CALL2UNLOCK

Certificate Generation for Active Directory Windows 2012

Enterprise Version

http://www.call2unlock.com

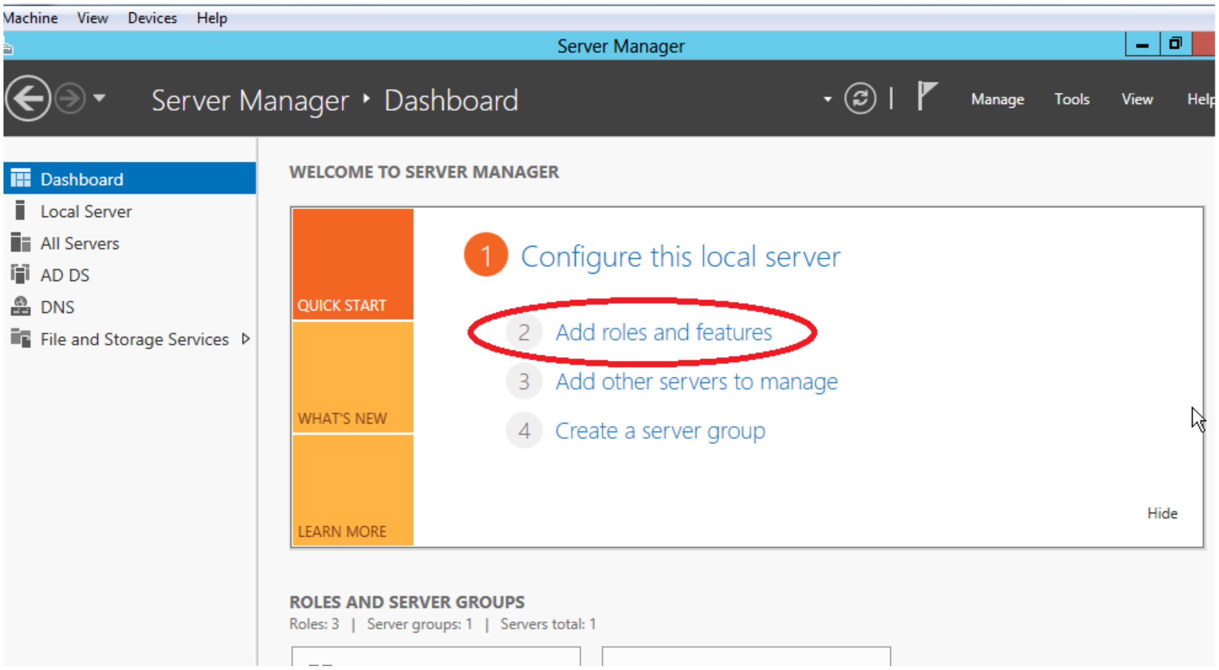
Introduction

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

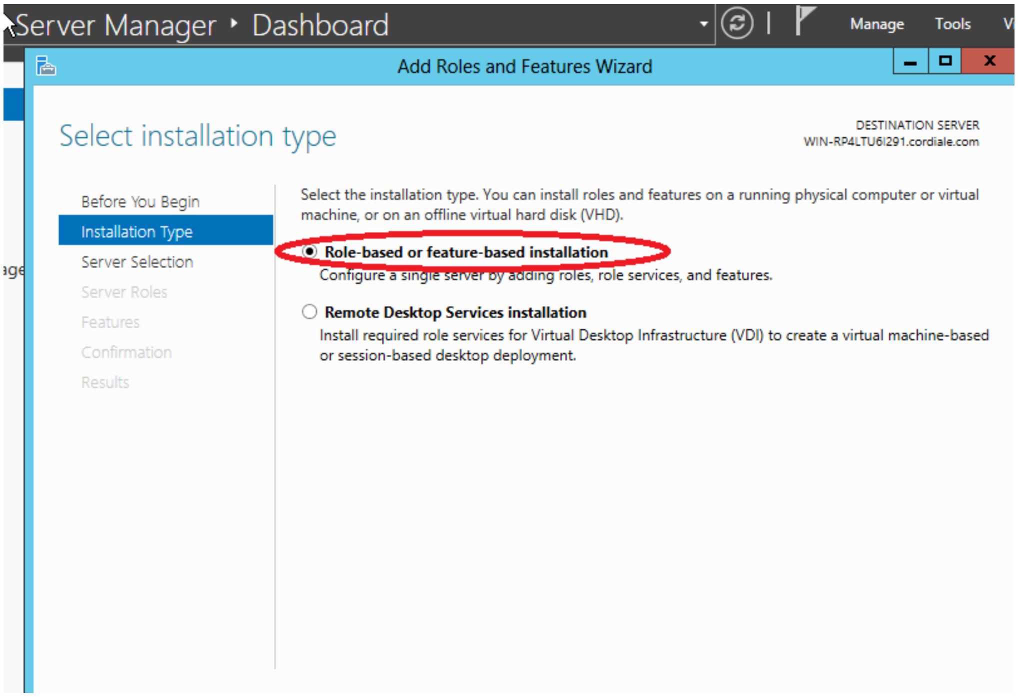
(Skip this step if is already done)

- Log in to the Active Directory server as an administrator.
- Go to the Server Manager click on **Dashboard**.
- Click in "Add roles and features".



- In the next screen "Before you Begin", just go to next, because is just informative.

