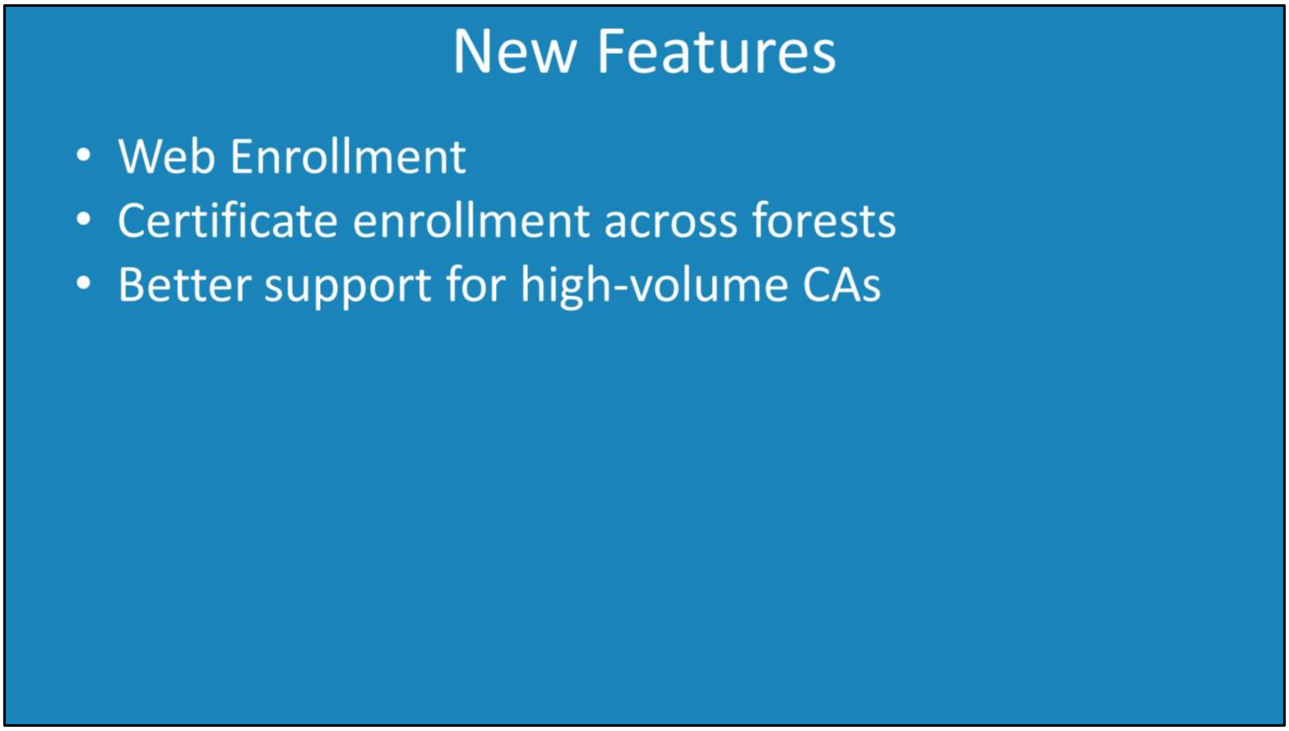
# What's new in certificate services in Windows Server 2008 R2

