TOMORROW
starts here.

Advanced AnyConnect Deployment and Troubleshooting with ASA

BRSEC-3033

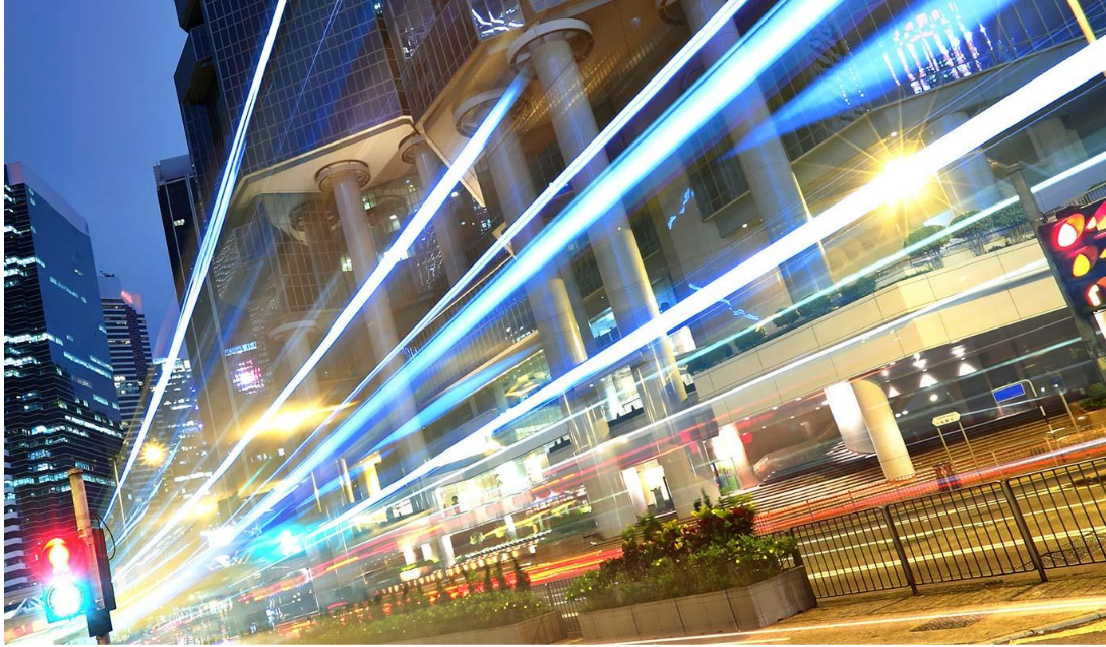
Rahul Govindan

Technical Services Engineer - APJC

#clmel

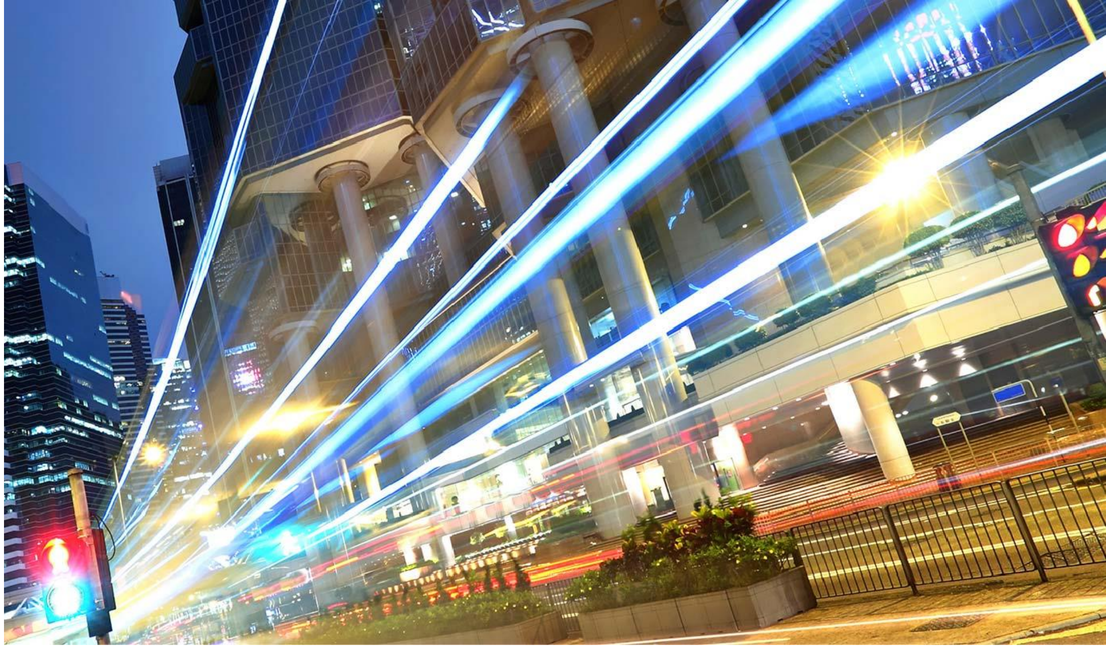
Agenda

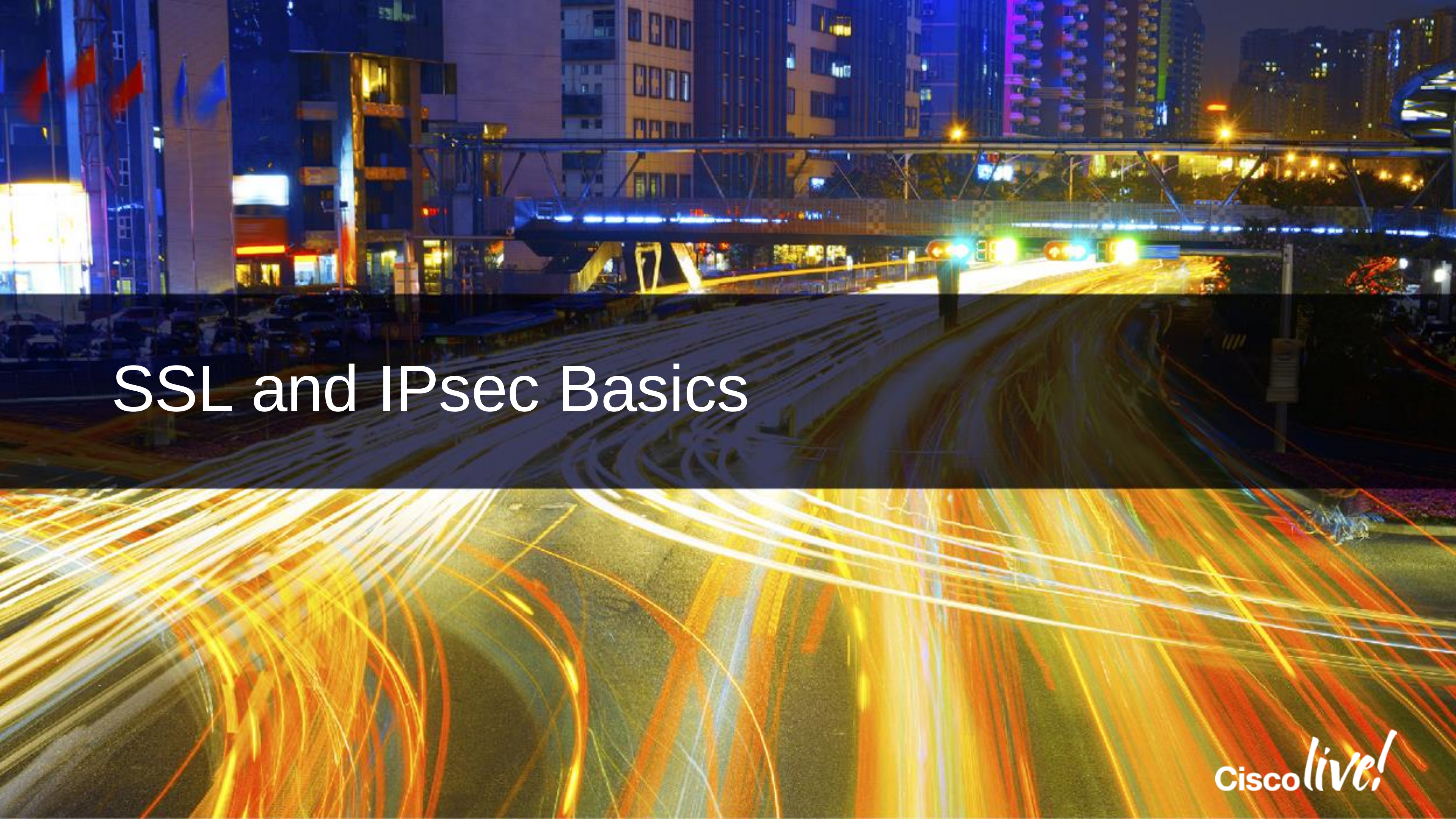
- SSL and IPsec Basics
- AnyConnect Fundamentals
- Authentication and Authorisation mechanisms
- Posture and Endpoint assessment
- AnyConnect Integration with ISE
- AnyConnect advanced features and customisation



Other Interesting Sessions

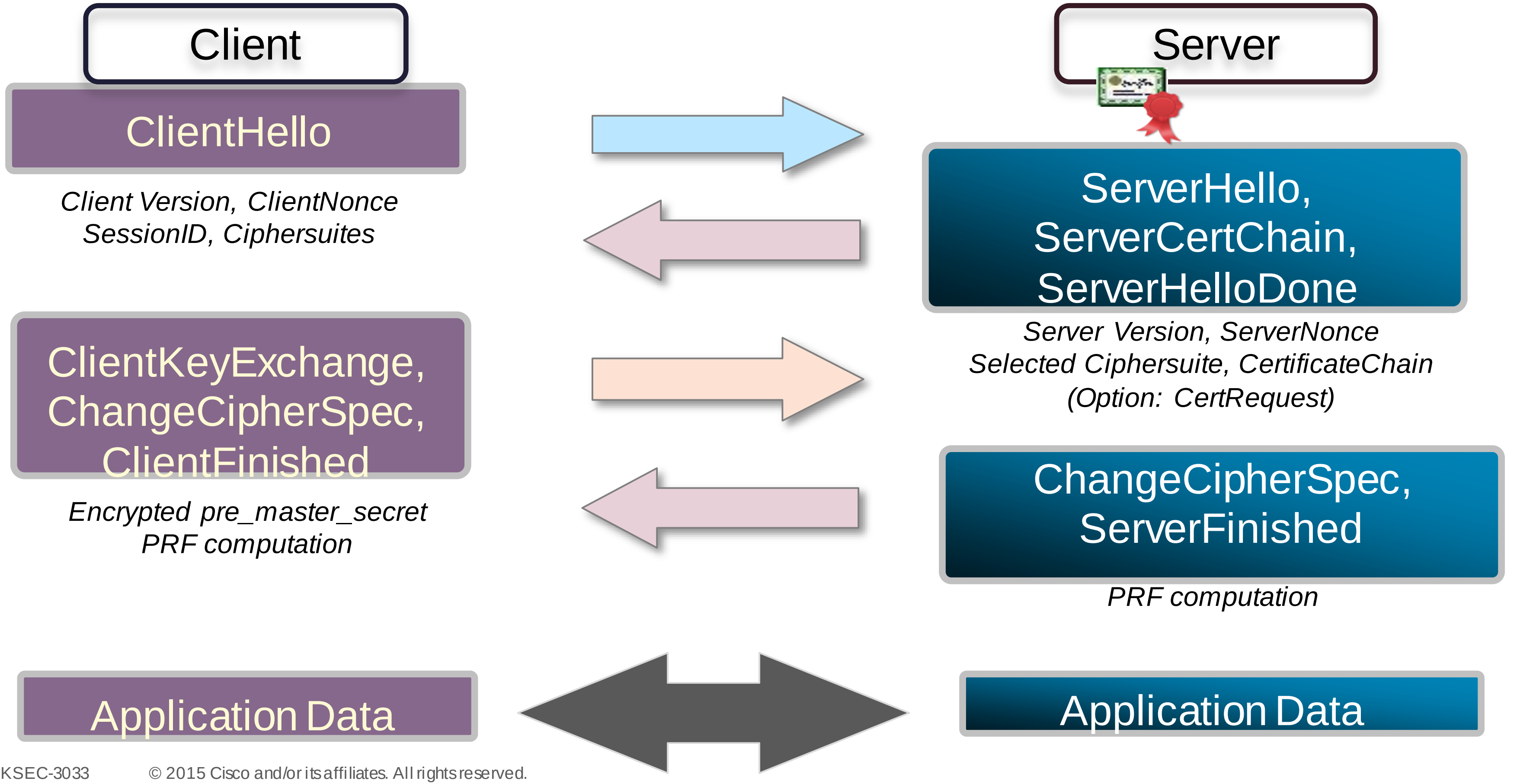
- BRKSEC-2044 - Building an Enterprise Access Control Architecure Using ISE and TrustSec
- BRKSEC-3013 - Deploying FlexVPN with IKEv2 and SSL
- BRKSEC-3045 - Advanced ISE and Secure Access Deployment
- LABSEC-1001 - TrustSec - Integrating ASA & ISE





SSL and IPsec Basics

The TLS Handshake



Client

Server

ClientHello

Client Version, ClientNonce
SessionID, Ciphersuites

ServerHello,
ServerCertChain,
ServerHelloDone

Server Version, ServerNonce
Selected Ciphersuite, CertificateChain
(Option: CertRequest)

ClientKeyExchange,
ChangeCipherSpec,
ClientFinished

Encrypted pre_master_secret
PRF computation

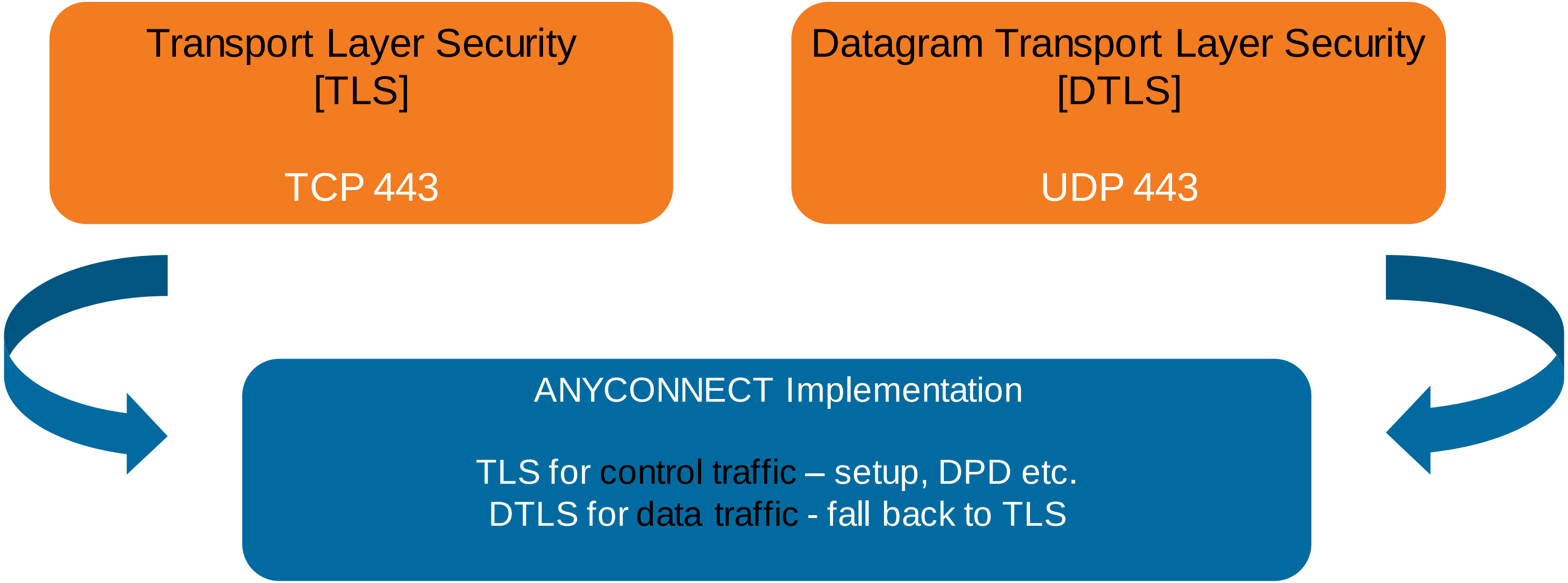
ChangeCipherSpec,
ServerFinished

PRF computation

Application Data

Application Data

TLS and DTLS



Transport Layer Security
[TLS]

TCP 443

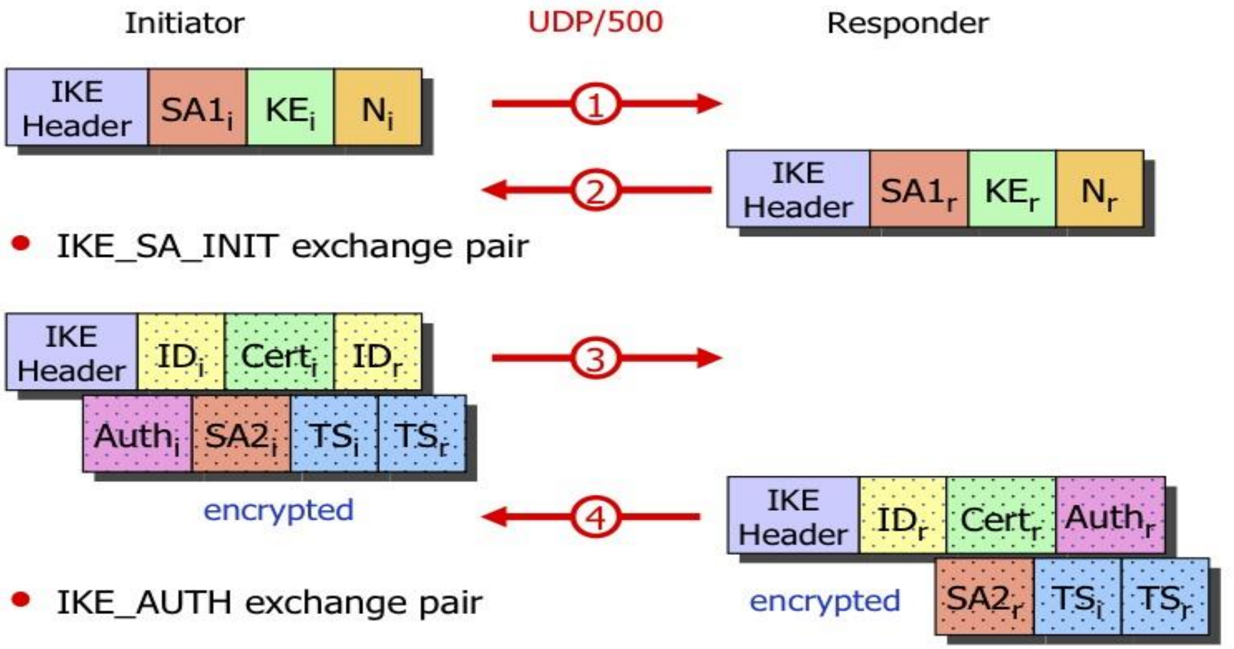
Datagram Transport Layer Security
[DTLS]

UDP 443

ANYCONNECT Implementation

TLS for control traffic – setup, DPD etc.
DTLS for data traffic - fall back to TLS

IKEv2



- IKE_SA_INIT exchange pair
- IKE_AUTH exchange pair

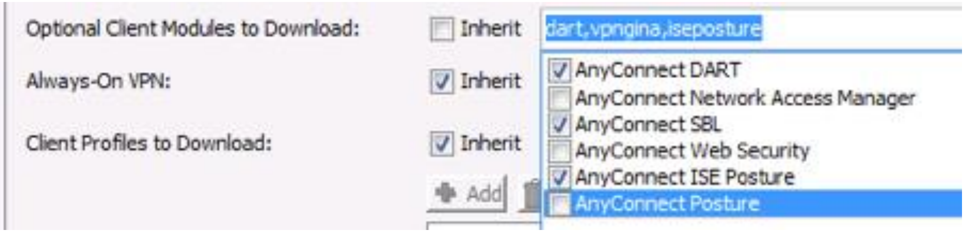
ASA IKEv2 Remote Access – AnyConnect 3.0+ or standard IKEv2 client [9.3.2 onwards]

AnyConnect IKEv2 supports Next Gen Crypto

Fundamentals of AnyConnect

AnyConnect - Modules

- Primary Module - VPN
- Optional modules to install
  - DART
  - Posture
  - ISE Posture
  - Start-Before-Logon
  - Web security, Network Access Manager
  - Feedback Module

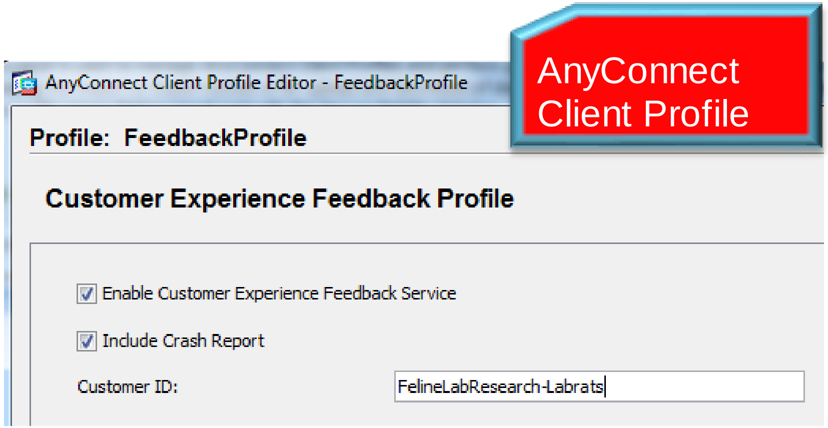


Optional Client Modules to Download: ☐ Inherit dart,vpngina,iseposture

Always-On VPN: ☑ Inherit

Client Profiles to Download: ☑ Inherit

☑ AnyConnect DART
☐ AnyConnect Network Access Manager
☑ AnyConnect SBL
☐ AnyConnect Web Security
☑ AnyConnect ISE Posture
☐ AnyConnect Posture



AnyConnect Client Profile Editor - FeedbackProfile

Profile: FeedbackProfile

Customer Experience Feedback Profile

☑ Enable Customer Experience Feedback Service

☑ Include Crash Report

Customer ID: FelineLabResearch-Labrats

AnyConnect Client Profile

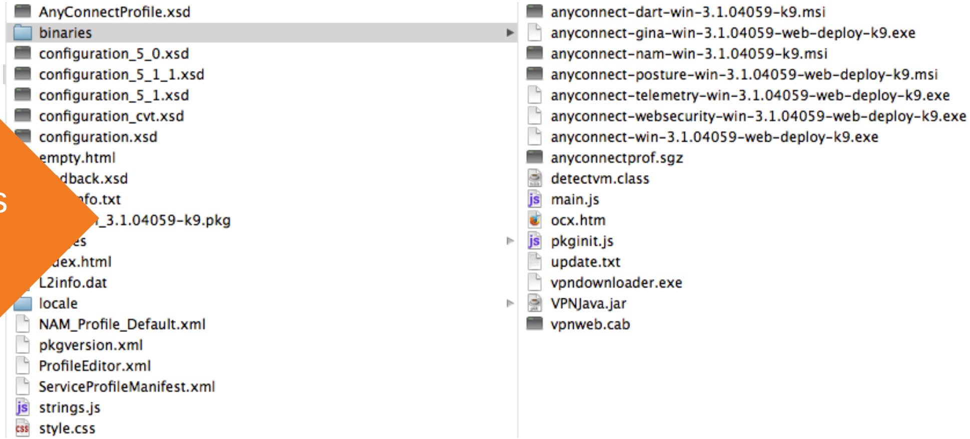
AnyConnect Deployment Options

Web Deployment

- Deployed using .pkg file
- Can be deployed via ASA or using ISE 1.3

Pre-deployment

- Install manually using .iso,.dmg files
- Enterprise management systems (SMS) or app store [iOS, Android]

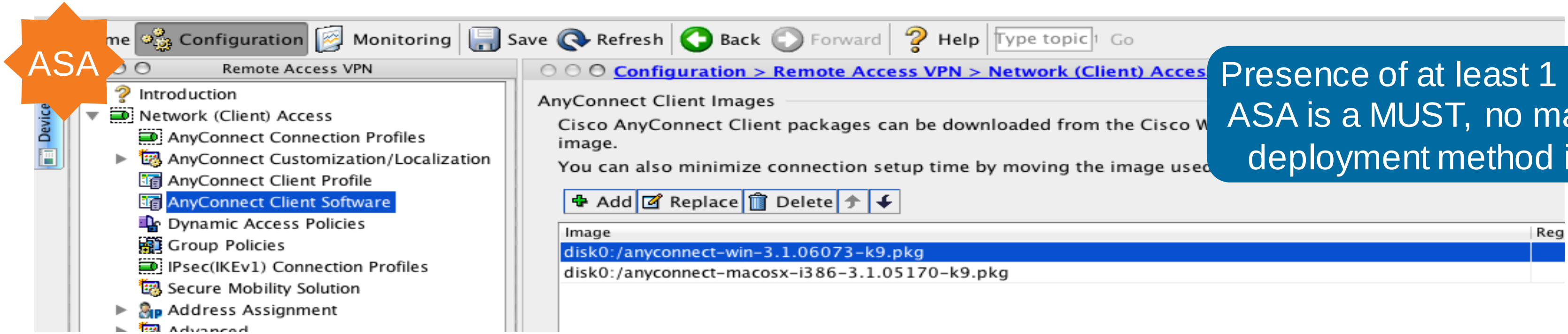


```
AnyConnectProfile.xsd                anyconnect-dart-win-3.1.04059-k9.msi
binaries                             anyconnect-gina-win-3.1.04059-web-deploy-k9.exe
configuration_5_0.xsd                anyconnect-nam-win-3.1.04059-k9.msi
configuration_5_1_1.xsd              anyconnect-posture-win-3.1.04059-web-deploy-k9.msi
configuration_5_1.xsd                anyconnect-telemetry-win-3.1.04059-web-deploy-k9.exe
configuration_cvt.xsd                anyconnect-websecurity-win-3.1.04059-web-deploy-k9.exe
configuration.xsd                    anyconnect-win-3.1.04059-web-deploy-k9.exe
empty.html                           anyconnectprof.sgz
dback.xsd                            detectvm.class
nfo.txt                              main.js
_3.1.04059-k9.pkg                    ocx.htm
es                                   pkginit.js
dex.html                             update.txt
L2info.dat                           vpndownloader.exe
locale                               VPNJava.jar
NAM_Profile_Default.xml              vpnweb.cab
pkgversion.xml
ProfileEditor.xml
ServiceProfileManifest.xml
strings.js
style.css
```

AnyConnect.pkg contains client binaries

AnyConnect Web Deployment

ASA



AnyConnect Client Images

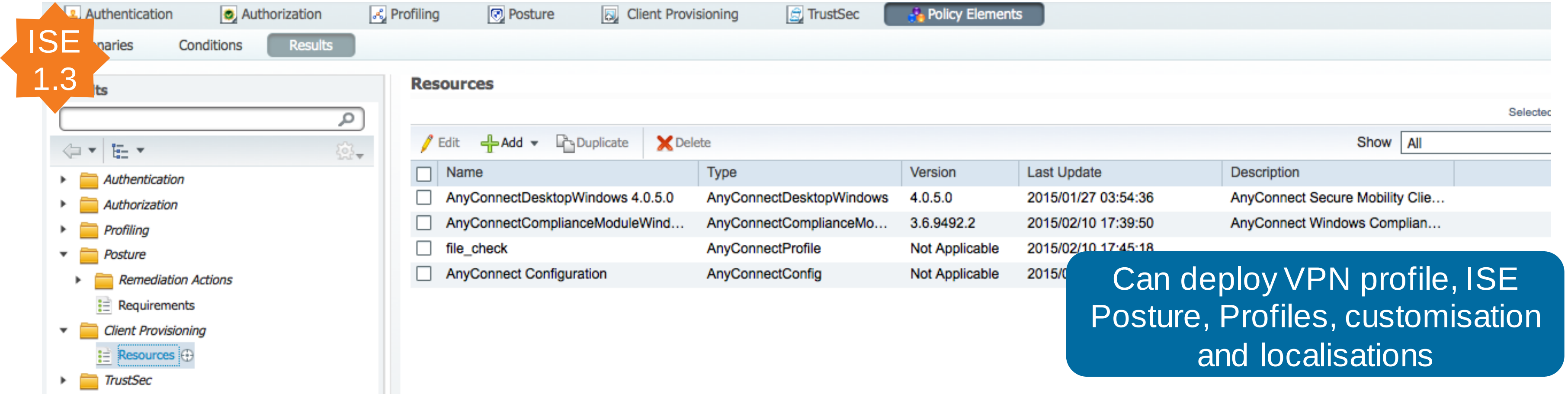
Cisco AnyConnect Client packages can be downloaded from the Cisco W image.

You can also minimize connection setup time by moving the image used

Image	Reg
disk0:/anyconnect-win-3.1.06073-k9.pkg	
disk0:/anyconnect-macosx-i386-3.1.05170-k9.pkg	

Presence of at least 1 .pkg file on ASA is a MUST, no matter which deployment method is used !!

ISE 1.3



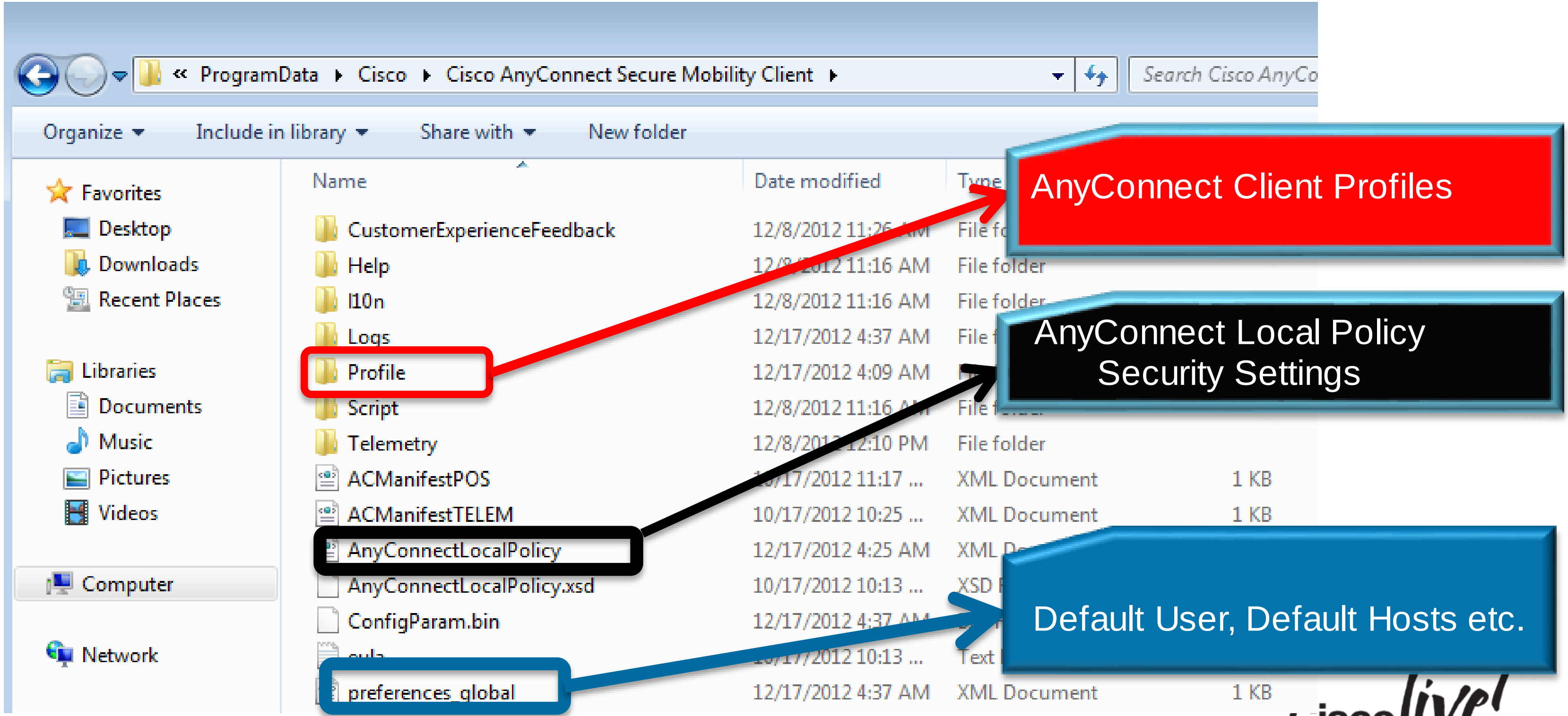
Resources

☐	Name	Type	Version	Last Update	Description
☐	AnyConnectDesktopWindows 4.0.5.0	AnyConnectDesktopWindows	4.0.5.0	2015/01/27 03:54:36	AnyConnect Secure Mobility Clie…
☐	AnyConnectComplianceModuleWind…	AnyConnectComplianceMo…	3.6.9492.2	2015/02/10 17:39:50	AnyConnect Windows Complian…
☐	file_check	AnyConnectProfile	Not Applicable	2015/02/10 17:45:18	
☐	AnyConnect Configuration	AnyConnectConfig	Not Applicable	2015/0	

Can deploy VPN profile, ISE Posture, Profiles, customisation and localisations

On the Client: AnyConnect Configuration Files

Apply to all Users logged onto the machine



« ProgramData ▸ Cisco ▸ Cisco AnyConnect Secure Mobility Client ▸

Name	Date modified	Type	
CustomerExperienceFeedback	12/8/2012 11:26 AM	File fo	
Help	12/8/2012 11:16 AM	File folder	
l10n	12/8/2012 11:16 AM	File folder	
Logs	12/17/2012 4:37 AM	File f	
Profile	12/17/2012 4:09 AM	F	
Script	12/8/2012 11:16 AM	File f	
Telemetry	12/8/2012 12:10 PM	File folder	
ACManifestPOS	10/17/2012 11:17 ...	XML Document	1 KB
ACManifestTELEM	10/17/2012 10:25 ...	XML Document	1 KB
AnyConnectLocalPolicy	12/17/2012 4:25 AM	XML D	
AnyConnectLocalPolicy.xsd	10/17/2012 10:13 ...	XSD F	
ConfigParam.bin	12/17/2012 4:37 AM		
eula	10/17/2012 10:13 ...	Text	
preferences_global	12/17/2012 4:37 AM	XML Document	1 KB

AnyConnect Client Profiles

AnyConnect Local Policy Security Settings

Default User, Default Hosts etc.

On the Client: AnyConnect Configuration Files

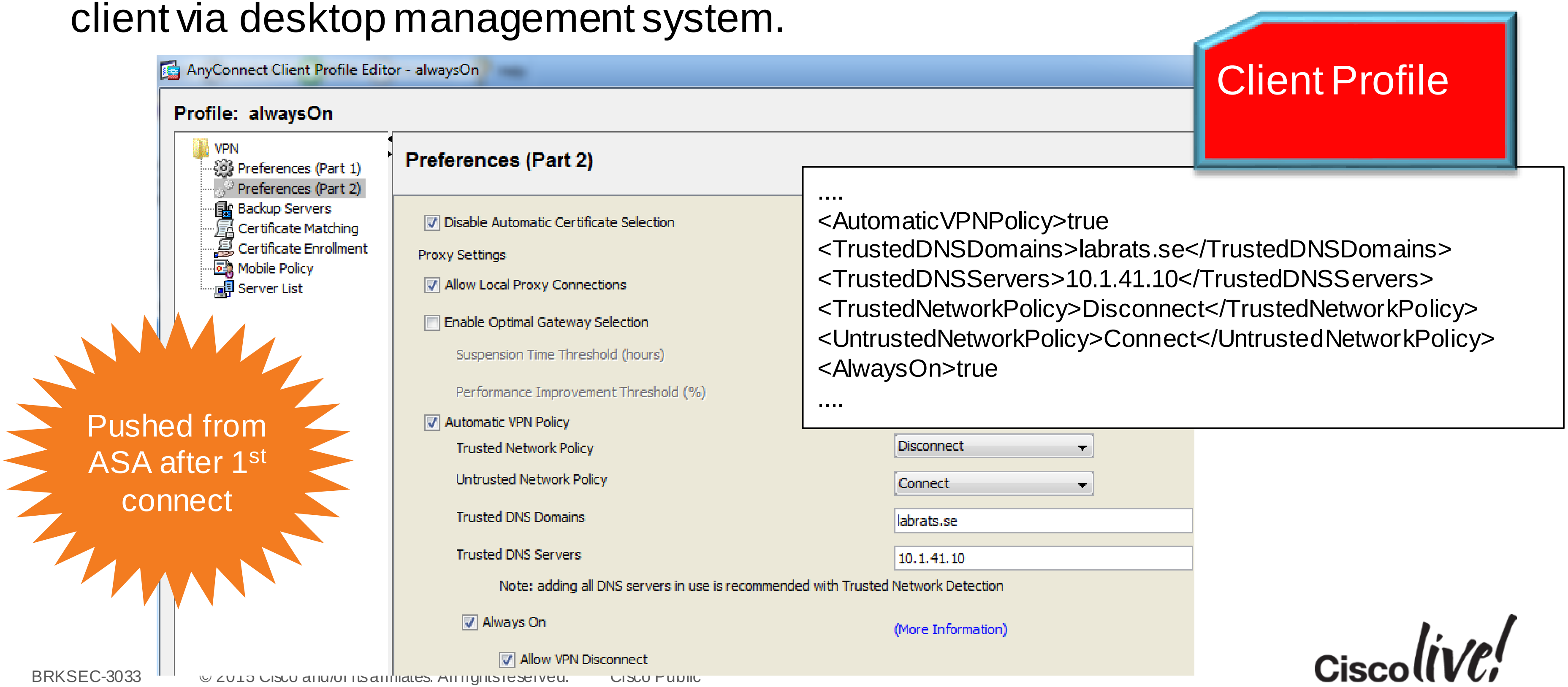
- AnyConnect Configuration Files are stored on the client in the following directories:

Windows 7 and Windows VISTA	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Windows XP	C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client
MAC OS X and Linux	/opt/cisco/anyconnect/

Windows 7 and Windows VISTA	C:\Users\username\AppData\Local\Cisco\ Cisco AnyConnect VPN Client\preferences.xml
Windows XP	C:\Documents and Settings\username\Local Settings\ApplicationData\ Cisco\Cisco AnyConnect VPN Client\preferences.xml
MAC OS X and Linux	/Users/username/.anyconnect

AnyConnect Client Profiles

- XML file created by ASDM, downloaded to client from ASA or pre-deployed to client via desktop management system.



AnyConnect Client Profile Editor - alwaysOn

Profile: alwaysOn

Preferences (Part 2)

☑ Disable Automatic Certificate Selection

Proxy Settings

☑ Allow Local Proxy Connections

□ Enable Optimal Gateway Selection

Suspension Time Threshold (hours)

Performance Improvement Threshold (%)

☑ Automatic VPN Policy

Trusted Network Policy: Disconnect

Untrusted Network Policy: Connect

Trusted DNS Domains: labrats.se

Trusted DNS Servers: 10.1.41.10

Note: adding all DNS servers in use is recommended with Trusted Network Detection

☑ Always On

(More Information)

☑ Allow VPN Disconnect

Client Profile

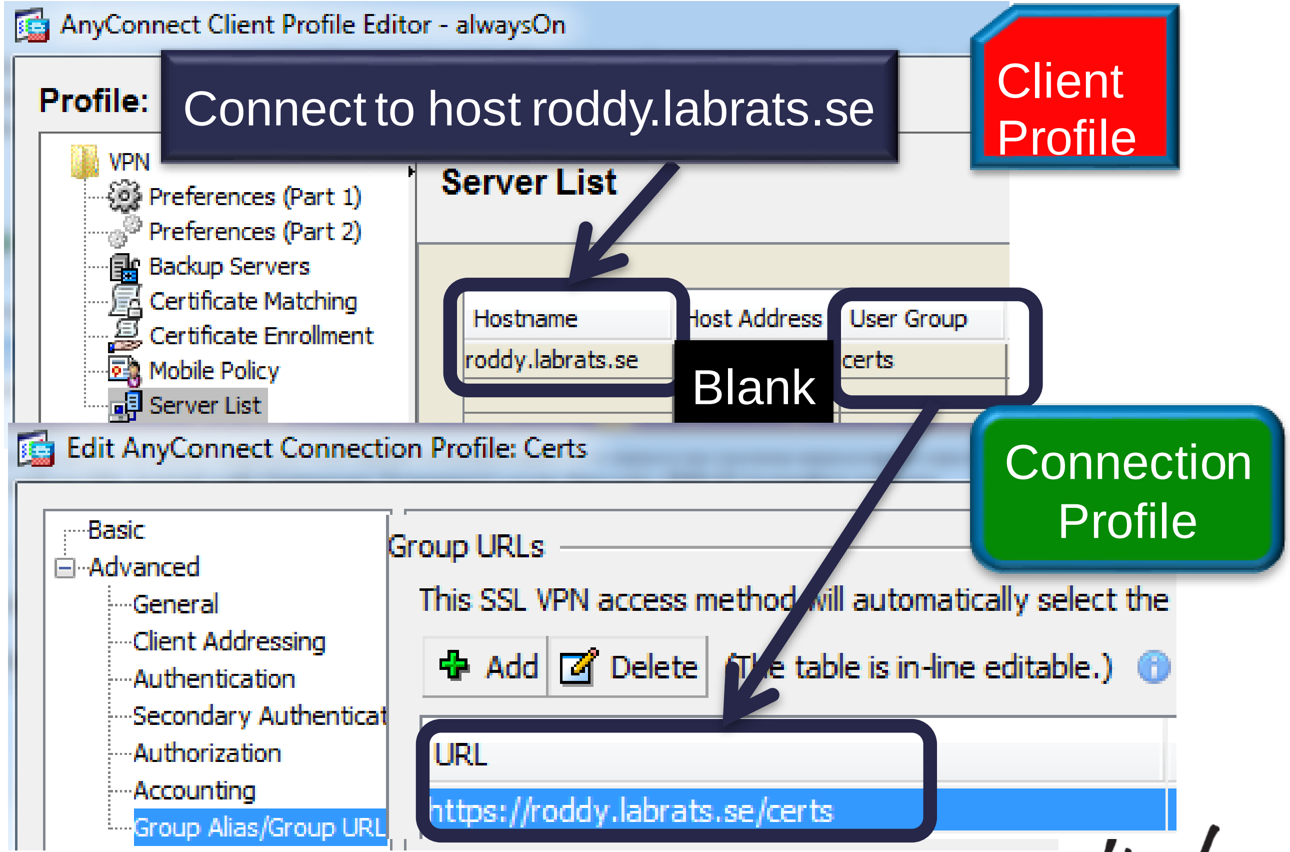
```
....
<AutomaticVPNPolicy>true
<TrustedDNSDomains>labrats.se</TrustedDNSDomains>
<TrustedDNSServers>10.1.41.10</TrustedDNSServers>
<TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
<UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
<AlwaysOn>true
....
```

Pushed from ASA after 1st connect

In the AnyConnect Client Profile : Server List

- Specify servers FQDN in the server list
- User can choose server from list.

Server List Entry essential for certain client-side features to work.



AnyConnect Client Profile Editor - alwaysOn

Profile:

Connect to host roddy.labrats.se

Client Profile

Server List

Hostname	Host Address	User Group
roddy.labrats.se	Blank	certs

Edit AnyConnect Connection Profile: Certs

Connection Profile

Group URLs

This SSL VPN access method will automatically select the

(The table is in-line editable.)