- In the next screen "Installation Type" , select **"Role-based or feature-based installation"**



Select installation type

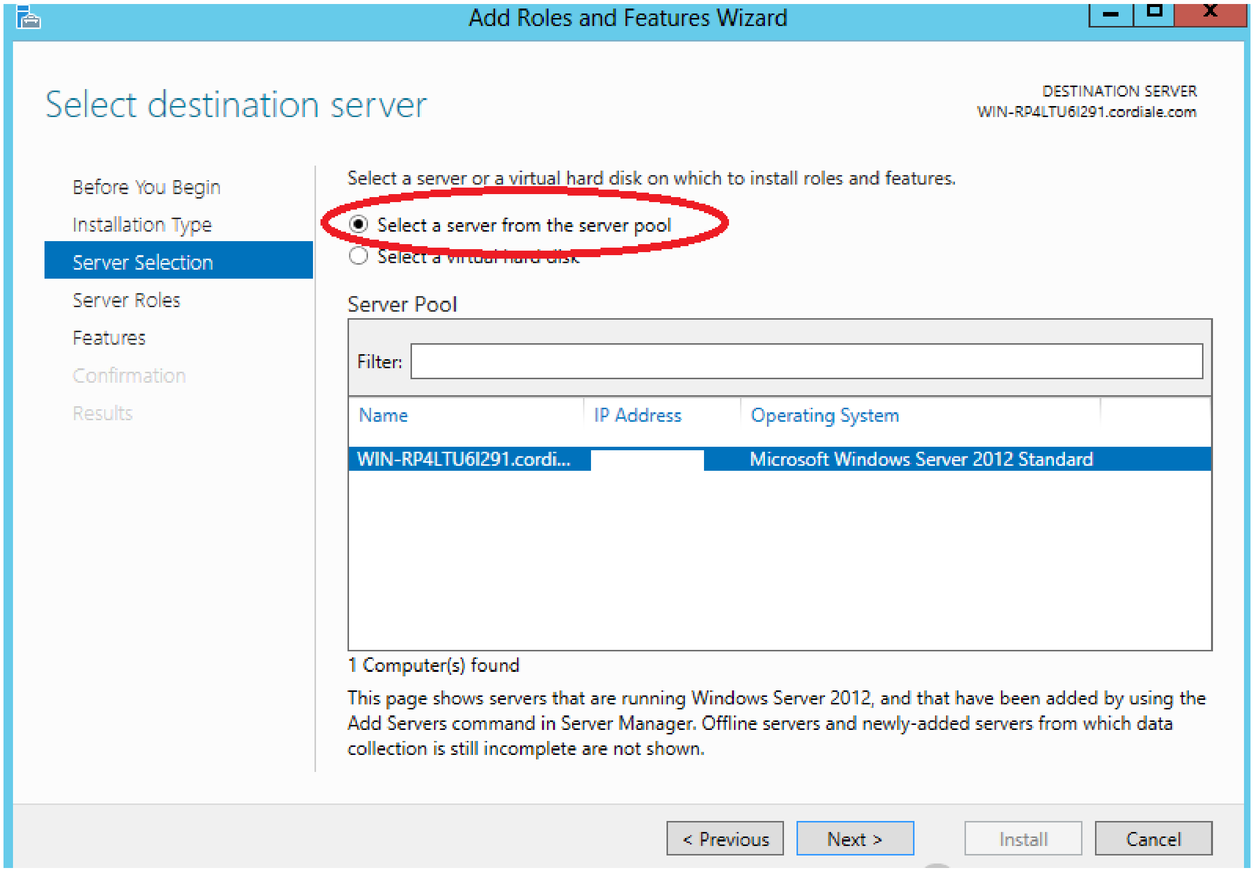
DESTINATION SERVER
WIN-RP4LTU6I291.cordiale.com

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

- In the next screen “Server Selection ” , select **“Select a server from the server pool”, (choosing your server), and click next**



Select destination server

DESTINATION SERVER
WIN-RP4LTU6I291.cordiale.com

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

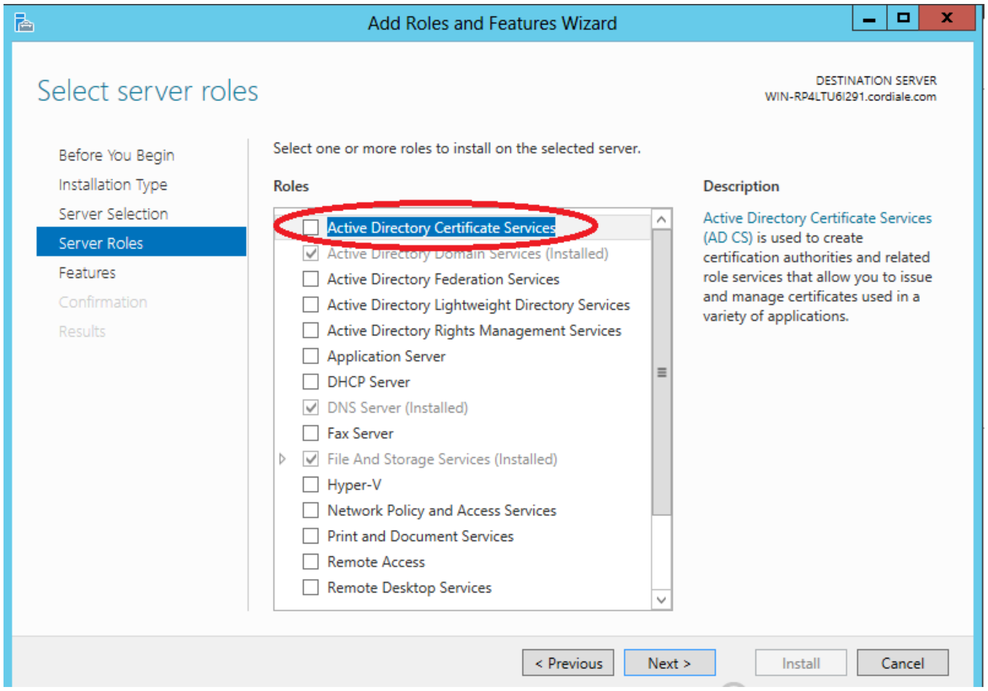
Filter:

