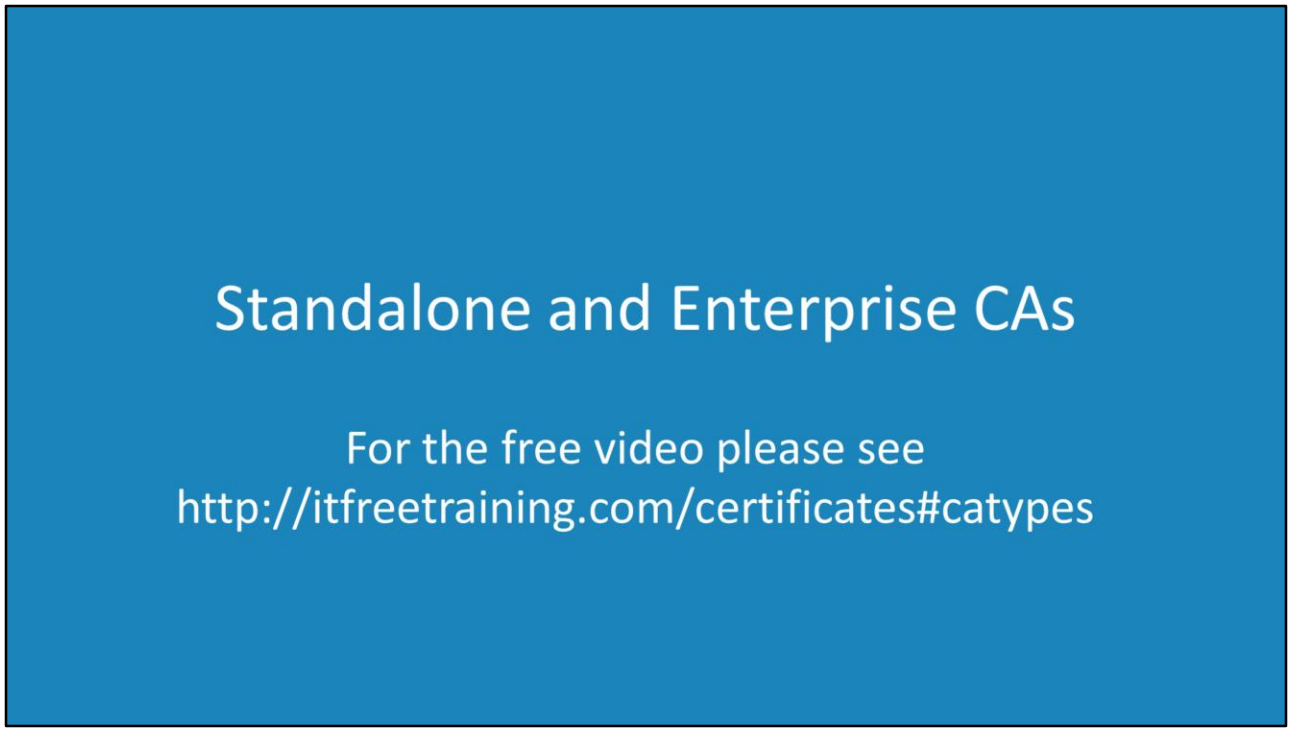
