# SECARDEO

certRevoke

Secardeo certRevoke is an automatic certificate revocation service. If an Active Directory object is modified or deleted cert-Revoke sends a revocation request for all its associated certificates to the CA. The object attributes and organizational units which should be monitored can be configured. By this, automatic re-enrollment of certificates will be triggered, for example in case of name or address changes. Secardeo certRevoke can be used with an existing Secardeo certEP installation or a Windows Enterprise CA.

The following features are supported:

- Support for Secardeo certEP v4 and Windows Enterprise CA
- Monitoring of user and machine objects in AD
- Flexible control of attributes to monitor
- Filter for specific OUs in the AD tree
- Configurable monitoring interval
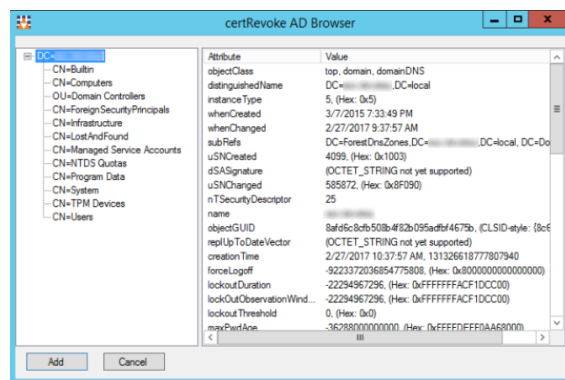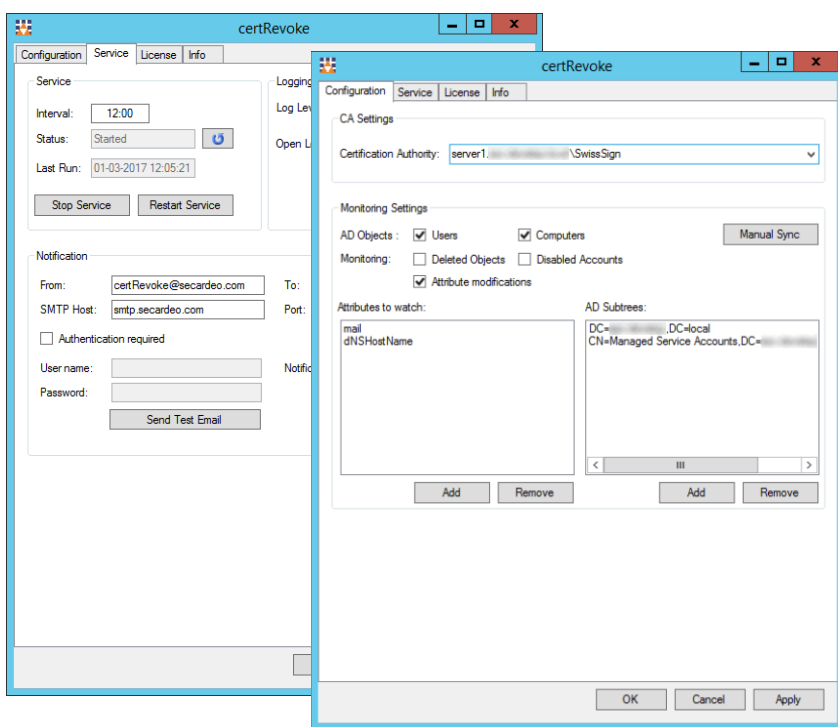
Supported Systems:

- Microsoft® Windows Server 2008 R2
- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2012 R2
- Microsoft® Windows Server 2016

Supported AD Versions:

- Microsoft® Active Directory 2008 R2, 2012, 2012 R2, 2016

Supported CAs:

- Secardeo certEP v4 with the following backends:
    - D-Trust
    - Dogtag CA
    - EJBCA
    - OpenSSL CA
    - OpenXPKI
    - SwissSign
    - Windows CA

Further backends on request.

- Microsoft® ADCS Enterprise CA

Software Requirements:

- Microsoft® .NET Framework 4.0

Standards:

- X.509-Certificates and CRLs RFC 5280
- CMS with PKCS#10 RFC 3852
- CMC RFC 5272

Further information on request.

SECARDEO