COMODO
Creating Trust Online®

Comodo
Certificate Manager

Code Signing on Demand
Hosted Version

Comodo CA Limited,
3rd Floor, 26 Office Village, Exchange Quay,
Trafford Road, Salford,
Greater Manchester M5 3EQ,
United Kingdom

1 Introduction

Code Signing on Demand (CSD) offers customers a faster, more intuitive and highly secure way to digitally sign their software. The service is available in both hosted and cloud versions and is capable of signing EXE .DLL .CAB .MSI .OCX .SY, JAVA JAR and Android application files. The service is available in two modes:

- **In-House Hosted Mode** - Requires a controller installed on your network. The controller will generate CSD enabled code-signing certificates for developers to sign files. The certificates and their private keys are stored in encrypted form in a local database created by the controller.

  HSM integration. You can also configure the controller to generate and store the code-signing certificate on a local Hardware Security Module (HSM). Keys will be generated in PKCS # 11 format and saved in non-extractable format on the HSM device.
- **Cloud Service Mode** - The signing service is hosted on Comodo's highly secure cloud servers. The service generates CSD enabled code signing certificates for developers to sign files. The certificates and their private keys are generated and stored in encrypted format in Comodo's data-center for the lifetime of the certificate, tightly protected by Comodo's military grade security infrastructure.

  HSM integration. Please contact your account manager if you want to setup HSM integration while using cloud service mode.

This document describes how to setup and use the CSD service in **In-House Hosted Mode**.

The Code Signing on Demand (CSD) feature is not enabled by default. If you require the CSD service, please contact your account manager.

Once enabled, the 'Code Signing on Demand' tab will appear in the title bar. The MRAO administrator can download the setup file for the CSD service controller from the 'Code Signing on Demand' > 'Configuration' interface and install on a local server to handle the code signing process.

CCM allows you to add developers and enroll CSD enabled code signing certificates for them. On enrolling for a code signing certificate, the controller generates the certificate request for the developer and submits the request to CCM. The controller tracks the order number. Once the certificate is issued, the controller will download the certificate and store it in your local network. The developer can then upload the files to the local portal for signing. Upon approval by the administrator, the controller signs the file and notifies the developer to download the signed file. Private keys are generated and stored in encrypted format within the host's network.

Please see the following links for help to set up the service:

- The 'Code Signing on Demand' Interface
- Set up the CSD controller
- Add Developers
- Obtain a Code Signing Certificate For CSD
- How to sign code using CSD
- Configure the CSD service

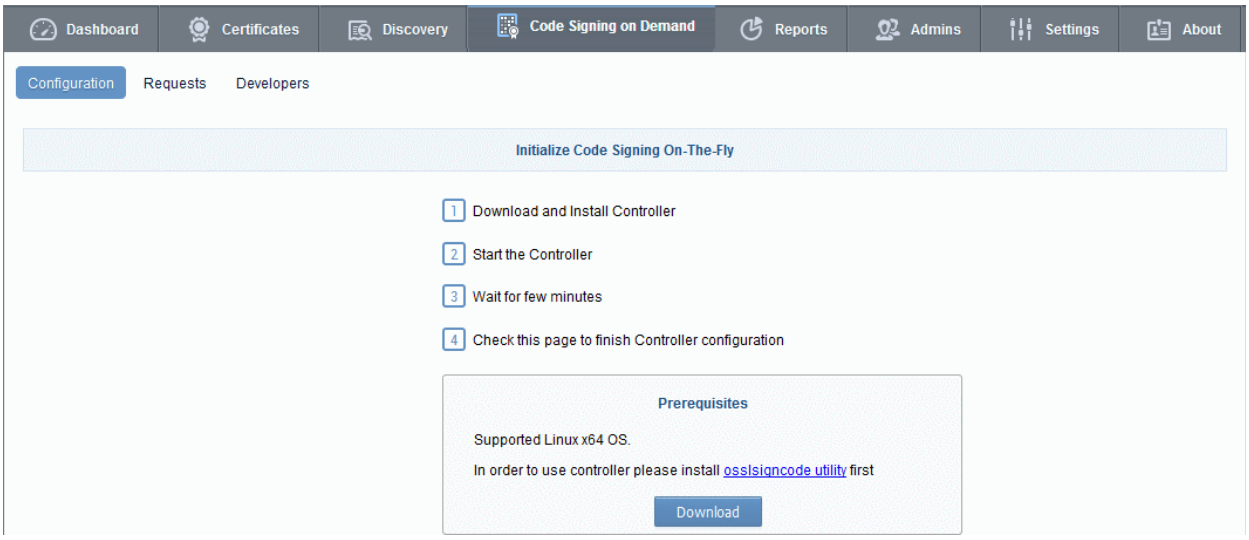
1.1 The 'Code Signing on Demand' Interface

The 'Code Signing on Demand' area allows you to configure the service controller, add and manage 'Developers', and manage developer signing requests.

The 'Code Signing on Demand' area is divided into three main administrative areas, namely:

- The 'Configuration' tab - Allows you to download the agent required for hosted mode
- The 'Requests' tab - Allows you to view and approve/decline code signing requests from developers

- The 'Developers' tab - Allows you to add and manage 'Developer' accounts in CCM.



Visibility of the 'Code Signing on Demand' area is restricted to:

- MRAO administrators - can configure the controller and add developers and manage code signing requests for any Organization or Department.
- RAO Code Signing administrators - can add developers and manage code signing requests only for Organizations (and any subordinate Departments) that have been delegated to them.
- DRAO Code Signing administrators - can add developers and manage code signing requests only for Departments that have been delegated to them.

1.2 Set-up the CSD Controller

You can download the controller software from the 'Code Signing on Demand' > 'Configuration' area and install it on a Linux server within your local network. Once installed and connected, the service can be configured from the same interface. See **Configure the CSD service** for more details.

Setting up the Code Signing on Demand (CSD) controller involves two steps:

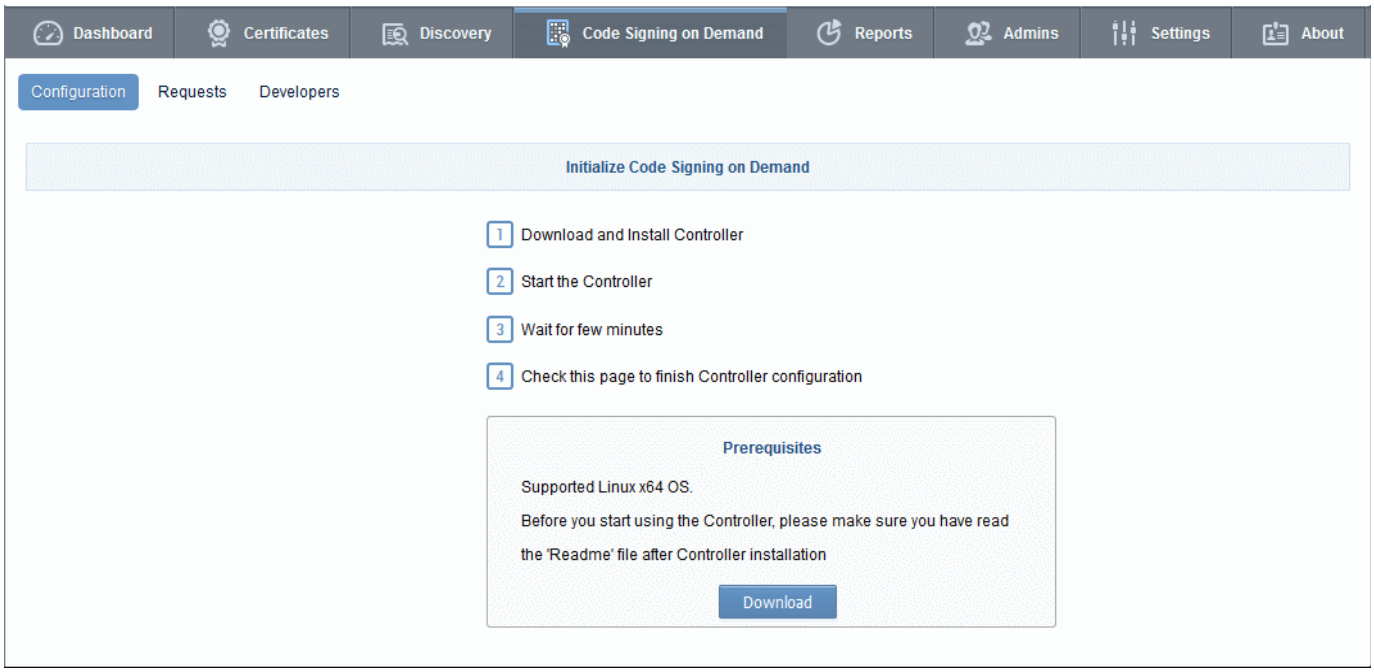
- **Installing the CSD Controller**
- **Installing the Osslsigncode tool**

Installing the CSD Controller

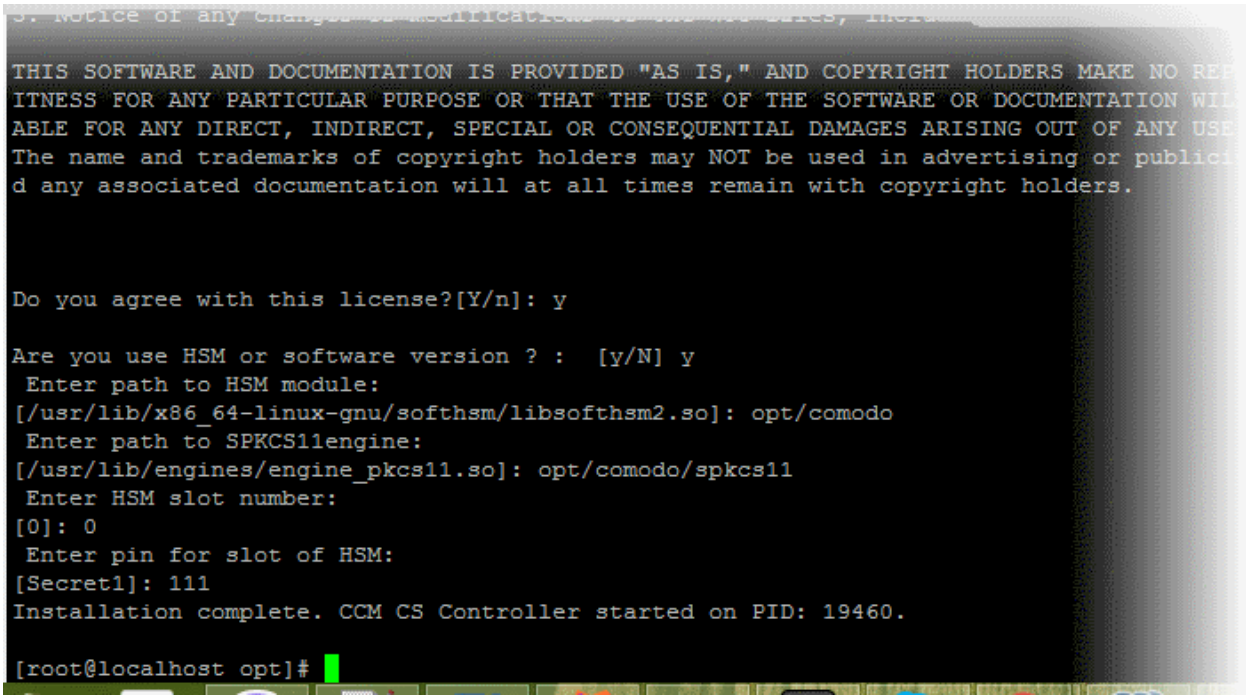
You can download the setup file for the CSD controller from the CCM interface as a .bin file and install it on the Linux server through command line. The controller can be configured to generate the private and public keys for the CS certificates. You may also elect to generate the keys on a Hardware Security Module (HSM).