For the free video please see
http://itfreetraining.com/certificates#new-2008

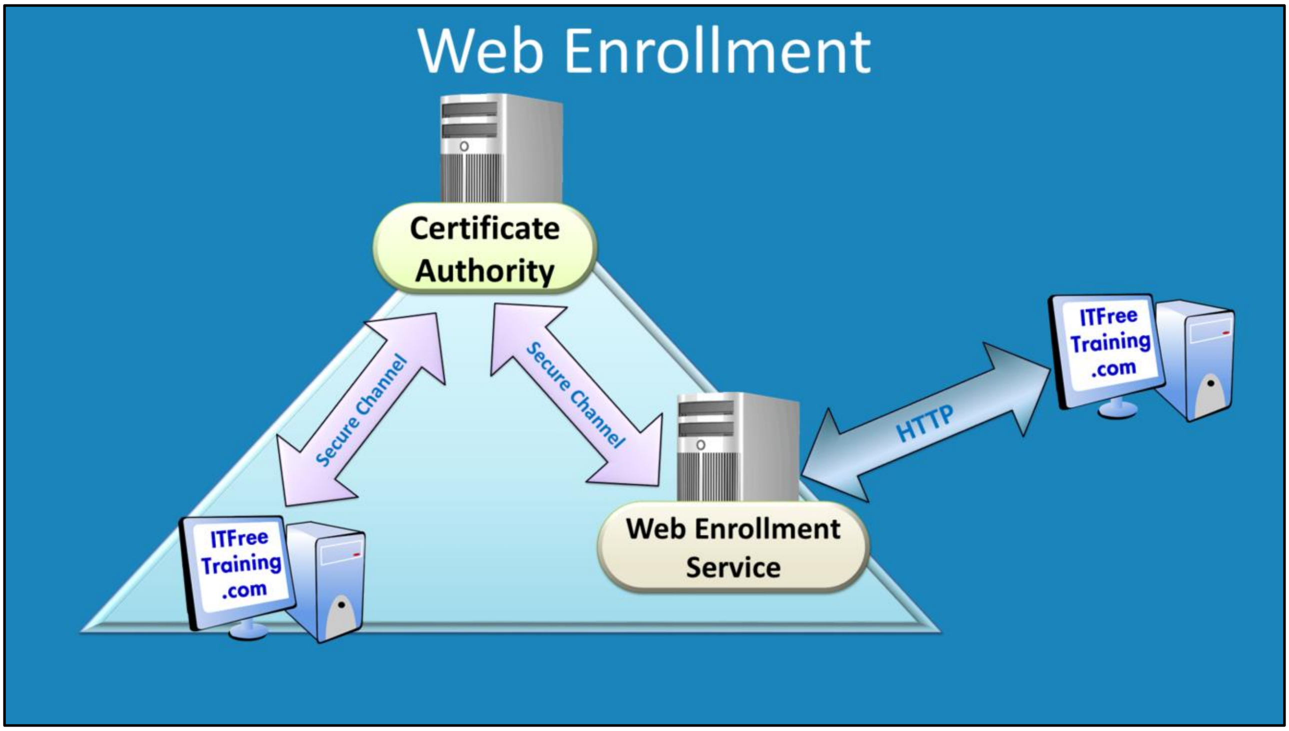
This video will look at the 3 new features that are included in Windows Server 2008 R2 Active Directory Certificate Services.



## New Features

- Web Enrollment
- Certificate enrollment across forests
- Better support for high-volume CAs

**New Features**
The new features added are Web Enrollment, certificates enrollment across forests and better support for high-volume CA’s.



