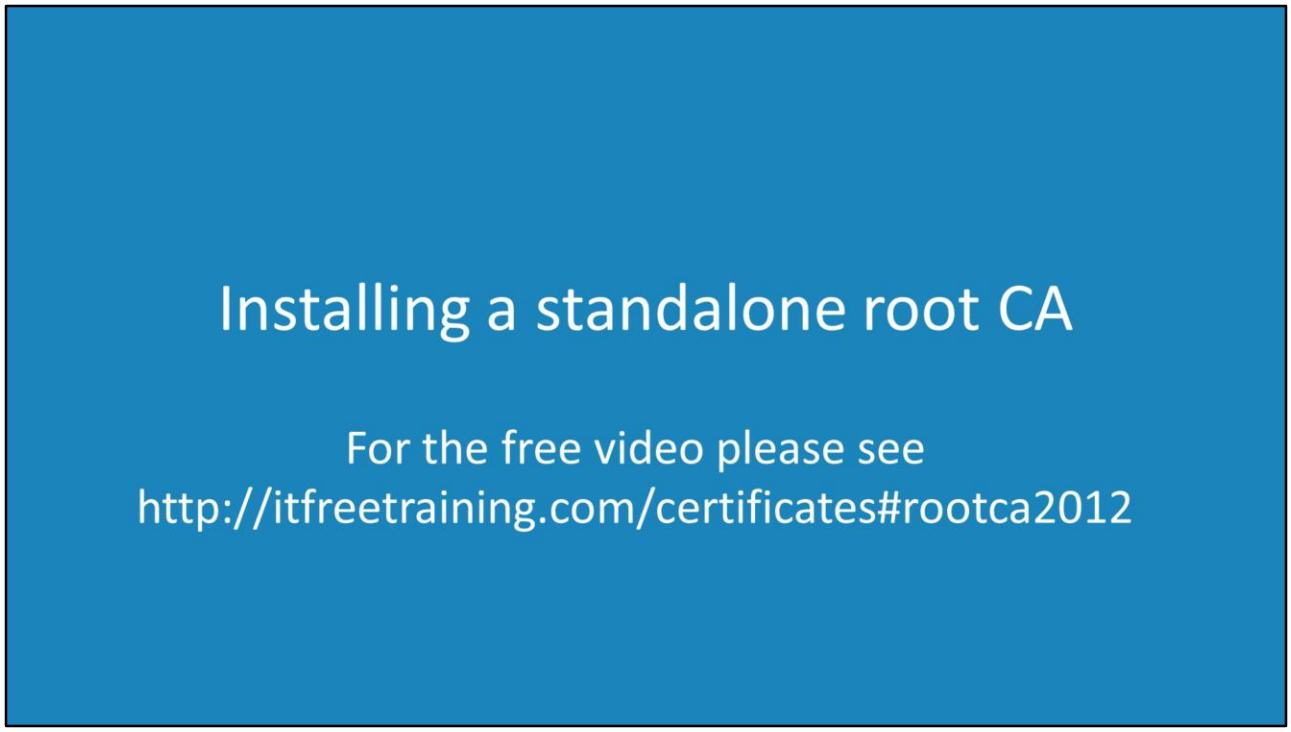
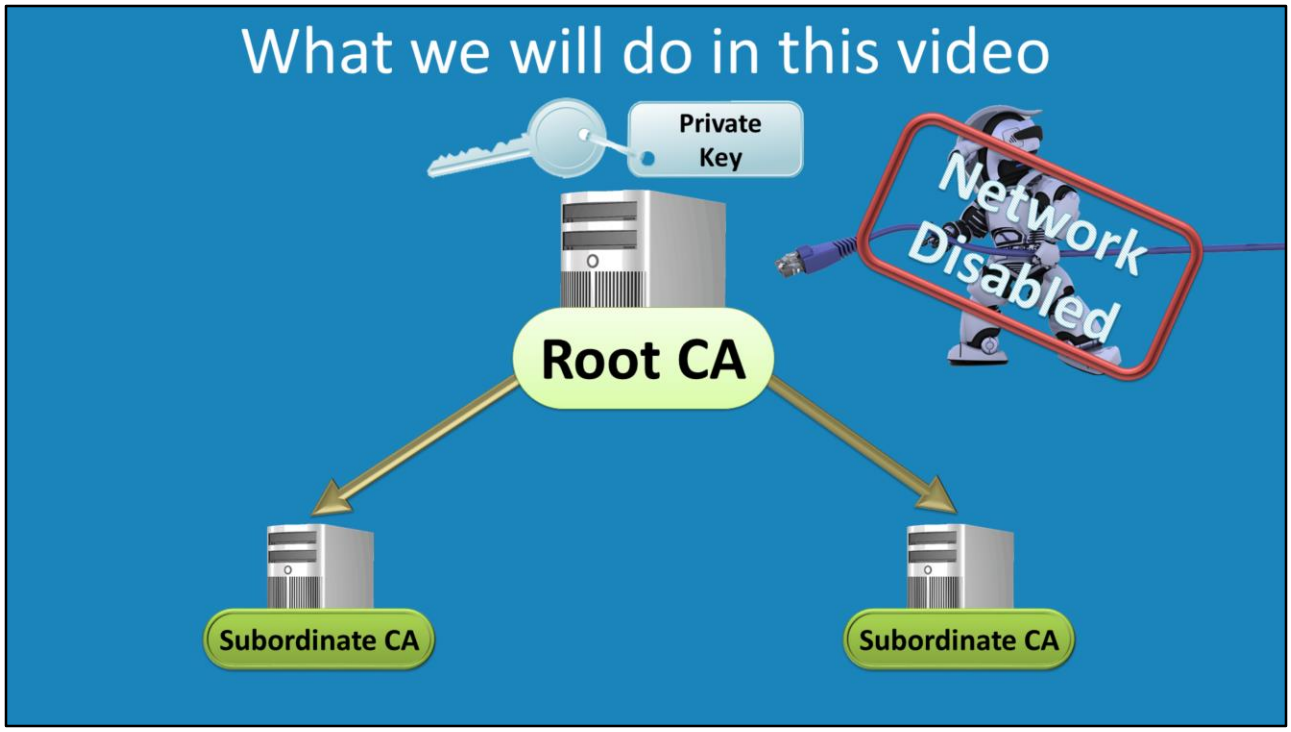