To download and install the controller setup file

- Click the 'Code Signing on Demand' tab then click 'Configuration'



- Click the 'Download' button.
- Transfer the file to your Linux server.
- Install the CSD Controller on the Linux server from the command line.



- After accepting to the EULA, the option for setting the HSM integration will appear.
- Enter 'Y' if you want to use a HSM or 'N' if you wish the controller to generate and store the keys in its vault
- If you elect to use a HSM, enter the following parameters one by one:
    - Network path to the HSM module
    - Path to SPKCS 11 Engine
    - HSM Slot Number to be used
    - PIN number for the HSM Slot

Upon successful connection, the controller will be installed and will connect to the CCM server. You can configure

the controller from the CCM interface. Refer to the section **In-House Hosted Mode** for more details.

> **Note**: Your HSM appliance may need some additional configuration to generate keys. Refer to the instructions in the owner's manual of your appliance.

Installation of Osslsigncode tool

- Download the tool from **http://sourceforge.net/projects/osslsigncode/**

The tool's installation procedure depends on the distributive version and your environment.

> **Note**: It is recommended to install the osslsigncode tool into /usr/bin. Otherwise, the CSD Controller may not have access to it and you will need to provide it manually.

1. **Latest CentOS**

   yum install gcc intltool libxml2-devel glib2-devel libcurl* openssl* bzip2* gdk*

   wget **http://ftp.gnome.org/pub/GNOME/sources/libgsf/1.14/libgsf-1.14.34.tar.xz**

   tar -xf libgsf-1.14.30.tar.xz

   cd libgsf-1.14.30

   ./configure --prefix=/usr

   make

   make install

   cp /usr/lib/pkgconfig/libgsf-1.pc /usr/lib64/pkgconfig/libgsf-1.pc

   pkg-config libgsf-1 --modversion

   cd ..

   cd osslsigncode-1.7.1

   ./configure

   make ; make install

2. **Latest Debian**

   apt-get install libbz2-dev libgdk-pixbuf2.0-dev glib2.0-dev libxml2-dev intltool libcurl4-openssl-dev libssl-dev

   wget **http://ftp.gnome.org/pub/GNOME/sources/libgsf/1.14/libgsf-1.14.34.tar.xz**

   tar -xf libgsf-1.14.34.tar.xz

   cd libgsf-1.14.34

   ./configure --prefix=/usr

   make

   make install

   cd ..

   cd osslsigncode-1.7.1

   ./configure

   make ; make install

3. **Other Linux**

   i. Download and unzip osslsigncode-1.7.1.tar.gz from http://sourceforge.net/projects/osslsigncode/

   ii. See README.txt. The usual installation has 3 steps:

./configure

make

make install

Note: Usually the installation will require extra dependencies that should be previously installed.

Environment Tuning

1. Configure Controller's Web Server

   The controller out of the box contains self signed certificate installed on Jetty Web Server. In case if client's browser restricts access to Sites without public trust certificates, you need to update Jetty Web Server certificate.

   Please follow the instructions:

   i. Get or Enroll public trust SSL Certificate.

   ii. Put the Certificate and Private key into Java Key Store (JKS) with password. E.g. file 'cs-agent.jks' and password '12345'

   iii. Copy the file into 'conf' directory inside the Controller. Usually: '/opt/comodo/ccmcscontroller/conf'

   iv. Update 'agent.properties' file which is located in 'conf' directory inside Agent.

   Usually: '/opt/comodo/ccmcscontroller/conf/agent.properties'. Specify JKS file and password

   ssl.keystore=cs-agent.jks

   ssl.keystore.password=12345

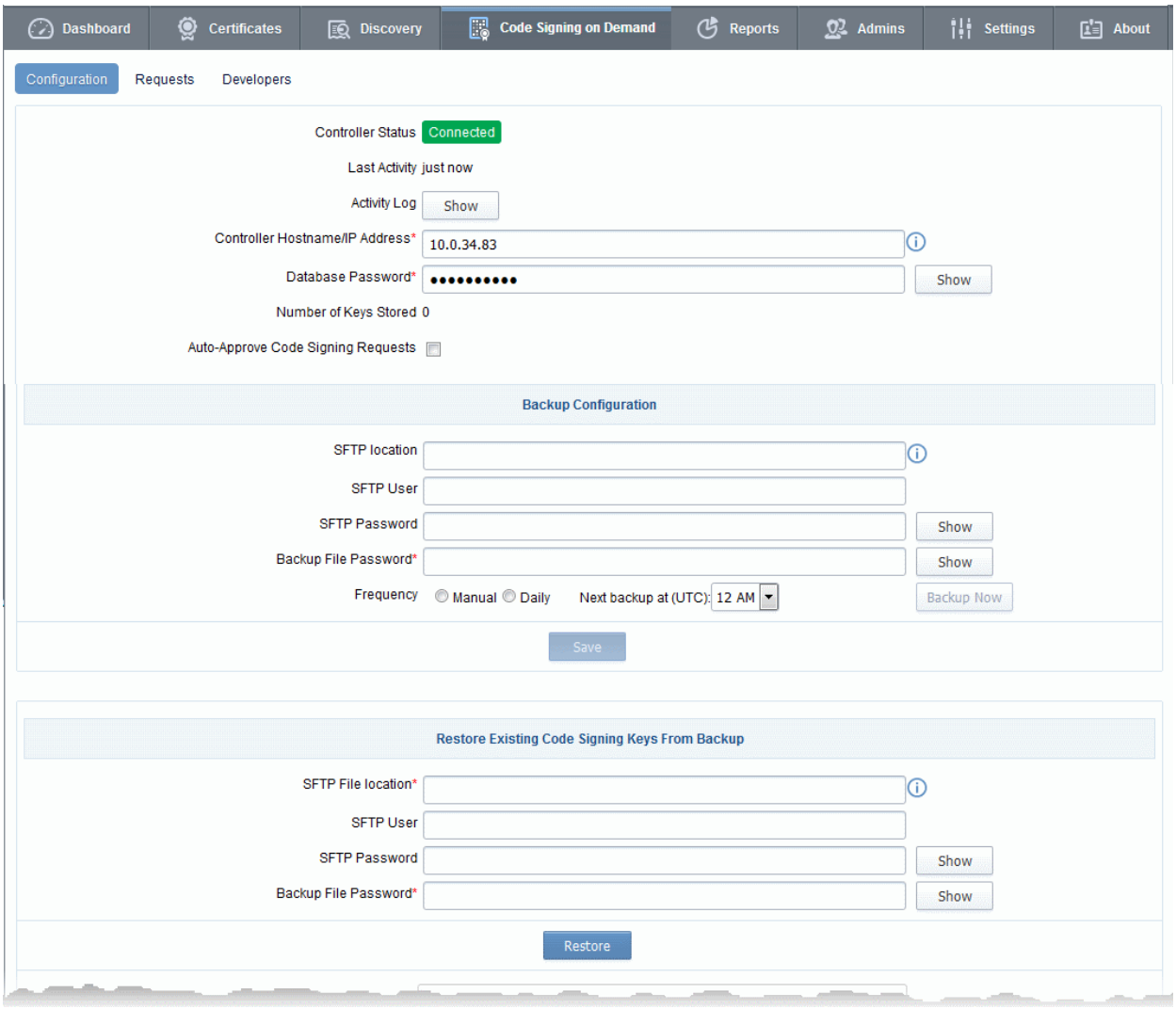
   v. Restart the Controller. Usually: '/etc/init.d/ccmcscontroller stop' and '/etc/init.d/ccmcscontroller start'

2. The Controller needs to accept incoming requests. Check that the default Controller's port 9092 is open.
3. Make sure that the 'hostname' command returns a valid Hostname.

On completion of installation, the controller will automatically establish connection to CCM and start running immediately.

During the first run, the controller connects to CCM, obtains the configuration files updates its configuration and generates a password for its database.

The 'Code Signing on Demand ' > 'Configuration' area will display the status as 'Connected' and shows the IP address of the server upon which the controller is installed. The controller periodically polls CCM and obtains the commands from it for execution.



Code Signing on Demand - Configuration Interface - Table of Fields and Controls	
Field	**Description**
Controller Status	Indicates whether the controller is currently connected to CCM or not.
Last Activity	Indicates the date and time of last polling of the Controller to CCM
Activity Log	Clicking the 'Show' button opens the Commands dialog that displays the list of command received by the controller form the CCM and their execution status. Refer to the section **View Activities of the CSD Controller** for more details.
IP Address	Displays the IP address of the server on which the controller is installed.
Database Password	The password for the protecting the database. The password is used for encrypting the stored certificates and their private keys in the database. The password is auto generated and cannot be changed by the administrator. • Clicking the 'Show' button displays the password.
Number of Keys Stored	Shows the number of certificates and their private keys stored and managed by the Private Key Store controller.
Backup Configuration	

SFTP location	The administrator can specify the location/URL of the SFTP server for the backup of the Code Signing certificates and their keys. Refer to the section **Backup/Restore Code Signing Certificates** for more details.
SFTP User	The username for the account in SFTP server, for access by the CSD service controller.
SFTP Password	The password for the account in SFTP server, for access by the CSD service controller.
Backup File Password	The password for encrypting the files stored in the backup server
Frequency	The frequency at which the database backup operations are executed. Refer to the section **Backup/Restore Code Signing Certificates** for more details.
Save	Saves the backup configuration

1.3 Add Developers

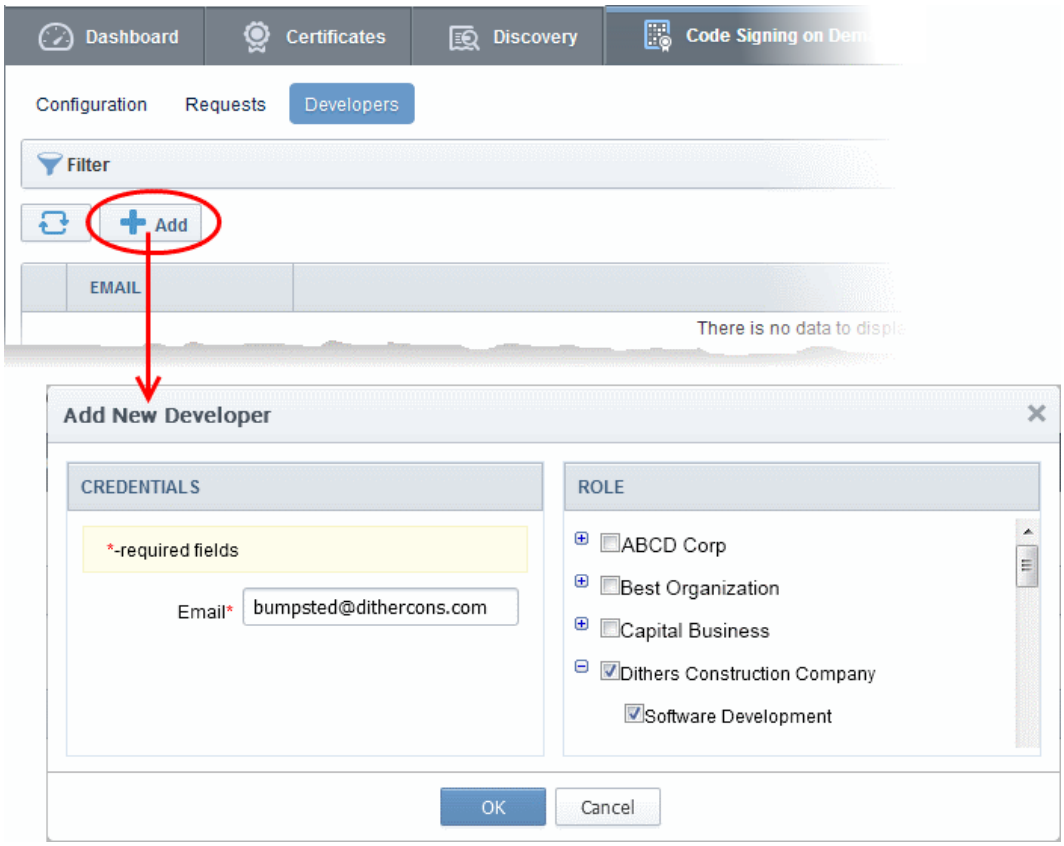
A 'Developer' is a role in CCM with permission to:

- Login to the CSD service
- Upload files for code-signing
- Download code-signed files

You can create a developer as a new user, or add developer privileges to an existing CCM user. An MRAO or RAO administrator will need to approve the developer's actual signing requests, unless you enable auto-approve in the **CSD configuration** screen.

