information about accounts, see “User account options” on page 102.

Topics in this section include:

- “Opening the Discovery Manager or Agent Interface” on page 22
- “Importing a Discovery Manager certificate license file” on page 23
- “Registering Discovery Agents with the Discovery Manager” on page 25
- “Configuring communication between the Discovery Manager and Discovery Agents” on page 26

Note:
You may get a untrusted certificate security warning from your browser when you open the user Interface of the Manager (Premises) or Agent for the first time. The warning can be safely ignored. Replacing Discovery’s self-signed SSL certificate with a certificate that is signed by a trusted CA prevents this from happening (see “Using an SSL certificate signed by a CA” on page 126).

Opening the Discovery Manager or Agent Interface

The Discovery Agent and Manager have separate Web browser-based interfaces allowing you to access them remotely.

Premises users can access Discovery (Manager or Agent) using the:

- default user name entconfig
- default password entrust.
The Discovery Manager interface times-out if left inactive. Users are forced to log back in using a password.

**Attention:**

If you access Discovery using a browser running on a locked-down server, the browser may not be able to run the Discovery scripts. In this case, either make an exception, allowing the scripts to run, or access Discovery from a remote client that does not have the same restrictions.

When you open the Discovery Manager interface for the first time, Discovery presents you with some information about Discovery Manager features. When you no longer want to see this information, Click **Don't show this again**.

**Opening the Discovery Manager interface (from a premises installation)**

In a browser, open the following URL:

https://<host>:27535/discovery-manager/

Where `<host>` is the IP address or host name of the server where the Discovery Manager software is installed.

**Opening the Discovery Agent interface**

In a browser open the following URL:

https://<host>:27534/discovery-agent/

Where `<host>` is the IP address or host name of the server where the Discovery Agent software is installed.

**Note:**

Certificate Services is a separate Cloud-based service. For information about enrolling in Certificate services see [https://www.entrust.com/solutions/certificate-services/](https://www.entrust.com/solutions/certificate-services/)

**Importing a Discovery Manager certificate license file**

If you are using the architecture described in “Entrust Discovery Manager with one or more Discovery Agents” on page 13 to manage certificates using Discovery Manager,
you must import the certificate license file that you purchased from Entrust (see “Licensing” on page 16). If you are using the Certificate Services.

The license file determines how many certificates Discovery can manage. Additional licenses can be purchased from Entrust and uploaded to the Discovery Manager as required.

If you want to check the file at a later date see the section, “Viewing detailed version information” on page 123.

**To import the license file**

1. After you purchase licenses from Entrust, you will receive a license file. Save the file to a location that is accessible to the Entrust Discovery Manager.
2. In the Discovery Manager menu, click **Options > License**.
3. Click **Import New License**.
4. Browse to the location of the license file.
5. Click **Submit**.
The **Current Status** field indicates the validity of the license. The interface shows the type and number of licenses.

### Registering Discovery Agents with the Discovery Manager

Registering Discovery Agents with the Discovery Manager starts the process of establishing secure communication between the Discovery components.

If you have are using Entrust Certificate Services see the Certificate Services online help for more information.

If you have a premises installation, register your Discovery Agents with the Discovery Manager running on your server.

**To register a Discovery Agent**

1. In the Discovery Manager’s menu, click **Agents**.
2. Click **Register New Agent**.
3 In the **Hostname** field, enter a descriptive name for the Discovery Agent.

4 Optionally, in the **Description** field, enter any additional information about the Discovery Agent (for example, its location, or devices that it monitors).

5 Click **Save**.

**Configuring communication between the Discovery Manager and Discovery Agents**

For each Agent:

- Create and download a token file using Discovery Manager. The token is used to configure secure communication with the Discovery Manager. If you are using Certificate Services, see the Certificate Services online help for more information.
- From the Discovery Agent, import the token and configure the Discovery Agent to recognize the Manager.

**To configure communication between the Discovery Manager and a Discovery Agent**

1 In the Discovery Manager interface menu, click **Agents**.
2 In the entry for the Discovery Agent being registered, click **Download Token** in the **Actions** column.

3 Download the file to a location accessible to the Discovery Agent.

4 In the Discovery Agent interface, select **Options > Agent/Manager Link**.

5 In the **Discovery Manager Location** field select the location of the Discovery Manager.
   - If the Discovery Manager is installed on a different machine, select **Remote Location**.
   - If the Discovery Manager is on the same host as the Discovery Agent select **Co-located with this agent**.
   - If you are using the **Entrust Certificate Services** see the Certificate Services online help for more information.
   - If you are not using a Discovery Manager, leave this link unconfigured or select **None configured**.

6 If you select **Remote Location**, additional fields appear to allow you to specify the host and port.
Getting started

In the **Manager Hostname** field, enter the host name or IP address of the Discovery Manager.

In the **Manager Port** field, accept the default value (27535) if you are connecting to the Discovery Manager directly and have not changed the default port number.

You can configure a different port if you decide to use a proxy server. The proxy server must use port 27535 to connect to the Discovery Manager or you must change the default port used by the Manager.

**7** In the **Upload Scan Results** field, select automatic or manual uploading of information from scans to the Discovery Manager. If you select **Automatically**, the Discovery Agent will send the file to the Discovery Manager.

If you select **Manually**, you can, periodically, download scans to another location and manually upload them to the Discovery Manager. For example, this option would be useful to obtain scan data from a Discovery Agent monitoring a part of your network that is isolated, or otherwise not able to contact the Discovery Manager.

**8** In the **Manager Token File** field, browse to the location of the token file.

**9** Click **Save**.

If the connection is established, the **Current Status** field displays a green check mark and the lines **Manager is reachable** and **Valid Manager Token Present**. These messages are updated periodically to reflect the state of the connection.

---

**Note:**

If a Discovery Agent cannot find the Discovery Manager or is rejected as unknown, be sure that: your machine can access the Discovery Manager host, the host name or IP address entered for the Discovery Manager is correct, and that you have imported the correct token for that Discovery Agent. Tokens are specific to each Agent.
Scanning devices and importing certificate information

After you have installed the Discovery Agents (and Discovery Manager, if you are using a premises deployment) and configured communication between the Agent and Manager software as explained in “Getting started” on page 17:

• Configure the Discovery Agents to scan devices on your network for certificates. Be aware that:
  - Each Agent can be configured to automatically run various scans on a schedule or users can run scans as needed. All scans including scheduled scans, can be started manually at any time.
  - Discovery allows you to create reusable lists for information like IP addresses (or host names) or ports, so users do not have to re-enter information when configuring a scan.
• Optionally, deploy the Certificate Scanning Utility to obtain certificate information from computer or user certificate stores (or both). The utility is only available to users who are using Discovery Manager.

This section of the guide contains the following topics:
 • “Configuring Discovery Agents to scan for certificates” on page 30
 • “Using the Entrust Certificate Scanning Utility” on page 41
 • “Manually importing certificates and Entrust Security Manager Reports” on page 44
Configuring Discovery Agents to scan for certificates

Discovery allows you to configure Agents to scan for certificate information according to a preset schedule, or to create and run scans as needed. Each Discovery Agent is capable of performing multiple scheduled scans, allowing you to check different sets of hosts and ports simultaneously or at different times.

Additionally, you can configure the Agent to stop running a scan during a set period (for example, during times of peak network usage) and resume the scan at the end of that period. When the scan is paused, the results collected to that point can be sent to the Discovery Manager in the Agent is configured to send scans automatically.

Only one instance of a given scan can run during any period. However, you can clone a scan and use the clone as a template for a similar scan.

Scan results from scheduled scans are sent to the Discovery Manager on an hourly basis. These periodic updates keep files sent over your network to a manageable size.

Note:
Discovery Manager cannot import a file larger than 10 megabytes. This limitation is not an issue for most scheduled scans because the information is sent to the Manager in chunks, on an hourly basis. If you create a manual scan, check the size of the output file against this limitation and raise or lower the number of devices scanned accordingly. You can scan a very large number of devices before exceeding this limit.

Discovery Manager administrators can configure rules that make Discovery perform some tasks automatically. If you intend to use the Discovery Manager Issuer Rule to automatically assign a management state to certificates found during scans, you should configure the rule before running your scans. Rules only affect certificates when they are first sent to the Discovery Manager.

For information about:
- management states, see “Discovery management states” on page 55.
- configuring an issuer rule to automatically assign a management state, see “Configuring an issuer rule for certificate management” on page 78.
Note:
If a host is not found during a scan, Discovery retains the information about certificates found on that host in previous scans. This behavior insures that information about certificates is not lost because a host is temporarily off-line.

Topics in this section include:
- “Configuring scan parameters” on page 31
- “Creating a preconfigured list of hosts” on page 36
- “Running a scan manually” on page 37
- “Manually uploading a scan to the Discovery Manager or Certificate Services” on page 39

Configuring scan parameters
All scans are configured using the interface for the specific Discovery Agent performing the scan.

To configure a scan
1. From the Main Menu select **Saved Scans**.
2. Click **Add New Scans**.
3 Fill out the information on the page as follows:

**Name**
Enter a meaningful name to identify this scan.

**Description**
Enter any information that you feel will be useful to someone using the scan—the purpose or extent of the scan, for example.

**Priority**
Use this setting to avoid impacting the performance of other scheduled scans by over-stressing network bandwidth. If scans might overlap, this setting determines which scan (if any) should take precedence. Be aware that it is possible to configure this scan in such a way that some lower priority scans never run at all.

- **High** priority scans always run, and suspend any other normal or low priority scan until they are complete.
- **Normal** scans run if no high priority scan is running. Any number of normal priority scans can run simultaneously.
- **Low** priority scans only run if no high or normal priority scan is running. If a normal or high priority scan is started, the low priority scan will be suspended until the other, higher priority scans are finished.
Schedule
To schedule a scan, select the frequency of the scan and time, or day and time for it to run. To run the scan manually, as needed select **Run Manually**.

Hosts to Scan
Individual host names or IP addresses must be space-separated, comma separated, semi-colon separated, or on separate lines. The field accepts any combination of:

- individual IP addresses or host names (for example, 192.51.100.20 or www.example.com)
- ranges of IP addresses using a dash to indicate the range, for example 192.51.100.0-24
- ranges of IP addresses using CIDR notation, for example 192.51.100.0/24

IPv6 addresses can only be specified by their individual IPv6 address or fully qualified host name. CIDR and octet ranges are not supported for IPv6.

If you are scanning a range of IP addresses you may find it more convenient to use **Select host ranges** and enter one or more preconfigured lists. See “Creating a preconfigured list of hosts” on page 36. This option only appears if host ranges are defined.

**Scan All Previously Found Hosts** lets you scan all hosts that have been found in a previous scan.

Port Range
Enter a port, range (or ranges) of ports, or comma-separated list of ports for the Discovery Agent to scan. Use a dash to indicate a range, for example 1-1443. The Discovery Agent looks for the active use of an SSL certificate on each port in turn. If only one port is entered in this field that port will be scanned. All ports in this field are scanned for every host listed in the **Hosts to Scan** field.

---

**Note:**
The port field will accommodate maximum of 255 characters. If you require more space to specify ports, please use a second scan.
**Advanced Options**

Expand this field to access additional options.

**Hosts to Exclude**

If you are scanning a range of hosts, and specifically want to exclude a host or hosts from the scan, select **List Hostnames Explicitly** and enter them as a space separated list. If you have preconfigured a list of hosts to exclude, select **Select host ranges**.

**Resolve Hostnames**

If you select **Always**, the Discovery Agent performs a reverse DNS lookup of the host name before contacting the host for all host names that are listed in the scan. If you select **Never**, the mapping is not checked.

**Check if hosts are alive first**

If you select **Check node before portscan**, the Discovery Agent attempts to contact the host before scanning it. If the Discovery Agent is unable to contact the host it will not perform any scans that are listed for that host. If you select **Assume host is alive**, the Discovery Agent attempts to perform each scan until successful, or until the Discovery Agent times out.

**Host order**

If you select **Normal**, hosts are scanned in the order that they appear in the list. If you select **Randomize**, hosts in the list are scanned in random order. This could be used
to minimize impact on segments of the network or (coupled with a slow scan rate) to help to avoid unwanted Intrusion Detection alarms.

**Scan Rate**

This field determines how aggressively the Discovery Agent acquires information. Consider the amount of network bandwidth available, (at the time of day that you intend to run the scan, if it is scheduled) and the hosts being scanned before selecting a timing template.

- **Slowest** waits the longest time for a response before sending another probe (maximum 300000 milliseconds), makes a maximum of 10 attempts to contact the host port, and has an initial (minimum) scan delay of 300000 milliseconds and maximum TCP scan delay of 300000 milliseconds.

