



Certificate Generation for Active Directory Windows 2008

Enterprise Version

@2015 Call2Unlock

<http://www.call2unlock.com>

Introduction

Call2unlock interacts with the Active Directory Server, sending commands to unlock and reset accounts, in the same way than one Help Desk Operator. In order to perform the reset of the accounts, is necessary generate and import one pem certificate from the Active Directory to Call2Unlock. Please follow the next steps to allow call2unlock reset accounts in your active directory in a secure way

1. Install the Active Directory Certificate Services

(Skip this step if is already done)

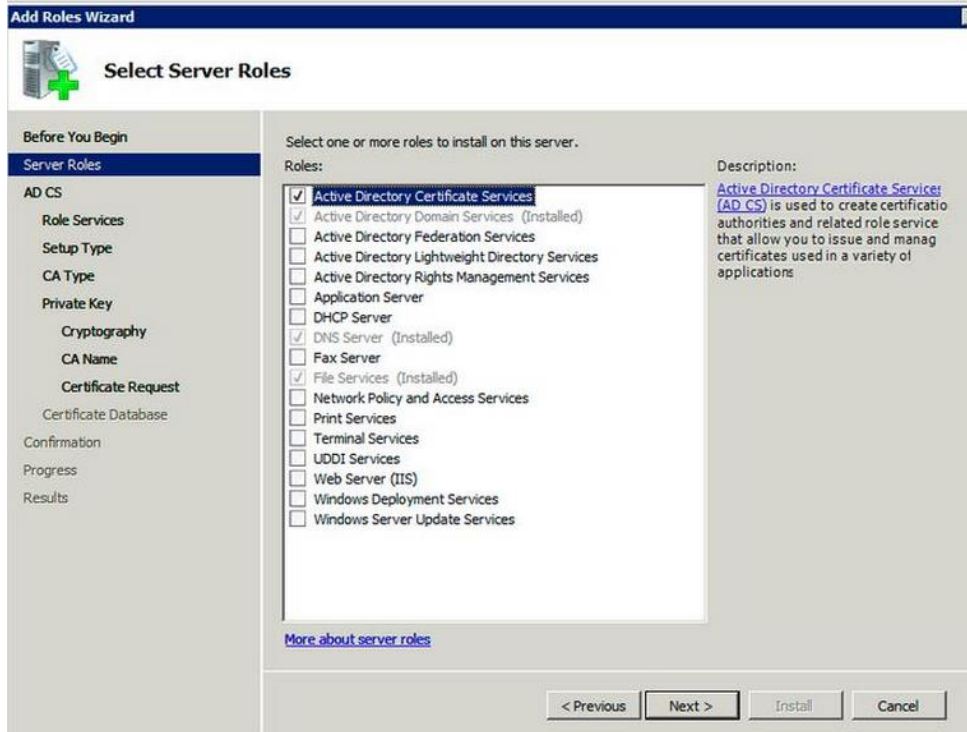
- Log in to the Active Directory server as an administrator.
- Click **Start**, click on **Administrative Tools**, and then click **Server Manager**.
- In the **Roles Summary** section, click **Add Roles**.

The screenshot displays the Windows Server Manager interface for a server named 'DC-ONE'. The left-hand navigation pane shows the 'Roles' section expanded, with sub-items for Active Directory Domain Services, DNS Server, File Services, Features, Diagnostics, Configuration, and Storage. The main pane shows the 'Roles' configuration page. At the top, it says 'View the health of the roles installed on your server and add or remove roles and features.' Below this is the 'Roles Summary' section, which indicates that 3 of 17 roles are installed. The installed roles are: Active Directory Domain Services (marked with a red X), DNS Server (marked with a yellow warning triangle), and File Services (marked with an information icon). To the right of the Roles Summary are buttons for 'Roles Summary Help', 'Add Roles', and 'Remove Roles'. Below the Roles Summary is the 'Active Directory Domain Services' section, which includes a description: 'Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.' This section also has a 'Go to Active Directory Domain Services' button. Underneath is the 'Role Status' section, showing 'Messages: None', 'System Services: 8 Running, 2 Stopped', and 'Events: 4 errors, 301 warnings, 9 informational in the last 24 hours'. At the bottom is the 'Role Services' section, which shows '1 installed' service. A table lists the role services and their status:

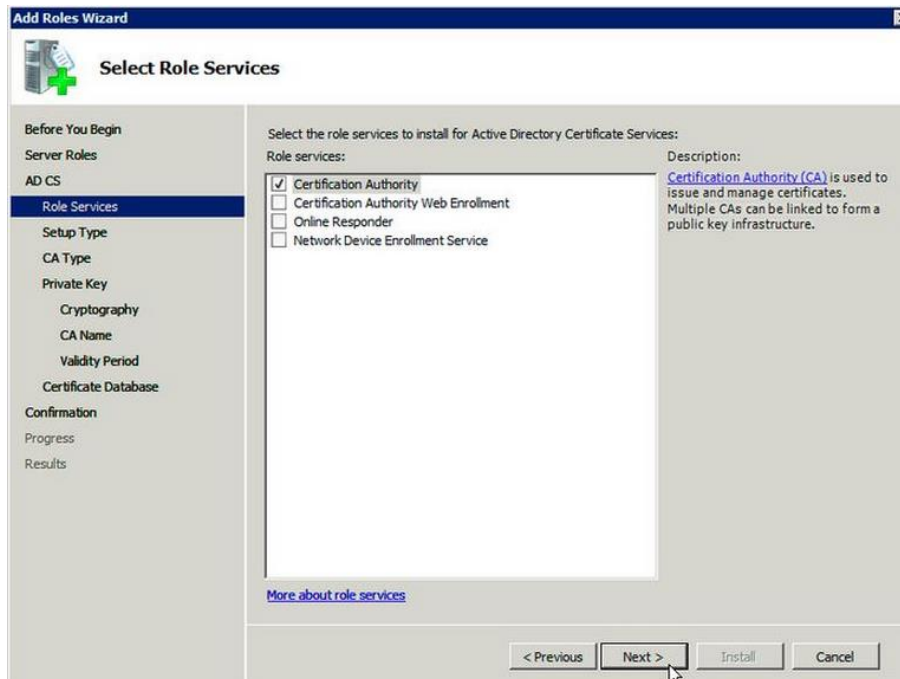
Role Service	Status
Active Directory Domain Controller	Installed
Identity Management for UNIX	Not installed
Server for Network Information Services	Not installed
Password Synchronization	Not installed
Administration Tools	Not installed

At the bottom of the console, there is a 'Description:' field and a status bar that reads 'Last Refresh: 21/02/2011 4:45:12 PM Configure refresh'.

- Once on the **Select Server Roles** page, select the **Active Directory Certificate Services** check box. Click **Next** twice. In the next screen “Installation Type”, select “**Role-based or feature-based installation**”



Once the **Select Role Services** page, select the **Certification Authority** check box, and then click **Next**



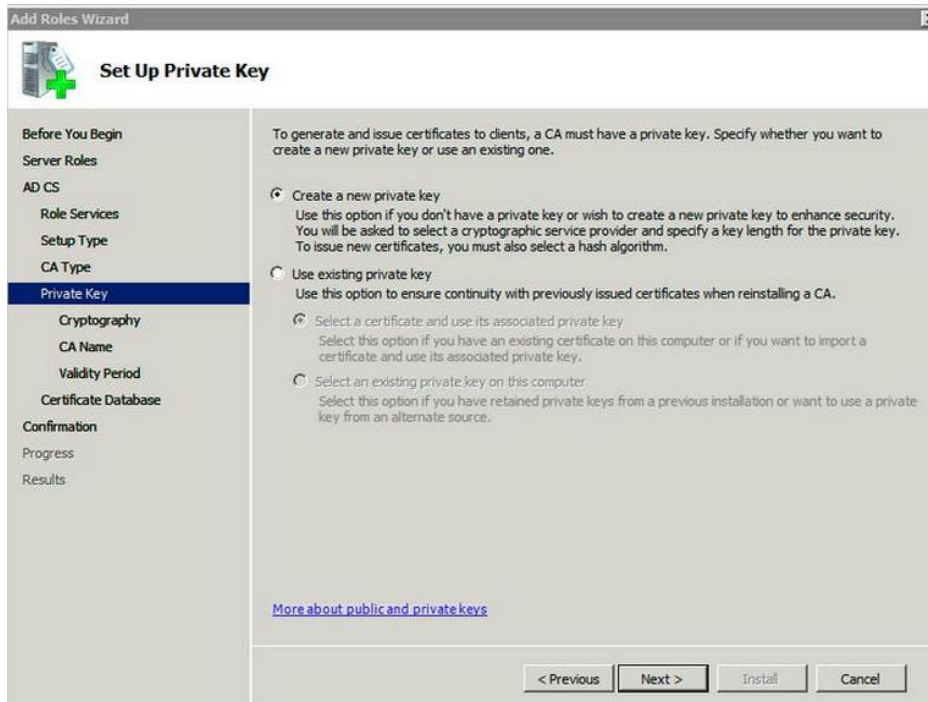
On the **Specify Setup Type** page, click **Enterprise**, and then click **Next**.