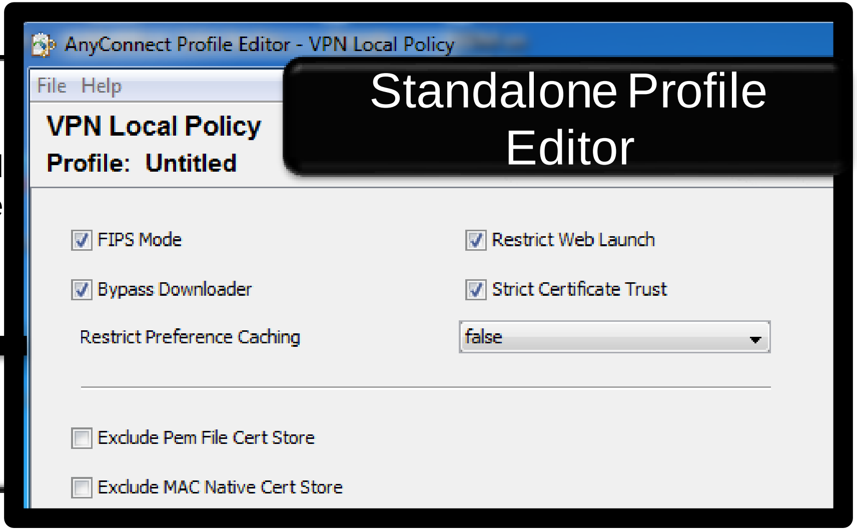
URL
https://roddy.labrats.se/certs

AnyConnect Local Policy

AnyConnect Local Policy File

- Not downloaded from ASA – local settings valid for user alone
- XML file defining important aspects of AnyConnect behaviour
  - allowing user to accept untrusted ASA certificates
  - allowing client software updates from ASA (and from which ASAs)
  - allowing client profile updates from ASA (and from which ASAs)
  - certificate stores, credentials caching etc.

```
<StrictCertificateTrust>false</StrictCertificateTrust>
<UpdatePolicy>
   <AllowSoftwareUpdatesFromAnyServer>false</AllowSoftwareUpd
   <AllowVPNProfileUpdatesFromAnyServer>false</AllowVPNProfile
   <AuthorizedServerList>
      <ServerName>itchy.labrats.se</ServerName>
      <ServerName>roddy.labrats.se</ServerName>
   </AuthorizedServerList>
</UpdatePolicy>
```



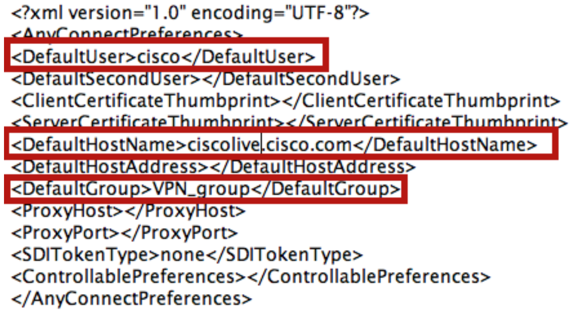
VPN Local Policy
Profile: Untitled

☑ FIPS Mode
☑ Restrict Web Launch
☑ Bypass Downloader
☑ Strict Certificate Trust
Restrict Preference Caching: false
□ Exclude Pem File Cert Store
□ Exclude MAC Native Cert Store

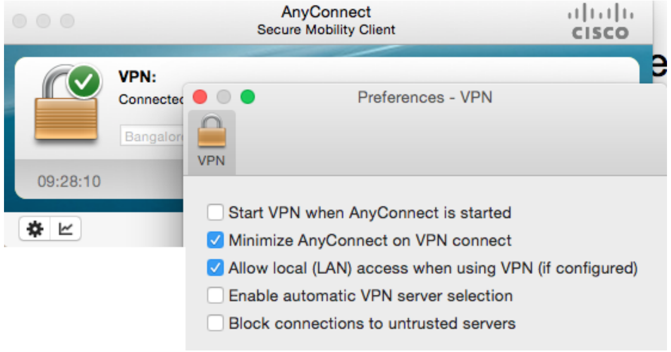
Standalone Profile Editor

AnyConnect Preferences

- Saves the last successful connection parameters for ease of use.
- User preferences saves settings like default username, group gateway etc.[preferences.xml]
- Controllable preferences can be modified by user in AnyConnect UI
- Global preferences – controllable preferences applied before use logon. ‘SBL enabled’ is checked against this file before logon. [preferences_global.xml]



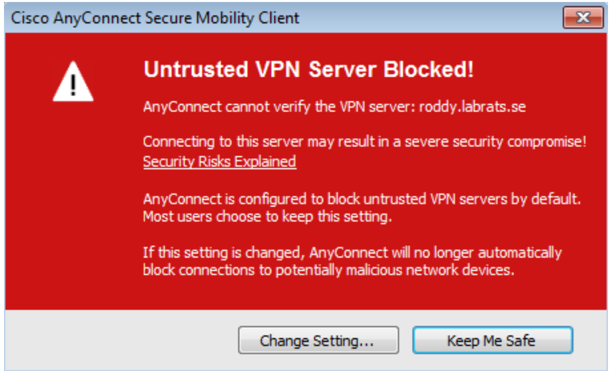
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectPreferences>
<DefaultUser>cisco</DefaultUser>
<DefaultSecondUser></DefaultSecondUser>
<ClientCertificateThumbprint></ClientCertificateThumbprint>
<ServerCertificateThumbprint></ServerCertificateThumbprint>
<DefaultHostName>ciscolive.cisco.com</DefaultHostName>
<DefaultHostAddress></DefaultHostAddress>
<DefaultGroup>VPN_group</DefaultGroup>
<ProxyHost></ProxyHost>
<ProxyPort></ProxyPort>
<SDITokenType>none</SDITokenType>
<ControllablePreferences></ControllablePreferences>
</AnyConnectPreferences>
```



□ Start VPN when AnyConnect is started
☑ Minimize AnyConnect on VPN connect
☑ Allow local (LAN) access when using VPN (if configured)
□ Enable automatic VPN server selection
□ Block connections to untrusted servers

ASA Server Certificate

- AnyConnect client throws a warning when it does not trust the ASA's identity cert
- ASA certificate can be from:
  - Public (well-known) Certificate Authority (e.g. Verisign, Thawte)
  - Enterprise Certificate Authority, e.g. Microsoft Active Directory
  - Self-Signed



Cisco AnyConnect Secure Mobility Client

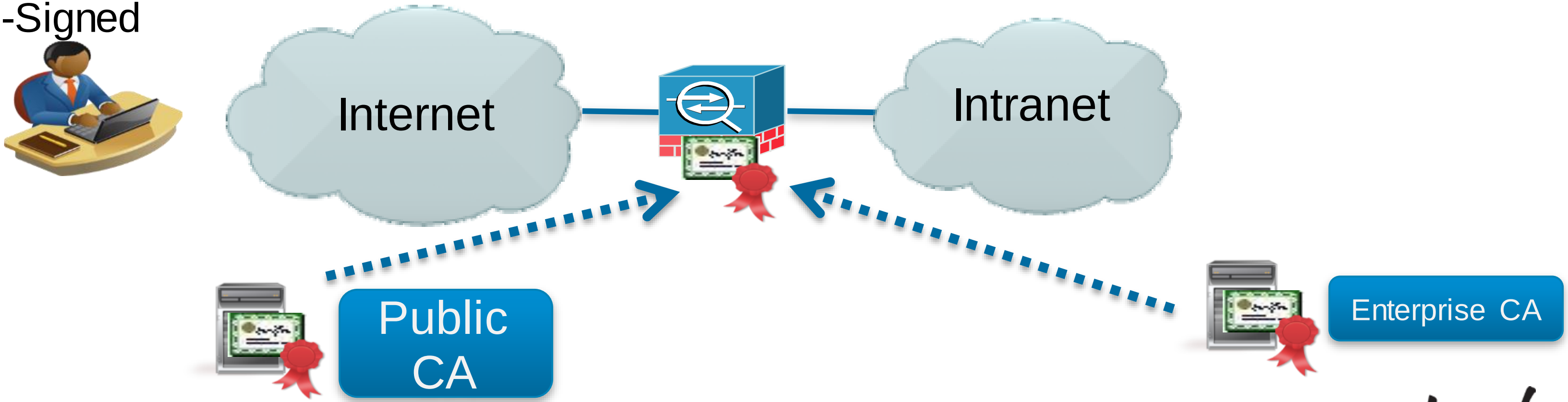
Untrusted VPN Server Blocked!

AnyConnect cannot verify the VPN server: roddy.labrats.se

Connecting to this server may result in a severe security compromise!
Security Risks Explained

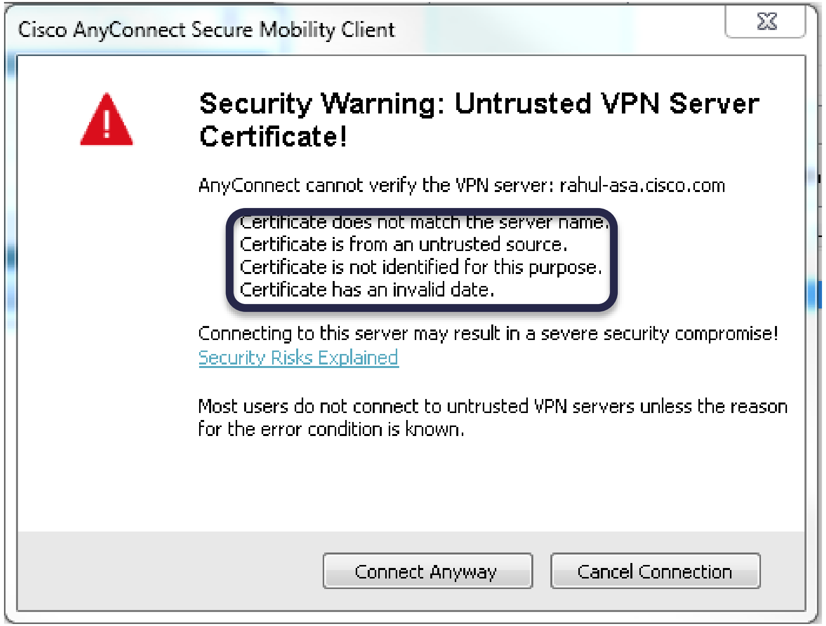
AnyConnect is configured to block untrusted VPN servers by default. Most users choose to keep this setting.

If this setting is changed, AnyConnect will no longer automatically block connections to potentially malicious network devices.



Trusting the ASA Certificate

- AnyConnect uses native OS to validate certificate:
  - Microsoft Windows: MS CAPI
  - MAC OS: Keychain
  - Linux: Varies with distribution
- AnyConnect client 4 checks for server cert:
  - Server certificate time validity
  - Server certificate issued by untrusted source
  - Server certificate name verification
  - KU and EKU setting



Cisco AnyConnect Secure Mobility Client

Security Warning: Untrusted VPN Server Certificate!

AnyConnect cannot verify the VPN server: rahul-asa.cisco.com

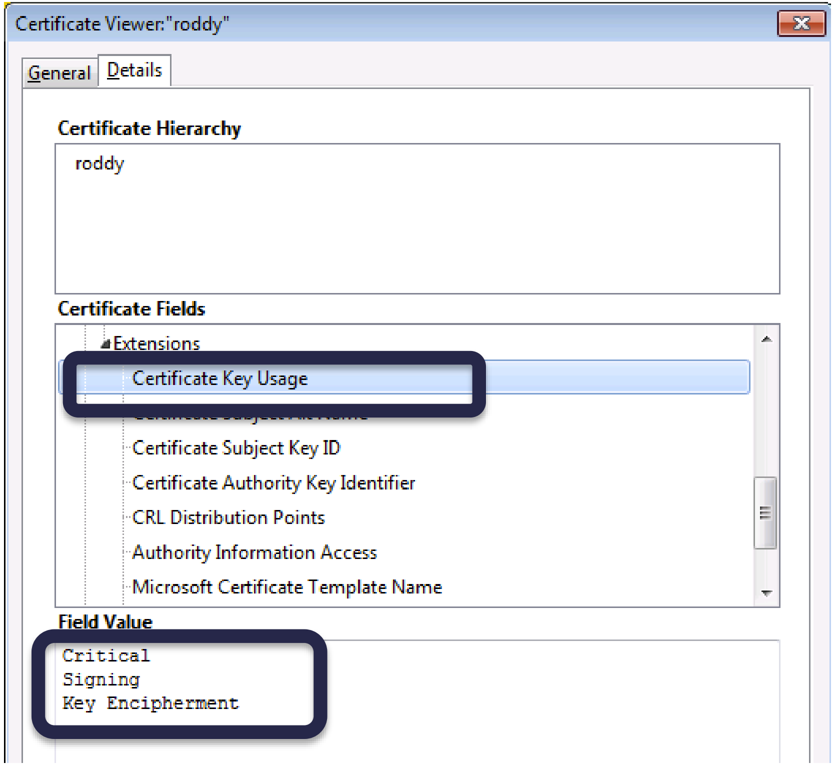
Certificate does not match the server name.
Certificate is from an untrusted source.
Certificate is not identified for this purpose.
Certificate has an invalid date.

Connecting to this server may result in a severe security compromise!
Security Risks Explained

Most users do not connect to untrusted VPN servers unless the reason for the error condition is known.

Key Usage and Extended Key Usage Checking

- Extended Key Usage (EKU) and Key Usage (KU) determine how certificate can be used (client authentication, server authentication, email encryption etc)
- AnyConnect does **not require** EKU or KU to be in ASA server certificate
- From AnyConnect 3.1: **if** EKU or KU are present, they **must** be correct
  - EKU must contain “Server Authentication”
  - KU must contain “Digital Signature” and “Key Encipherment”



Certificate Viewer:"roddy"

General | Details

Certificate Hierarchy

roddy

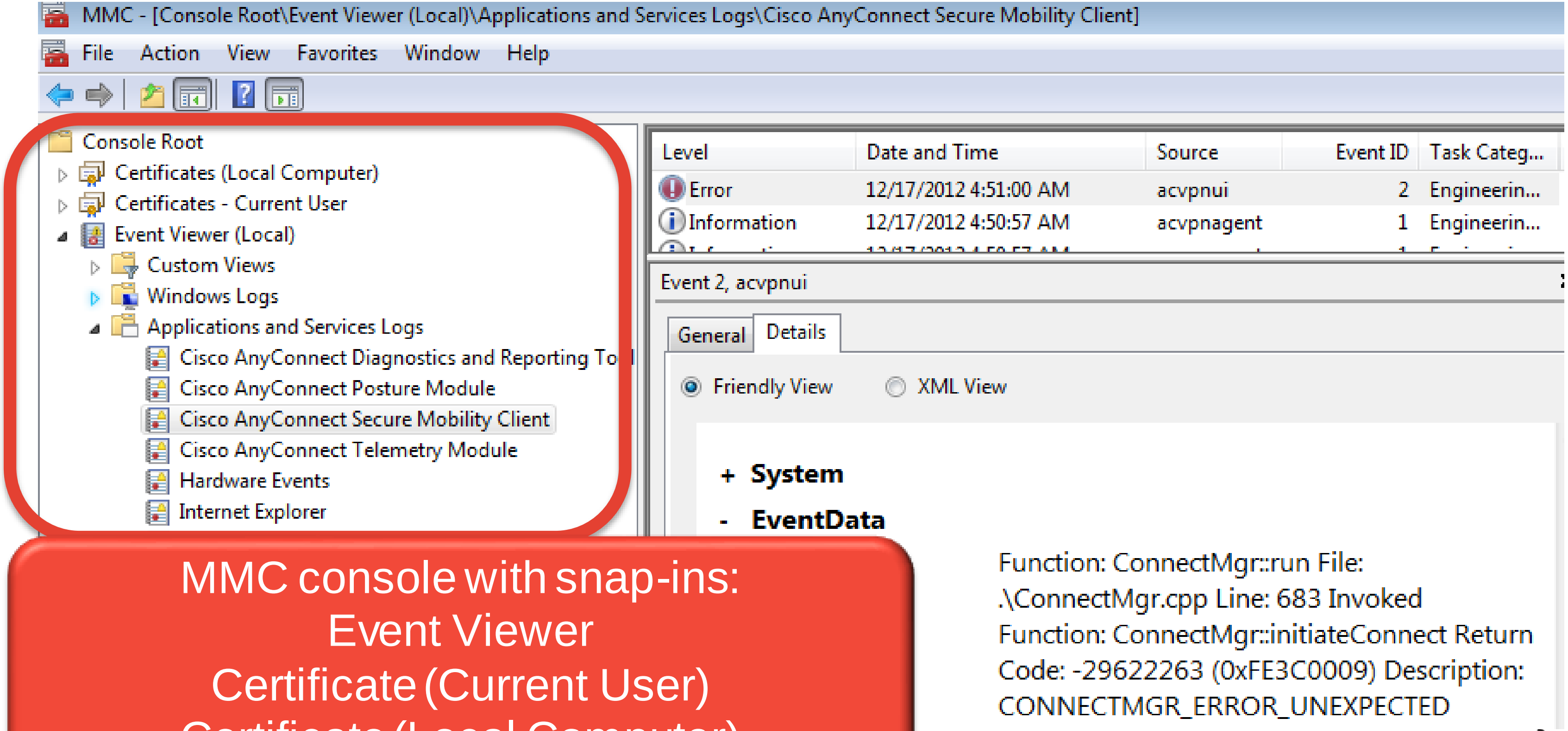
Certificate Fields

Extensions
- Certificate Key Usage
- Certificate Subject Alt Name
- Certificate Subject Key ID
- Certificate Authority Key Identifier
- CRL Distribution Points
- Authority Information Access
- Microsoft Certificate Template Name

Field Value

```
Critical
Signing
Key Encipherment
```

AnyConnect Troubleshooting Toolbox (Windows)


MMC - [Console Root\Event Viewer (Local)\Applications and Services Logs\Cisco AnyConnect Secure Mobility Client]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Certificates - Current User
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Cisco AnyConnect Diagnostics and Reporting To
Cisco AnyConnect Posture Module
Cisco AnyConnect Secure Mobility Client
Cisco AnyConnect Telemetry Module
Hardware Events
Internet Explorer

Level	Date and Time	Source	Event ID	Task Categ...
Error	12/17/2012 4:51:00 AM	acvpnui	2	Engineerin...
Information	12/17/2012 4:50:57 AM	acvpnagent	1	Engineerin...

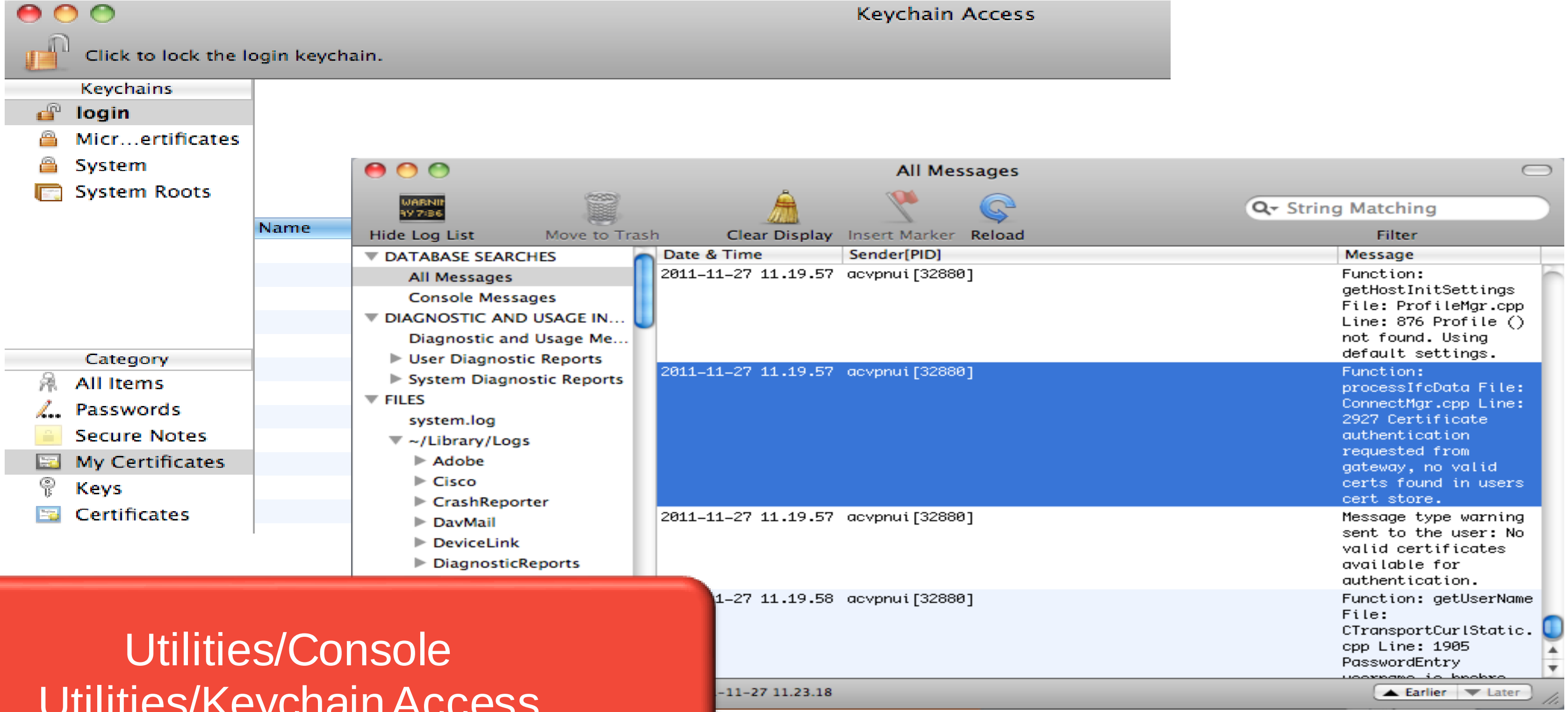
Event 2, acvpnui

General
Details
● Friendly View
○ XML View
+ System
- EventData

Function: ConnectMgr::run File: .\ConnectMgr.cpp Line: 683 Invoked Function: ConnectMgr::initiateConnect Return Code: -29622263 (0xFE3C0009) Description: CONNECTMGR_ERROR_UNEXPECTED

MMC console with snap-ins:
Event Viewer
Certificate (Current User)
Certificate (Local Computer)

AnyConnect Troubleshooting Toolbox (MAC)



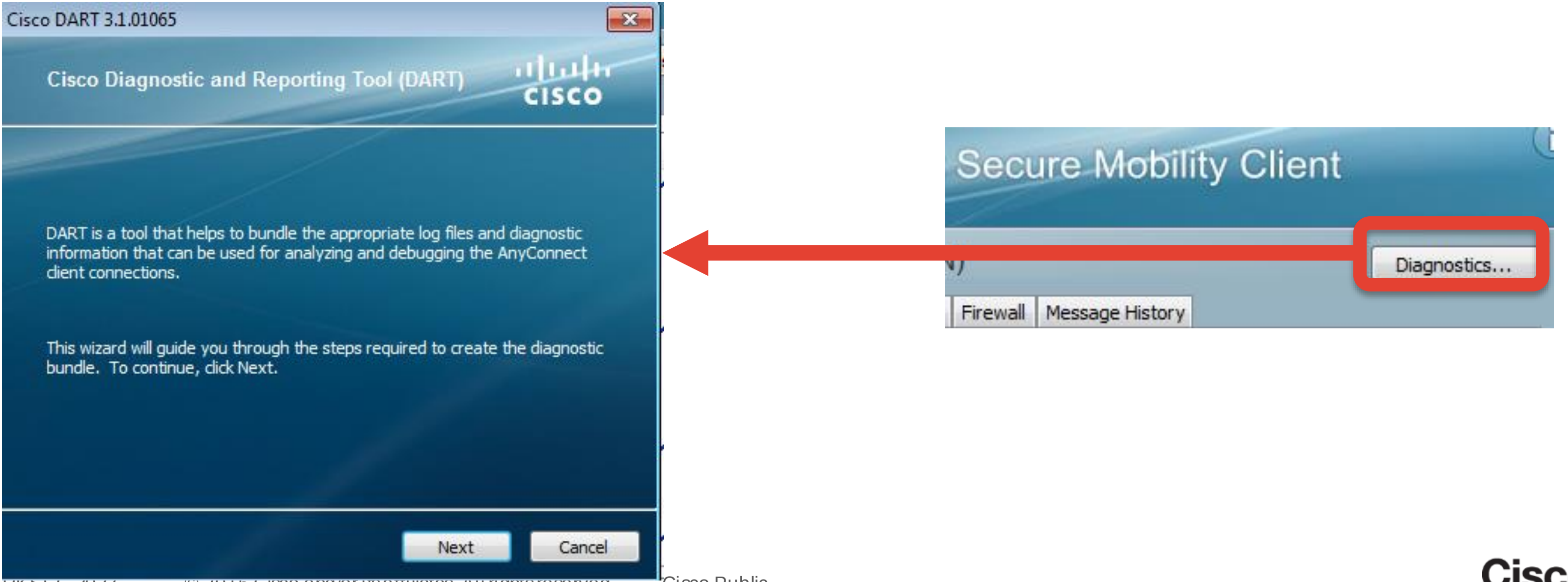
Date & Time	Sender[PID]	Message
2011-11-27 11.19.57	acvpnui[32880]	Function: getHostInitSettings File: ProfileMgr.cpp Line: 876 Profile () not found. Using default settings.
2011-11-27 11.19.57	acvpnui[32880]	Function: processIfcData File: ConnectMgr.cpp Line: 2927 Certificate authentication requested from gateway, no valid certs found in users cert store.
2011-11-27 11.19.57	acvpnui[32880]	Message type warning sent to the user: No valid certificates available for authentication.
1-27 11.19.58	acvpnui[32880]	Function: getUserName File: CTransportCurlStatic.cpp Line: 1905 PasswordEntry

-11-27 11.23.18

Utilities/Console
Utilities/Keychain Access

DART Tool (Windows and MAC)

- DART Tool can be installed along with the Client
- Similar to "show tech" on the client
- Gathering of OS Data, App Data and logfiles into a single ZIP File



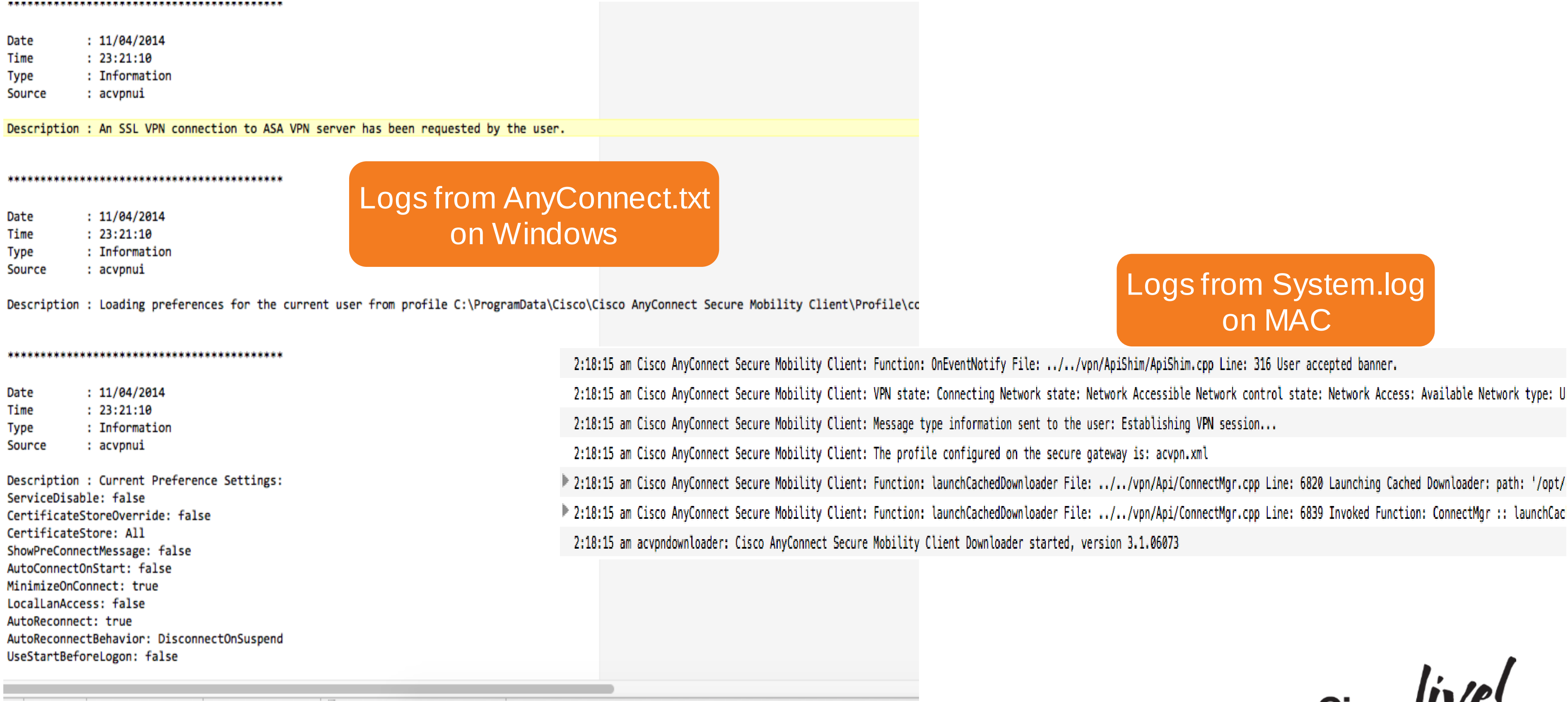
Cisco DART 3.1.01065

Cisco Diagnostic and Reporting Tool (DART)

DART is a tool that helps to bundle the appropriate log files and diagnostic information that can be used for analyzing and debugging the AnyConnect client connections.

This wizard will guide you through the steps required to create the diagnostic bundle. To continue, click Next.

Sample DART Logs – Windows and MAC



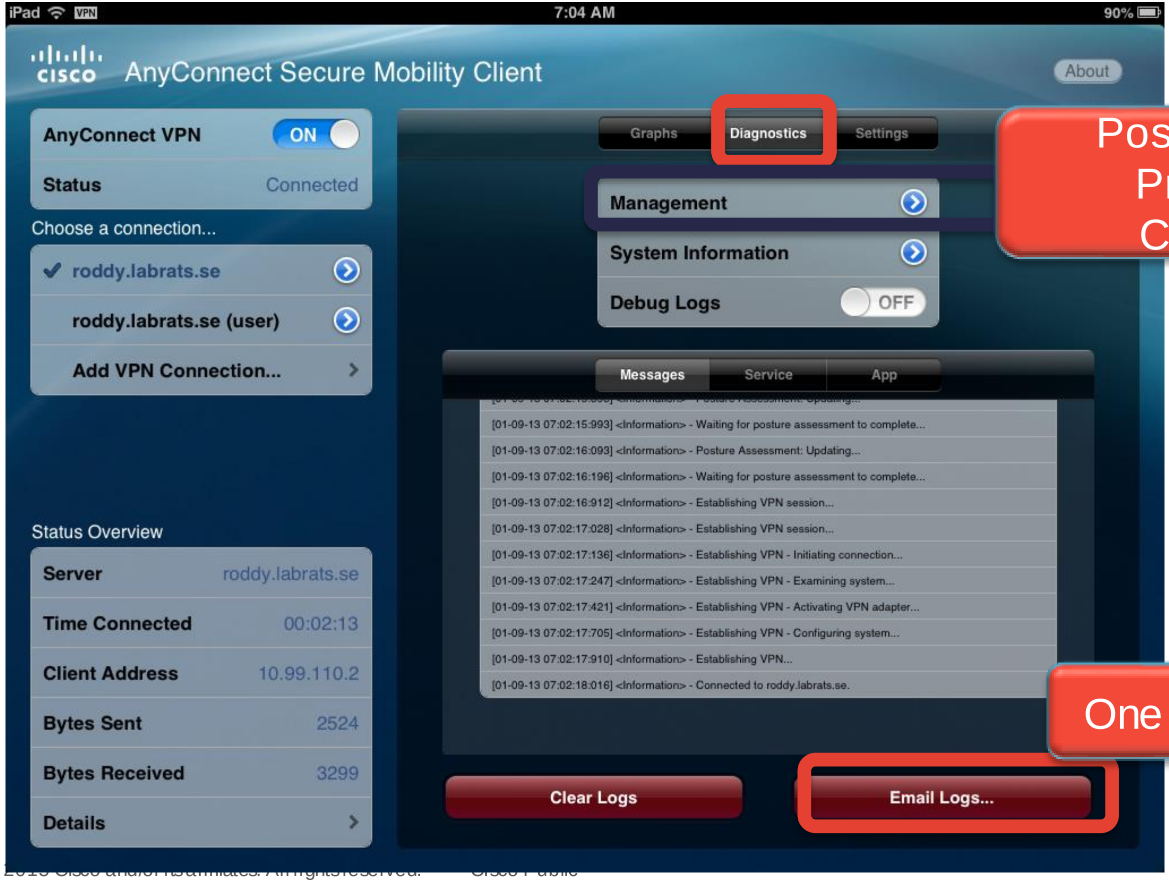
```
*******************************************

Date        : 11/04/2014
Time        : 23:21:10
Type        : Information
Source      : acvpnui

Description : An SSL VPN connection to ASA VPN server has been requested by the user.


*******************************************

Date        : 11/04/2014
Time        : 23:21:10
Type        : Information
Source      : acvpnui

Description : Loading preferences for the current user from profile C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\cc


*******************************************

Date        : 11/04/2014
Time        : 23:21:10
Type        : Information
Source      : acvpnui

Description : Current Preference Settings:
ServiceDisable: false
CertificateStoreOverride: false
CertificateStore: All
ShowPreConnectMessage: false
AutoConnectOnStart: false
MinimizeOnConnect: true
LocalLanAccess: false
AutoReconnect: true
AutoReconnectBehavior: DisconnectOnSuspend
UseStartBeforeLogon: false
```

Logs from AnyConnect.txt on Windows

Logs from System.log on MAC

```
2:18:15 am Cisco AnyConnect Secure Mobility Client: Function: OnEventNotify File: ../../vpn/ApiShim/ApiShim.cpp Line: 316 User accepted banner.
2:18:15 am Cisco AnyConnect Secure Mobility Client: VPN state: Connecting Network state: Network Accessible Network control state: Network Access: Available Network type: U
2:18:15 am Cisco AnyConnect Secure Mobility Client: Message type information sent to the user: Establishing VPN session...
2:18:15 am Cisco AnyConnect Secure Mobility Client: The profile configured on the secure gateway is: acvpn.xml
2:18:15 am Cisco AnyConnect Secure Mobility Client: Function: launchCachedDownloader File: ../../vpn/Api/ConnectMgr.cpp Line: 6820 Launching Cached Downloader: path: '/opt/
2:18:15 am Cisco AnyConnect Secure Mobility Client: Function: launchCachedDownloader File: ../../vpn/Api/ConnectMgr.cpp Line: 6839 Invoked Function: ConnectMgr :: launchCac
2:18:15 am acvpndownloader: Cisco AnyConnect Secure Mobility Client Downloader started, version 3.1.06073
```

AnyConnect Troubleshooting Toolbox (iOS, Android)



AnyConnect VPN: ON

Status: Connected

Choose a connection...

- ✓ roddy.labrats.se
- roddy.labrats.se (user)
- Add VPN Connection...

Management

System Information

Debug Logs: OFF