**Note:**

Although it is very bandwidth-friendly, the **Slowest** scan may take a very long time to complete.

- **Slower** waits a relatively long time for a response before sending another probe (maximum 15000 milliseconds), makes a maximum of 10 attempts to contact the host port, and has an initial (minimum) scan delay of 15000 milliseconds and a maximum TCP scan delay of 15000 milliseconds.

- **Slow** waits a moderate time for a response before sending another probe (maximum 10000 milliseconds), makes a maximum of 10 attempts to contact the host port, and has an initial (minimum) scan delay of 400 milliseconds and a maximum TCP scan delay of 1000 milliseconds.

- **Normal** waits a moderate time for a response before sending another probe (maximum 10000 milliseconds), makes a maximum of 10 attempts to contact the host port, and has an initial (minimum) scan delay of 0 milliseconds and a maximum TCP scan delay of 1000 milliseconds.

- **Aggressive** waits less time for a response before sending another probe (maximum 1250 milliseconds), makes a maximum of 6 attempts to contact the host port, and has an initial (minimum) scan delay of 0 milliseconds and a maximum TCP scan delay of 10 milliseconds.

- **Very Aggressive** waits for a short time for a response before sending another probe (maximum 300 milliseconds), makes a maximum of 2 attempts to contact the host port, and has an initial (minimum) scan delay of 0 milliseconds and a maximum TCP scan delay of 5 milliseconds.

**Pause scan between**

Use this field to specify a period during which the scan should pause if it is active, or a time period when the scan should not start. At the end of this period, the scan will
Scanning devices and importing certificate information

resume at the point where it paused. Scans that are scheduled to pause cannot be manually restarted during the pause period.

4 Click **Save**.

After a scan is created, it is listed in the **Saved Scans** page. If you need to edit the information in the scan, use the **Edit** command in the **Actions** column to revisit this page. Actions available from the **Saved Scans** page include:

- **Run**
- **View**
- **Edit**
- **Clone**
- **Delete**

Creating a preconfigured list of hosts

To streamline scan creation, you can preconfigure lists of hosts. These can be hosts that you want to include in various scans, or hosts to exclude (for example, because they have no SSL certificates).

Lists of hosts and host ranges are preconfigured independently on each Discovery Agent. A list that is configured on one Agent will not appear automatically on another Agent.

**To preconfigure a list of hosts**

1 In the main menu, select **Options > Host Ranges**.
2 Click **Add New Host Range**.
3 In the **Name** field, enter a meaningful name to identify the contents of the list. For example, if this is a list of hosts to exclude from scans, you may want to put that in the name.

4 In the **Description** field, describe the list.

5 In the **Entries** field, enter a list of IP addresses or hostnames. Individual host names or IP addresses must be space-separated, comma separated, semi-colon separated, or appear on separate lines. The field accepts:
   - individual IP addresses or hostnames (for example, 198.51.100.20 or www.example.com)
   - ranges of IP addresses using a hyphen to indicate the range, for example 198.51.100.0-24
   - ranges of IP addresses using CIDR notation, for example 198.51.100.0/24

IPv6 addresses can only be specified by individual IPv6 address or fully qualified hostname. CIDR and octet ranges are not supported for IPv6.

Note:
The port field will accommodate maximum of 255 characters. If you require more space to specify ports, please use a second scan.

6 Click **Save**.

**Running a scan manually**

Scheduled scans run automatically. However, you can run an existing scan at any time, or create scans specifically to use, as needed.
Scanning devices and importing certificate information

Report any errors or omissions

After a scan is created (see “Configuring Discovery Agents to scan for certificates” on page 30 for information about creating a scan), it is listed in the Saved Scans page. If you need to stop a scan, click Cancel in the entry for that scan on the Current Scan Results page.

Note:
The browser session does not time out automatically if a scan is in progress, however users can log out manually. The scan will run to completion even if no one is logged in.

To start an unscheduled scan

1. From the main menu select Saved Scans.
2. Click Scan now in the Actions column.

The scan appears under Active Scans on the Current Scan Results page.

Use the pause [ ] or stop [ ] icons to control the scan if necessary.
Manually uploading a scan to the Discovery Manager or Certificate Services

If you chose the Manual option in the Upload Scan Results field of the Discovery Agent's Agent/Manager Link page, or if you are manually uploading a scan from the Certificate Scanning Utility (see “Entrust Discovery Certificate Scanning Utility” on page 10), the data file is not sent to the Discovery Manager automatically. (See “Configuring communication between the Discovery Manager and Discovery Agents” on page 26.)

Scans that have not been uploaded to the Discovery Manager, are listed in the Current Scan Results as Pending. Results from all scans marked Pending are downloaded as a single ZIP file.

If you delete a scan results line from the table on the page, the file containing the data is preserved and can be uploaded.

Note:
For information about uploading scans to Certificate Services, see the Certificate Services online help.

To upload the data to the Discovery Manager:
• download the scan data to a location that can be reached by the Discovery Manager or to a portable storage device, such as a flash drive
• import the scan data into the Discovery Manager

To download a data file from the Discovery Agent
1 From the Discovery Agent menu, click Current Scan Results.

2 To download the scan results, click Download Now.
3 You are asked for a location for the saved file. The file is called agentScanResults.zip.
If the ZIP file is accidentally lost or deleted you can download the files again using the **Download Now** button. The last five ZIP files that were created are retained.

**To manually upload a scan to the Discovery Manager**

1. In the Discovery Manager interface, select **Upload > Upload Scan**.
2. In the **Results** field, browse to the location of the data file.
3. Click **Submit**.
4. The Discovery Manager displays a message about the success of the certificate import process.

<table>
<thead>
<tr>
<th>Results From</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>By hostname</td>
<td>20 Dec 2011 13:19:29</td>
<td></td>
</tr>
</tbody>
</table>
Using the Entrust Certificate Scanning Utility

Entrust Discovery Certificate Scanning Utility is a console application that is designed to find certificates in the certificate stores of computers in the network. You can run it directly from the command line, within a login script, or remotely using various deployment tools.

By default, the export only includes certificates from the Personal certificate store. When the Trusted Root Certification Authorities certificate store is included, certificates from the Third Party physical store are not included. The Third Party physical store contains the certificates from the Microsoft Root Certificate Program and is identical on all computers receiving Windows Updates.

When properly configured, the Discovery Agent periodically checks a specified location for scan results and uploads them to the Discovery Manager.

Only a Super Administrator can configure the Certificate Store Result Monitoring page, however Administrators can run the update as needed.

Procedures in this section include:

- “To use the utility to scan for certificates:” on page 41
- “To use the Agent to upload scan utility results automatically” on page 42

**Note:**

For the Discovery Agent to find and upload scan results from a server it must run as a domain account that has Logon as a service permissions on the computer where the files are stored. Additionally the account must be added to the computer with administrative permissions so the service can read and write locally.

**To use the utility to scan for certificates:**

1. To export the computer's certificates, run the application with the computer option. For example, from the command line type:

   `<path_to_executable>/edcertscan.exe -scan computer`

   Where:

   `computer` scans the computer certificate store

2. While the user is logged in with their usual Windows credentials, run the application with the user option, to export the user's certificates. For example, from the command line type:

   `<path_to_executable>/edcertscan.exe -scan user`

   Where:
Scanning devices and importing certificate information

user scans the user’s certificate store

Other options include:

- **includepeople** which includes certificates from the Other People and Trusted People certificate stores
- **includeca** which includes certificates from the Intermediate Certification Authorities and Trusted Root Certification Authorities certificate stores
- **-output <path>** specifies the folder where the application puts the output file

If no path is specified, the application creates a folder within the current working directory to store the results. The output is always placed within a generated subfolder. This subfolder is named automatically based on the computer name, user name or both so that a large number of computers and users can be scanned in parallel without creating a single folder with too many files.

**Uploading the Scan Utility results**

- If you are importing a ZIP file, see “Manually uploading a scan to the Discovery Manager or Certificate Services” on page 39 for information about uploading it to the Discovery Manager.
- If you are importing individual certificates use the procedure described in the section “To manually add a certificate using the copy and paste method” on page 45.
- To import the information automatically see the following procedure.

**To use the Agent to upload scan utility results automatically**

1. From the main menu select **Options > Certificate Store Result Monitoring**.
2. Click **here**.

![Certificate Store Result Monitoring](image)
3 Select **Enable** from the pull-down menu to start periodically checking for results.

4 In the **Path to monitor** field, enter the path to the folder where the results are stored (the output from the utility specified in the `-output <path>` option). For example, if you have mapped the computer where the files are stored to the Agent host, you can use the format `\<path to folder>\` or if the files are stored on the Agent, the local path to the folder.

5 In the **Check for new results every (minutes)**, schedule how often (in minutes) the Agent should check for scans.

6 Click **Save**.

---

**Note:**

The **Last Scan Time** and **Updated Results** fields on the **Found Certificate Store Result Monitoring Page** are updated after a scheduled scan runs.

To upload the scan results between scheduled checks or if you prefer not to schedule checks, click the icon in the **Status** field.
Manually importing certificates and Entrust Security Manager Reports

Certificates can be imported directly into the Discovery Manager, either individually or as a ZIP archive. This is not the same as importing a scan—this section discusses how to manually import a certificate file or files. Importing a certificate scan is discussed in “Manually uploading a scan to the Discovery Manager or Certificate Services” on page 39.

**Note:**
For information about manually importing certificates into Certificate Services, see the Certificate Services online help.

Individual certificates (or certificate chains) in PEM (Privacy-enhanced Electronic Mail) format can be pasted into the interface (as shown in Figure 4). Certificates in binary or PEM format and ZIP archives containing multiple certificates in binary or PEM format can be uploaded to Discovery Manager (see Figure 5).

Discovery can be used to manage information from reports created by Entrust Authority Security Manager. Configure the following report options in Security Manager before generating the report:

- The reports must be produced in XML format.
- Certificates must be in PEM format.

**Note:**
You cannot import Security Manager reports into Certificate Services.

**Note:**
The management state set in this page overrides the state set in any certificate rules that you may have created. If the state field is left at Default, any certificate rules that have been configured are used.
To manually add a certificate using the copy and paste method

1. Obtain the certificate from the host in PEM format. This procedure varies according to the type of host where the certificate is installed. See the documentation for the host if you require more information.

2. Open the PEM file and copy the certificate (and certificate chain if desired).

Note:
When copying a certificate, be sure to include the ---Begin Certificate--- and ---End Certificate--- lines.

3. In Discovery Manager, select **Upload > Manually Import Certificates**.

4. Paste the certificate into the space provided as shown in Figure 4.

**Figure 4:** Manually copying a certificate into Discovery Manager
5 Optionally, set the management state for the certificate being imported. Table 1 on page 55 describes the management states.

6 Click Submit.

A confirmation page containing a summary of the certificate information is displayed.

To manually upload a certificate or ZIP archive

1 Obtain the certificate or certificates from the host where they are installed in PEM or binary format. Obtaining a certificate varies according to the type of host where the certificate is installed. See the documentation for the host if you require more information.

2 If you are uploading multiple certificates, create a ZIP archive containing all certificates.

3 In Discovery Manager, select Upload > Manually Import Certificates.

4 Browse to the certificate file as shown in Figure 5.

Figure 5: Uploading a zip file archive containing certificates
5 Optionally, set the management state for the certificates being imported. Certificates in the file that are imported for the first time are given this management state. Table 1 on page 55 describes the management states.

6 Click Submit.

A confirmation page containing a summary of the certificate information is displayed.

Importing a report from Entrust Authority Security Manager

Security Manager administrators can use Entrust Authority Security Manager to create reports about certificates managed by the CA. If this type of report is generated in XML format, Discovery Manager can import the file and display the information.

Importing the information into Discovery allows administrators to use the flexible certificate information management features in Discovery Manager with the Security Manager report.

To import an Entrust Authority Security Manager report

1 Create a report using Entrust Security Manager Administration. Select the XML format option for reports and PEM format for certificates.

2 Download the report to location that is accessible by the Discovery Manager.

3 In Discovery Manager select Upload > Manually Import Certificates.

4 Click Browse and select the report.

5 Optionally, set the management state for the certificates being imported. Certificates in the file that are imported for the first time are given this management state. Table 1 on page 55 describes the management states.