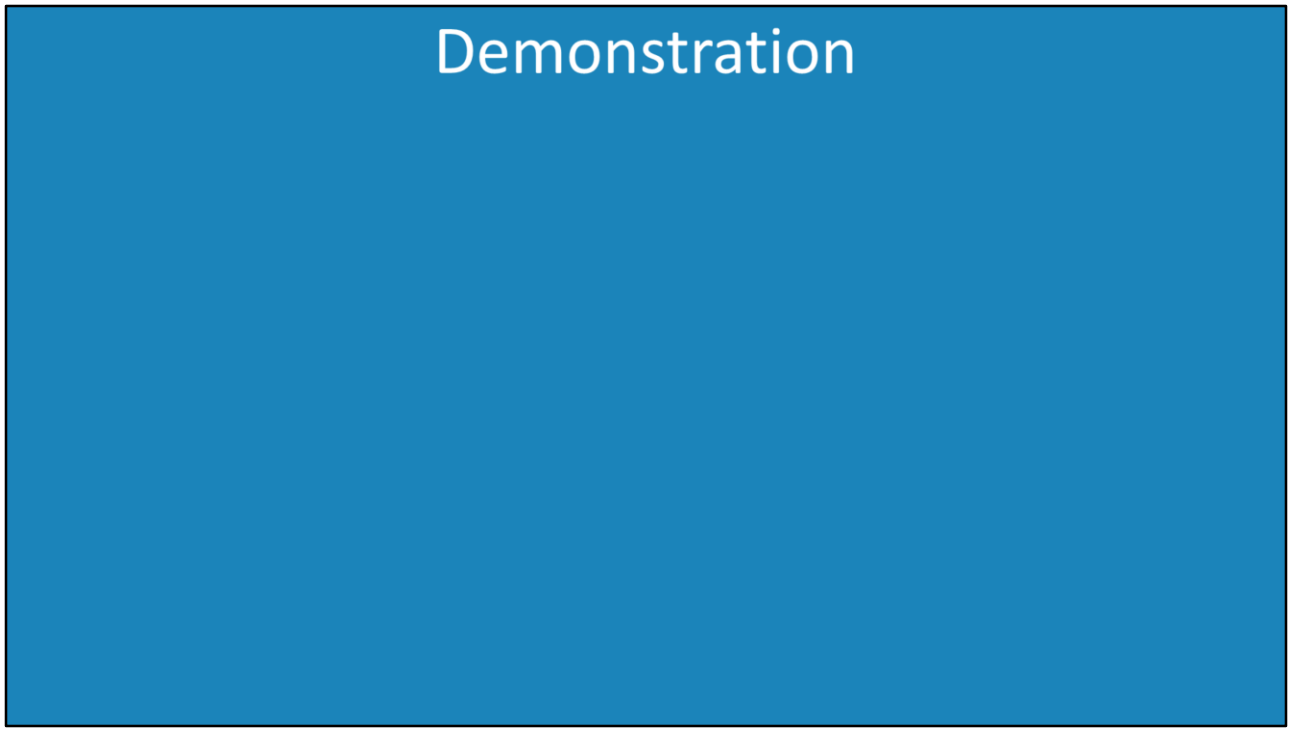


