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 (CSoD) 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, WAR, JAVA JAR and Android application files.
- CCM is also capable of hash signing, whereby developers upload a hash of their files for signing instead of the files themselves. The developer then needs to embed the hash with their files.

Code signing on demand is available in two deployment options:

- **In-House Hosted Mode**
  - Developers upload software to a local portal. The code signing process is handled by a locally installed controller. The controller will generate CSoD 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. HSM integration is mandatory if you use the controller in cluster mode. All CSoD agents should be configured to connect to a single HSM.

- **Cloud Mode**
  - The signing service is hosted on Comodo's highly secure cloud servers. The service generates CSoD 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 CSoD in **In-House Hosted Mode**.

Note : CSoD is not enabled by default. Please contact your account manager if you require the service.

Process in brief

- A new 'Code Signing on Demand' tab will appear in the CCM title bar after the service is enabled.
- MRAOs should download the CSoD service controller setup file from 'Settings' > 'Agents' > 'CSoD Agents'
- CSoD agent (aka CSoD controller) can be installed on a single server or on multiple servers.
- If installed on a single server, use of Hardware Security Module (HSM) is optional. If you opt to install the agent on multiple servers (cluster mode), then network HSM and Network File System are mandatory.
- Admins need to assign a person as a 'Developer' in CCM. Admins will request and approve the CSoD certificates on behalf of the developer. The developer will submit files for signing and subsequently collect the signed files.
- After enrolling for a code signing certificate, the controller generates the certificate request and submits the request to CCM.
- The controller tracks the order number and, once the certificate is issued, will download it and store it on your local network.
- The developer can then upload files to the local portal for signing. After admin approval, the controller will sign the file and notify the developer to collect 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:

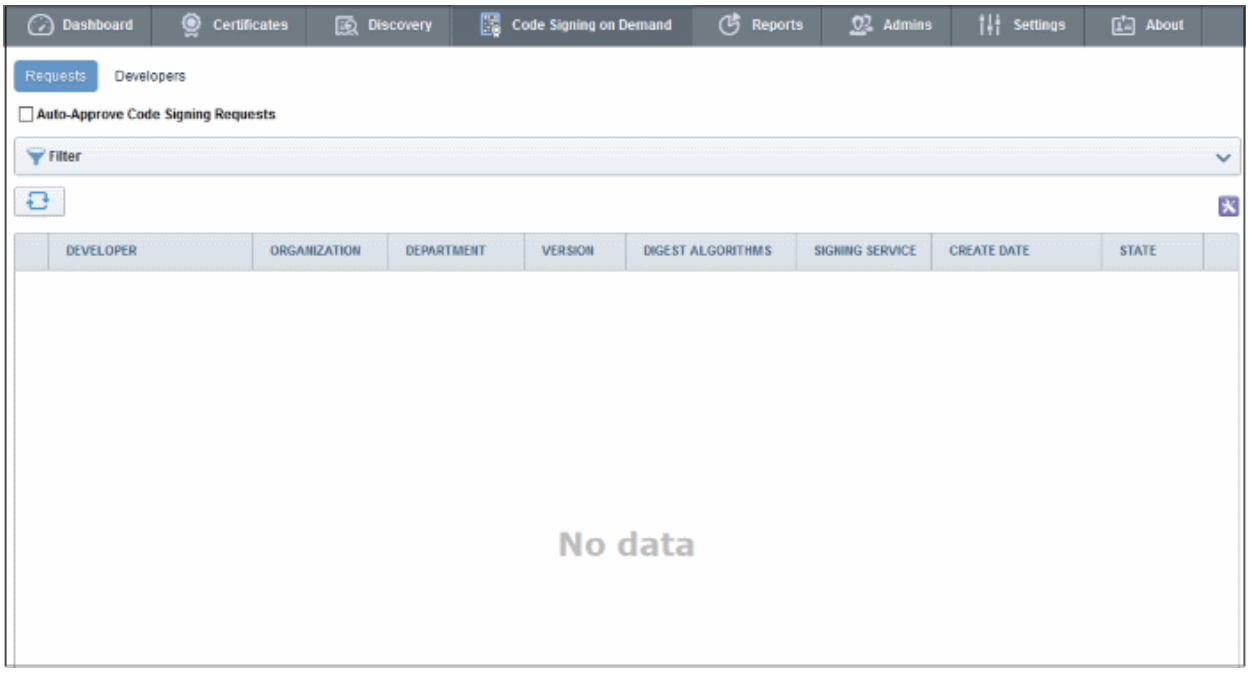
- The 'Code Signing on Demand' Interface
- Set up the CSoD controller
- Add Developers
- Obtain a Code Signing Certificate For CSoD
- How to sign code using CSoD
- Configure the CSoD service

1.1 The 'Code Signing on Demand' Interface

The 'Code Signing on Demand' area lets you manage 'Developers' and signing requests.

The interface is divided into two main sections:

- The 'Requests' tab - View and approve/decline code signing requests from developers
- The 'Developers' tab - Add and manage 'Developer' accounts in CCM.



Visibility of the CSoD area is restricted to:

- MRAO administrators - Can configure the controller, add developers and manage code signing requests for any organization or department.
- RAO Code Signing administrators - Can add developers and manage code signing requests for organizations/departments that have been delegated to them.
- DRAO Code Signing administrators - Can add developers and manage code signing requests for departments that have been delegated to them.

1.2 Set-up the CSoD Controller

You can install the CSoD agent on a single machine and opt to use a HSM appliance. CCM also supports the installation of CSoD agent on multiple machines for redundancy.

Standard Mode

- The CSoD agent is downloaded and installed on a single server
- The use of a HSM appliance is optional
- The Osslsigncode tool should also be installed on the same server

Cluster Mode

- CSoD agents are downloaded and installed on multiple servers. A separate agent must be downloaded and installed on each server. You cannot use the same agent setup file on different servers.
- The use of HSM and Network File System is mandatory.
- The Osslsigncode tool should also be installed on all servers.
- All agents should be configured to work with the same HSM appliance.
- Network file system should be available. All the CSoD agents should be configured to have the same directory for input files and the same directory for output files.
- The input and output folders should be configured in CSoD agent properties. Typically the path of the agent is: /opt/comodo/ccmcscontroller/conf/agent.properties (this may vary depending on the Linux environment). Example folder configuration is shown below:
  - sign_input_path=/mnt/smb/csod/in
  - sign_output_path=/mnt/smb/csod/out
- The 'Download Agent' button will available in 'Settings' > 'Agents' > 'CSoD Agents' once the configuration to the HSM and input/output files is complete. The button allows you to download a new CSoD agent for installation on another server.
- Once installed and connected, the service can be configured from the agent's interface. See **Configure the CSoD service** for more details.

Controller (agent) setup involves two steps:

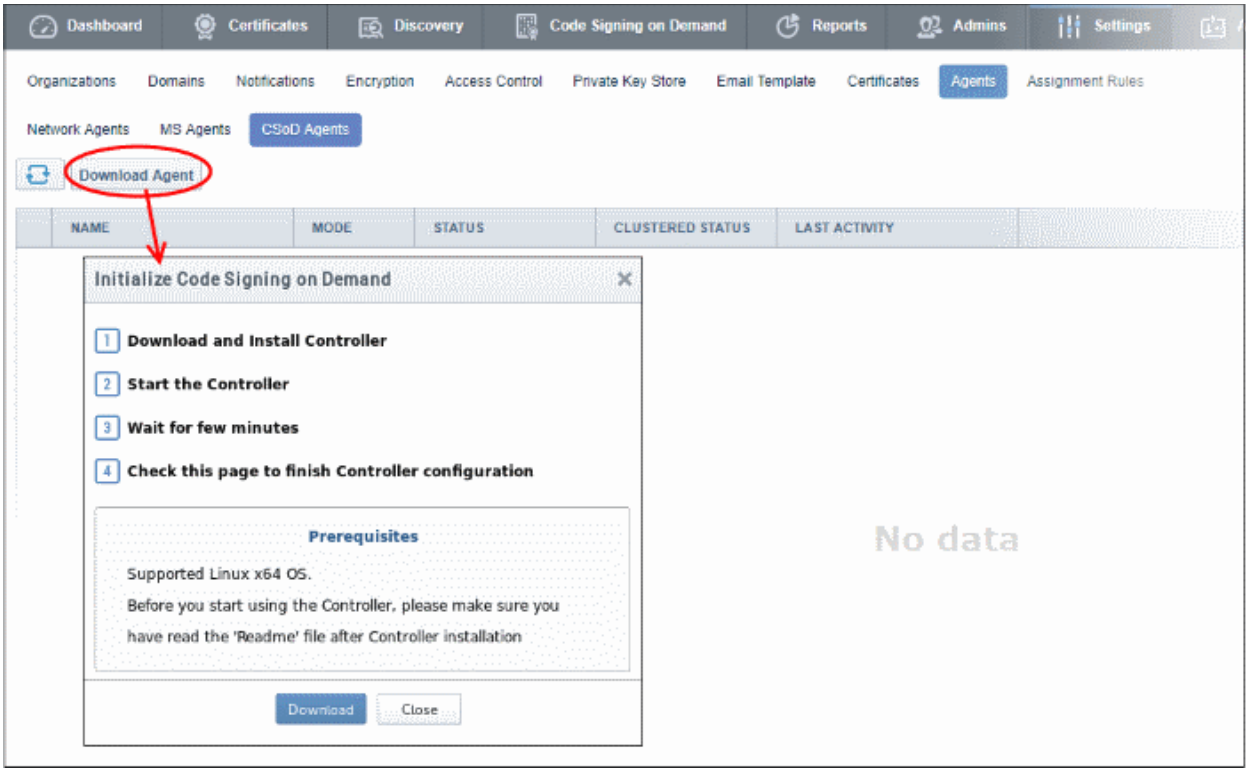
- **Install the CSoD Controller**
- **Install the Osslsigncode tool**

Install the CSoD Controller

You can download the setup file for the CSoD controller from the CCM interface as a .bin file and install it on the Linux server through a 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 'Settings' tab > 'Agents' > 'CSoD Agents'



- Click the 'Download' button.
- Transfer the file to your Linux server.
- Install the CSoD controller on the server from the command line:

```
This End User License Agreement (this "EULA") constitutes the final binding agre
ement between a validly formed legal entity ("Subscriber") that has entered into
 a legally enforceable CCM Enterprise Certificate Agreement with Comodo and has
an active CCM account, and Comodo CA Ltd. ("Comodo") which has its principal pla
ce of business at 3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Sa
lford Manchester, M5 3EQ, United Kingdom.

1. General.
Do you accept license agreement? [Y/n]: y

Will You use HSM? :  [y/N] y
 Enter path to HSM module:
[/usr/lib/x86_64-linux-gnu/softhsm/libsofthsm2.so]: /usr/lib64/pkcs11/libsofthsm
2.so
 Enter path to SPKCS11engine:
[/usr/lib/engines/engine_pkcs11.so]: /usr/lib64/openssl/engines/pkcs11.so
 Enter HSM slot number:
[0]: 0
 Enter pin for slot of HSM:
[Secret1]: secret1
CCM CSoD Controller started on PID: 18027.
Installation complete. CCM CS Controller started on PID: 18027.
[root@csagent02 comodo]#
```

- After agreeing to the EULA you will be offered a choice between HSM or regular installation.
- Enter 'Y' if you want to use a HSM. Enter 'N' if you wish the controller to generate and store the keys in its vault.
    - Please note for cluster mode HSM is mandatory.