6 Click Submit.
Scanning devices and importing certificate information

Report any errors or omissions
Managing certificates

This section of the guide outlines Entrust Discovery’s options for monitoring and managing certificates. Topics in this section of the guide include:

- “Monitoring scan information from the Discovery Agent” on page 50
- “Viewing detailed certificate information” on page 52
- “Assigning a management state to a certificate” on page 54
- “Deleting a certificate” on page 60
- “Configuring management options for an individual certificate” on page 61
- “Changing certificate details and options in bulk” on page 64
- “Configuring email notification and reports” on page 66
- “Creating custom fields” on page 70
- “Assigning a friendly name to a Certification Authority (CA)” on page 73
- “Exporting a certificate summary report” on page 75
- “Configuring rules” on page 77

Most of the topics in this section apply to a Discovery Agent and Manager architecture.
Monitoring scan information from the Discovery Agent

Information about the progress of a scan can be viewed from the Current Scan Results page.

Any scan can be paused manually. Scans that have been paused manually can be resumed manually. Scans that have been suspended automatically due to scheduling or priority cannot be resumed manually.

**Note:**

Scan results in the Discovery Agent's interface are updated automatically if a scan is in progress.

Scans are categorized as:

- **Active**
  - the scan that is currently running; any concurrent scan with a lower priority will be suspended and listed in the **Suspended** pane

- **Suspended**
  - scans that have been paused for some reason (for example, because a higher priority scan started)

- **Recent**
  - the last scan to run: including scans with partial result sets

- **Upcoming**
  - the next scan to run, be suspended, or resumed after a suspension or pause
A summary of the scan information appears on the home page of the Discovery Agent after a scan.

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Cert Count</th>
<th>Expires</th>
<th>1-30 Days</th>
<th>31-60 Days</th>
<th>61-120 Days</th>
<th>121-365 Days</th>
<th>Later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entrust Non-Public CAs</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entrust Certification Authority-L1C</td>
<td>2</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Non-Public CAs</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entrust Certification Authority-L1E</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entrust Certification Authority-L1C</td>
<td>2</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VanSign Trial Secure Server CA-G2</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>6</strong></td>
<td><strong>2</strong></td>
<td><strong>1</strong></td>
<td><strong>1</strong></td>
<td><strong>1</strong></td>
<td><strong>2</strong></td>
<td></td>
</tr>
</tbody>
</table>

The total number of certificates issued by each category of CA (Entrust Non-Public CAs, for example) is shown in the highlighted title lines. The number of certificates issued by each CA (Entrust Certification Authority-L1C, for example) are indicated in the rows below each title line. The **Total** line indicates the total number of certificates, and the total number of certificates that will expire in each time period. Expired certificates appear in the expired column (in red if you have color).

Detailed information about individual certificates is available from the Discovery Manager.
Managing certificates

Viewing detailed certificate information

The Certificate Details page contains information about:

• the certificate
• the certificate owner
• the host or hosts where the certificate is installed
• the trust path (chain of CAs that signed the certificate)
• a brief history of Entrust Discovery's interactions with the certificate (for example, when the certificate was found or licensed)

The download link on this page allows you to download the certificate to a convenient location and view it on your local machine.

Note:
The information in this section does not apply to Certificate Services. See the Certificate Services online help for more information

Viewing certificate information

1. From the Discovery Manager menu, click Certificates > Certificates list > <management state>.
2. Click Update.
3. Click the name of the certificate that you want to view.
The **Certificate Details** page appears, displaying detailed information about the certificate.

**Note:**
To obtain more details about a certificate, you can download it to a convenient location using the **Download Certificate** link and view it from your local machine.
Assigning a management state to a certificate

The Manager allows you to assign one of four management states (Monitored, Registered, Discovered, or Ignored) to each certificate. Details about the characteristics of each management state are described in Table 1.

Certificates can be assigned to a management state on either:

- an individual basis (see “To assign a certificate to a management state” on page 56)
- in bulk (see “To assign certificates to a management state in bulk” on page 58)
- automatically, by configuring a rule (see “Configuring rules” on page 77).

Each certificate moved to the Registered or Monitored state uses a license. Detailed information and various management options are available for certificates that have been assigned a license. If you decide later that a certificate or certificates do not need to be managed, certificates can be moved from a managed to unmanaged state using Bulk Update (see “Changing certificate details and options in bulk” on page 64).

After the Discovery Agent sends the results of a scan to the Discovery Manager, information about newly found certificates appears in the Manager’s Certificate > Discovered page by default. Use a rule to automatically specify a different initial management state, if desired.
### Table 1: Discovery management states

<table>
<thead>
<tr>
<th>Management state</th>
<th>Characteristics</th>
</tr>
</thead>
</table>
| Monitored        | • uses one license per certificate  
|                  | • listed on the Monitored Certificates page (when the Monitored master filter is applied)  
|                  | • certificate type is included in the policy filters (can be included in a policy)  
|                  | • details of the certificate including custom fields, location information, trust path, or history are visible  
|                  | • can download the binary certificate  
|                  | • certificates are included in expiry notification emails, if you have set up email notification  
|                  | • can receive ownership reports |
| Registered       | • uses one license per certificate  
|                  | • listed on the Registered Certificates page (when the Registered master filter is applied)  
|                  | • certificate type is included in the policy filters (can be included in a policy)  
|                  | • details of the certificate, including custom fields, location information, trust path, and history are visible  
|                  | • can download the binary certificate  
|                  | • certificates are not included in expiry notification emails  
|                  | • can receive ownership reports |
| Discovered       | • does not require a license  
|                  | • certificates are listed on the Discovered Certificates page (when the Discovered master filter is applied)  
|                  | • certificates cannot be listed using the policy filters  
|                  | • details of the certificate are visible, but no custom fields, location information, trust path, or history can be seen (even if the certificate was previously registered)  
|                  | • not able to download the binary certificate Discovery Manager  
|                  | • certificates are not included in expiry notification emails  
|                  | • all certificates that have not been assigned a management state start as Discovered |
Managing certificates

<table>
<thead>
<tr>
<th>Management state</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignored</td>
<td>• does not require a license</td>
</tr>
<tr>
<td></td>
<td>• certificates are listed on the Ignored Certificates page (when the</td>
</tr>
<tr>
<td></td>
<td>Ignored master filter is applied)</td>
</tr>
<tr>
<td></td>
<td>• certificates cannot be listed using the policy filters</td>
</tr>
<tr>
<td></td>
<td>• details of the certificate are visible, but no custom fields, location</td>
</tr>
<tr>
<td></td>
<td>information, trust path, or history can be seen (even if the certificate</td>
</tr>
<tr>
<td></td>
<td>was previously registered)</td>
</tr>
<tr>
<td></td>
<td>• not able to download the binary certificate from Discovery Manager</td>
</tr>
<tr>
<td></td>
<td>• certificates are not included in expiry notification emails</td>
</tr>
<tr>
<td></td>
<td>• designed to separate certificates that are intentionally ignored</td>
</tr>
<tr>
<td></td>
<td>from those that are Discovered but not assigned</td>
</tr>
<tr>
<td></td>
<td>• certificate records can only be deleted if the certificate is placed</td>
</tr>
<tr>
<td></td>
<td>in the ignored state</td>
</tr>
</tbody>
</table>

To assign a certificate to a management state

1. From the Discovery Manager menu, select Certificates > Certificates list > <management state> (for example, Certificates > Certificates list > Discovered).
2. Click Update.
   A list of certificates appears on the page.

<table>
<thead>
<tr>
<th>Name</th>
<th>Hostname</th>
<th>,issuer</th>
<th>Expire</th>
<th>Key Type</th>
<th>SAN</th>
<th>Cert Signed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>DM\Administrator</td>
<td>17041 days</td>
<td>RSA</td>
<td>RSA-2048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Root Agency</td>
<td>DM\Root Agency</td>
<td>10251 days</td>
<td>RSA</td>
<td>RSA-512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Root Trust CA</td>
<td>DM\Dynamic Root</td>
<td>10261 days</td>
<td>RSA</td>
<td>RSA-4096</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DnsDynamicRootTrust, Snap</td>
<td>DnsDynamicRoot</td>
<td>8370 days</td>
<td>RSA</td>
<td>RSA-2048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTN\ID\Teks Exelent Authentication and Email</td>
<td>UTN\ID\Teks Exelent Authentication and Email</td>
<td>8370 days</td>
<td>RSA</td>
<td>RSA-2048</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• To filter the list of certificates, use the filter options.
• Use the view options to adjust what is displayed on the page.
Note:
After setting filters or views, you can save that particular set of options for reuse. For information about these display options, see the section “Setting filter, view, and policy options (Premises only)” on page 86.

3 Select the certificate from the list.
The **Certificate Details** page appears.

4 Click **Add to Managed**.
Managing certificates

Note:
You must have an available Entrust Discovery license to assign a certificate to the Monitored or Registered state. For information about how to import a license file, see “Importing a Discovery Manager certificate license file” on page 23.

To assign certificates to a management state in bulk

1. From the Discovery Manager menu, select Certificates > Certificates list > <management state>.

Note:
If you are adding previously unknown certificates, or certificates that you have not to assigned to a management state, the certificate will be in the Discovered state.

2. Click Update.
A list of certificates appears on the page.

3. Click Bulk Update.
Check boxes appear beside each item in the list. The Change Management State field appears in the menu.

4. Select the check box beside each certificate that you want to move. All of the certificates that you select will be moved to the selected management state. If you are
moving certificates to different categories, repeat this procedure for each management state.

<table>
<thead>
<tr>
<th>Days</th>
<th>Certificate</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>ca.trust.com</td>
<td>server1.domain.example.com</td>
</tr>
<tr>
<td>30</td>
<td>ca.trust.com</td>
<td>server2.domain.example.com</td>
</tr>
<tr>
<td>90</td>
<td>ca.trust.com</td>
<td>server3.domain.example.com</td>
</tr>
<tr>
<td>125</td>
<td>ca.trust.com</td>
<td>server4.domain.example.com</td>
</tr>
</tbody>
</table>

5 From the **Change Management State** drop down menu select the management state for these certificates.

6 Click the check mark beside the **Change Management State** field to save your changes.
Deleting a certificate

Certificate records can be deleted permanently. After you have permanently deleted the entry, the certificate will no longer appear.

**Note:**
The information in this section does not apply to Certificate Services. See the Certificate Services online help for more information.

To delete a certificate

1. Move the certificate to the ignored state (for more information see “Assigning a management state to a certificate” on page 54).
2. In the Ignored Certificates page select **Bulk Update > Delete completely**.
3. Select the certificates to delete.
4. Click the green check mark beside **Bulk Update** to complete the deletion.
Configuring management options for an individual certificate

After you have assigned a certificate to a management state, you can configure additional management options. The options available depend on the management state selected for the certificate.

Note:
The information in this section does not apply to Certificate Services. See the Certificate Services online help for more information.

If a managed certificate is replaced at a later date, the management state, contact information, and custom fields are added to the new certificate.

To configure management options for a certificate

1. From the Discovery Manager menu, click Certificates > Certificates list > <management state>.
2. Click Update.
3. Click on the certificate name in the list.
4. Click Edit.

The Certificate Details page opens.

5. Click Edit.
5 In the **Certificate Details** page, enter a friendly name for the certificate. Use a name that will help you to identify it in future communications.

Fill in the owner information fields. These fields identify the person responsible for the certificate. The owner is notified by email when the certificate approaches its expiry date if the notification option is configured (see “Configuring email notification and reports” on page 66). You can enter multiple email addresses. Email addresses should be separated by a comma or semicolon. For example:

alice.gray@example.com,bob.lee@example.com

Or

alice.gray@example.com;bob.lee@example.com

**Note:**

Change the owner listed for the certificate if that person leaves the company or the responsibility is assumed by someone else.

Any custom fields that you have created appear at the end of this column (see “Creating custom fields” on page 70 for information about custom fields).

The **Download Certificate** link allows you to download the certificate. After downloading the certificate you can view its contents using a some other tool (a browser, for example).

6 Location information that is derived from the certificate appears under **Locations** automatically. To add additional information about the certificate location, or if you
have manually imported the certificate and data normally collected by the Discovery Agent is not available, click **Add**, and select or enter the additional information.

7 Select the green check mark icon to save any added information.

8 The trust path for the certificate is indicated on the lower right side. Discovery can find and record intermediate certificates in the chain of trust, even if the chain that was received from the server is incomplete. A green check mark next to the path indicates a trusted certificate.

**Note:**

A broken link icon in the **Last Seen** column under **Locations** indicates an incomplete certificate chain was obtained from the server. Discovery may use information obtained from other certificates to complete the certificate chain when it creates the chain seen in the **Trust Path** pane. The **Trust Path** that Discovery displays includes missing the certificates.