Web Enrollment

Certificate Authority

Secure Channel

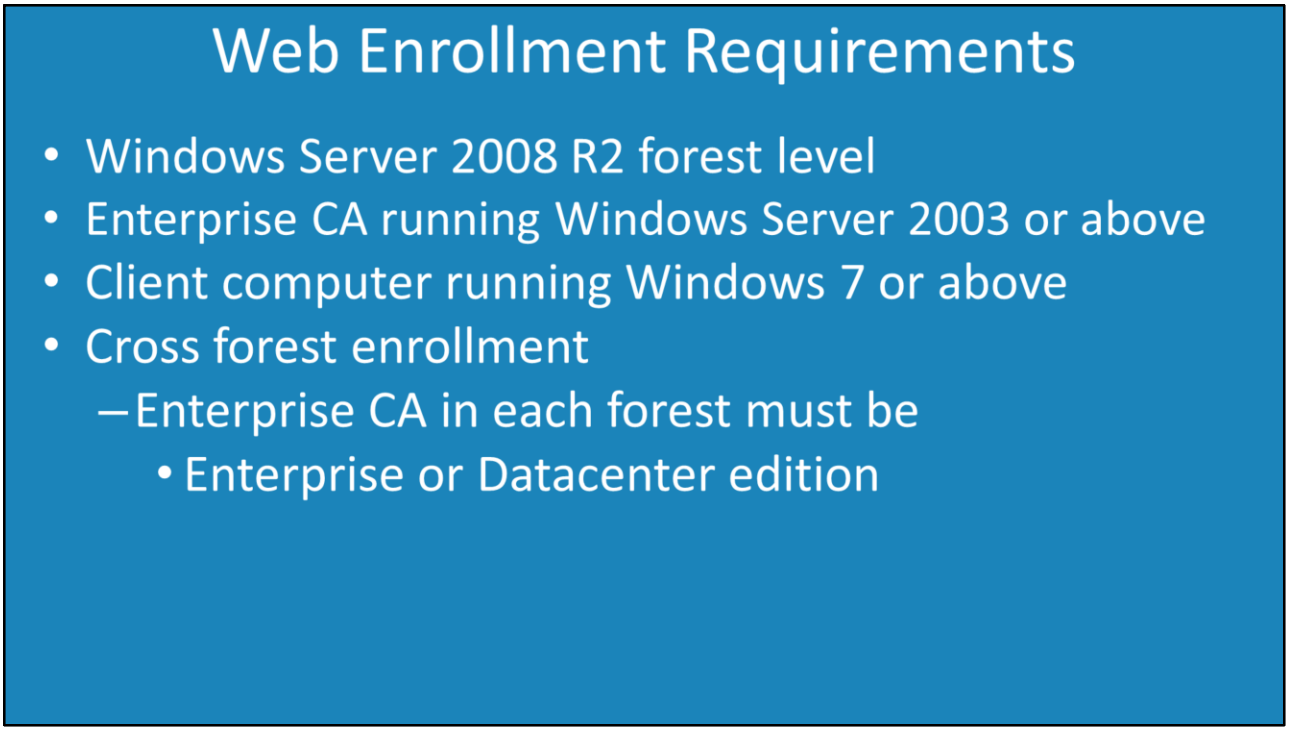
Secure Channel

Web Enrollment Service

HTTP

**Web Enrollment**

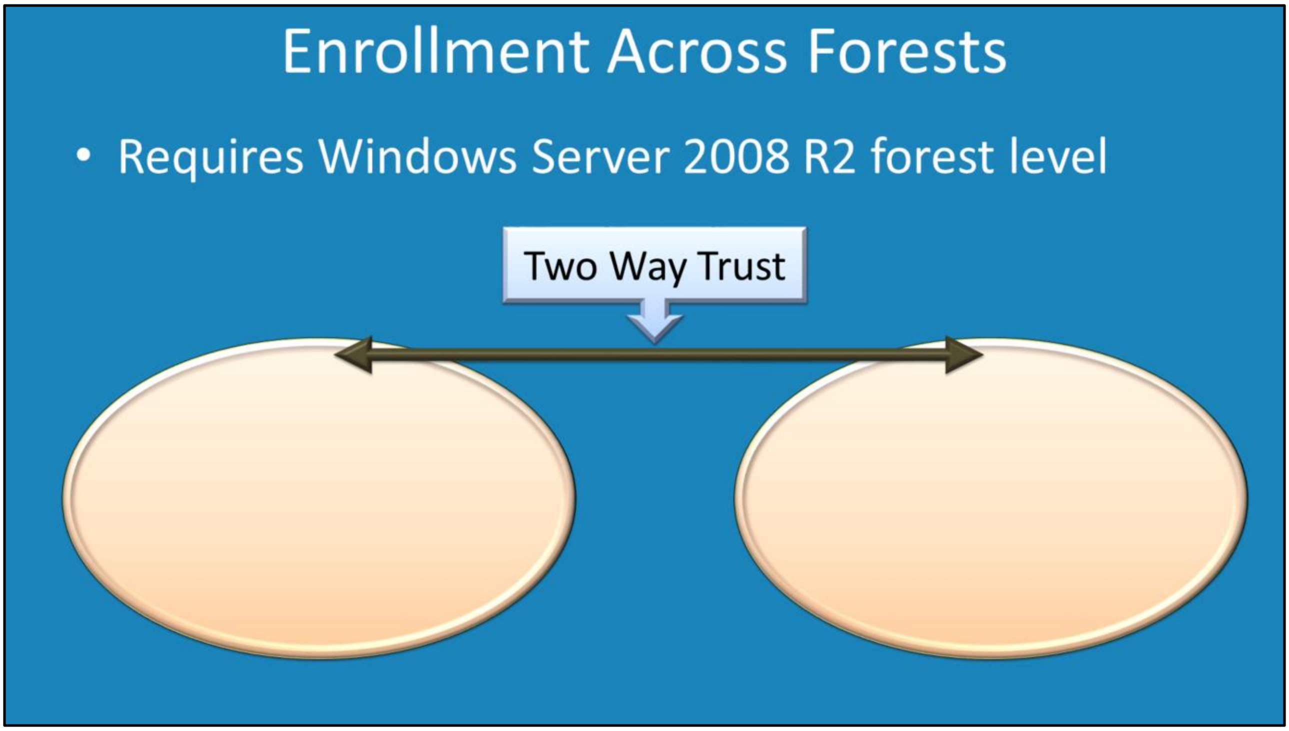
A certificate authority (CA) creates certificates that are used by clients on the network. In a domain, a certificate authority can make use of the trust relationship created when a computer is added to the domain. This is referred to as a secure channel and allows a certificate to be transferred to the client securely. If you have a need to issue certificates to computers that are not part of the domain, for example to an external company, this cannot be done using a secure channel since the computer is not part of the domain. To get around this problem, the component Web Enrollment Services can be added to a Windows Server. This component allows external clients to request certificates using the HTTP protocol. These certificates, once approved for issue, can be transferred to the Windows Server using the secure channel to the certificate authority. This helps protect the certificate authority as external clients do not need to access it directly in order to obtain certificates.



## Web Enrollment Requirements

- Windows Server 2008 R2 forest level
- Enterprise CA running Windows Server 2003 or above
- Client computer running Windows 7 or above
- Cross forest enrollment
  - Enterprise CA in each forest must be
    - Enterprise or Datacenter edition

**Web Enrollment Requirements**
In order to use web enrollment you must meet the following requirements.
1) Windows Server 2008 R2 forest level
2) Enterprise CA running Windows Server 2003 or above
3) Client computer running Windows 7 or above
4) Cross forest enrollment requires the CA’s in each forest to be Enterprise or Datacenter editions



