Secunia
Stay Secure

BCD SINTRAG
Ein Unternehmen der ADN® Gruppe
value add distribution

MEMBER OF EVENT
CONFIGMGR.CH

Armoring your mobile workforce warriors for the 21st century

with System Center Configuration Manager 2012 R2

--- Advanced Warfare ---

Tim De Keukelaere
Kenny Buntinx

#CMCE_CH

Feb 9th 2015

About Kenny

MVP
Microsoft®
Most Valuable
Professional

meet the
experts

meet Microsoft
Extended Experts Team

WWW.SCUG.BE
BELGIAN COMMUNITY POWER

@KennyBuntinx

http://be.linkedin.com/KennyBuntinx

http://scug.be/blogs/sccm

Kenny Buntinx

Managing Consultant

Kenny.Buntinx@kbsolutions.be

About Tim

MVP Microsoft® Most Valuable Professional

meet the experts

meet Microsoft Extended Experts Team

WWW.SCUG.BE ★ BELGIAN COMMUNITY POWER ★

@Tim_DK

http://be.linkedin.com/in/timdekeukelaere/

http://scug.be/tim/

Tim De Keukelaere

Managing Consultant

Tim.De.Keukelaere@IT-Essence.be

Key Takeaways

Understanding

- These concepts:
  - Extending Settings Management (OMA-DM)
  - Deploying Certificate Profiles
  - Company Resource Access

Knowing

- How to implement them

Assumptions

About our audience

- Practical experience with System Center Configuration Manager 2012 SP1/R2
- Knowledge of Windows Intune and Device Enrollment

About us

- Not aiming to explain in detail
  - "How certificates work"
  - "All possible UDM capabilities"

INTRODUCTION

UDM Management Capabilities

- Over the air enrollment
- Retire and wipe devices
- **Configure compliance settings on devices**
  - **Extending Settings Management thru OMA-DM.**
- **Deploy NDES thru SCEP (Simple Certificate enrollment Protocol) in your environment to**
  - **To be able to deploy certificate Profiles on your devices**
  - **To be able to deploy VPN & WIFI Profiles.**
- Deploy line of business apps to device
- Deploy apps from the store that the device connects to
- Collect inventory
  - Hardware
  - Software

Is your ConfigMgr Environment ready for UDM?

- Cumulative Update 3
  - https://support.microsoft.com/kb/2994331
- Additional Hotfixes:
  - http://support.microsoft.com/kb/2990658
  - http://support.microsoft.com/kb/3002291

EXTENDING SETTINGS MANAGEMENT THROUGH OMA-DM

OMA-DM

- Specification designed for management of mobile devices
  - Mobile Phones
  - PDA's
  - Tablets

- Supporting following use case scenarios
  - **Provisioning** – Configuration of the device (including first time use), enabling and disabling features
  - **Device Configuration** – Allow changes to settings and parameters of the device
  - **Software Upgrades** – Provide for new software and/or bug fixes to be loaded on the device, including applications and system software
  - **Fault Management** – Report errors from the device, query about status of device

- OMA-DM for WP8.1:
  - http://technet.microsoft.com/en-us/library/dn499787.aspx

Windows Phone 8.1 MDM Protocol.pdf

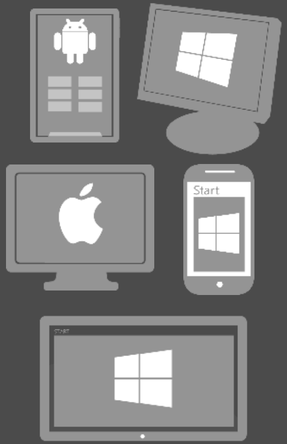
DEMO

Extending Settings Management

Business Scenario

- At a customer during a Windows Intune UDM Proof of concept :
  - Customer was ordering 1000 corporate owned (COPE) Nokia Lumia 630 Windows Phones
  - He wanted us to provide the option when a '**device owner**' in CM12 R2 is set to "**corporate**" , a user **can't unenroll** a "corporate" device.
  - Unless you are the ConfigMgr 2012 MDM admin , you can't.
- Read the full story here :
  - http://scug.be/sccm/2014/04/24/configmgr-2012-r2-windows-intune-udm-how-to-prevent-an-end-user-can-un-enroll-his-corporate-windows-phone-8-1/

Remember ! Personal vs Corporate !