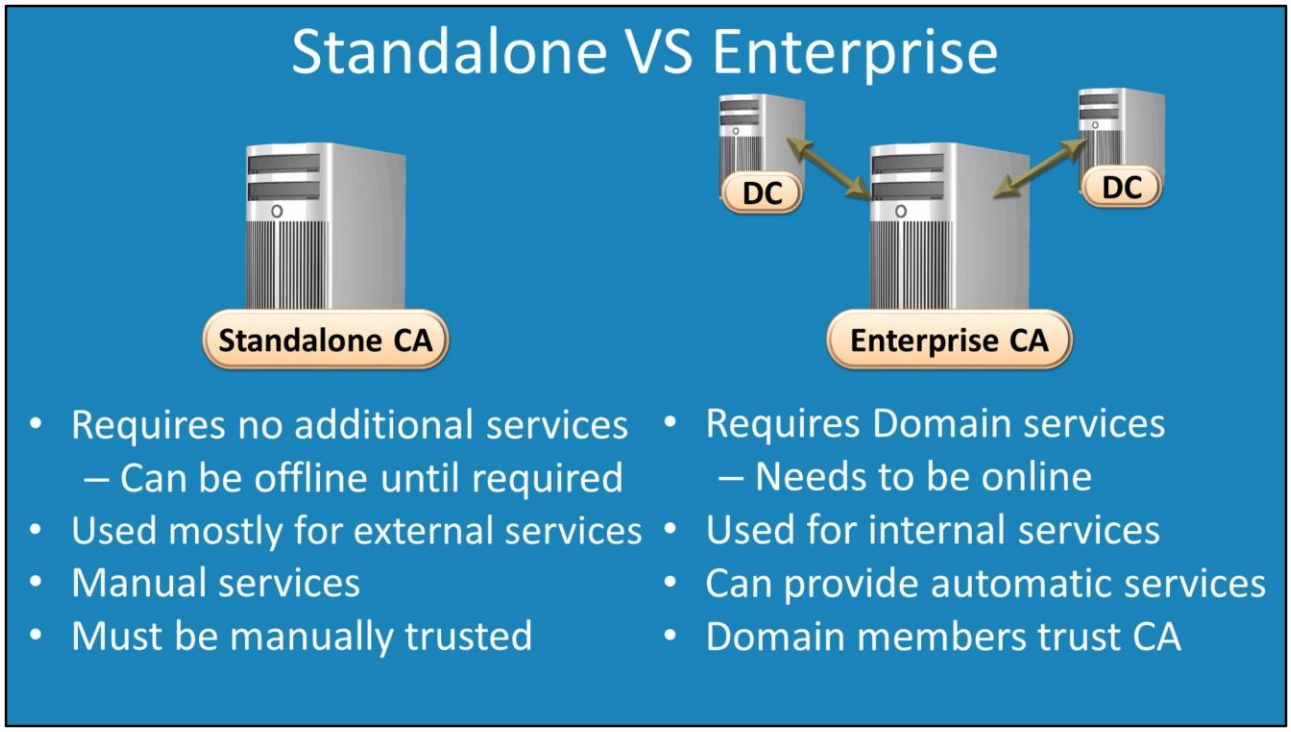