- It is optional to use a HSM for standard mode (single installations)
- If you elect to use a HSM, enter the following parameters:
  - Network path to the HSM module
  - Path to SPKCS 11 Engine
  - HSM Slot Number to be used
  - PIN number for the HSM Slot

For cluster mode, the CSoD agents should be configured to work with the same HSM appliance. All the CSoD agents should be configured to have the same directory for input files and the same directory for output files. Typically the path of the agent is: /opt/comodo/ccmcscontroller/conf/agent.properties (this may vary depending on the Linux environment). Example folder configuration is given below:

- sign_input_path=/mnt/smb/csod/in
- sign_output_path=/mnt/smb/csod/out

The controller will connect to the CCM server once installation is complete. You can configure the controller from the CCM interface. See **Configure the CSoD service** for more details.

Note: Your HSM appliance may need some additional configuration to generate keys. Refer to the instructions in the user manual of your appliance.

Installation of Osslsigncode tool

- Download the tool from **http://sourceforge.net/projects/osslsigncode/**
- For cluster mode, the tool should be installed on all servers on which the CSoD agent is installed

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

Note: It is recommended you install the osslsigncode tool to /usr/bin. Otherwise, the CSoD controller may not be able to access it and you will need to manually provide access.

1. **CentOS versions: 6, 7**

   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. **Debian versions: 7, 8**

   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.

Note: Supported OpenSSL versions: Not lower than version 0.9.8, and not higher version than 1.0.x

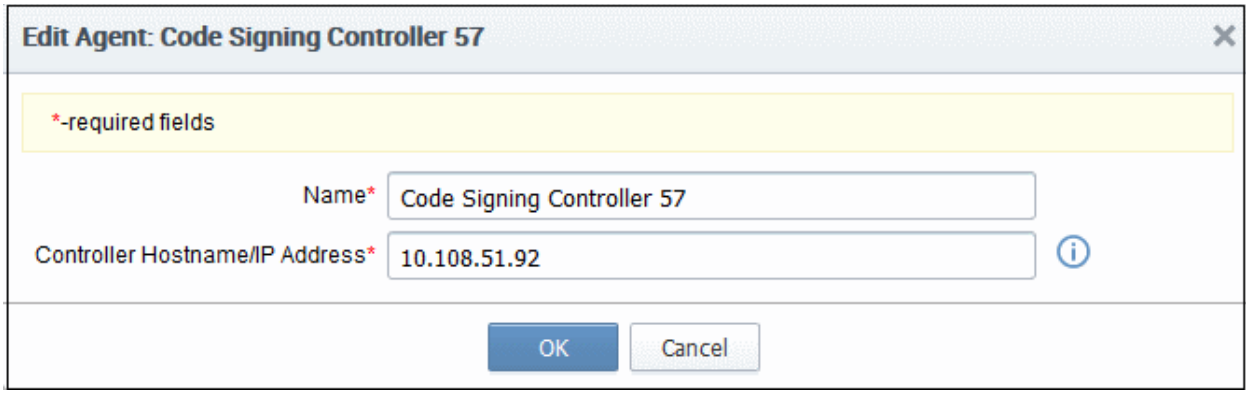
Environment Tuning

1. Configure the controller server

   By default, the controller is set to use a self-signed certificate installed on the Jetty Web Server. However, there are certain circumstances when a customer may need to use a publicly trusted certificate instead. For example, a client's browser may restrict access to sites that do not use a publicly trusted certificate.

   Please follow these instructions if you need to use a different certificate:

   i. Make sure the server on which the controller is installed has a valid hostname. If it doesn't then please assign one. Also create a DNS record for the server so it is accessible through the intranet.
   ii. Login to CCM and click the 'Settings' tab > 'Agents' > 'CSoD Agents' then select the agent and click 'Edit' at the top



   - Replace the default hostname/IP address with the hostname of the controller server
   iii. Enroll for, or retrieve, a publicly trusted certificate for the server. The hostname should be in the

'Common Name' field in the certificate.

iv. Put the certificate and private key into the Java Key Store (JKS) with a password. E.g. file 'cs-agent.jks' and password '12345'

v. Copy the file into the 'conf' directory of the controller's install directory. Usually '/opt/comodo/ccmcscontroller/conf'

vi. Update the 'agent.properties' file. This is located at '/opt/comodo/ccmcscontroller/conf/agent.properties' Specify JKS file and password:

ssl.keystore=cs-agent.jks

ssl.keystore.password=12345

vii. Restart the controller. Usually: '/etc/init.d/ccmcscontroller stop' and '/etc/init.d/ccmcscontroller start'

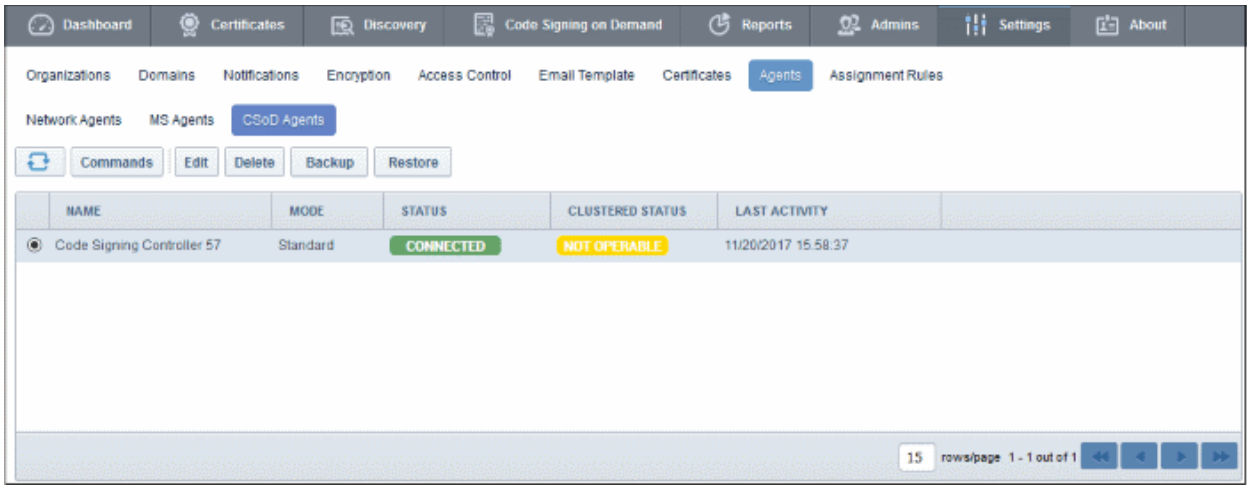
2. Make sure port 9092 is open. The controller uses this port for incoming requests.

3. Make sure that the 'hostname' command returns the assigned hostname.

- After installation, the controller will automatically connect to CCM and start running immediately. Go to 'Settings' > 'Agents' > 'CSoD Agents' to check connection status.
- On first connection, the controller will download the latest configuration files from CCM and generate a password for its database.
- The controller will periodically poll CCM to retrieve instructions

The CSoD Agents Interface

- Click 'Settings' > 'Agents' > 'CSoD Agents' to open the CSoD Agent interface:



CSoD Agents Interface – Column Descriptions	
Column Header	**Description**
Name	Name of the CSoD Agent.
Mode	Indicates whether the agent is using a HSM or not. • Standard – Indicates the agent is not using the HSM • HSM – Indicates the agent is using HSM
Status	The current connection status of stand-alone and clustered agents. The possible states are: • Connected - The agent is communicating with CCM.

		• Not Connected - The agent is not communicating with CCM • N/A – No connection has been established so far.
Clustered Status		Indicates whether the agent is configured to use HSM. • Not Operable – The agent is installed in standard mode or the agent hasn't been correctly configured to use a HSM. • Operable – The agent is correctly configured to work with a HSM and can be used as cluster. • N/A (Not Available) – The agent has been downloaded and CCM is yet identify whether the agent satisfies the criteria of cluster
Last Activity		The last date and time the agent communicated with CCM

Controls	Download Agent	Download and create a new CSoD agent for installation. The button may be available in the interface again after the first download depending on the mode in which the primary agent was installed.
		• Standard mode – The download button will not appear in the interface again if you installed in standard mode and are not using a HSM.
		• Clustered mode – The download button will be available again If you installed the agent in clustered mode and configured it to use a HSM.
		  • You can download the agent and install it on another machine. The agent must be configured to use the same HSM.
		  • You have to download and install a new agent for each new machine.
		  • A single CSoD agent setup file cannot be used on multiple machines.

	Commands	View commands executed by the agent. Commands include generate CSR and manage private keys.
	Refresh	Updates the list of agents.
Agent Controls	Edit	Modify the agent name and the hostname/IP address of the machine on which the agent is installed.
	Delete	Removes the agent.
	Backup	Copy the CSoD database to a remote SFTP server. See 'Configure the CSoD Service' for details.
	Restore	Restore code signing keys from backup. See 'Configure the CSoD Service' for details.

1.3 Add Developers

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

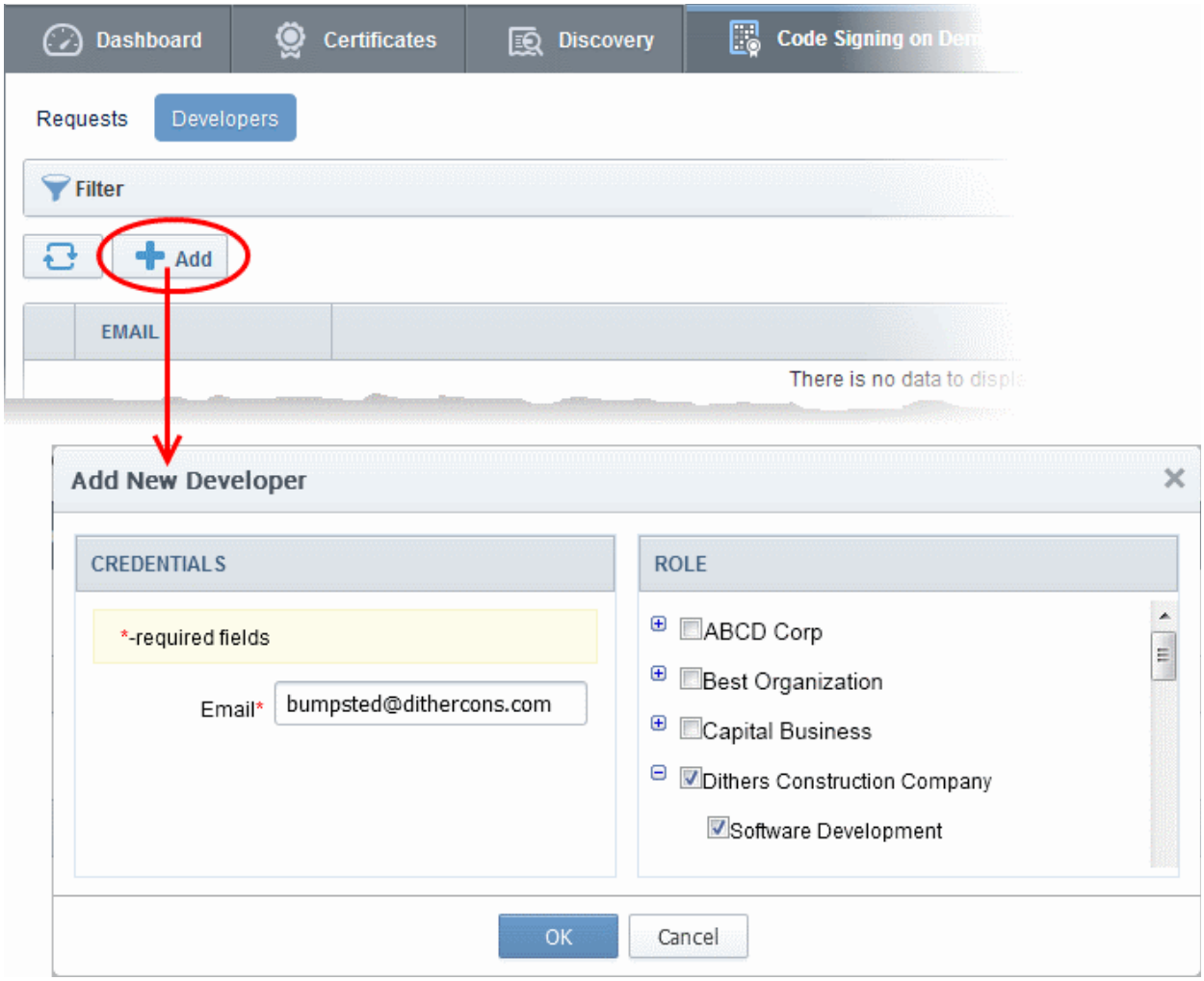
- Login to the CSoD service
- Upload files or hashes for code-signing
- Download the signed file or signed hash