Personal
vs.
Corporate Owned
Devices

App Management

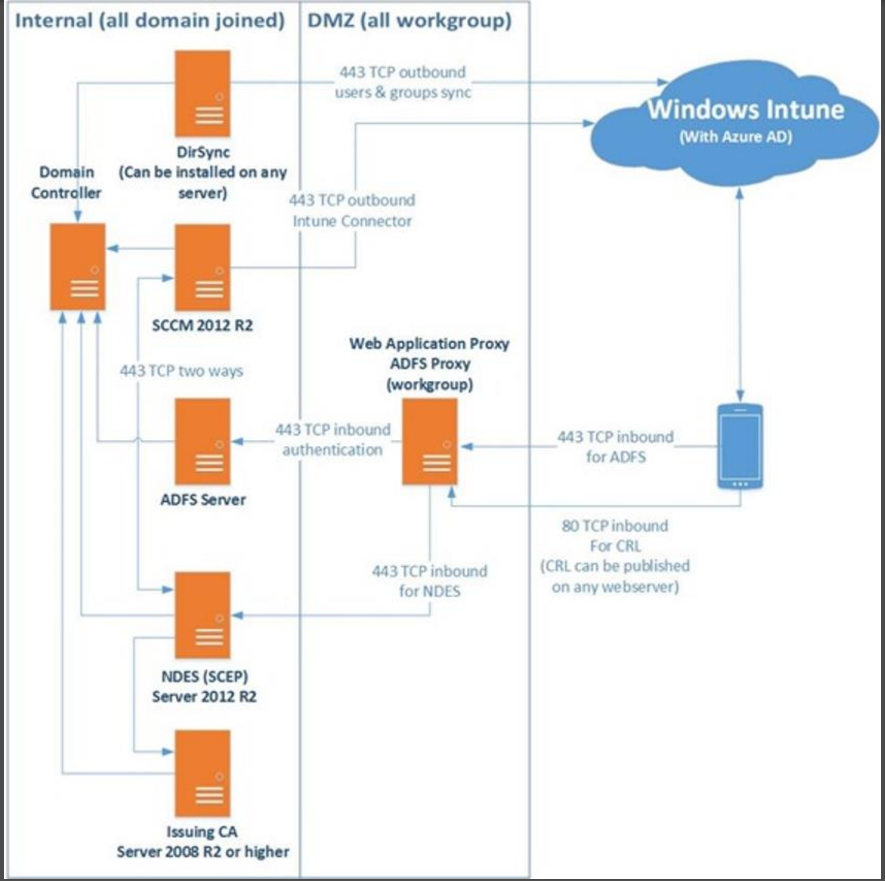
- By default, user-enrolled devices are “Personal”
- Admin can specify corporate-owned devices !

Solution Outline

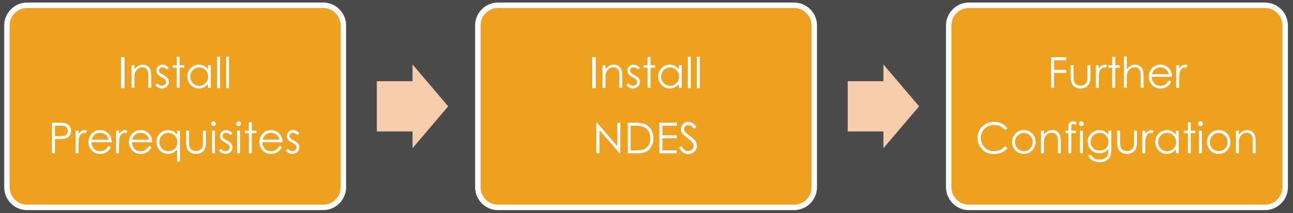
- Create configuration item "Deny WP8.1 MDM UnEnrollment'
- Select the checkbox : 'Configure additional settings that are not in the default settings groups'
- Hit the "Create Setting" tab.
  - Give it a Name
  - 1. Settings Type : OMA-URI
  - 2. Data Type : Integer
  - 3. OMA-URI : ./Vendor/MSFT/PolicyManager/My/Experience/AllowManualMDMUnenrollment
- Highlight your recently created 'Deny MDM Unenrollment' and hit the 'Select' button
  - 1. Rule Type : Value
  - 2. Data Type : 0 (0 = un-enroll not allowed / 1 = enroll allowed)
  - 3. Set 'Remediate noncompliant rules when supported'
  - 4. Set Noncompliance severity for reports to 'Warning'
- Create the baseline
- Create the collection
- Deploy the baseline
- Wait 5 minutes