Name	IP Address	Operating System
WIN-RP4LTU6I291.cordi...		Microsoft Windows Server 2012 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

- In the next screen “Server Roles ” , select **“Active Directory Certificate Services” , and click next**



Select server roles

DESTINATION SERVER
WIN-RP4LTU6I291.cordiale.com

Select one or more roles to install on the selected server.

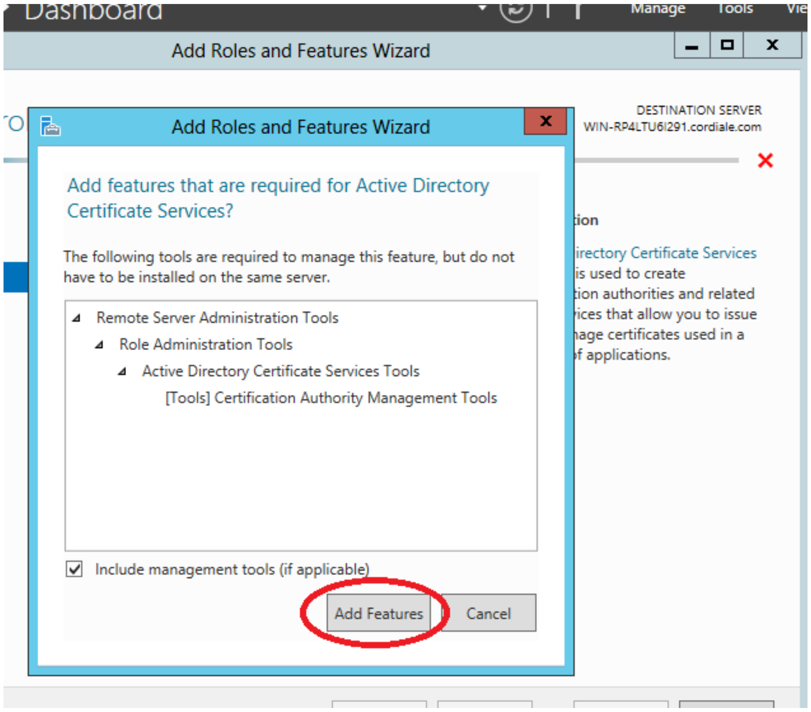
Roles

□ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
□ DHCP Server
☑ DNS Server (Installed)
□ Fax Server
☑ File And Storage Services (Installed)
□ Hyper-V
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

- In the next screen, check “Include management tools”, and click on “Add features”


Dashboard
Manage
Tools
Vie
Add Roles and Features Wizard
DESTINATION SERVER
WIN-RP4LTU6I291.cordiale.com
ion
irectory Certificate Services
is used to create
ion authorities and related
ices that allow you to issue
age certificates used in a
f applications.
Add Features
Cancel

Add Roles and Features Wizard

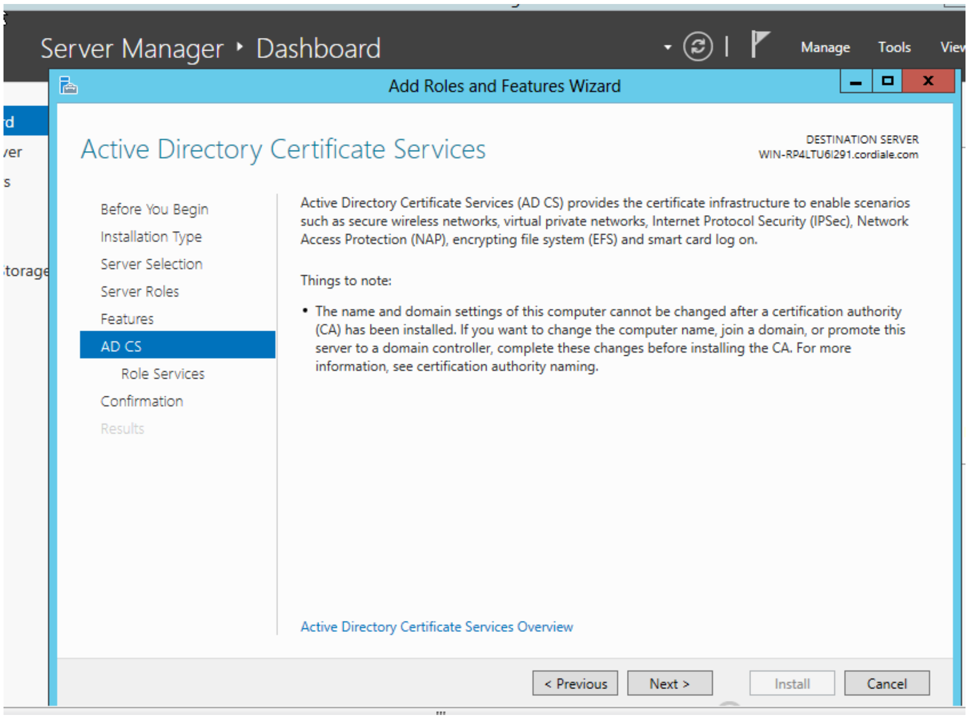
Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