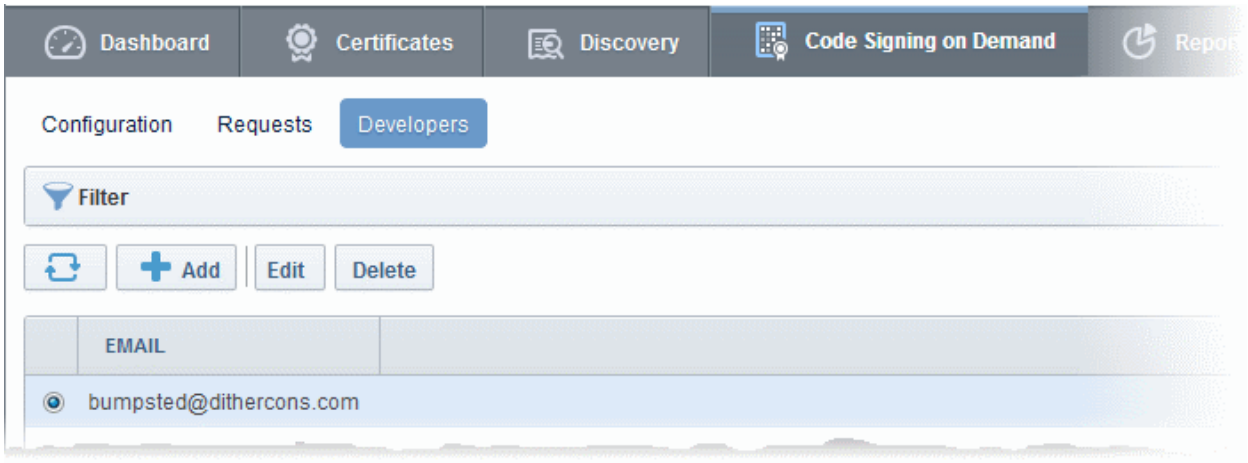
To add a developer

- Open the 'Developers' interface by clicking 'Code Signing on Demand' > 'Developers'
- Click the 'Add' button. This will open 'Add New Developer' dialog.

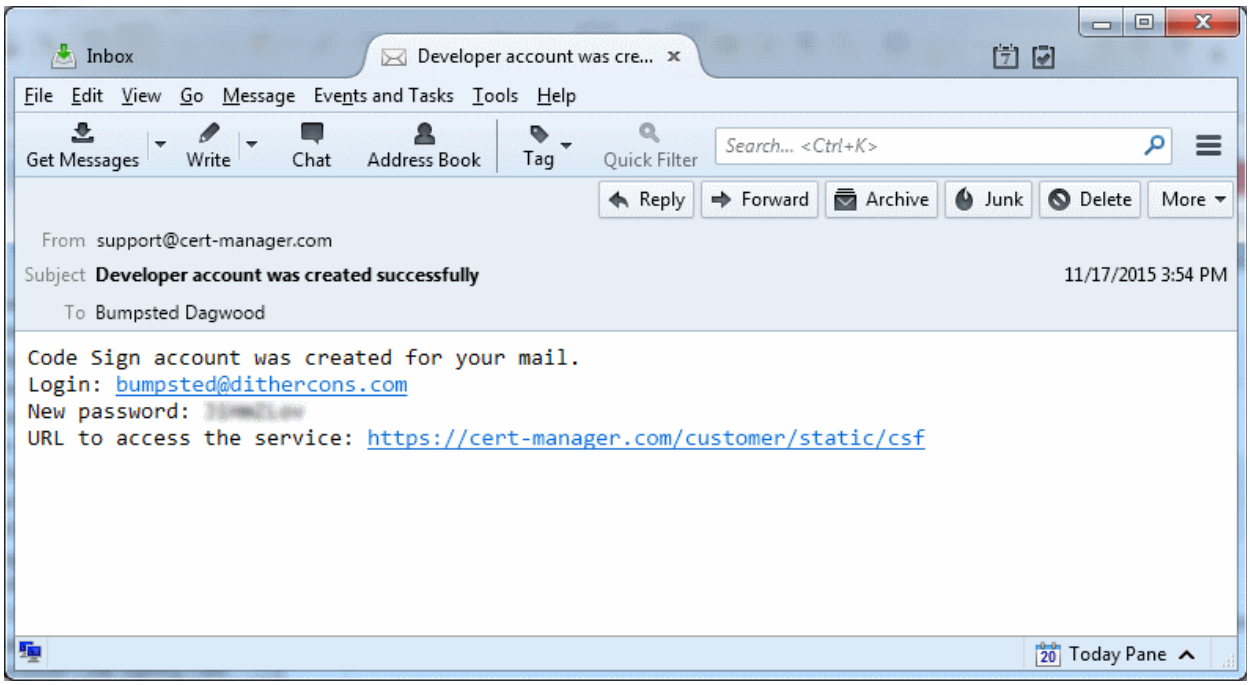


- Type the email address of the developer in the email field.
- Select the Organization(s) / Department(s) to which the developer should belong on the right
- Click 'OK' to confirm your selection.

The developer will be added to the list. You can edit the user to change their Organization/Department, reset their password or remove the developer.



A notification email will be sent to the developer with the credentials to access the CSD service. An example is shown below:

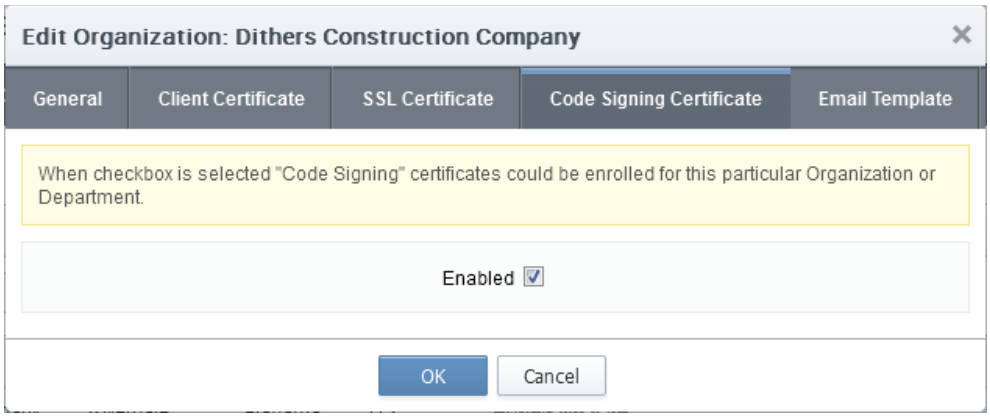


1.4 Obtain a code-signing certificate for CSD

Prerequisites:

- You have created a 'Developer' role as explained in the preceding section.
- The domain for which the code signing certificate is to be issued has been enabled for Code Signing certificates and that the domain has been activated by your Comodo account manager. For example, if you wish to issue code signing certs to end-user@mycompany.com, then mycompany.com must have been validated by Comodo. All certificate requests made on validated domains or sub-domains are issued automatically. Certificate requests for new domains will first have to undergo validation by Comodo.

- The domain from which the code signing certificates are to be issued has been delegated to the Organization or Department.
- The RAO Code Signing or DRAO Code Signing administrator has been delegated control of this Organization or Department.
- The MRAO or delegated RAO administrator has enabled Code Signing Certificates for the Organization/Department by selecting the 'Enabled' check-box in the 'Code Signing tab' of the 'Add New/Edit' Organizations dialog box (see screen-shot below)



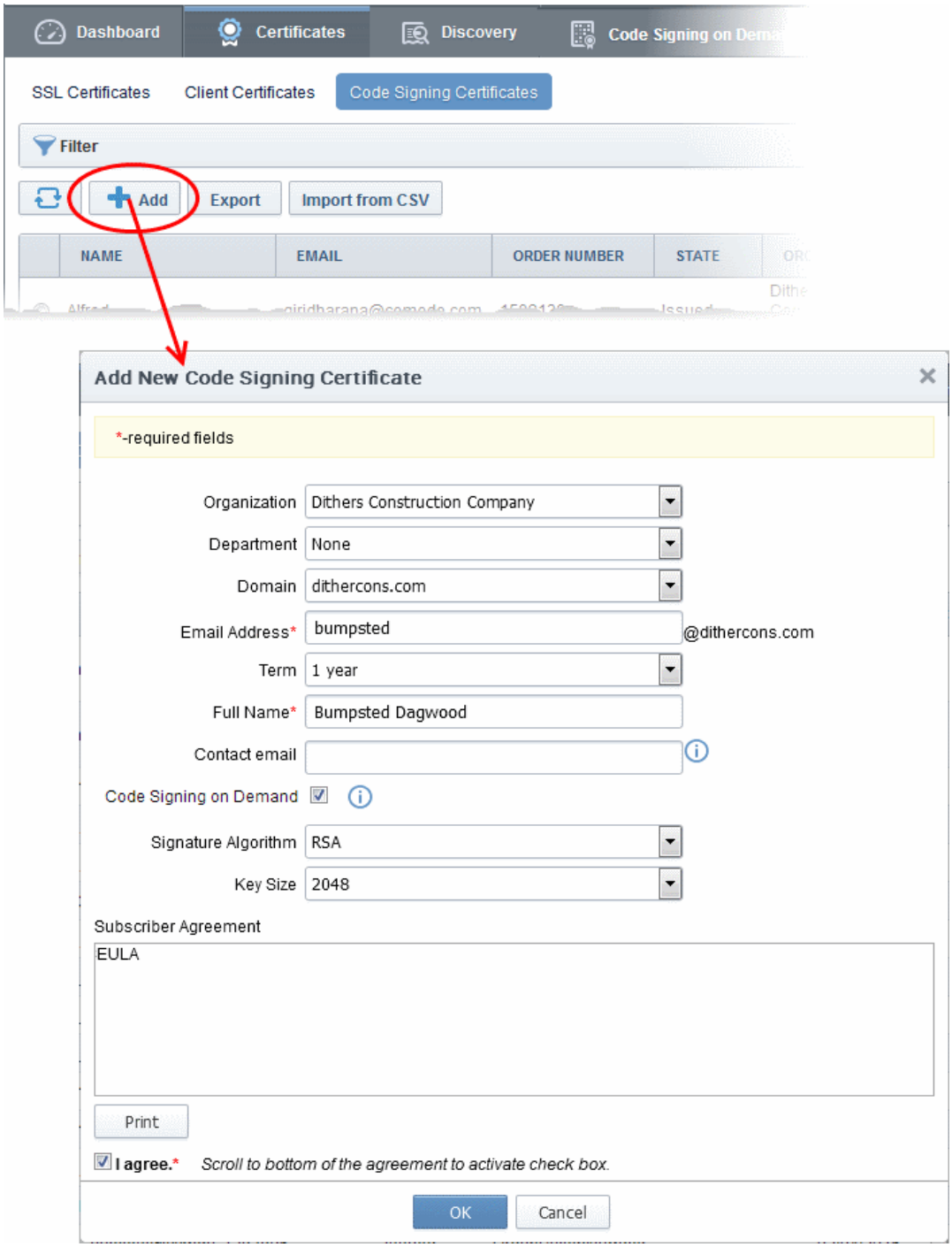
- The CSD service controller is installed on the local network and connected to CCM.
- Optional. You have chosen to generate and store keys on a HSM appliance.