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

CSoD configuration screen.

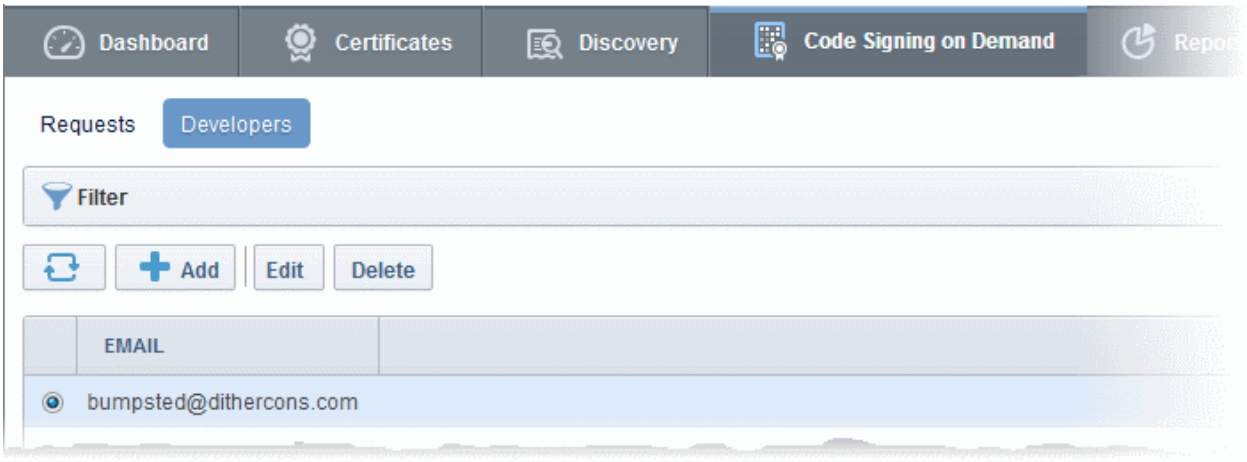
To add a developer

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

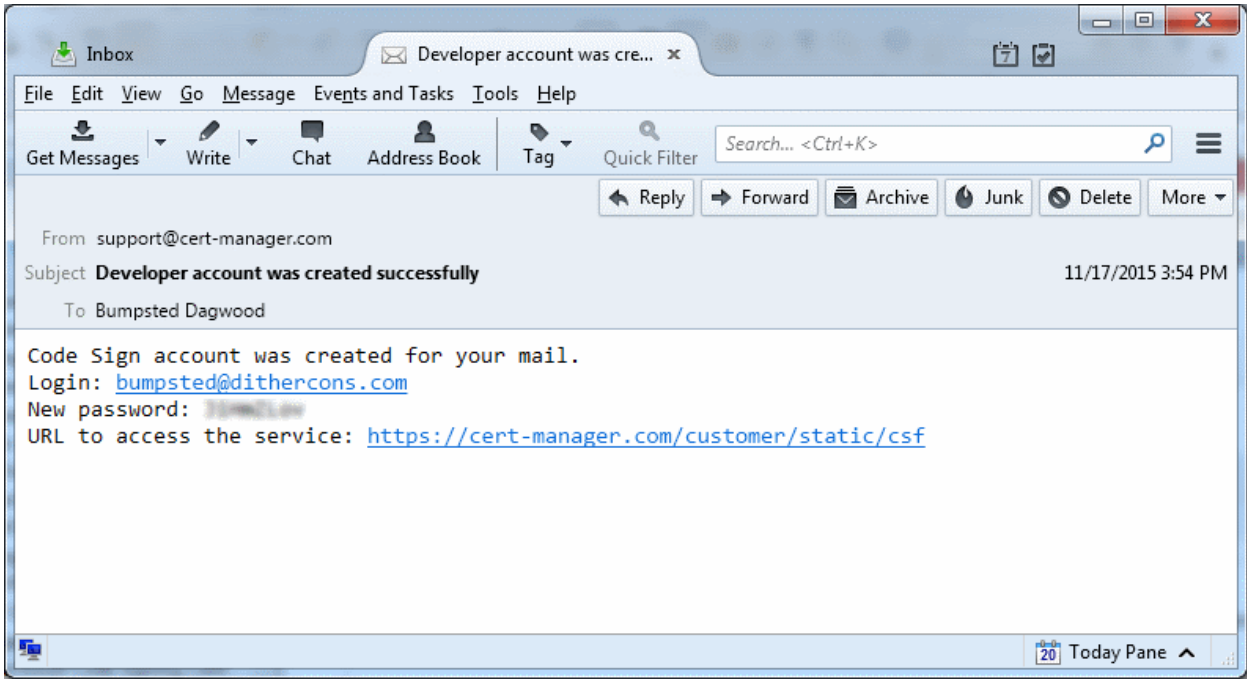


- Type the email address of the developer in the email field.
- Use the right-hand pane to select the Organization(s) / Department(s) to which the developer should belong.
- Click 'OK' to confirm your selection.

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



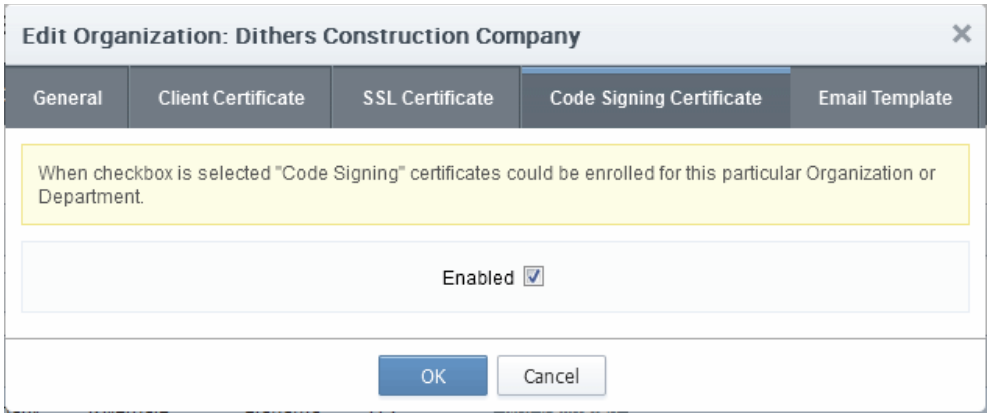
A notification email will be sent to the developer with the credentials to access the CSoD service. An example is shown below:



1.4 Obtain a code-signing certificate for CSoD

Prerequisites:

- You have created a 'Developer' role as explained in the preceding section.
- The domain from which the 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.
- The domain has been delegated to an organization or department.
- An 'RAO Code-Signing' or 'DRAO Code-Signing' admin has been delegated control of the organization/ dept.
- The admin has enabled code signing certificates for the organization in the 'Code Signing tab' of the organization's settings (see screen-shot below). 'Edit' an organization to access these settings.



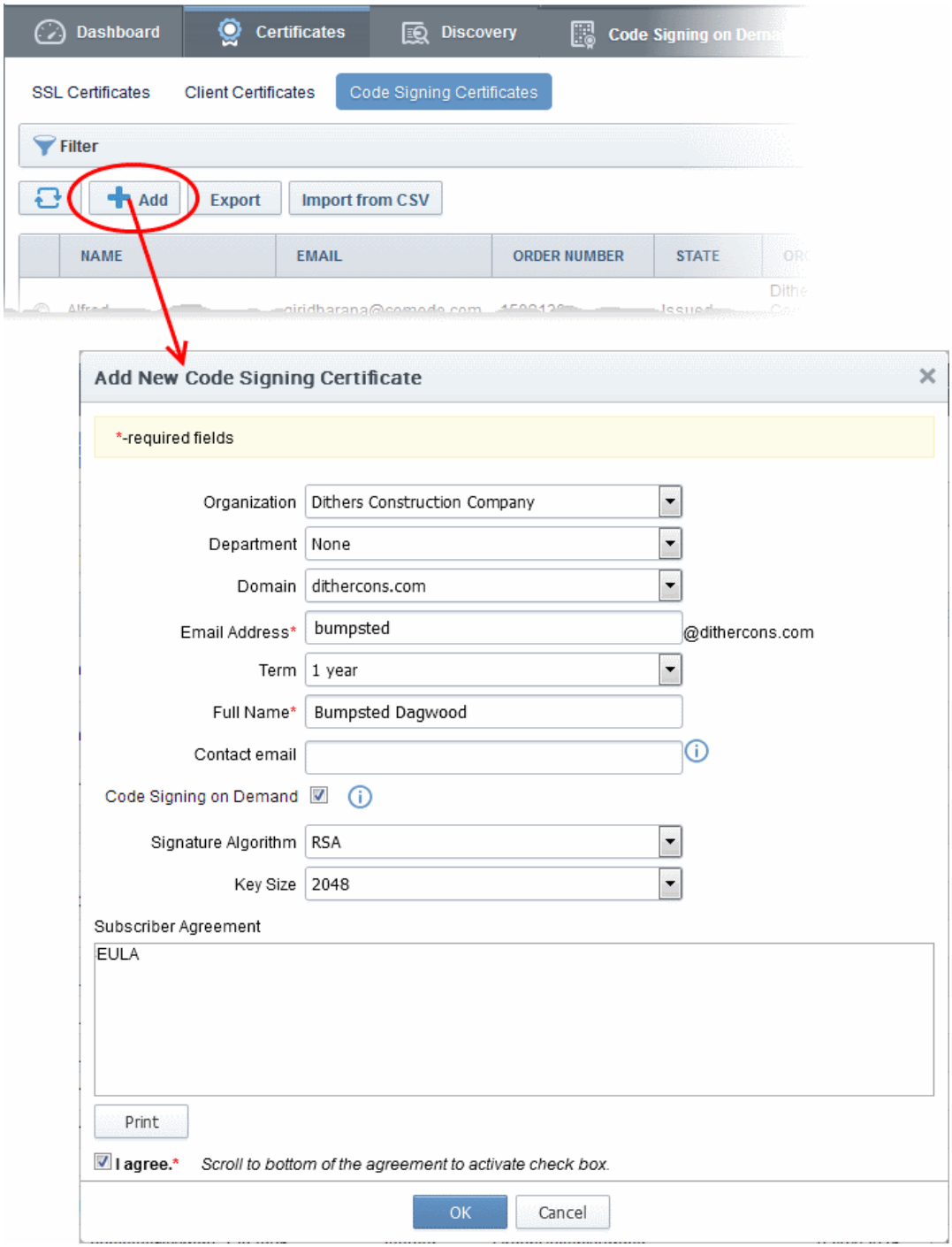
- Hosted mode - the CSoD service controller also needs to be installed on the local network and connected to CCM.
- Cluster Mode - If the controllers are installed on multiple servers then they must be configured to generate and store keys on a HSM appliance. If you install the controller on a single server then it is optional to use a HSM appliance to generate and store keys.