This video will look at how to install a Root CA on Windows Server 2012. The root CA forms the top of the certificate hierarchy. If compromised, all certificates in your hierarchy are also compromised. This video looks at not only how to install the root CA but also how to protect it from attack.



What we will do in this video

This video will look at installing and configuring a root CA using Windows Server 2012 that is not connected to the network. Any certificates that are created on this server will be transported to other servers using a floppy disk or a USB flash drive. Having the root CA not connected to the network helps protect the private key installed on the server.



Demonstration
The installation of the Root CA is divided into 3 parts. Pre configuration is done before the Active Directory Certificate Service role is installed so that the certificate created during the install have the right settings. Once these settings are used to create the certificate, the settings in the certificate cannot be modified later on. The second part of the install of the role involves adding of the role through server manager and selecting some options. The last step is post configuration which is needed in order to ensure that certificates that are created by the Root CA have the right options. This needs to be done before the root CA issues any certificates.
The files used in the demonstration are available for download. See the references part of the video for the URL.

Demonstration

- Pre Configuration

Pre configuration
When the Certificate Authority role is installed, a certificate for the root CA is created, unless you have a certificate from a previous install. In order to create this certificate, a number of options needed to be configured which cannot be configured using the wizard. These additional options are read from a file in
the Windows directory called CAPpolicy.inf. An example of this file is shown below.

```
[Version]
Signature="$Windows NT$"

[PolicyStatementExtension]
Policies=InternalPolicy

[InternalPolicy]
OID= 1.2.3.4.1455.67.89.5
Notice="Legal Policy Statement"
URL=http://ITFreeTraining.com/cps.txt

[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
```

AlternateSignatureAlgorithm=1
CRLDeltaPeriod=Days
CRLDeltaPeriodUnits=0
See below for a description for each part of the file.

[Version]
Signature="$Windows NT$"
This identifies the file as a setting file. This part simply needs to be copied and pasted to the top of the file and is always the same. There is no need to change any part of this file.