9 Click **Save** to retain your changes.
Changing certificate details and options in bulk

To facilitate certificate management, you can update some of the fields shown in the certificate details page in bulk. The contact name, telephone number, email address, location, and the date that they were changed can be altered from the Bulk Update option in the registered and monitored certificate pages.

Note:
The information in this section does not apply to Certificate Services. See the Certificate Services online help for more information.

To bulk update certificate details
1. From the main menu select Certificates > Monitored (or Registered).
2. Use the check boxes at the left of each entry to select the certificates to update.
3. In the menu for the certificate list click Bulk Update and select the field to change, for example contact name.
4. In the new field enter the information for the field, for example the name of the contact for the selected certificates.
5 Click the check mark to save your changes. The changes appear in the certificate list.

**Note:**
Change the owner listed for a certificate if that person leaves the company or the responsibility is assumed by someone else.
Configuring email notification and reports

The Discovery Manager provides the following standard notifications and reports:

Note:
The information in this section does not apply to Certificate Services. See the Certificate Services online help for more information.

- **Admin Report**
  - notifies the default administrator about certificate expiry information (for certificates past the error threshold), system notices that have not been cleared, and license details
- **Certificate Expiry report:**
  - notifies the certificate owner (or the default Discovery administrator if no owner is specified) about certificates that are close to expiry
  - by default, includes information about the certificates from the Certificates details page including information from custom fields but can be customized using a global view
  - the number remaining
- **Certificate Ownership report**
  - notifies the certificate owners that they have been assigned certificates
- **Policy Violation report**
  - Global and personal policy reports are handled in different ways.
    - Global policy violation reports go to the account or accounts specified as the default administrator—not all administrators. Multiple email addresses can be specified on the reporting configuration page.
    - Personal policy violation reports go to the individual users who have configured them, and only to the user.
    - If no certificates violate a policy (of any type), no report is sent.
- **License report**
  - notifies the default administrator about the number of licenses used
- **System Notices report**
  - compiles all notices that have not been cleared from the Dashboard page, and sends them to the default administrator

  Notices are brief messages about the health and operation of the Discovery Manager or Agent that appear on the Dashboard page of the interface.
Discovery Manager provides a notice rule that administrators can use to select what action to take for specific notices. See “Configuring a notice rule” on page 79 for information about notice rules.

### Configuring reports

To receive reports by email:

- Configure the SMTP options, allowing Discovery to use your email system.
- Configure the appropriate thresholds to alert your administrators to certificates that are close to expiry.
- Configure the frequency that reports are issued and customize the headers for ease of identification. Saved global views can be used to customize the content of the expiry, ownership, and admin reports. For information about creating and saving views see “Configuring a view” on page 93. The name of the view appears in the report.

#### To configure SMTP options

1. In the menu select **Reports > SMTP Configuration**.
2. In the SMTP options pane, configure:
   - the sender address to use for notifications, for example, discovery@example.com
   - the email host, for example, mail.example.com
   - the port to use, for example 25
   - username and password (if required)
   - the sending domain, if the Manager's hostname cannot be resolved through DNS
3. Click **Verify SMTP settings** to be sure that Discovery can use them.
4. Click **Save** to retain your changes or **Cancel** to discard them.

#### To configure the expiry notice

1. In the menu select **Reports > Expiry Notice Configuration**.
2. In the Admin **Contact Email Field**, This administrator should be someone other than a certificate owner. Discovery notifies this administrator if the certificate breaches the
error threshold. Multiple comma or semicolon-separated addresses can be entered if you want to list multiple administrators.

Enter appropriate thresholds (or retain the default values, depending on your requirements). If certificates exceed these thresholds, information about the certificate is added to reports.

The certificate owner is alerted about breaches of the warning and information thresholds. The administrator is alerted if the error threshold is breached. Configuring the error threshold to occur closer to the expiry date than the information threshold allows the owner to resolve the issue.

3 Click **Save** to retain your changes or **Cancel** to discard them.

**To send reports by email**

1 In the menu select **Reports > Reports Scheduling**.
2 Use the pull-down menu to control the frequency that each type of report is issued.
3 Global saved views can be used to customize the format of the information that appears in the expiry, ownership, and admin reports.

4 Optionally, customize the header text to appear in the Certificate Expiry or Ownership report.

5 In the Certificate Expiry report, if **Additional Recipient** email addresses have been configured using a Custom Field, select the level of notification (**Info**, for example) at which to send the report to a specific address.

6 Click **Save** to retain your changes or **Cancel** to discard them.

**Note:**

Use the **Generate Now** link to generate reports manually at any time.
Creating custom fields

If you add specific information about certificates to the certificate details page, it will appear as a column in the Certificates page, allowing you to filter the certificate list against information of your choosing (see “Setting filter, view, and policy options (Premises only)” on page 86). Super Administrators have the option of making specific custom information mandatory or optional.

Note:
The information in this section does not apply to Certificate Services. See the Certificate Services online help for more information.

To add a custom field to the certificate details page

1. Select Options > Custom Fields.
2. In the Custom Fields page, click Add.

![Custom Fields](image-url)
3. In the **Custom Fields New/Edit** page:

- In the **Name** field, enter the name that you want to appear on the **Certificate Details** page. This field is mandatory.
- In the **Description** field, optionally add a description of the field’s purpose.
- In the **Mandatory** field, select **true** if this information is required on the **Certificate Details** page. If you select **true**, this field must be completed when the certificate details page is edited.
- In the **Type** field, select the type of information that will be entered:
  - **Text** allows the user to add whatever text you choose.
  - **Number** allows the user to add a number.
  - **Date** allows the user to add a date from a calendar popup.
  - **Yes/No** adds a field that allows the user to enter **Yes** or **No**.
Managing certificates

- **Choice** allows you to create a pick list. Enter the options for the pick list in the fields that appear below. Use the check mark icon to set each option.
- **e-mail** allows you to add a fields for additional email addresses. These addresses appear on the certificate details page and allow additional email addresses to be specified for notifications.

**Note:**
After the custom field has been created, you cannot change the **Type** field. Create another custom field instead.

4 Click **Save** to create the custom field.
The field or fields appear in the **Certificate Details** page.
Assigning a friendly name to a Certification Authority (CA)

CA names appear in numerous places in lists and notifications. For convenience, the Discovery Manager can replace the CA name with a shorter or more meaningful name.

**Note:**
The information in this section does not apply to Certificate Services. See the Certificate Services online help for more information.

You can add a Friendly Name for a CA using the link in certificate entry on the Certificate Summary page or use issuer rules (for information about issuer rules “Configuring an issuer rule for certificate management” on page 78).

**To assign a friendly name to a CA (Certificate Summary page entry)**

1. In the Discovery Manager main menu, select Certificates > Certificate Summary.
2. In the All Certificates Summary page, hover the pointer over the CA name and click Add Friendly Name.

The CA Friendly Names-Add New/Edit page opens.
3  Enter a friendly name and description for the CA.

**Issuer Rules - Add New/Edit**

* required

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer DN: *</td>
<td>CN=Our Private CA, OU=IT, O=&quot;Example.com&quot;, C=US</td>
</tr>
<tr>
<td>Friendly Name: *</td>
<td>CA1</td>
</tr>
<tr>
<td>Description:</td>
<td>Our CA for ...</td>
</tr>
<tr>
<td>Automatically move certificates to management state:</td>
<td>Monitored</td>
</tr>
<tr>
<td>URL for renewing certificates:</td>
<td><a href="http://www.example.com/CA1/renew/">http://www.example.com/CA1/renew/</a></td>
</tr>
</tbody>
</table>

4  Click **Save**.
Exporting a certificate summary report

You can download a summary report of the certificate information as a CSV file.

Note:
The information in this section does not apply to Certificate Services. See the Certificate Services online help for more information.

To download the report

1. From the Discovery Manager **Certificates** menu, select the management state of the report (Registered and Monitored, Monitored, Registered, Discovered, or Ignored).
2. Click **Export**.

**Monitored Certificates**

The report contains the following information:

- **FriendlyName**: the friendly name assigned to the certificate (if you have assigned one; if no friendly name is assigned the DN appears in this column)
- **CertLocations**: a comma separated list of the FQDN (fully qualified domain name) and port of the certificate locations
- **subjectDN**: the distinguished name of the certificate
- **issuerDN**: the distinguished name of the CA that issued the certificate
- **KeyAlgorithm**: the encryption algorithm used by the certificate's public key
- **KeyLength**: the size (in bits) of the public key used by the certificate
- **CertSignedWithAlgorithm**: the algorithm used to sign the certificate
- **CertSignatureSize**: the size of the key used in the signing algorithm
- **ValidFrom**: the date that the certificate became valid
- **ValidUntil**: the date that the certificate expires
- **entrustIssued**: Y (yes) if the certificate was issued by Entrust
- **publicRoot**: the name of the public root (if the certificate has a public root)
- **SHA1Thumbprint**: a unique identifier for a certificate
- **KeyUsage**: (optional) used to specify the usage of the public key contained in the certificate
Managing certificates

- **ExtendedKeyUsage**: (optional) used by some systems to specify the purpose of the public key contained in the certificate
- **SubjectAltNameCount**: The number of SubjectAltNames in the certificate
- **SubjectAltNames**: any SubjectAltNames added to the certificate (often used to add hostnames, if the certificate is used in more than one place)
- **CertSerialNumberHex**: certificate serial number in hexadecimal notation—uniquely identifies a certificate issued by a particular CA
- **CRLDistributionPoints**: where the certificate verifying application (for example, a browser) expects to find updated certificate revocation lists
- **ContactName, ContactEmail, ContactPhone**: the name and contact information of the person responsible for the certificate (name, email address, and phone number)
- **Location**: The location of the certificate.
- **Entity Type**: The type of entity that signed the certificate (for example, self-signed root)
- **Organization**: the organization that the certificate is assigned to

The report also contains any custom fields.

**Figure 1**: Certificate report viewed in Microsoft Excel
Configuring rules

Entrust Discovery incorporates a rule engine for efficient management of large numbers of certificates. Assigning organization, management state, contacts, and other information can be done automatically, based on specific information about the certificate. Configuration of rules is optional.

Note:
The information in this section does not apply to Certificate Services. See the Certificate Services online help for more information.

Each rule is configured according to:
- the event that starts the rule (importing a certificate, for example)
- the filter that determines which certificates are affected by the rule
- the action or actions that are performed on the certificates as a result

Topics in this section include:
- “Types of rules” on page 77
- “Configuring an issuer rule for certificate management” on page 78
- “Configuring a notice rule” on page 79
- “Configuring a certificate rule” on page 82

Types of rules

Discovery includes four types of rules:
- Issuer rules allow administrators to specify that all certificates from a particular CA are placed in a specific management state (monitored, registered, or ignored).
- Notice rules allow you to specify an automatic action if a particular notice appears on the Discovery Dashboard page. Administrators have the option of configuring the rule if the notice appears. There are four possible actions for notice rules although most of them only apply to specific notices.
- Certificate rules are triggered by an event that the administrator specifies when the rule is configured—for example, when the certificate is imported or if a certificate is added to managed certificates. Administrators have the option of using these rules to apply one or more actions—for example, setting a management state or a contact name. Rules can also be created that stop an action from occurring in specified cases by selecting the Stop processing rules option.
Managing certificates

- Login rules apply to user accounts that are managed through Microsoft Active Directory (see “Login rules for Active Directory” on page 110 for information about using Active Directory).

**Note:**
In some cases rules will not reapply information. If, for example, you set a physical location using a rule, change the physical location information manually, and then run the rule a second time, the physical location that was entered manually is retained.

### Configuring an issuer rule for certificate management

By creating issuer rules, administrators can configure Discovery to automatically assign new certificates from an issuer to a specific management state as they are discovered. This feature decreases the amount of hands-on certificate management required by administrators.

Each new certificate added to a managed state requires a license from inventory. If no license is available, certificates are assigned the Discovered state.

**Note:**
Issuer rules only run when new certificates are first uploaded to the Discovery Manager. Certificates that have already been assigned to a state (Monitored, for example) are not reassigned.

**To create an issuer rule**

1. In the Discovery Manager top menu select **Rules > Issuer Rule** and click **Add friendly name**.
2. In the **Issuer Rules** page, click **Add**.
3. In the **Issuer DN** field enter the distinguished name of the CA that issues the certificates. An example of an issuer DN is:

   `CN=Entrust CA, OU=entrust, O="Entrust, Inc.", C=US`
In the **Friendly Name** field enter the friendly name you have selected for the issuer CA.