Procedure Overview:

1. The administrator confirms 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 CSoD controller generates and stores the key pair locally and submits the CSR to Comodo CA. Once the certificate is issued, the CSoD controller automatically downloads the certificate and stores it on 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

- Click 'Certificates' > 'Code Signing Certificates' to open the 'Code Signing Certificates' interface
- Click the 'Add' button to open the 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.

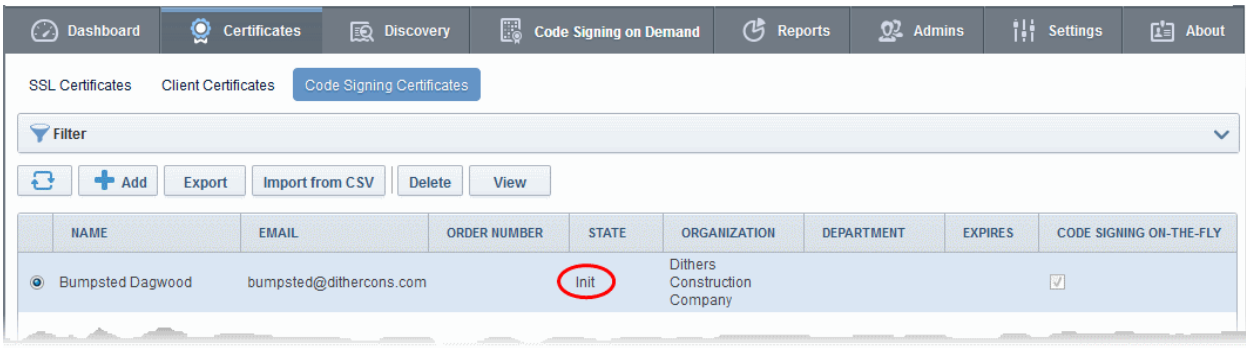

Dashboard
Certificates
Discovery
Code Signing on Dema
SSL Certificates
Client Certificates
Code Signing Certificates
Filter
Add
Export
Import from CSV
NAME
EMAIL
ORDER NUMBER
STATE
Add New Code Signing Certificate
*-required fields
Organization
Dithers Construction Company
Department
None
Domain
dithercons.com
Email Address*
bumpsted
@dithercons.com
Term
1 year
Full Name*
Bumpsted Dagwood
Contact email
Code Signing on Demand
Signature Algorithm
RSA
Key Size
2048
Subscriber Agreement
EULA
Print
I agree.*
Scroll to bottom of the agreement to activate check box.
OK
Cancel

The following table explains the fields on the form:

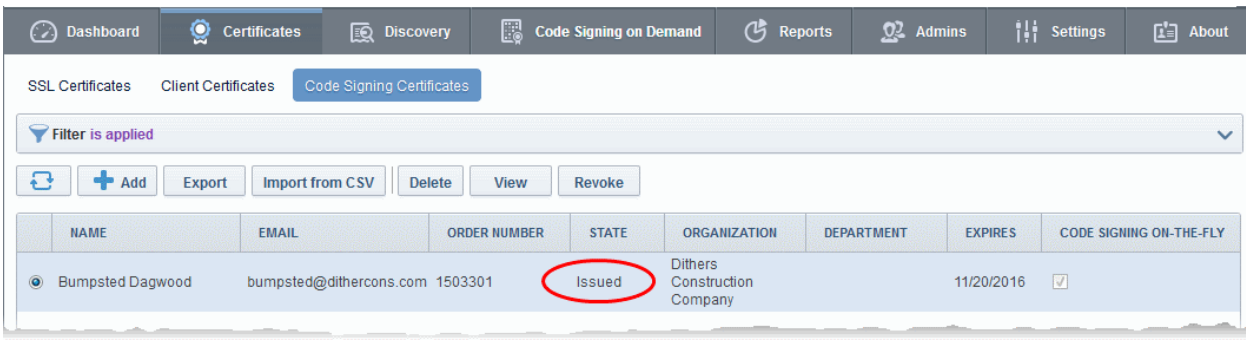
Field	Description
Organization	Select the Organization to which the developer belongs.
Department	Select the Department to which the developer belongs.
Domain	Select the domain to which you want to issue the certificate. This will be a domain that is assigned to the organization/department.
Term	Select the term of the certificate.
Email Address	Enter the email address of the developer.
Full Name	Full name of the applicant.
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 to allow the certificate to be used by the CSoD service.
Signature Algorithm	Choose the signature algorithm to be used by the certificate. Recommended = 2048 bit or higher.
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.



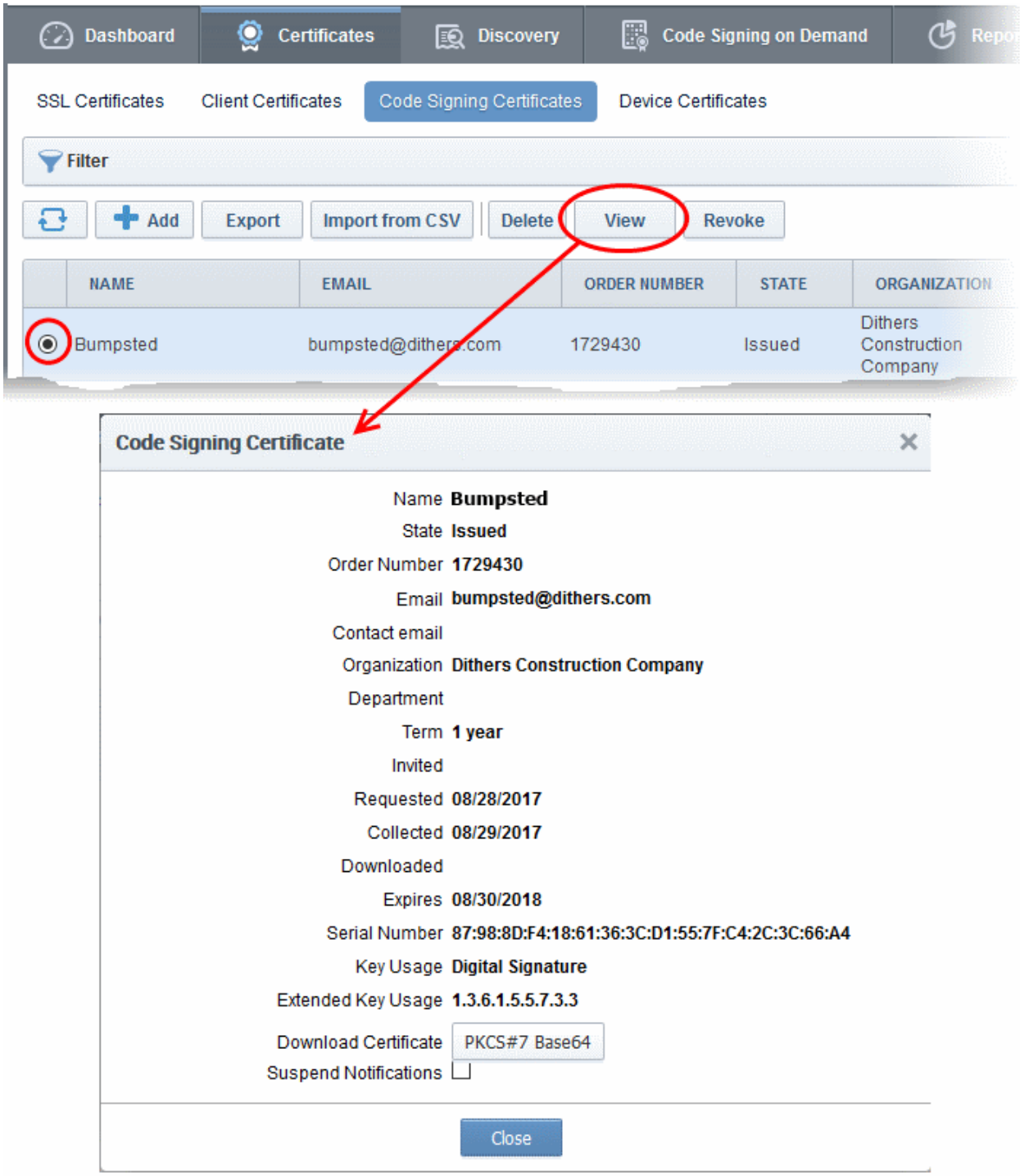
Once issued, the state of the certificate will change to 'Issued': The controller will download and save the certificate in the local network.



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 CSoD interface.

Viewing and Downloading the certificate

- Select the certificate and click 'View' to see certificate details:



- Click the 'Download' button to download the certificate in PKCS#7 format

1.5 How to sign code using CSoD

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

- Code Signing – Developers can upload EXE .DLL .CAB .MSI .OCX .SY, JAVA JAR, WAR and Android application files.
- Hash Signing – Developers can upload a text file containing the SHA or MD5 hash value of their software which will be signed with their code signing certificate. Developers can embed the signed hash and certificate with their binary. This is useful if:
  - The source files are large and the developer wishes to avoid longer upload times
  - Company policy allows code signing of binaries to be performed only within a local system

See **Obtain a code-signing certificate for CsoD** if you need help with getting a code-signing certificate.

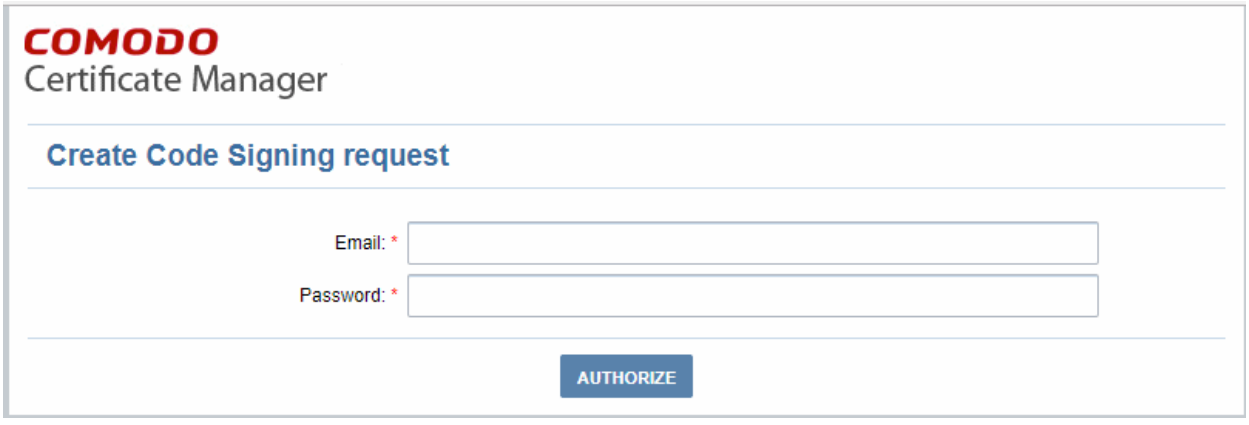
Note: The 'Hash Signing' feature is only available if enabled for your account. Please contact your Comodo account manager if you wish to add this service.