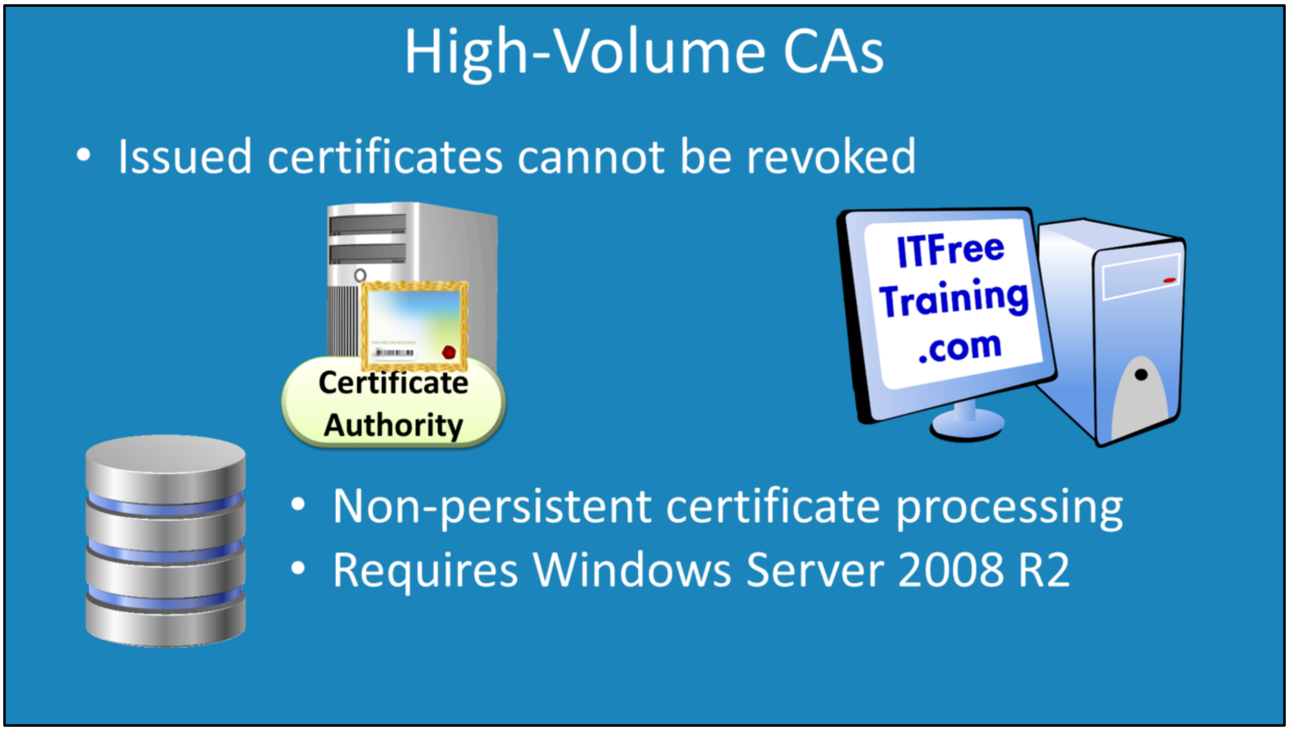
# Enrollment Across Forests

- Requires Windows Server 2008 R2 forest level

Two Way Trust

**Enrollment across Forests**

This feature allows clients in one forest to obtain certificates from a CA in another forest. This makes the certificate infrastructure a lot simpler as the two forests only require one certificate infrastructure. In order to use enrollment across forests, the two forests require a forest trust. A forest trust is supported by Windows Sever 2003 function level, however enrollment requires Windows Server 2008 R2 forest level. For this reason, you require a forest trust and the forests to be Windows Server 2008 R2 forest level.



# High-Volume CAs

- Issued certificates cannot be revoked
- Non-persistent certificate processing
- Requires Windows Server 2008 R2

Certificate Authority
ITFree Training .com

**High-Volume CAs**

This is a setting found only on Windows Server 2008 R2 certificate Authorities (CA). This setting is called non-persistent certificate processing. When enabled, this setting stops a copy of a certificate being saved to the local certificate database. This improves performance of the certificate authority; however, it does mean that once a certificate is issued it cannot be revoked. Revoking a certificate effectively means canceling the certificate so that it cannot be used. If a CA issues a lot of certificates that are only used for a short period of time, for example Network Access Protection (NAP), this is a good choice for this option. This is because without the revoke option, a client keeps using a certificate until it expires. In the case of NAP, these certificates often have short validity times and thus will expire quickly and thus serve less of a security risk.

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 788-790
“What's New in Active Directory Certificate Services”
http://technet.microsoft.com/en-us/library/dd448537(v=ws.10).aspx