NDES

ARMORING YOUR MOBILE WORKFORCE WARRIORS FOR THE 21ST CENTURY



Step by step



Install Prerequisites

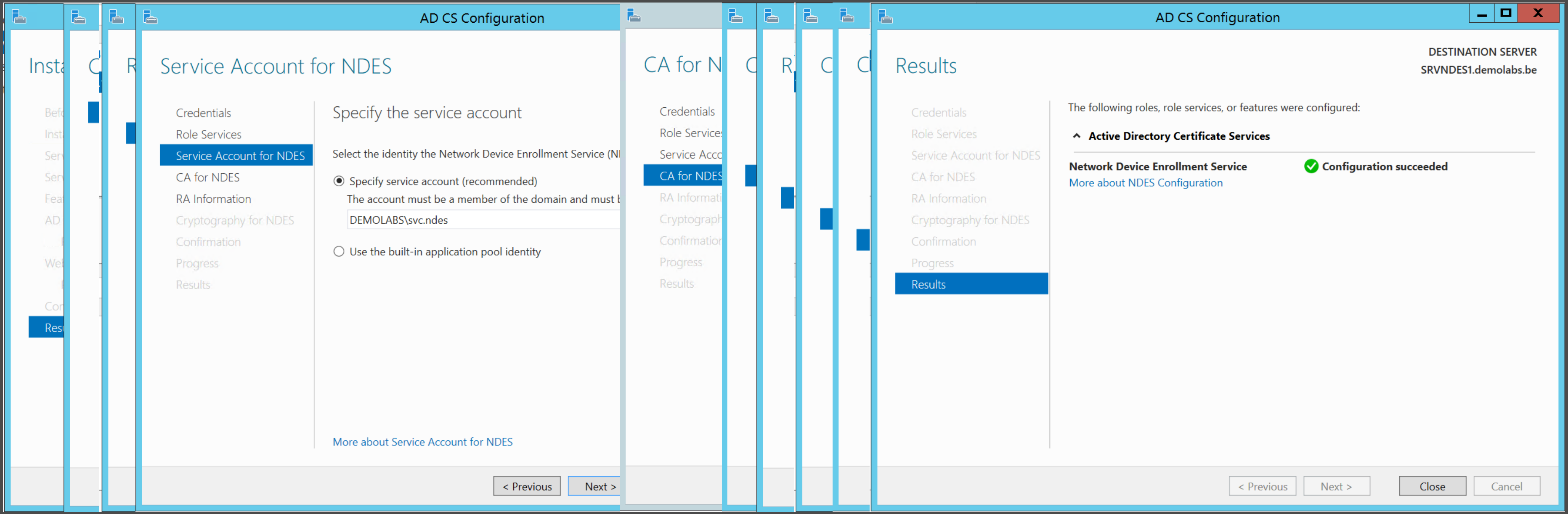
Install NDES

Further Configuration

Prerequisites

- Root & Intermediate CA
  - Intermediate: Windows Server 2012 R2 (for NDES)
- ADFS / WAP
  - KB3013769
    - Profile Installation Failed on iOS (workplace join)
    - Large URI request in Web Application Proxy fails in Windows Server 2012 R2 (NDES)
- CA (2008 R2)
  - KB2483564
- Details: http://scug.be/sccm/2014/12/29/hybrid-scenarios-with-system-center-configuration-manager-2012-r2-windows-intune-adfs-wap-ndes-workplace-join-hotfixes-you-really-need-in-your-environment/

Configuring NDES



AD CS Configuration

Service Account for NDES

Specify the service account

Select the identity the Network Device Enrollment Service (NI

● Specify service account (recommended)

The account must be a member of the domain and must l

DEMOLABS\svc.ndes

○ Use the built-in application pool identity

More about Service Account for NDES

AD CS Configuration

Results

DESTINATION SERVER
SRVNDES1.demolabs.be

The following roles, role services, or features were configured:

Active Directory Certificate Services

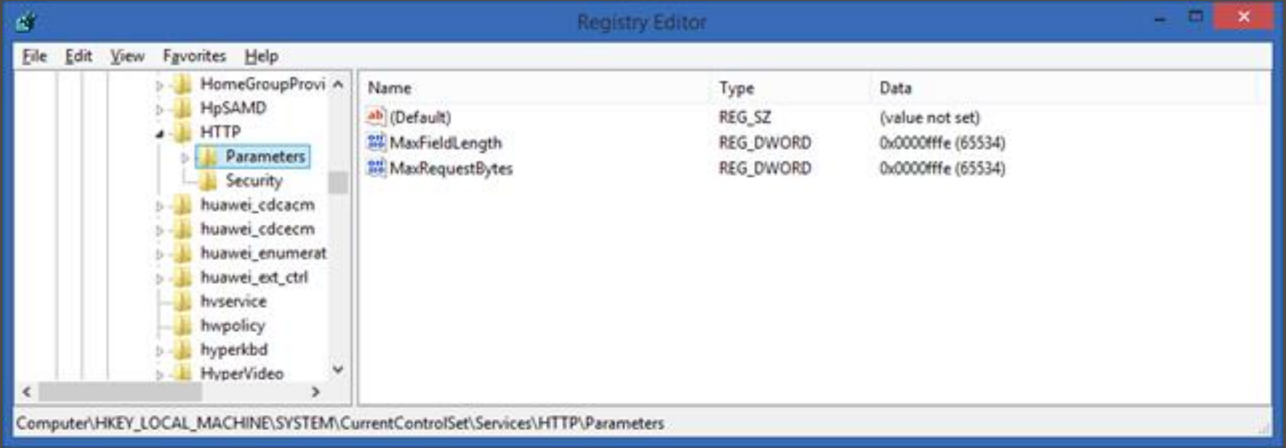
Network Device Enrollment Service ✓ **Configuration succeeded**