Overview of steps:

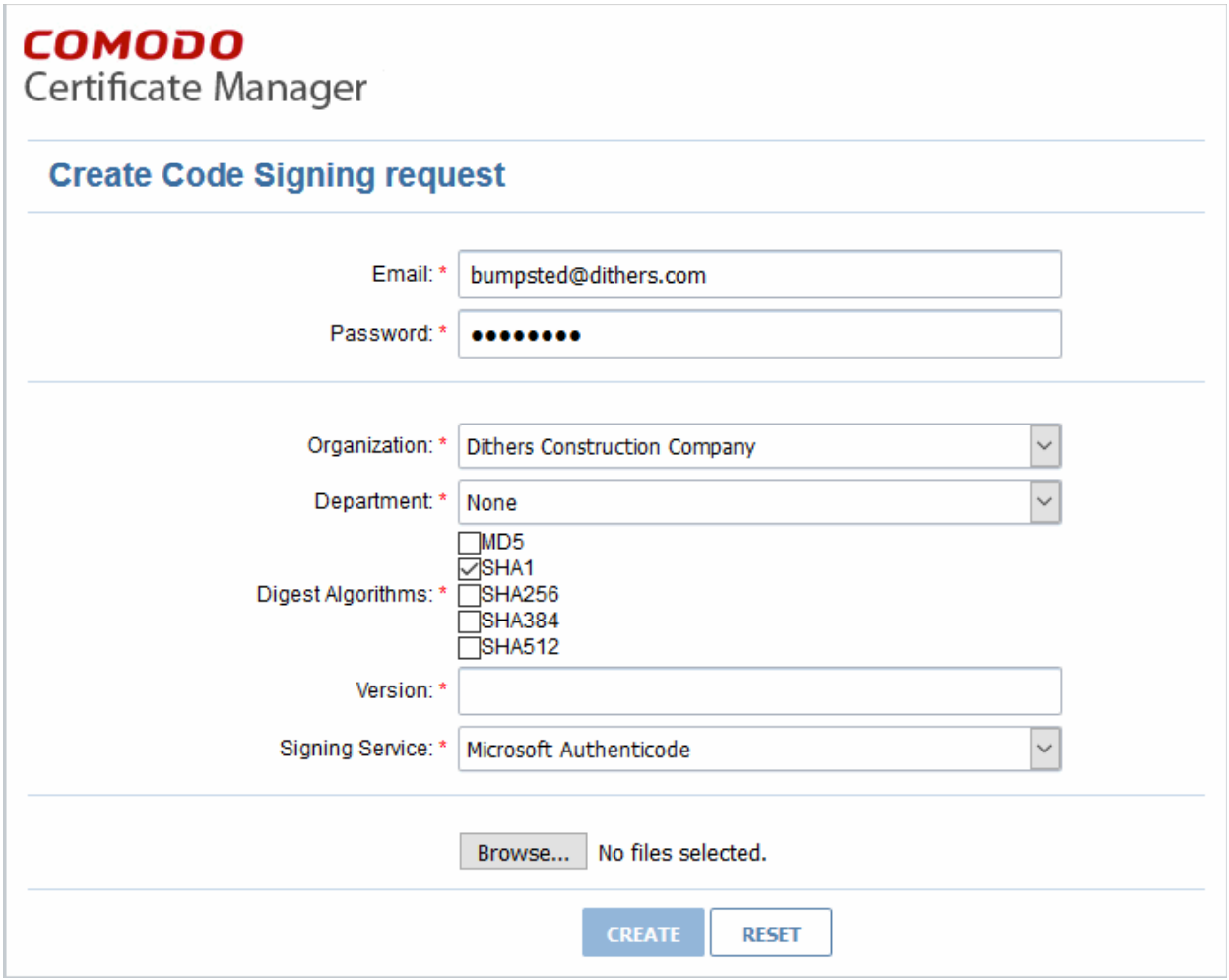
- **Step 1 - Upload the files to be Signed** - The developer logs-in to the CSoD service portal, enters the details of the file(s) to be signed, selects the signing service and uploads their code or hash. This will create a request which can be viewed in the 'Code Signing on Demand' > 'Requests' interface.
- **Step 2 - Approve the Code Signing Request** (optional) - An administrator views the request, checks the files to be signed and approves the request from the 'Code Signing on Demand' > 'Requests' interface. Note - this step can be skipped if 'Auto-Approve Code Signing Requests' is enabled in the CSoD interface.
- **Step 3 - Download Code-Signed files** - After the signing process is complete, 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.

Step 1 - Upload the files to be Signed

- Once a developer has been added, 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]/csod.



- Developers can then upload files using the following form:

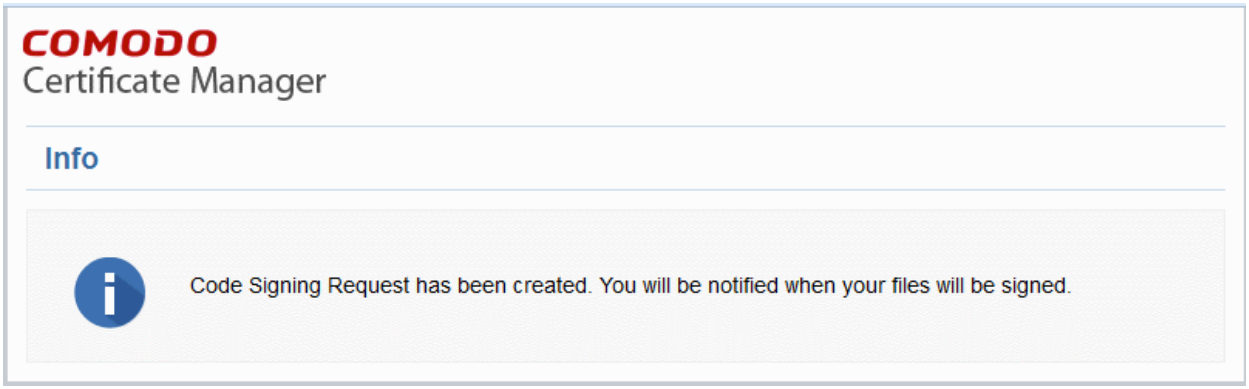


- **Organization** - The organization(s) to which the developer belongs. The organization selected here will be shown in the certificate as the publisher of the software.
- **Department** - Allows the developer to choose a department If departmental information is also required in the certificate.
- **Digest Algorithm** - Select the algorithm you wish to use to create the file hash-code (aka 'digest). The hash-code is used by client software to verify the integrity of your signed code. Recommended = SHA256 and upwards.
- **Version** - Developer should type the version number of the software they wish to sign
- **Signing Service** - Select the appropriate signing service for the type of file you want to sign:
  i. ***Files*** - Choose 'Microsoft Authenticode', 'Java' or 'Android' as the signing service
  ii. ***Hash values*** - Choose 'Hash Signing' as the signing service. You need to generate a hash-code of your file with the SHA or MD5 algorithm (to generate a .sha or .md5 file). Alternatively, create a .txt file containing the hash value.

  Note: 'Hash Signing' is only available if the service is enabled for your account. Contact your account manager if you want to enable 'Hash Signing'.
- **Browse...** - Choose the files or hashes you want to upload for signing. Multiple files can be uploaded.

- The developer should complete the form and click the 'Create' button to submit the signing request to the CSoD service.

A confirmation dialog will be displayed:



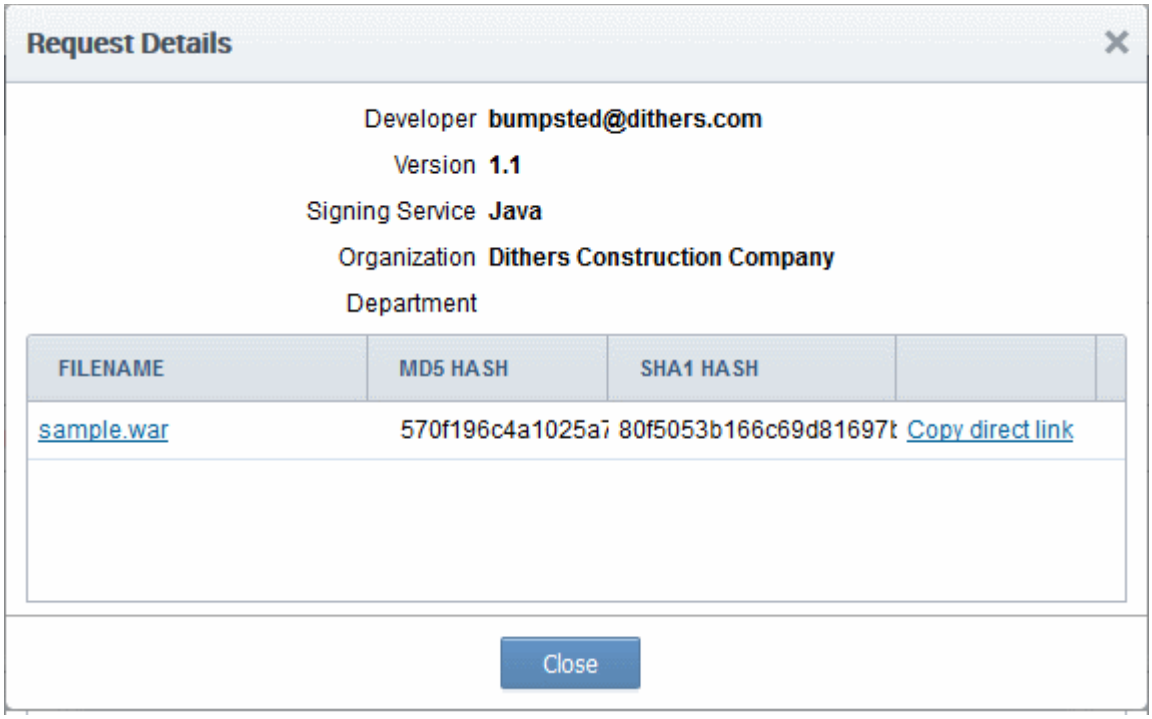
- The code signing request can be seen in 'Code Signing on Demand' > 'Requests'.
- By default, the request needs to be approved by the appropriate MRAO, RAO or DRAO administrator before the signing will take place.
- If 'Auto-Approval' of Code Signing Requests is enabled, the service will sign the code immediately. See 'Configure the CSoD service' to enable this feature.