The screenshot shows the 'Specify Setup Type' page of the 'Add Roles Wizard'. The left-hand navigation pane lists the following steps: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type' (highlighted), 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main content area contains the following text: 'Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.' Below this text are two radio button options: 'Enterprise' (selected) and 'Standalone'. The 'Enterprise' option has a tooltip that reads: 'Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.' The 'Standalone' option has a tooltip that reads: 'Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.' At the bottom of the main area is a link: '[More about the differences between enterprise and standalone setup](#)'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

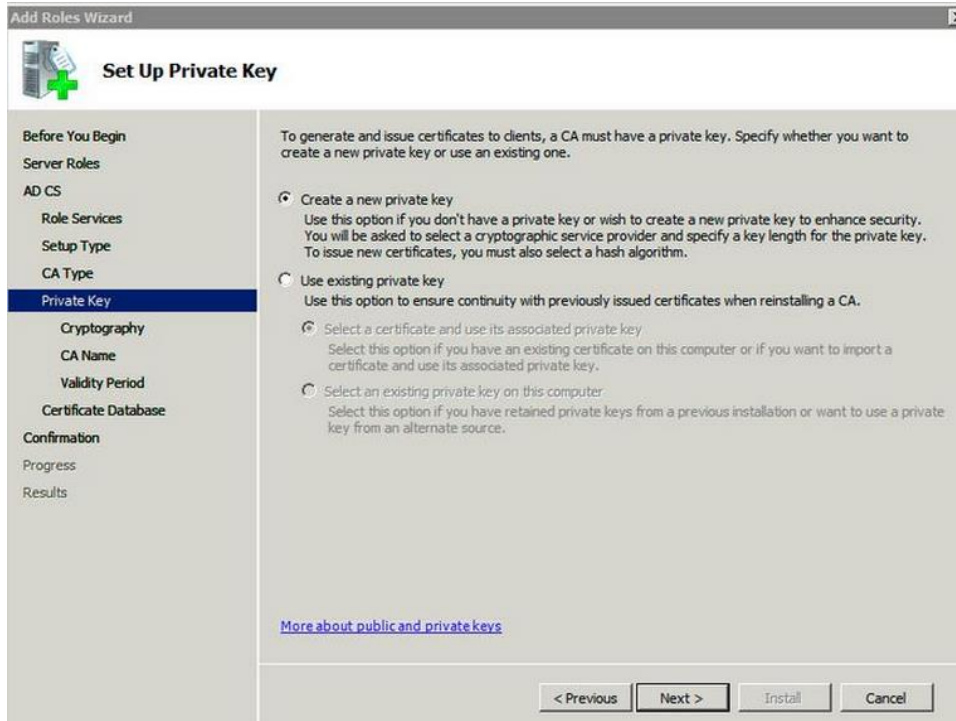
On the **Specify CA Type** page, click **Root CA**, and then click **Next**.

The screenshot shows the 'Specify CA Type' page of the 'Add Roles Wizard'. The left-hand navigation pane lists the following steps: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type' (highlighted), 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main content area contains the following text: 'A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.' Below this text are two radio button options: 'Root CA' (selected) and 'Subordinate CA'. The 'Root CA' option has a tooltip that reads: 'Select this option if you are installing the first or only certification authority in a public key infrastructure.' The 'Subordinate CA' option has a tooltip that reads: 'Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.' At the bottom of the main area is a link: '[More about public key infrastructure \(PKI\)](#)'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

On the **Set Up Private Key** and **Configure Cryptography for CA** , you can configure optional configuration settings, including cryptographic service providers. The default values should be ok. Click **Next** twice.



In the **Common name for this CA** box, type the common name of the CA, and then click **Next**.