Remote Server Administration Tools
  Role Administration Tools
    Active Directory Certificate Services Tools
      [Tools] Certification Authority Management Tools

☑ Include management tools (if applicable)

- In the next screen “AD CS ”,click next, and in the Roll services section check **“Certification Authoritty” , and click next**



Active Directory Certificate Services

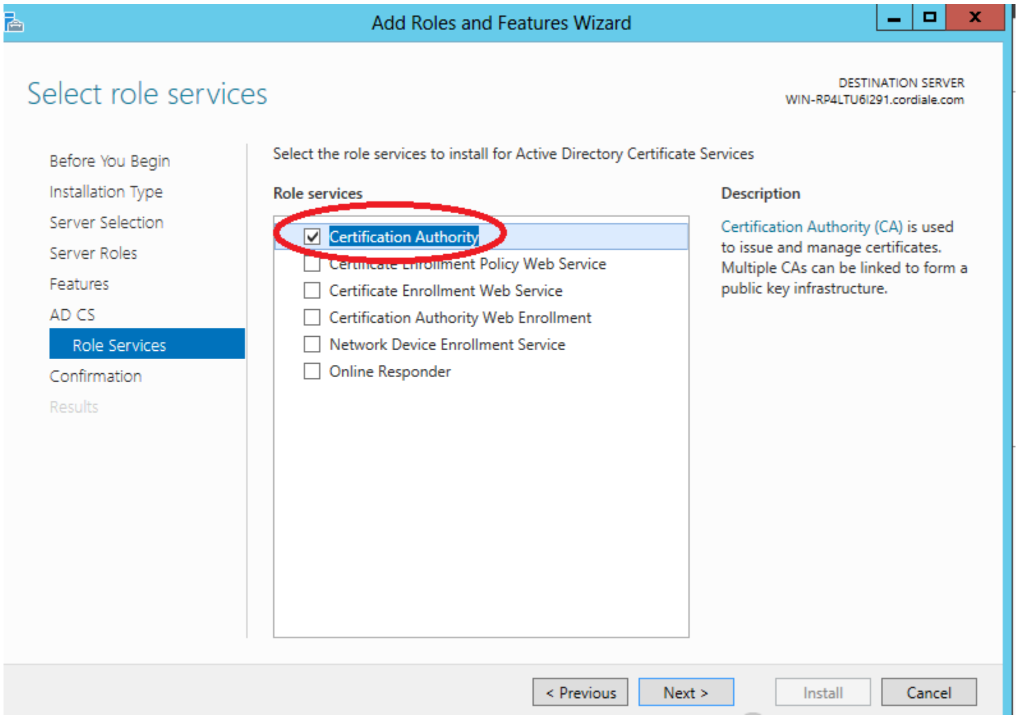
DESTINATION SERVER
WIN-RP4LTU6I291.cordiale.com

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

Things to note:

- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

Active Directory Certificate Services Overview



Select role services

DESTINATION SERVER
WIN-RP4LTU6I291.cordiale.com

Select the role services to install for Active Directory Certificate Services

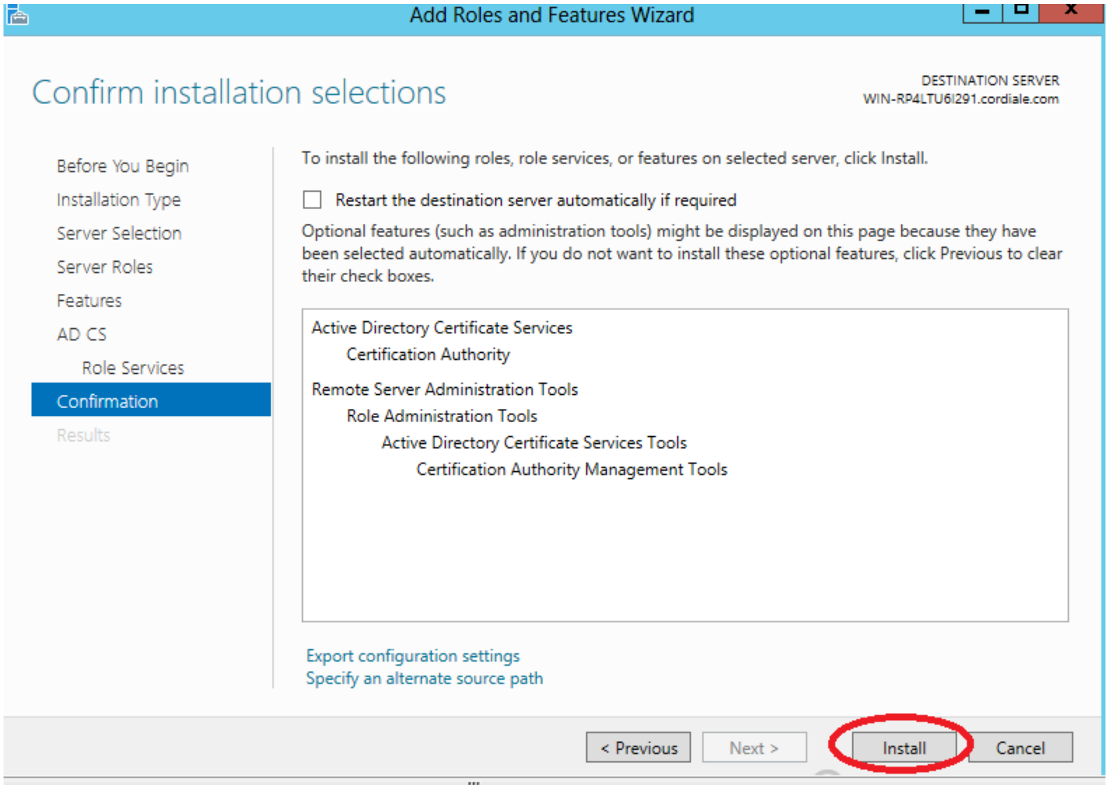
Role services

- ☑ Certification Authority
- ☐ Certificate Enrollment Policy Web Service
- ☐ Certificate Enrollment Web Service
- ☐ Certification Authority Web Enrollment
- ☐ Network Device Enrollment Service
- ☐ Online Responder

Description

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

- In the next screen “Confirmation”, click on “Install”.



Confirm installation selections

DESTINATION SERVER
WIN-RP4LTU6I291.cordiale.com

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

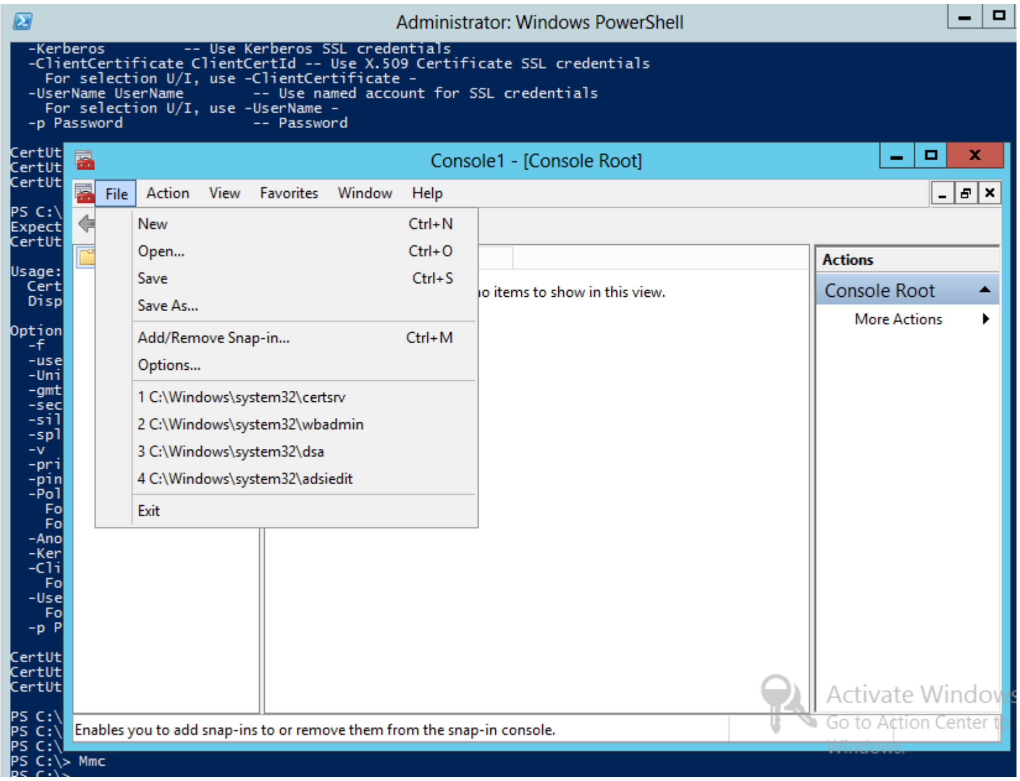
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Certificate Services
    Certification Authority
Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools

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.