Step 2 - Approve the Code Signing Request

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

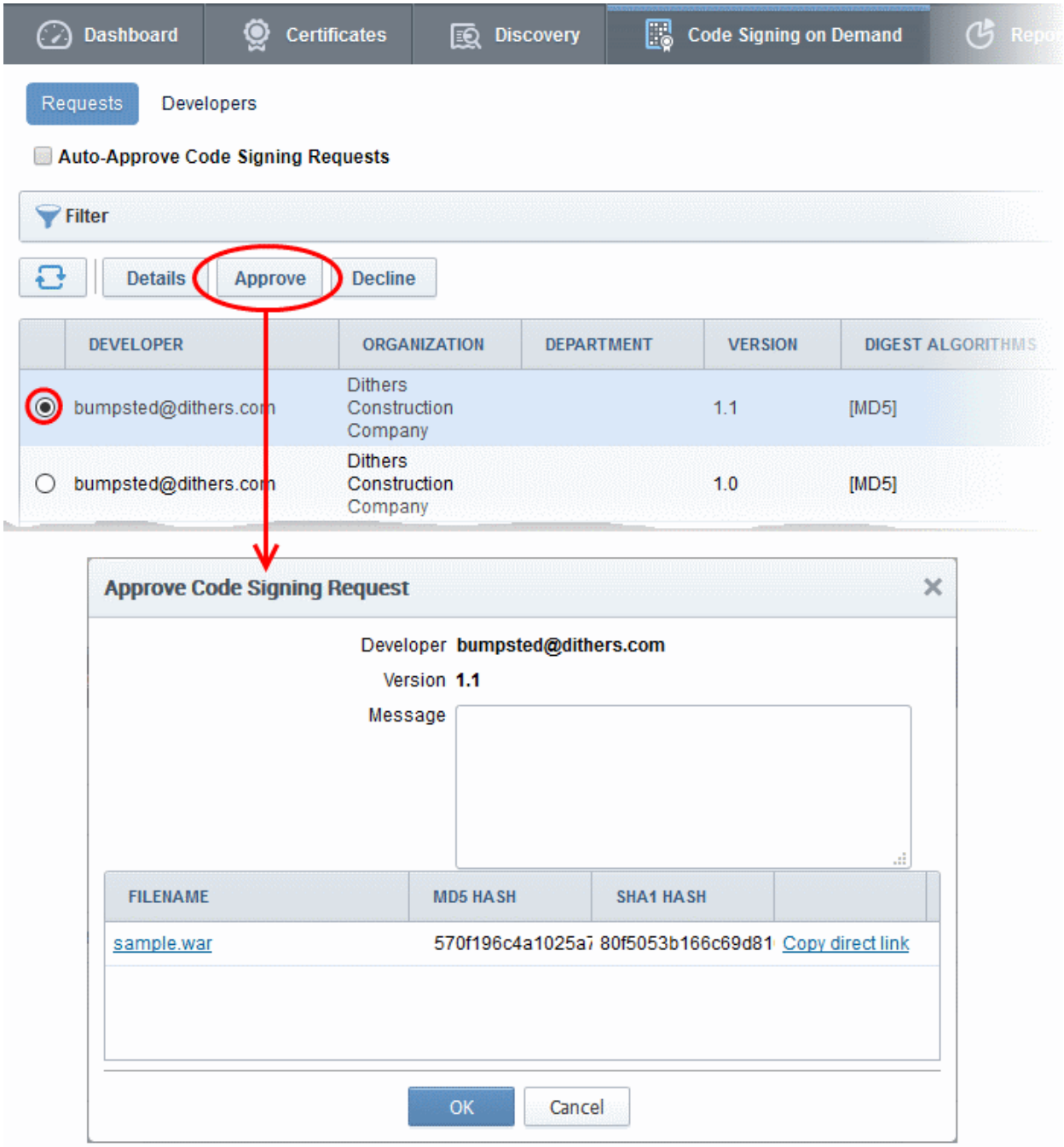
- Click the 'Code Signing on Demand' tab and choose the 'Requests' sub tab
- A list of requests will be displayed:

- Click 'Details' to view the specifics of the request:

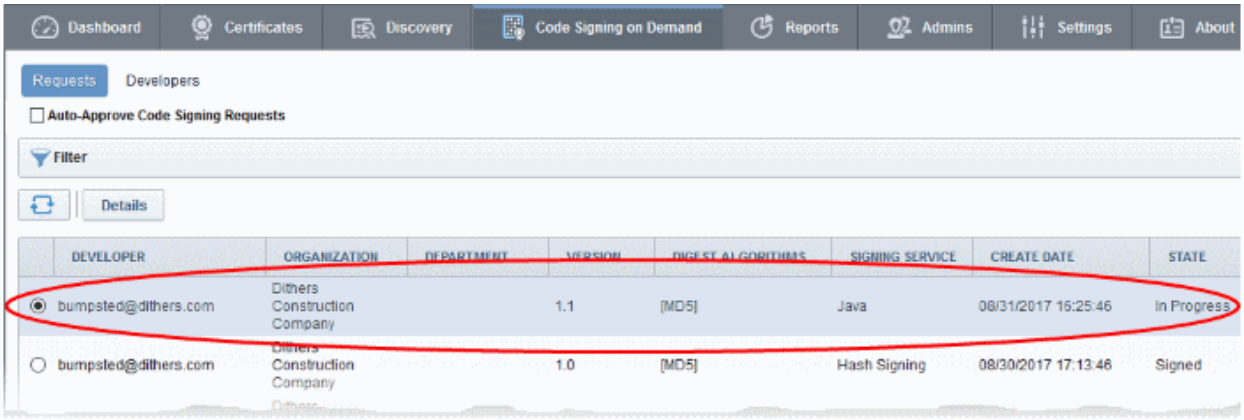


The details dialog shows the developer's name, file details, and the MD5 and SHA1 hash values of the files.

- Click the file name to download the file for examination
- Select the request and click 'Approve' to allow the signing process to go ahead



- Enter an approval message in the 'Message' field and click 'OK'
- The request will be approved and its state will change to 'In Progress':

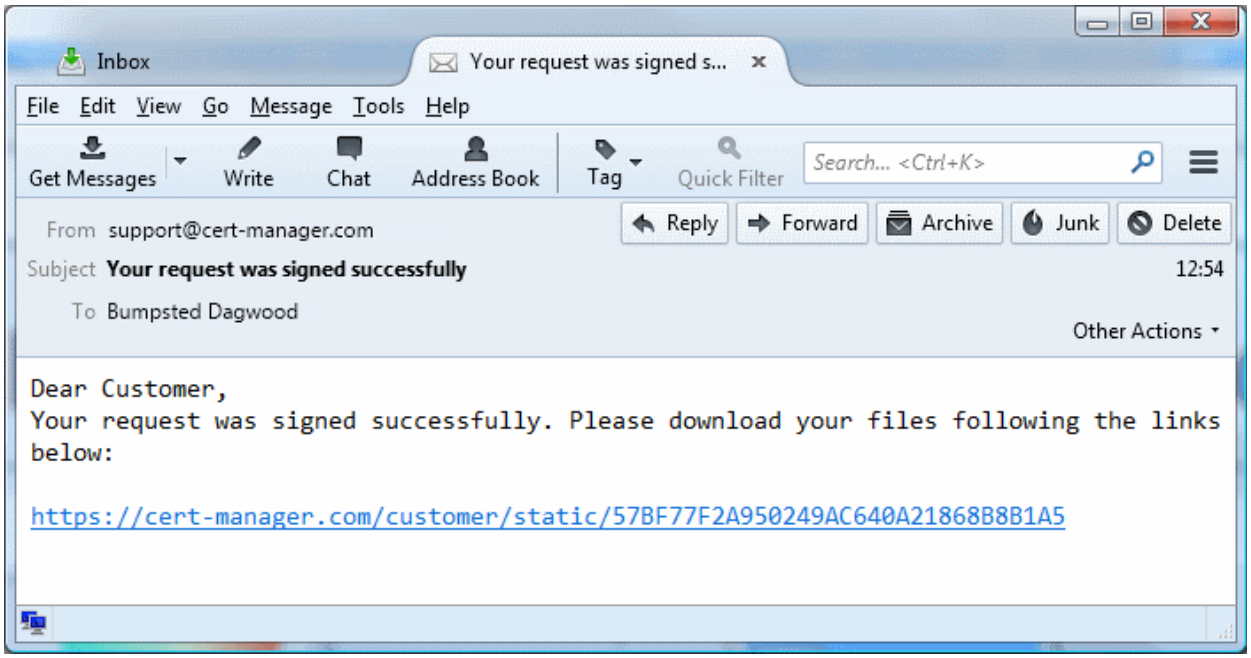


- The request state will change to 'Signed' once the signing process is complete.
- A notification mail will be sent to the developer to download the signed file.
- The Developer must download the signed files within three days of the notification. The files will be removed from the database three days after signing.
- If required, you can resend the email by clicking 'Resend Signed Notification'

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

Step 3 - Download Code-Signed files

After completing the signing process, the developer will receive an email with links to download each signed file. An example is shown below.

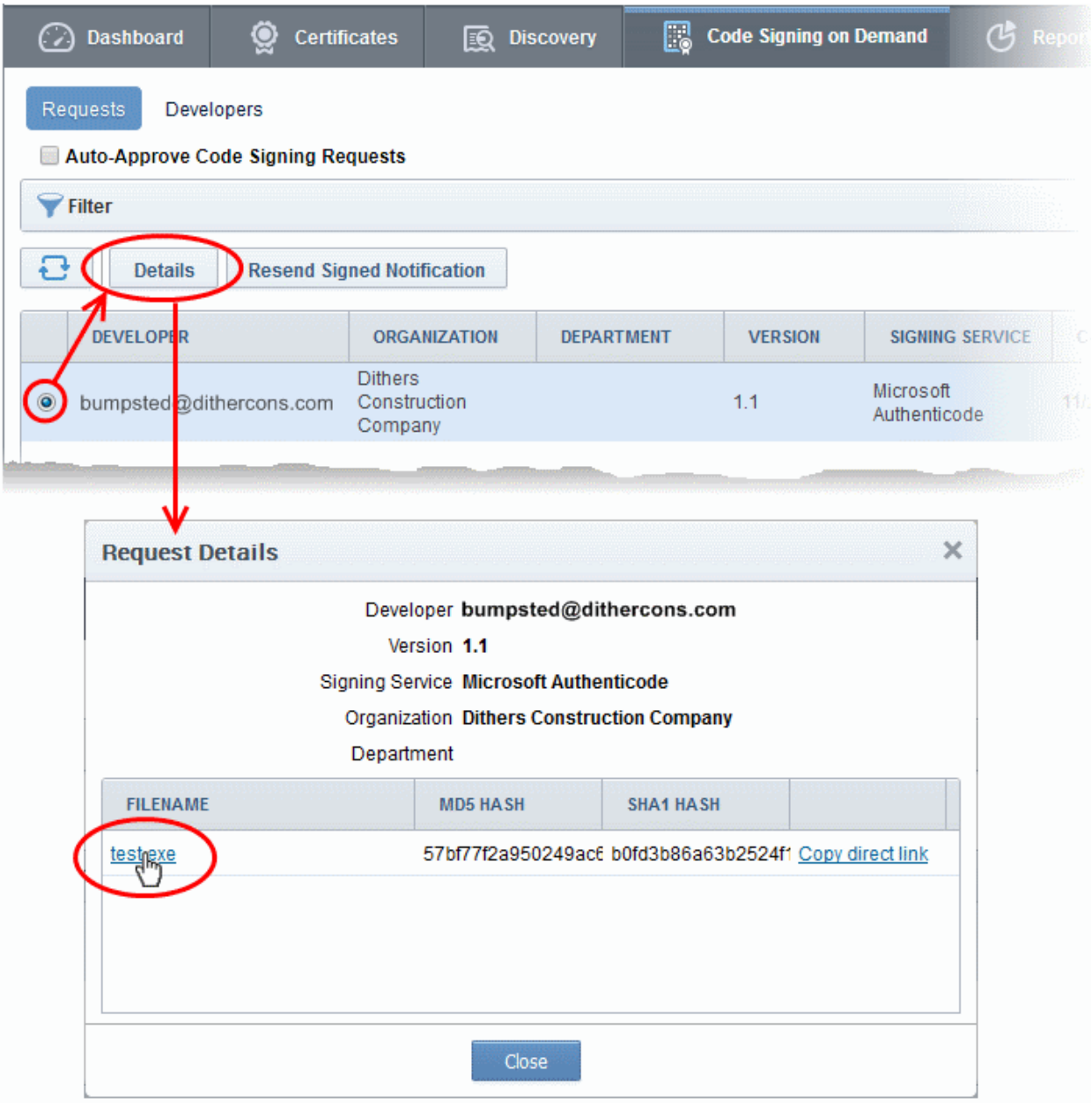


If a hash was uploaded, the developer can download the signed hash and embed it into the binary to create a digitally signed file.