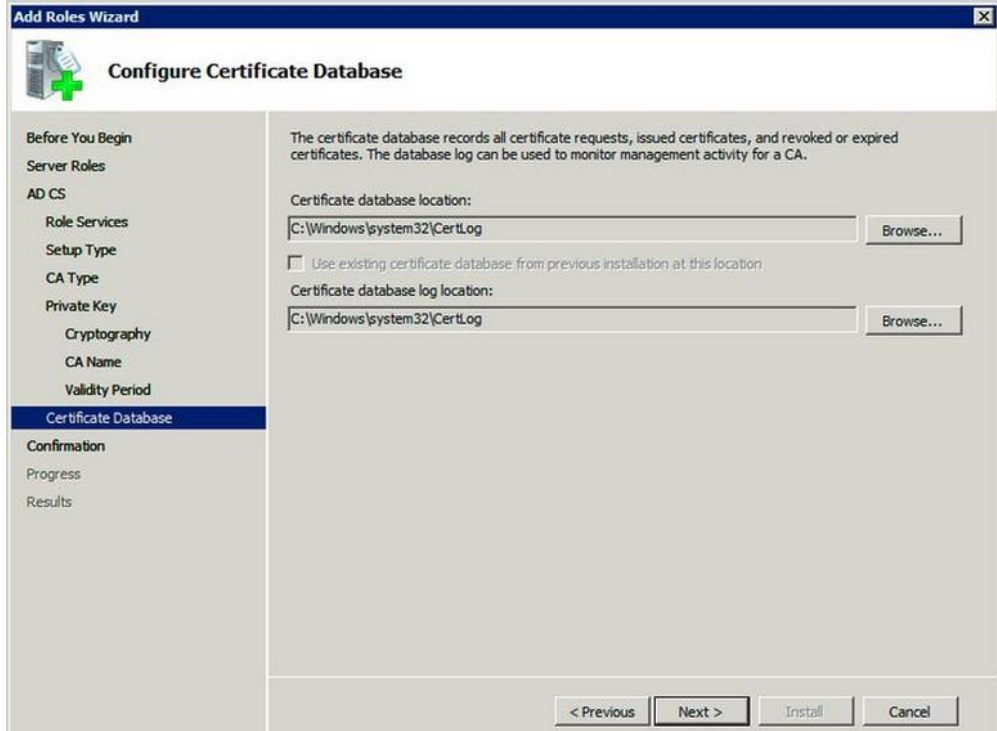


In the **Common name for this CA** screen, type the common name of the CA, and then click **Next**

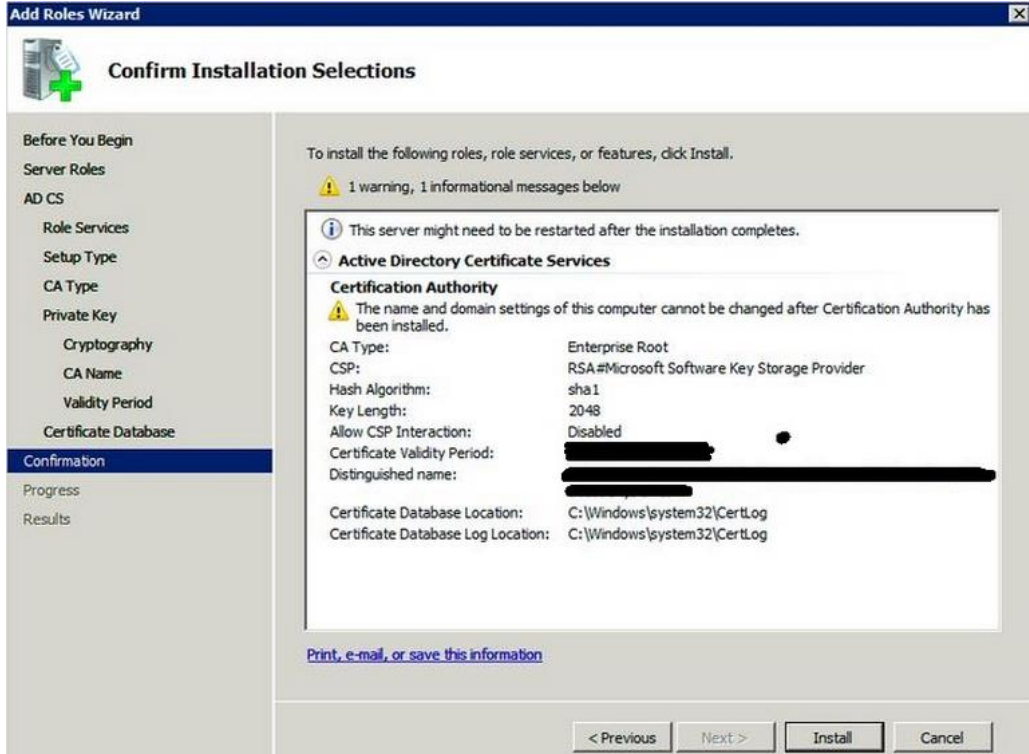
The screenshot shows the 'Configure CA Name' step of the 'Add Roles Wizard'. The left-hand navigation pane lists various steps, with 'CA Name' currently selected and highlighted in blue. The main content area contains the following text: 'Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.' Below this text are three input fields: 'Common name for this CA:', 'Distinguished name suffix:', and 'Preview of distinguished name:'. All three fields contain redacted text. At the bottom of the main area, there is a blue hyperlink: '[More about configuring a CA name](#)'. At the very bottom of the window, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

On the **Set Validity Period** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and then click **Next**.