Procedure Overview:

1. The administrator confirms the completion of the prerequisite steps.
2. The administrator adds a new code-signing certificate for the Developer from the 'Certificates' > 'Code Signing Certificates' interface, with 'Code Signing on Demand' enabled for the certificate. The CSD controller generates and stores the key pair locally and submits the CSR to Comodo CA. Once the certificate is issued, the CSD controller automatically downloads the certificate and stores it in your local network. If a HSM appliance is used, the key pair is generated and stored on the HSM. On issuance of the certificate, the controller downloads the certificate and stores it on the HSM appliance.

To enroll a code signing certificate for the developer

- Open the 'Code Signing Certificates' interface by clicking 'Certificates' > 'Code Signing Certificates'
- Click the 'Add' button to open the code-signing certificate application form.
- Complete all required fields on the form, making sure:
  - The correct developers email address is used.
  - The correct Organization and Department are specified for the developer.
  - The 'Code Signing on Demand' box is checked.



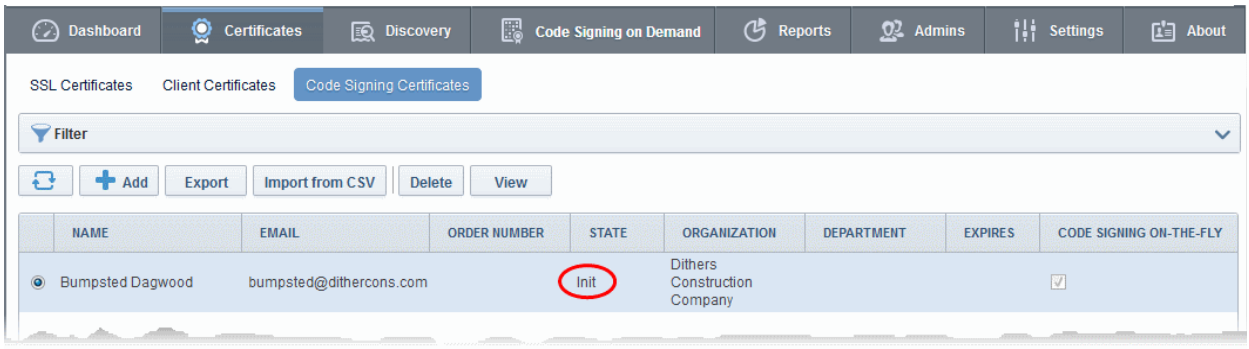
The following table explains the fields on the form:

Field	Description
Organization	Select the Organization to which the developer belongs.
Department	Select the Department to which the developer belongs.
Domain	Select the domain pertaining to the Organization/Department
Term	Select the term of the certificate.
Email Address	Enter the email address of the developer.
Full Name	Full name of the applicant.

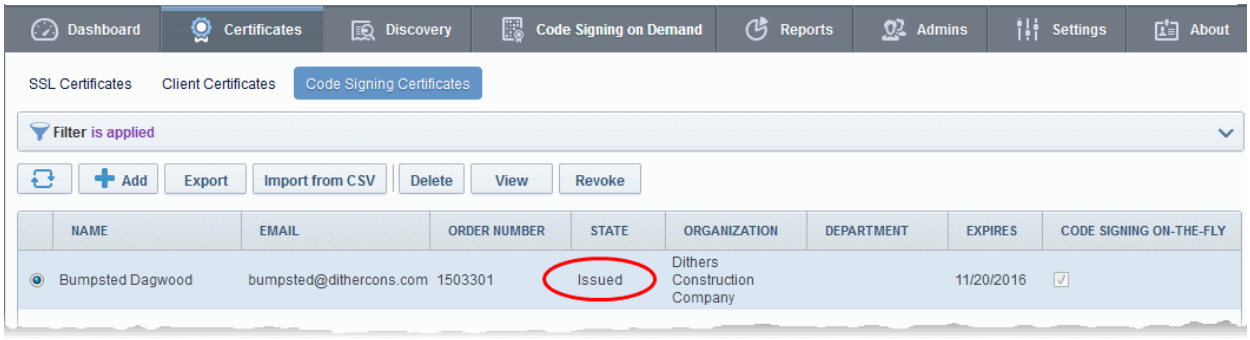
Field	Description
Organization	Select the Organization to which the developer belongs.
Contact Email	Enter the contact email address of the applicant that should be included in the certificate. The contact email address may be the customer facing email address like support@company.com, sales@company.com etc.
Code Signing on Demand	Enable this check-box to allow the certificate to be used by the CSD service.
Signature Algorithm	Choose the signature algorithm to be used by the certificate.
Keysize	Choose the key-size (in bits) by the certificate.
Subscriber Agreement	Displays the End-User License Agreement (EULA) for the certificate. Read through the EULA and accept to it by selecting the 'I agree' checkbox for the application to proceed.

- Click 'OK' to submit the request.

The certificate will be added with the state 'init' indicating that the certificate enrollment has been initiated.



Once issued, the state of the certificate will change to 'Issued': The controller will download and save the certificate in the local network.



The certificate can now be used to sign code submitted by your developer. Each signing action will, however, need to be approved by an administrator UNLESS you enable 'Auto-approve code signing requests' in **CSD Configuration**.

1.5 How to sign code using CSD

Once you have **created a developer** and **obtained at least one CSD enabled code-signing certificate**, your developer is ready to upload files for signing.

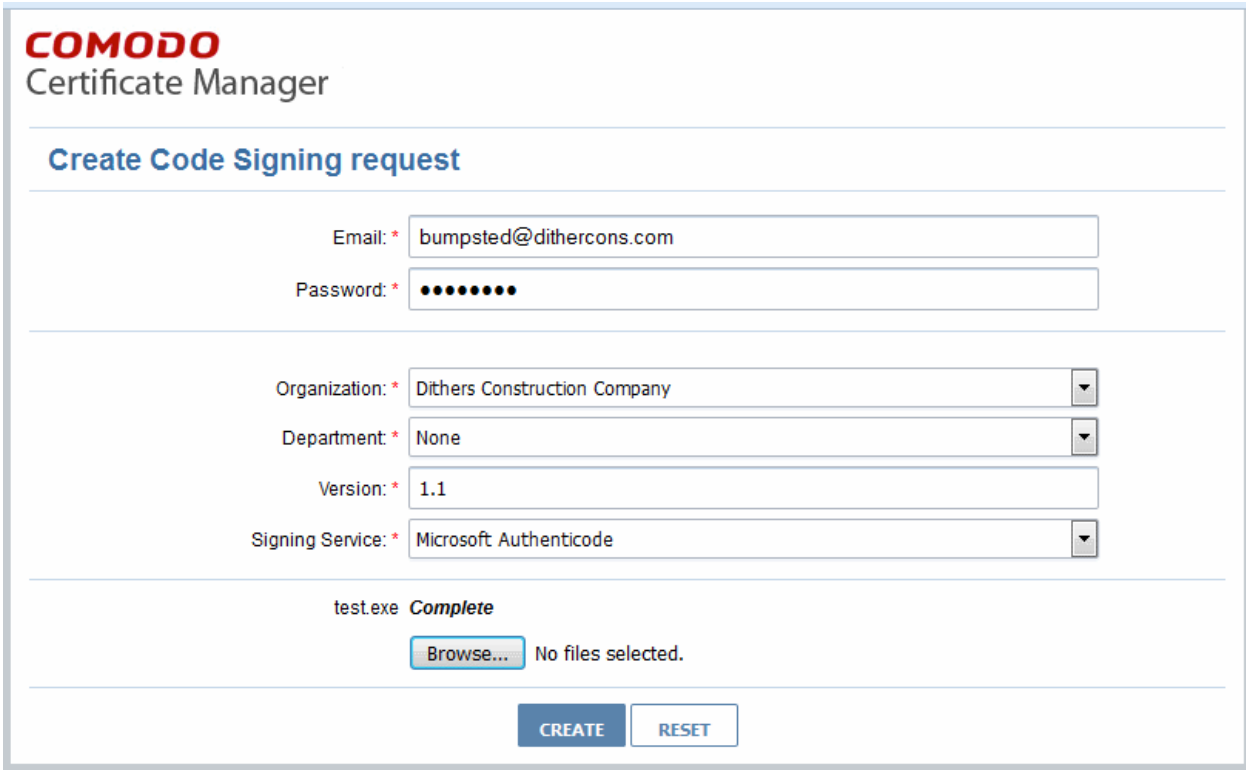
Overview of steps:

- **Step 1 - Upload the files to be Signed** - The developer logs-in to the CSD service portal, enters the details of the file(s) to be signed, selects the signing service and uploads the files. This will create a request which can be viewed in the 'Code Signing on Demand' > 'Requests' interface. See **Step 1 - Upload the files to be Signed** for more details.
- **Step 2 - Approve the Code Signing Request** (optional) - The Administrator views the request, checks the files to be signed and approves the request from the 'Code Signing on Demand' > 'Requests' interface. See **Step 2 - Approve the Code Signing Requests** for more details. Note - this step can be skipped if 'Auto-Approve Code Signing Requests' is enabled in 'Configuration'.
- **Step 3 - Download Code-Signed files** - Once approved and digitally signed, the status of the request will change to 'Signed'. A notification mail is sent to the developer with a URL to download the signed files. See **Step 3 - Download Code Signed Files** for more details.