5 In the **Description** field, add any pertinent information about the CA.

6 Select a management state for certificates from the CA (for information about management states, see “Assigning a management state to a certificate” on page 54).

7 In the **URL for issuing certificates** field, add the URL of the issuing CA.

8 Click **Save**.

**Configuring a notice rule**

Notice rules are configured individually for each system notice. System notices appear on the Dashboard page of the Discovery Manager and provide information about Discovery system events. Using the notice rules, you can determine what action Discovery should take concerning individual types of notices. The rule is applied immediately.
Note:
After you create a notice rule the notice that it applies to will not appear again unless you delete the rule.

Entrust Discovery can be set to perform one of four possible actions are explained in Table 2. Not all actions are available for all notices.

Table 2: Notice rule actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Condition causing the notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Notice</td>
<td>An available option for most conditions. The only option for most notices.</td>
</tr>
<tr>
<td></td>
<td>Clears all future notices of this type automatically.</td>
</tr>
<tr>
<td>Add to managed</td>
<td>Discovery has found an unmanaged certificate in a location where it previously found a managed certificate—for example, a new certificate has been issued for this location.</td>
</tr>
<tr>
<td></td>
<td>Puts any certificate that triggers the notice into the managed state each time the notice is received. clears all future notices of this type automatically.</td>
</tr>
<tr>
<td>Remove from management</td>
<td>Discovery is unable to find a certificate that it manages—for example, Discovery does not find a previously found certificate because it has been replaced.</td>
</tr>
<tr>
<td></td>
<td>Moves any certificate that triggers the notice from the managed state to the unmanaged state. clears all future notices of this type automatically.</td>
</tr>
</tbody>
</table>
To configure a notice rule

1. On the Discovery Manager Dashboard page, under **System Notices**, hover your pointer beside the notification and just to the left of the action icon. The **Add Rule** link appears.

   ![Add Rule icon]

2. Click **Add Rule** to create the rule. (To perform an action for the individual notice—for example swap monitoring of a specific certificate for a new one—click the relevant icon.)

<table>
<thead>
<tr>
<th>Action</th>
<th>Condition causing the notice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch</strong></td>
<td>Changes the state of the new certificate to managed and the old certificate to unmanaged (combination of Add to managed and Remove from managed). Clears all future notices of this type automatically.</td>
</tr>
<tr>
<td></td>
<td>Discovery has found an unmanaged certificate in a location where it previously found an managed certificate and does not find the certificate that it has listed as managed. If you have configured specific information for the certificate (custom fields, for example) this information is preserved and applied to the new certificate.</td>
</tr>
</tbody>
</table>
Managing certificates

3. In the Notice Rules page, select an action from the **Action to Perform** menu. The rule that this applies to appears in the **Description** field near the top of the page. See Table 2 on page 80 for information about these actions.

4. Click **Save**.

**Configuring a certificate rule**

Certificate rules use global filters to select which certificates are affected by the rule. Before creating a certificate rule, create the filter that you want to use with it. Be sure that the filter targets the certificates that you want the rule to affect. Discovery allows you to create complex filters.

Similarly, if you want to use certificate rules to assign certificates to organizations, create the organizations before creating the rule. Only existing organizations appear in the drop-down list.

Only Super Administrators can create a certificate rule.

**To configure a certificate rule**

1. In the Discovery Manager top menu, select **Rules > Certificate Rule**.
2. In the **Certificate Rules** page, click **Add**.

3. In the **Name** field, enter a meaningful name for the rule.
4 In the Run rule when field, select the condition or conditions that will trigger the rule. Use Ctrl + click to select additional conditions.

Certificate first imported, starts the rule if a new certificate is imported by any method.

New location added to certificate, starts the rule if a certificate is found in an additional location. This condition could trigger the rule multiple times for the same certificate.

Certificate added to management, starts the rule if the certificate is changed to a management state.

Certificate Organization updated, starts the rule if the certificate organization is modified.

5 In the If rule matches field, select Continue to specify conditions where the actions are applied or Stop processing rules to conditions for not applying an action.

6 In the Filter results by field, select the filter to use. Only global filters appear in the list. Use the filter to select which certificates are affected by the rule.

7 In the Add Rule Action field, select the action or actions apply when the rule runs. Each time that you select an action, a field allowing you to set specific information appears—for example, if you select Set management state, a drop down list appears allowing you to select a management state.

8 Click Save.
Entrust Discovery administration

This section explains some administration, customization, and troubleshooting options.

- “Setting filter, view, and policy options (Premises only)” on page 86
- “Creating and using charts (Premises only)” on page 95
- “Using organizations to manage certificates (Premises only)” on page 101
- “User account options (Premises only)” on page 103
- “Using Microsoft Active Directory (Premises only)” on page 108
- “Uninstalling Entrust Discovery (Premises only)” on page 118
- “Manually stopping and starting the application (Premises only)” on page 119
- “Monitoring the Agent (Premises only)” on page 120
- “Viewing the license information (Premises only)” on page 121
- “Backing-up and restoring Discovery (Premises only)” on page 122
- “Database maintenance (Premises only)” on page 125
- “Viewing Discovery logs and System Notices (Premises only)” on page 126
- “Viewing detailed version information (Premises only)” on page 127
- “Changing the default listen port for the Agent or Manager (Premises only)” on page 128
- “Using an SSL certificate signed by a CA (Premises only)” on page 130
- “Listing certificate location by hostname or IP address (Premises only)” on page 132
- “Configuring the Switch or renew button (Premises only)” on page 133
Setting filter, view, and policy options (Premises only)

Discovery Manager has a number of options designed to enable users to configure the content and format of the certificate information displayed in the certificates pages. Users can save useful configurations for repeated use. Filters, views, and policies can be saved as **Personal** for use by their creator. Super Administrators can create **Global** settings for use by all Discovery users.

---

**Note:**
The information in this section does not apply to Certificate Services.

---

**Note:**
Only global filters can be used in certificate rules.

---

**Figure 2:** Display menu

Topics discussed in this section include:

- “Setting filters” on page 87
- “Adding an intermediate CA certificate to the list of filters” on page 93
- “Editing a saved filter or policy, or creating a policy” on page 91
- “Configuring a view” on page 93
Filters

Use the Filter menu to display certificates with specific characteristics. Saved filters are used to specify certificates for any certificate rules that you configure (see “Configuring rules” on page 77 for information about Certificate Rules) and determine what certificate information appears in your charts (see “Creating and using charts (Premises only)” on page 95 for information about charts).

Policies

Policies are filters that have been created to select certificates with characteristics that Discovery administrators feel require more immediate attention—for example, certificates issued by specific untrusted CAs. Certificate lists are automatically checked against policies when the Dashboard page is displayed and certificates that fit the policy criteria appear under Policy Violations in the Dashboard page.

Additionally, certificates that violate policies are listed in Global or Personal policy violation reports depending on how the policy was saved. For more information about Discovery reports, see “Configuring email notification and reports” on page 66.

Views

Use the View menu to determine which columns appear on a certificates page. Use the options to temporarily remove or add columns. Saved views can also be used to customize the content of some reports. See “Configuring email notification and reports” on page 66 for information about email notification options.

Setting filters

Super Administrators or Administrators can save custom filters as global or personal. Users can only create personal filters.

**Note:**

By default, after you have set a filter it, remains set if you change the view or certificate list until you clear the filter (Filter > Clear filters). To change the default behavior select <Account name > Preferences > Reset Filters.

Many of the filters correspond to fields listed in the certificate Details page of Microsoft’s certificate viewer. For more detailed information about these fields, open the certificate in certificate viewer (double-click the certificate file) and, under the details tab, click Learn more about certificate details.
To set filters

1. Open the filter pull-down menu.

2. Configure the filter options that you want. Filters are ANDed together. Only certificates meeting all criteria are displayed.

For example, if RSA is entered in the key type field and 2048 is entered in the key length field, only certificates using RSA-2048 keys will appear in the list. Any logical combination of these fields can be used as a filter and saved for future use. If you have created custom fields, they also appear in this list.
Using the drop-down menu, some options such as DN can be phrased in the negative to filter for certificates that do not contain a particular characteristic: for example in DN field, building the logical statement DN doesn’t contain domain1 would filter out certificates with domain1 in the DN.

Common building blocks include:
- contains — is contained within the value—in a DN filter you might use contains myorg to find all certificates with the CN=<domain>.myorg.com.
- equals — is the exact value (for example, the exact and complete DN)
- < (less than) > (greater than) = (is equal to) <= (less than or equal to) => (greater than or equal to)
- in fields that accept a string, values can be ORed together to accept more than one value. For example in DN field, the logical statement DN contains domain1 OR domain2 would list certificates with domain1 or domain2 in the DN.

Note:
If you are attempting to get a list of Wildcard certificates using the asterisk (*) character, be aware that Discovery interprets the asterisk as a search for all certificates. Escape the asterisk using single quotes ‘*’ instead. The single quotes cause Discovery to search for the character: for example, contains ‘CN=*’ would find all certificates with CN=* in the DN.

- Load: Use this pull-down menu to load a saved filter.
- Save as: used to save the filter; specify a name by entering it here and press enter to save the filter.

In the Common Certificate Details menu:
- Subject DN: is the distinguished name of whatever is being protected by the certificate.
- Issuer DN: is the distinguished name of the CA that issued the certificate
- Cert Type: Certificate types can be:
  - End Entity: a computer or a user account on a computer
  - Self-signed root CA: a root certification authority
  - Subordinate CA: a certification authority not at the top of the chain of trust.
  - Self-issued CA (link cert): a certificate issued by the CA to itself when its keys are updated; they link the two self-signed certificates together
- Entrust Issued: Yes if issued by Entrust: No if not
- Public Trust: Yes if issued by a Public CA: No if not
• **Expires within**: only certificates that expire within this time period will appear in the list
• **Expires after**: only certificates that expire after this time period will appear in the list
• **Key Type**: the algorithm of the certificate key (for example, RSA)
• **Key Length**: the length of the certificate key (for example, 2048)
• **Key Usage**: this filter corresponds to the information that appears in Key Usage in the certificate details (see Figure ). Scroll to select the desired key usage. Use shift-select to select multiple options from the list. After you select an option a check mark appears beside the Key usage field.
• **Extended validation** (EV): EV certificates require additional validation of the authentication information supplied by the purchaser and are designed to promote consumer confidence in a Web site name.

In the **Other Certificate Details** menu:

• **Serial number**: the serial number of the certificate
• **SAN Count**: the number of subject alternative names in the certificate (the <> symbol indicates not equal to)
• **SAN contains**: one of the values in the SAN—for example, the certificate may be used in multiple locations with a value for every location
• **Signed By**: the algorithm used to sign the certificate (for example RSA-2048)
• **Digest Alg**: the algorithm used to create the digest (SHA-1, for example)

In the **Location types** menu:

**SSL**

• **SSL Hostname**: the hostname of the server where the certificate was found
• **Port**: the port protected by the certificate
• **Cert chain**:
  - **unknown**: filters for certificates where the completeness of the certificate chain cannot be verified—these certificates are usually scanned or manually added
  - **complete**: filters for certificates in which the certificate chain is verified to be complete
  - **incomplete**: filters for certificates in which the certificate chain is incomplete
    This is only meaningful if the CA is publicly trusted. Discovery stores information about certificate chains from public certificates that it has found previously and compares this information when establishing the completeness of a chain. Certificates from private CAs may be caught by this filter.
  - **self-signed**: filters for CA certificates where the signature of the issuing CA is the root signature

**Certificate Store**
• **Store Hostname**: the host name associated with the certificate store
• **Physical Store**: Enter the friendly name of the physical store (for example, registry).
• **System Store**: Enter the friendly name of the system store (for example, personal, trusted root, trusted people, other people).
• **Store Type**: specify computer or user to filter by
• **Store Username**: the user name associated with the store: an account—for example, for Alice Gray, a user in the test domain, the store might be test/agray

**Common**
• **# of locations**: the number of locations protected by the certificate

In the **Fields** menu:
• **Contact Name**: the contact name associated with the certificate in the Certificate Details page
• **Contact E-mail**: the email address associated with the contact
• **Contact Phone**: the telephone number associated with the contact
• **Physical Location**: the location specified in the Certificate Details page

In the **Miscellaneous** menu:
• **Organization**: allows you to filter by organization—any organizations that you have created appear in this list
• **Agent source**: allows you to filter by the Agent that reported the certificate.

The certificate page loads displaying the resulting list so you can confirm that the filter does what you intended.

3 If you want to save the filter:
   a  Click **Filter** a second time and type a name for the filter in the **Save as** field.
   b  Press Enter to save the filter.