A standalone CA does not require any domain membership, however an enterprise CA does. Both have their advantages and disadvantages. This video will look at what features you get and lose which will help you decide which CA is the best choice for you.



Standalone vs Enterprise

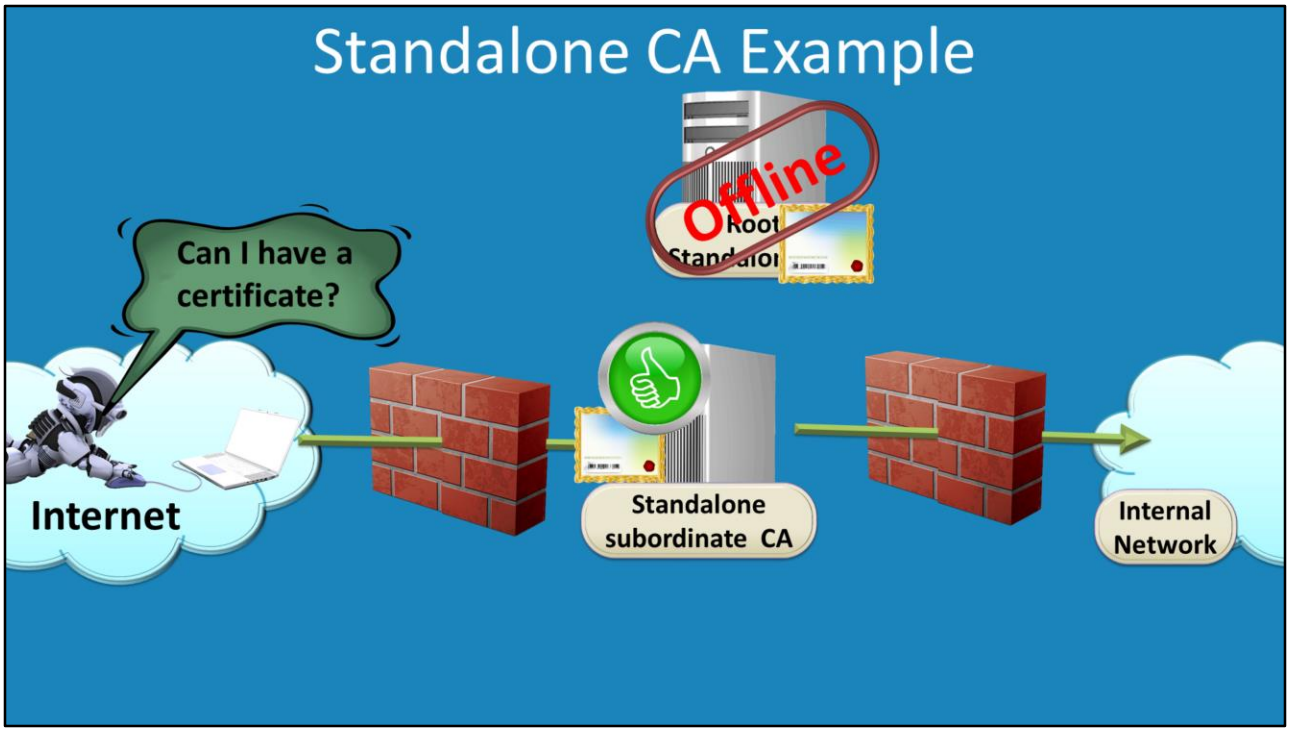
At the most basic level, the basic different between a standalone CA and an Enterprise CA is that an Enterprise CA needs to be a member of the domain while a standalone CA does not. If you decide to, you can install a standalone CA on a server that is a member of the domain. It should be remembered that once you install a Certificate Authority, properties for the server like the computer name cannot be changed. For this reason, if you only require a standalone CA, it may be a better choice to not have the server holding that standalone CA a member of the domain. Having the server a member of the domain also means that the server will need to check in with a domain controller once in a while. This essentially means that the server cannot be taken offline for extended periods. In some cases, a standalone CA may only be used to issue a couple of certificates, for example when it is used as a root CA. If this is the case, a non-domain member is a better choice as once the CA has issued these certificates it can stay offline for extended periods of time without issue. Having the CA offline means that the keys that are on the CA are protected from attack. If an attacker was to gain access to these keys, this means any certificates below this would need to be reissued. For this reason, being able to take the standalone CA offline for extended periods helps protect the key and the CA.

A Standalone CA is often used for external services. Since external services often require access from the internet, using a standalone CA means that CA's can be installed on perimeter or DMZ networks. Since no domain services are required, the

CA does not require a domain controller on the perimeter network or a rule to be created in the firewall in order to allow it access to the domain. This helps improve security, as if the CA was to become compromised, that attacker would only have access to what is on the CA and would not have access to any domain information. Enterprise CA's are often installed on internal networks as they require access to Domain Controllers.