Step 1 - Upload the files to be Signed

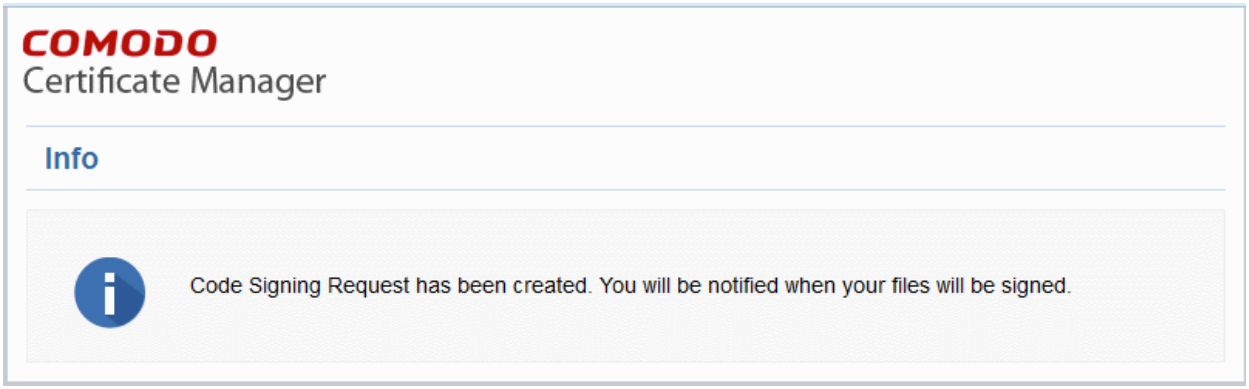
Once a developer has been added to CCM they will be able to login to CCM using the link in their confirmation email. By default, the format of this URL is: https://cert-manager.com/customer/[REAL CUSTOMER URI]/csd.

- After logging in they can upload files using the following form:



- **Organization** - Displays the organization(s) to which the developer belongs. The organization selected here will be shown in the certificate as the publisher of the software.
- **Department** - Allows the developer to choose a department If departmental information is also required in the certificate.
- **Version** - Developer should type the version number of the software they wish to sign
- **Signing Service** - Select the signing service. Choices are 'Microsoft Authenticode', 'Java' and 'Android'.
- **Browse...** - Developer should choose the files they wish to upload and sign.

One all fields are complete and the file has been selected, click the 'Create' button to submit the signing request to the CSD service. A confirmation dialog will be displayed:



A code signing request will be created in the 'Code Signing on Demand' > 'Requests' interface. By default, the request needs to be approved by the appropriate MRAO, RAO or DRAO administrator before the code-signing action will take place. If 'Auto-Approval' of Code Signing Requests is enabled, the service starts the signing process immediately. See '**Configure the CSD service**' to enable this feature.

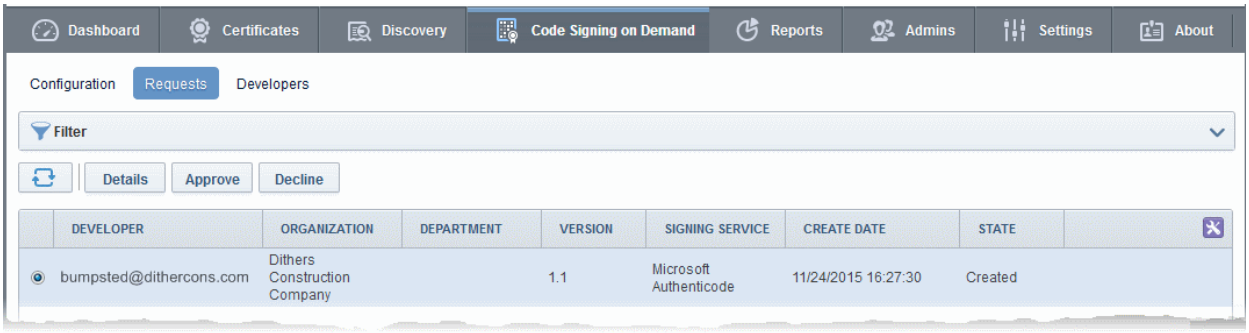
Step 2 - Approve the Code Signing Request

After the files have been uploaded the developer, a code signing request will appear in the 'Code Signing on Demand' > 'Requests' area. Under the default settings, an administrator needs to review and approve the request before the service will actually sign the files.

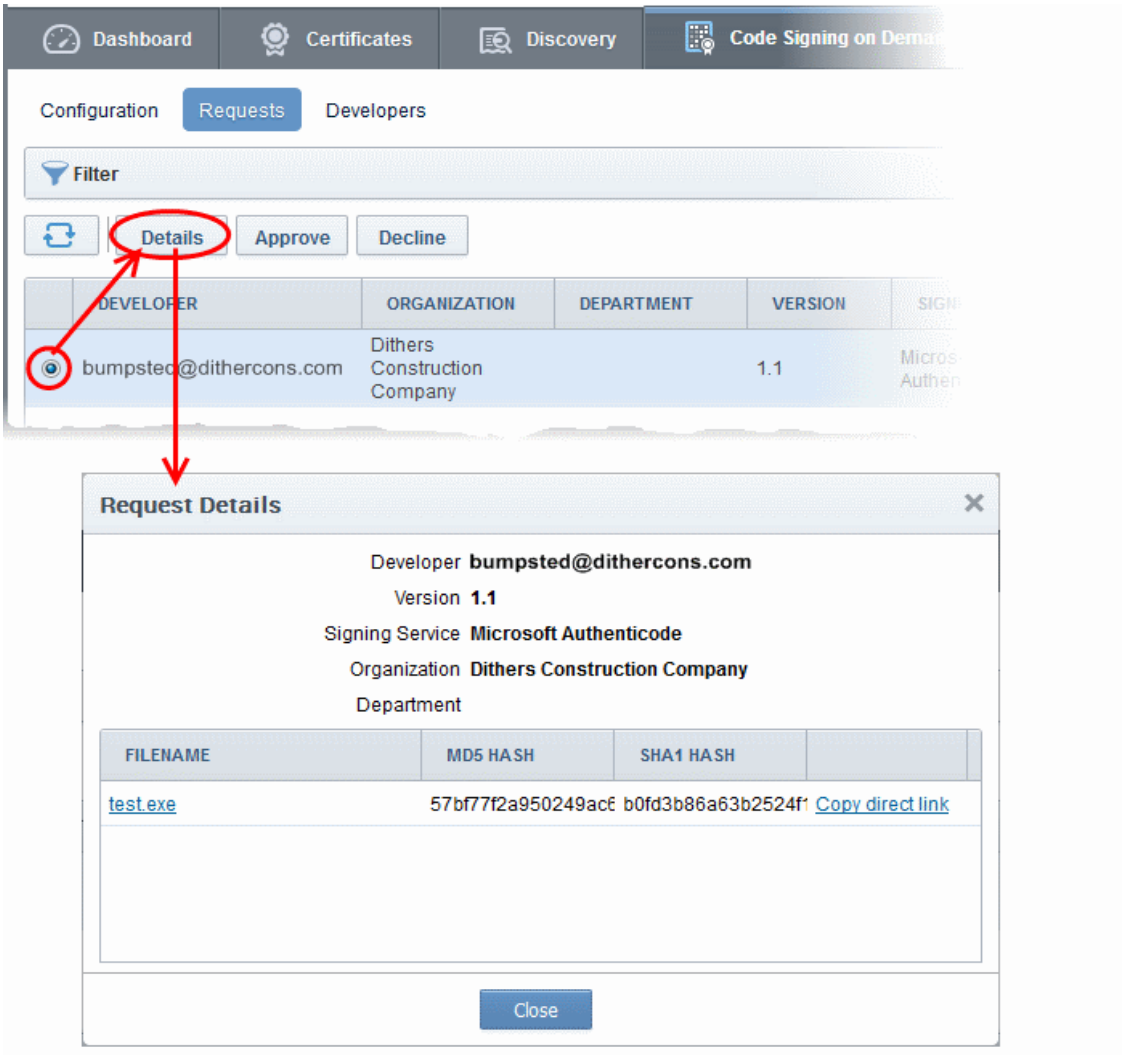
To view and approve/decline the code signing requests

- Click 'Code Signing on Demand' tab and choose the 'Requests' sub tab.

A list of requests will be displayed.

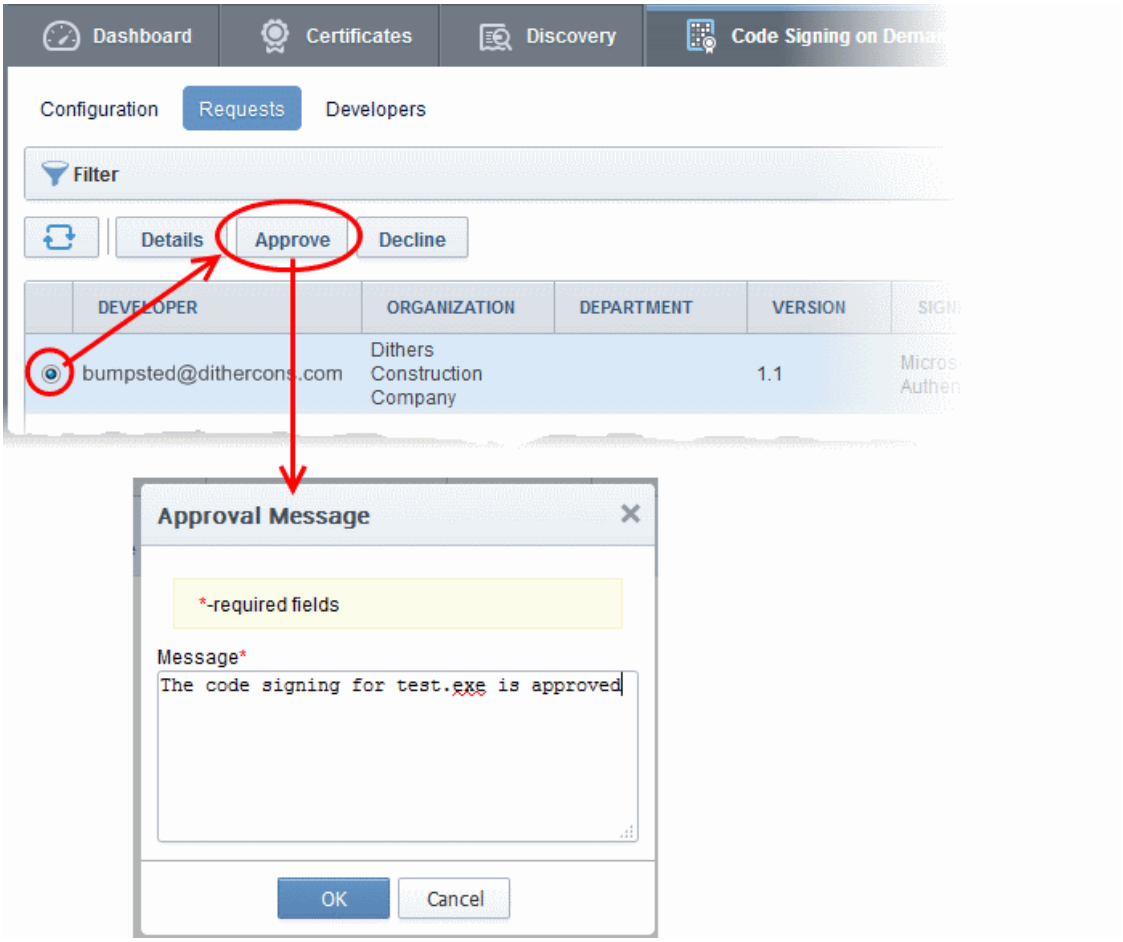


- To view the details of a request and check the files, choose the request and click 'Details'.