If you want to return the page to the default filter and column settings, click **Clear Filters**.

**Editing a saved filter or policy, or creating a policy**

Filters that have been saved can be edited as required.

Filters can also be made into policies. Certificates that match policy filters are shown as policy violations on the Dashboard screen and in the Policy Violation Report.
To edit a filter or policy or to create a policy

1. In the Discovery Manager interface, on the upper right side of the page open the <user name > pull down menu.

2. Select Saved Filters.

3. Click Edit in the actions column for the filter you want to change.

For information about the various fields see “Setting filter, view, and policy options (Premises only)” on page 86.

4. In the Query Scope field select either User-Specific Query or Global Query. User specific queries are only available to the Administrator who created them. Global queries are available to any user. Only Super Administrators can create Global Queries.

5. If you want to flag this filter as a policy, select Enforces Policy.

6. Click Save to retain your changes.
Adding an intermediate CA certificate to the list of filters

If you are managing an intermediate CA certificate, Discovery gives you the option to track, on a per SSL location, basis which certificates were presented. Discovery also enables you to filter certificates based on whether a given intermediate certificate is presented.

1. From the Discovery Manager menu, click Certificates > Certificates list > <management state>.
2. Select the certificate from in the list.
   The Certificate Details page opens.
3. Select Find to add this intermediate certificate as a filter option.

The certificate becomes a selectable filter option in the Filter menu.

Configuring a view

Discovery allows you to customize the columns that appear on the Certificates page. Super Administrators or Administrators can save custom views as global or personal. Users can only create personal views.

To change how the certificate information appears on the Certificates page, open the View pull-down menu and deselect columns that you do not want to appear. Only columns that have been selected will appear. To rearrange the columns on the page, drag and drop them to the position that you want. To save the new configuration as a view, enter a name for it in the Save as field and press Enter. To use a saved view, select it from the Load menu.

Existing views can be edited or new views created in the Saved Views-Add New/ Edit page.
To edit or create a view

1. In the Discovery Manager interface, on the upper right side of the page open the <user name > pull-down menu.

2. Select Saved Views.

3. Click Edit in the actions column for the view that you want to change.

4. Optionally, if you want to save the edited view under a different name, type a different name in the Name field.

5. Optionally, type a description of the view in the Description field—for example, what distinguishes the view.

6. From the Scope menu select personal or global. Global views are shared with all users.

7. Select the columns for the view by moving entries between the Shown Columns and Hidden Columns panes. Shown columns appear in the view. Similarly the order of the Shown Columns determines the order of the columns on the Certificates page.

8. In the Sort By menu, select the default criterion to use to sort the certificate entries on the page.

9. Click Save to retain your changes.
Creating and using charts (Premises only)

Discovery provides a set of customizable charts for easy assessment of the status of certificates in your network. Super Administrators, Administrators, and Users can create additional types of charts. Super Administrators or Administrators can save custom chart types as global or personal. Users can only create personal charts.

To chart certificates that have a particular set of characteristics, create a filter to use with your chart (for information about configuring a filter see “Setting filters” on page 87). For example, you can use filters to exclude expired certificates or to only include SSL certificates with specific key types. Filters are extremely flexible.

Note:

If you have created organizations in Discovery, Administrators, and Users can only chart information from organizations that are assigned to them or information that is unassigned. Super Administrators have access to all of the information.

Charts can be added directly to the Dashboard page or, to avoid clutter and scrolling in the Dashboard page, Discovery provides a separate charts page. Drag and drop charts to reorder them on the page.

Procedures in this section include:

- “To add or edit a chart on the Dashboard page” on page 95
- “To add or edit a chart on the Charts page” on page 97
- “To create a chart type” on page 99

To add or edit a chart on the Dashboard page

1. From the main menu bar select Dashboard.
2. Select the plus icon (+) to the right of the **Charts** title to add a new chart to the page or select one of the existing charts to edit it.

The tool icons appear to the left of the chart if you are editing an existing chart. The pencil icon allows you to edit the page. The magnifying glass icon opens a larger image of the chart in a separate window. The x icon removes the chart from the page.

3. Select the pencil icon to edit the chart.

4. To use an existing type of chart and management state, use the pull-down menus. To configure a new type of chart select **Configure Charts** and go to “To create a chart type” on page 99. Custom chart types appear in the menu after they are created.
The list of chart types is user-specific. Global chart types appear to all users but personal charts appear to the person who created them. The following types of charts are included by default:

- **Certs by Expiry** charts certificates by the amount of time left before they are due to expire.
- **Certs by Agent** charts certificates by the Agent that reported them.

**Note:**
Only end entity certificates are used in the **Certs by Agent** chart. CA and intermediate certificates can be found by more than one Agent and would give a deceptive result if included.

- **Certs by Issuer Type** charts certificates according to the type of CA that issued them—for example, Entrust private for a privately operated Entrust CA.
- **Certs by Top Issuer Type** charts certificates according to the type of CA that issued the largest number of certificates.

5 Select the certificate state to be charted: Licensed (Monitored and Registered together) Monitored, Registered, or Discovered.

6 Click the green check mark icon to create the chart or the red x icon to cancel your changes.

**To add or edit a chart on the Charts page**

1 From the main menu bar select **Reports > Charts**.
2 Click **Add** to create a chart, or select an existing chart to edit it. The tool icons appear to the left of the chart. Select the pencil icon to edit the chart. The magnifying glass icon opens a larger image of the chart in a separate window.
3 In **Select a Chart to Display** select a chart type.
The list of chart types is user-specific. Global chart types appear to all users but personal charts appear to the person who created them. The following types of charts are included by default:

- **Certs by Expiry** charts certificates by the amount of time left before they are due to expire.
- **Certs by Agent** charts certificates by the Agent that reported them.

---

**Note:**

Only end entity certificates are used in the Certs by Agent chart. CA and intermediate certificates can be found by more than one Agent and would give a deceptive result if included.

- **Certs by Issuer Type** charts certificates according to the type of CA that issued them—for example, Entrust private for a privately operated Entrust CA.
- **Certs by Top Issuer Type** charts certificates according to the type of CA that issued the largest number of certificates.

4. Select the certificate state (Licensed is Monitored and Registered together, Monitored, Registered, or Discovered). Only certificates in the selected state are charted.

5. Use the green check mark icon to create the chart or the red x icon to cancel your changes.
To create a chart type

1. In the <account menu> select Saved Charts.

2. In the Saved Charts page, click Add.

3. Give the chart a meaningful name and description. Super Administrators have the option of creating global charts, which are available to all users.

4. Any filters that you have created appear in the Filter results by list. Use a filter to refine the results displayed in the chart. For example, you may want to display only certificates that have not expired or only SSL certificates. Filters can be configured with many different options. For information about creating filters see “Setting filters” on page 87.
5 Decide how you want the information to appear in the chart. Use the primary and secondary groupings to determine where the information appears in the chart. Discovery can create bar or pie charts.

6 By typing a numerical value in the **Only show # of results** field you can specify that the chart only displays the results from the top x number of whatever you are using in the “Group by” field. For example, if you are grouping by location and you enter 5 in the **Only show # of results** field, it will only use information from the five locations with the largest number of results. This allows you to simplify the chart if you expect a large number of instances of the category (for example a large number of locations).

7 Click **Save** to retain your changes.

The chart appears is the list of chart types the next time you configure a chart.
Using organizations to manage certificates (Premises only)

Use organizations to:

• assign the management of groups of certificates to specific Administrators
• compartmentalize the certificate information available to specific Administrators and Users

Super Administrators are able to see all Discovery information. Administrators and Users who are assigned to organizations can only see the information from those organizations or information about unassigned certificates.

Discovery allows Super Administrators to assign organizations to certificates either:

• individually from the **Certificate Information** page
• in bulk from a **Certificates** page
• using rules (“Configuring rules” on page 77)
• using the Web service (see the *Entrust Discovery Manager Web Service Guide* for information about using the Web service)

Only Super Administrators can assign organizations to Administrators. Administrators can assign unassigned certificates to their organizations or move certificates back and forth between organizations that are assigned to them. For example, if an Administrator is assigned to the Marketing and ISIT organizations, that Administrator can move certificates back and forth between the Marketing and ISIT organizations as well as the unassigned category.

**To create an organization**

1. From the main menu, select **Options > Organizations**.
2. Click **Add**.
3 Enter a meaningful name and description for the organization.

4 You can assign a contact email address to the organization. In the event that there is no contact entered, the organization’s Administrator gets the expiry mail for the organization. If there is no organization Administrator, notifications go to the default Administrator.

Administrators are assigned using the User Accounts page—see “Adding a user account” on page 103 for more information.

5 Click **Save** to create the organization.
User account options (Premises only)

This section explains how to perform common user account administration tasks. Topics in this section include:

- “Adding a user account” on page 103
- “Using Microsoft Active Directory (Premises only)” on page 108
- “Using Microsoft Active Directory (Premises only)” on page 108
- “Changing a user account password (premises only)” on page 114
- “Adding or editing a Web service account (Premises only)” on page 116

Adding a user account

Note:
The term user (lower case u) is used to refer to any account type (Super Administrator, Administrator, or User). The term User (upper case U) refers to a specific account type. The term administrator (lower case a) is used to refer to any administrative account (Administrator or Super Administrator)

Note:
The information in this section does not apply to Certificate Services.

Both Manager and Agent information in this section applies to Premises architecture. Premises architecture is described in “Entrust Discovery Manager with one or more Discovery Agents” on page 12.

If you are using a Premises installation, by default, Discovery has one (Super Administrator) account (entconfig) with all permissions. Super Administrators then create accounts as required. Three types of accounts with different permissions can be assigned to users as shown in the following tables.

Note:
If the user does not have permission to perform an action, the menu item associated with that action may not appear in the interface.
### Table 3: Discovery Manager permissions by role

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Super Admin</th>
<th>Administrator</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, delete, or rename customer organizations</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Move certificates from one organization to another</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign or unassign a certificate in any organization</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign or unassign a certificate within an organization that they administer</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Create, edit, or delete a user or Web service account</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Register, edit, or delete an Agent</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, edit, or delete custom fields</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, edit, or delete a Certificate Authority (CA) friendly name</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Create, edit, or delete email notification</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run email notifications</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import scan results or individual certificates</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Update configuration</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update license</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify an Issuer Rule</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>View an Issuer Rule</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Modify a Notice Rule</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a Notice Rule</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify a Certificate Rule</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a Certificate Rule</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Modify a chart (Administrators and Users are restricted to information from organizations Assigned to them)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Table 4: Discovery Agent permissions by role

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Super Admin</th>
<th>Administrator</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>View a chart (Administrators and Users are restricted to information from organizations assigned to them)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Modify saved filters</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Preferences</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

### Table 5: Web service permissions by role

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Super Admin</th>
<th>Administrator</th>
<th>User</th>
<th>Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get certificate information</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Import a certificate</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Modify a certificate</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Assign a certificate to an organization</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Get a list of organizations</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To add a user account to the Discovery Manager (Premises only) or Agent

1. From the Options menu, select Accounts > User Accounts.
2. In the User Accounts page, click Add.

3. Fill in the information about the account.
Username must be in the form of an email address. This is the name used with the password to log in to the discovery interface.

Optionally, enter a first name and last name for the user.

Select the account Role from the pull-down menu. Permissions associated with various roles are explained in Table 3, “Discovery Manager permissions by role,” on page 104 and Table 4, “Discovery Agent permissions by role,” on page 105.

If you are creating a Discovery Manager account, and you have created organizations, they appear in the Organizations pane. To assign the administration of an organization to this account, select it from the list. See “Using organizations to manage certificates (Premises only)” on page 101 for information about organizations.

Enter a password for the account and confirm it.

4 Click Save.
Using Microsoft Active Directory (Premises only)

Administrators can use Active Directory to manage Entrust Discovery Manager and Agent accounts. Before configuring this feature browse through the Login Rules for Active Directory section and decide how you want to structure Discovery user management.

Note:
The information in this section does not apply to Certificate Services.

If you are using an SSL connection between Active Directory and Discovery, before following these procedures:
- configure Active Directory to use SSL
- import the certificate from Active Directory into the Discovery Agent or Manager certificate store

Discovery accounts managed using Active Directory are listed as Externally-Validated Accounts on the User Accounts page.

Topics in this section are:
- “Configuring the connection, domain, and search base” on page 108
- “Setting caching for credentials” on page 110
- “Login rules for Active Directory” on page 110

Configuring the connection, domain, and search base

These parameters are used by Discovery when accessing Active Directory.