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

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

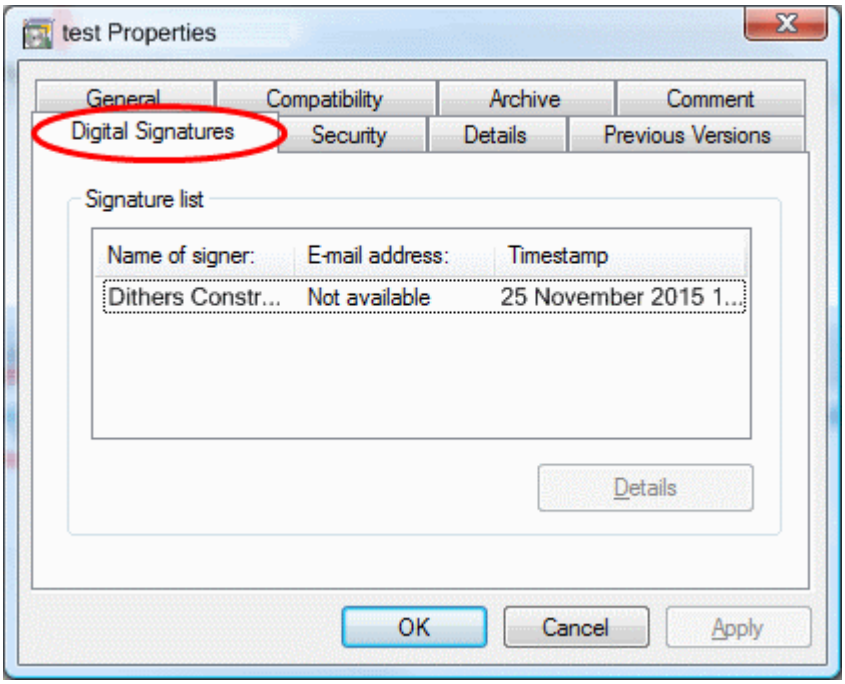
- Choose the request from the 'Code Signing on Demand' > 'Requests' interface and click 'Details'



- 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.

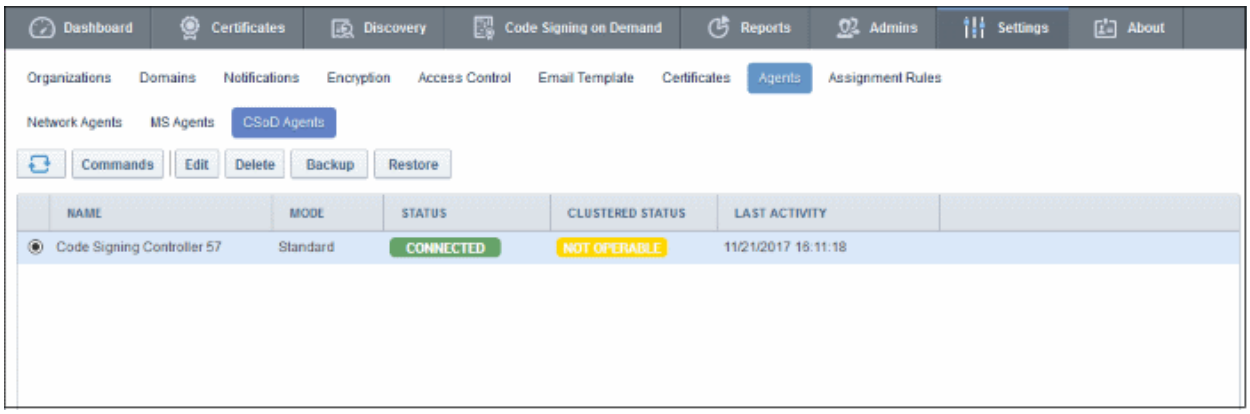
1.6 Configure the CSoD service

Each CSoD agent can be configured for backup and restore operations and for auto-approval of developer code-signing requests. The configuration options available to you depend on the mode of service enabled for your account.

The CSoD controller creates an encrypted 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.

The 'CSoD' agents area lets you configure the controller to automatically backup this database to a specific location (applies to standard mode installations, not cluster mode).

- Click 'Settings' > 'Agents' > 'CSoD Agents' to open the configuration interface



The interface allows you to:

- View the activities of the CSoD controller
- Backup/Restore Code Signing Certificates and their private keys (standard mode only)

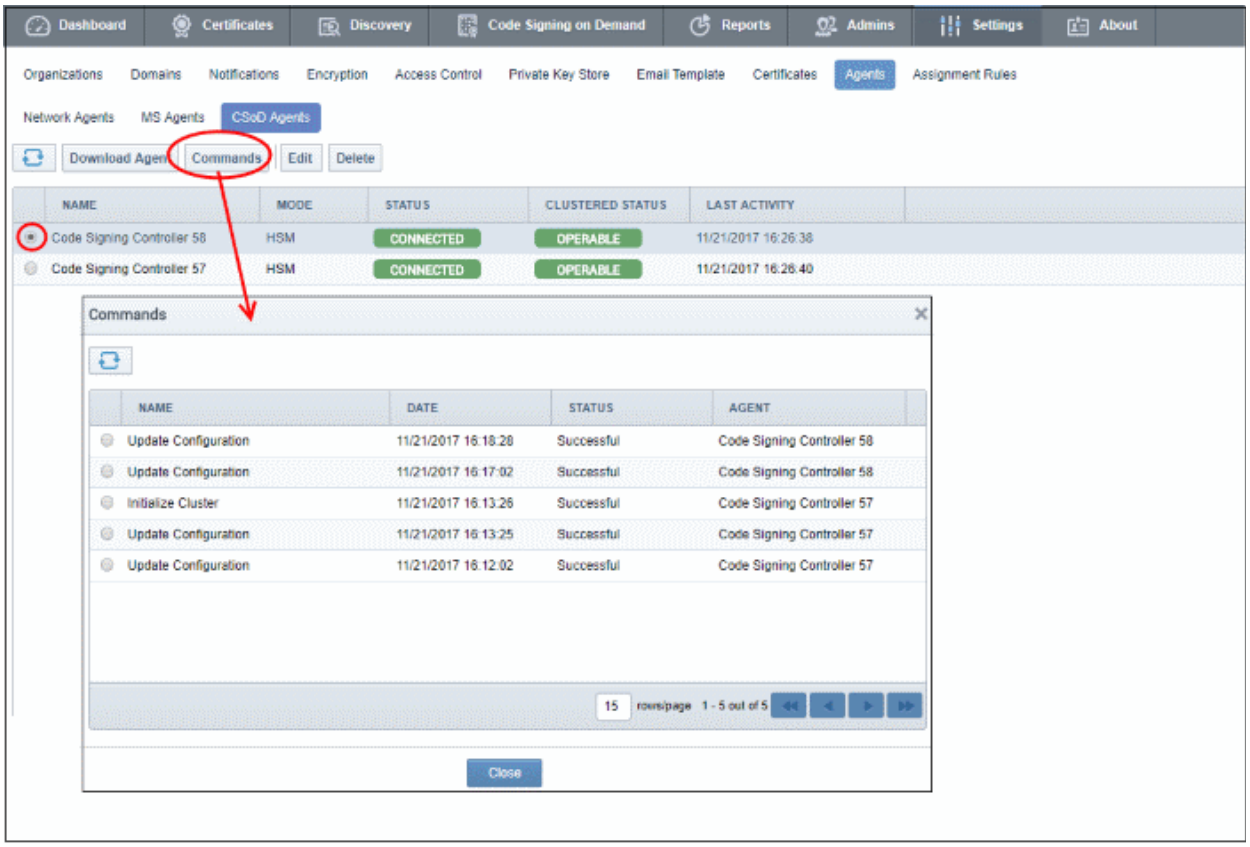
The 'Code Signing on Demand' > 'Requests' interface allows you to:

- Configure for auto approval of code signing requests

View the Activities of the CSoD Controller

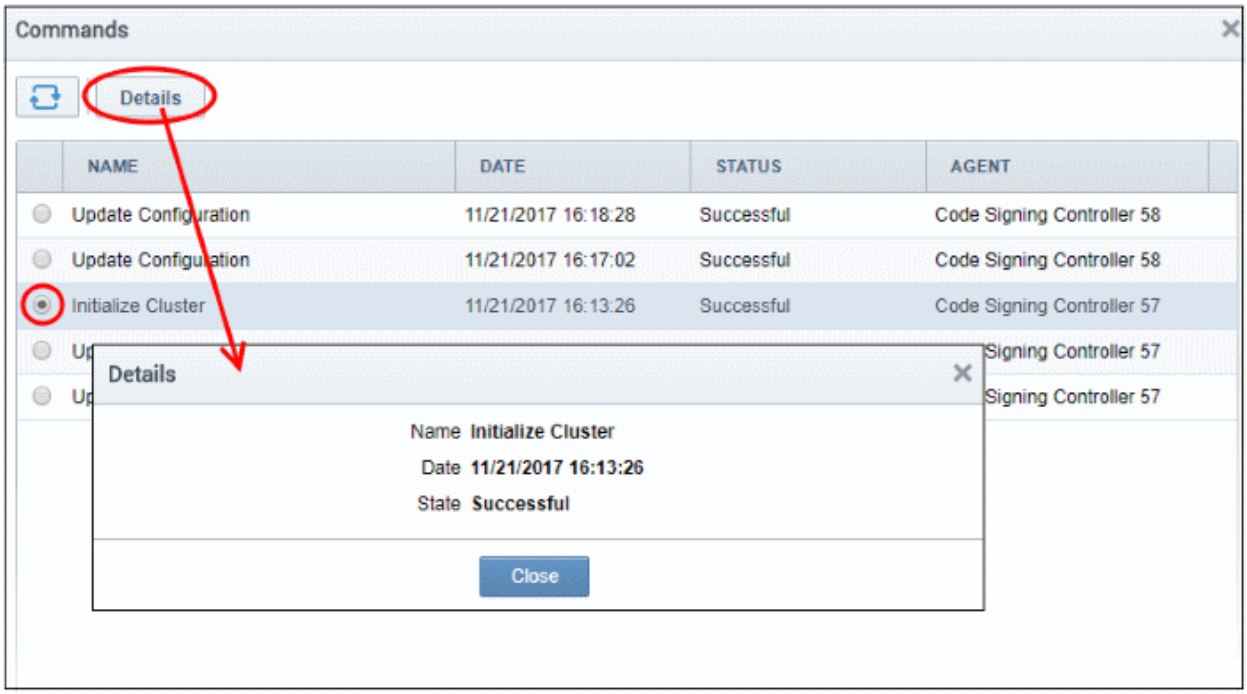
Once the controller is installed on your local network it automatically connects to CCM. The connection status is shown in the 'Settings' > 'Agents' > 'CSoD Agents' interface. You can view a list of commands sent by CCM to the controller and their execution status.