1. Open a Microsoft Management Console (“mmc: from the command line)’
2. Go to File / Add/Remove Snap-in..

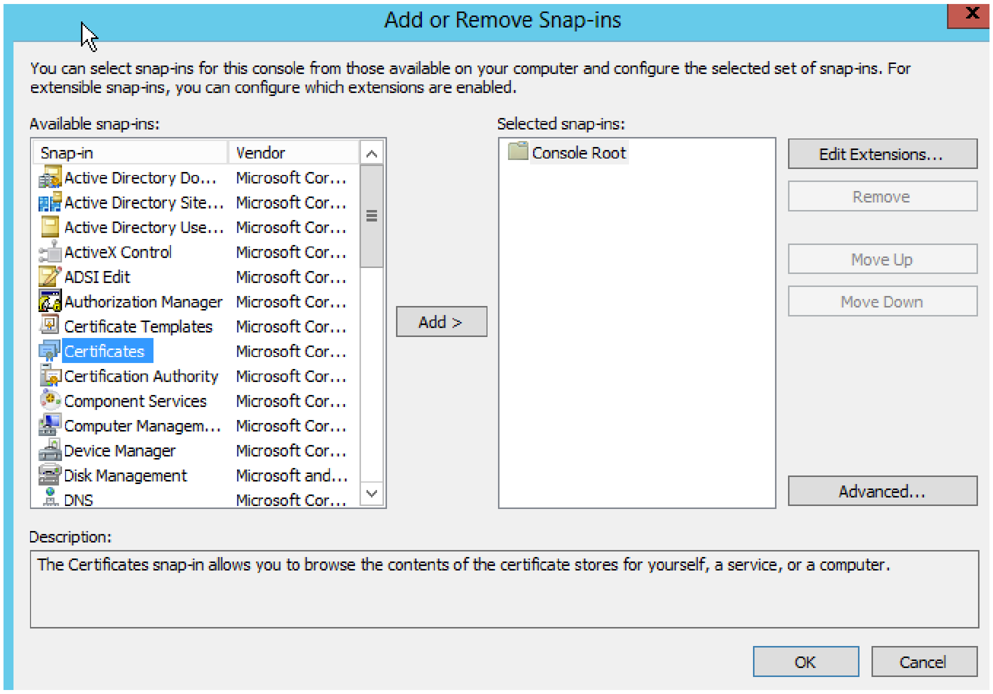

Administrator: Windows PowerShell
Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\certsrv
2 C:\Windows\system32\wbadmin
3 C:\Windows\system32\dsa
4 C:\Windows\system32\adsiedit
Exit
Actions
Console Root
More Actions
Activate Windows
Go to Action Center t

```
  -Kerberos          -- Use Kerberos SSL credentials
  -ClientCertificate ClientCertId -- Use X.509 Certificate SSL credentials
    For selection U/I, use -ClientCertificate -
  -UserName UserName        -- Use named account for SSL credentials
    For selection U/I, use -UserName -
  -p Password               -- Password

CertUt
CertUt
CertUt

PS C:\
Expect
CertUt

Usage:
  Cert
  Disp

Option
  -f
  -use
  -Uni
  -gmt
  -sec
  -sil
  -spl
  -v
  -pri
  -pin
  -Pol
    Fo
    Fo
  -Ano
  -Ker
  -Cli
    Fo
  -Use
    Fo
  -p P

CertUt
CertUt
CertUt

PS C:\
PS C:\
PS C:\
PS C:\> Mmc
```

o items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

3. Select Certificates from the list on the left, and click “Add”



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
DNS	Microsoft Cor...

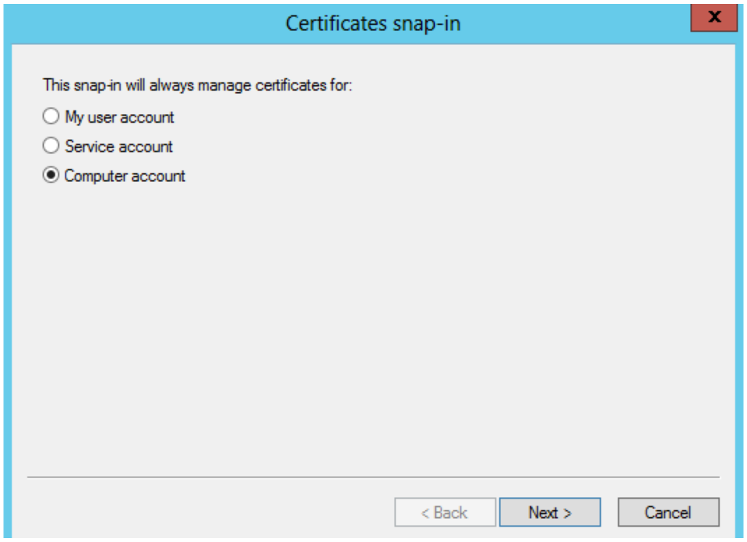
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. Choose “Computer account” as option in the screen and click Next



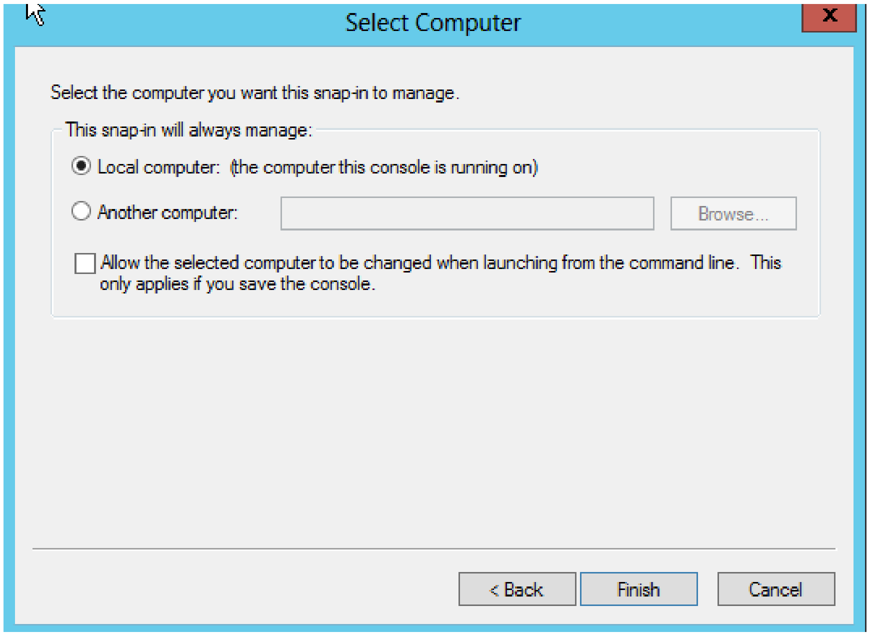
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

5. Select "Local Computer" and click on "Finish"



Select the computer you want this snap-in to manage.

