

Re: Cert Server – Changed Enterprise CA

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2006-06/msg00088.html

- *From:* "Scott Townsend" <scooter@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 6 Jun 2006 17:03:42 -0700
-

So as per the Instructions I added an IPSec Cert Template and added that to the Default Group Policy. That worked fine. I rebooted and not my machine has an IPSec Cert from the new CA.

Though the Computer Certificate was already in the Default GPO and I did properties on it and went through all the pages and it didn't ask to reassociate it with the new CA. Would I want to Delete it and readd the Computer Template?

Thanks,

Scott<-

"Vincent Xu [MSFT]" <v-xuwen@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:pgOjN9ghGHA.2260@xxxxxxxxxxxxxxxxxxxxxxxx

Hi,

To manually request a Cert, you can refer to following article:

323342 How to install a certificate for use with IP Security in Windows Server 2003

<http://support.microsoft.com/default.aspx?scid=kb;EN-US:323342>

To automatically get a Cert by GP, you can refer to following steps:

Before you create an automatic certificate request, you must know the following:

1. The type of certificate you want computers to enroll for automatically.
2. The certification authority (CA) that will issue the certificate.

Install a Certificate Template

Use the following steps to install a certificate template, and note that these steps must be performed on an enterprise CA in the Active Directory domain:

1. Click Start , point to Programs , point to Administrative Tools , and then click Certificate Authority .
2. In the Certification Authority console, expand your domain name, right-click the Policy Settings node in the left pane, point to New , and then click Certificate to Issue .

Re: Cert Server – Changed Enterprise CA

3. In the Select Certificate Template dialog box, click the certificate template you require. In this example, click the IPSEC certificate , and then click OK .
4. Quit the Certification Authority console.

Configure the Automatic Certificate Request Policy

- Use the following steps to configure an automatic certificate request policy that allows automatic enrollment for domain computers:
1. Click Start , point to Programs , point to Administrative Tools , and then click Active Directory Users and Computers .
 2. In the Active Directory Users and Computers console, right–click your domain name, and then click Properties .
 3. Click the Group Policy tab, click a domain group policy object, and then click Edit .
 4. In the Group Policy console, expand the Computer Configuration node, expand the Windows Settings node, expand the Security Settings node, and then expand the Public Key Policies node.
 5. Right–click the Automatic Certificate Request Settings node, point to New , and then click Automatic Certificate Request .
 6. When the Automatic CertificateRequest Setup Wizard starts, click Next .
 7. On the Certificate Template page, click the template you require. In this example, click the IPSEC template, and then click Next .
 8. On the Certificate Authority page, select the enterprise CA for your domain by placing a checkmark in the check box to the left of the CA. Click Next .
 9. On the Completing the Automatic Certificate Request Setup page, click Finish . The new certificate is automatically requested the next time the user logs on or the next time the domain Group Policy is refreshed. The certificate will be installed on new computers when they join the domain.

Hope this helps.

Best regards,

Vincent Xu
Microsoft Online Partner Support

=====
Get Secure! – www.microsoft.com/security
=====

When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from this issue.

=====
This posting is provided "AS IS" with no warranties, and confers no rights.
=====

Re: Cert Server – Changed Enterprise CA

From: "Scott Townsend" <scooter@xxxxxxxxxxxxxxxxxxxx>
References:
<u0qmgrBhGHA.1520@xxxxxxxxxxxxxxxxxxxxxxxx>

<WOcuY4FhGHA.5608@xxxxxxxxxxxxxxxxxxxxxxxx>

Subject: Re: Cert Server – Changed Enterprise CA
Date: Thu, 1 Jun 2006 10:05:44 -0700
Lines: 79
X-Priority: 3
X-MSMail-Priority: Normal
X-Newsreader: Microsoft Outlook Express 6.00.2900.2869
X-RFC2646: Format=Flowed; Original
X-MimeOLE: Produced By Microsoft MimeOLE
V6.00.2900.2869
Message-ID:
<eHN8f2ZhGHA.3572@xxxxxxxxxxxxxxxxxxxxxxxx>
Newsgroups: microsoft.public.win2000.active_directory
NNTP-Posting-Host: 204-145-245-49.enm.com
204.145.245.49
Path:
TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP04.phx.gbl
Xref: TK2MSFTNGXA01.phx.gbl

microsoft.public.win2000.active_directory:114076

X-Tomcat-NG: microsoft.public.win2000.active_directory

How do I have them do that?

Can I put it in the Login Script for the Domain?

Thank you,
"Vincent Xu [MSFT]"
<v-xuwen@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:WOcuY4FhGHA.5608@xxxxxxxxxxxxxxxxxxxxxxxx

Hi Scott,

Of course you need to have the PCs/Servers
request a new Cert from the
new
CA

Thanks.

Best regards,

Vincent Xu

Re: Cert Server – Changed Enterprise CA

Microsoft Online Partner Support

Get Secure! – www.microsoft.com/security

When responding to posts, please "Reply to Group" via your newsreader

so

that others

may learn and benefit from this issue.

This posting is provided "AS IS" with no warranties, and confers no

rights.

From:
"Scott
Townsend"
<scooter@xxxxxxxxxxxxxxxxxxxx>
Subject:
Cert Server
– Changed
Enterprise
CA
Date: Tue,
30 May
2006
11:57:18
–0700
Lines: 19
X–Priority:
3
X–MSMail–Priority:
Normal
X–Newsreader:
Microsoft
Outlook
Express
6.00.2900.2869
X–RFC2646:
Format=Flowed;
Original
X–MimeOLE:

Re: Cert Server – Changed Enterprise CA

Produced
By
Microsoft
MimeOLE
V6.00.2900.2869
Message-ID:
<u0qmgrBhGHA.1520@xxxxxxxxxxxxxxxxxxxxxxxx>
Newsgroups:
microsoft.public.win2000.active_directory
NNTP-Posting-Host:
204-145-245-49.enm.com
204.145.245.49
Path:
TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTN
Xref:
TK2MSFTNGXA01.phx.gbl

microsoft.public.win2000.active_directory:114022

X-Tomcat-NG:
microsoft.public.win2000.active_directory

We had
some issues
with one of
our DCs
and with
MS
Support's
Advice we

had

to demote
it, which
involved
removing
the
Enterprise
Root CA
that was

on

it.

I installed a
new
Enterprise
Root CA on
a new DC,

Re: Cert Server – Changed Enterprise CA

though not
sure that

AD

is

happy.

I originally
installed the
CA to be
used with
our Cisco
PIX and
VPN
connections,
though later
found out
that you
could not
use an

Enterprise

Root and
needed a
Standalone
Root. I just
left the
Enterprise
Root

there.

I

didn't think
it was really
used for
anything.
Though
now I think
it

might

have been.

The old cert
server had

Re: Cert Server – Changed Enterprise CA

Re: Cert Server – Changed Enterprise CA

Certs issued
to each of
the
PCs/Servers
in the
domain.
How do I
get the new
Cert Server
to issue new
certs to the
PCs/Servers
or have the
PCs/Servers
request a
new Cert
from the
new

CA?

Thanks,
Scott<-