More about NDES Configuration

Further Configuration

- On the NDES and WAP server

- The NDES server will receive very long URL's (queries) and therefore a few changes are needed. Open the registry editor and add two entries:

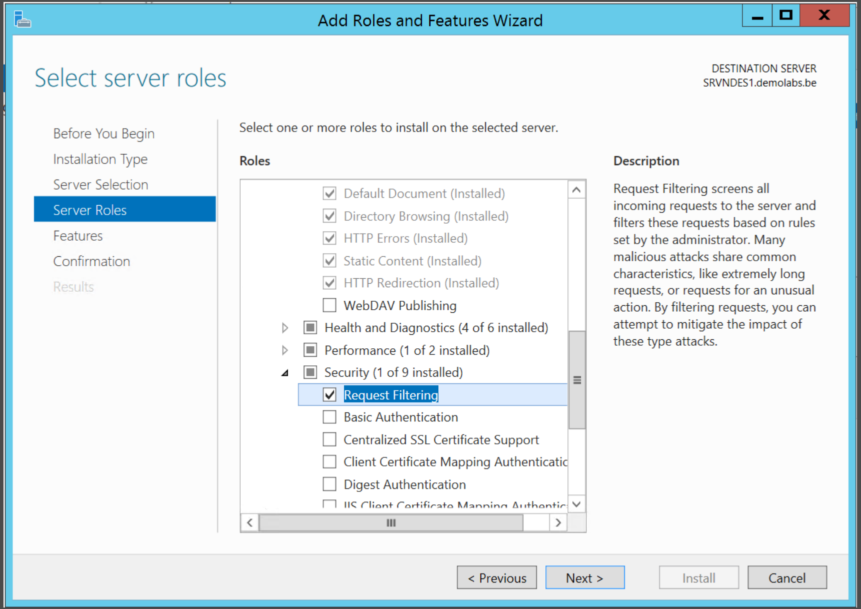


Name	Type	Data
(Default)	REG_SZ	(value not set)
MaxFieldLength	REG_DWORD	0x0000fffe (65534)
MaxRequestBytes	REG_DWORD	0x0000fffe (65534)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters

Further Configuration (2)

- On the NDES server
- Add Request Filtering role



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
SRVNDES1.demolabs.be

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

Roles

- ☑ Default Document (Installed)
- ☑ Directory Browsing (Installed)
- ☑ HTTP Errors (Installed)
- ☑ Static Content (Installed)
- ☑ HTTP Redirection (Installed)
- □ WebDAV Publishing
- ▪ Health and Diagnostics (4 of 6 installed)
- ▪ Performance (1 of 2 installed)
- ▪ Security (1 of 9 installed)
  - ☑ Request Filtering
  - □ Basic Authentication
  - □ Centralized SSL Certificate Support
  - □ Client Certificate Mapping Authenticatic
  - □ Digest Authentication
  - □ IIS Client Certificate Mapping Authentic

Description

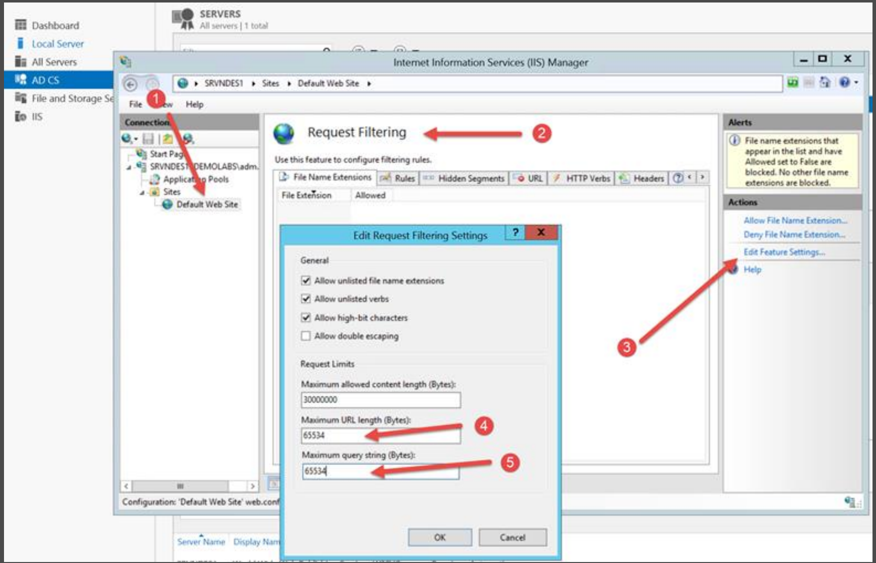
Request Filtering screens all incoming requests to the server and filters these requests based on rules set by the administrator. Many malicious attacks share common characteristics, like extremely long requests, or requests for an unusual action. By filtering requests, you can attempt to mitigate the impact of these type attacks.