```
[01-09-13 07:02:15:993] <Information> - Waiting for posture assessment to complete...
[01-09-13 07:02:16:093] <Information> - Posture Assessment: Updating...
[01-09-13 07:02:16:196] <Information> - Waiting for posture assessment to complete...
[01-09-13 07:02:16:912] <Information> - Establishing VPN session...
[01-09-13 07:02:17:028] <Information> - Establishing VPN session...
[01-09-13 07:02:17:136] <Information> - Establishing VPN - Initiating connection...
[01-09-13 07:02:17:247] <Information> - Establishing VPN - Examining system...
[01-09-13 07:02:17:421] <Information> - Establishing VPN - Activating VPN adapter...
[01-09-13 07:02:17:705] <Information> - Establishing VPN - Configuring system...
[01-09-13 07:02:17:910] <Information> - Establishing VPN...
[01-09-13 07:02:18:016] <Information> - Connected to roddy.labrats.se.
```

Status Overview

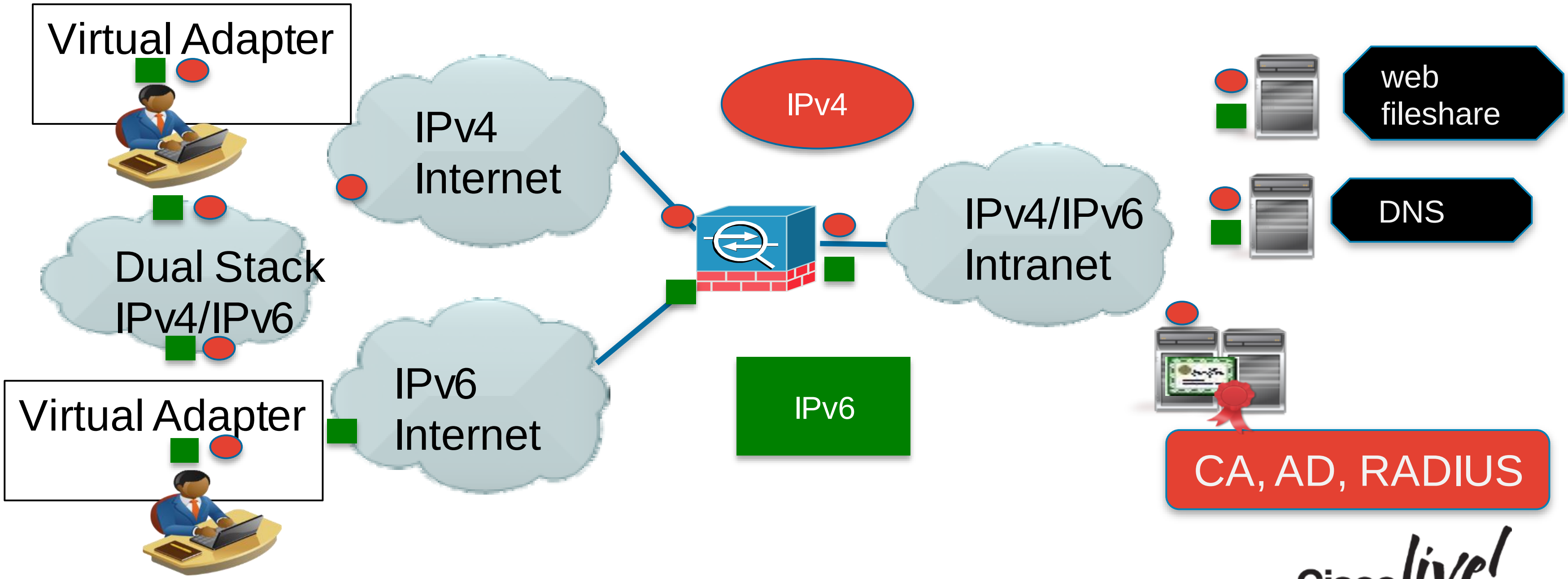
Server	roddy.labrats.se
Time Connected	00:02:13
Client Address	10.99.110.2
Bytes Sent	2524
Bytes Received	3299
Details	›

Possible to view Profiles and Certificates

One click email of logs

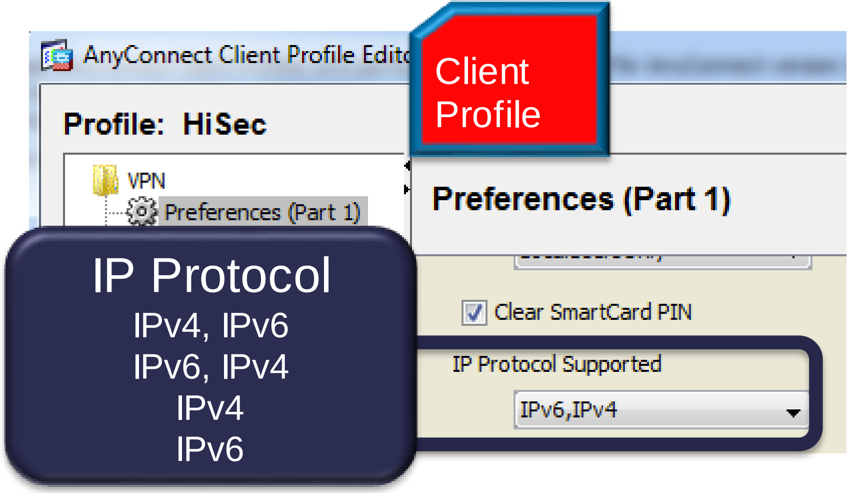
AnyConnect Fundamentals : IPv4 and IPv6

- AnyConnect 3.1 and above supports **IPv6** tunneled inside **IPv4** or **IPv6**
  - management/control servers (CA, AD, RADIUS) IPv4 only



Which IP protocol should be used to Connect to ASA

- A dual-stacked host has the choice of connecting via IPv4 or IPv6
- Default: try to connect to ASA via its IPv4 address first, if that fails try IPv6
- Roaming between IPv6 and IPv4 supported



AnyConnect Client Profile Edito

Client Profile

Profile: HiSec

VPN

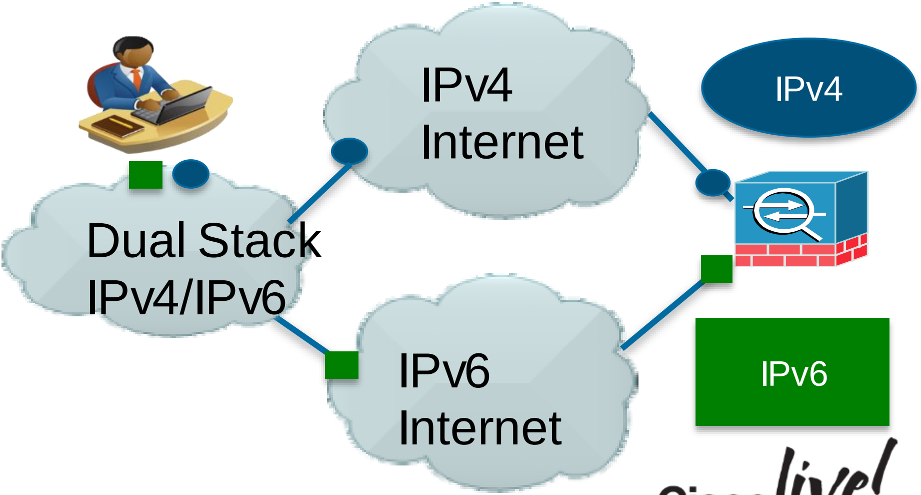
Preferences (Part 1)

Preferences (Part 1)

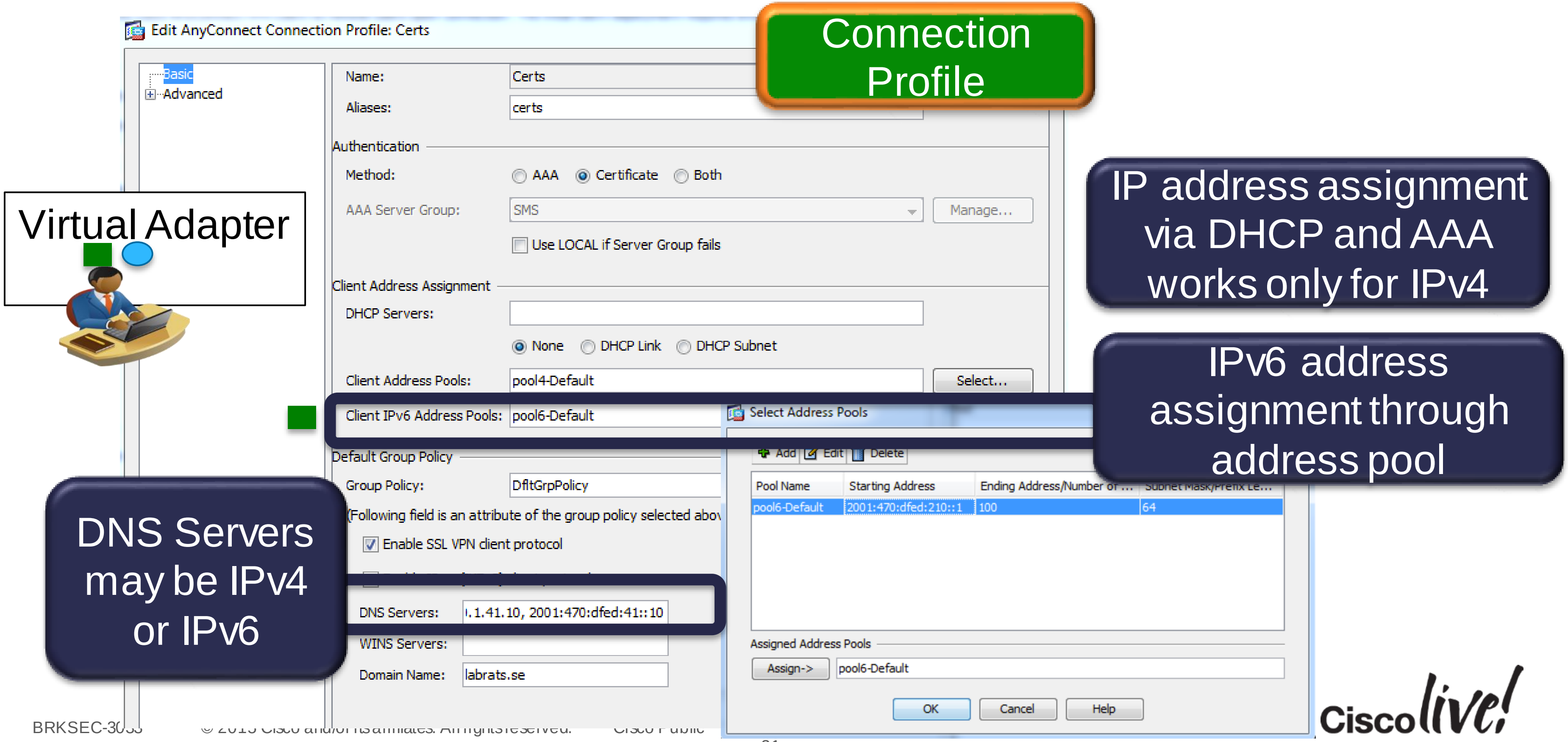
☑ Clear SmartCard PIN

IP Protocol Supported: IPv6,IPv4

IP Protocol
IPv4, IPv6
IPv6, IPv4
IPv4
IPv6



Configuring (inside) IPv6 Address Pools and DNS



Connection Profile

Virtual Adapter

IP address assignment via DHCP and AAA works only for IPv4

IPv6 address assignment through address pool

DNS Servers may be IPv4 or IPv6

Edit AnyConnect Connection Profile: Certs

Name: Certs

Aliases: certs

Authentication

Method: ○ AAA ● Certificate ○ Both

AAA Server Group: SMS

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: pool4-Default

Client IPv6 Address Pools: pool6-Default

Default Group Policy

Group Policy: DfltGrpPolicy

(Following field is an attribute of the group policy selected abov

☑ Enable SSL VPN client protocol

DNS Servers: ı.1.41.10, 2001:470:dfed:41::10

WINS Servers:

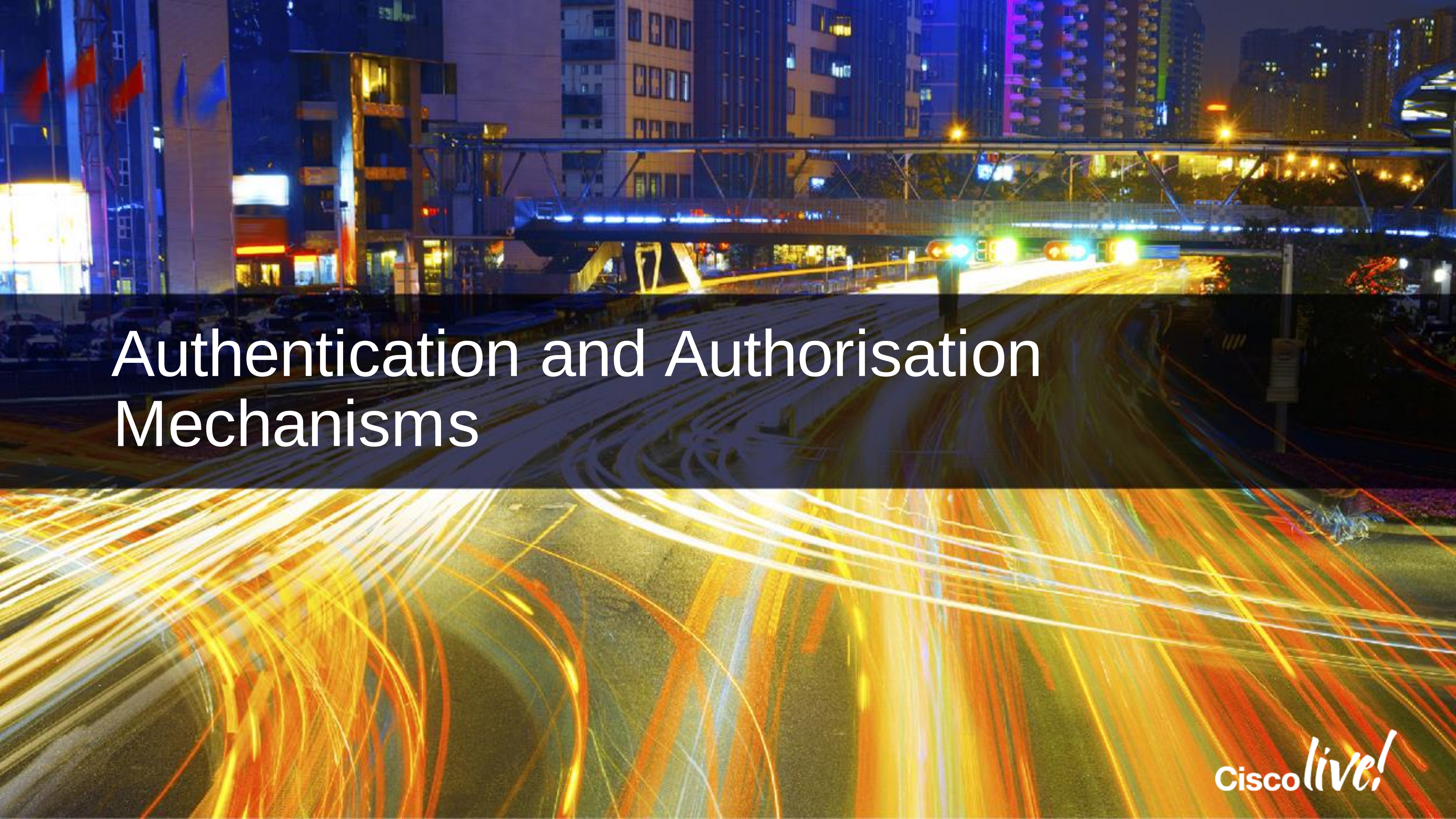
Domain Name: labrats.se

Select Address Pools

Pool Name	Starting Address	Ending Address/Number of ...	Subnet Mask/Prefix Le...
pool6-Default	2001:470:dfed:210::1	100	64

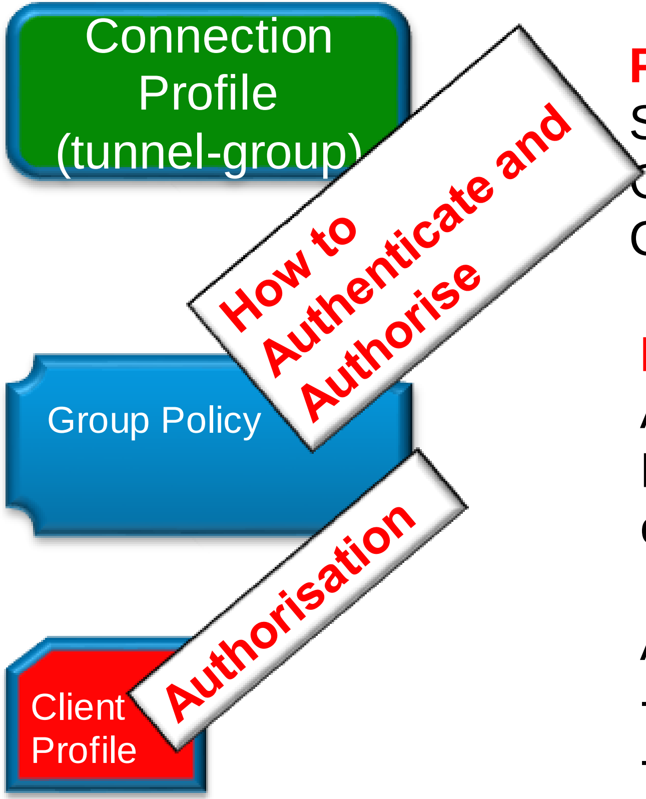
Assigned Address Pools

Assign-> pool6-Default



Authentication and Authorisation Mechanisms

AAA in ASA : Some Important Concepts


Connection Profile (tunnel-group)
How to Authenticate and Authorise
Group Policy
Authorisation
Client Profile

Proving Who you are

Static Passwords (local to ASA, Active Directory, LDAP)

OTP (One-Time-Passwords), typically RADIUS

Certificates

Determining What You are and What You can do

ACL, Split Tunnelling

Proxy settings, Timeouts

etc..

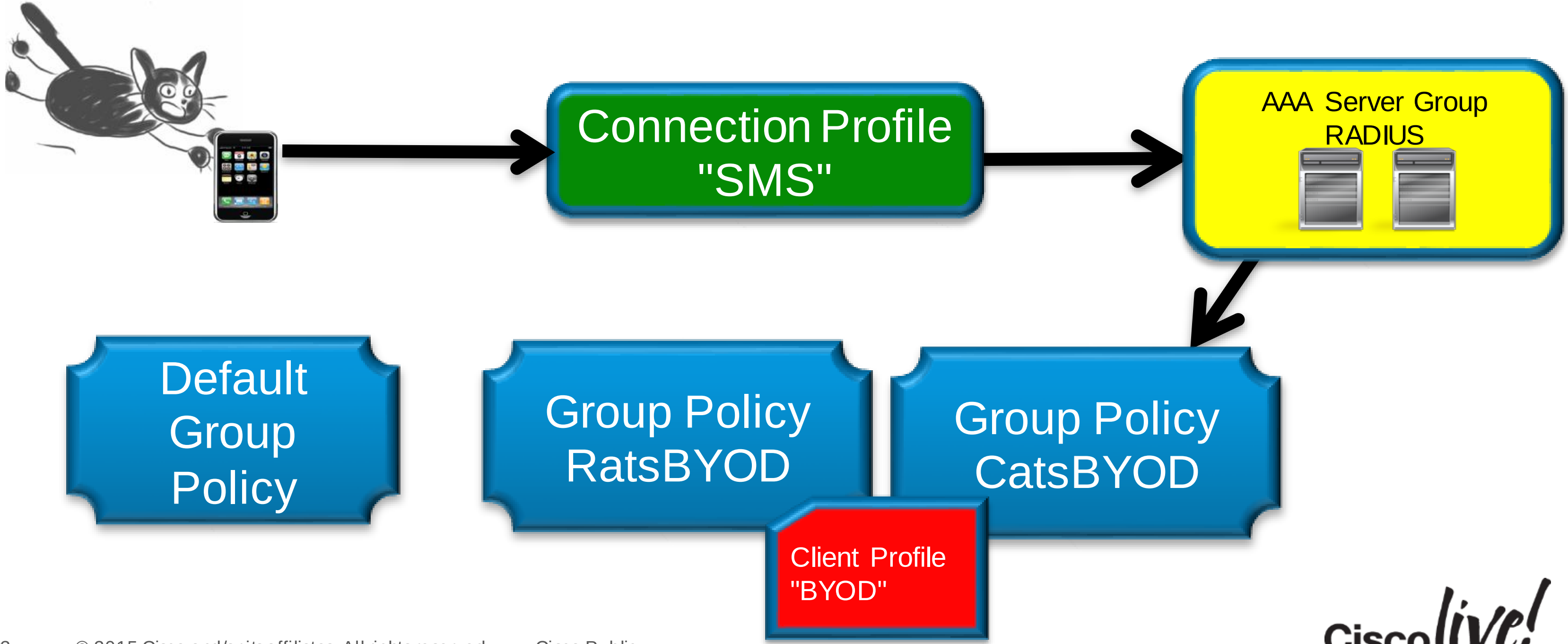
AnyConnect behaviour...

- Which ASA and Connection Profile to connect to
- "Always On"

- which certificate to use, etc...

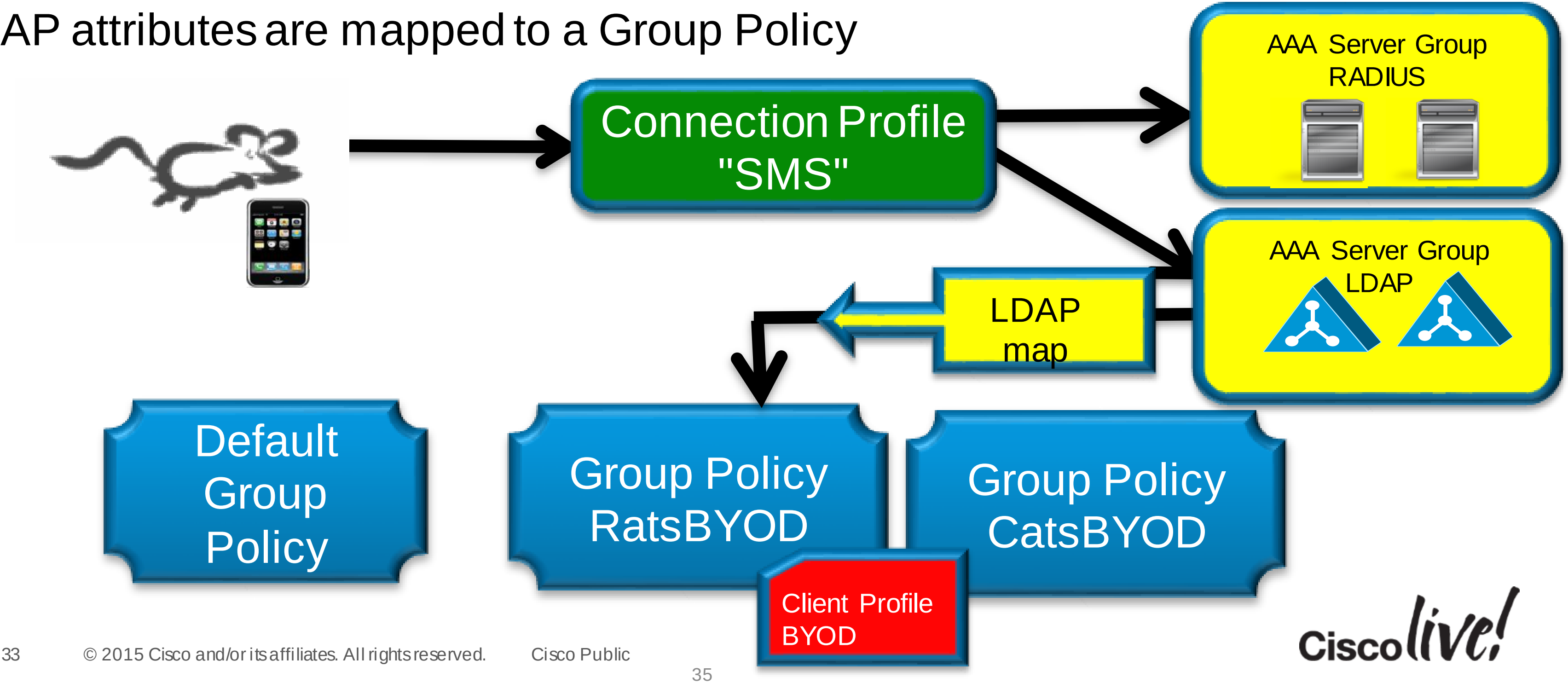
Authentication and Authorisation by RADIUS

- User can be authenticated and authorised by RADIUS.
- RADIUS attribute IETF 25 (Class) is used to assign the group policy.



Authentication by RADIUS Authorisation by LDAP

- User authenticated by RADIUS (typically strong authentication, OTP)
- Username used for LDAP lookup
- LDAP attributes are mapped to a Group Policy



Connection Profile "SMS"

AAA Server Group RADIUS

AAA Server Group LDAP

LDAP map

Default Group Policy

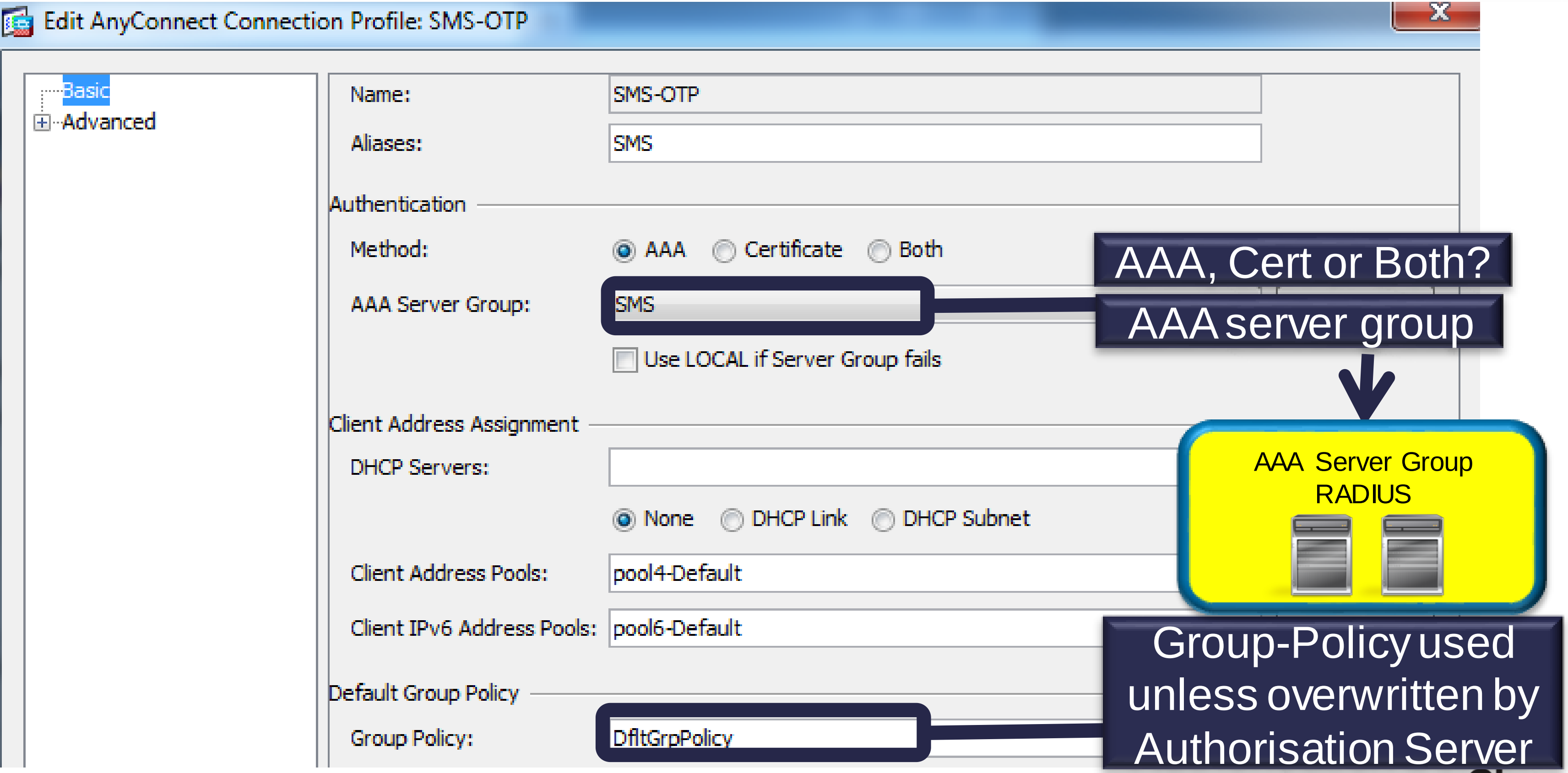
Group Policy RatsBYOD

Group Policy CatsBYOD

Client Profile BYOD

Connection Profile : How to Authenticate

Connection Profile



Edit AnyConnect Connection Profile: SMS-OTP

Name: SMS-OTP

Aliases: SMS

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: SMS

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: pool4-Default

Client IPv6 Address Pools: pool6-Default

Default Group Policy

Group Policy: DfltGrpPolicy

AAA, Cert or Both?

AAA server group

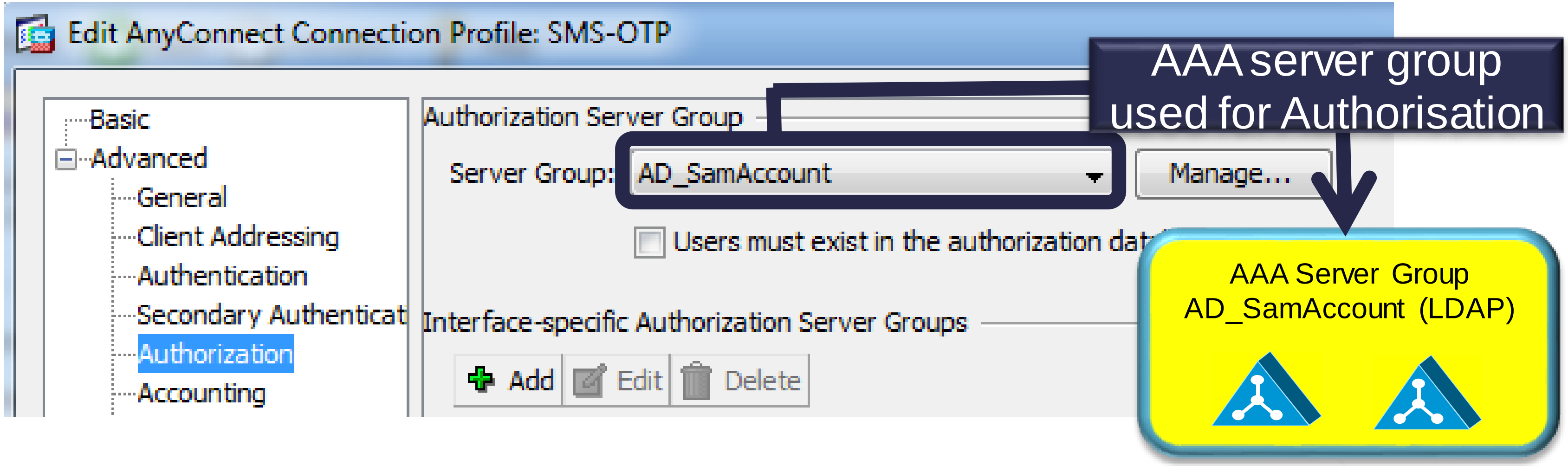
AAA Server Group RADIUS

Group-Policy used unless overwritten by Authorisation Server

Connection Profile : How to Authorise

Connection Profile

- Possible to define different AAA server group for authorisation (if not specified, the same group is used for authentication and authorisation).



Edit AnyConnect Connection Profile: SMS-OTP

Authorization Server Group

Server Group: AD_SamAccount

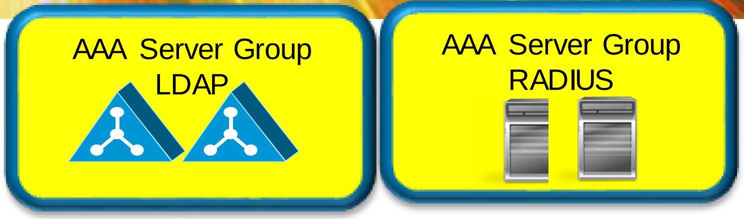
□ Users must exist in the authorization dat

Interface-specific Authorization Server Groups

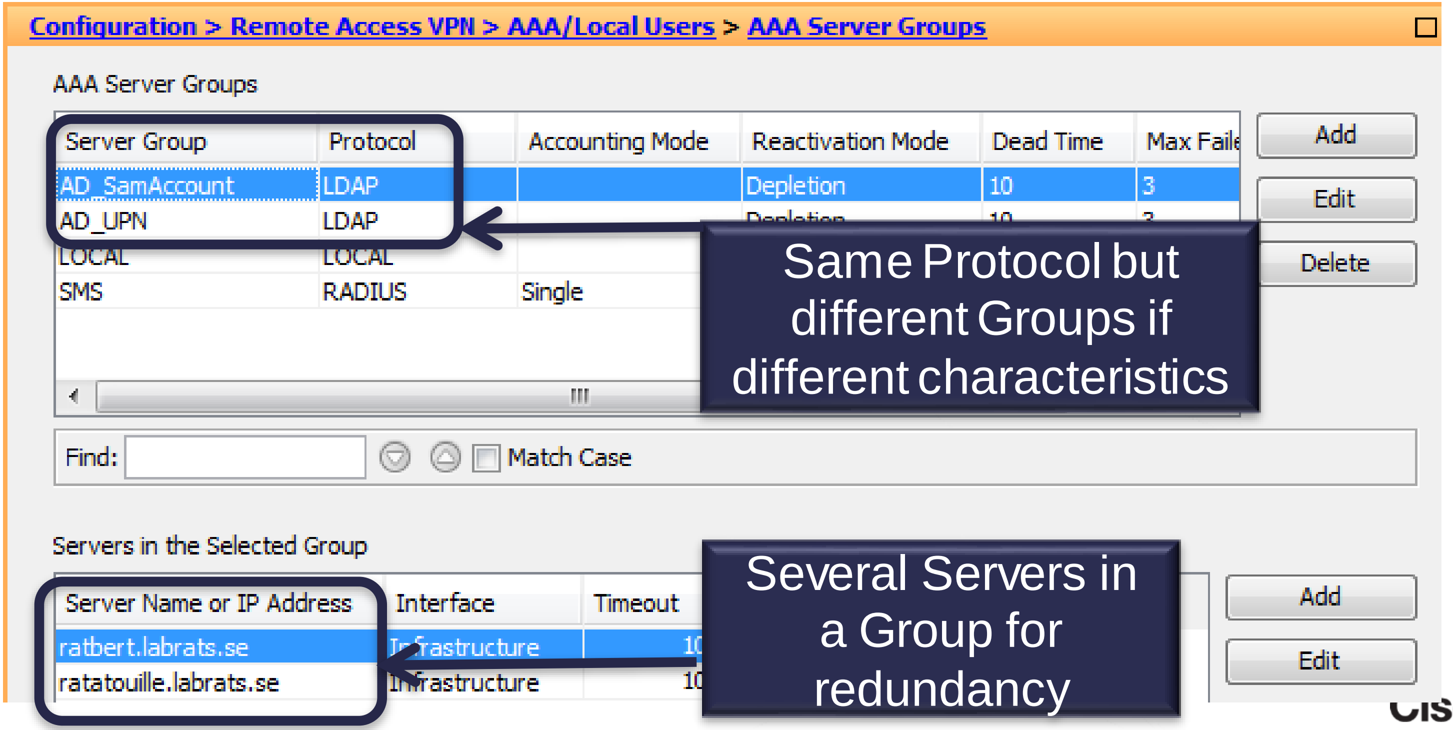
AAA server group used for Authorisation

AAA Server Group AD_SamAccount (LDAP)

AAA Server Groups



- Using the same authentication protocol and characteristics



Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Faile
AD_SamAccount	LDAP		Depletion	10	3
AD_UPN	LDAP		Depletion	10	3
LOCAL	LOCAL				
SMS	RADIUS	Single			

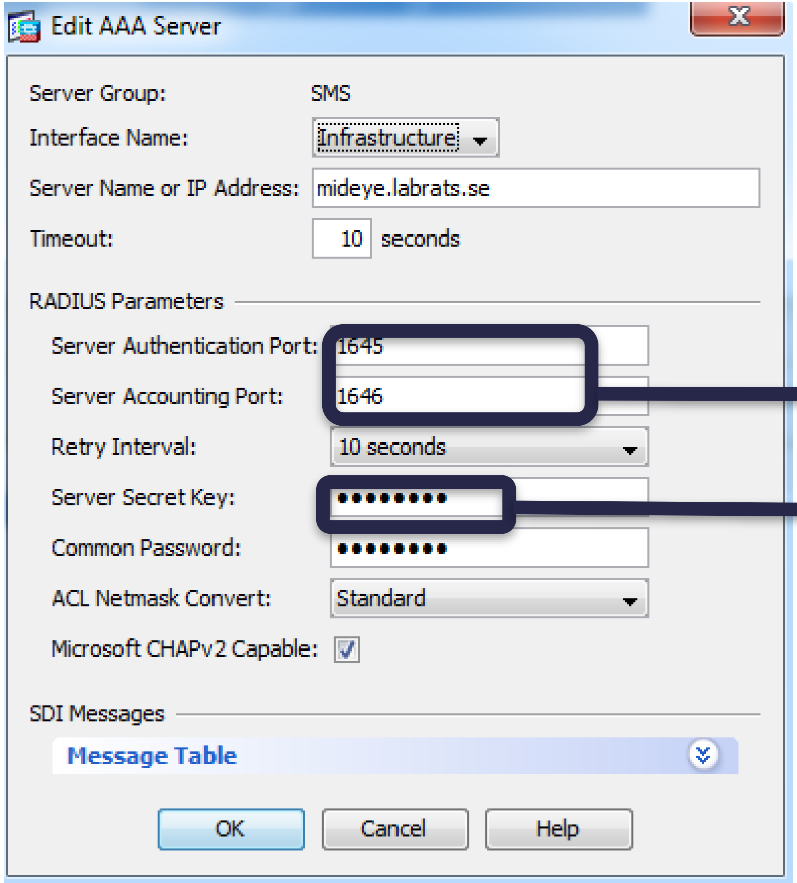
Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
ratbert.labrats.se	Infrastructure	10
ratatouille.labrats.se	Infrastructure	10

Same Protocol but different Groups if different characteristics

Several Servers in a Group for redundancy

RADIUS Server Definition



Edit AAA Server

Server Group: SMS

Interface Name: Infrastructure

Server Name or IP Address: mideye.labrats.se

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: •••••••••

Common Password: •••••••••

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable: ☑

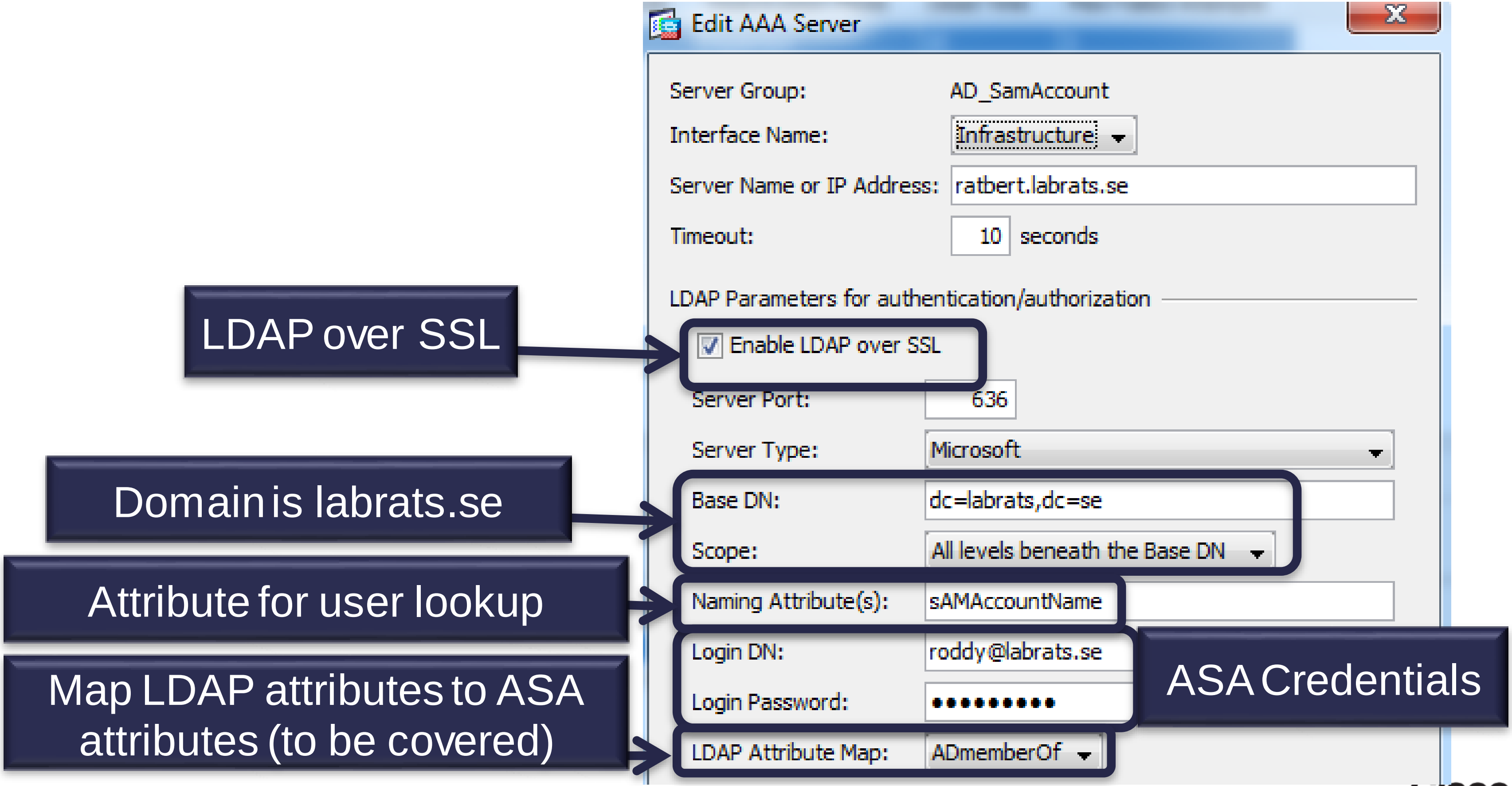
SDI Messages

Message Table

Double check port numbers on RADIUS server

Shared Secret must match with RADIUS server

LDAP Server Definition (Active Directory)



Edit AAA Server

Server Group: AD_SamAccount

Interface Name: Infrastructure

Server Name or IP Address: ratbert.labrats.se

Timeout: 10 seconds

LDAP Parameters for authentication/authorization

☑ Enable LDAP over SSL

Server Port: 636

Server Type: Microsoft

Base DN: dc=labrats,dc=se

Scope: All levels beneath the Base DN

Naming Attribute(s): sAMAccountName

Login DN: roddy@labrats.se

Login Password: ••••••••••

LDAP Attribute Map: ADmemberOf

LDAP over SSL

Domain is labrats.se

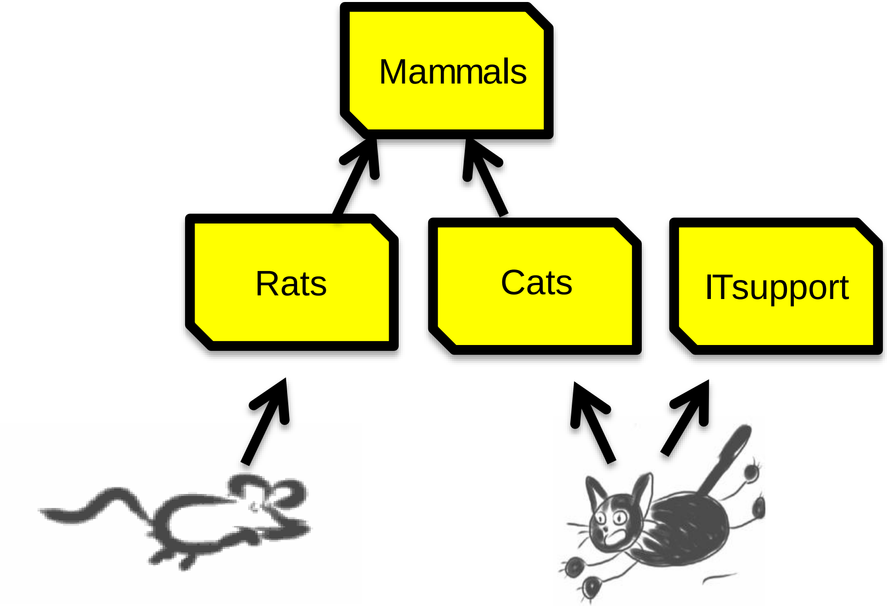
Attribute for user lookup

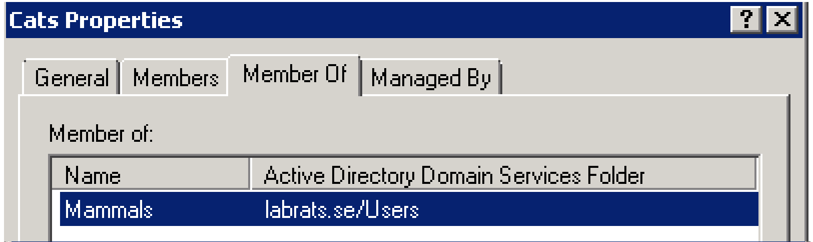
Map LDAP attributes to ASA attributes (to be covered)

ASA Credentials

Using Active Directory “memberOf”

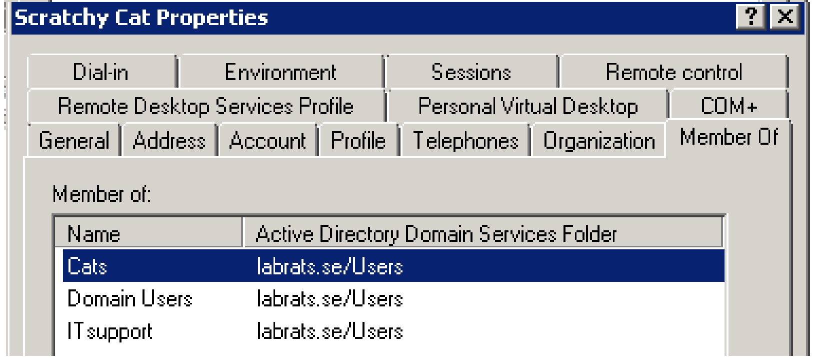
- A user in Active Directory can be a member of **many** groups
  - But can only belong **one** Group Policy in ASA
- A group may be a member of another group in AD
  - ASA will not do recursive lookup





Member of:

Name	Active Directory Domain Services Folder
Mammals	labrats.se/Users



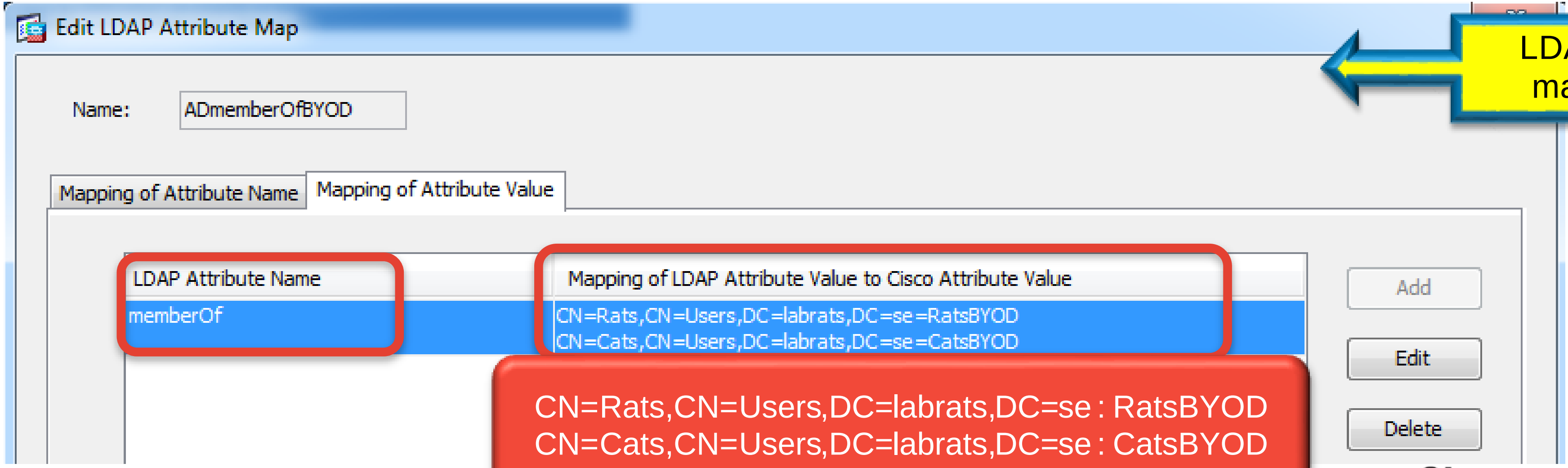
Member of:

Name	Active Directory Domain Services Folder
Cats	labrats.se/Users
Domain Users	labrats.se/Users
IT support	labrats.se/Users

Mapping “memberOf” to Group Policy

- Map “memberOf” to ASA Group Policy with an LDAP attribute map
- **Beware:** First match will apply (many memberOf → one Group Policy)
- **Beware:** No support for lookup of nested groups (“group in group”)
- Using Cisco ISE allows for better flexibility in assigning Group Policy
- DAP (covered later) allows for more flexibility in handling "many memberOf"

Warning



Name: ADmemberOfBYOD

LDAP Attribute Name	Mapping of LDAP Attribute Value to Cisco Attribute Value

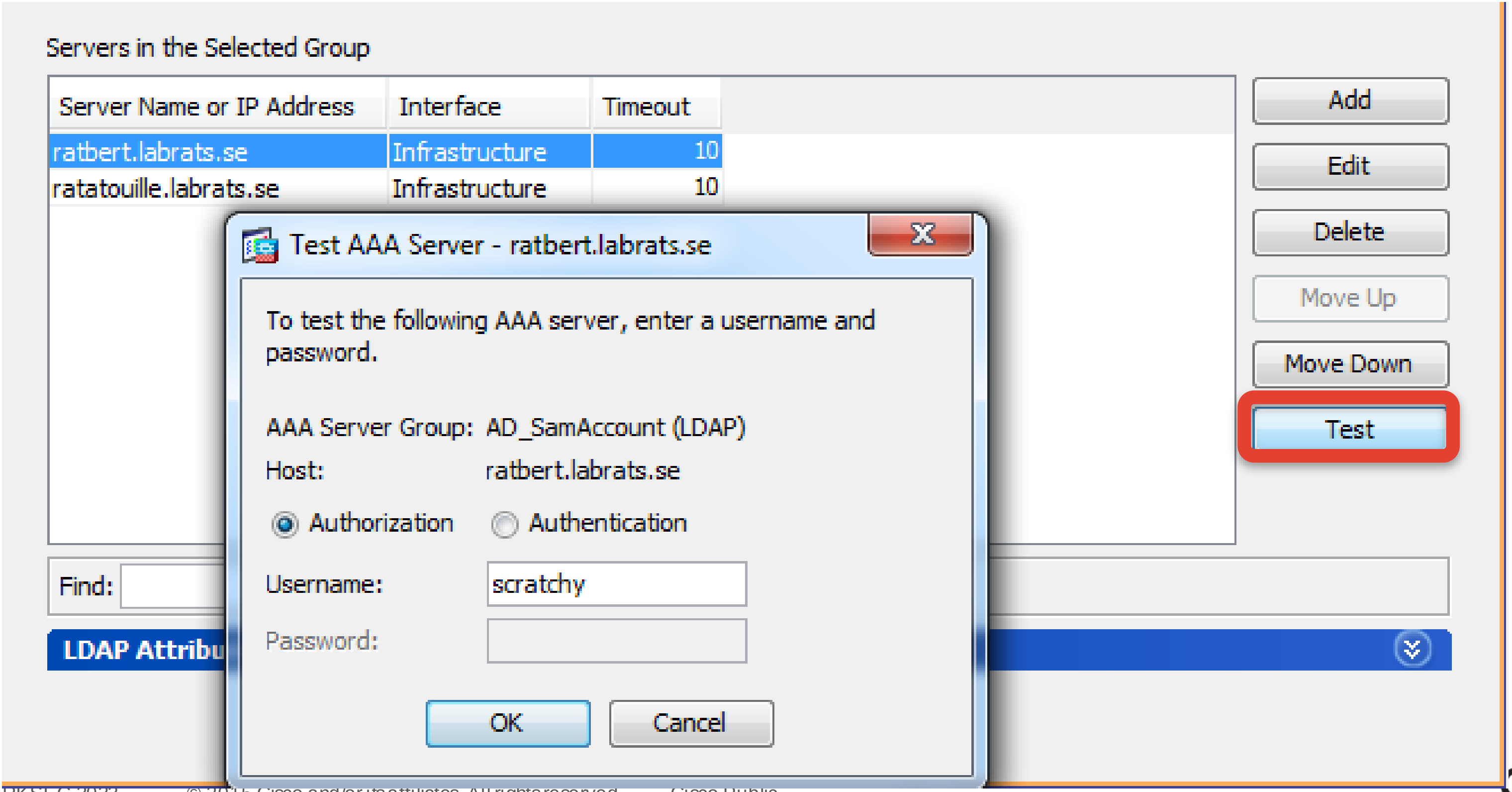
memberOf	CN=Rats,CN=Users,DC=labrats,DC=se=RatsBYOD
	CN=Cats,CN=Users,DC=labrats,DC=se=CatsBYOD

LDAP map

CN=Rats,CN=Users,DC=labrats,DC=se : RatsBYOD
CN=Cats,CN=Users,DC=labrats,DC=se : CatsBYOD

Troubleshooting AAA Server

- Test that AAA server works



Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
ratbert.labrats.se	Infrastructure	10
ratatouille.labrats.se	Infrastructure	10

Test AAA Server - ratbert.labrats.se

To test the following AAA server, enter a username and password.

AAA Server Group: AD_SamAccount (LDAP)

Host: ratbert.labrats.se

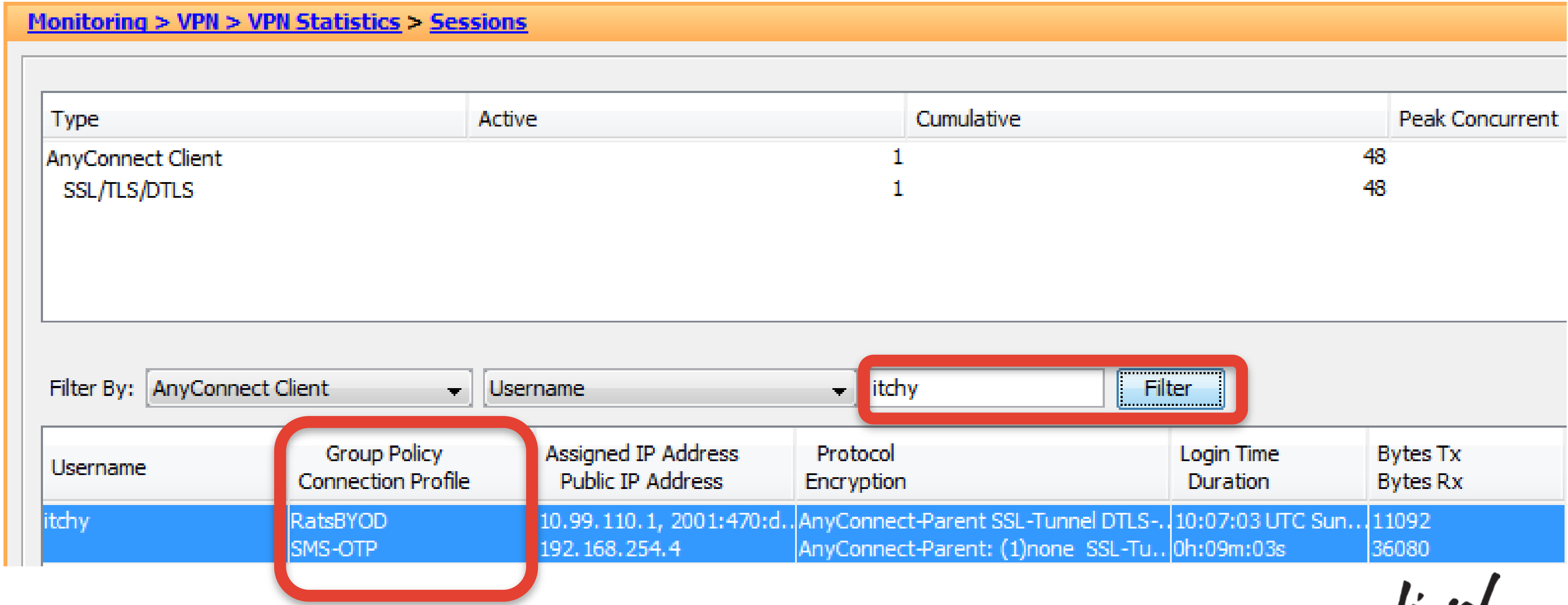
● Authorization ○ Authentication

Username: scratchy

Password:

Troubleshooting AAA

- Checking that the right Group Policy has been assigned



Monitoring > VPN > VPN Statistics > Sessions

Type	Active	Cumulative	Peak Concurrent
AnyConnect Client	1	48	
SSL/TLS/DTLS	1	48	

Filter By: AnyConnect Client | Username | itchy | Filter

Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
itchy	RatsBYOD SMS-OTP	10.99.110.1, 2001:470:d... 192.168.254.4	AnyConnect-Parent SSL-Tunnel DTLS-... AnyConnect-Parent: (1)none SSL-Tu...	10:07:03 UTC Sun... 0h:09m:03s	11092 36080

Troubleshooting RADIUS : debug radius (1)

```
roddy(config)# sh debug
debug radius session
debug radius decode
roddy(config)# radius mkreq: 0xa1......
got user 'scratchy'    got password
add_req 0xade2da48 session 0xa1 id 80
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=192.168.254.4

RADIUS packet decode (authentication request)
--------------------------------------
Raw packet data (length = 172).....
01 50 00 ac 10 09 0e 2f 3c c5 1a 4b 28 41 e6 27    | .P...../<..K(A.'
d4 7d 72 c3 01 0a 73 63 72 61 74 63 68 79 02 12    | .}r...scratchy..
67 58 f2 72 53 db 00 ee 29 1a 49 b4 f1 c7 1a c7    | gX.rS...).I.....
05 06 00 04 b0 00 1e 0f 31 39 32 2e 31 36 38 2e    | ........192.168.
31 31 30 2e 31 1f 0f 31 39 32 2e 31 36 38 2e 32    | 110.1..192.168.2
35 34 2e 34 3d 06 00 00 00 05 42 0f 31 39 32 2e    | 54.4=.....B.192.
31 36 38 2e 32 35 34 2e 34 04 06 0a 01 29 6e 1a    | 168.254.4....)n.
22 00 00 00 09 01 1c 69 70 3a 73 6f 75 72 63 65    | "......ip:source
2d 69 70 3d 31 39 32 2e 31 36 38 2e 32 35 34 2e    | -ip=192.168.254.
34 1a 0f 00 00 0c 04 92 09 53 4d 53 2d 4f 54 50    | 4........SMS-OTP
1a 0c 00 00 0c 04 96 06 00 00 00 02                | ............
```

Access-Request from ASA to RADIUS Server

Troubleshooting RADIUS : debug radius (2)

```
Parsed packet data.....
.........
..........
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 15 (0x0F)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
53 4d 53 2d 4f 54 50                              | SMS-OTP
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
send pkt 10.1.41.51/1645
```

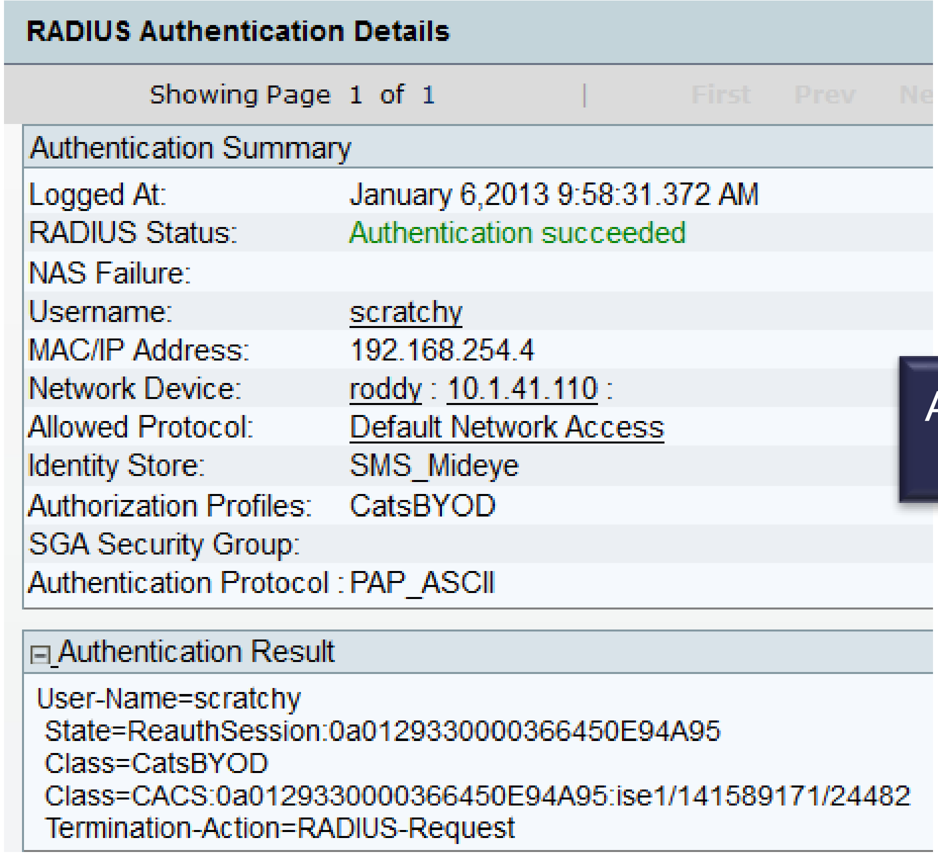
ASA also sends Connection Profile (Tunnel-Group) and Client-Type (AnyConnect) to RADIUS Server in ACCESS-REQUEST

Troubleshooting RADIUS : debug radius (3)

```
RADIUS packet decode (response)
--------------------------------------
Raw packet data (length = 142).....
02 51 00 8e 13 94 12 5d 9c 56 84 ab bc 99 85 0d   | .Q.....].V......
6a 71 7b 18 01 0a 73 63 72 61 74 63 68 79 18 28   | jq{...scratchy.(
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61   | ReauthSession:0a
30 31 32 39 33 33 30 30 30 30 33 35 31 45 35 30   | 0129330000351E50
44 42 33 31 35 42 19 0e 52 65 73 65 61 72 63 68   | DB315B..Research
42 59 4f 44 19 34 43 41 43 53 3a 30 61 30 31 32   | BYOD.4CACS:0a012
39 33 33 30 30 30 30 33 35 31 45 35 30 44 42 33   | 9330000351E50DB3
31 35 42 3a 69 73 65 31 2f 31 34 31 35 38 39 31   | 15B:ise1/1415891
37 31 2f 32 32 34 33 31 1d 06 00 00 00 01         | 71/22431......