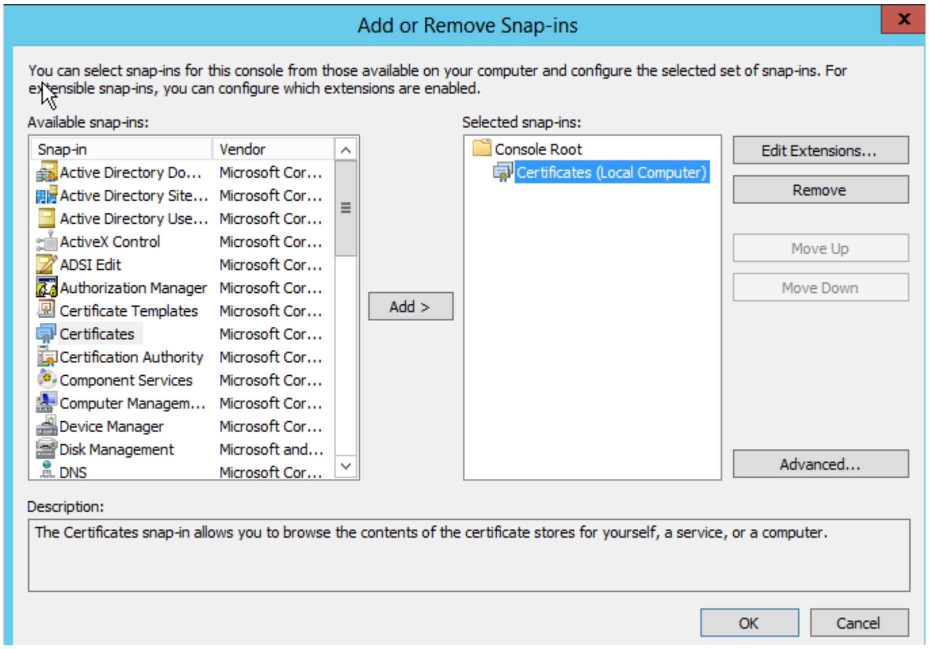
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

6. Select the snap-in "Certificates" on the right on the list, and click "OK"



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
DNS	Microsoft Cor...

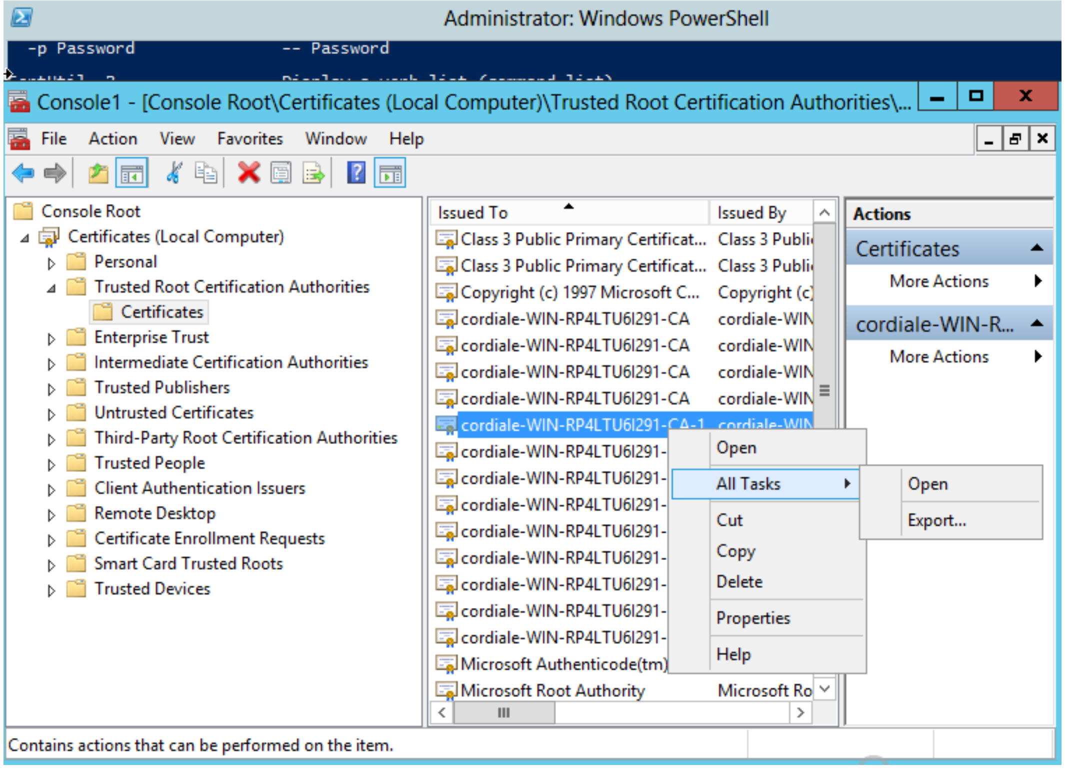
Selected snap-ins:

Console Root
Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

7. Navigate to "Trusted Rool Certification Authorities/ Certificates" and right click the certificate you want to export. Then Select All Tasks/Export