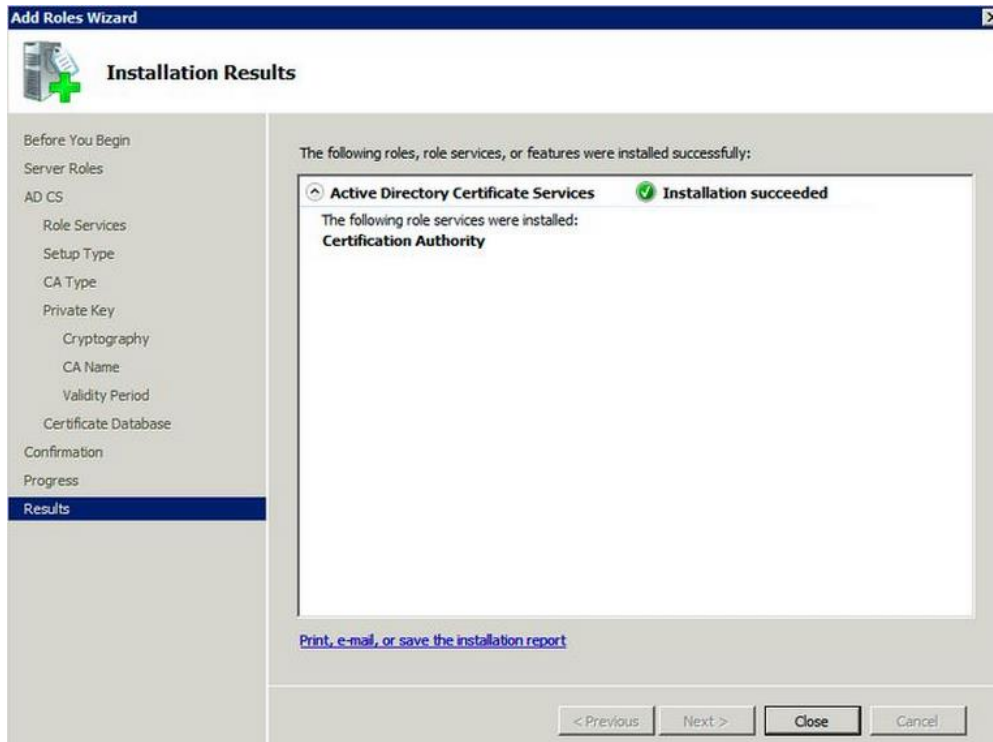
The screenshot shows the 'Set Validity Period' step of the 'Add Roles Wizard'. The left-hand navigation pane lists various steps, with 'Validity Period' currently selected and highlighted in blue. The main content area contains the following text: 'A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.' Below this text is a section titled 'Select validity period for the certificate generated for this CA:' which includes a dropdown menu showing '5' and the word 'Years'. Underneath is the text 'CA expiration Date: [redacted]'. A note follows: 'Note that CA will issue certificates valid only until its expiration date.' At the bottom of the main area, there is a blue hyperlink: '[More about setting the certificate validity period](#)'. At the very bottom of the window, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.



After verifying the information on the **Confirm Installation Selections** page, click **Install**.



Review the information on the results screen to verify that the installation was successfully done.



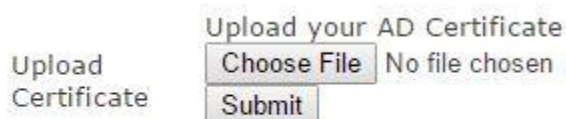
2. Obtain and upload the Server Certificate to Call2Unlock

The steps above describe how to install the certification authority (CA) on your Microsoft Active Directory server. Next, you will need to add the Microsoft Active Directory server's SSL certificate to the list of accepted certificates used by Call2Unlock, specially for reset accounts.

Execute this command on the Active Directory server in the power shell console:

```
certutil -ca.cert client.crt
```

Finally just copy the file created (in this case client.crt) to your local machine and import the file using **the LDAP Configuration** section of Call2Unlock Enterprise edition



Certificate generated, using the Active Directory Certifi
Once you upload your certificate, wait untill you get th
Uploaded message. To learn how to generate a CA Cer
Active Directory Server, **check this guide**