Parsed packet data.....
.........
Radius: Type = 25 (0x19) Class
Radius: Length = 14 (0x0E)
Radius: Value (String) =
43 61 74 73 42 59 4f 44                           | CatsBYOD
.......
Radius: Type = 29 (0x1D) Termination-Action
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT:  normal termination
```

RADIUS server may assign Group Policy with the Class attribute

Troubleshooting RADIUS



RADIUS Authentication Details

Showing Page 1 of 1 | First Prev Ne

Authentication Summary

Logged At:	January 6,2013 9:58:31.372 AM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	scratchy
MAC/IP Address:	192.168.254.4
Network Device:	roddy : 10.1.41.110 :
Allowed Protocol:	Default Network Access
Identity Store:	SMS_Mideye
Authorization Profiles:	CatsBYOD
SGA Security Group:	
Authentication Protocol :	PAP_ASCII

⊟ Authentication Result

```
User-Name=scratchy
 State=ReauthSession:0a0129330000366450E94A95
 Class=CatsBYOD
 Class=CACS:0a0129330000366450E94A95:ise1/141589171/24482
 Termination-Action=RADIUS-Request
```

Authentication logs from Cisco ISE

Troubleshooting LDAP

debug ldap

```
roddy(config)# debug ldap 100
debug ldap  enabled at level 100
roddy(config)#
[42] Session Start
[42] New request Session, context 0xaddbaacc, reqType = Other
[42] Fiber started
[42] Creating LDAP context with uri=ldaps://10.1.41.10:636
[42] Connect to LDAP server: ldaps://10.1.41.10:636, status = Successful
[42] supportedLDAPVersion: value = 3
[42] supportedLDAPVersion: value = 2
[42] Binding as roddy@labrats.se
[42] Performing Simple authentication for roddy@labrats.se to 10.1.41.10