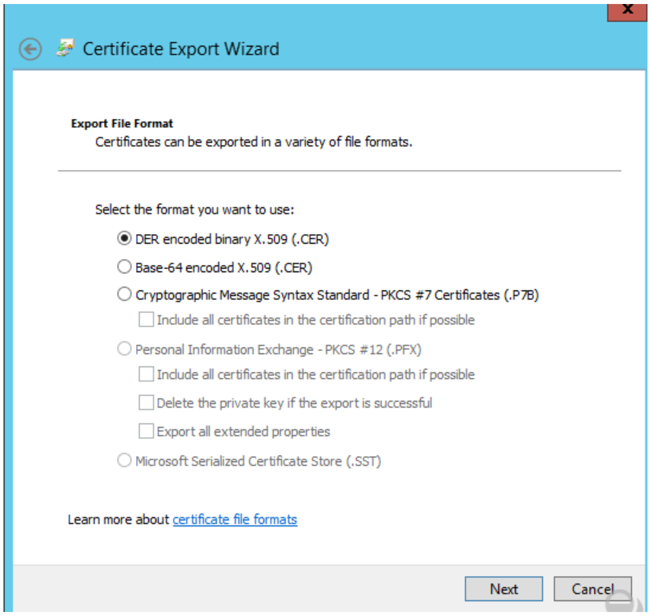
```
 -p Password              -- Password
```

Console Root
- Certificates (Local Computer)
  - Personal
  - Trusted Root Certification Authorities
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authorities
  - Trusted People
  - Client Authentication Issuers
  - Remote Desktop
  - Certificate Enrollment Requests
  - Smart Card Trusted Roots
  - Trusted Devices

Issued To	Issued By
Class 3 Public Primary Certificat...	Class 3 Publi
Class 3 Public Primary Certificat...	Class 3 Publi
Copyright (c) 1997 Microsoft C...	Copyright (c)
cordiale-WIN-RP4LTU6I291-CA	cordiale-WIN
cordiale-WIN-RP4LTU6I291-CA	cordiale-WIN
cordiale-WIN-RP4LTU6I291-CA	cordiale-WIN
cordiale-WIN-RP4LTU6I291-CA	cordiale-WIN
cordiale-WIN-RP4LTU6I291-CA-1	cordiale-WIN
cordiale-WIN-RP4LTU6I291-	
cordiale-WIN-RP4LTU6I291-	
cordiale-WIN-RP4LTU6I291-	
cordiale-WIN-RP4LTU6I291-	
cordiale-WIN-RP4LTU6I291-	
cordiale-WIN-RP4LTU6I291-	
cordiale-WIN-RP4LTU6I291-	
cordiale-WIN-RP4LTU6I291-	
Microsoft Authenticode(tm)	
Microsoft Root Authority	Microsoft Ro

Contains actions that can be performed on the item.

8. The Export Wizard will start, then select "Der encoded binary X.509 (.CER), like in the picture below



Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

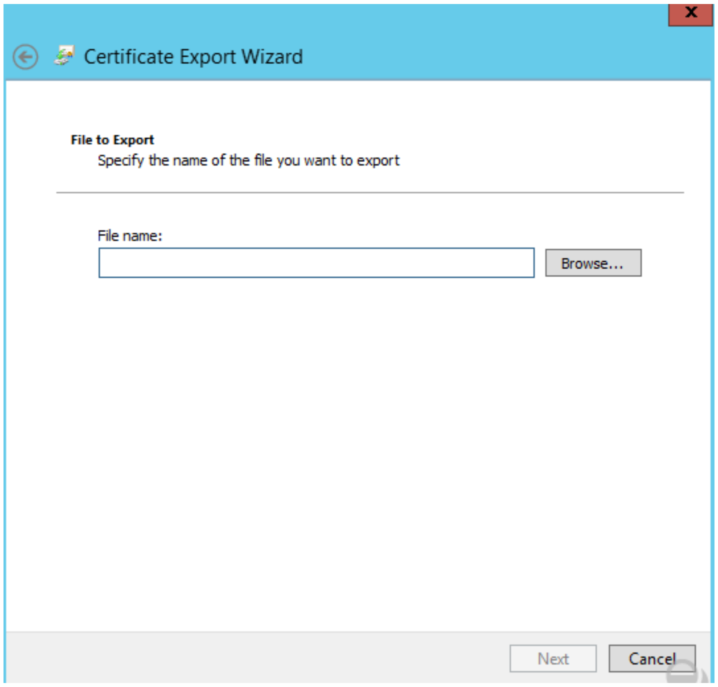
□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

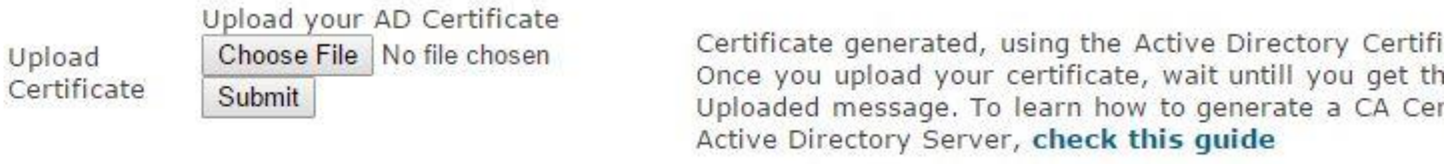
9. Finally, select the place to export the certificate.



File to Export
Specify the name of the file you want to export

File name:

10. 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**