- Select an agent and click 'Commands' to view all commands received by the controller.



Commands Dialog - Column Descriptions	
Column Header	**Description**
Name	The label of the command received from CCM
Date	Date and time the command was received.
Status	Execution status/result of the command.
Agent	Name of the controller

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

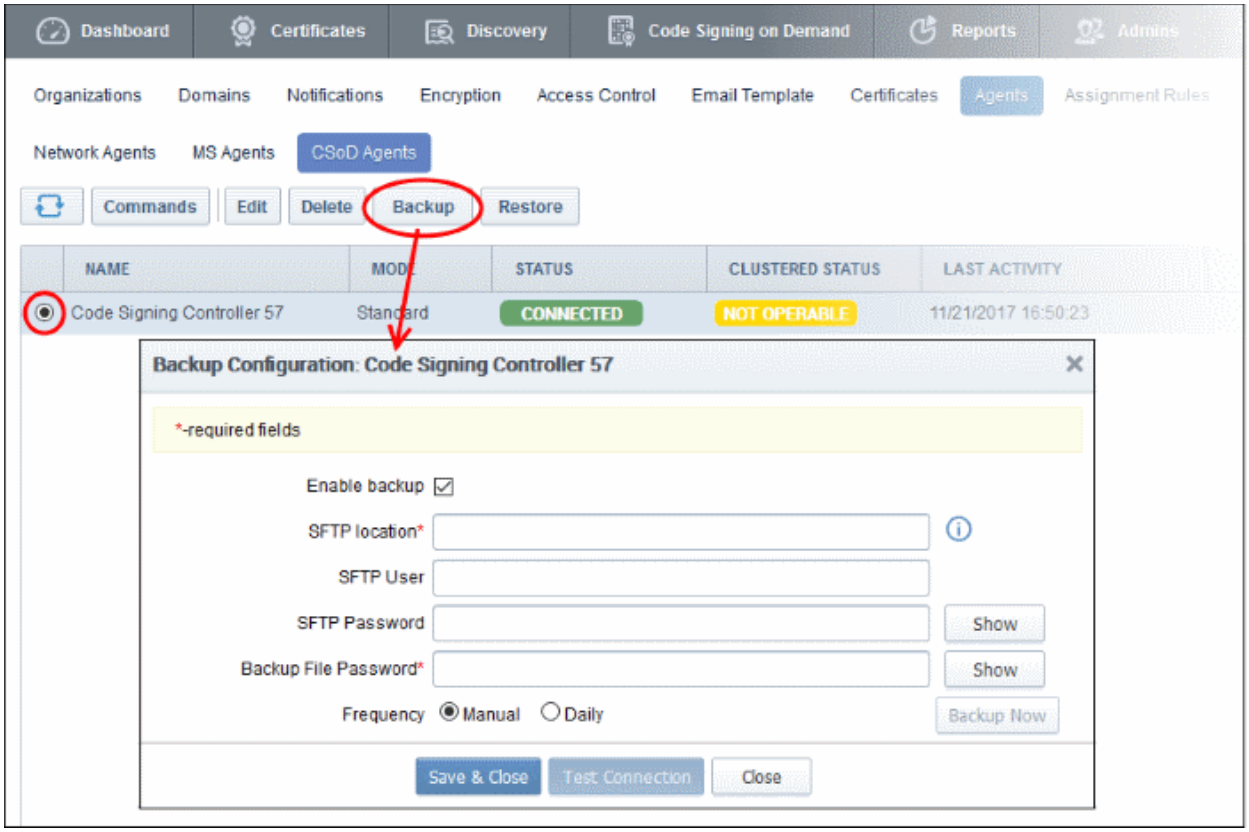


Backup/Restore Code Signing Certificates and Their Private Keys (standard mode only)

You can schedule regular backups of the CSoD database to a remote SFTP server, or run on-demand backup operations when required. Certificates and private keys can be restored from the backup.

To configure a backup

- Click 'Settings ' > 'Agents' > 'CSoD Agents'
- Select the controller and click 'Backup' at the top



Backup Configuration - Table of Parameters	
Parameter	**Description**
Enable backup	Activate or deactivate backup capability.
SFTP Location	Path on the SFTP server where the backup should be stored.
SFTP User	Username of an appropriately privileged account on the SFTP server. The controller will use this account to access the SFTP server.
SFTP Password	Password of the account mentioned above.
Backup File Password	Password for your backup file. You will need this to restore from the backup.
Frequency	Schedule at which backups should be taken. • Manual - The backup will run automatically. Click the 'Backup Now' button to run an on-demand backup. • Daily - Backups will be created daily at the time specified in the 'Next backup at:' drop-down. Choose the time in UTC when it should run.

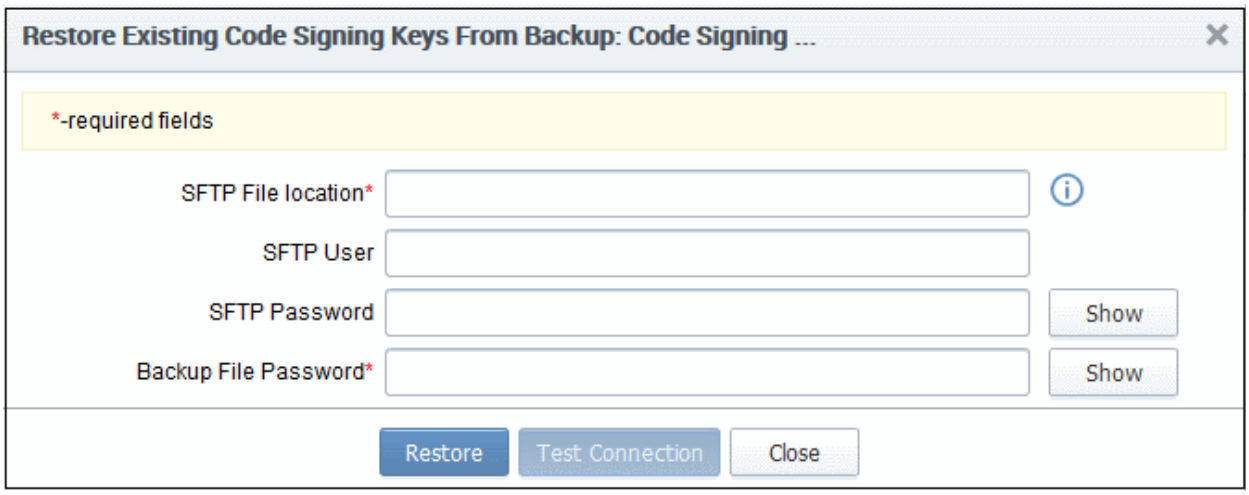
- Click 'Test Connection' to check the connection between CCM and the backup server
- Click 'Close' to cancel the backup configuration
- Click 'Save & Close' to apply your changes
- Click 'Backup Now' to run an instant backup

To restore the keys

- If there are problems with a controller and certificates belonging to the developer are lost, you can install a new controller and restore the certificates from a backup.
- Download the setup file for the new controller from 'Settings' > 'Agents' > 'CSoD Agents' and install it on your network. See '**Setup the CSoD Controller** ' if you need help with this.

If the installation is successful, the new controller will connect to CCM and will have a status of 'Connected'.

- Select the controller and click the 'Restore' button at the top
- You next need to specify the location of the backup file, and provide access credentials:



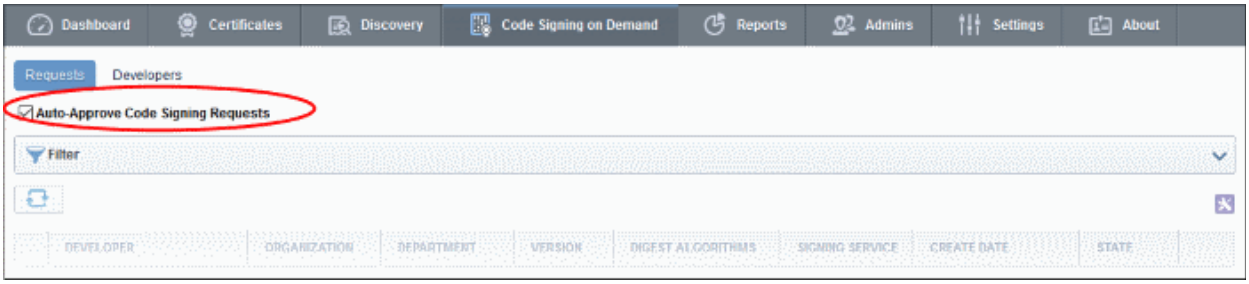
Restore Existing Code Signing Keys from Backup Configuration - Table of Parameters	
Parameter	**Description**
SFTP File Location	Path on the SFTP server where the CSoD service backup is stored. For example, sftp://my_sftp/backup/pkagent_yyyymmdd_HHmmss.jks
SFTP User	Username of an account with privileges to access the backup on the SFTP server.
SFTP Password	Password of the account mentioned above.
Backup File Password	Enter the password of the backup file.

- Click 'Test Connection' to check communication between CCM and the backup server.
- Click 'Close' to cancel the restore process
- Click 'Restore' to restore the backed up file

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

Configure for Auto Approval of Code Signing Requests

- By default, code signing requests from developers must be approved by an MRAO, RAO or DRAO administrator. Requests can be viewed, managed and approved in the 'Code Signing on Demand' > 'Requests' interface.
- Alternatively, you can configure the controller for auto-approval if you want to skip the manual approval process. If enabled, the controller will sign files right after they are uploaded by the developer. See **How to Sign Code using CSoD** for more details.



- Auto-Approve Code Signing Requests - Enable this setting if you want signing to commence without administrator approval. The service will start the signing process immediately after files are uploaded by the developer. See **How to sign code** using CSoD for more details.

About Comodo CA

Comodo Certificate Authority is one of the world's largest providers of SSL certificates by volume having issued over 91 million certificates and serving over 200,000 customers across 150 countries. The company provides a full suite of certificate products spanning all validation levels for website certificates, certificates for code-signing and email-signing, and the Comodo Certificate Manager (CCM) platform. Comodo CA has its US headquarters in New Jersey and international offices in the United Kingdom, Ukraine and India.

Comodo CA Limited

3rd Floor, 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