[42] LDAP Search:       Base DN = [dc=labrats,dc=se]       Filter  =
[sAMAccountName=scratchy]       Scope   = [SUBTREE]
[42] User DN = [CN=Scratchy Cat,CN=Users,DC=labrats,DC=se]
```

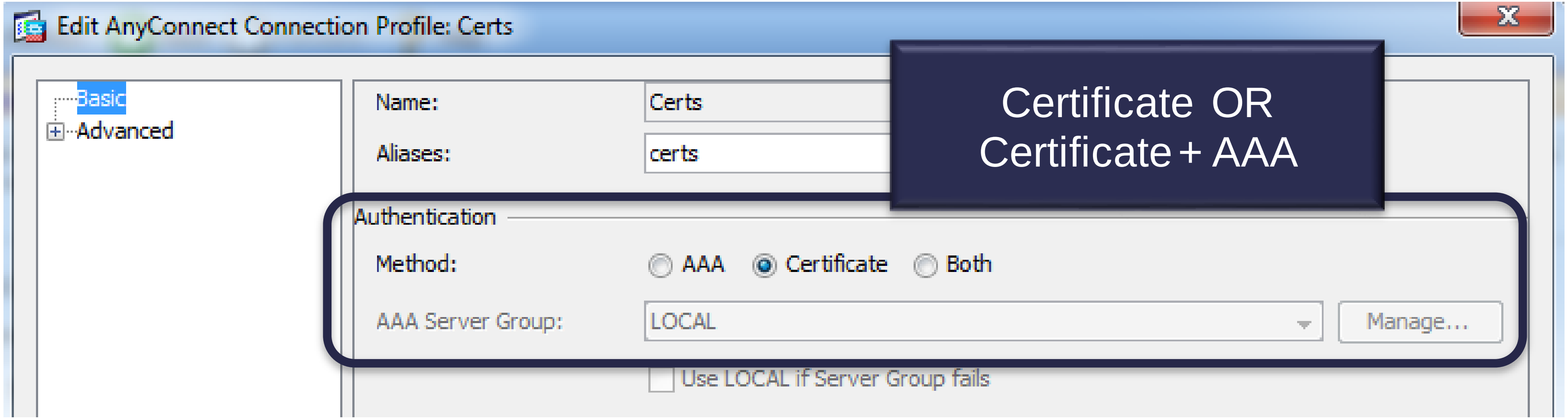
Connect (layer 4)

Bind (authentication)

LDAP search

Authentication with Client Certificates

- Defined in Connection Profile
- Choosing "both" means that user first has to authenticate with certificate, then with username/password
  – Use case : Checking that user uses a corporate machine (with a soft certificate)



Edit AnyConnect Connection Profile: Certs

Name: Certs

Aliases: certs

Authentication

Method: ○ AAA ● Certificate ○ Both

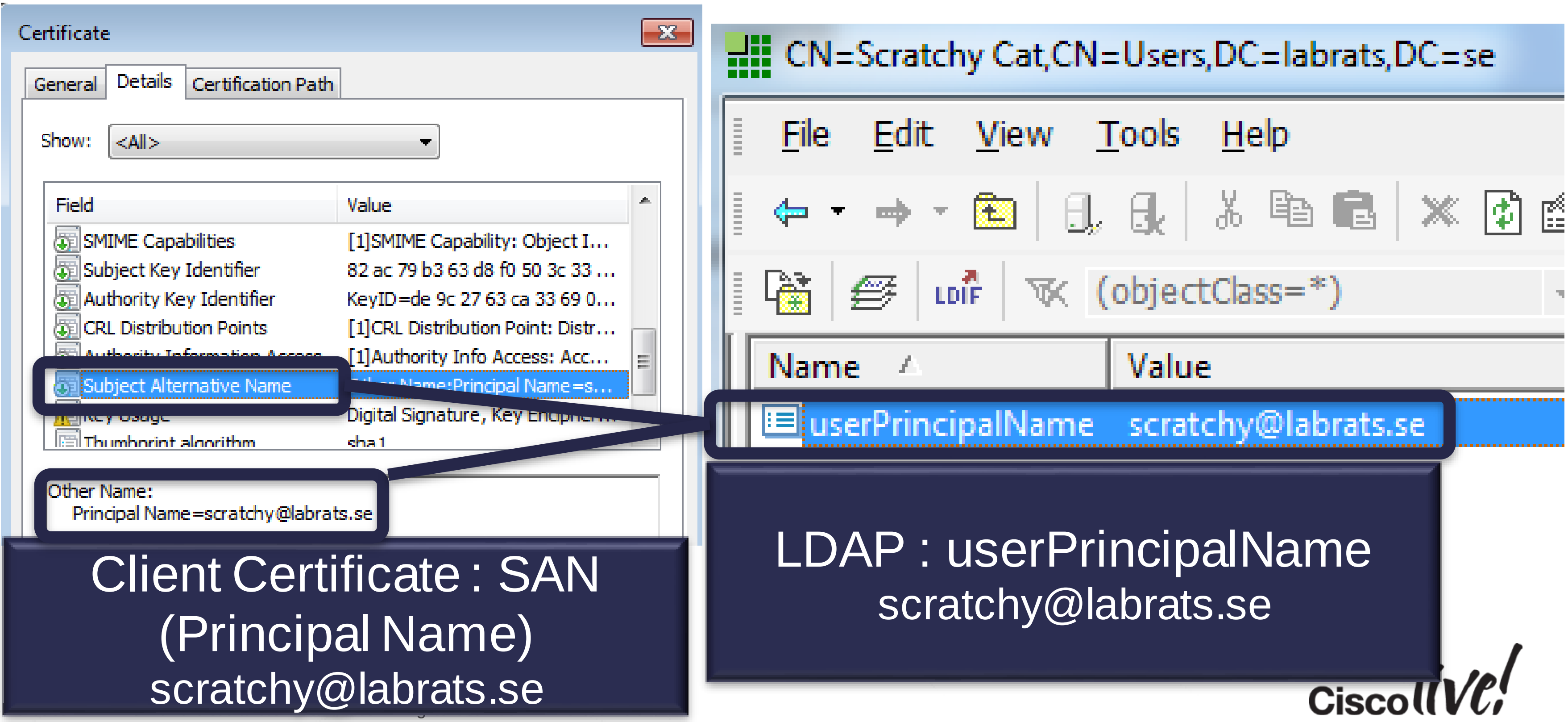
AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Certificate OR
Certificate + AAA

Authorisation with Client Certificates

- Work out which fields in cert to use and how to map to LDAP



Field	Value
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	82 ac 79 b3 63 d8 f0 50 3c 33 ...
Authority Key Identifier	KeyID=de 9c 27 63 ca 33 69 0...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=s...
Key Usage	Digital Signature, Key Encipherm...
Thumbprint algorithm	sha1

Other Name:
Principal Name=scratchy@labrats.se

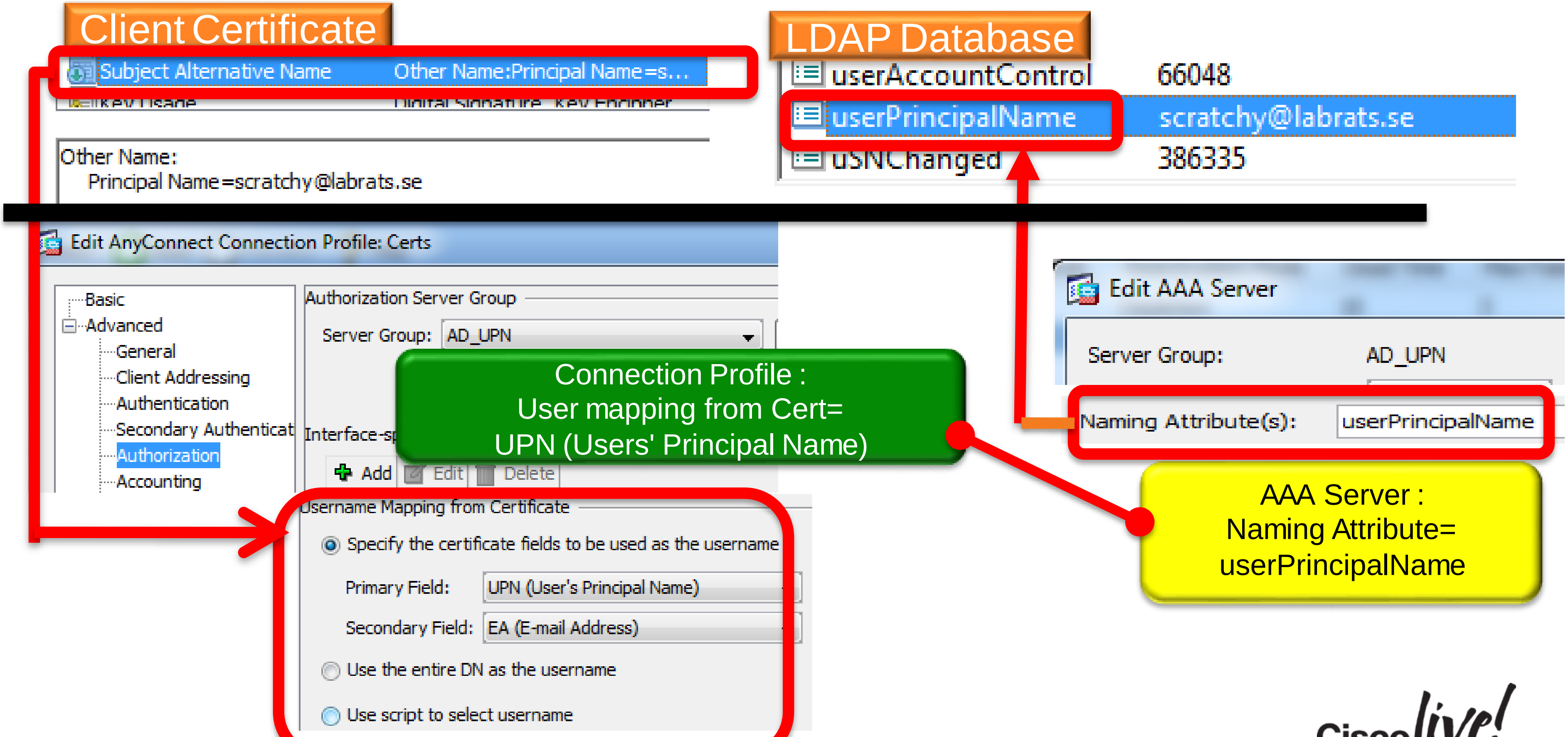
CN=Scratchy Cat,CN=Users,DC=labrats,DC=se

Name	Value
userPrincipalName	scratchy@labrats.se

Client Certificate : SAN (Principal Name)
scratchy@labrats.se

LDAP : userPrincipalName
scratchy@labrats.se

Authorisation with Client Certificates



Client Certificate

Subject Alternative Name   Other Name:Principal Name=s...

Key Usage   Digital Signature, Key Encipher

Other Name:
Principal Name=scratchy@labrats.se

LDAP Database

userAccountControl	66048
userPrincipalName	scratchy@labrats.se
uSNChanged	386335

Edit AnyConnect Connection Profile: Certs

Authorization Server Group

Server Group: AD_UPN

Username Mapping from Certificate

● Specify the certificate fields to be used as the username

Primary Field: UPN (User's Principal Name)

Secondary Field: EA (E-mail Address)

○ Use the entire DN as the username

○ Use script to select username

Connection Profile :
User mapping from Cert=
UPN (Users' Principal Name)

Edit AAA Server

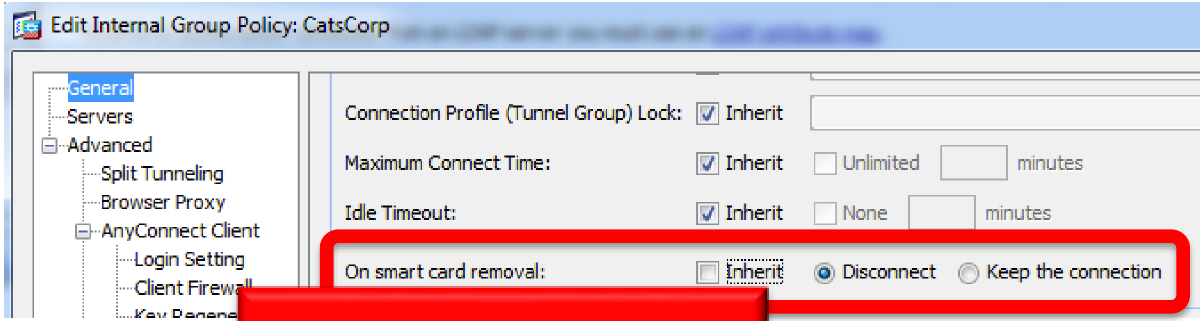
Server Group: AD_UPN

Naming Attribute(s): userPrincipalName

AAA Server :
Naming Attribute=
userPrincipalName

A smart card is just another client certificate

- Same principles and configuration as for soft client certificates
- …with the option of having AnyConnect disconnecting VPN when smart card is removed (configured under Group Policy/General)
- ASA/AnyConnect currently do not support “double” cert authentication
  - First with computer certificate, then with user certificate/smart card
  - Workaround : Use Posture checks to verify that it is corporate machine



Edit Internal Group Policy: CatsCorp

Connection Profile (Tunnel Group) Lock: ☑ Inherit

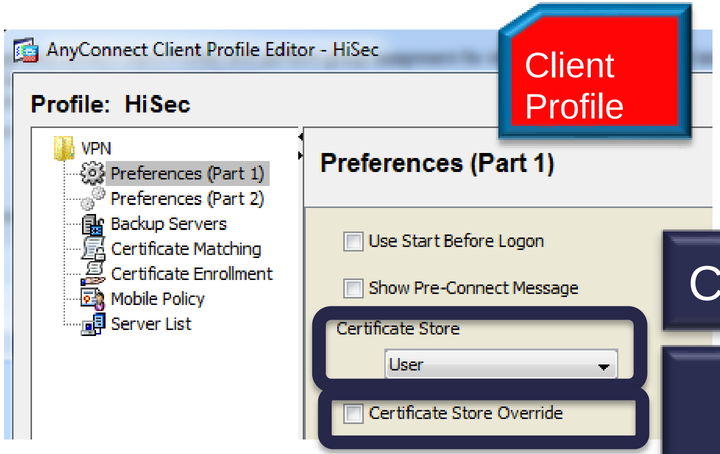
Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ None minutes

On smart card removal: □ Inherit ● Disconnect ○ Keep the connection

Optionally disconnect if Smartcard is removed

Client profile options to select the right certificate



AnyConnect Client Profile Editor - HiSec

Profile: HiSec

- VPN
  - Preferences (Part 1)
  - Preferences (Part 2)
  - Backup Servers
  - Certificate Matching
  - Certificate Enrollment
  - Mobile Policy
  - Server List

Preferences (Part 1)

☐ Use Start Before Logon

☐ Show Pre-Connect Message

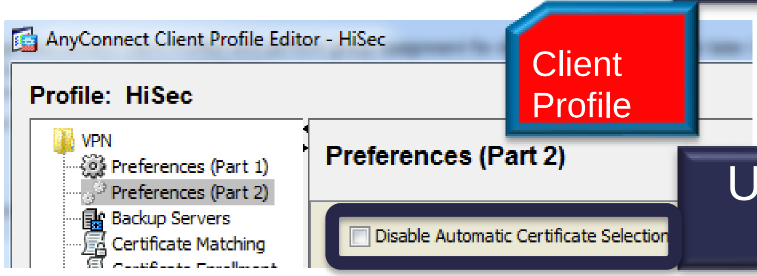
Certificate Store: User

☐ Certificate Store Override

Client Profile

Certificate Store : User, Machine or All

Certificate Store Override : Check if non administrator needs access to machine certificate



AnyConnect Client Profile Editor - HiSec

Profile: HiSec

- VPN
  - Preferences (Part 1)
  - Preferences (Part 2)
  - Backup Servers
  - Certificate Matching

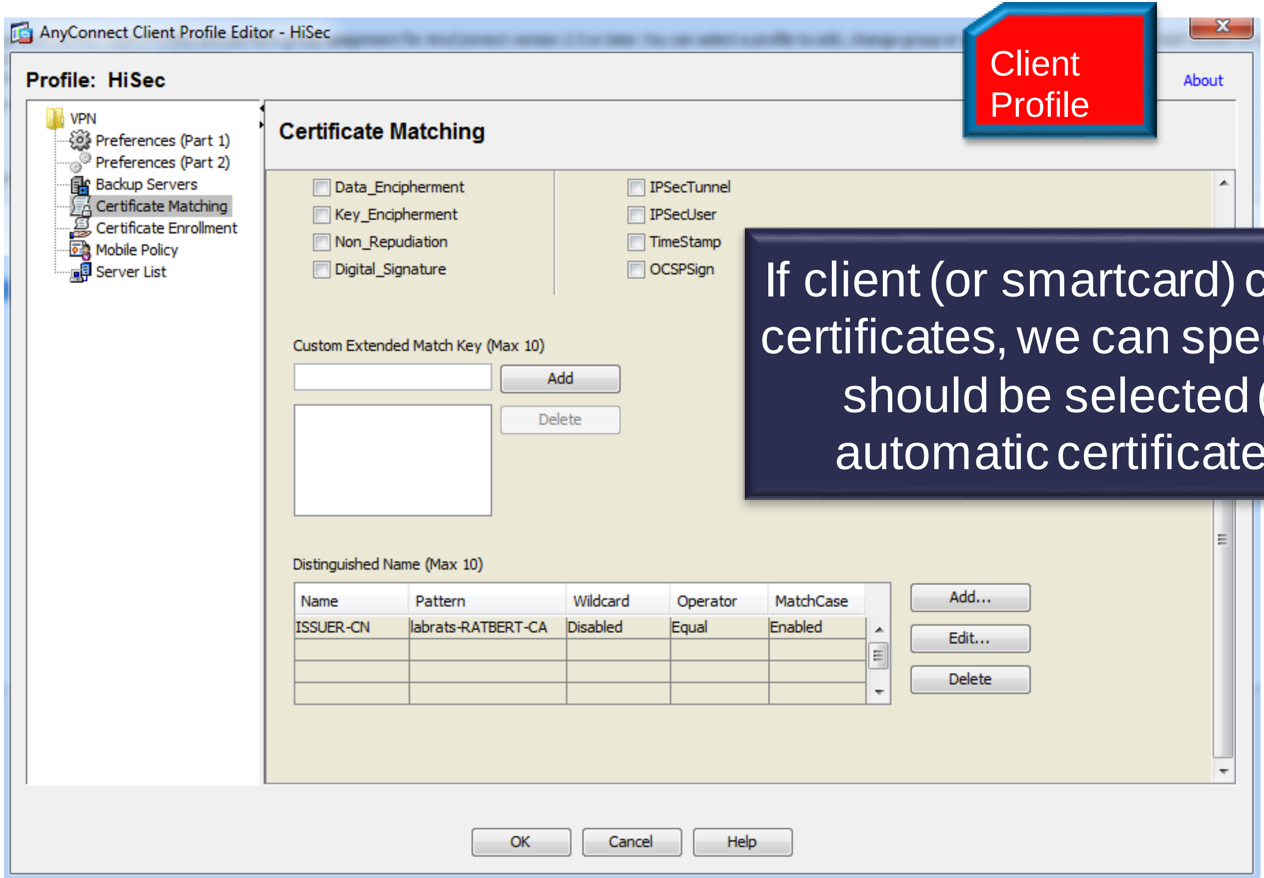
Preferences (Part 2)

☐ Disable Automatic Certificate Selection

Client Profile

Uncheck for Automatic certificate Selection

Certificate Matching (for automatic cert selection)



Certificate Matching

□ Data_Encipherment
□ Key_Encipherment
□ Non_Repudiation
□ Digital_Signature
□ IPSecTunnel
□ IPSecUser
□ TimeStamp
□ OCSPSign

Custom Extended Match Key (Max 10)

Distinguished Name (Max 10)

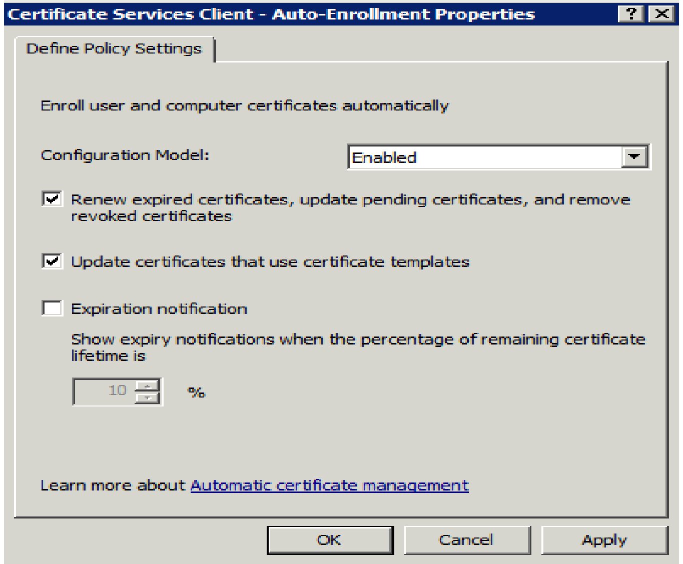
Name	Pattern	Wildcard	Operator	MatchCase
ISSUER-CN	labrats-RATBERT-CA	Disabled	Equal	Enabled

Client Profile

If client (or smartcard) contains many certificates, we can specify which one should be selected (used with automatic certificate selection)

Certificate Enrollment : Active Directory

- Microsoft Active Directory supports automatic certificate enrolment for user and machine certificates
- User and machine are members of Active Directory Domain: Their certificates can be pushed by GPOs (Group Policy Objects)



Certificate Services Client - Auto-Enrollment Properties

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

☐ Expiration notification

Show expiry notifications when the percentage of remaining certificate lifetime is

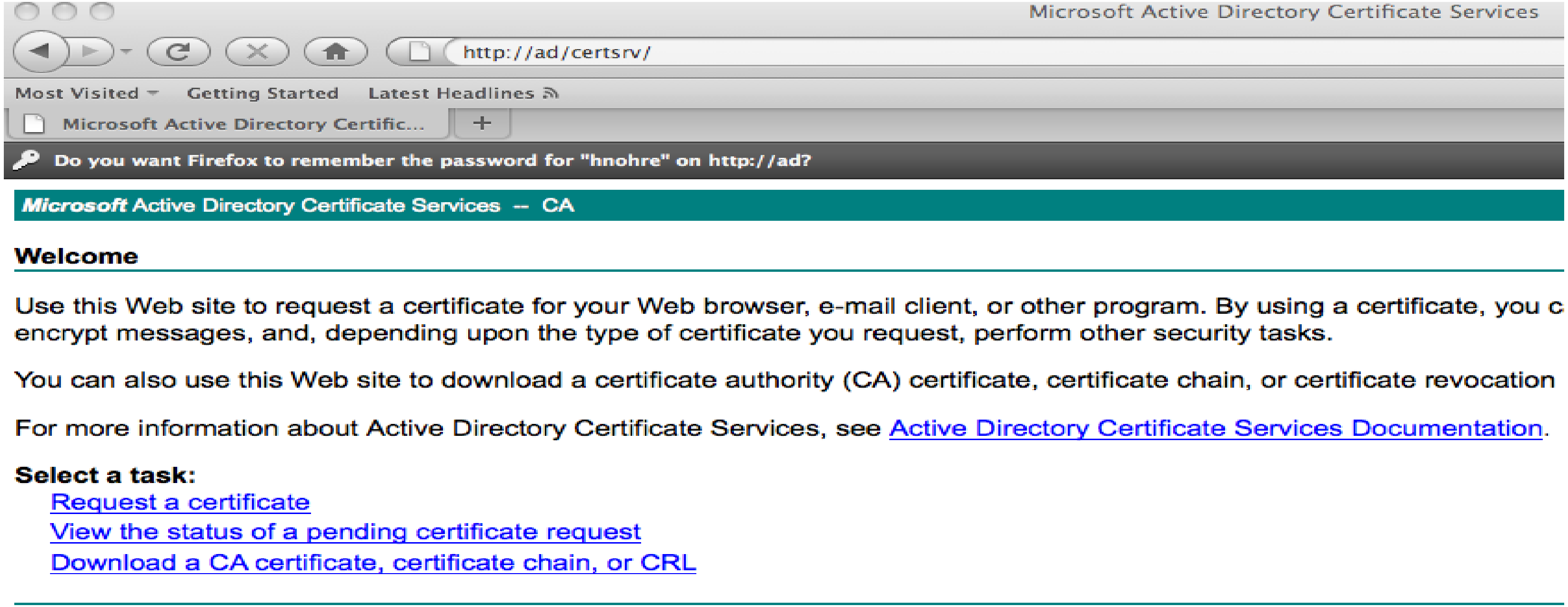
10 %

Learn more about Automatic certificate management

http://technet.microsoft.com/en-us/library/cc770546.aspx

Certificate Enrollment : Active Directory (2)

- Microsoft CA also supports web enrolment
- Can be used by non-domain members, e.g. MACs



Microsoft Active Directory Certificate Services
http://ad/certsrv/
Most Visited
Getting Started
Latest Headlines
Microsoft Active Directory Certific...
+

Do you want Firefox to remember the password for "hnohre" on http://ad?

Microsoft Active Directory Certificate Services -- CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you c encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation

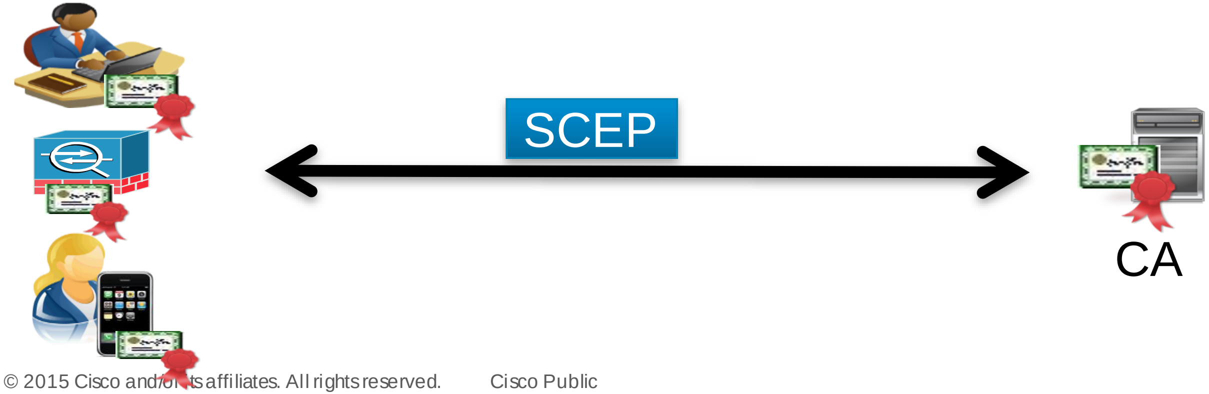
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

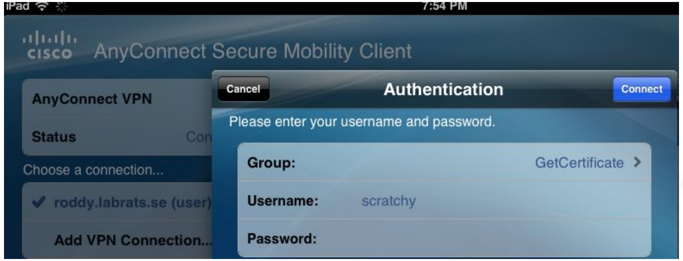
Simple Certificate Enrollment Protocol (SCEP)

- http://tools.ietf.org/id/draft-nourse-scep-21.txt
- Protocol for enrolling certificates over HTTP (basically encapsulating PKCS#10, PKCS#7 over HTTP)
- Originally developed by Verisign for Cisco
- **Widely** supported by network devices (including ASA and AnyConnect), clients and most Certificate Authorities (including Microsoft CA)



AnyConnect SCEP Proxy Support

- ASA can be an SCEP proxy, enabling AnyConnect on the outside to enroll to a CA on the inside of ASA without poking holes in Firewall
- Not to be confused with Legacy SCEP, where AnyConnect speaks directly to the CA over the VPN tunnel.
- SCEP proxy requires AnyConnect 3.0 :



iPad 7:54 PM

cisco AnyConnect Secure Mobility Client

AnyConnect VPN

Status Con

Choose a connection...

✓ roddy.labrats.se (user)

Add VPN Connection...

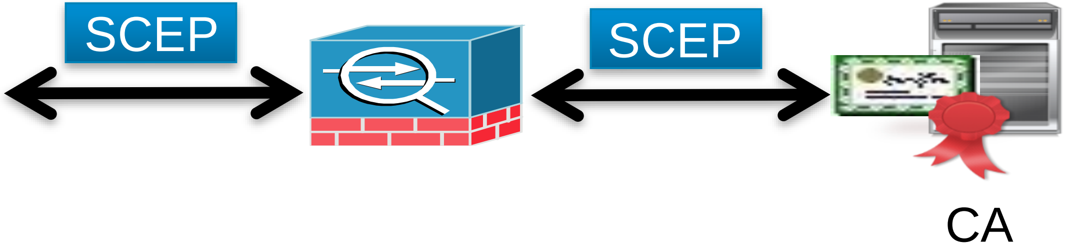
Cancel **Authentication** Connect

Please enter your username and password.

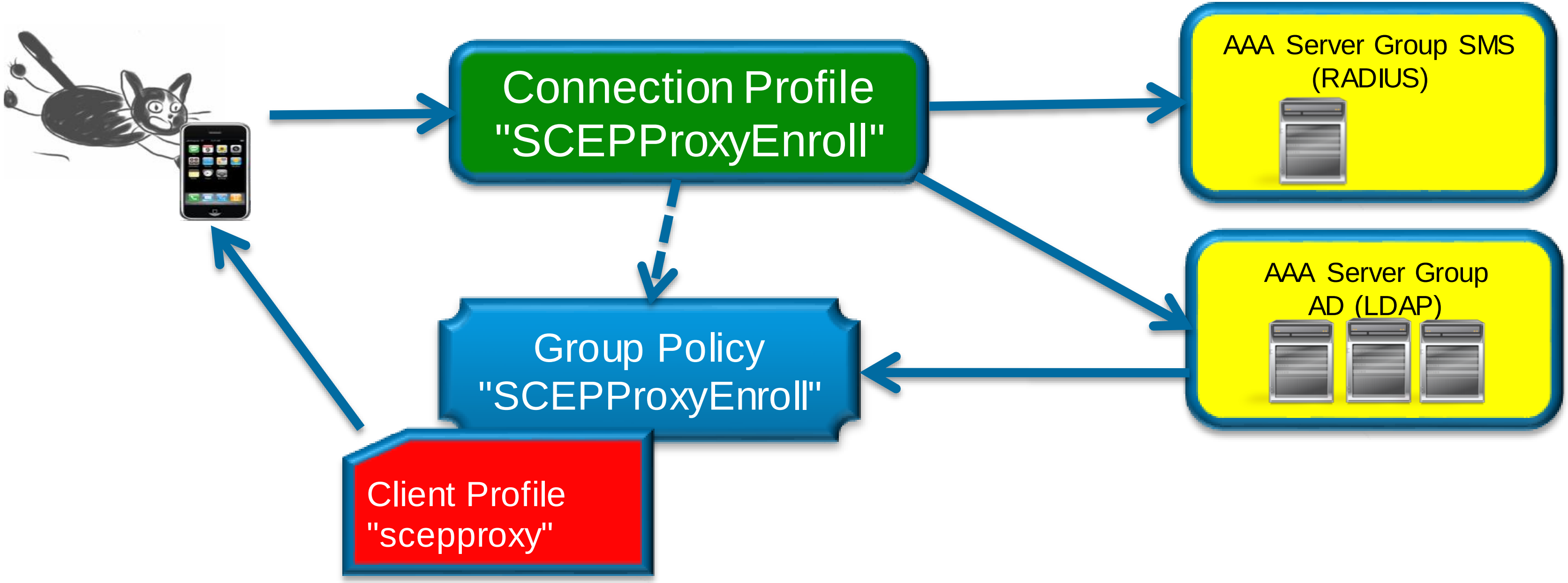
Group: GetCertificate >

Username: scratchy

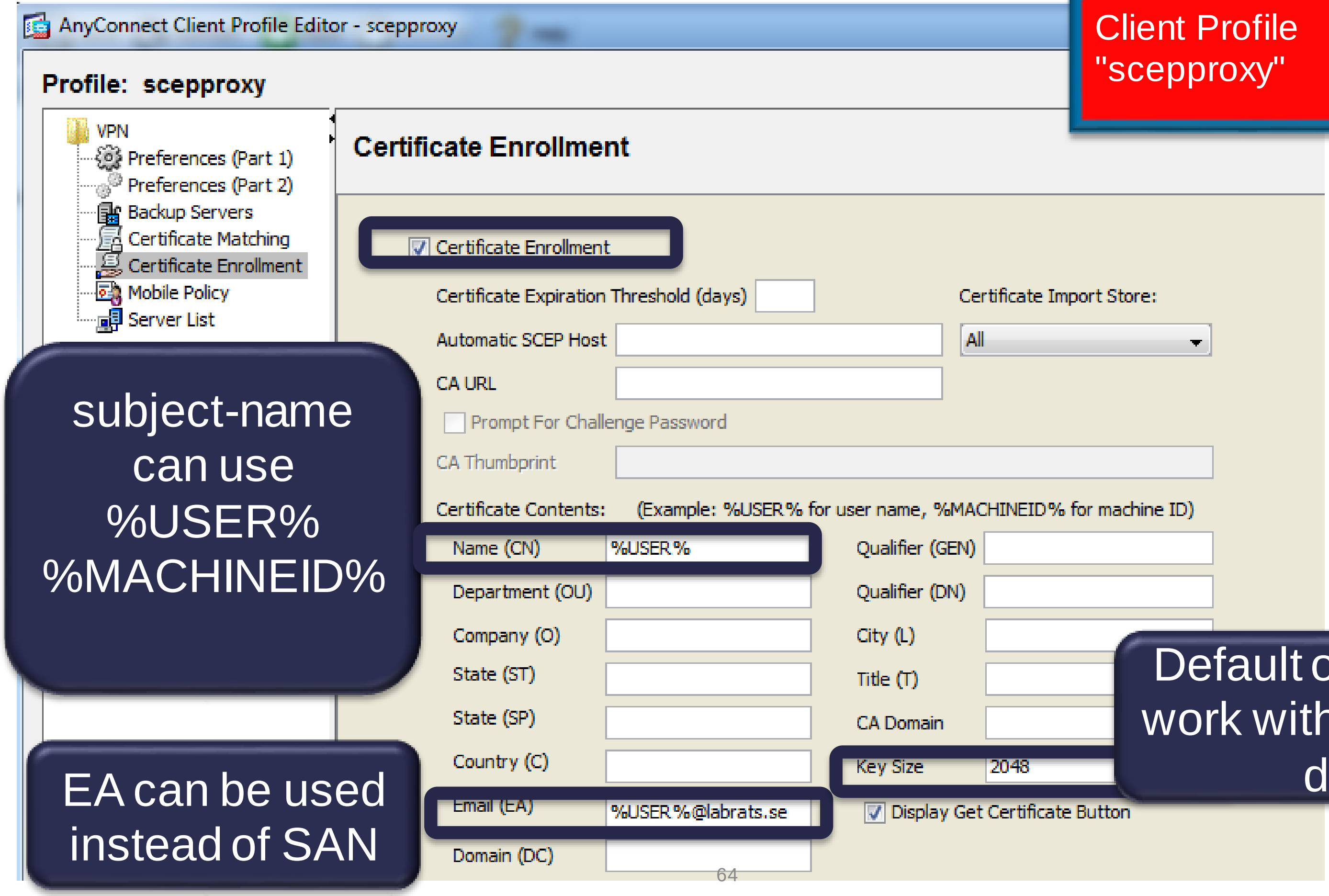
Password:



What to Configure on ASA



Client Profile For Certificate Enrollment



AnyConnect Client Profile Editor - scepproxy

Profile: scepproxy

- VPN
  - Preferences (Part 1)
  - Preferences (Part 2)
  - Backup Servers
  - Certificate Matching
  - Certificate Enrollment
  - Mobile Policy
  - Server List

Certificate Enrollment

☑ Certificate Enrollment

Certificate Expiration Threshold (days)

Certificate Import Store: All

Automatic SCEP Host

CA URL

□ Prompt For Challenge Password

CA Thumbprint

Certificate Contents: (Example: %USER% for user name, %MACHINEID% for machine ID)

Name (CN)	%USER%	Qualifier (GEN)	
Department (OU)		Qualifier (DN)	
Company (O)		City (L)	
State (ST)		Title (T)	
State (SP)		CA Domain	
Country (C)		Key Size	2048
Email (EA)	%USER%@labrats.se	☑ Display Get Certificate Button	
Domain (DC)			

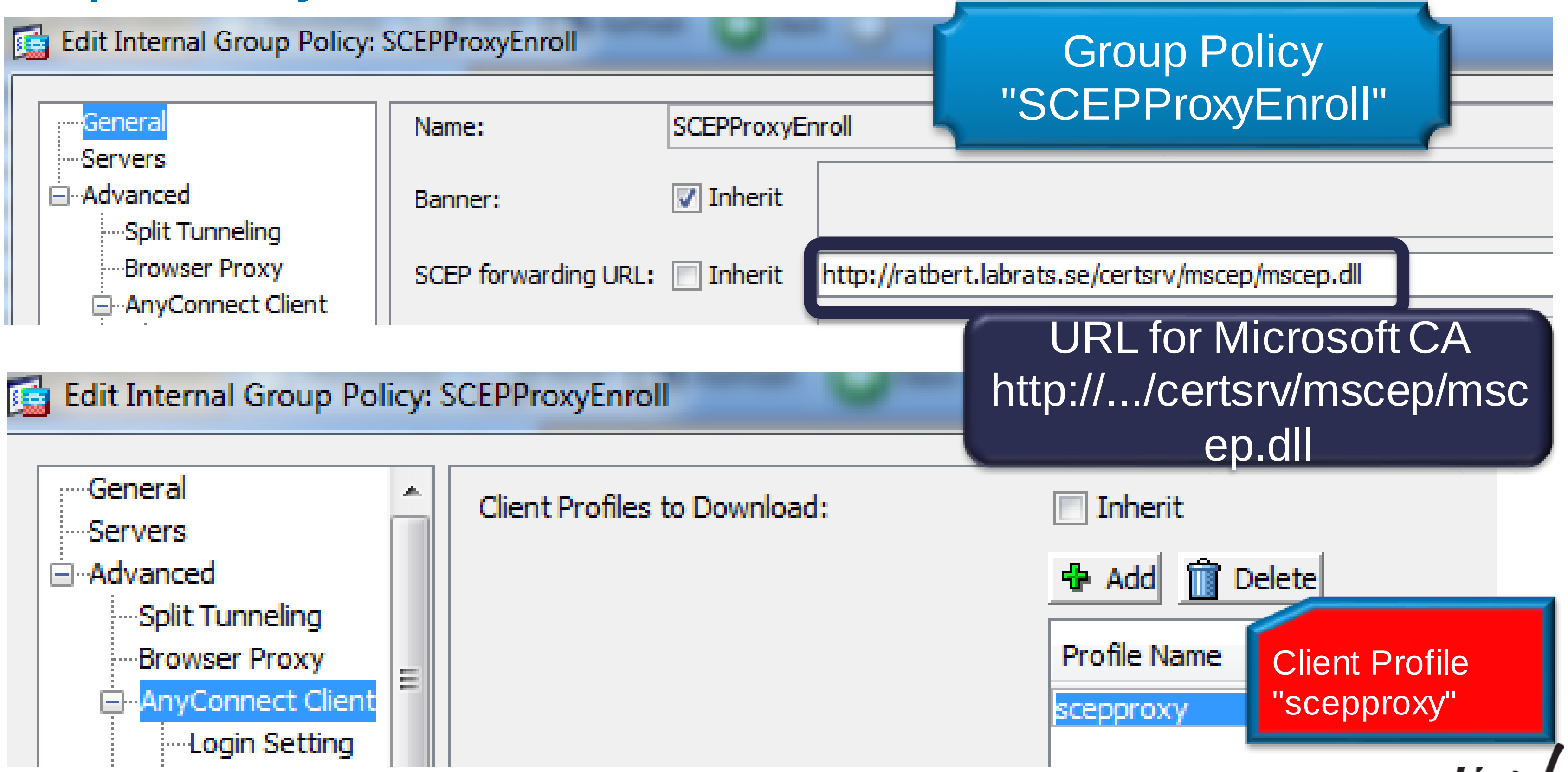
Client Profile "scepproxy"

subject-name can use %USER% %MACHINEID%

Default of 512 will not work with Windows CA default

EA can be used instead of SAN

Group Policy for Certificate Enrollment



Edit Internal Group Policy: SCEPProxyEnroll

Name: SCEPProxyEnroll

Banner: ☑ Inherit

SCEP forwarding URL: □ Inherit http://ratbert.labrats.se/certsrv/mscep/mscep.dll

Group Policy "SCEPProxyEnroll"

URL for Microsoft CA http://.../certsrv/mscep/mscep.dll

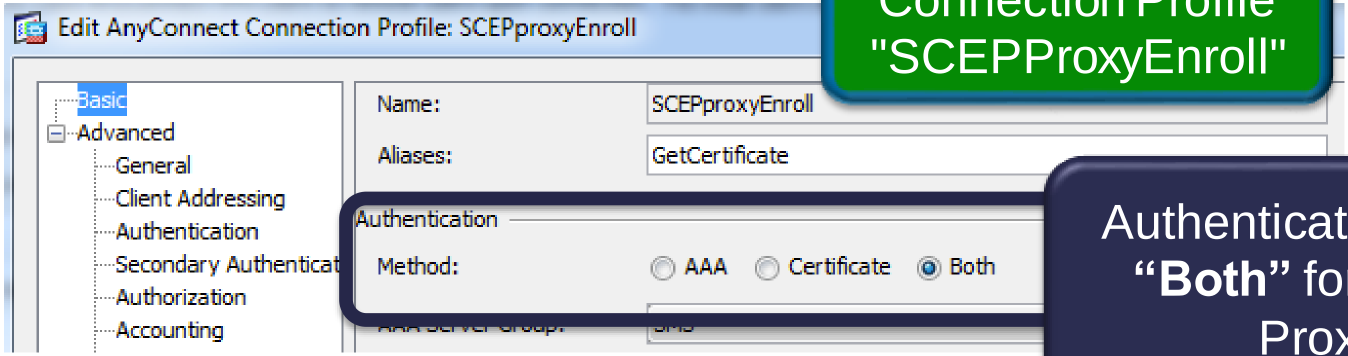
Edit Internal Group Policy: SCEPProxyEnroll

Client Profiles to Download: □ Inherit

Profile Name
sceppproxy

Client Profile "sceppproxy"

Connection Profile for Certificate Enrollment



Edit AnyConnect Connection Profile: SCEPproxyEnroll

Name: SCEPproxyEnroll

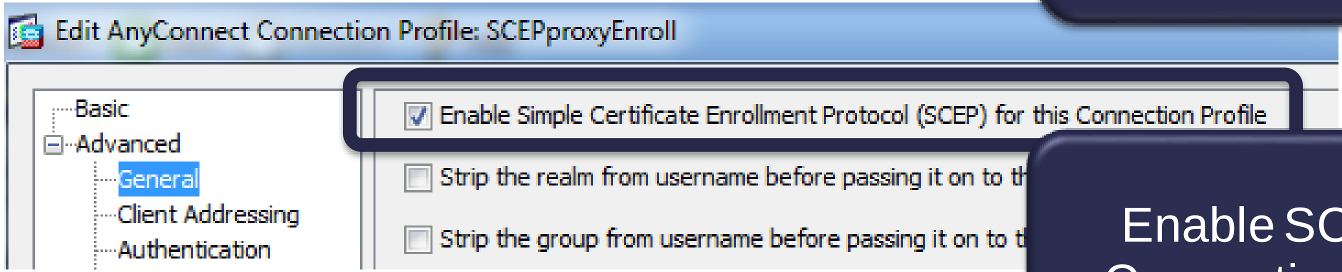
Aliases: GetCertificate

Authentication

Method: ○ AAA ○ Certificate ● Both

Connection Profile "SCEPProxyEnroll"

Authentication set to **"Both"** for SCEP Proxy



Edit AnyConnect Connection Profile: SCEPproxyEnroll

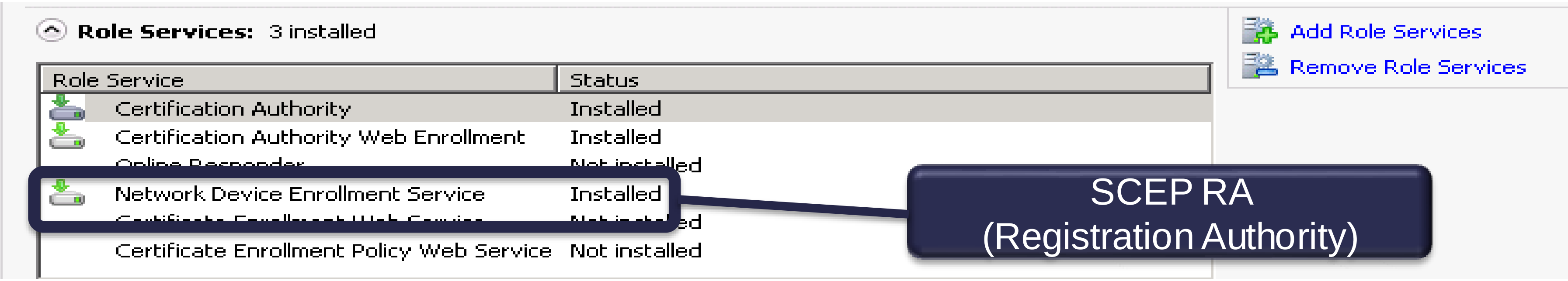
☑ Enable Simple Certificate Enrollment Protocol (SCEP) for this Connection Profile

□ Strip the realm from username before passing it on to th

□ Strip the group from username before passing it on to t

Enable SCEP on Connection Profile

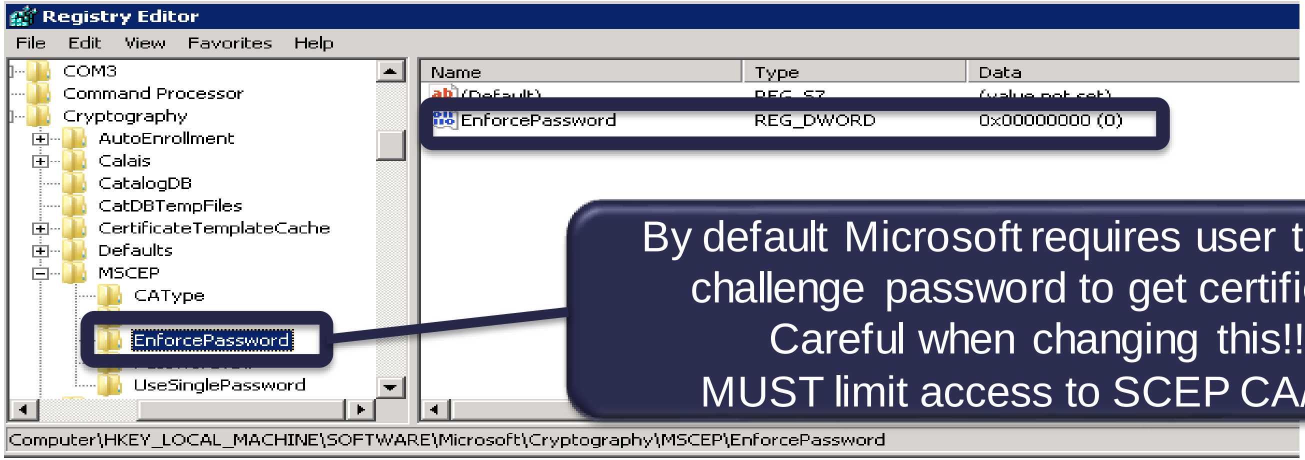
Configuration on Windows 2008 R2 Server (1)



Role Services: 3 installed

Role Service	Status
Certification Authority	Installed
Certification Authority Web Enrollment	Installed
Online Responder	Not installed
Network Device Enrollment Service	Installed
Certificate Enrollment Web Service	Not installed
Certificate Enrollment Policy Web Service	Not installed

SCEP RA
(Registration Authority)



Name	Type	Data
(Default)	REG_SZ	(value not set)
EnforcePassword	REG_DWORD	0x00000000 (0)

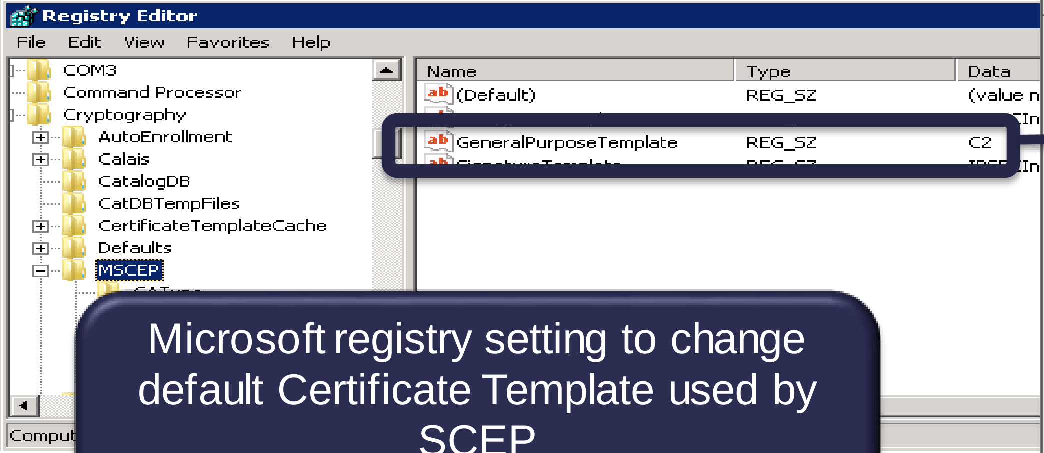
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

By default Microsoft requires user to enter challenge password to get certificate
Careful when changing this!!
MUST limit access to SCEP CA/RA

Security Risk

Configuration on Windows 2008 R2 Server (2)

- Good Microsoft document on
  - http://www.microsoft.com/download/en/details.aspx?id=1607



Registry Editor

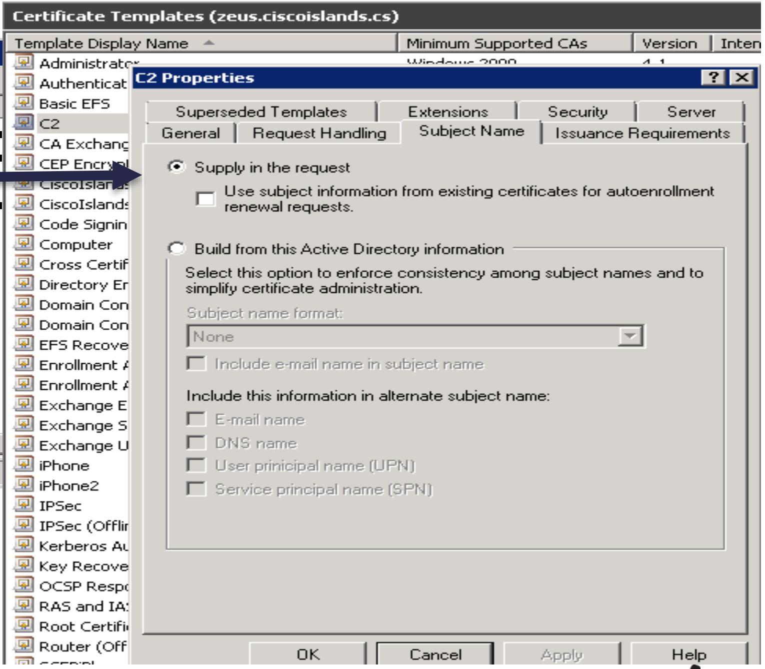
COM3
Command Processor
Cryptography
AutoEnrollment
Calais
CatalogDB
CatDBTempFiles
CertificateTemplateCache
Defaults
MSCEP
CAType

Name	Type	Data
(Default)	REG_SZ	(value n
GeneralPurposeTemplate	REG_SZ	C2
SignatureTemplate	REG_SZ	IPSEC(In

Comput

Microsoft registry setting to change default Certificate Template used by SCEP

Hint : the default template does not work for SSL VPN



Certificate Templates (zeus.ciscoislands.cs)

Template Display Name	Minimum Supported CAs	Version	Inten
Administrator	Windows 2000	4.1	
Authenticat			
Basic EFS			
C2			
CA Exchang			
CEP Encryp			
CiscoIslands			
CiscoIslands			
Code Signin			
Computer			
Cross Certif			
Directory Er			
Domain Con			
Domain Con			
EFS Recove			
Enrollment A			
Enrollment A			
Exchange E			
Exchange S			
Exchange U			
iPhone			
iPhone2			
IPSec			
IPSec (Offlir			
Kerberos Au			
Key Recove			
OCSP Respo			
RAS and IA:			
Root Certifi			
Router (Off			
SCEPOL			

C2 Properties

● 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

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

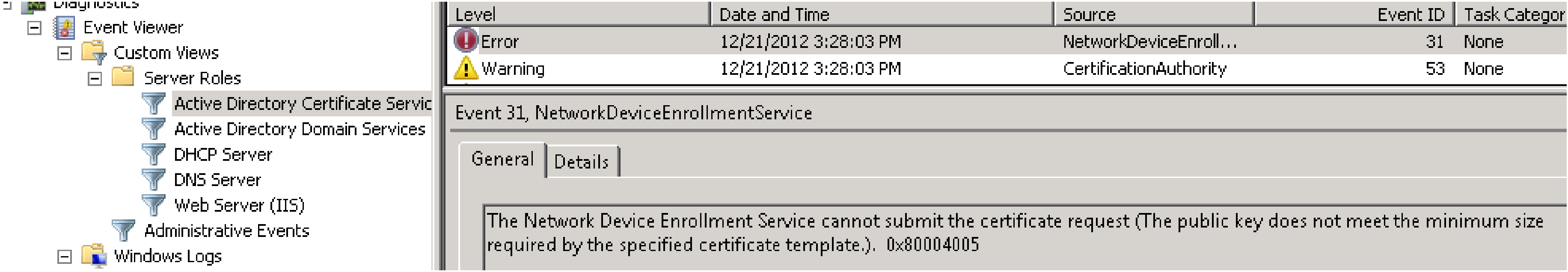
□ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

Troubleshooting Tips

- Pay attention to the certificate templates used by Microsoft CA
  - certificate usage
  - security permissions
  - minimum key length
- Logs from Microsoft Server may be helpful
  - Event Viewer : Server Roles
  - IIS access logs



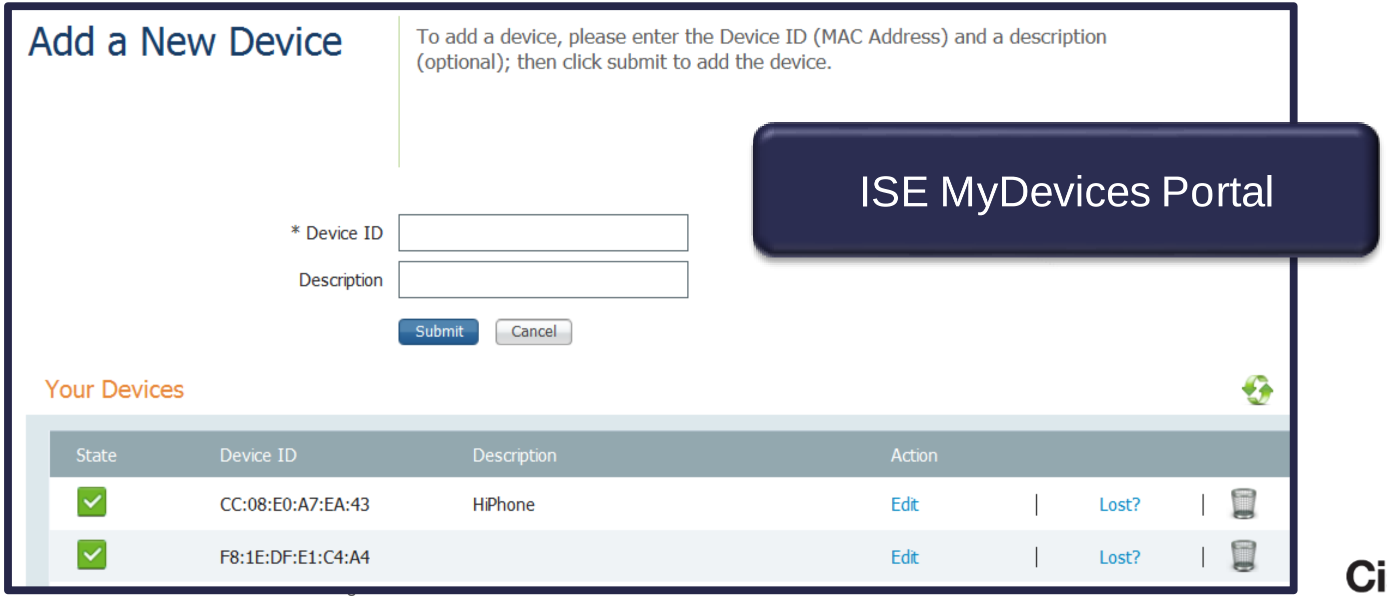
Level	Date and Time	Source	Event ID	Task Categor
Error	12/21/2012 3:28:03 PM	NetworkDeviceEnroll...	31	None
Warning	12/21/2012 3:28:03 PM	CertificationAuthority	53	None

Event 31, NetworkDeviceEnrollmentService

The Network Device Enrollment Service cannot submit the certificate request (The public key does not meet the minimum size required by the specified certificate template.). 0x80004005

Alternative Certificate Provisioning for AnyConnect

- ISE allows for certificate and supplicant provisioning through My Devices Portal
  - works for provisioning devices over local LAN (Cisco switch or WLC)
  - user can also use portal to blacklist device
- Certificates provisioned via ISE can also be used by AnyConnect



Add a New Device

To add a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.

* Device ID	
Description	

Your Devices

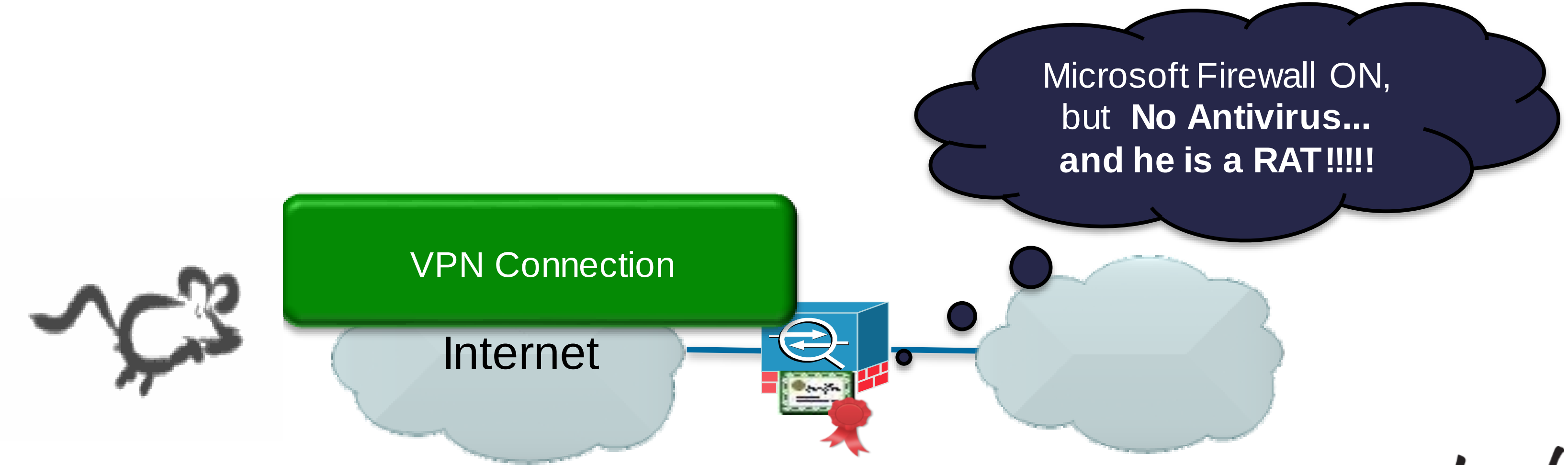
State	Device ID	Description	Action		
✓	CC:08:E0:A7:EA:43	HiPhone	Edit	Lost?	🗑
✓	F8:1E:DF:E1:C4:A4		Edit	Lost?	🗑

ISE MyDevices Portal

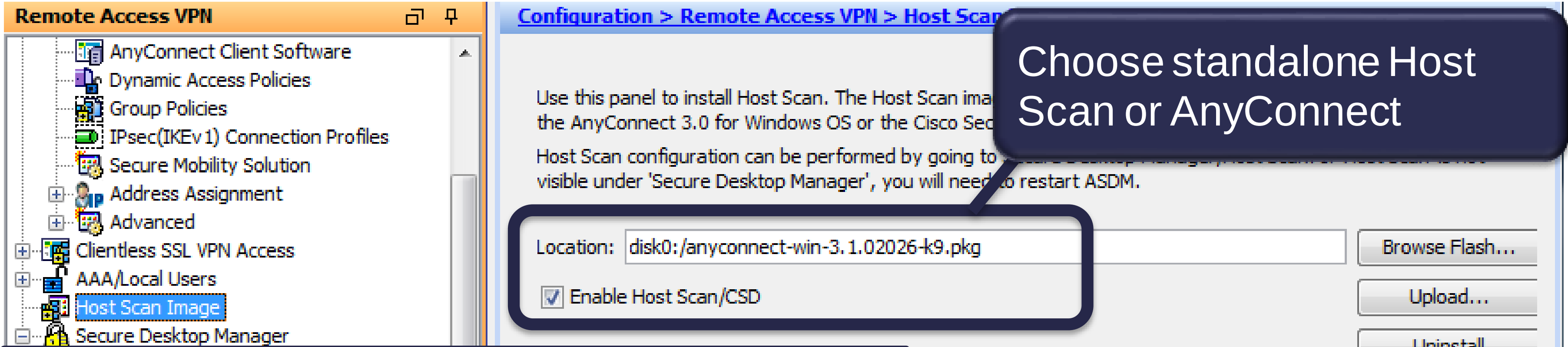
Endpoint Posture Assessment

AnyConnect Posture:
Do the Clients meet Requirements?

- Possible to check that client meets Posture Requirements : OS, Anti-Virus, Personal Firewall, Registry Keys, Open Ports etc
- Used in combination with Dynamic Access Policies (DAP) to grant access to clients depending on their posture status



Specifying Host Scan Image



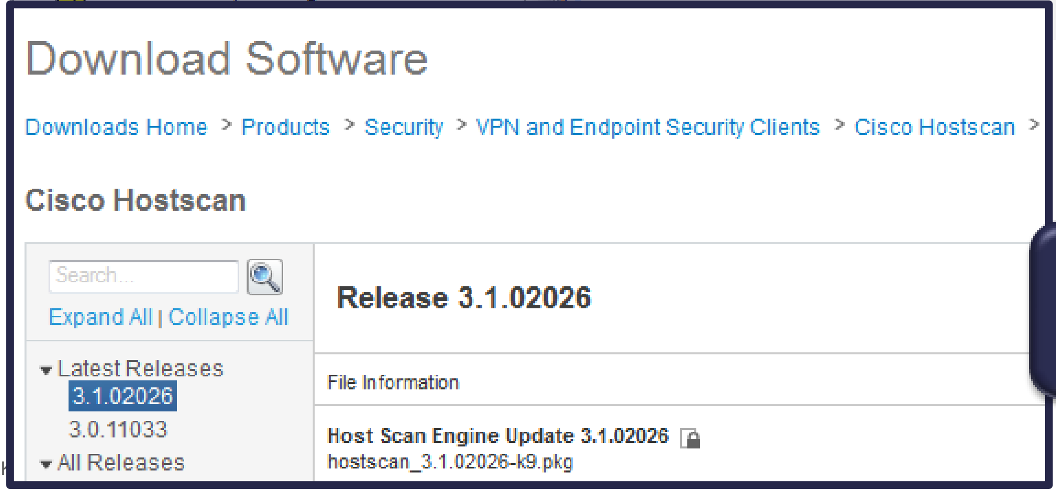
Use this panel to install Host Scan. The Host Scan ima
the AnyConnect 3.0 for Windows OS or the Cisco Sec

Host Scan configuration can be performed by going to
visible under 'Secure Desktop Manager', you will need to restart ASDM.

Location: disk0:/anyconnect-win-3.1.02026-k9.pkg

☑ Enable Host Scan/CSD

Choose standalone Host Scan or AnyConnect


Downloads Home > Products > Security > VPN and Endpoint Security Clients > Cisco Hostscan >
Search...
Expand All | Collapse All
Latest Releases
3.1.02026
3.0.11033
All Releases

Download Software

Cisco Hostscan

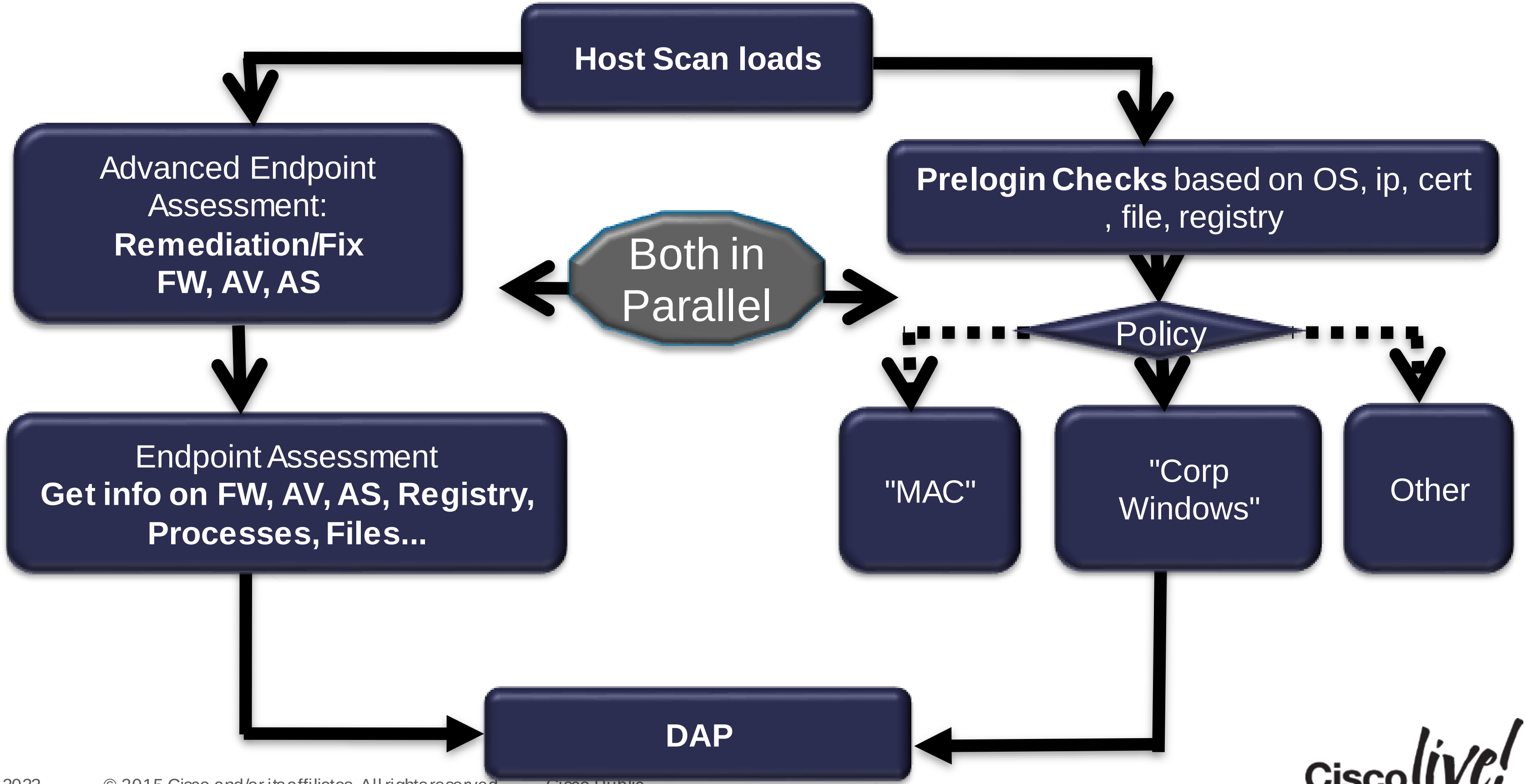
Release 3.1.02026

File Information

Host Scan Engine Update 3.1.02026
hostscan_3.1.02026-k9.pkg

Standalone Host Scan location on CCO

The Host Scan Process



Host Scan loads

Advanced Endpoint Assessment: **Remediation/Fix FW, AV, AS**

Both in Parallel

Prelogin Checks based on OS, ip, cert , file, registry

Policy

"MAC"

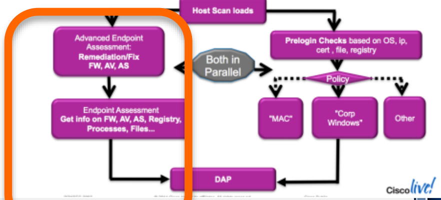
"Corp Windows"

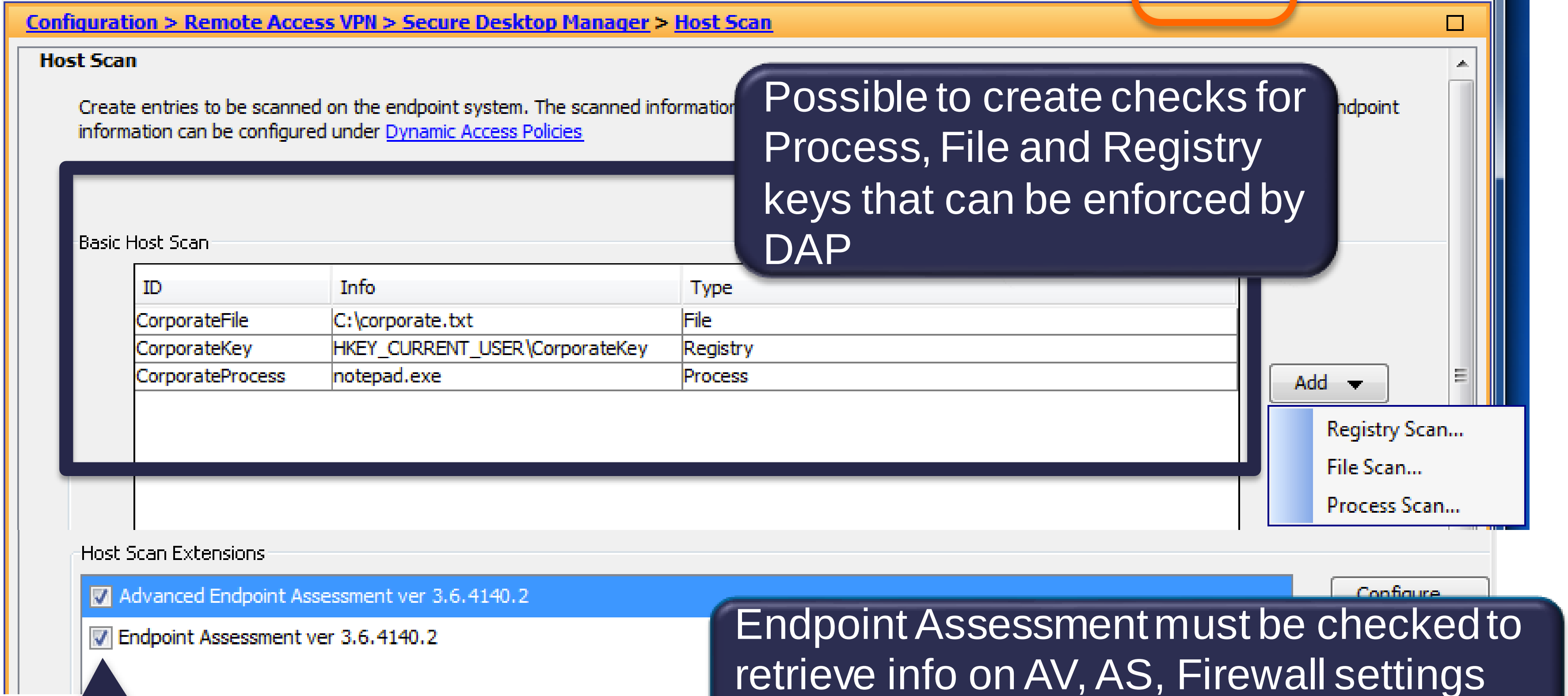
Other

Endpoint Assessment **Get info on FW, AV, AS, Registry, Processes, Files...**

DAP

Configuring Host Scan


Host Scan loads
Advanced Endpoint Assessment: Remediation/Fix FW, AV, AS
Both in Parallel
Prelogin Checks based on OS, ip, cert , file, registry
Policy
Endpoint Assessment Get info on FW, AV, AS, Registry, Processes, Files...
"MAC"
"Corp Windows"
Other
DAP
Cisco live!



Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan

Host Scan

Create entries to be scanned on the endpoint system. The scanned information ... endpoint information can be configured under Dynamic Access Policies

Basic Host Scan

ID	Info	Type
CorporateFile	C:\corporate.txt	File
CorporateKey	HKEY_CURRENT_USER\CorporateKey	Registry
CorporateProcess	notepad.exe	Process

Host Scan Extensions

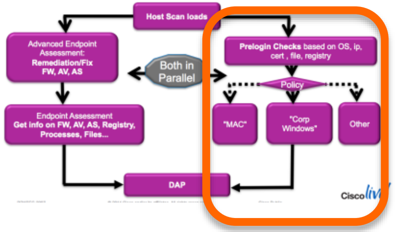
☑ Advanced Endpoint Assessment ver 3.6.4140.2

☑ Endpoint Assessment ver 3.6.4140.2

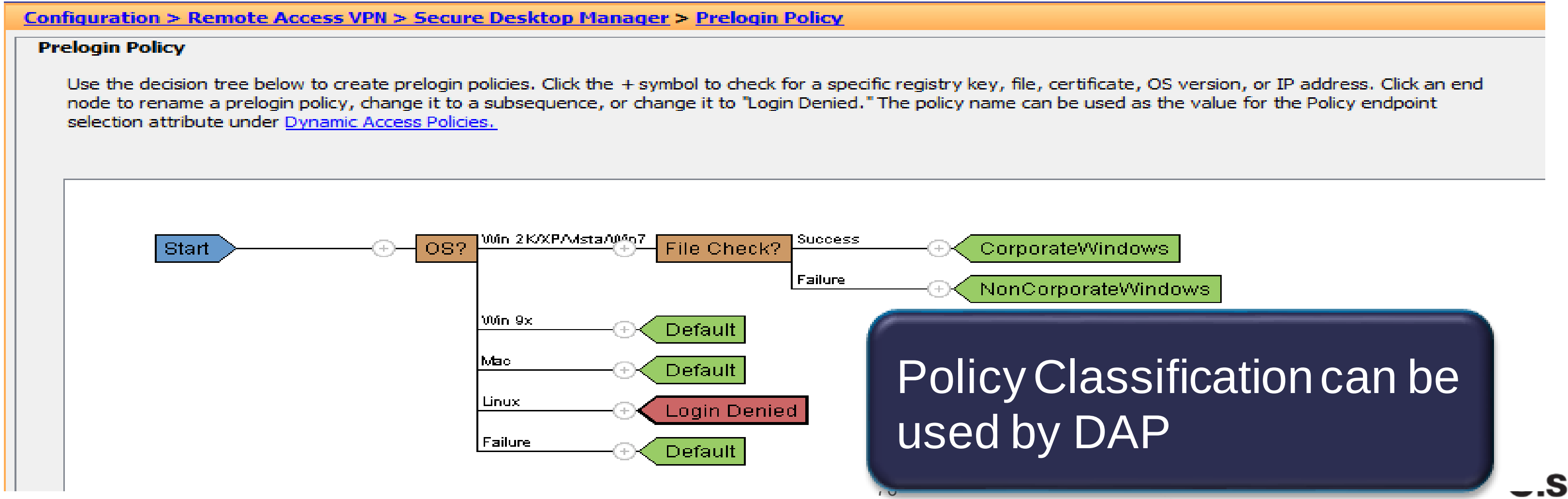
Possible to create checks for Process, File and Registry keys that can be enforced by DAP

Endpoint Assessment must be checked to retrieve info on AV, AS, Firewall settings that can be enforced by DAP

Prelogin Policy


Host Scan loads
Advanced Endpoint Assessment: Remediation/Fix FW, AV, AS
Both in Parallel
Prelogin Checks based on OS, ip, cert , file, registry
Policy
"MAC"
"Corp Windows"
Other
Endpoint Assessment Get info on FW, AV, AS, Registry, Processes, Files...
DAP
Cisco live

- Typical use case is to differentiate corporate devices
- Check client ip address, OS, that file exists, registry keys/values and certificate
  - client ip is the ip of network adapter (before any NAT…)
  - note : certificate check only checks if certificate exist, it does not cryptographically verify that the private key is there
- Possible to deny login immediately, or pass Policy Name to DAP for enforcement



Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy

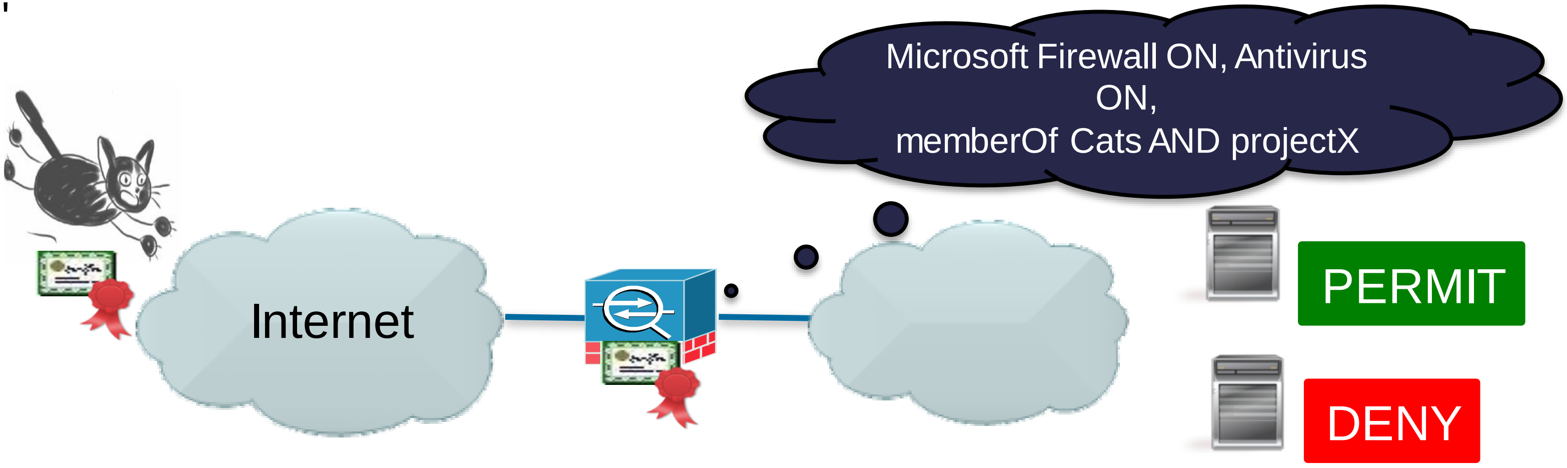
Prelogin Policy

Use the decision tree below to create prelogin policies. Click the + symbol to check for a specific registry key, file, certificate, OS version, or IP address. Click an end node to rename a prelogin policy, change it to a subsequence, or change it to "Login Denied." The policy name can be used as the value for the Policy endpoint selection attribute under Dynamic Access Policies.

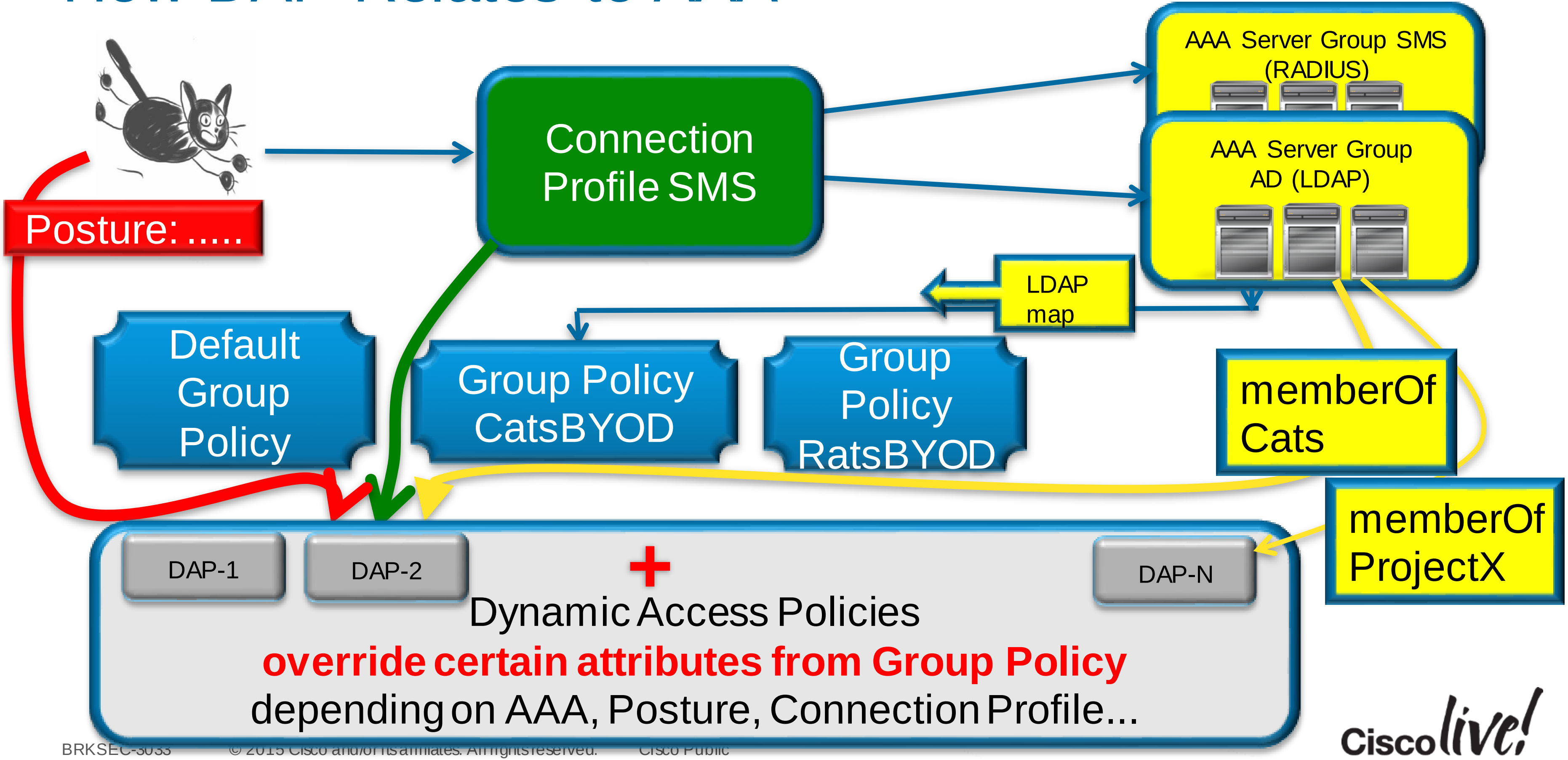
Policy Classification can be used by DAP

Dynamic Access Policies (DAP)

- DAP allows **granular access control** to resources based on authentication method, AAA parameters and Posture
- Very flexible, allowing policies set by **Data Owners** access to Data :
  - "to access **my data** you must be member of AD groups Cats and ProjectX, you must be logged in with strong authentication and you must have Antivirus on a corporate machine"


Microsoft Firewall ON, Antivirus ON,
memberOf Cats AND projectX
Internet
PERMIT
DENY

How DAP Relates to AAA



Posture: .....

Connection Profile SMS

AAA Server Group SMS (RADIUS)

AAA Server Group AD (LDAP)

LDAP map

Default Group Policy

Group Policy CatsBYOD

Group Policy RatsBYOD

memberOf Cats

memberOf ProjectX

DAP-1

DAP-2

DAP-N

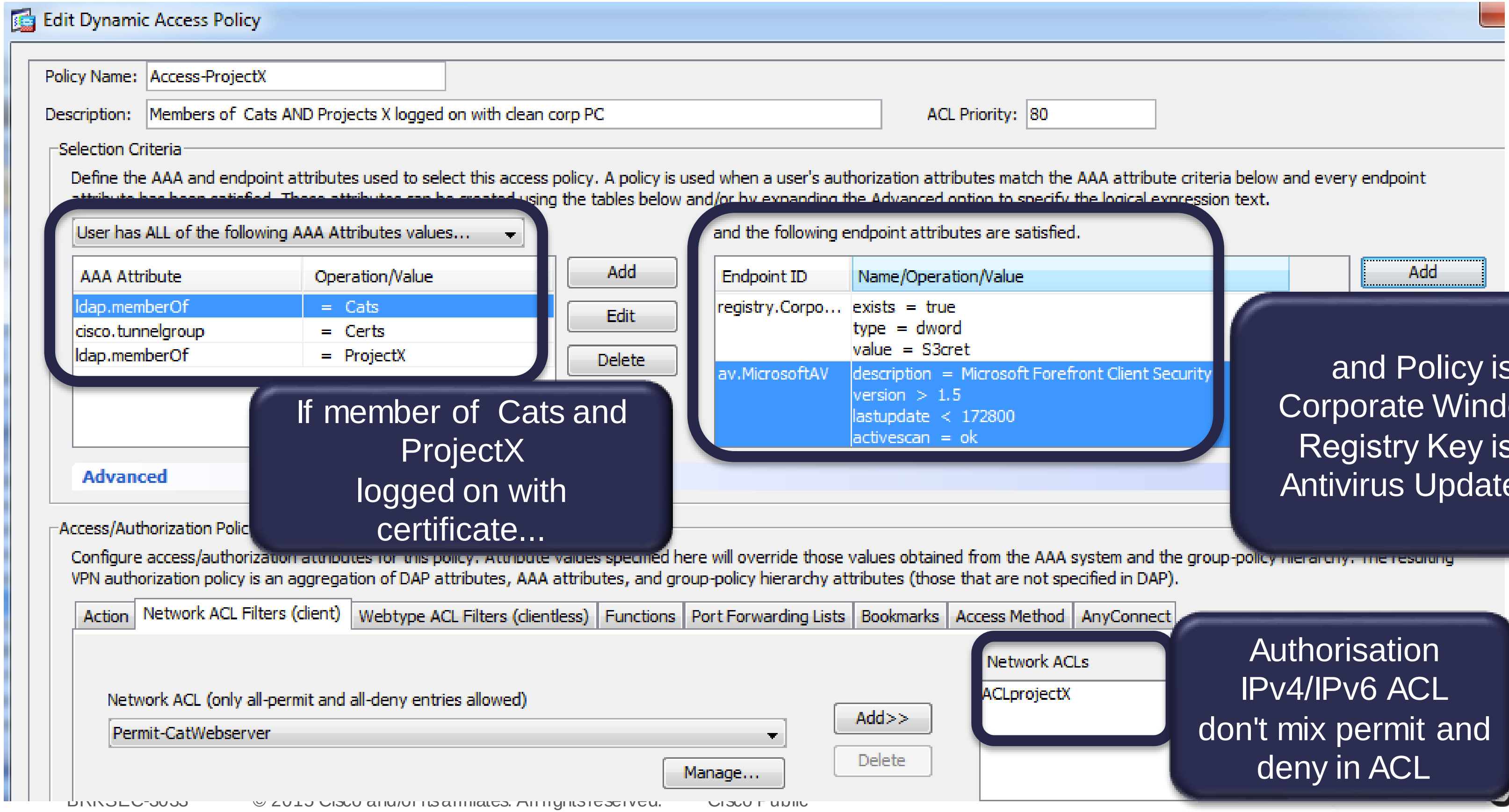
+

Dynamic Access Policies

override certain attributes from Group Policy

depending on AAA, Posture, Connection Profile...

Configuring DAP



Edit Dynamic Access Policy

Policy Name: Access-ProjectX

Description: Members of Cats AND Projects X logged on with clean corp PC

ACL Priority: 80

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ALL of the following AAA Attributes values...

AAA Attribute	Operation/Value
ldap.memberOf	= Cats
cisco.tunnelgroup	= Certs
ldap.memberOf	= ProjectX

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value

registry.Corpo...	exists = true
	type = dword
	value = S3cret

av.MicrosoftAV	description = Microsoft Forefront Client Security
	version > 1.5
	lastupdate < 172800
	activescan = ok

Access/Authorization Polic

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Network ACL (only all-permit and all-deny entries allowed)

Permit-CatWebserver

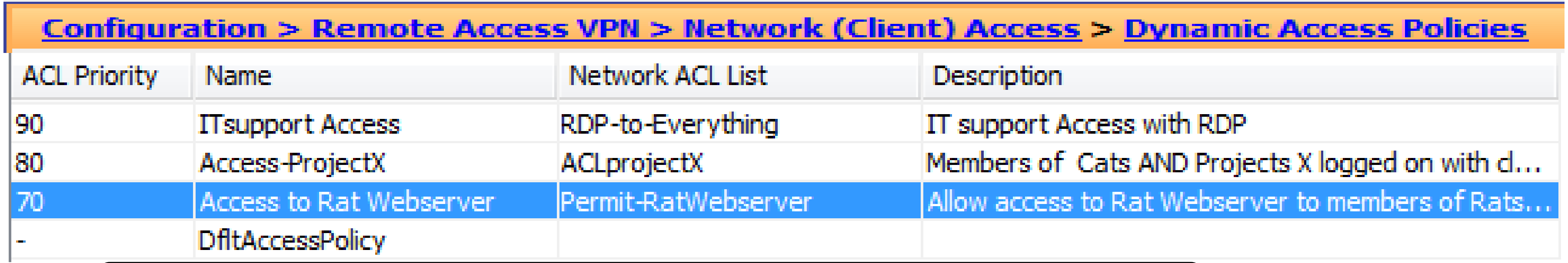
Network ACLs
ACLprojectX

If member of Cats and ProjectX logged on with certificate...

and Policy is Corporate Windows Registry Key is… Antivirus Updated...

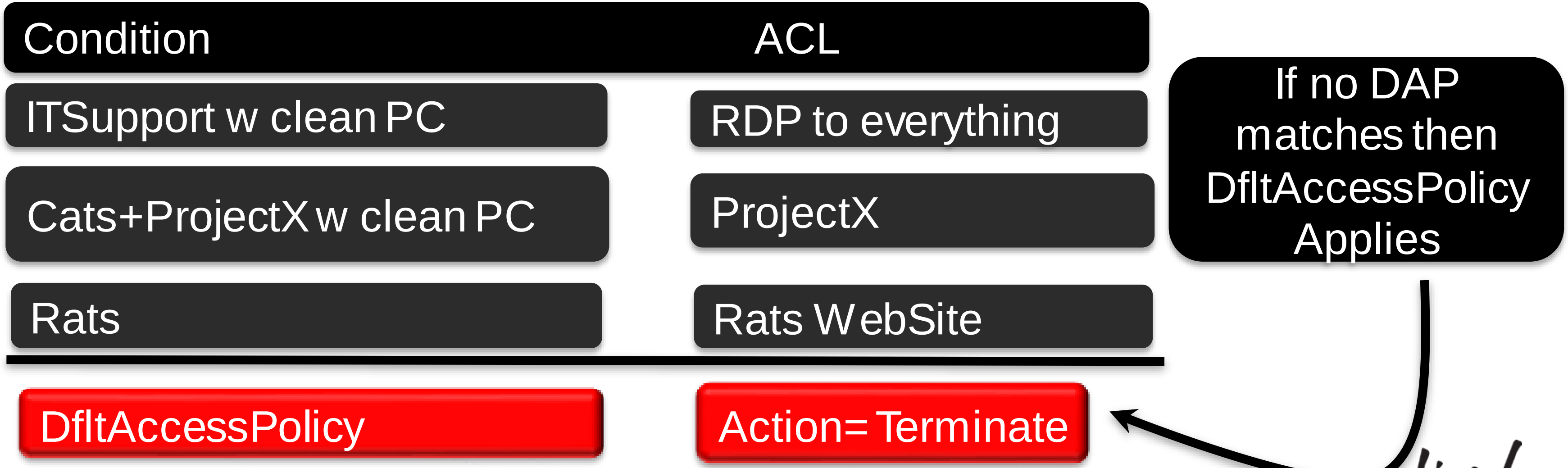
Authorisation IPv4/IPv6 ACL don't mix permit and deny in ACL

Default DAP (DfltAccessPolicy)



Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

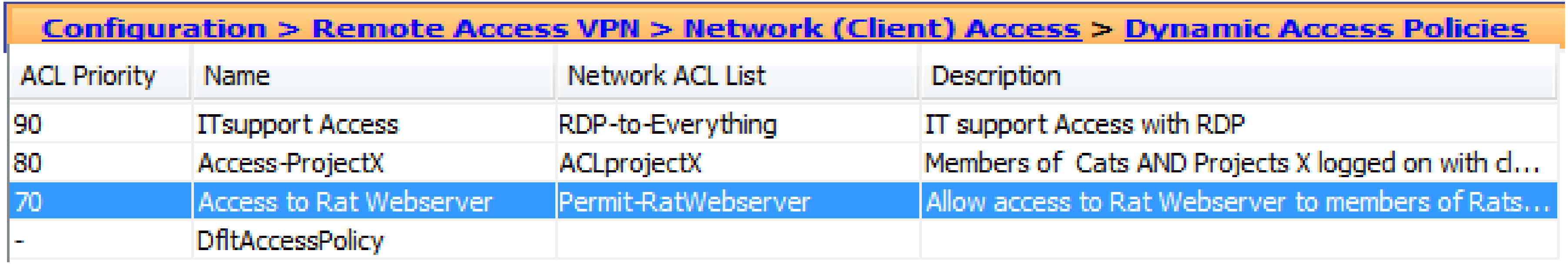
ACL Priority	Name	Network ACL List	Description
90	ITsupport Access	RDP-to-Everything	IT support Access with RDP
80	Access-ProjectX	ACLprojectX	Members of Cats AND Projects X logged on with cl...
70	Access to Rat Webserver	Permit-RatWebserver	Allow access to Rat Webserver to members of Rats...
-	DfltAccessPolicy		



Condition	ACL
ITSupport w clean PC	RDP to everything
Cats+ProjectX w clean PC	ProjectX
Rats	Rats WebSite
DfltAccessPolicy	Action= Terminate

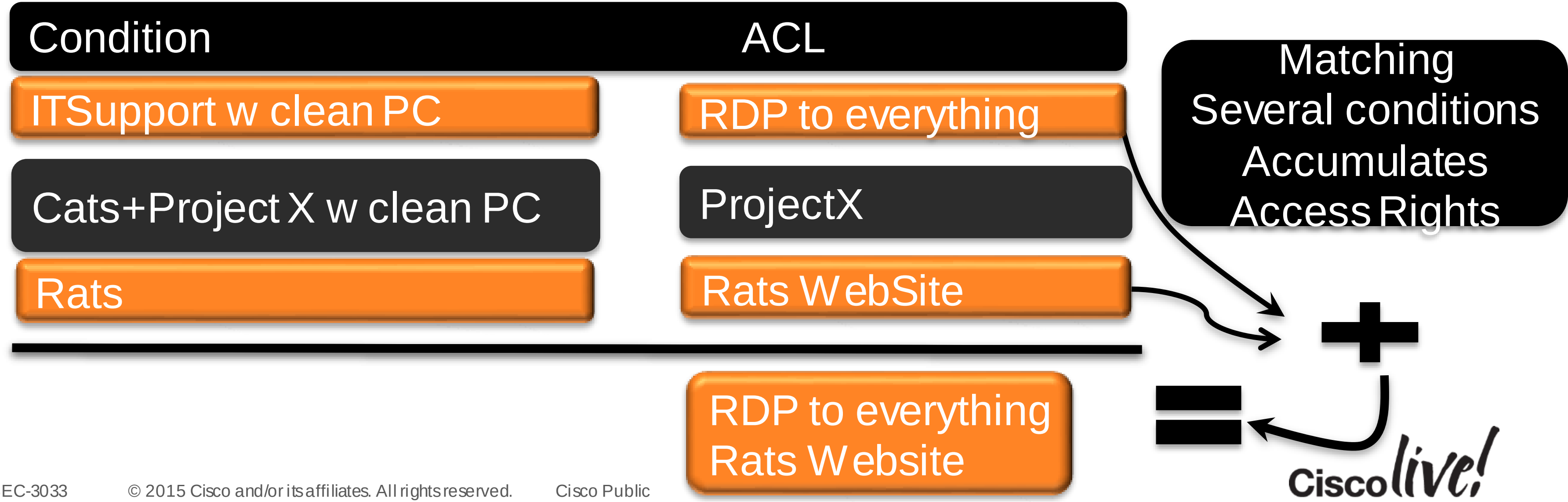
If no DAP matches then DfltAccessPolicy Applies

DAP Grows On You! (DAP accumulates)



Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

ACL Priority	Name	Network ACL List	Description
90	ITsupport Access	RDP-to-Everything	IT support Access with RDP
80	Access-ProjectX	ACLprojectX	Members of Cats AND Projects X logged on with d...
70	Access to Rat Webserver	Permit-RatWebserver	Allow access to Rat Webserver to members of Rats...
-	DfltAccessPolicy		

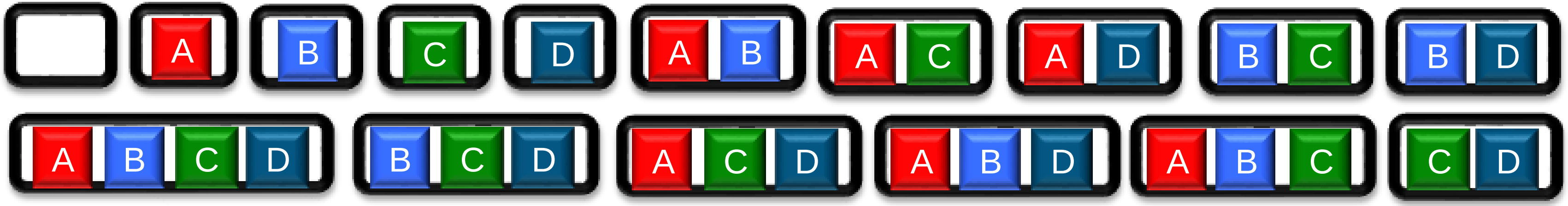


Condition	ACL
ITSupport w clean PC	RDP to everything
Cats+Project X w clean PC	ProjectX
Rats	Rats WebSite
	RDP to everything Rats Website

Matching Several conditions Accumulates Access Rights

The Power of DAP

- Very flexible mapping to multiple "memberOf"
  - Example : 4 groups in Directory A B C D
  - A user may be a member of 0 to 4 groups : 16 combinations (2^n)



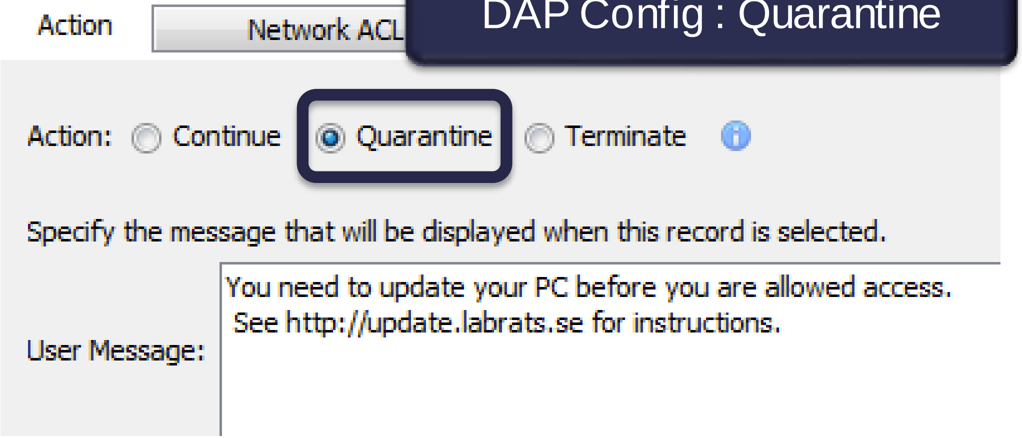
- **Quiz** : How many DAP policies do you need to cover the 16 combinations?

Condition (memberOf)	ACL
A	ACL-A
B	ACL-B
C	ACL-C
D	ACL-D

DAP with Quarantine

- Possible to create a DAP (with ACL) that gives a user limited access to the network to remediate posture, after which he can "reconnect".
- Used together with "Advanced Endpoint Assessment"
- Remember that DAP accumulates ACL privileges (if other DAPs are matched user may still get full access to the network).

DAP Config : Quarantine



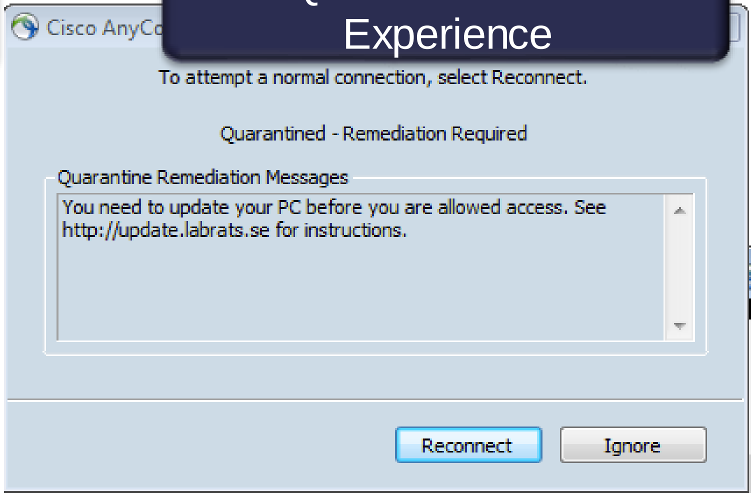
Action: Network ACL

Action: ○ Continue ● Quarantine ○ Terminate

Specify the message that will be displayed when this record is selected.

User Message: You need to update your PC before you are allowed access. See http://update.labrats.se for instructions.

Quarantine User Experience



To attempt a normal connection, select Reconnect.

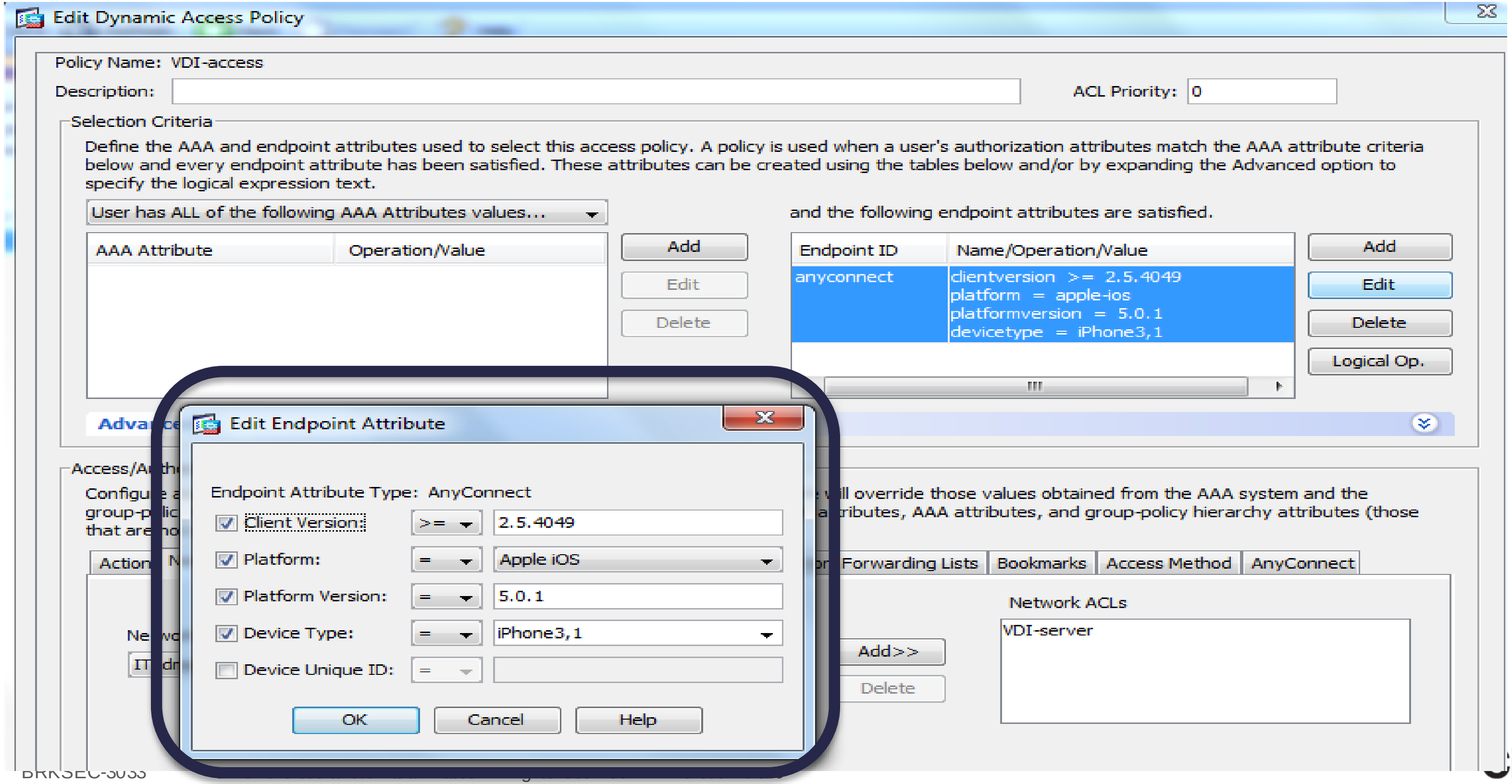
Quarantined - Remediation Required

Quarantine Remediation Messages

You need to update your PC before you are allowed access. See http://update.labrats.se for instructions.

DAP for Mobile Devices (iOS, Android)

"Mobile Posture Assessment"



Edit Dynamic Access Policy

Policy Name: VDI-access

Description:

ACL Priority: 0

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ALL of the following AAA Attributes values...

AAA Attribute	Operation/Value

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value

anyconnect	clientversion >= 2.5.4049
	platform = apple-ios
	platformversion = 5.0.1
	devicetype = iPhone3,1

Edit Endpoint Attribute

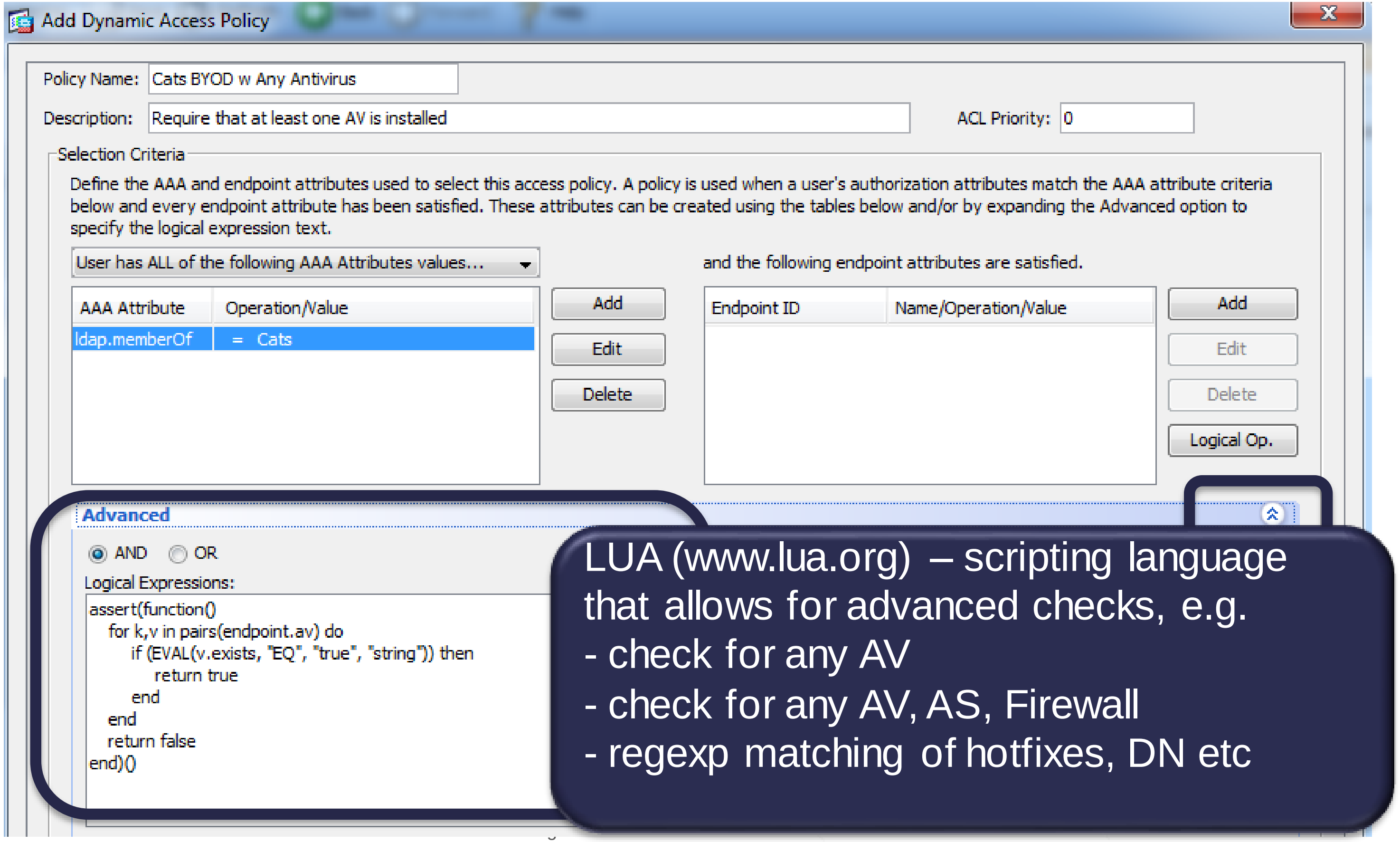
Endpoint Attribute Type: AnyConnect

☑ Client Version:	>=	2.5.4049
☑ Platform:	=	Apple iOS
☑ Platform Version:	=	5.0.1
☑ Device Type:	=	iPhone3,1
☐ Device Unique ID:	=	

Network ACLs: VDI-server

Add
Edit
Delete
Logical Op.
Advanced
Access/Authorization
Configure ... will override those values obtained from the AAA system and the group-policy ... attributes, AAA attributes, and group-policy hierarchy attributes (those that are no...
Action
Forwarding Lists
Bookmarks
Access Method
AnyConnect
Add>>
OK
Cancel
Help

DAP with LUA



Policy Name: Cats BYOD w Any Antivirus

Description: Require that at least one AV is installed

ACL Priority: 0

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ALL of the following AAA Attributes values...

AAA Attribute	Operation/Value
ldap.memberOf	= Cats

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value

● AND ○ OR

Logical Expressions:

```
assert(function()
  for k,v in pairs(endpoint.av) do
     if (EVAL(v.exists, "EQ", "true", "string")) then
        return true
     end
  end
  return false
end)()
```

LUA (www.lua.org) – scripting language that allows for advanced checks, e.g.

- check for any AV
- check for any AV, AS, Firewall
- regexp matching of hotfixes, DN etc

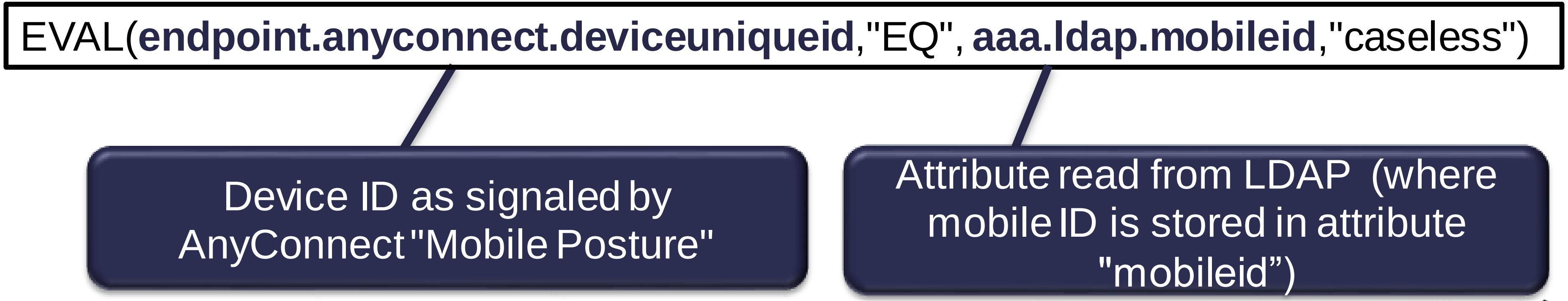
LUA Examples

```
assert(function()
    function check(antix)
      if (type(antix) == "table") then
        for k,v in pairs(antix) do
          if (EVAL(v.exists, "EQ", "true", "string")) then
            return true
          end
        end
      end
      return false
    end
    return (check(endpoint.av) or check(endpoint.fw) or check(endpoint.as))
  end)()
```

Check for Any Antivirus, Firewall or AntiSpyWare

LUA checks that user connects with the "right" device

- Problem : A user with admin privileges may move a cert (and the private keys) from an "approved" device to a non-approved.
- LUA can detect this by comparing device ID signaled by AnyConnect with
  - name in certificate (if certificate contains device ID)
  - an attribute from LDAP lookup (requires device IDs to be stored in LDAP server)



EVAL(**endpoint.anyconnect.deviceuniqueid**,"EQ", **aaa.ldap.mobileid**,"caseless")

Device ID as signaled by AnyConnect "Mobile Posture"

Attribute read from LDAP (where mobile ID is stored in attribute "mobileid")

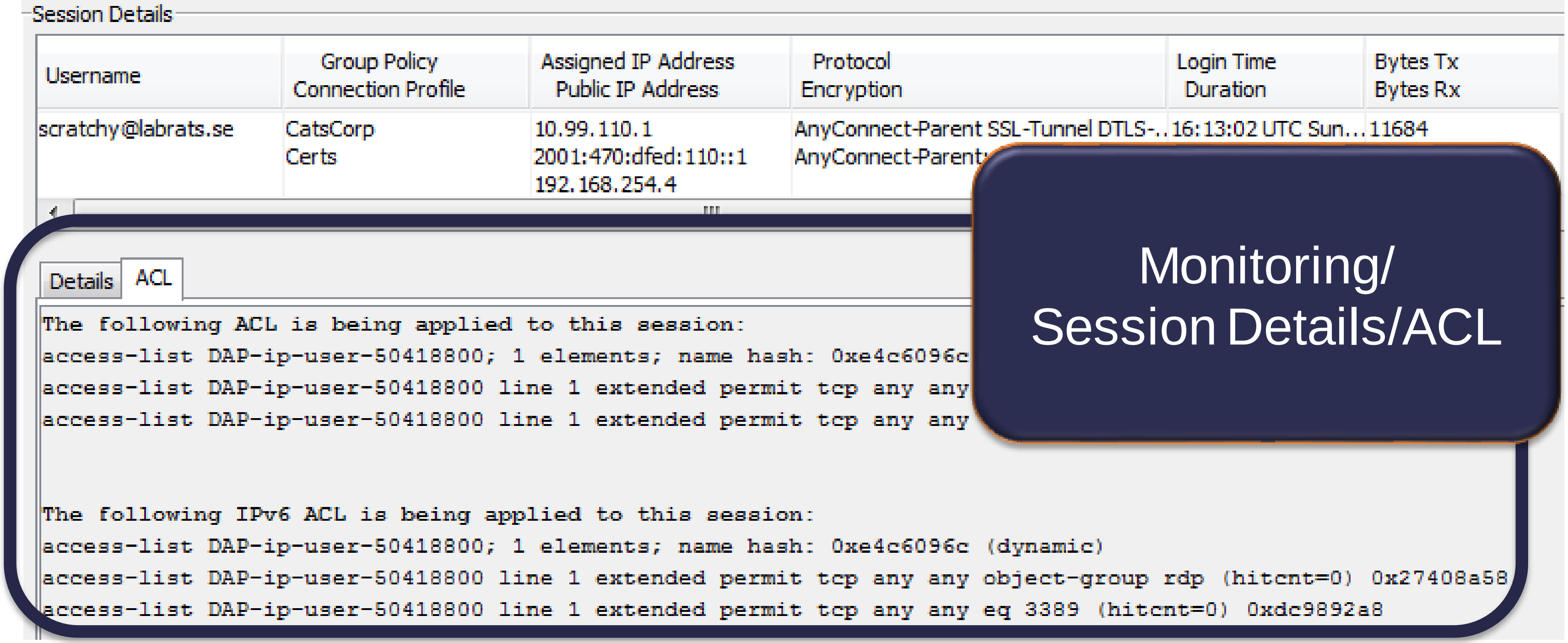
Troubleshooting DAP : debug dap trace

```
DAP_TRACE: DAP_open: B09086B0
DAP_TRACE: DAP_add_CSD: csd_token = [2441266B55C307BA5BEB70E5]
.....
DAP_TRACE: Username: scratchy@labrats.se, aaa.ldap.logonCount = 15
DAP_TRACE: Username: scratchy@labrats.se, aaa.ldap.sAMAccountName = scratchy
.....
DAP_TRACE:
dap_install_endpoint_data_to_lua:endpoint.as["MicrosoftAS"].description="Windows Defender"
DAP_TRACE: name = endpoint.as["MicrosoftAS"].description, value = "Windows Defender"
DAP_TRACE:dap_install_endpoint_data_to_lua:endpoint.as["MicrosoftAS"].version="6.1.76
DAP_TRACE: name = endpoint.as["MicrosoftAS"].version, value = "6.1.7600.16385"
.....
DAP_TRACE: name = endpoint.os.hotfix["KB2654428"], value = "true"
DAP_TRACE: dap_install_endpoint_data_to_lua:endpoint.os.hotfix["KB2656373"]="true"
DAP_TRACE: name = endpoint.os.hotfix["KB2656373"], value = "true"
```

LDAP info

Posture
(Subset)

Troubleshooting DAP : Monitoring



Session Details

Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
scratchy@labrats.se	CatsCorp Certs	10.99.110.1 2001:470:dfed:110::1 192.168.254.4	AnyConnect-Parent SSL-Tunnel DTLS-... AnyConnect-Parent:	16:13:02 UTC Sun...	11684

```
The following ACL is being applied to this session:
access-list DAP-ip-user-50418800; 1 elements; name hash: 0xe4c6096c
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any


The following IPv6 ACL is being applied to this session:
access-list DAP-ip-user-50418800; 1 elements; name hash: 0xe4c6096c (dynamic)
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any object-group rdp (hitcnt=0) 0x27408a58
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any eq 3389 (hitcnt=0) 0xdc9892a8
```

Monitoring/
Session Details/ACL

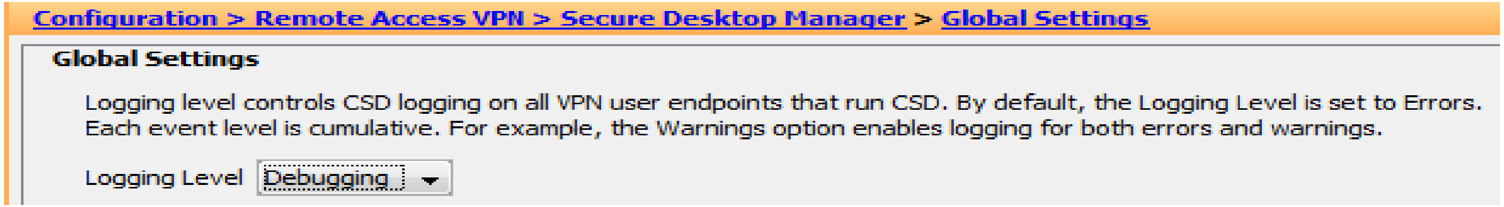
Troubleshooting DAP : Syslog

- Debug DAP trace not always practical in production
  - too much info [pre 9.x]
  - no filtering on username
- Syslog Message with good DAP info : **username** and **selected DAP records**