Further Configuration (3)

- On the NDES server

- Change the Maximum URL length and Maximum query string to 65534 on the Request Filtering tab of the default website.

- Reboot the server.
  (restarting IIS is not sufficient!)



Internet Information Services (IIS) Manager

SRVNDES1 ▸ Sites ▸ Default Web Site ▸

Request Filtering

Use this feature to configure filtering rules.

Alerts: File name extensions that appear in the list and have Allowed set to False are blocked. No other file name extensions are blocked.

Edit Request Filtering Settings

General

☑ Allow unlisted file name extensions

☑ Allow unlisted verbs

☑ Allow high-bit characters

☐ Allow double escaping

Request Limits

Maximum allowed content length (Bytes): 30000000

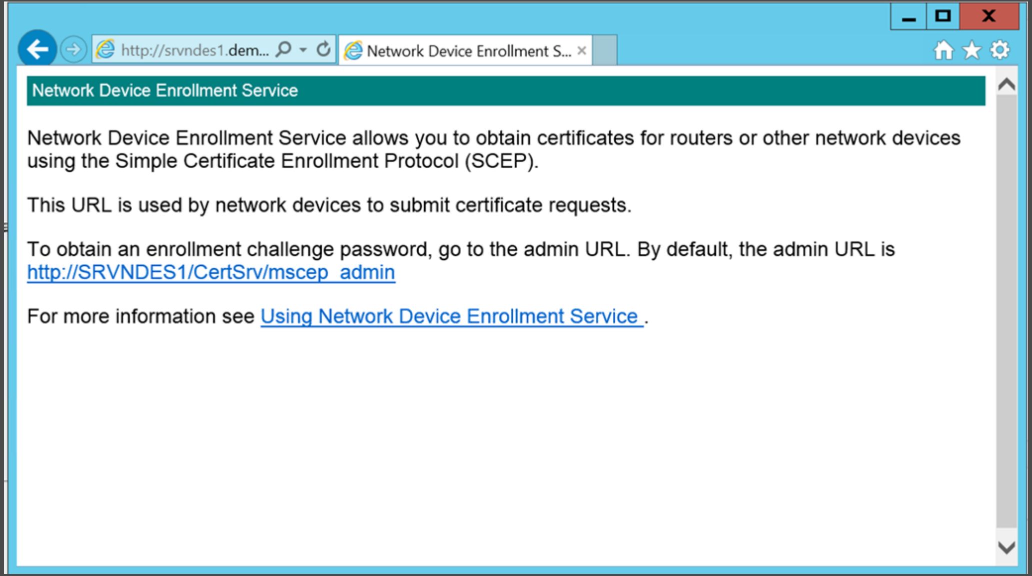
Maximum URL length (Bytes): 65534

Maximum query string (Bytes): 65534

Configuration: 'Default Web Site' web.conf

Time to test!

- http://FQDN/certsrv/mscep/mscep.dll



Network Device Enrollment Service

Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).

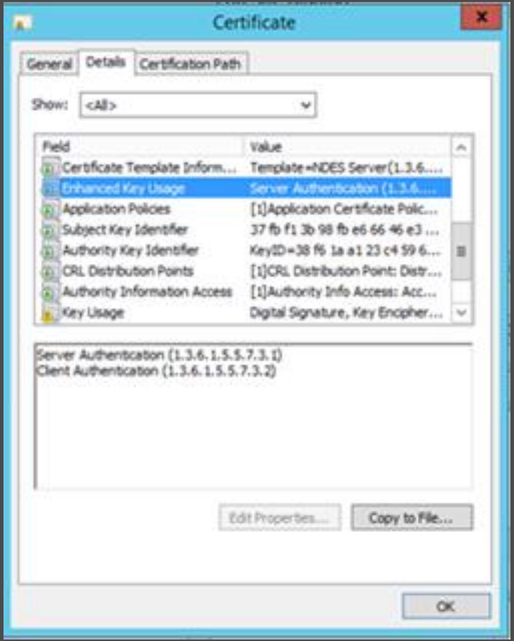
This URL is used by network devices to submit certificate requests.

To obtain an enrollment challenge password, go to the admin URL. By default, the admin URL is http://SRVNDES1/CertSrv/mscep_admin

For more information see Using Network Device Enrollment Service .

So far so good …

- Traffic between the NDES server and the CM12 CRP needs to be encrypted using SSL.
- The NDES server needs a certificate with Client Authentication Enhanced Key Usages (EKU's)
- A certificate using with a Server authentication EKU that it will use as it's SSL certificate for the IIS web server
- Test Again : https://FQDN/certsrv/mscep/mscep.dll



Field	Value
Certificate Template Inform...	Template=NDES Server(1.3.6....
Enhanced Key Usage	Server Authentication (1.3.6....
Application Policies	[1]Application Certificate Polic...
Subject Key Identifier	37 fb f1 3b 98 fb e6 66 46 e3 ...
Authority Key Identifier	KeyID=38 f6 1a a1 23 c4 59 6...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature, Key Encipher...