[PolicyStatementExtension]
Policies=InternalPolicy

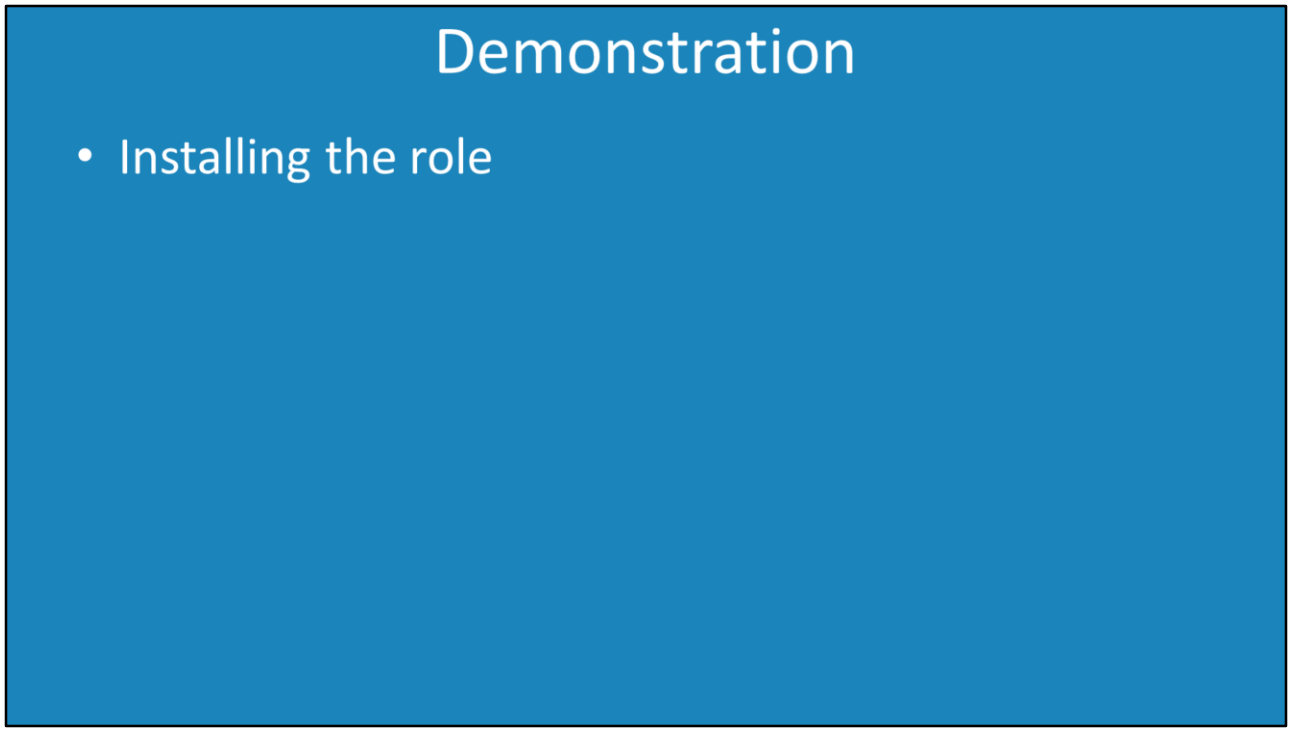
This part indicates the policies that relate to the certificate. These policies do not affect the operation of the CA or how the certificates work. They define how the certificate can be used just like a license agreement would define how a piece of software can be used. The policies defined in the setting file are embed in each certificate so the person using the certificate is able to read them or can find where to look them up.

[InternalPolicy]
OID= 1.2.3.4.1455.67.89.5
Notice="Legal Policy Statement"
URL=http://ITFreeTraining.com/cps.txt
This part is an example of a policy. The OID (Object Identifier) is a unique number. See the references for a link on where you can register your own OID. The notice setting is the text that is embedded in the certificate and the URL is a link to where the user of the certificate can download the policy text if they wish.

[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
AlternateSignatureAlgorithm=1
CRLDeltaPeriod=Days
CRLDeltaPeriodUnits=0

These settings determine renewal key length, how long the certificate will be valid for, signature algorithm and when CRL time differences are sent out. A lot of the settings are combined with a second setting ending in Units, when combined, determines the amount of time and whether it is in hours, weeks, months or years.

AltenateSignatureAlgorithm uses a new encryption method, which requires Windows Vista and Windows server 2008 or above. The CRLDeltaPeriod is set to 0. The Delta period determines when updates to the CRL (Certificate Revocation List) are sent out. The root CA is not connected to the network so it is impractical to have the root CA send out changes to the CRL, so it is best to disable it by setting the value to 0.



Installing the role
Once the CAPolicy.inf has been configured you can install the role. It is important to configure the CAPolciy.inf file first as the settings in this file will be used to create the root CA certificate. Once the root CA certificate has been created the settings in the Root CA certificate cannot be changed.

To install the role, open server manager and under the manage menu select Add Roles and Features. Once past the welcome screen, select the option “Role-based or feature-based installation” since the role will be added on the local server.

On the next screen, you will need to select the server that you want to install the role. In this case, the local server is selected, however you could always select a remote server if you wanted to.

For the roles select Active Directory Certificate Services. When prompted, also add the feature “Active Directory Certificate Services Tools”.

On the add features screen, no additional features are required so you can press next with no features selected and move on.

On the welcome screen of certificate services screen, there is a reminder that you will not be able to change the computer name of the server or its domain membership

once certificate services is installed.
On the components screen, the only component that you need to select is Certificate Authority. Once selected it is just a matter of finishing the wizard and the required components will be installed.

The components are installed in the background. Once the install is complete the server still needs to be configured. In server manager on the left hand side, select AD CS. At the top of the screen will be a warning message saying configuration required for Active Directory Services. To see the tasks that need to be configured, press the more option on the right hand side. This will show that post-deployment configuration is required for the certificate authority. Select this to start the post configuration wizard.