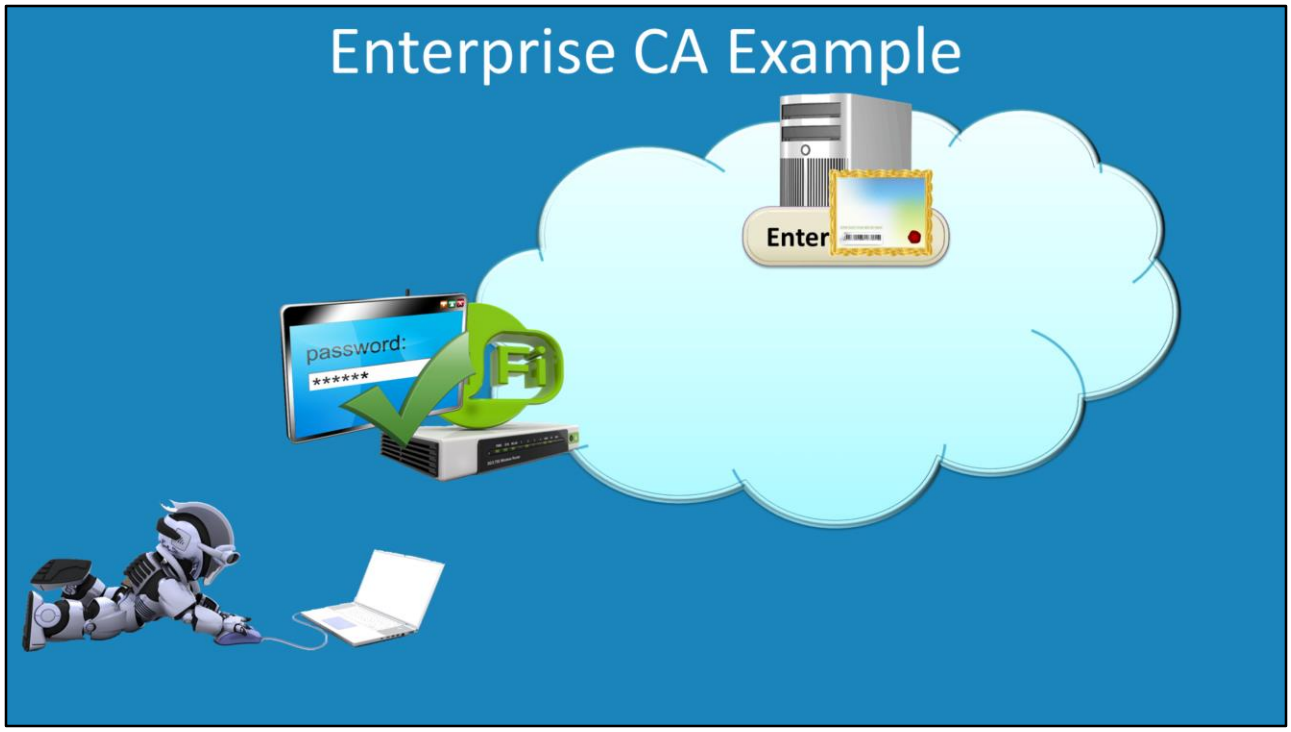
Even though Enterprise CA's essentially have to be online most of the time to access Domain Services and are domain members this makes them harder to secure and there is more opportunity for an attacker to do damage as they potentially have access to domain resources, but there are some advantages to having an enterprise CA. Since an Enterprise CA is a member of the domain, domain members can use automatic processes in order to obtain certificates. A standalone CA cannot use automatic processes and certificates allocated must be approved manually. This means that an Enterprise CA is a good choice if certificates need to be issued regularly. For example, health certificates that are issued daily to clients before they can access the network. Example of these include Wifi and Network Access Protection (NAP). A NAP client requires a health certificate before they can access the network and these certificates generally have a short life span. Certificates that are once issued and are valid for a few years a standalone CA may be good choice for this. Since on a standalone CA the certificate needs to be approved by an administrator having to manually approve certificates becomes time consuming if they are required to be approved on a regular basis. The exception to this is if there were a lot of certificates being issued. When this occurs, you may want to automate the process even though the certificates are valid for a long time. At the end of the day the decision is based on the amount of administrator time required versus how secure you want your network to be.

The last difference between a standalone CA and an Enterprise CA is the certificate issued can be automatically trusted by the client. In some cases, the certificate is automatically trusted by the client due to the trust relationship that is created when the client is added to the domain. In other cases, Group Policy can be used to set up the client to trust certificates issued by the CA. Either way, when a certificate is issued by a standalone CA, there is no automated system that assists to ensure the client automatically trusts that CA and thus can use the certificate. In order to use certificates from a standalone CA, often a certificate will need to be added to a local certificate store on the client using the certificate and then the client will trust certificates from that CA. Group Policy could also be used to install a standalone certificate on a client computer local certificate store. The point to remember is that there is some process required to get the standalone certificate on to the computer. The standalone certificate authority cannot take advantage of the trust relationship in the domain in order to setup and use certificates.