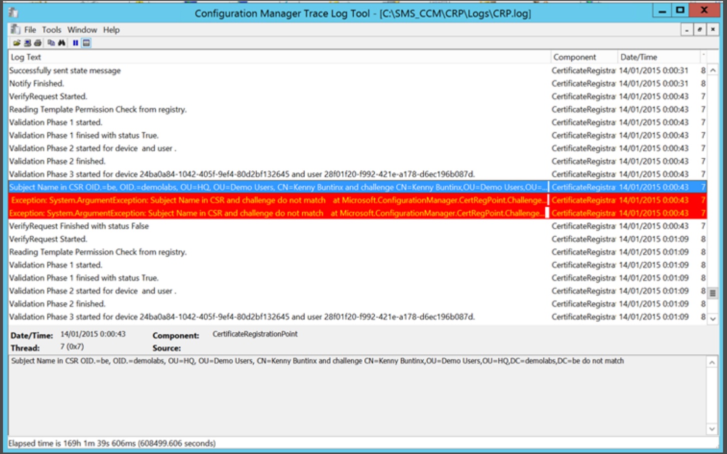
```
Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)
```

And some more configuration ...

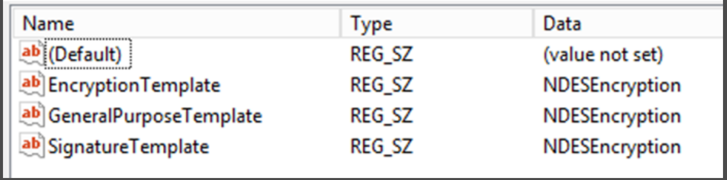
- EncryptionTemplate : Key Usage of Encryption selected on cert template

- GeneralPurposeTemplate : Key Usage of Signature and Encryption selected on cert template

- SignatureTemplate : Key Usage of Signature selected on cert template

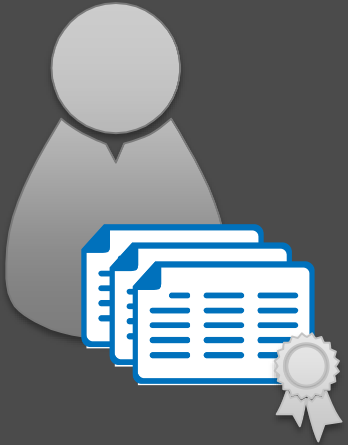

Configuration Manager Trace Log Tool - [C:\SMS_CCM\CRP\Logs\CRP.log]
File
Tools
Window
Help

```
Log Text                                                                                                     Component            Date/Time
Successfully sent state message                                                                              CertificateRegistra  14/01/2015 0:00:31  8
Notify Finished.                                                                                             CertificateRegistra  14/01/2015 0:00:31  8
VerifyRequest Started.                                                                                       CertificateRegistra  14/01/2015 0:00:43  7
Reading Template Permission Check from registry.                                                             CertificateRegistra  14/01/2015 0:00:43  7
Validation Phase 1 started.                                                                                  CertificateRegistra  14/01/2015 0:00:43  7
Validation Phase 1 finised with status True.                                                                 CertificateRegistra  14/01/2015 0:00:43  7
Validation Phase 2 started for device  and user .                                                            CertificateRegistra  14/01/2015 0:00:43  7
Validation Phase 2 finished.                                                                                 CertificateRegistra  14/01/2015 0:00:43  7
Validation Phase 3 started for device 24ba0a84-1042-405f-9ef4-80d2bf132645 and user 28f01f20-f992-421e-a178-d6ec196b087d.   CertificateRegistra  14/01/2015 0:00:43  7
Subject Name in CSR OID.=be, OID.=demolabs, OU=HQ, OU=Demo Users, CN=Kenny Buntinx and challenge CN=Kenny Buntinx,OU=Demo Users,OU=...   CertificateRegistra  14/01/2015 0:00:43  7
Exception: System.ArgumentException: Subject Name in CSR and challenge do not match    at Microsoft.ConfigurationManager.CertRegPoint.Challenge...   CertificateRegistra  14/01/2015 0:00:43  7
Exception: System.ArgumentException: Subject Name in CSR and challenge do not match    at Microsoft.ConfigurationManager.CertRegPoint.Challenge...   CertificateRegistra  14/01/2015 0:00:43  7
VerifyRequest Finished with status False                                                                     CertificateRegistra  14/01/2015 0:00:43  7
VerifyRequest Started.                                                                                       CertificateRegistra  14/01/2015 0:01:09  8
Reading Template Permission Check from registry.                                                             CertificateRegistra  14/01/2015 0:01:09  8
Validation Phase 1 started.                                                                                  CertificateRegistra  14/01/2015 0:01:09  8
Validation Phase 1 finised with status True.                                                                 CertificateRegistra  14/01/2015 0:01:09  8
Validation Phase 2 started for device  and user .                                                            CertificateRegistra  14/01/2015 0:01:09  8
Validation Phase 2 finished.                                                                                 CertificateRegistra  14/01/2015 0:01:09  8
Validation Phase 3 started for device 24ba0a84-1042-405f-9ef4-80d2bf132645 and user 28f01f20-f992-421e-a178-d6ec196b087d.   CertificateRegistra  14/01/2015 0:01:09  8

Date/Time:  14/01/2015 0:00:43        Component:  CertificateRegistrationPoint
Thread:     7 (0x7)                   Source:

Subject Name in CSR OID.=be, OID.=demolabs, OU=HQ, OU=Demo Users, CN=Kenny Buntinx and challenge CN=Kenny Buntinx,OU=Demo Users,OU=HQ,DC=demolabs,DC=be do not match

Elapsed time is 169h 1m 39s 606ms (608499.606 seconds)
```