On the welcome screen of the configuration wizard, this will give you some more information and ask which user you want to perform the install with. In this case the install is being performed with the local administrator.

The next screen asks which components of certificate services you want to configure. In this case only the Certification Authority component was installed so this is the only component that requires configuration.

The next screen will ask if you want to setup an enterprise CA or a standalone CA. In this demonstration, the certificate authority will be installed as a standalone CA. If an enterprise CA option was chosen then the CA would need a connection to the network and also be able to connect to a valid Domain Controller.
When asked, “choose Root CA”, you would only choose subordinate CA if you already had a root CA and you were adding a child CA to the network.

In this demonstration, the option “create a new private key” is chosen. If you had an existing certificate, perhaps the certificate was from another server that crashed, you could use the option “use existing private key” to use a certificate that was used previously rather than creating a private key.
When asked what type of encryption you want to use, key size, and hash algorithm, choose carefully. These settings will affect which certificates can be used by user, computer and devices. For example, if you have a device that only supports 2048 bit key length and you use a higher key length, you cannot reduce the key length later on. This is because certificates in a hierarchy effectively are chained together. The settings you use on the certificate above effects the certificate below. So even if you use a different key size later on, the higher key size used before will still have an effect on the certificate and make it unusable to that user, computer or device that does not support that key length. If you use a setting that has a # at the start, then this will use a newer encryption algorithm that is more secure, however it also requires Windows

Vista or Windows Server 2008 or above.

The wizard will ask for a common name for the certificate. This will be embedded in the root CA certificate and also any certificate issued from the root CA or its subordinate. Choose wisely as once it is chosen the common name cannot be changed.
When asked to choose how long the certificate will be valid for, choose a value based on where the CA is in the hierarchy. For a root CA, it is not a bad idea to choose 20 years. As you go down the hierarchy this value should be at least halved at each level.

For the log and database location you can choose to install these on separate hard disks for performance reasons. A Root CA does not issue many certificates so you can leave this setting on the default.

Demonstration

- Post Configuration

Post Configuration
The following commands needs to be run in order to finish the configuration of the Root CA and should be run before any certificates are created.

This command configures the domain that will be embedded in each certificate that is created by the Root CA.

Certutil -setreg CA\DSConfigDN CN=Configuration,DC=ITFreeTraining,DC=com

These two commands configure the time period that certificates issued from the Root CA will be valid. In this case, they are set to 10 years, half the time period of the root CA. This setting should be at least half of the root CA.

Certutil -setreg CA\ValidityPeriodUnits 10
Certutil -setreg CA\ValidityPeriod "Years"

These two commands determine how long a CRL (Certificate Revocation List) is valid from. In this case this means that after 52 weeks the CRL will be recreated rather than being updated.
Certutil -setreg CA\CRLPeriodUnits 52
Certutil -setreg CA\CRLPeriod "Weeks"

These two setting determine the overlap period for CRL's.

Certutil -setreg CA\CRLOverlapPeriodUnits 12
Certutil -setreg CA\CRLOverlapPeriod "Hours"

The next two commands determine where the root CA certificate and CRL can be located. The commands are quite long but are essentially divided into 3 different locations. These are, the local hard disk, Active Directory and a web server. Before you run these commands you should change the location of the web server from http://pki.ITFreeTraining.com to point to your own web server. Other than this, no other part of the command needs to be changed.

certutil -setreg CA\CACertPublicationURLs
"1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt\n2:ldap:///CN=%7,CN=AIA,CN=Public Key
Services,CN=Services,%6%11\n2:http://pki.ITFreeTraining.com/CertEnroll/%1_%3%4.crt"

certutil -setreg CA\CRLPublicationURLs
"1:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl\n10:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key
Services,CN=Services,%6%10\n2:http://pki.ITFreeTraining.com/CertEnroll/%3%8%9.crl"
Make sure you restart the certificate authority service before you start issuing certificates.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
"MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition" pg 780
"Cryptographic Service Provider"
http://en.wikipedia.org/wiki/Cryptographic_Service_Provider
"Cryptography Next Generation" http://technet.microsoft.com/en-us/library/cc730763(v=ws.10).aspx
"Windows Server 2008 PKI and Certificate Security" pg 89