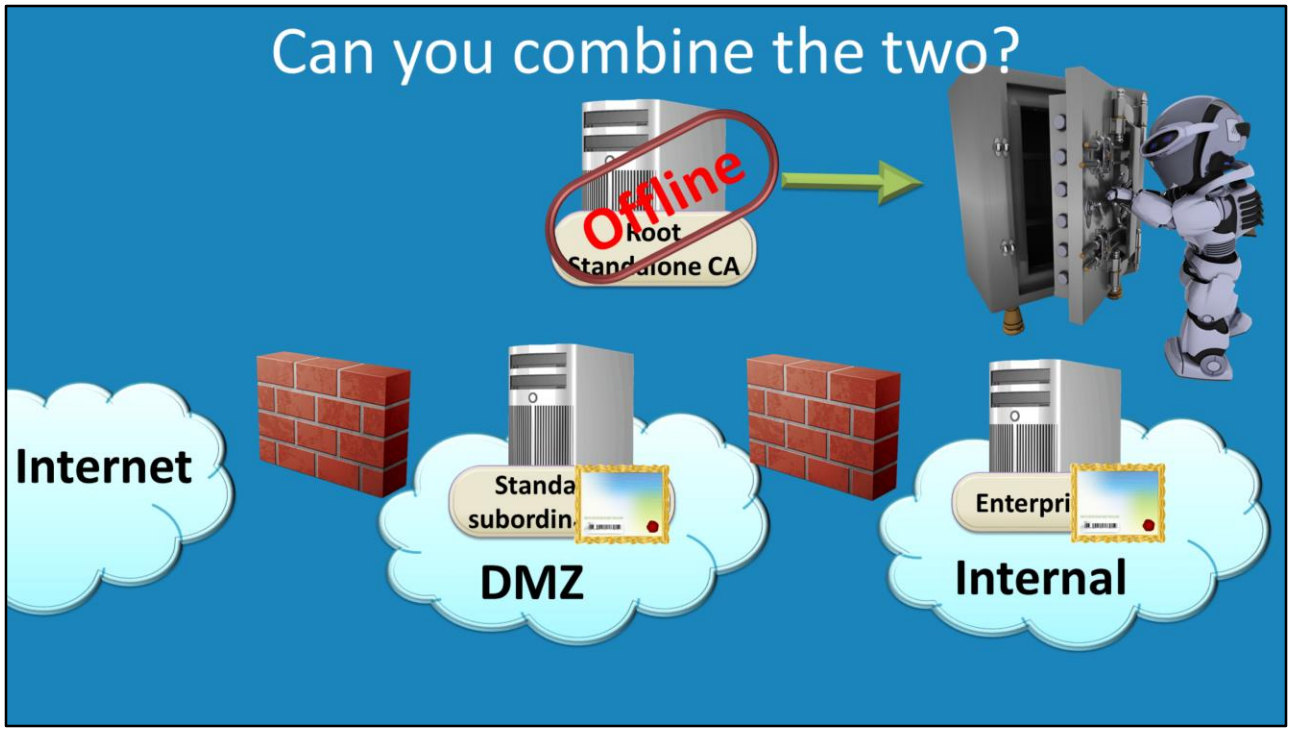
Standalone CA Example
In a lot of cases, a standalone CA will form the root of the certificate hierarchy. Even though you could also use an enterprise CA, the advantage is that the root CA can issue a certificate to subordinate CA's and then be taken offline. Since the root CA contains the private key to the whole certificate hierarchy, if this certificate was to be obtained by an attacker, this would compromise all certificates that have been issued in that hierarchy.

A typical deployment of certificates is to have subordinate CA's placed on a DMZ or perimeter network. This Standalone CA issues certificates directly to clients. Since it does not have the root certificate on it, it offers better security. The disadvantage is that all certificates that are issued need to be approved.



Enterprise CA Example

Often an Enterprise CA will be used when a lot of certificates need to issued and they need to be approved quickly. For example, when a domain user connects up to a wireless device to access the network, a certificate may be issued and used to provide secure communication for the client over the wireless connection. In this case you need to automatically approve the certificate because the user does not have time to wait for the administrator to approve the certificate and an administrator does not have time to manually approve a lot of certificates on a busy network.



Can you combined the two?
Standalone and enterprise CA's can be combined together in the hierarchy. The most common example of this is to use a standalone root CA at the top of the hierarchy. Since the CA is a standalone, after it has issued the certificate to the subordinate CA's it can be taken offline. It is possible for the root CA to be installed on removable media. If this is the case, some companies will place the removable media that the server was installed on into a secure area like a safe. Regardless which type of CA you install as the root CA, subordinate CA's can be standalone or enterprise or a mixture of the two. Often companies will install a standalone CA on the perimeter network and an enterprise CA on the internal network so they get the most features and best security.

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 780-782