Name	Type	Data
(Default)	REG_SZ	(value not set)
EncryptionTemplate	REG_SZ	NDESEncryption
GeneralPurposeTemplate	REG_SZ	NDESEncryption
SignatureTemplate	REG_SZ	NDESEncryption

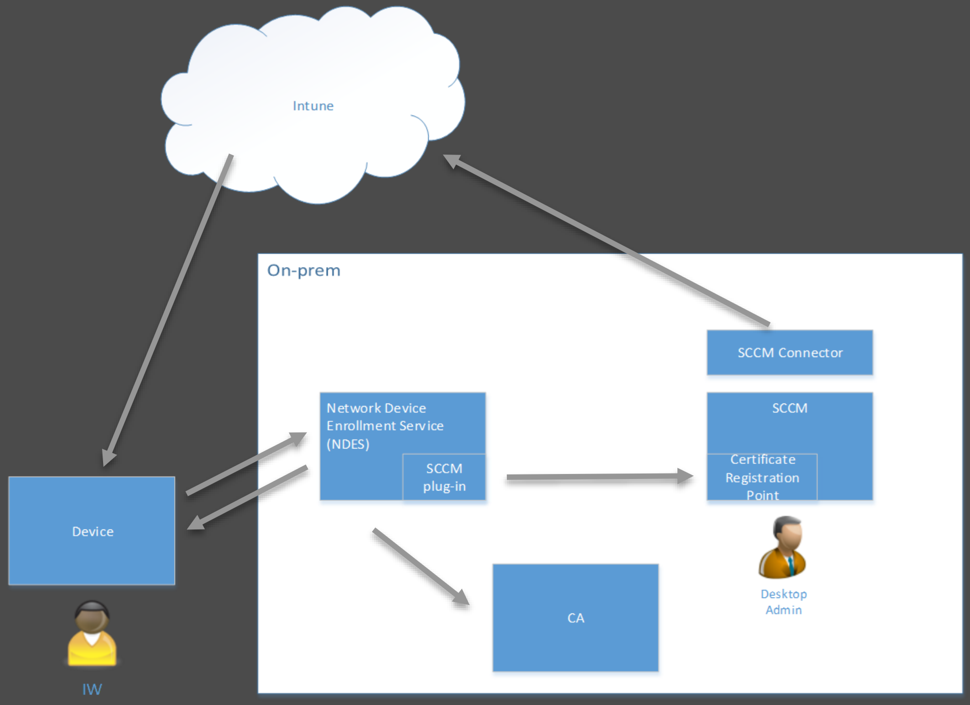
Certificate Profiles



Manage and distribute certificates

Deploy trusted root certificates
Support for Simple Certificate Enrollment Protocol (SCEP)

Certificate enrollment via NDES


Intune
On-prem
SCCM Connector
Network Device Enrollment Service (NDES)
SCCM plug-in
SCCM
Certificate Registration Point
Device
CA
Desktop Admin
IW

1. Certificate profile deployed to device
2. Device sends SCEP request
3. Challenge is validated
4. Certificate is issued