```
%ASA-6-734001: DAP: User scratchy@labrats.se, Addr 192.168.254.4,
Connection AnyConnect: The following DAP records were selected for this
connection: ITsupport Access
```

Troubleshooting Hostscan Component

- Enable Debugging level at ASDM, then rerun test on problematic client



Configuration > Remote Access VPN > Secure Desktop Manager > Global Settings

Global Settings

Logging level controls CSD logging on all VPN user endpoints that run CSD. By default, the Logging Level is set to Errors. Each event level is cumulative. For example, the Warnings option enables logging for both errors and warnings.

Logging Level: Debugging

- Check Host Scan log files on problematic client
  - libcsd.log
  - cscan.log, detailed posture attributes
- These are located at
  - Windows %LOCALAPPDATA%\Cisco\Cisco HostScan\log
  - MAC/Linux : ~/.cisco/hostscan/log/
- Examine Windows Event logs

GOT DART?

AnyConnect and ISE Integration

Secure Unified Access

Profiling & Device Inventory

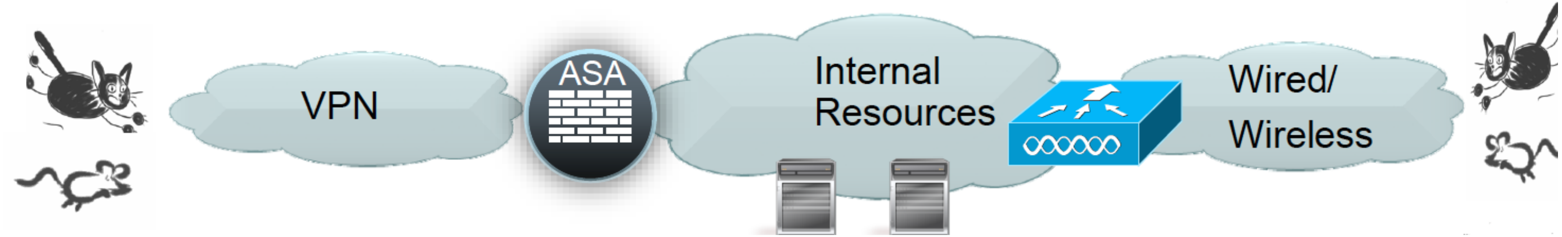
Desktop Posture Checking and Remediation

3rd Party Mobile Device Management

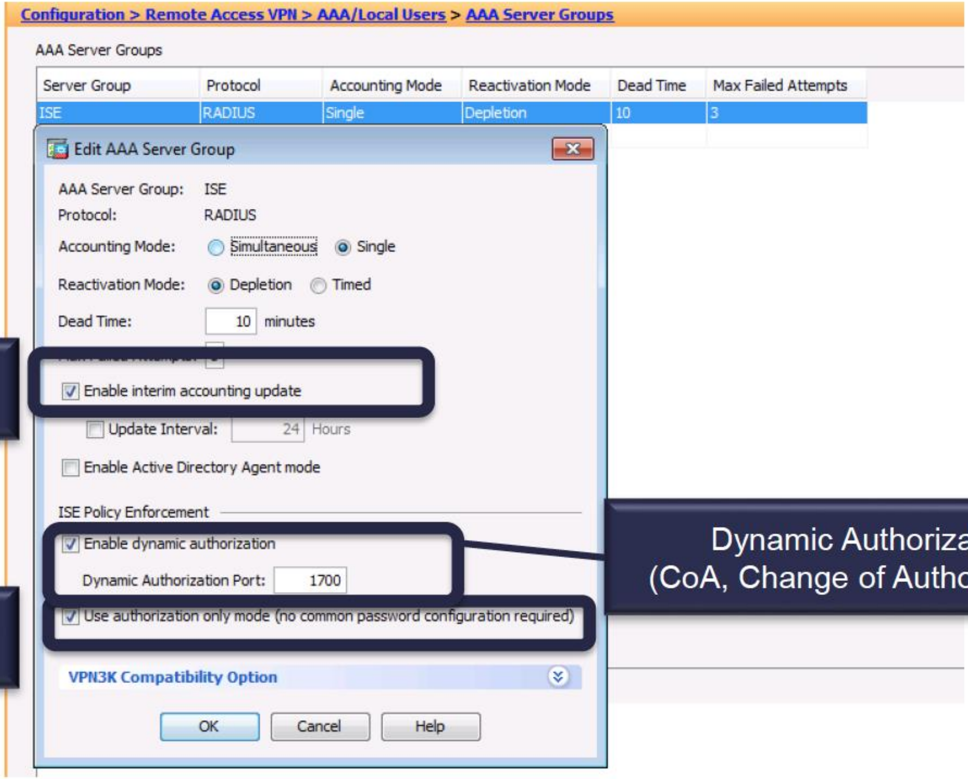
3rd Party Information Sharing

Unified Control of all Access

Flexible Directory Integration



ASA Configuration of ISE Server



Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
ISE	RADIUS	Single	Depletion	10	3

Edit AAA Server Group

AAA Server Group: ISE

Protocol: RADIUS

Accounting Mode: ○ Simultaneous ● Single

Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

☑ Enable interim accounting update

□ Update Interval: 24 Hours

□ Enable Active Directory Agent mode

ISE Policy Enforcement

☑ Enable dynamic authorization

Dynamic Authorization Port: 1700

☑ Use authorization only mode (no common password configuration required)

VPN3K Compatibility Option

Interim Accounting

Authorization-Only

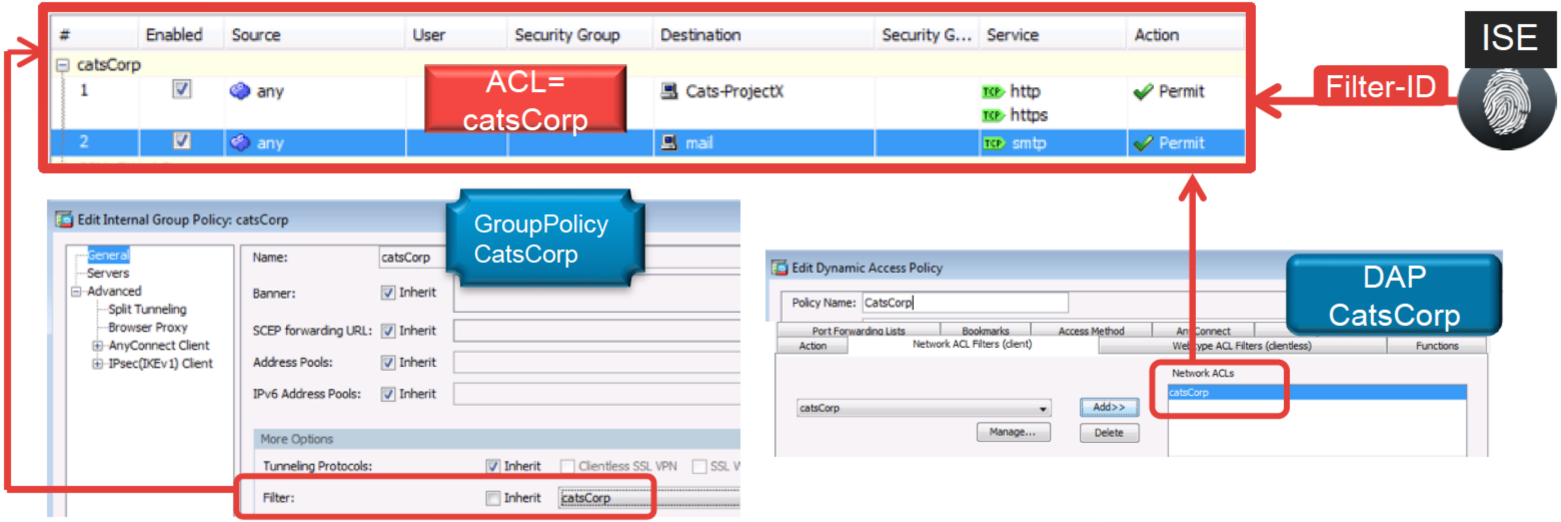
Dynamic Authorization
(CoA, Change of Authorization)

ASA Authorisation Options

- IETF Class Attribute
  - Map to Group Policy where Filter ACL, VLAN restriction etc. defined
- IETF Filter ID Attribute
  - Map to ACL pre-defined on ASA
- DAP (Dynamic Access Policy) specifying ACL
- Downloading ACL (dACL)
  - ACL defined on ISE and downloaded with RADIUS to ASA
- Security Group Tag (SGT)

ACLs Downloaded to ASA

- Other ACL options: Group Policy, DAP, Filter-ID, dACL
  - applied from different places in GUI, separate from main Firewall Ruleset
  - applied from RADIUS (Filter-ID)



#	Enabled	Source	User	Security Group	Destination	Security G...	Service	Action
⊟ catsCorp								
1	☑	any			Cats-ProjectX		http https	✓ Permit
2	☑	any			mail		smtp	✓ Permit

Edit Internal Group Policy: catsCorp

- General
- Servers
- ⊟ Advanced
  - Split Tunneling
  - Browser Proxy
  - ⊞ AnyConnect Client
  - ⊞ IPsec(IKEv1) Client

Name: catsCorp

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: ☑ Inherit □ Clientless SSL VPN □ SSL V

Filter: □ Inherit catsCorp

Edit Dynamic Access Policy

Policy Name: CatsCorp

Port Forwarding Lists | Bookmarks | Access Method | AnyConnect

Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions

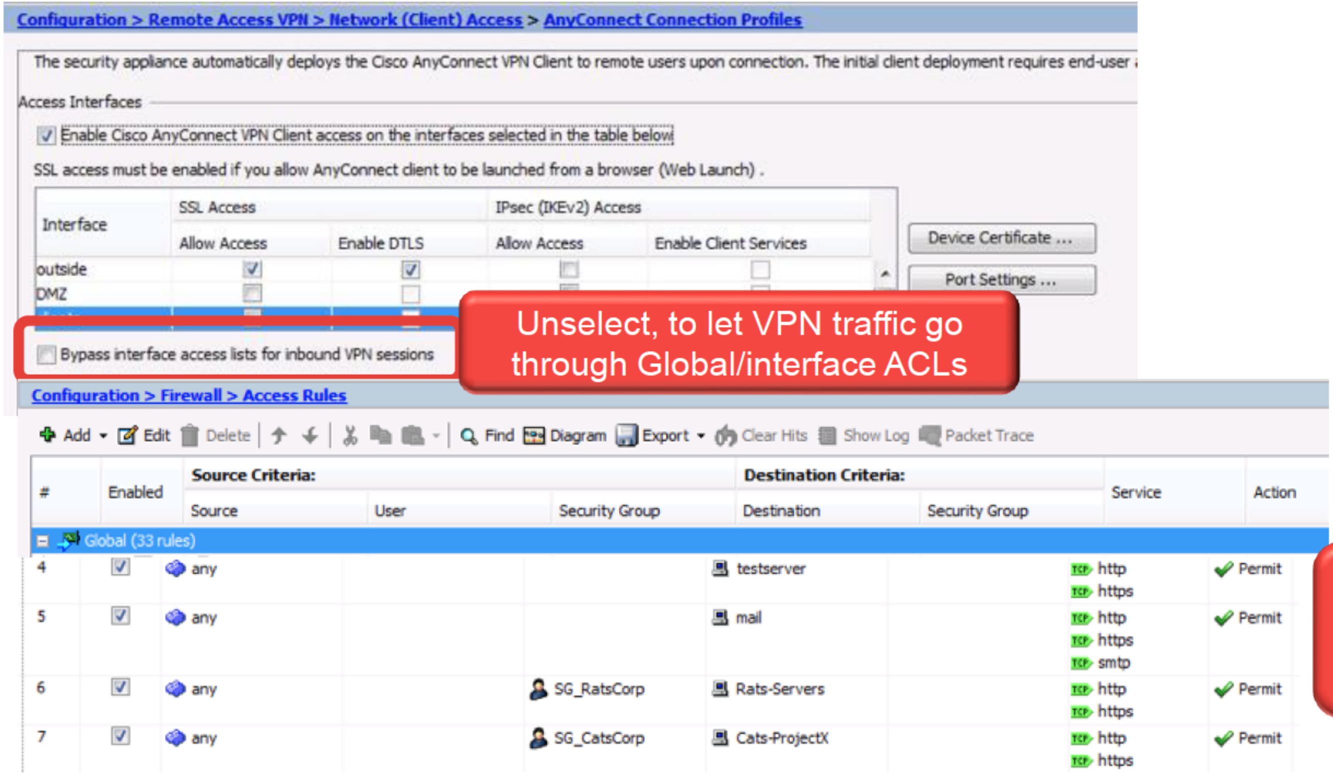
catsCorp

Add>> Manage... Delete

Network ACLs

catsCorp

Consolidated Stateful Access Policy



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☐	☐
DMZ	☐	☐		

☐ Bypass interface access lists for inbound VPN sessions

Unselect, to let VPN traffic go through Global/interface ACLs

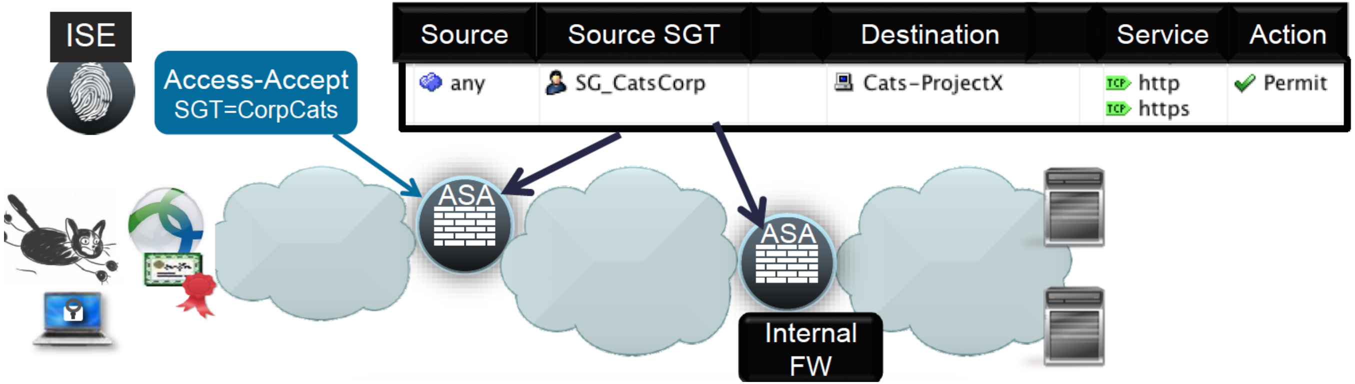
Configuration > Firewall > Access Rules

#	Enabled	Source Criteria:			Destination Criteria:		Service	Action
		Source	User	Security Group	Destination	Security Group		
Global (33 rules)								
4	☑	any			testserver		http https	✓ Permit
5	☑	any			mail		http https smtp	✓ Permit
6	☑	any		SG_RatsCorp	Rats-Servers		http https	✓ Permit
7	☑	any		SG_CatsCorp	Cats-ProjectX		http https	✓ Permit

Mix and Match ACEs with and without SGTs

Secure Group Tagging Authorisation

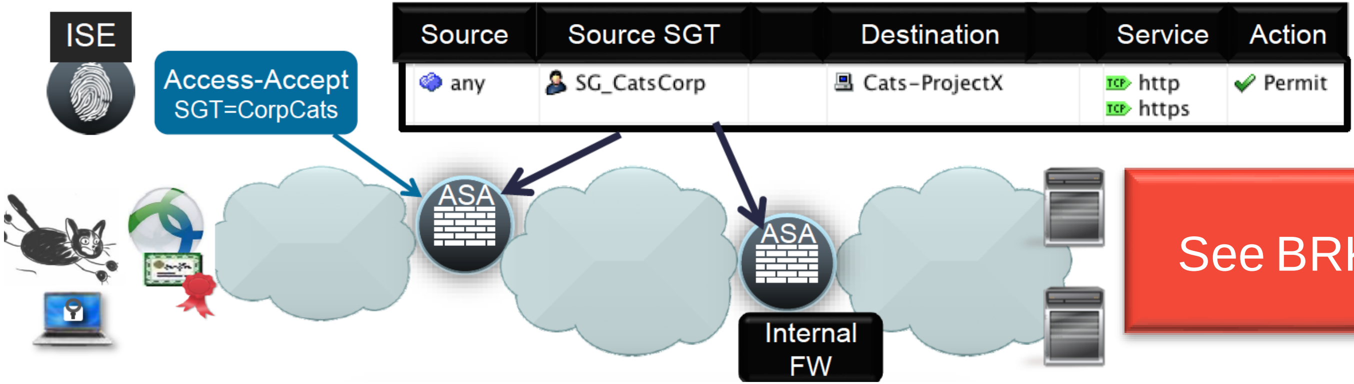
- ISE assigns SGTs to client session
- SGT used by ASA terminating Remote Access for policy enforcement
- ...and/or enforced by downstream device (e.g. ASA or Nexus in DC)
  - SGT info propagated by SXP or native SGT tagging (ASA 9.3.2)



Source	Source SGT	Destination	Service	Action
any	SG_CatsCorp	Cats-ProjectX	TCP http TCP https	✓ Permit

SGT Benefits

- De-coupling ip addressing from security
- Adding context (corporate device, AD group, posture status) to Firewall Rules
- Easy to configure same policy for VPN, Wired, Wireless
- ASA RA config: Consolidated, Stateful Security Policy.



Source	Source SGT	Destination	Service	Action
any	SG_CatsCorp	Cats-ProjectX	TCP http TCP https	✓ Permit

See BRKSEC-2044

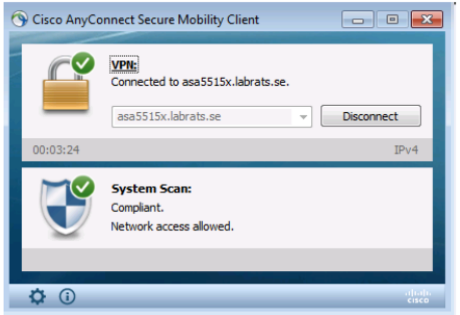
AnyConnect ISE Posture Module

- Windows and MAC
- Checks and Remediates Posture
  - Works on campus (wired, wireless 802.1X)
  - Works with AnyConnect VPN
- Software and XML config file provisioned from
  - ASA
  - ISE or
  - via Desktop Management System
- Requires Compliance Module provisioned from
  - ISE or
  - via Desktop Management System

Desktop Posture Assessment

Agent Listing	Windows AnyConnect / NAC Agent	MAC OSX AnyConnect / NAC Agent
Client Provisioned by ISE	🟩	🟩
Posture Assessment		
Microsoft Updates		**Not Applicable**
Service Packs	🟩	
Hotfixes	🟩	
OS / Browser Versions	🟩	
AntiVirus		
Installation / Signatures	🟩	🟩
AntiSpyware		
Installation / Signatures	🟩	🟩
File Data	🟩	**Not Available**
Services	🟩	
Application / Processes	🟩	
Registry Keys	🟩	
Posture Remediation	🟩	🟩
Passive Re-Assessment (PRA)	🟩	🟩

AnyConnect ISE Posture Flow



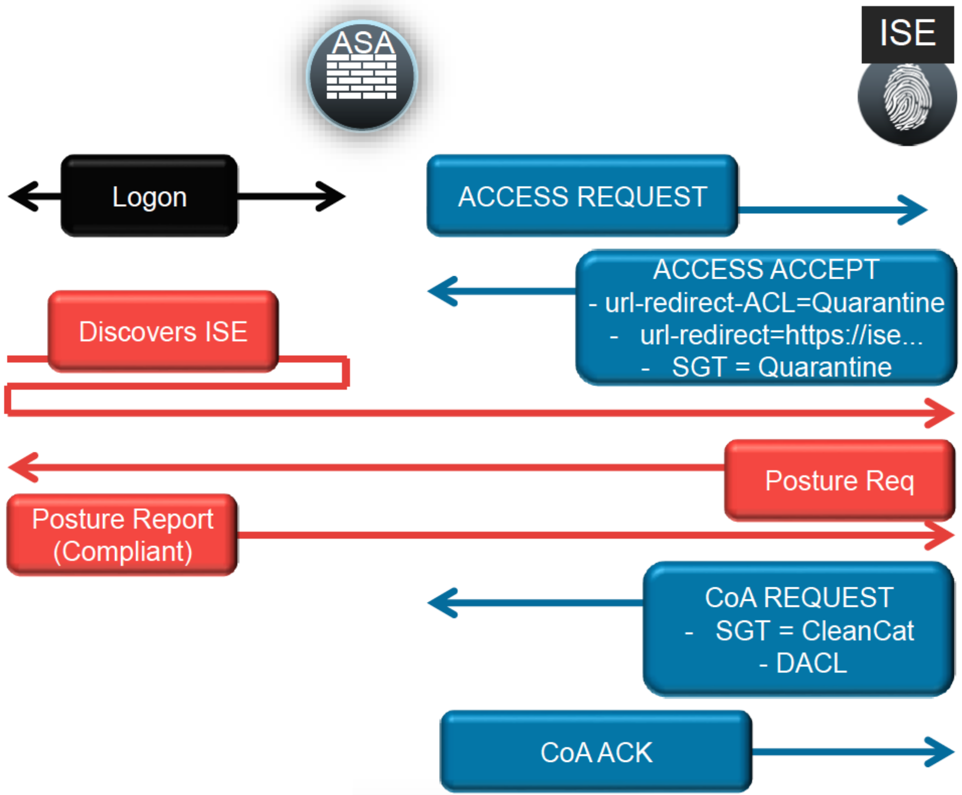
Cisco AnyConnect Secure Mobility Client

VPN:
Connected to asa5515x.labrats.se.

asa5515x.labrats.se
Disconnect

00:03:24
IPv4

System Scan:
Compliant.
Network access allowed.



ASA

ISE

Logon

ACCESS REQUEST

ACCESS ACCEPT
- url-redirect-ACL=Quarantine
- url-redirect=https://ise...
- SGT = Quarantine

Discovers ISE

Posture Req

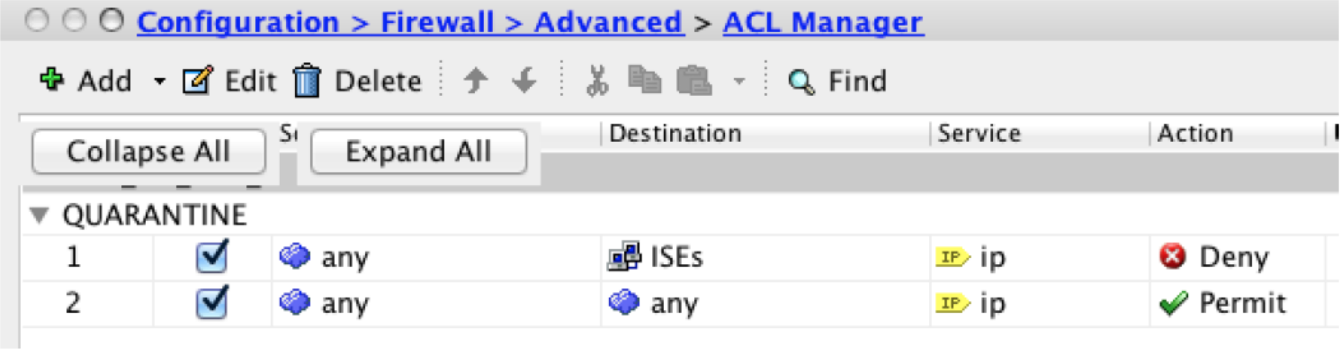
Posture Report
(Compliant)

CoA REQUEST
- SGT = CleanCat
- DACL

CoA ACK

ASA Configuration Requirement

- Configure a standalone ACL
  - permit means redirect traffic to ISE (default)
  - deny means do not redirect : this is traffic to ISE itself, traffic to remediation servers...
  - name of ACL must match RADIUS attribute "url-redirect-acl" signaled by ISE



Configuration > Firewall > Advanced > ACL Manager

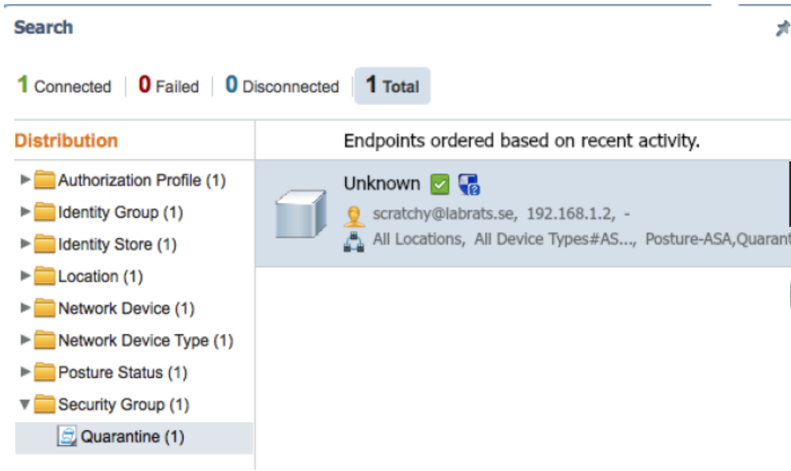
		S	Destination	Service	Action
▼ QUARANTINE					
1	☑	any	ISEs	IP ip	✖ Deny
2	☑	any	any	IP ip	✓ Permit

Deny means "Do not Redirect"

Permit means "Redirect to ISE"

pxGrid with ISE

- ISE knows identity, device, posture status, authentication method for everything
- ISE shares info via pxGrid



Search

1 Connected | 0 Failed | 0 Disconnected | 1 Total

Distribution

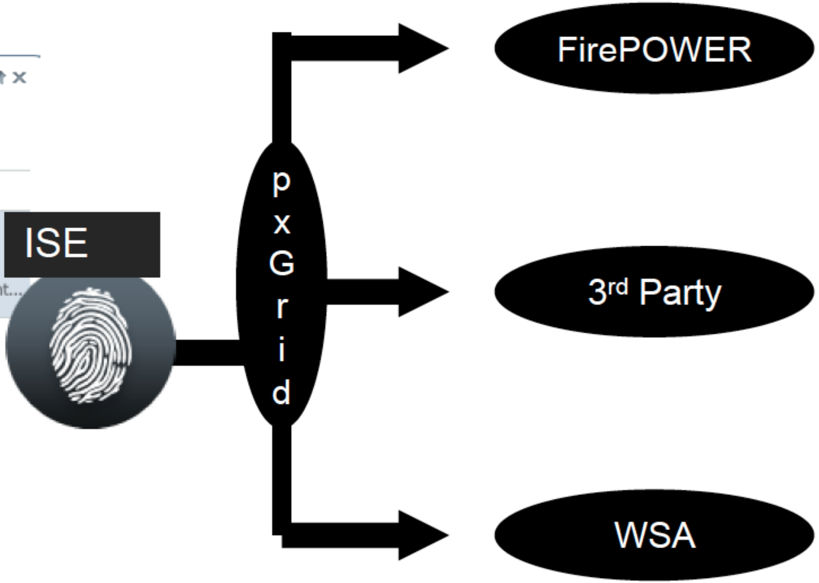
- Authorization Profile (1)
- Identity Group (1)
- Identity Store (1)
- Location (1)
- Network Device (1)
- Network Device Type (1)
- Posture Status (1)
- Security Group (1)
  - Quarantine (1)

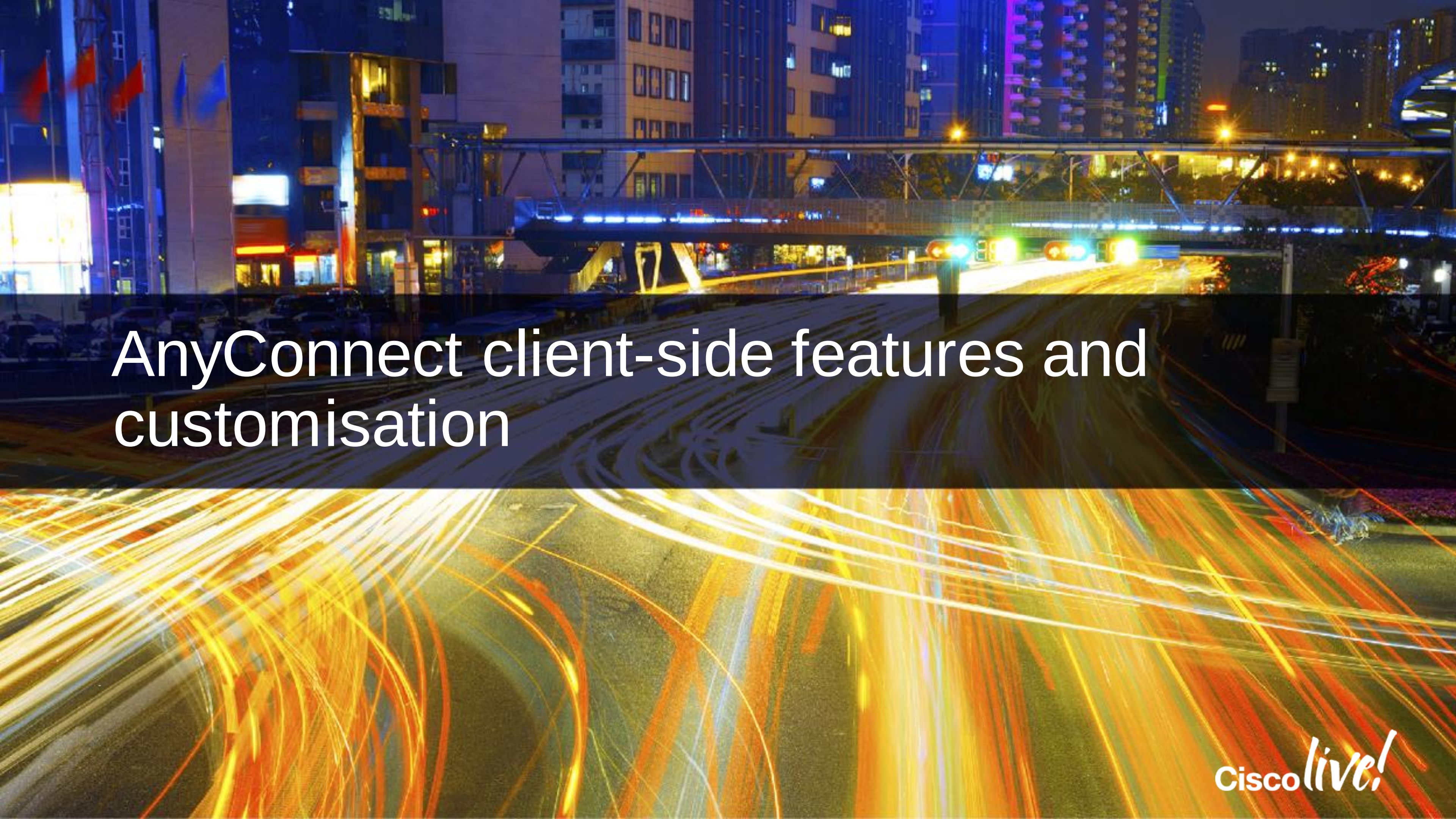
Endpoints ordered based on recent activity.

Unknown

scratchy@labrats.se, 192.168.1.2, -

All Locations, All Device Types#AS..., Posture-ASA,Quarant...

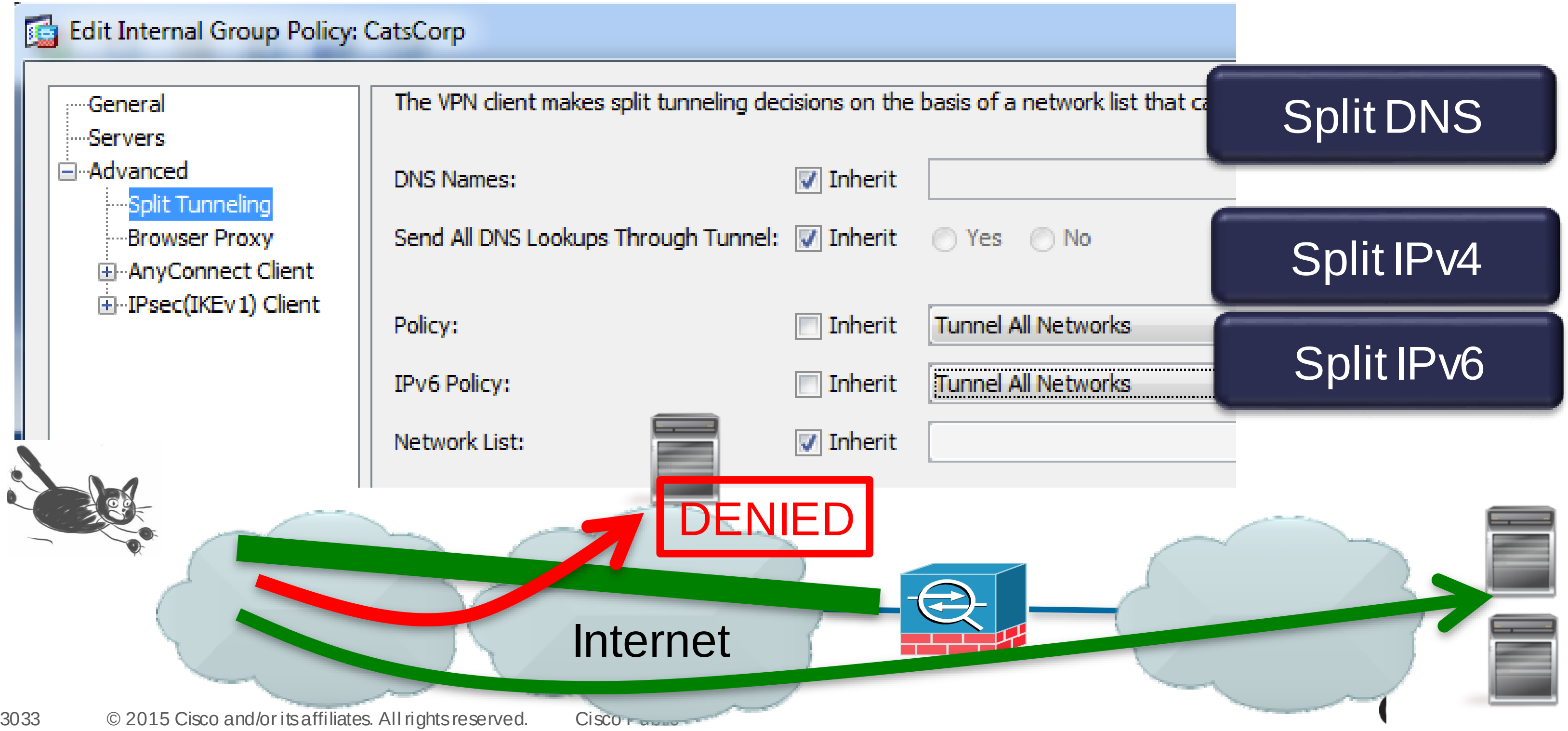




AnyConnect client-side features and customisation

(No) Split Tunnelling Policy

- Defined in Group Policy : whether to allow traffic outside of the tunnel



Edit Internal Group Policy: CatsCorp

The VPN client makes split tunneling decisions on the basis of a network list that ca

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: ☑ Inherit ○ Yes ○ No

Policy: □ Inherit Tunnel All Networks

IPv6 Policy: □ Inherit Tunnel All Networks

Network List: ☑ Inherit

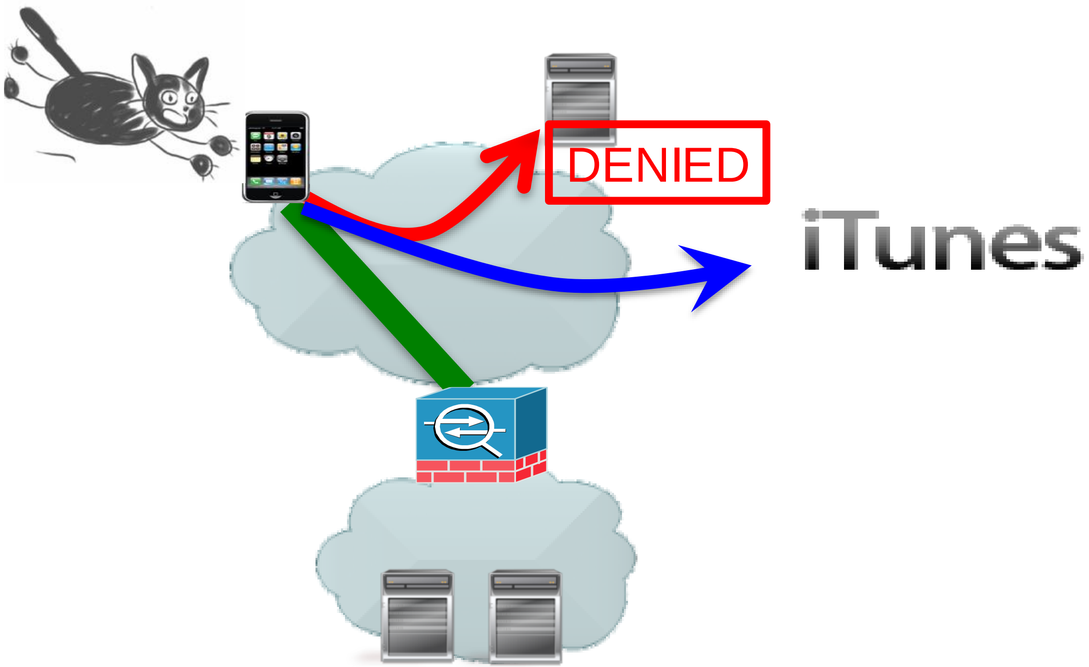
Split DNS

Split IPv4

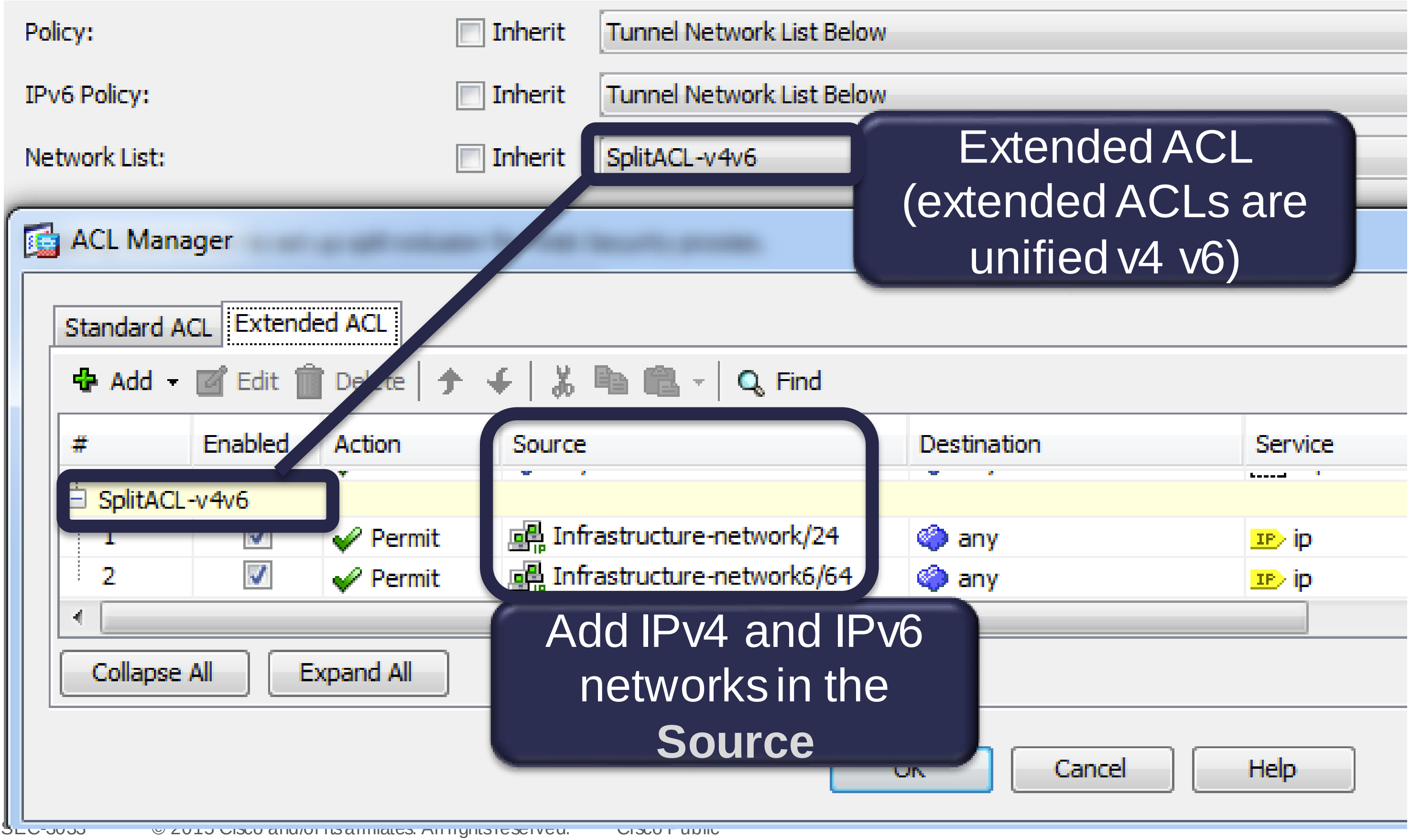
Split IPv6

Note on Split Tunnelling Policy for Mobile Devices

- Even with no Split Tunnelling (Tunnel All Networks), certain traffic from mobile devices (e.g. iTunes) goes outside the tunnel



Split Tunnelling Example (IPv4 and IPv6)



Policy: □ Inherit Tunnel Network List Below

IPv6 Policy: □ Inherit Tunnel Network List Below

Network List: □ Inherit SplitACL-v4v6

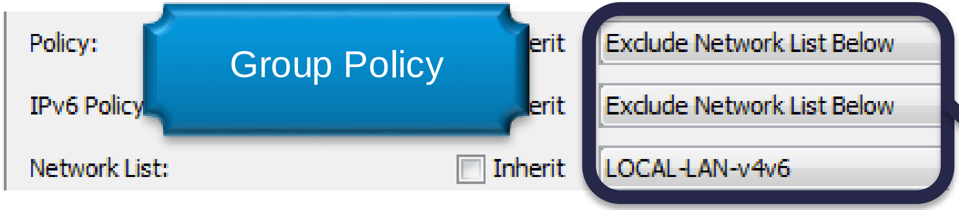
ACL Manager

#	Enabled	Action	Source	Destination	Service
SplitACL-v4v6					
1	☑	✓ Permit	Infrastructure-network/24	any	ip
2	☑	✓ Permit	Infrastructure-network6/64	any	ip

Extended ACL (extended ACLs are unified v4 v6)

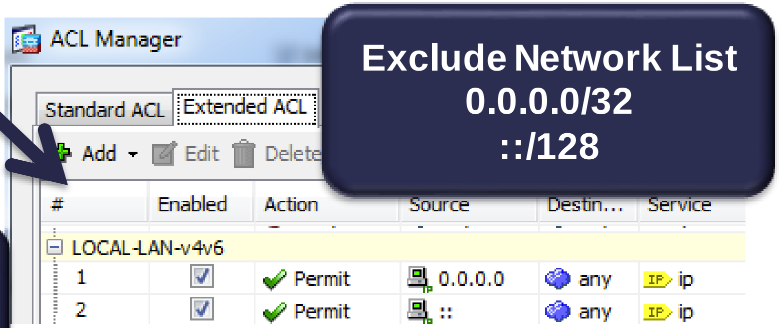
Add IPv4 and IPv6 networks in the **Source**

No Split Tunnelling but Allow Local LAN Access



Group Policy

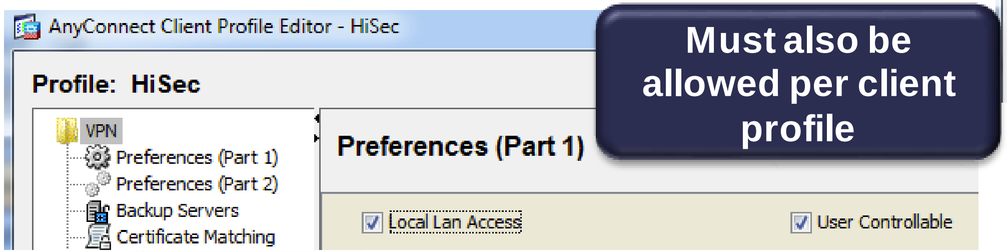
Policy:	erit	Exclude Network List Below
IPv6 Policy	erit	Exclude Network List Below
Network List:	□ Inherit	LOCAL-LAN-v4v6



ACL Manager

Exclude Network List
0.0.0.0/32
::/128

#	Enabled	Action	Source	Destin...	Service
LOCAL-LAN-v4v6					
1	☑	✓ Permit	0.0.0.0	any	ip
2	☑	✓ Permit	::	any	ip



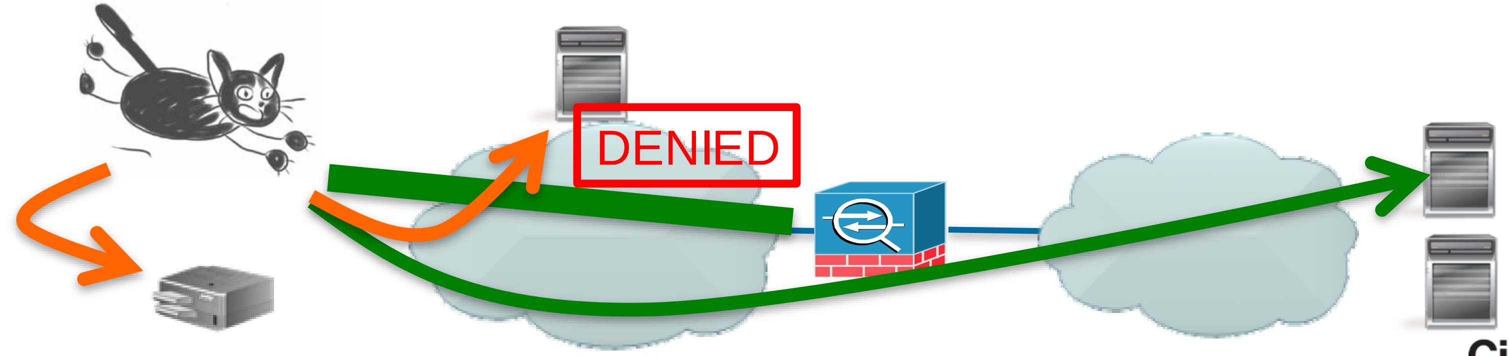
AnyConnect Client Profile Editor - HiSec

Profile: HiSec

Preferences (Part 1)

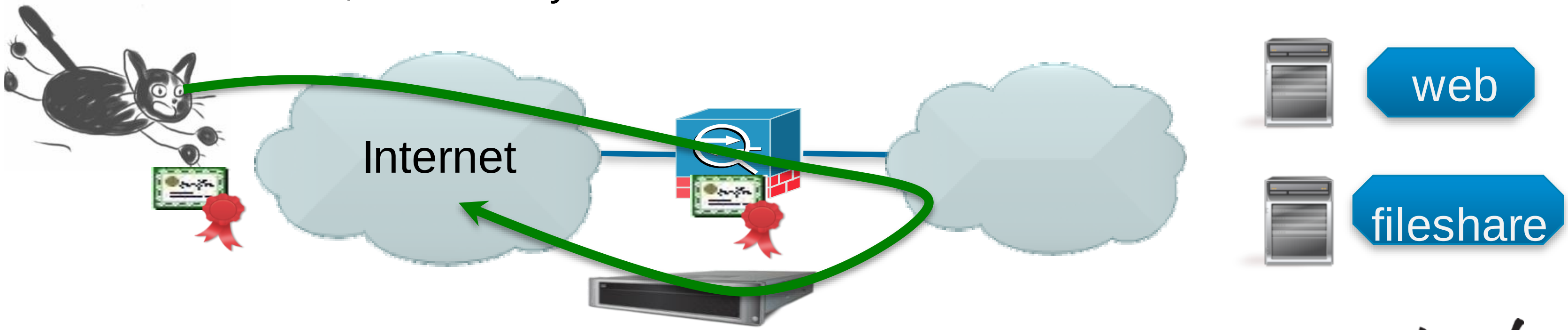
☑ Local Lan Access ☑ User Controllable

Must also be allowed per client profile



Seamless Security with Always-On

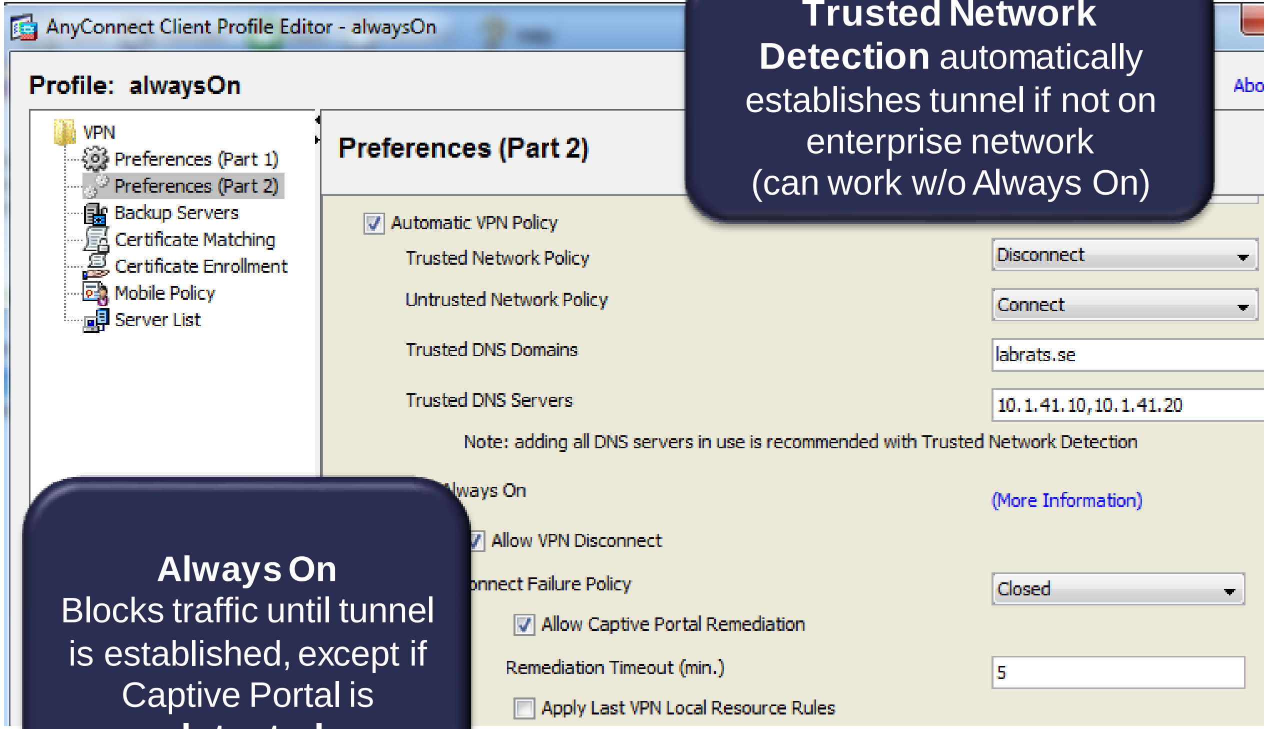
- Force (some) users to always be connected over VPN when off-premises
  - works on Windows, MAC
- Objective #1: Increased Security if surfing out via Enterprise Proxy
  - WCCP or Explicitly Proxy (centrally configured at ASA)
- Objective #2 : Seamless, simple user experience
  - Automatic Connection, "I am always at work" ☺



AnyConnect Client Profile with Always-On

AnyConnect Client Profile

- Define conditions for Trusted Network Detection (DNS Servers and Domain)
- Define Always-On (don't forget Server List)
- Connection Failure Policy : Open or Closed
  - Balance Security Requirements vs. Risk of No Network...
  - If Closed, specify if traffic will be allowed for X minutes if Captive Portal is **detected**
  - "Last VPN Local Resource Rules" : Last Client Firewall Rules



Profile: alwaysOn

Preferences (Part 2)

☑ Automatic VPN Policy

Trusted Network Policy: Disconnect

Untrusted Network Policy: Connect

Trusted DNS Domains: labrats.se

Trusted DNS Servers: 10.1.41.10,10.1.41.20

Note: adding all DNS servers in use is recommended with Trusted Network Detection

lways On

☑ Allow VPN Disconnect

nnect Failure Policy: Closed

☑ Allow Captive Portal Remediation

Remediation Timeout (min.): 5

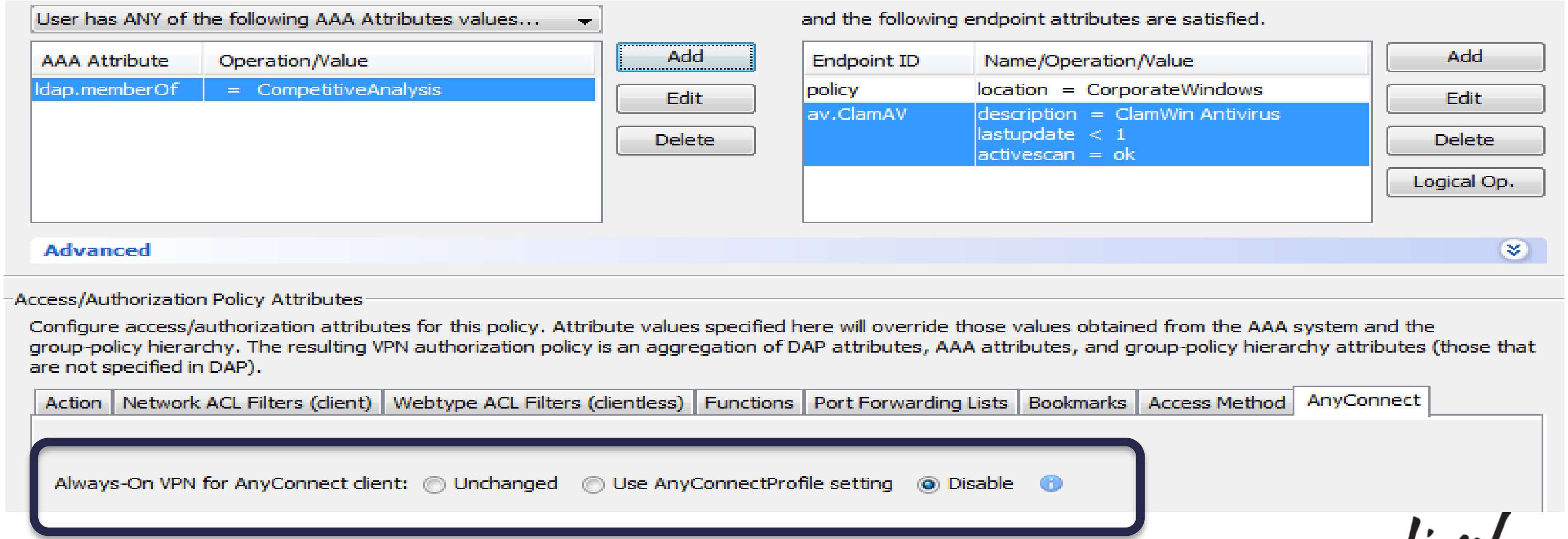
☐ Apply Last VPN Local Resource Rules

Trusted Network Detection automatically establishes tunnel if not on enterprise network (can work w/o Always On)

Always On
Blocks traffic until tunnel is established, except if Captive Portal is **detected**

Disabling Always-On with DAP

- Always-On can be disabled by DAP
- AnyConnect will remember this setting when disconnected



User has ANY of the following AAA Attributes values...

AAA Attribute	Operation/Value
ldap.memberOf	= CompetitiveAnalysis

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
policy	location = CorporateWindows

av.ClamAV	description = ClamWin Antivirus
	lastupdate < 1
	activescan = ok

Access/Authorization Policy Attributes

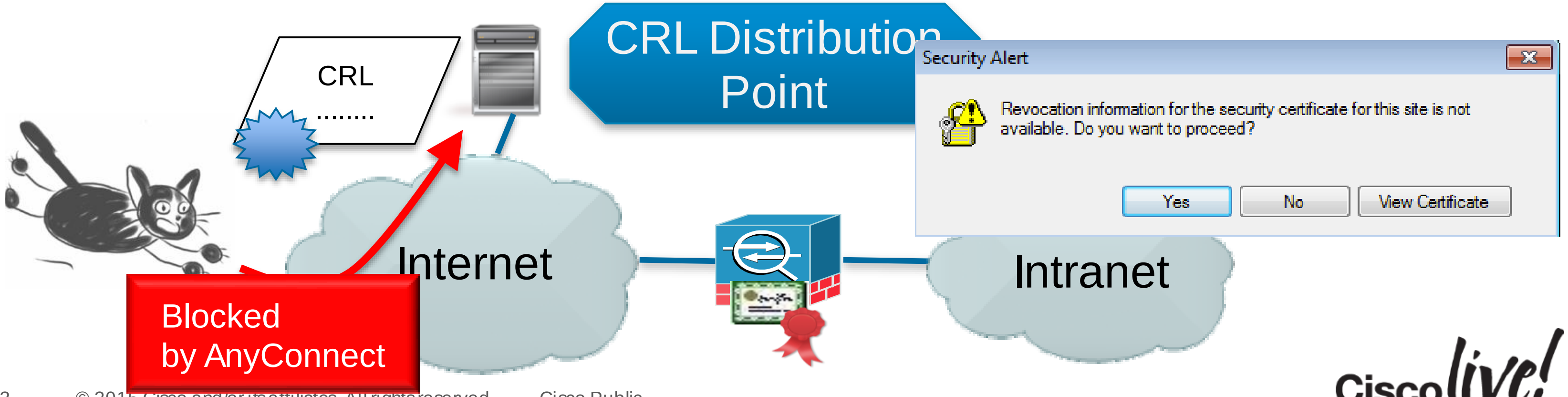
Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Always-On VPN for AnyConnect client: ○ Unchanged ○ Use AnyConnectProfile setting ● Disable

Always-On and Strict Certificate Trust

Warning

- With Always-On, AnyConnect always applies **strict certificate trust** (regardless of the localpolicy file)
- With Always-On, AnyConnect **blocks outgoing traffic** to all destinations other than the ASAs in the server-list of the client profile (and DNS and DHCP)
  - If the CRL of ASA certificate has expired, the client will not be able to retrieve a new CRL, and connection will fail in **previous** versions of AnyConnect



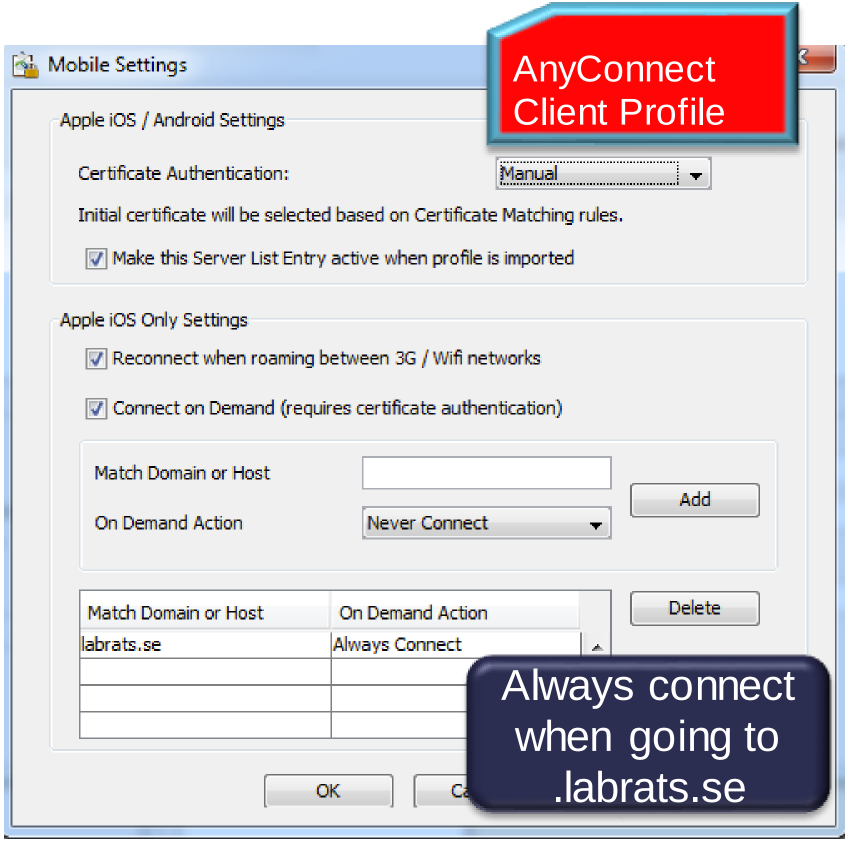
Security Alert

Revocation information for the security certificate for this site is not available. Do you want to proceed?

Always On Does Not Work for Mobile Devices

- Forcing Always-On not possible due to lack of OS APIs
  - ... vendor considerations for battery life, security
- Trusted Network Detection (TND) for Android
- On Demand VPN for iOS

On Demand VPN for iOS - Configuration



Mobile Settings

Apple iOS / Android Settings

Certificate Authentication: Manual

Initial certificate will be selected based on Certificate Matching rules.

☑ Make this Server List Entry active when profile is imported

Apple iOS Only Settings

☑ Reconnect when roaming between 3G / Wifi networks

☑ Connect on Demand (requires certificate authentication)

Match Domain or Host:

On Demand Action: Never Connect

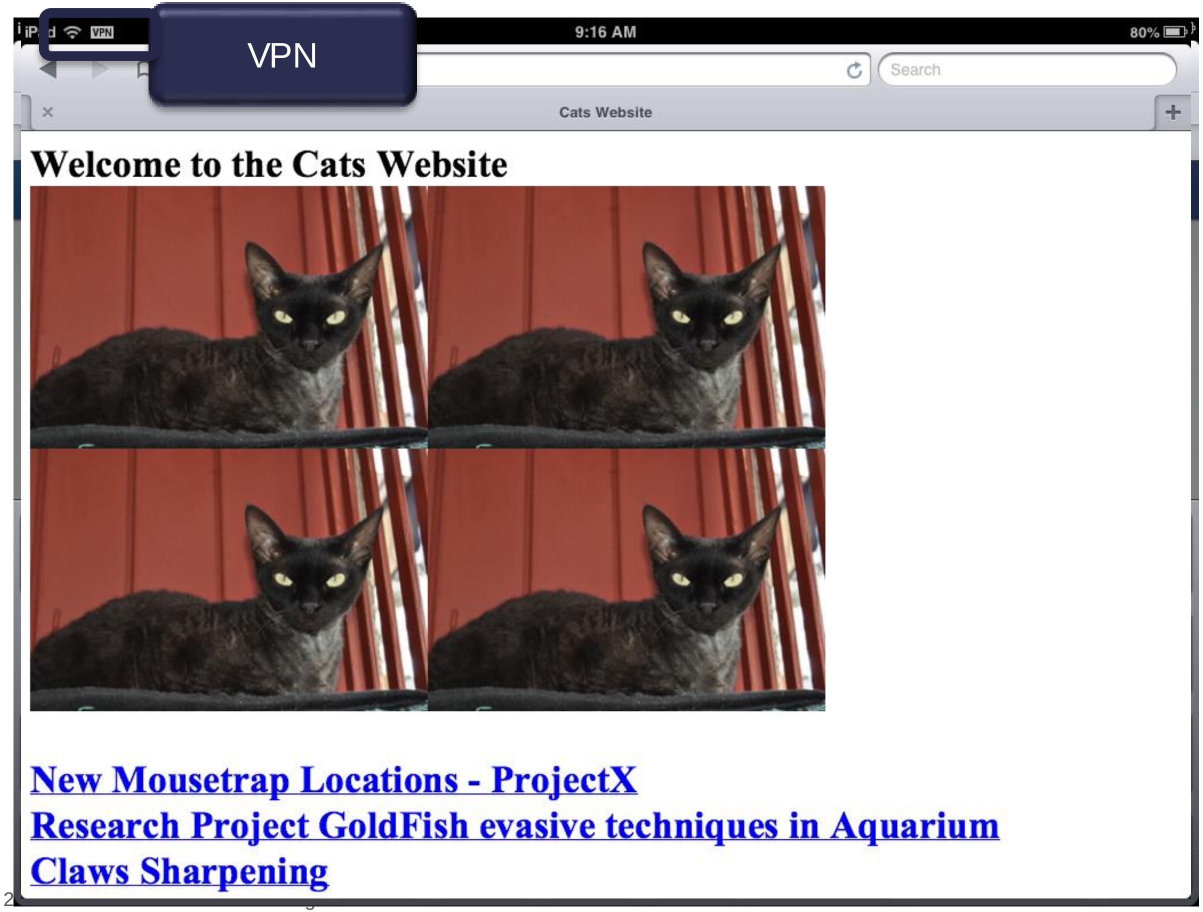
Match Domain or Host	On Demand Action
labrats.se	Always Connect

AnyConnect Client Profile

Always connect when going to .labrats.se

- VPN automatically connected when traffic directed to predefined domain
- Requires client certificate
- Configured in Client Profile/Server List/Additional Mobile Only Settings

On Demand VPN for iOS – User Experience

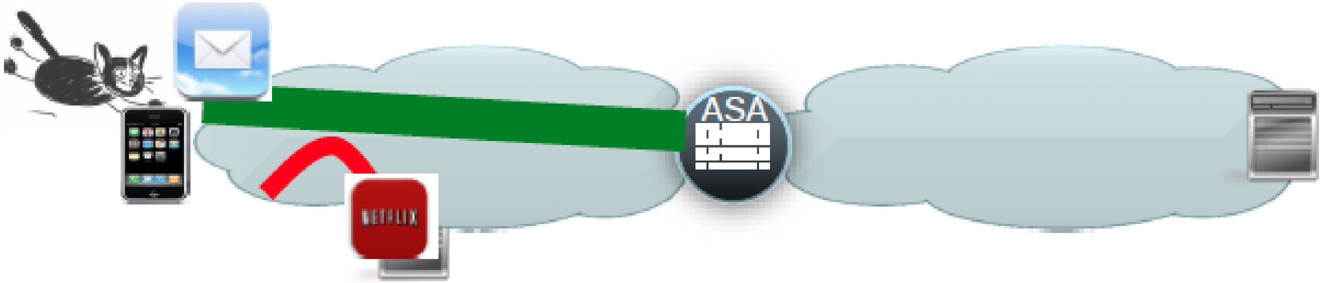


Welcome to the Cats Website

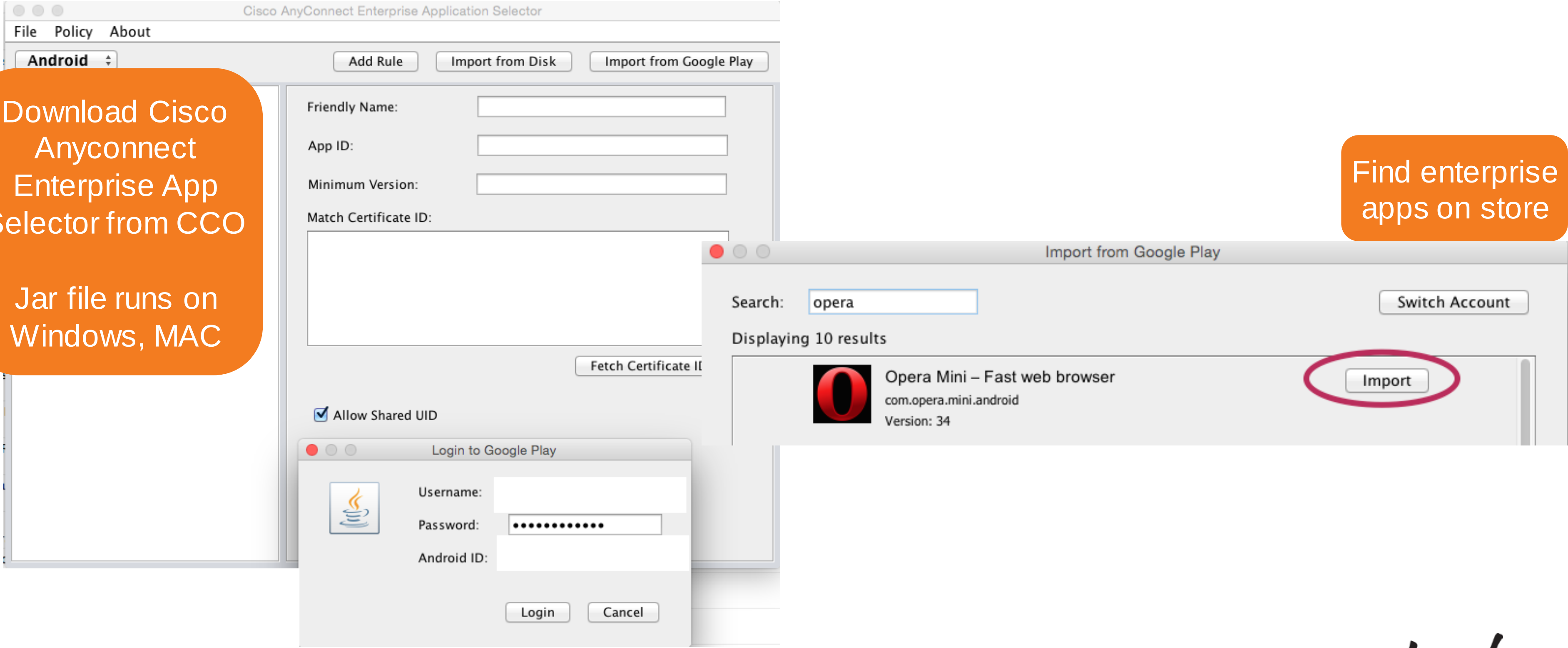
New Mousetrap Locations - ProjectX
Research Project GoldFish evasive techniques in Aquarium
Claws Sharpening

Per-App VPN

- Available for iOS 7.0+, Samsung Knox, Generic Android 5.0+
- Allows for tunnelling specified subset of apps through one AnyConnect tunnel
  - save resources : don’t Netflix over VPN tunnel
  - security: don’t allow non enterprise apps on enterprise network
- Configured via DAP
- Works with or without an Enterprise MDM



Per-app VPN Example - Android



Friendly Name:

App ID:

Minimum Version:

Match Certificate ID:

☑ Allow Shared UID

Username:

Password: •••••••••••••

Android ID:

Search: opera

Displaying 10 results

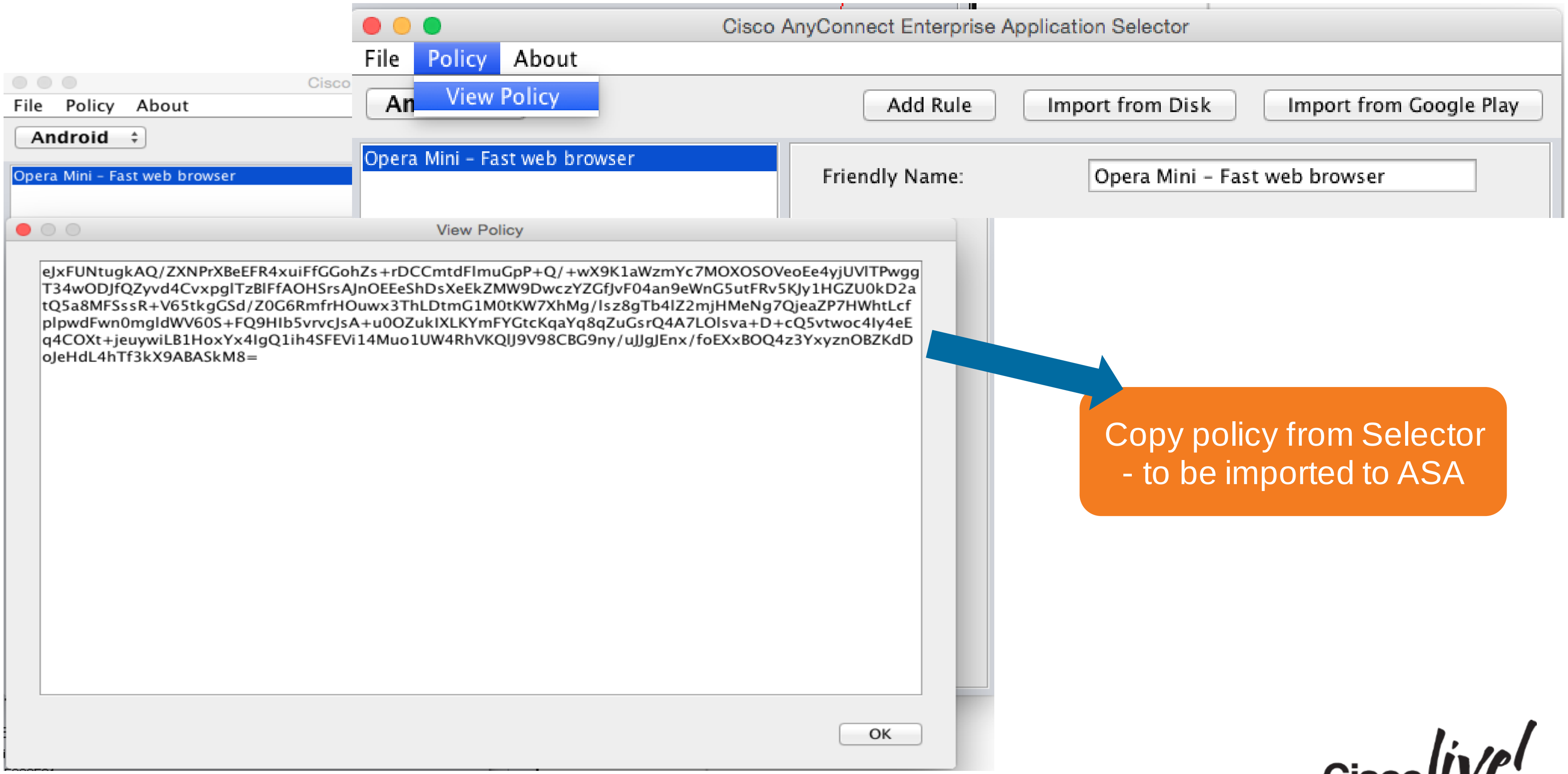
Opera Mini – Fast web browser
com.opera.mini.android
Version: 34

Download Cisco Anyconnect Enterprise App Selector from CCO

Jar file runs on Windows, MAC

Find enterprise apps on store

Per-app VPN Example - Android

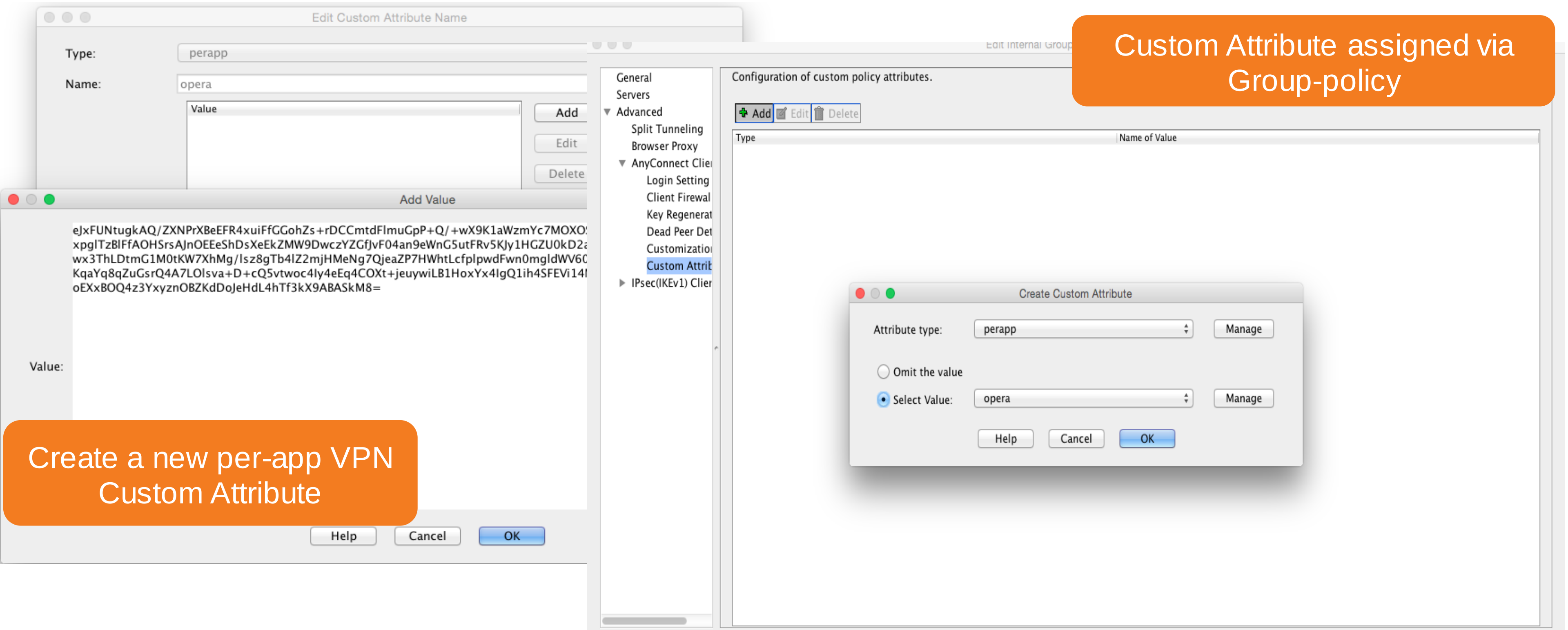


Friendly Name: Opera Mini – Fast web browser

eJxFUNtugkAQ/ZXNPrXBeEFR4xuiFfGGohZs+rDCCmtdFlmuGpP+Q/+wX9K1aWzmYc7MOXOSOVeoEe4yjUVlTPwgg
T34wODJfQZyvd4CvxpglTzBlFfAOHSrsAJnOEEeShDsXeEkZMW9DwczYZGfJvF04an9eWnG5utFRv5KJy1HGZU0kD2a
tQ5a8MFSssR+V65tkgGSd/Z0G6RmfrHOuwx3ThLDtmG1M0tKW7XhMg/lsz8gTb4lZ2mjHMeNg7QjeaZP7HWhtLcf
plpwdFwn0mgldWV60S+FQ9HIb5vrvcJsA+u0OZukIXLKYmFYGtcKqaYq8qZuGsrQ4A7LOlsva+D+cQ5vtwoc4ly4eE
q4COXt+jeuywiLB1HoxYx4lgQ1ih4SFEVi14Muo1UW4RhVKQlJ9V98CBG9ny/uJJgJEnx/foEXxBOQ4z3YxyznOBZKdD
oJeHdL4hTf3kX9ABASkM8=

Copy policy from Selector - to be imported to ASA

Per-app VPN Example - Android



Type: perapp

Name: opera

Value

Value:

eJxFUNtugkAQ/ZXNPrXBeEFR4xuiFfGGohZs+rDCCmtdFlmuGpP+Q/+wX9K1aWzmYc7MOXO
xpglTzBlFfAOHSrsAJnOEEeShDsXeEkZMW9DwczYZGfJvF04an9eWnG5utFRv5KJy1HGZU0kD2
wx3ThLDtmG1M0tKW7XhMg/lsz8gTb4lZ2mjHMeNg7QjeaZP7HWhtLcfplpwdFwn0mgldWV6
KqaYq8qZuGsrQ4A7LOlsva+D+cQ5vtwoc4ly4eEq4COXt+jeuywiLB1HoxYx4IgQ1ih4SFEVi14
oEXxBOQ4z3YxyznOBZKdDoJeHdL4hTf3kX9ABASkM8=

Configuration of custom policy attributes.

Attribute type: perapp

○ Omit the value

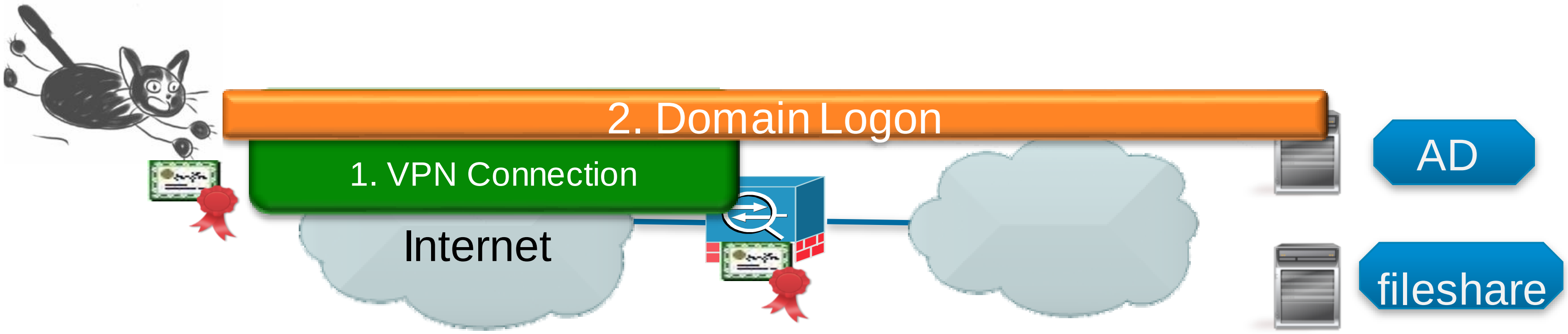
● Select Value: opera

Create a new per-app VPN Custom Attribute

Custom Attribute assigned via Group-policy

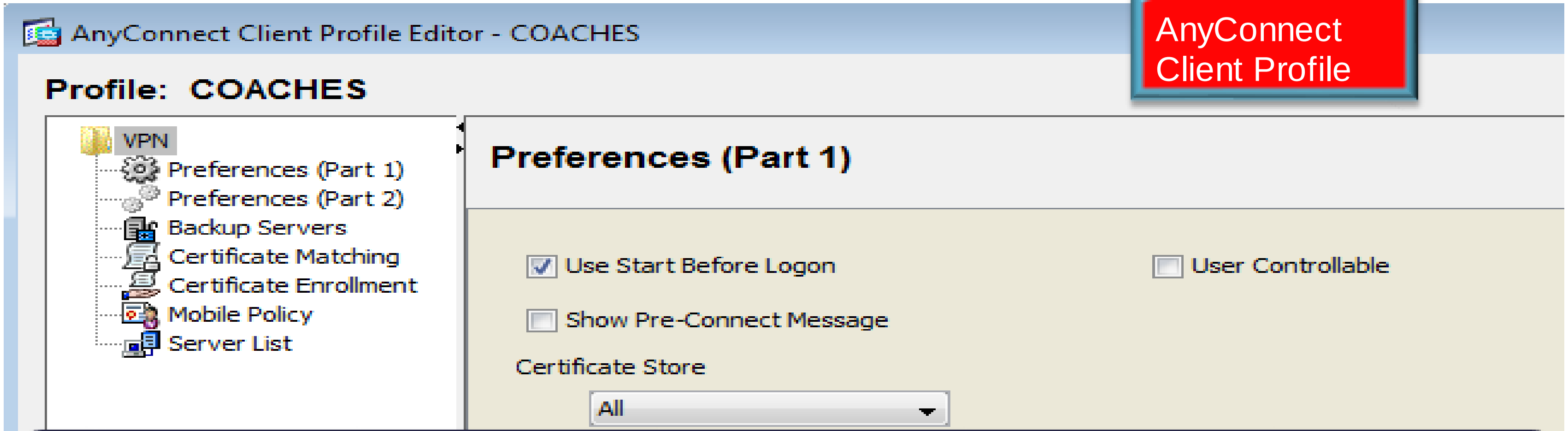
Seamless Office Experience by Start-Before-Logon

- Allows (some) Windows users to connect VPN before logging into computer
- Why? Allow domain-logon, GPOs, logon-scripts, change passwords, etc...
- Can be used with or without Always-On



Configuring SBL in Client Profile

- May make it user controllable



AnyConnect Client Profile

AnyConnect Client Profile Editor - COACHES

Profile: COACHES

Preferences (Part 1)

☑ Use Start Before Logon

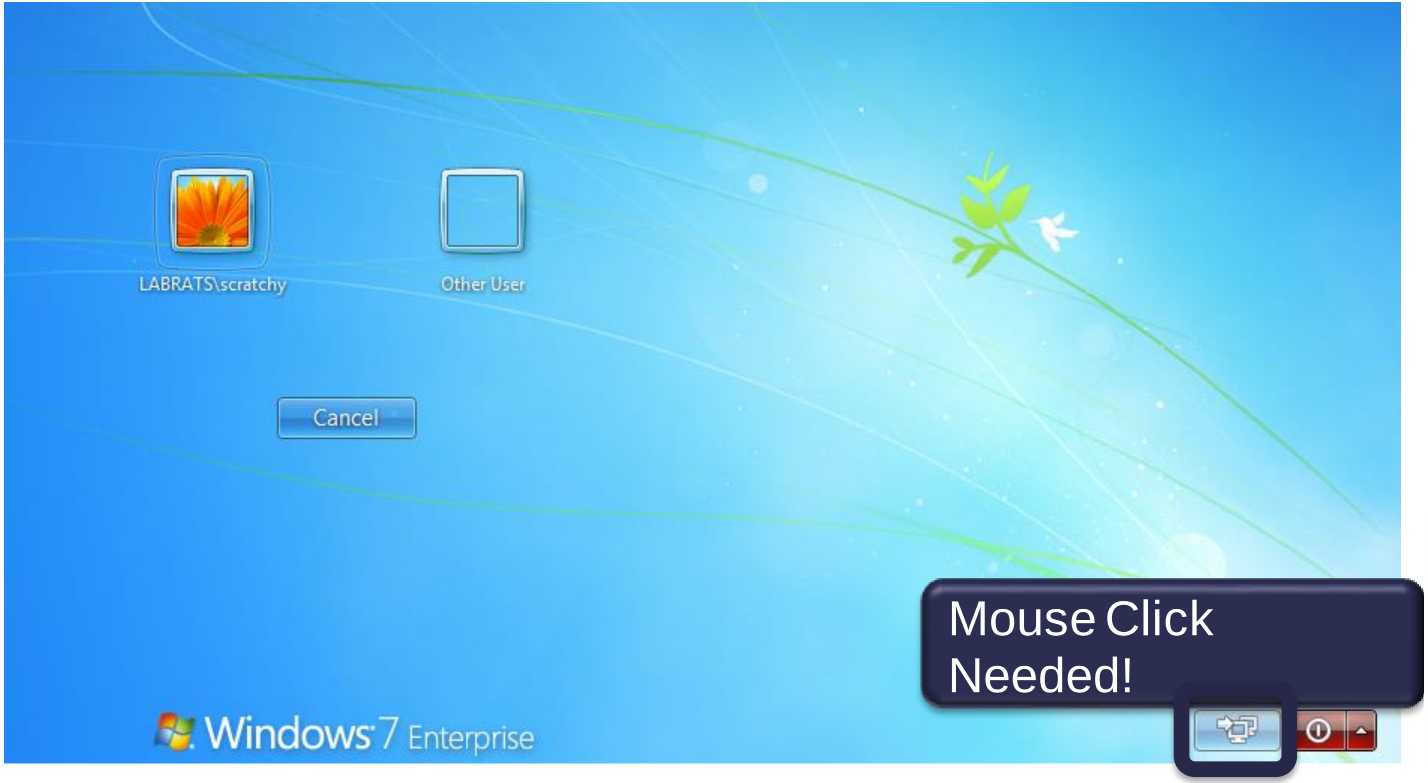
□ User Controllable

□ Show Pre-Connect Message

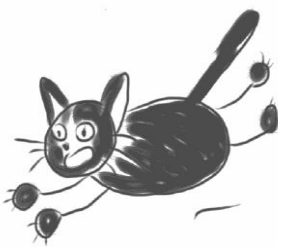
Certificate Store: All

Note : Client certificates in User Store typically not accessible before logon (no knowledge of who the user is).
Client certificates on Smart Cards will work!

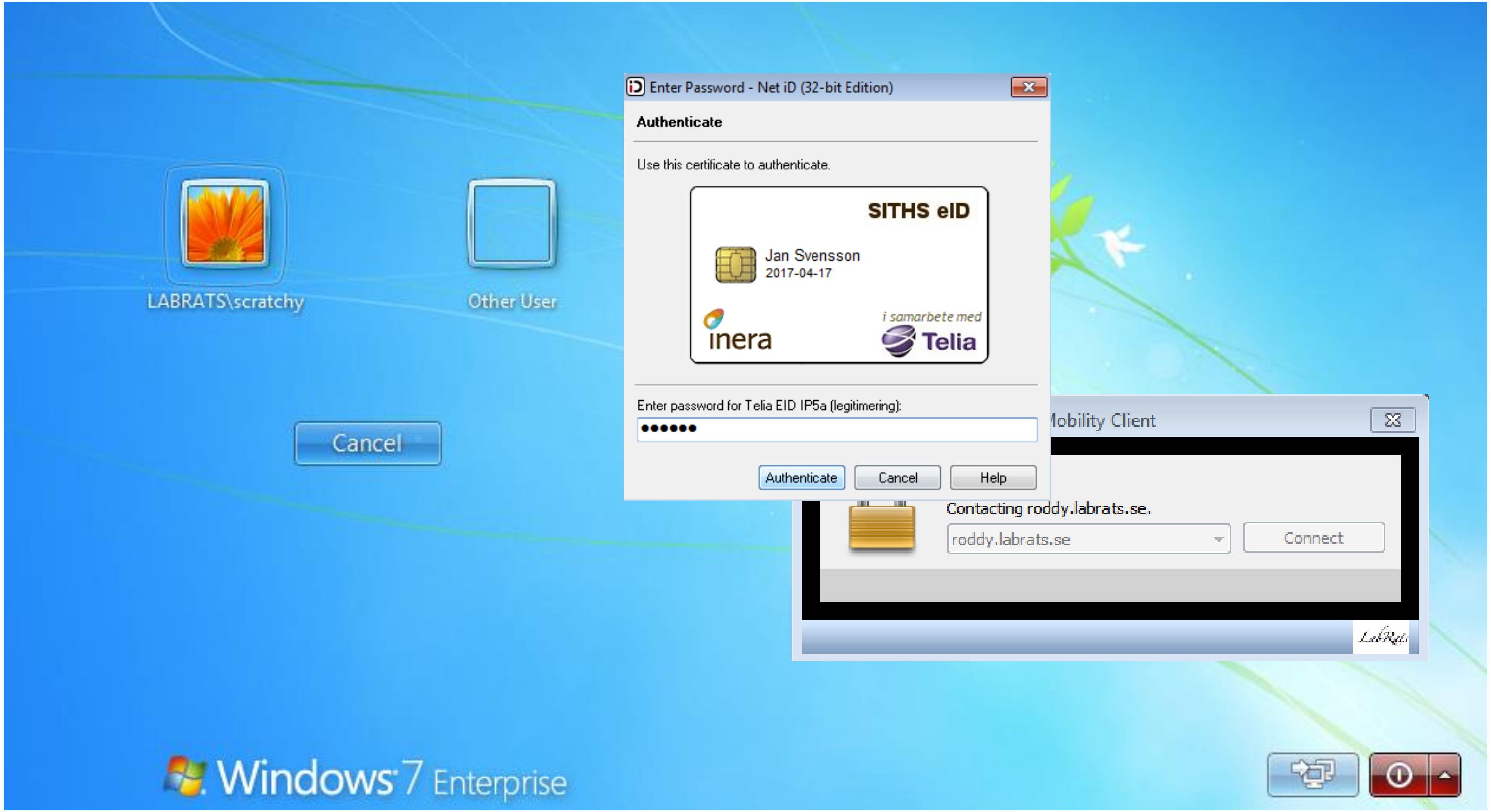
SBL User Experience



Mouse Click Needed!



SBL User Experience with Smart Cards (2)



Enter Password - Net iD (32-bit Edition)

Authenticate

Use this certificate to authenticate.

SITHS eID

Jan Svensson
2017-04-17

inera

i samarbete med Telia

Enter password for Telia EID IP5a (legitimering):

●●●●●●

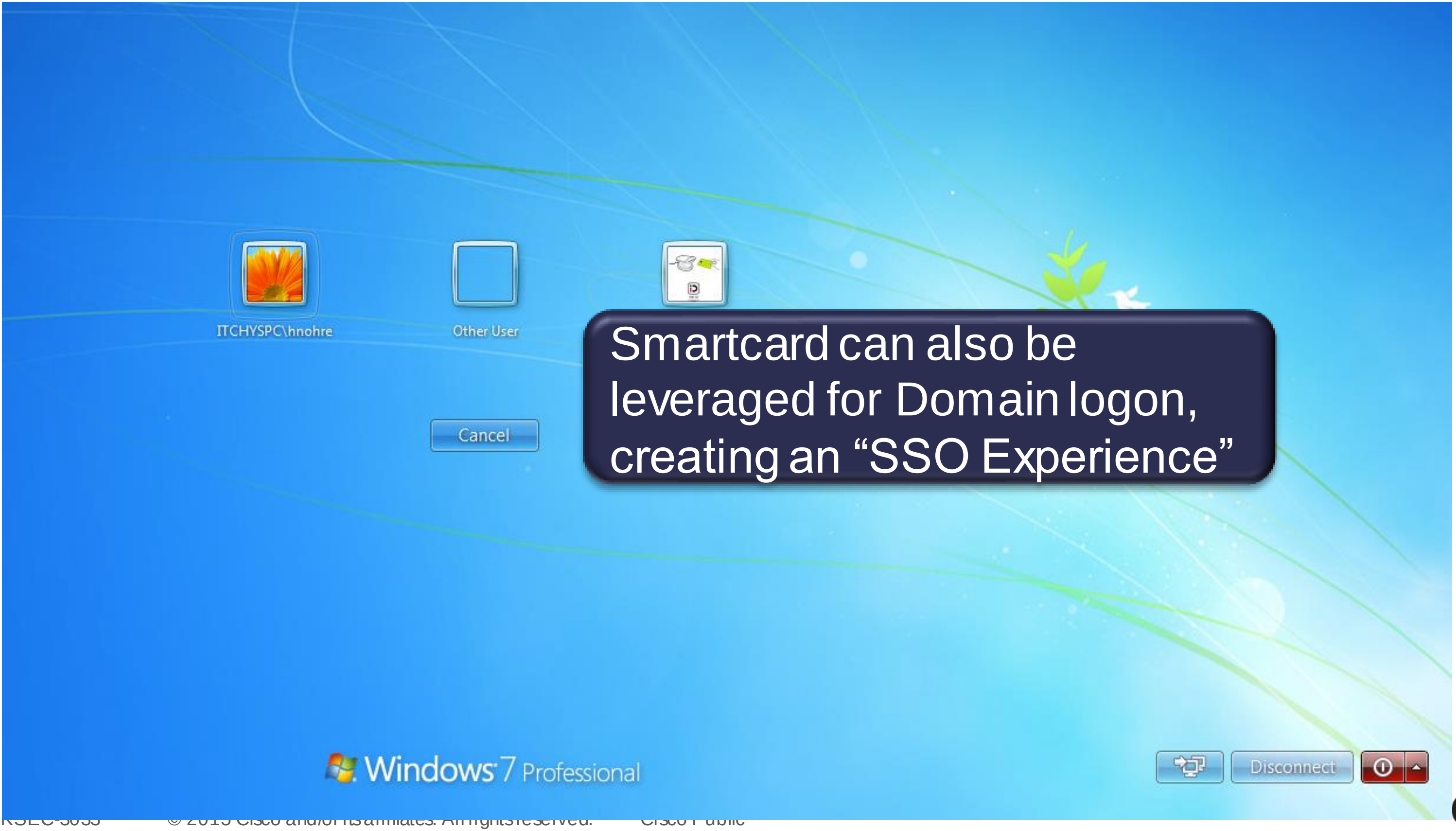
Authenticate | Cancel | Help

Mobility Client

Contacting roddy.labrats.se.

roddy.labrats.se | Connect

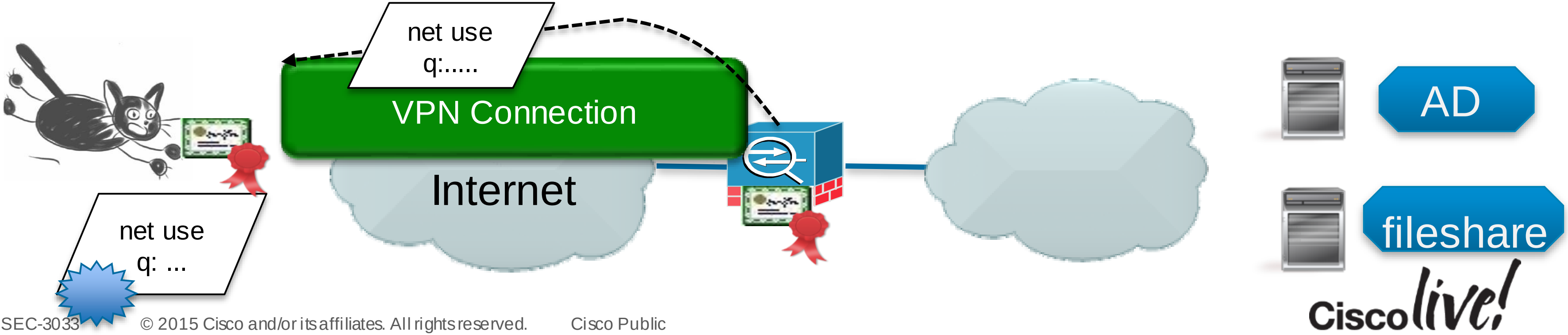
SBL User Experience with Smartcards (3)



Smartcard can also be leveraged for Domain logon, creating an “SSO Experience”

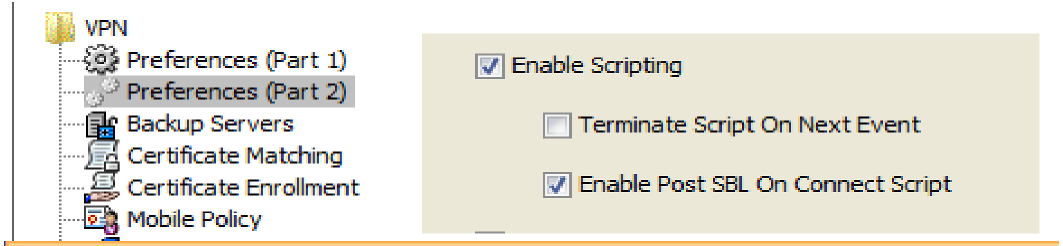
Running Scripts after Connect and Disconnect

- Runs a predefined script when (some) users connect to (or disconnect from VPN)
- Any native script language understood by client (*.vbs, *.sh etc)
- Script can be downloaded from ASA, or distributed by some other means
- Why?
  - Allow mapping of drives, GPO-update when SBL is not possible (e.g. behind a captive portal).
  - Also works on non domain members, including MAC, Linux



Configuring Scripting

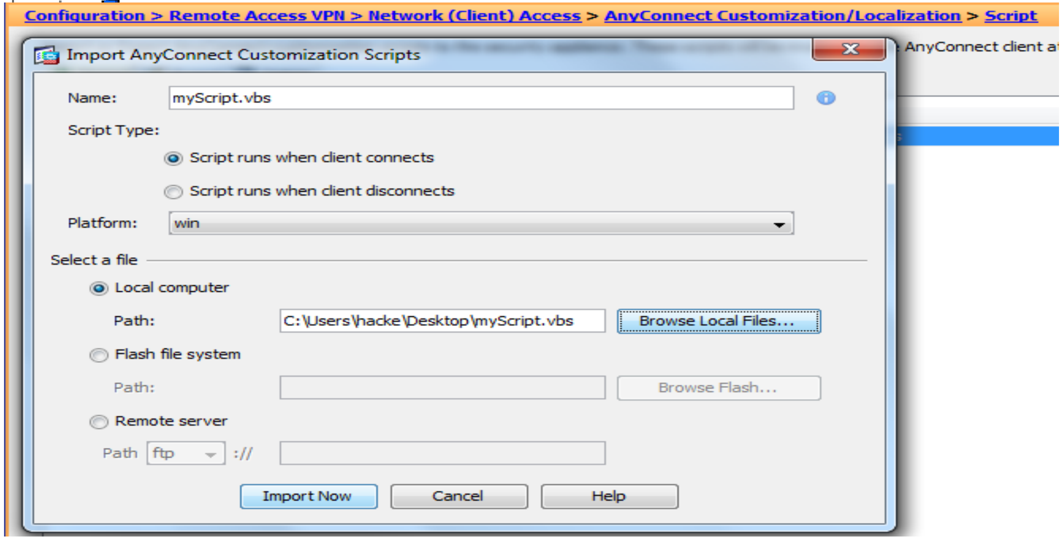
- Enable Scripting in AnyConnect Client Profile
- Optionally : Import script to ASA for download to **all** clients
- Alternatively, use other means of putting the script in the script directory for desired clients



☑ Enable Scripting

□ Terminate Script On Next Event

☑ Enable Post SBL On Connect Script



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Script

Import AnyConnect Customization Scripts

Name: myScript.vbs

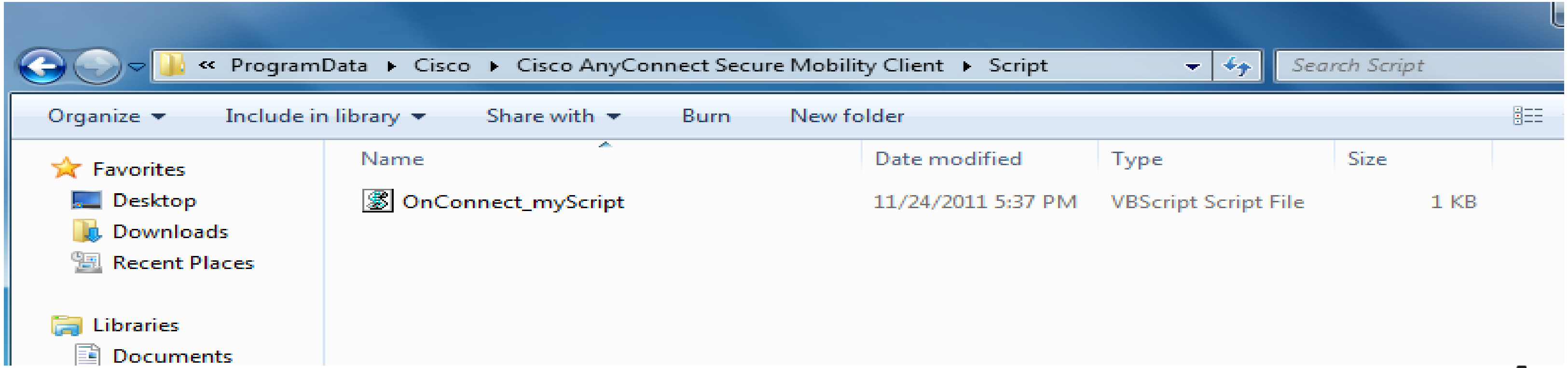
Script Type:
● Script runs when client connects
○ Script runs when client disconnects

Platform: win

Select a file
● Local computer
Path: C:\Users\hacke\Desktop\myScript.vbs
○ Flash file system
Path:
○ Remote server
Path ftp ://

On the Client: The Scripts Folder

- AnyConnect executes the script in the folder that starts with "OnConnect"/"OnDisconnect" after VPN connection/disconnection
- Only one script is executed, but that script can launch other scripts
- Troubleshooting :
  - Check that script exists in folder and that AnyConnect Profile allows scripting.
  - Check that script executes ok when invoked from local machine (permissions etc).



« ProgramData ▸ Cisco ▸ Cisco AnyConnect Secure Mobility Client ▸ Script

Name	Date modified	Type	Size
OnConnect_myScript	11/24/2011 5:37 PM	VBScript Script File	1 KB

Conclusion

- Secure Client with a Seamless User Experience
- Strong authentication and Granular Access Control with AAA and DAP
- Consider using ISE for Unified Access (VPN, Wired, Wireless)
- Find Balance between Requirements and Complexity (testing, maintenance)
- Good security and networking skills are essential, but also knowledge of adjacent technologies such as Active Directory, LDAP and PKI, ISE… as well as different client platforms

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

Thank you.

cisco