To configure Discovery to use your Active Directory settings

1. Under Options > Active Directory, select Active Directory Configuration.
2 Enter the IP address or hostname of the Active Directory host.

3 To secure the connection using Secure Sockets Layer (SSL), select **Use SSL**. SSL must be configured on the Active Directory end of the connection and you must have imported the SSL certificate from the Active Directory server.

4 Enter the port used by Active Directory. If you are using the default Active Directory port and you are using SSL, the port number is 636. If you are not using SSL, the default port number is 389. If you have changed the default port numbers of your Active Directory server, use your customized settings.

5 In **Bind Username** and **Bind Password** enter the user name and password of the account that will be used to access Active Directory. The Active Directory account only requires read access as Discovery does not write to Active Directory.

6 Enter the default Active Directory domain.
7 Enter the DN Search Base.

**Setting caching for credentials**

Options > Active Directory > Active Directory Advanced Settings allows you set the number of hours that Discovery caches credentials from Active Directory. If Discovery is unable to contact Active Directory, users will still be able to log in and have the correct role and accompanying privileges using the cached credential.

**Login rules for Active Directory**

For convenience, configure rules to determine the role that Discovery assigns to users from their characteristics in Active Directory. For flexibility, Discovery allows Super Administrators to configure rules using any combination of three different Active Directory characteristics:

- Base DN
- Required Entry Properties.
- Group

---

**Note:**

Rules can be activated and deactivated using the power icon.

---

**To configure a rule**

1 Under Options > Active Directory select Login Rules.
2 Click Add.
3 Enter a meaningful name in the Name field for easy identification. You may have several rules.
4 Determine how Active Directory identifies the users that will have a particular role. You can use Base DN, Required Entry Properties, Group membership, or a combination of these. If more than one field is used they are “ANDed” together.

If you are using the Member of Group field, enter the group name and click Look up matching Groups. Discovery will find the complete DN. Select the group from the drop down list and click the green check mark.
Note:
When you start to enter a Group and click Look up matching Groups, Discovery displays a drop-down list of possible groups. Although the entire DN of the group is shown in the drop-down list, only the part that you originally typed is displayed in the field, after you select a DN.

Discovery users who are familiar with Active Directory should find the criteria used to define the user accounts familiar. If you are not sure, the following sections contain a brief explanation of how to use the fields alone or in combination. If you require additional help, consult the Active Directory documentation provided by Microsoft or the Microsoft Developer Network Web site.

**Base DN**

Any of the components of the base DN can be used to specify a group of users in Active Directory. Using a second criteria you can further narrow the users with a role to a specific group. For example, a Login Rule for Discovery Super Administrators might include:

- a base DN that includes a specific CN such as CN=DiscoveryIT
- a second factor, such as a group or Required Entry Property (or both) that further restricts the Super Administrator role to a specific subgroup.

**Required Entry Properties**

Active directory stores a large number of entry properties. A property and its value can be used to define or restrict (if used with a group and/or a base DN value) the specific Active Directory users to whom the rule applies.

An simple example of the use of an entry property would be to use the CN property with a specific name as the value. In that case, the rule would apply only to a person with that name.

**Group**

Login rules can be used to restrict roles to members of specific Active Directory groups. If, for example, you have an existing administrator group and want the members or a subset of the members to have the Discovery administrator role, specify it in the group field. Base DN or required entry properties could be used to define a subset.

In the simplest case you can create a group for each of the three roles and assign Active Directory users to each group. An example of this method is:
• Create a group in Active Directory called Discovery Super Administrators.
• In Active Directory, assign all Discovery Super Administrators to the group.
• Create a rule in Discovery that all members of Active Directory’s Discovery Super Administrators group have the Super Administrator role.
• All members of the group will be able to log in with the Super Administrator role.
Changing a user account password (premises only)

By default, the password used to access the Discovery Agent or Discovery Manager entconfig account is entrust. While password change is not mandatory, it is recommended.

Note:
If you have only one account and you forget the new password you can uninstall and reinstall Discovery. This resets the entconfig account to the default password.

Super Administrators can update Administrator and User account passwords.

To change the password used to access the Discovery Agent

1 In the Discovery Agent interface, on the top left side of the page, select your user account name.
2 In the menu click My account.
3 Enter the new password and confirm it.
4 Click Submit.

To change your password for the Discovery Manager (Premises version only)

1 In the Discovery Manager interface, on the top left side of the page, select your user account name.
2 In the menu click My account.
3 Enter your existing password.
4 Enter the new password and confirm it.
5 Click Submit.

To update an Administrator or User Account password Discovery Manager (Super Administrator on Premises version only)

1 In the Discovery Manager main menu, select Options > Accounts.
2 Select the edit pencil icon next in the account row.
3 Click Update Password.
4 Enter the new password and confirm it.
5. Click **Save**.
Adding or editing a Web service account (Premises only)

A Web service account allows an application using the Discovery Web service to access the Discovery Manager. When the Web service account is created, Discovery assigns a login ID. The login ID and the password are used by the application for authorization to the Web service and should be relayed securely to the person creating the application using the Web service.

Web service accounts are associated with a role and have the permissions that go with that role. Be sure that the type of account has sufficient permissions to access the information.

To add or edit a Web service account

1. In the Discovery Manager interface, from the Options menu, select Accounts > Web Service Accounts.
2. In the Web Service Accounts page, click Add (to add an account) or select an existing account and click Edit to modify an existing account.
3. Enter the information about the account.

**Identifier** is any name that you want to use for the account.

**Role** corresponds to user roles. Permissions associated with various roles are explained in Table 5, “Web service permissions by role,” on page 105.

**Organizations** optionally allow Super Administrators to both delegate administration of specific groups and compartmentalize access to information about certificates.
Organizations appear as a list, (if you have created organizations). To assign an organization to this account, select it from the list. See “Using organizations to manage certificates (Premises only)” on page 101 for more information about organizations.

4 Assign a password to the account.

5 Click **Save**.

The Login ID appears in the entry for the account on the **Web Service Accounts** page.
Uninstalling Entrust Discovery (Premises only)

This section provides information about uninstalling Entrust Discovery. Topics in this section include:

- “Uninstalling Entrust Discovery from a Microsoft Windows platform” on page 118
- “Uninstalling Entrust Discovery from a Red Hat Linux platform” on page 118

Uninstalling Entrust Discovery from a Microsoft Windows platform

Entrust Discovery is uninstalled using Windows, like any other application. Data files are not uninstalled when you remove the Discovery application.

To uninstall the Entrust Discovery software

1. Select Start > Control Panel > Add or Remove Programs.
2. Select Entrust Discovery Manager (or Agent) and click Change/Remove.
3. Confirm that you want to remove the application.

Uninstalling Entrust Discovery from a Red Hat Linux platform

Entrust Discovery is uninstalled using Red Hat’s Package Manager, like any other application. Data files are not uninstalled when you remove the Discovery application.

To uninstall the Entrust Discovery software

1. Select System > Administration > Add/Remove Software.
2. In the Package Manager page select discovery-agent<version>.i386 (Discovery Agent) or discovery-manager<version>.i386 (Discovery Manager).
3. Click Apply.
4. Confirm your actions, when prompted.
Manually stopping and starting the application (Premises only)

Entrust Discovery applications start automatically after they are installed. If you shut down or restart your server and the Discovery software does not restart automatically:

- To start the Discovery Agent application on a Linux machine, as root, open a command-line terminal and type the following command:
  
  ```bash
  service discovery-agent start
  ```

  To stop and start the service substitute `restart` for `start`. To stop the service substitute `stop`.

- To start the Discovery Manager application on a Linux machine, as root, open a command-line terminal and type following command:

  ```bash
  service discovery-manager start
  ```

  To stop and start the service substitute `restart` for `start`. To stop the service substitute `stop`.

- On a Windows server, either application can be started from the Services list (listed as **Entrust Discovery Agent** and **Entrust Discovery Manager**).
Monitoring the Agent (Premises only)

The Discovery Manager **Agents** page indicates the state of the Agent-Manager link.

<table>
<thead>
<tr>
<th>Status</th>
<th>HostName</th>
<th>Description</th>
<th>Reported Version</th>
<th>Certificates Found</th>
<th>Last Sent</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthy</td>
<td>0.4.96(1.10)</td>
<td>OCMTLS</td>
<td>2.0.174</td>
<td>10</td>
<td>23 Feb 2012 09:44:07</td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>ISO-11508</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>ISO-11508</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Agent contacts the Manager once an hour and the time and date of the contact is recorded. If the Agent is late making contact, the Manager indicates a change in status.

- If the Agent has been in contact within the last hour the state is considered to be healthy, and a green check mark icon (✓) is displayed in the status column.
- If the Agent has not been in contact for 3 hours, a warning threshold is breached and the Manager displays an inverted yellow triangle and exclamation mark icon (!) in the **Status** column.
- If the Agent has not been in contact for 24 hours, an alarm threshold is breached and the Manager displays an x (✗) in the **Status** and generates a system notice.
- If the Agent-Manager link has never been established, a blue i icon (ℹ️) is displayed in the **Status** column.

The number of certificates recorded by the Manager as uniquely discovered by each Agent is displayed in the **Certificates Found** column. If Agent scans overlap and a certificate is discovered by more than one Agent, it will only appear in one Agent’s count.
Viewing the license information (Premises only)

To see your license information

1. From the main menu select **Options > Licenses**.

The page indicates:

- the status of the license (this should be “valid” if the license is usable)
- the name of the licensee
- version number
- the total number of certificates that can be licensed
- the number of uses remaining
- the number of certificates that have been licensed
- the type of license
Backing-up and restoring Discovery (Premises only)

Follow the procedures below to back-up and restore the Discovery Manager and Discovery Agents. The backup and restore process is simple and easily automated.

**Note:**
The information in this section does not apply to Certificate Services.

**To back up a Manager or Agent installed on Windows 2008**

1. On the machine hosting Discovery, stop the Discovery Manager or Agent service:
   a. Select **Start > Administrative Tools > Services**.
   b. Right-click **Discovery-Manager** or **Discovery-Agent**.
   c. Select **Stop**.

2. Copy the Data folder to a safe location, preferably on a different machine. By default, the Data folder is located in:
   - `c:\Program Files (x86)\Entrust\Discovery-Manager`
   - `c:\Program Files (x86)\Entrust\Discovery-Agent`

3. To continue using Discovery, restart the service:
   a. Select **Start > Administrative Tools > Services**.
   b. Right-click **Discovery-Manager** or **Discovery Agent**.
   c. Select **Start**.

**To restore a Manager or Agent installed on Windows 2008**

1. Install the Discovery Manager or Agent. Be sure that you can connect to the browser interface before continuing.

2. On the Discovery machine, stop the Discovery-Manager service:
   a. Select **Start > Administrative Tools > Services**.
   b. Right-click **Discovery-Manager** or **Discovery Agent**.
   c. Select **Stop**.

3. Overwrite the current Data folder with the backup Data folder. By default, the Data folder used by the Discovery Manager is located in:
c:\Program Files (x86)\Entrust\Discovery-Manager
or
c:\Program Files (x86)\Entrust\Discovery-Agent

4 To continue using Discovery Manager or Agent, restart the service:
   a Select Start > Administrative Tools > Services.
   b Right-click Discovery-Manager or Discovery Agent.
   c Select Start.

To back up a Manager or Agent installed on Red Hat Linux
1 On the machine hosting Discovery, stop the Discovery Manager or Agent service:
   From the command line enter:
   service discovery-manager stop
   Or
   service discovery-agent stop

2 Copy the Data folder to a safe location, preferably on a different machine. By default, the Data folder is located in:
   /opt/entrust/discovery-manager
   or
   /opt/entrust/discovery-agent

3 To continue using Discovery, re-start the service:
   service discovery-manager start
   Or
   service discovery-agent start

To restore a Manager or Agent installed on Linux
1 Install the Discovery Manager or Agent. Be sure that you can connect to the browser interface before continuing.

2 On the Discovery machine, stop the service:
   service discovery-manager stop
   Or
   service discovery-agent stop

3 Overwrite the current Data folder with the backup Data folder. By default, the Data folder used by the Discovery Manager or Agent is located in:
   /opt/entrust/discovery-manager
   or
/opt/entrust/discovery-agent

4 To continue using Discovery Manager or Agent, restart the service:

  service discovery-manager start

  Or

  service discovery-agent start
Database maintenance (Premises only)

Entrust Discovery does not do regular database maintenance. Discovery provides a manual tool that enables you to recover space in the database.