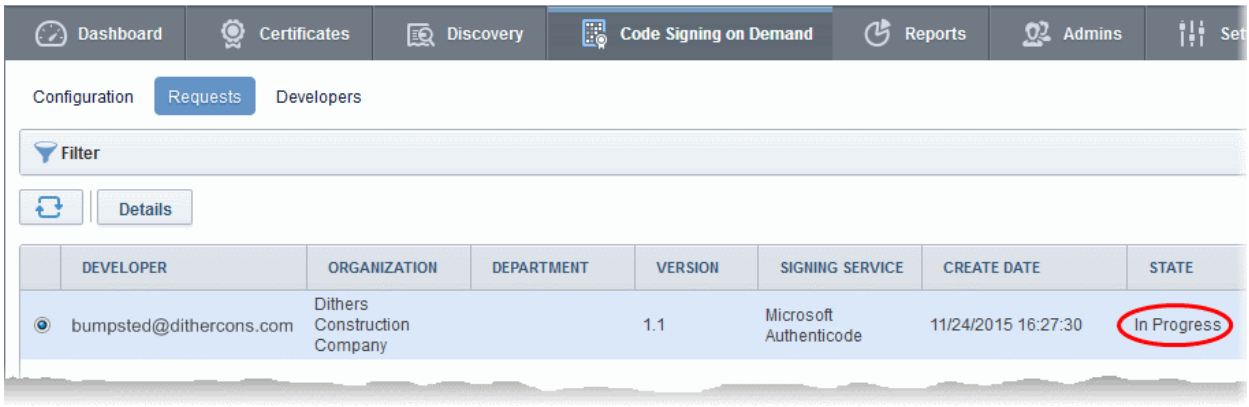
The 'Request Details' dialog displays the developer's name and the file details along with the MD5 and SHA1 hash values of the files.

- To download the file for examination, click the file name.
- To approve the code signing request, select the request and click 'Approve':



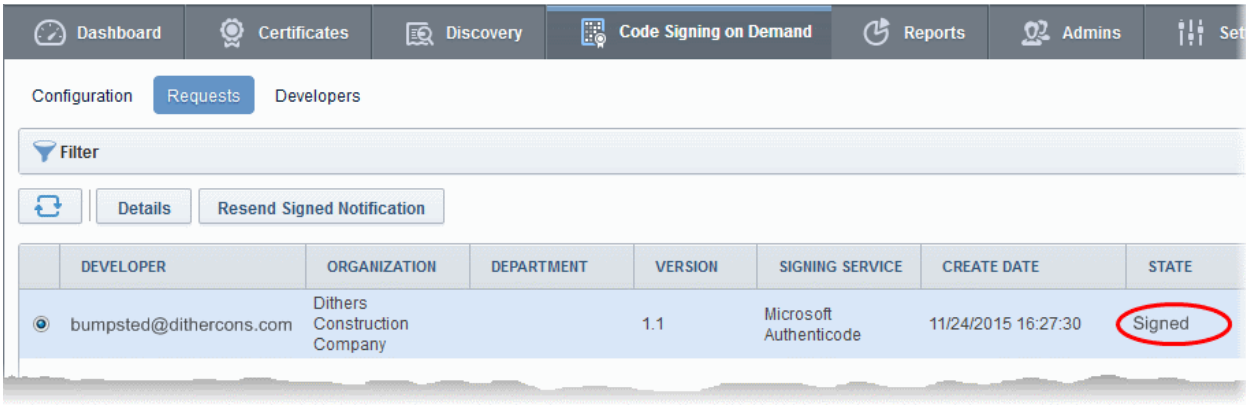
- Enter an approval message and click OK.

The request will be approved and its state will change to 'In Progress':



Once the code-signing process has completed, the request state will change to 'Signed' and a notification mail will be sent to the developer to download the signed file.

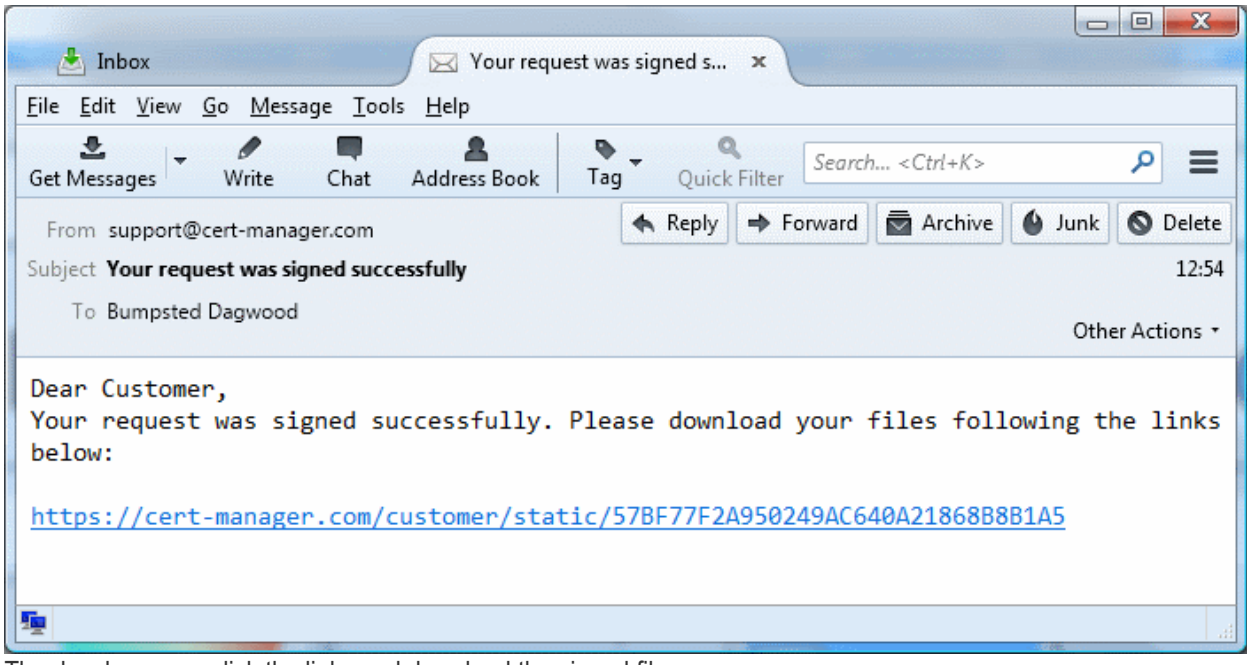
The Developer must download the signed files within three days of the notification. The files will be removed from the database after three days after signing. If required, administrators can resend this notification by clicking the 'Resend Signed Notification' button:



Note. As mentioned earlier, administrators have the option to forgo the approval process by enabling 'Auto-Approve Code Signing Requests' in the 'Configuration' interface.

Step 3 - Download Code-Signed files

On successful completion of the signing process, the developer will receive a notification email with links to download each signed file. An example is shown below.

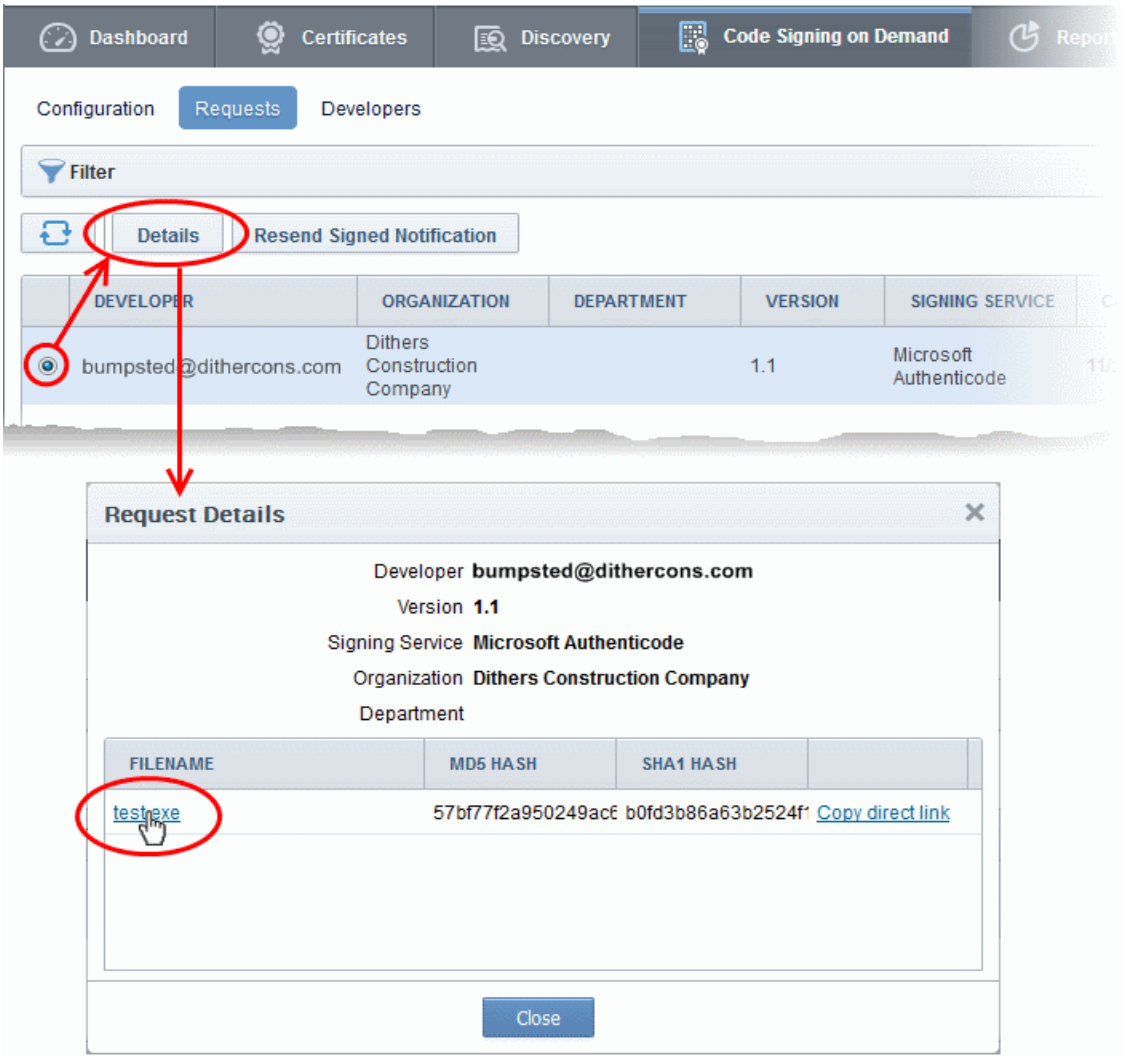


The developer can click the links and download the signed files.

Note: The Developer must download the signed files within three days of the notification. The files will be removed from the database after three days from the date of signing.

Administrators can also download signed files from the 'Details' dialog of the request.