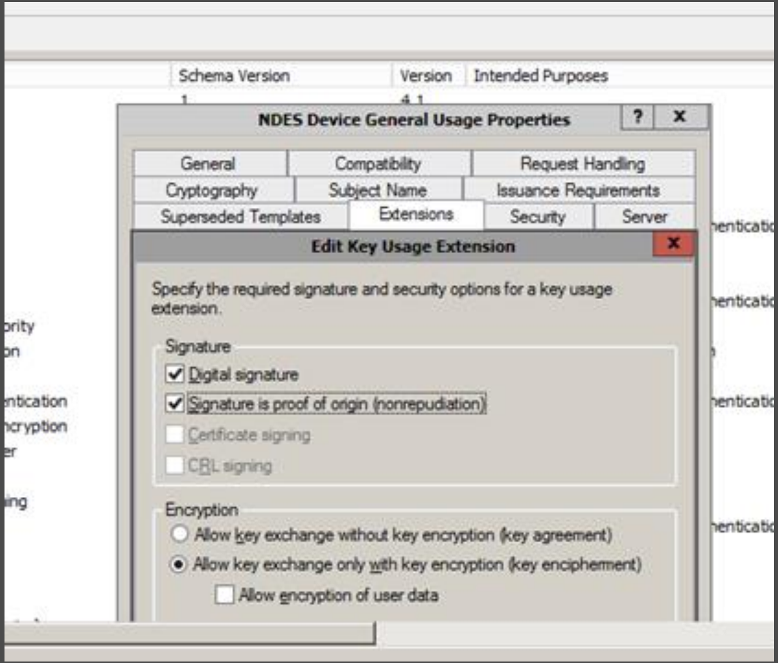
Why CU's Matter (*again*)

- CU3 improvements for NDES (now also in CU4)
- Tips:
  - Target to user instead of devices
    > Ensures fastest delivery
  - Pre CU3 templates need to be recreated
    > Re-targetting from device to user is not sufficient

As a side note …

- Certificate deployment to iOS 8
  - Required modification to template: Remove Signature in proof of origin

- See:
  - http://blog.coretech.dk/kea/troubleshooting-certificate-deployment-on-ios-devices-with-configmgr-intune/



Specify the required signature and security options for a key usage extension.

Signature

☑ Digital signature

☑ Signature is proof of origin (nonrepudiation)

□ Certificate signing

□ CRL signing

Encryption

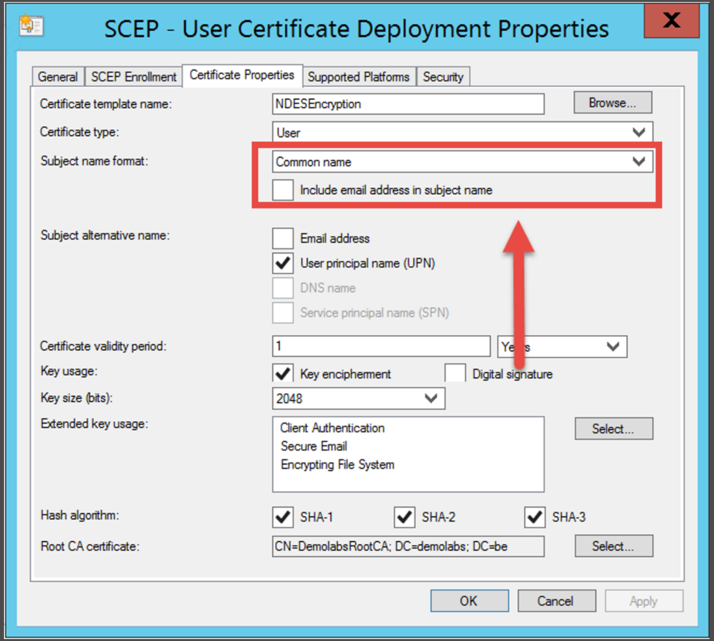
○ Allow key exchange without key encryption (key agreement)

● Allow key exchange only with key encryption (key encipherment)

□ Allow encryption of user data

As a side note … (2)

- User based Certificate deployment to iOS 8
  - Required modification to “subject name format” for user deployments: Only “Common name” supported



SCEP - User Certificate Deployment Properties

Certificate template name:	NDESEncryption
Certificate type:	User
Subject name format:	Common name □ Include email address in subject name
Subject alternative name:	□ Email address ☑ User principal name (UPN) □ DNS name □ Service principal name (SPN)
Certificate validity period:	1 Years
Key usage:	☑ Key encipherment □ Digital signature
Key size (bits):	2048
Extended key usage:	Client Authentication Secure Email Encrypting File System
Hash algorithm:	☑ SHA-1 ☑ SHA-2 ☑ SHA-3
Root CA certificate:	CN=DemolabsRootCA; DC=demolabs; DC=be

DEMO

Certificate deployment

Q & A

Herzlichen Dank

Mirko Colemberg @mirkocolemberg @configmgr_ch #cmcu_ch
blog.colemberg.ch

Bewertung der Session: Configmgr.ch

• Xing:	https://www.xing.com/net/cmce
• Facebook:	https://www.facebook.com/groups/411231535670608/
• Linkedin:	http://www.linkedin.com
• Twitter:	https://twitter.com/configmgr_ch

Nächster Event: Freitag 19. Juni Digicomp Bern
(begrenzte Anzahl Teilnehmer)