To view the database information, enter the following URL in your browser:

https://<host_name>:27535/discovery-manager/StoreMaintenance.action

Typically, unused allocated space exists when data is deleted from a table, or indexes are updated. By default, the database does not return unused space to the operating system. For example, once a page has been allocated to a table or index, it is not automatically returned to the operating system until the table or index is destroyed.

The Discovery DB Info page displays information about the used space, unused space and total space for various tables in the database. Use the db.compress.text link to compact specific tables and regain unused space.
Viewing Discovery logs and System Notices (Premises only)

Discovery Agent logs are written to:
<installation_root>/entrust/discovery-agent/log.

In the premises architecture, Discovery Manager logs are written to:
<installation_root>/entrust/discovery-manager/log.

Discovery includes several levels of logging so you can configure the degree of detail that you require, or you can turn off logging completely.

To change the log level on Discovery Agent or Discovery Manager (premises)

1. From the Discovery main menu select Options > Logging.
2. In the Logging page select the level that you require from the pull-down menu.

Note:
The host’s system logs may also be helpful in troubleshooting any connection problems.

System Notices are brief messages containing information about Entrust Discovery health and events. These messages appear on the Dashboard page of both the Discovery Agent and the Discovery Manager.

Administrators can use notice rules to manage notices. See “Configuring rules” on page 77 for details about the notice rules.

Note:
You can schedule Discovery to periodically send existing system notices to administrators, using email. For more information, see “Configuring email notification and reports” on page 66.
Viewing detailed version information
(Premises only)

To aid in determining the version of specific files after patches have been applied, Super Administrators can access a page containing detailed version information. This information may be useful for troubleshooting.

To access the Discovery Manager (Premises only) page containing this information, use the URL:

https://<hostname>:27535/discovery-manager/VersionInfo.action

For Discovery Agent use the URL:

https://<hostname>:27534/discovery-agent/VersionInfo.action
Changing the default listen port for the Agent or Manager (Premises only)

By default the Discovery Agent and Manager use ports 27534 and 27535 respectively. The port used can be reconfigured as outlined in the following procedures. These settings are not retained after an upgrade.

Note:
For a 32 bit Microsoft operating system, substitute Program Files for Program Files (x86) in the path used in these procedures.

To change the default Agent port:

1. Edit the Program Files (x86)\Entrust\Discovery-Agent\tomcat\conf\server.xml file and change connector port="27534" on a Windows OS or /opt/entrust/discovery-agent/tomcat/conf/server.xml on a Linux OS to the desired port number.
2. Restart the Agent service.
3. Use the new port in the URL used to access the Agent interface. If the new port is 443 then it can be left out of the URL since it's the default for HTTPS URLs.
4. If you use the Windows shortcut to access the Agent interface, update the shortcut file in Discovery-Agent\bin to use the new URL.

To change the default Manager port:

1. Edit the Program Files (x86)\Entrust\Discovery-Manager\tomcat\conf\server.xml file on a Windows OS, or /opt/entrust/discovery-manager/tomcat/conf/server.xml on a Linux OS and change connector port="27535" to the desired port number.
2. Restart the Manager service.
3. Access the Manager interface using the new port number in the URL. If the new port is 443 then it can be left out of the URL since it's the default for HTTPS URLs.
4. If you use the Windows shortcut to access the Manager interface, update the shortcut file in Discovery-Manager\bin to use the new URL.
5. For each Agent, under Options > Agent/Manager Link, specify the Manager location as Remote Location and set the Manager host name and port.
Attention:
If Manager and Agent are co-located, do not use the same port for both—doing so will cause connectivity issues.
Using an SSL certificate signed by a CA (Premises only)

By default, Entrust Discovery uses a self-signed SSL certificate. This causes the browser to issue a trust warning when users first log into either the Manager or the Agent. To eliminate the initial warning, use a certificate that is signed by a CA that is recognized by the browser.

The process of creating and importing the certificate is well documented. A utility such as keytool is commonly used for this purpose. A summary of the process is:

- Generate a private/public key pair on the server.
- Generate a certificate signing request (CSR) on the server.
- Using the CSR obtain a certificate from a CA.

**Note:**
If the certificate comes from a Publicly Rooted CA, the root certificate will already be in the trusted certificate store of client machines (provided they are up-to-date). If the certificate comes from a private CA, clients will need to import the root certificate into the trusted root store of their machines.

- Optionally, import the chain certificate (if the CA is not on the JRE trusted CA list).
- Import the SSL certificate into the new key store in Java format.

**To update Discovery to use the SSL certificate (Agent or Manager)**

2. In the https connector configuration, change `keystoreFile` and `keystorePass` to the key store you want to use.

**Note:**
Do not copy your key store over the default key store filename `tomcat.keystore`. Discovery checks this store and will overwrite it with its own self-signed certificate if it has changed. Use a different filename for your key store.

For example:

```xml
<Connector port="27535" maxThreads="200"
```
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="/opt/entrust/<public_keystore>.jks"
keystorePass="password" clientAuth=false sslProtocol="TLS"
maxPostSize="10485760" />
Listing certificate location by hostname or IP address (Premises only)

Starting with version 2.3, certificates are listed by the IP address of the host when they are discovered, and both hostname and IP address appear. Prior to Discovery Manager 2.3, certificates were listed against the hostname rather than the IP address of the scanned host. Additionally, the IP address of the host did not appear in the list of locations.

This change applies to certificates that are discovered after version 2.3 is installed, not to certificates found by earlier versions of Discovery, although new scans of existing locations will update the information to this format.

The advantage to using the IP address (default) option is that a certificate is listed in the Discovery certificates page as having one rather than multiple locations if several servers with different host names are used with a single host and IP Address—for example, in the case where example1.example.com, example2.example.com, and example3.example.com map to the same IP address.

The IP address setting (default) is the best choice in most cases, however the setting is configurable, allowing Super Administrators to change back to listing by hostname instead of IP address. Change this option if you want Discovery to discard IP address information and only use the hostname—for example, in cases where your organization restricts the IP address information.

---

**Note:**

If you are using the default (IP address option) Discovery recognizes that more than one certificate is valid when multiple IP addresses that are mapped to a single hostname. An example would be if mybank.example.com maps to more than one IP address (protected by a single certificate). Each IP address would be listed against that certificate on the certificates page.

---

**To switch between IP address and hostname**

1. In the Discovery Manager main menu, select **Options > Advanced Settings**.
2. In the IP Address in SSL Locations menu, select the identifier.
3. Click **Save** to retain the change or cancel to discard it.
Configuring the Switch or renew button (Premises only)

Either a Switch to Entrust or a Renew with Entrust button may appear on the Certificate Details page. Table 6 explains when they appear. The Switch or Renew URLs open the Entrust Certificate Services Web site, where you can purchase Entrust certificates. These URLs are configurable.

Table 6: When the Switch to Entrust or Renew buttons appear

<table>
<thead>
<tr>
<th>If the certificate type is:</th>
<th>the Switch. button appears?</th>
<th>the Renew. appears?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entrust public</td>
<td>No</td>
<td>Yes (by default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If an issuer-specific renewal URL is configured for an Entrust public CA, it overrides the default Renew Certificate URL button.</td>
</tr>
<tr>
<td>Non-Entrust public</td>
<td>Yes</td>
<td>No (by default)</td>
</tr>
<tr>
<td>Non-Entrust private</td>
<td></td>
<td>Yes —If issuer-specific renewal URL is configured under Rules &gt; Issuer Rules &gt; URL for renewing certificates.</td>
</tr>
</tbody>
</table>
If you want to change these URLs, select **Options > Certificate Enrollment**.

**Certificate Enrollment**

Use this page to configure the URL that is presented when a user clicks the “Switch to Entrust” or “Renew configured” button.

* required

<table>
<thead>
<tr>
<th>URL Type</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Certificate URL</td>
<td><a href="http://www">http://www</a> Entrust.net/</td>
</tr>
<tr>
<td>Renew Certificate URL</td>
<td><a href="http://www">http://www</a> Entrust.net/</td>
</tr>
</tbody>
</table>

**Issuer-Specific URLs**

There are no issuer-specific renewal URLs configured.

[Save] [Cancel]

Edit the URL to reflect the link or links that you want and click **Save**.
Index

A
Accessing the Agent interface 23
Accessing the premises Manager interface 23
Account
  adding an 103
  permissions 104
Active Directory
  configuring Discovery to use 108
  credential caching 110
  login rules 110
Agent 8
  accessing the interface 23
  installing Linux 18
  installing Windows 19
  registering 25
Agent health 120
Architecture
  agents only 14
  distributed 11
As needed certificate scan 37
Assigning a CA friendly name 73

B
Bulk update
certificate details 64

C
CA
  friendly name 73
Caching credentials
  Active Directory 110
CAPI scanning utility 41
Certificate
  information collected 8
  licenses 54
  management states 54
  manually importing 44
  scan 30
  summary report 75
Certificate Details 91
Certificate details
  changing fields in bulk 64
  custom fields 70
  management options 61
Certificate details page 52
Certificate management options 61
Certificate scan
  configuring 31
  manual 37
  monitoring 50
  uploading manually 39
Certificate scanning utility 8, 41
Certificate Store Result Monitoring 41
Changing
  passwords 114
Charts
  configuring 95
Communication, Agent/Manager 26
Configuring 78
  account permissions 104
  charts 95
  custom fields 70
  display options 86
  filters 87
  list filters 86
  organizations 101
  reports 67
  scan parameters 31
  views 93
  Web service account 116
Configuring Agent/Manager communication 26
Credential caching
  Active Directory 110
CSV report format 75
Custom fields 70

D
Database
  maintenance 125
Detailed information 10
Discovered state 55
Discovery Agent 8
Discovery components 8
Discovery Manager 9
Display options 86
Displaying certificate lists 86

E
Email notification 66
End Entity 89
Excluding hosts 34
Exporting a report 75

F
Filter options
- # of locations 91
- Cert chain 90
- Cert Type 89
- Contact E-mail 91
- Contact Name 91
- Contact Phone 91
- Digest Alg 90
- Entrust Issued 89
- Expires after 90
- Expires within 90
- Extended validation 90
- Hostname 90
- Issuer DN 89
- Key Length 90
- Key Type 90
- Key usage 90
- Location 91
- Organization 91
- Physical Store 91
- Port 90
- Public Trust 89
- SAN contains 90
- SAN Count 90
- Serial number 90
- Signed By 90
- Store Hostname 91
- Store Type 91
- Store Username 91
- Subject DN 89

System Store 91
Filters
- configuring 87
- editing 91
- fields 87
- resetting 87
- Friendly name 73

G
Getting started 22

H
Host list 36
- creating 34
- Hosts 33
- preconfigured list 36

I
Ignored state 55
Importing a license file 23
Importing certificates manually 44
Information collected 8
Installing
- Agent, Linux 18
- Agent, Windows 19
- Manager, Linux 20
- Manager, Windows 21

L
License file
- importing 23
Licensing 16
Licensing certificates 54
Location of log files 126
Logs
- changing log levels 126
- files, location of 126
- setting the logging level 126
M
Management options
certificates 61
Management states
assigning 54
assigning in bulk 58
definitions 55
Manager 9
installing, Linux 20
installing, Windows 21
what is 8
Manager interface premises
opening 23
Manual certificate upload 39
Manual import 44
Manually starting a scan 37
Microsoft Active Directory
see Active Directory 108
Monitored state 55
Monitoring
agent health 120
certificate scan 50

N
Notices
custom fields 70
Notification
e-mail 66

O
Organization 9
adding to a user account 107
and chart information 95
assigning with a rule 82
creating 101
permissions 104

P
Password
changing 114
Permissions
Administrator 104
Super Administrator 104
user 104
Policy 67
creating 91
violations 91
Policy Violation Report 91
Port range 33
Preconfigured scan list 36
Preferences 87

R
Registered state 55
Registering Discovery Agents 25
Reports
configuring 67
custom fields 70
e-mail 66
Rule
certificate 82
configuring 77
issuer 78
notice 79
Types 77

S
Scan
configuring 30
parameters 31
schedule 33
Scan information, monitoring 50
Scan list, preconfigured 36
Scan Rates 35
Scanning as needed 37
Security Manager 47
Self-issued CA (link cert) 89
Self-signed root CA 89
Starting the discovery application 119
Subordinate CA 89
Summary report 75
Switch to Entrust link 133
System notices 126

T
Table options 86
Token
generating 25
what is  26

U
Uninstalling
   Linux  118
   Windows  118
Uploading a certificate scan
   manually  39

V
Version information
   detailed  127
View
   configuring  93

W
Web service account  116