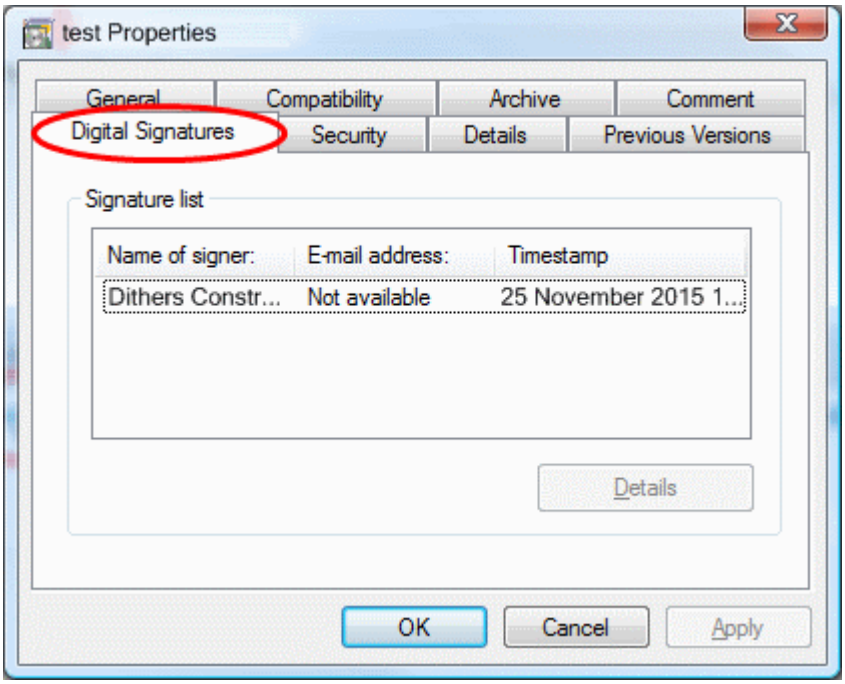
- Choose the request from the 'Code Signing on Demand' > 'Requests' interface and click 'Details'



- Click the file name in the 'Request Details' dialog to download the signed file.

To check whether the file is signed

- Right click on the file and choose 'Properties'
- Choose the 'Digital Certificates' tab



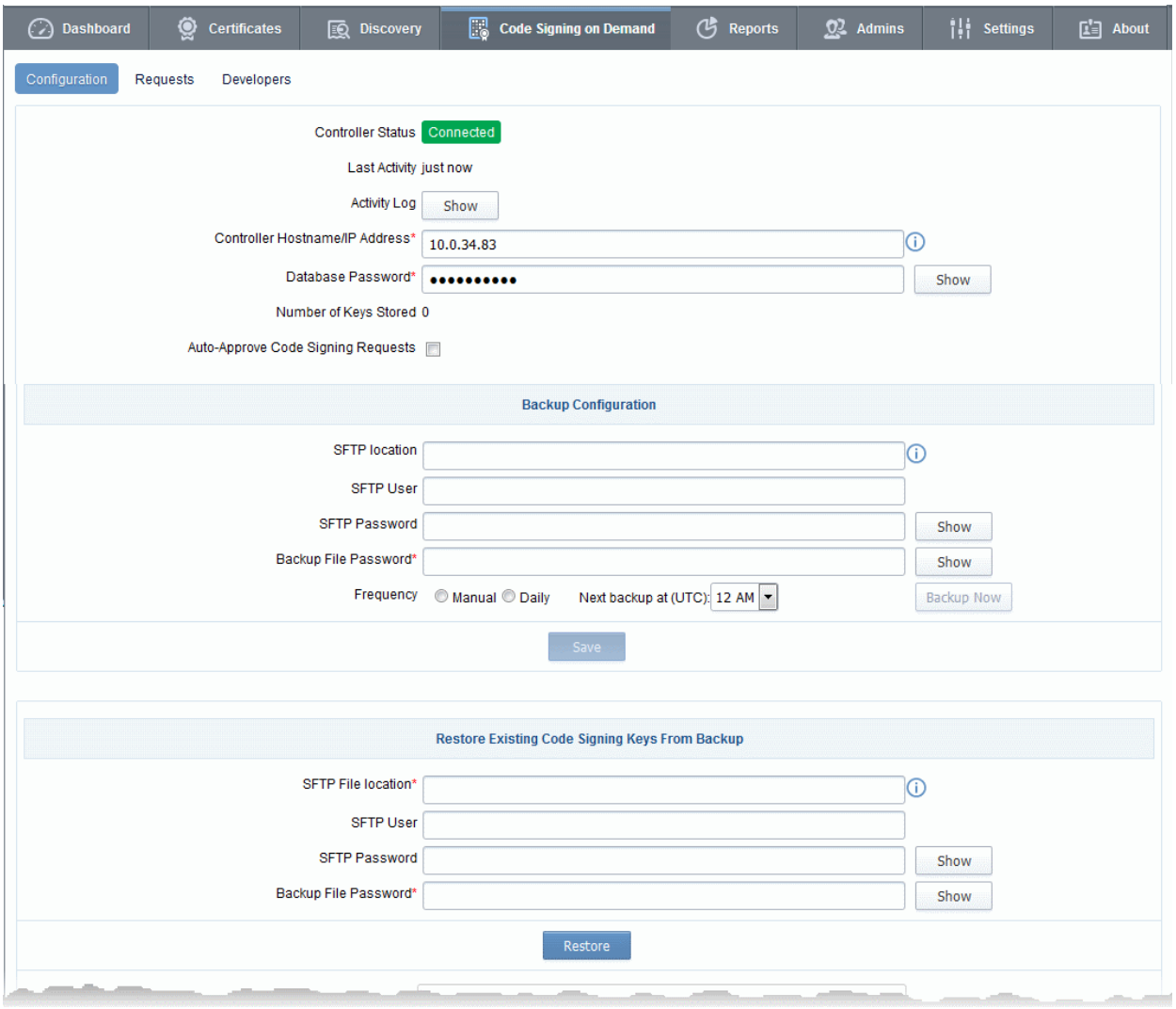
The details of the signer will be displayed.

1.6 Configure the CSD service

The CSD service can be configured for local database password protection, backup and restore operations and auto-approval of code-signing requests from the developers.

The CSD controller creates a database inside your local network and stores the certificates issued for the developers and their private keys in it. You can configure the controller for periodical backup operations of the database and auto-approval of the requests. In case the certificates are lost, you can restore them by installing a new controller for your account.

To configure the CSD controller, click the 'Code Signing on Demand' tab and choose 'Configuration' sub tab.



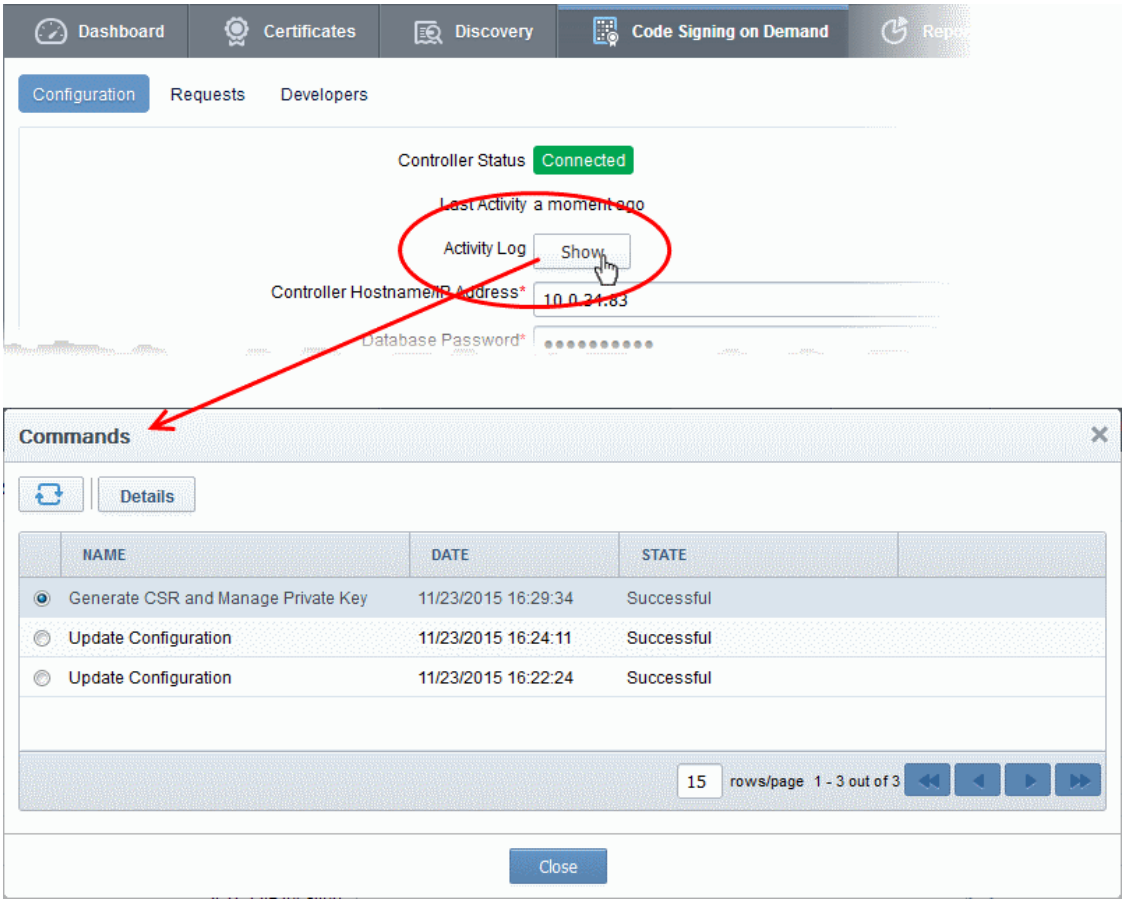
The 'Code Signing on Demand' > 'Configuration' interface allows you to:

- View the activities of the CSD controller
- Configure for auto approval of code signing requests
- Backup/Restore Code Signing Certificates and their private keys

View the Activities of the CSD Controller

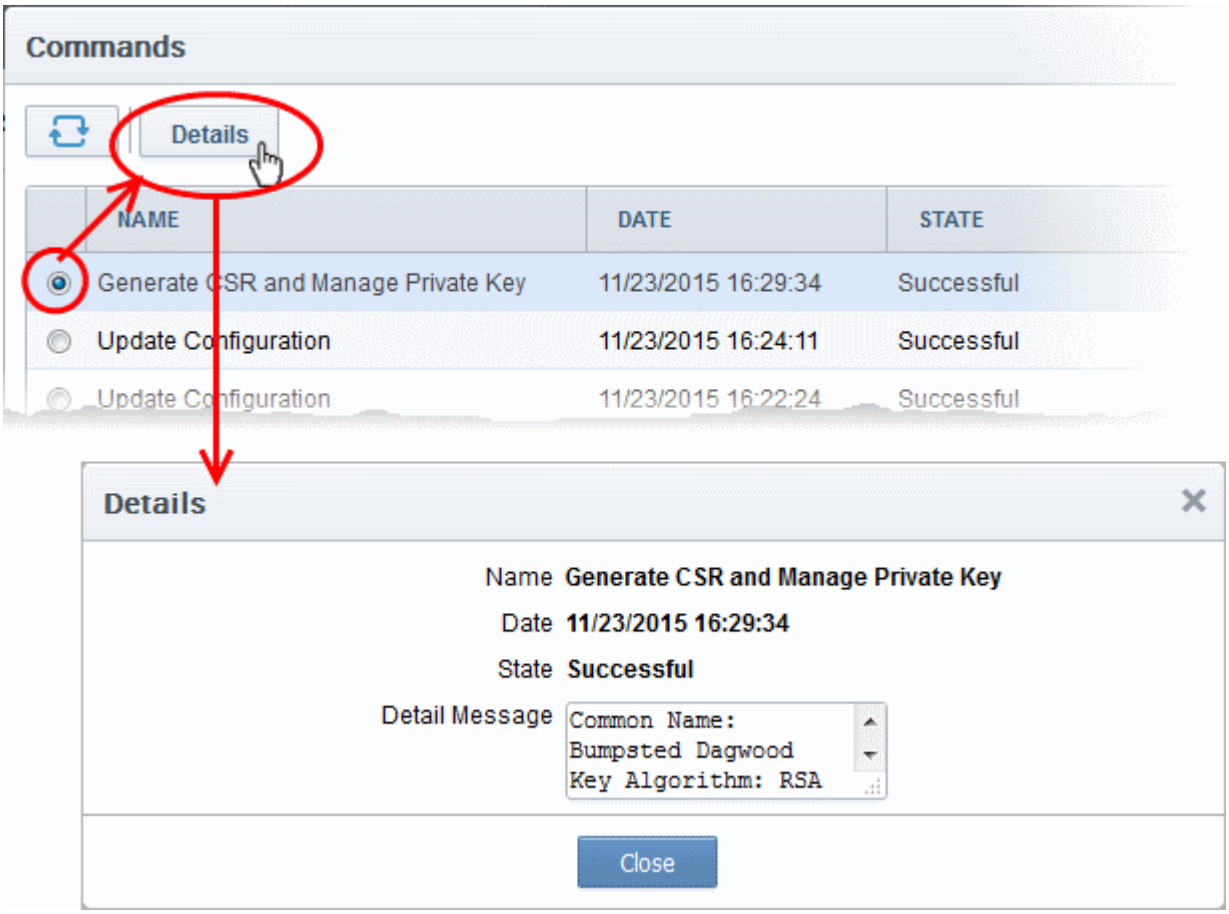
Once the controller is installed on your local network it automatically connects with CCM. The connection status is displayed in the upper pane of the 'Code Signing on Demand' > 'Configuration' interface. You can view the list of commands received by the controller from the CCM and their execution status at any time.

- Clicking the 'Show' button beside 'Activity Log' in the 'Code Signing on Demand' > 'Configuration' interface, opens the 'Commands' dialog with the list of commands received by the controller in chronological order.



Commands Dialog - Column Descriptions	
Column Header	**Description**
Name	Shows the command received from CCM during the consecutive polls.
Date	Indicates the precise date and time, the command was received.
State	Indicates the execution state and result of the command.

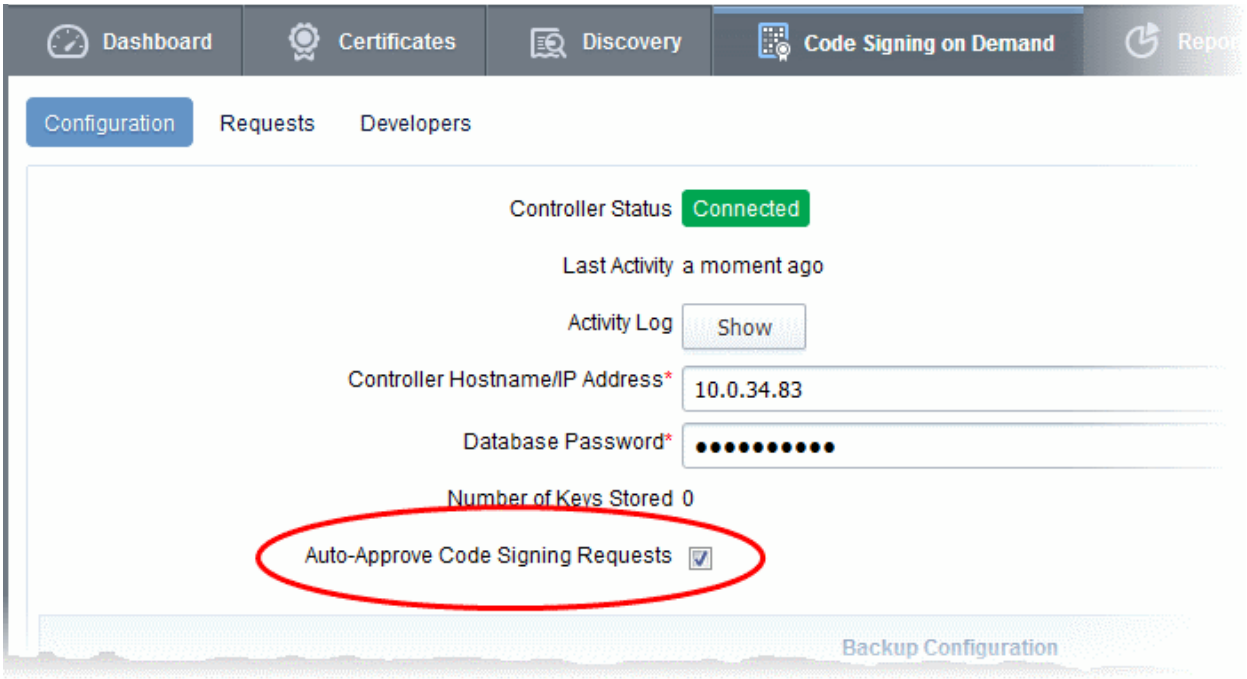
- Choosing a command and clicking the 'Details' button at the top, displays the details of the command.



Configure for Auto Approval of Code Signing Requests

By default, the code signing requests, generated by the developers by uploading the files to be signed, are to be approved by the MRAO, RAO or the DRAO administrator for the CSD service controller to sign the code file. The administrator can view, manage and approve the requests from the 'Code Signing on Demand' > 'Requests' interface. You can configure the controller for auto-approval, If you want the requests to be auto-approved without the manual approval of the administrator to speed up the process. The controller will start the signing processes, once the files are uploaded by the developer. Refer to the section **How to sign code using CSD** for more details.

- To enable auto-approval of code signing requests, select the 'Auto-Approve Code Signing Requests' checkbox in the 'Code Signing on Demand' > 'Configuration' interface.

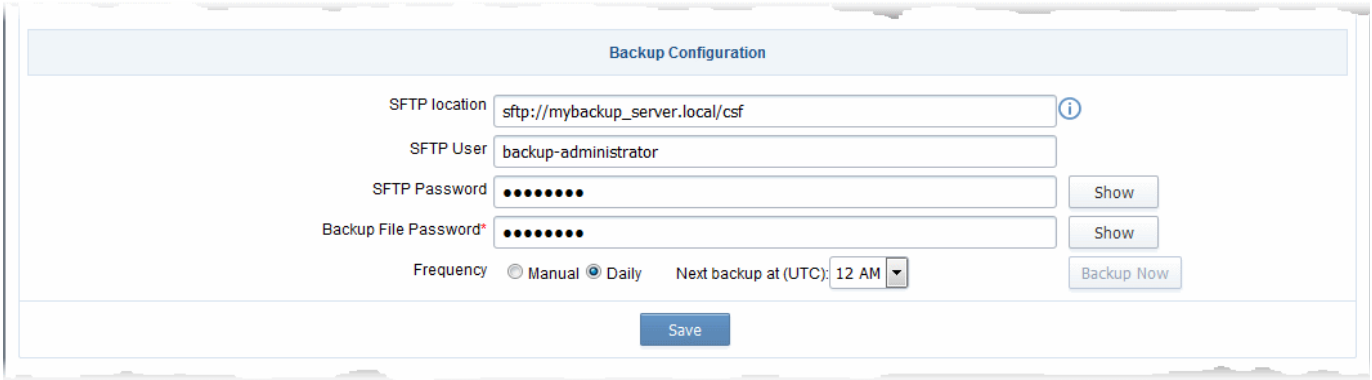


Backup/Restore Code Signing Certificates and Their Private Keys

The administrator can configure backup for the CSD database at a remote SFTP server and schedule periodic backup operations or run backups manually. In case the code signing certificates belonging to the developers and their private keys are lost, they can be restored from the backup.

To configure for backup

- Click 'Code Signing on Demand' > 'Configuration' to open the 'Configuration' interface
- Enter the details of the SFTP server to be configured as the backup location, under 'Backup Configuration'



Backup Configuration - Table of Parameters	
Parameter	**Description**
SFTP Location	Enter the path of the backup location in the SFTP server, at which the CSD service backup is to be created.
SFTP User	Enter the username of your user account in the SFTP server for the CSD controller to access the SFTP server.

SFTP Password	Enter the password of your user account in the SFTP server. Clicking the 'Show' button displays the password.
Backup File Password	Enter the password for the backup file to be created. Clicking the 'Show' button displays the password.
Frequency	Set the schedule at which the backup operations are to be executed. • Manual - The Backup will be run only on clicking the 'Backup Now' button manually • Daily - The Backups are created daily at the time specified in the 'Next backup at:' drop-down. Choose the time in ETC at which the backups are to be run daily.

- Click 'Save' for your configuration to take effect.
- To run an instant backup, click the 'Backup Now' button.

The Backup is configured. You can run the backup any time you want by clicking the 'Backup Now' button from the 'Code Signing on Demand' > 'Configuration' interface or the backup operations will be executed as per the schedule.

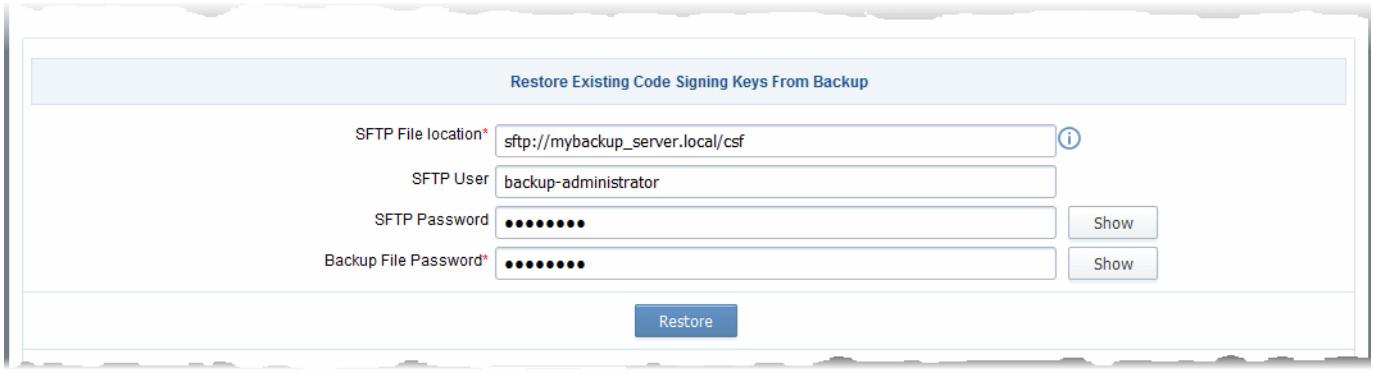
In case the CSD controller and/or the code signing certificates with their private keys are lost from the server for some reason, you can restore them from the backup, by installing another controller in the same or a different server in your local network and configuring it from the 'Code Signing on Demand' > 'Configuration' interface

To restore the keys

- Download the setup file for the new controller, from the 'Code Signing on Demand' > 'Configuration' interface and install it on your network.

Upon successful installation, the controller will connect to CCM and its state will be displayed as 'Connected' in the 'Code Signing on Demand' > 'Configuration' interface.

- Enter the SFTP details of the remote SFTP server configured as backup location under 'Restore Existing Code Signing Keys From Backup' and click 'Restore'.



The code signing certificates and their keys will be restored to the database created by the new controller.

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

Email: EnterpriseSolutions@Comodo.com

For additional information on Comodo - visit http://www.comodo.com.