

Cisco Context Directory Agent Identity Firewall configuration example.

Lab using CDA 1.0.0.011 – patch 1 -> 6

Guillermo González
GVE VSE Security
gugonza2@cisco.com

Table of Contents

Goal.....	3
Documentation.....	3
Lab Environment.....	3
Lab Schema	4
Installation and Configuration Process.....	4
CDA VM Installation.....	5
Active Directory preparation.....	13
CDA configuration.....	26
ASA configuration	29
Configuring ASA in CDA.....	32
Test	34

NOTE:

This document explain with some notes and screenshot sequences the configuration of “Identity Firewall” features using Cisco Firewall based on ASA Software and the Cisco Context Directory Agent.

Goal

Install and Configure a Laboratory for testing “Identity Firewall” using Context Directory Agent (CDA) with Active Directory and ASA v.

With Identity Firewall, we can configure access-list and allow/restrict permission based on users and/or groups that exist in the Active Directory Domain.

Documentation

This example was implemented with the aid of the following documents:

Installation and Configuration Guide for CDA, release 1.0:

https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_install.html

CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide 9.10:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config.html>

ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide, 7.10:

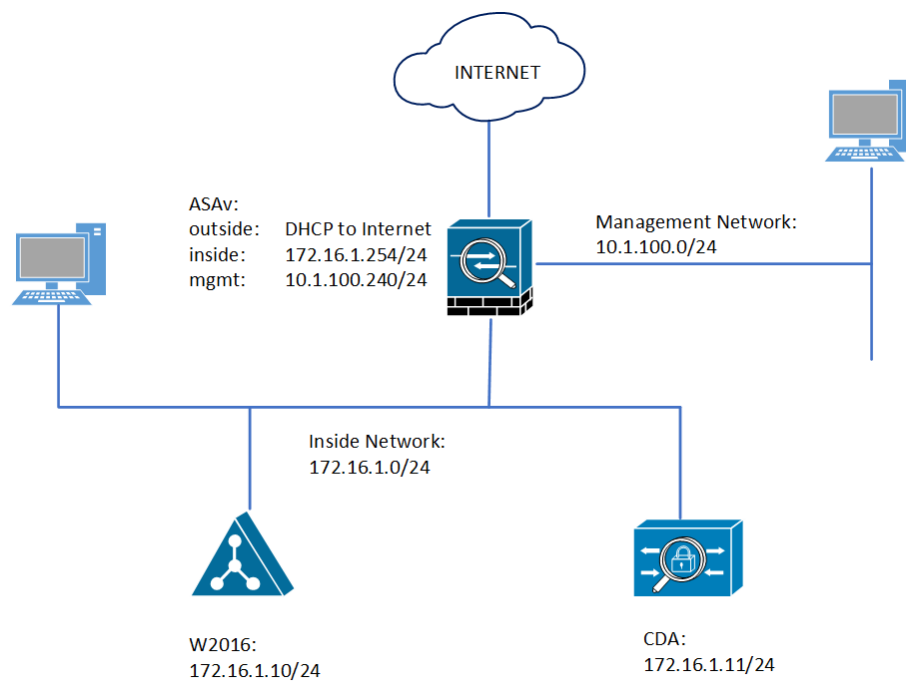
<https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/asdm710/firewall/asdm-710-firewall-config.html>

Lab Environment

- CDA version 1.0.0.011 with all patches installed (1 -> 6).
- ASA v version 9.10
- Windows Server 2016 with DNS, DHCP and Active Directory Roles installed and configured.
- Windows 10 as client stations.

This Lab was installed and configured using VMware Fusion 10.1.5 as Virtual Platform.

Lab Schema



CDA Lab – Network Schema.

Installation and Configuration Process

- CDA Installation.
- Active Directory preparation.
- CDA configuration.
- ASAv configuration.

CDA VM Installation

Requirements:

- 2 vCPUs
- 2 GB RAM
- 120 GB HDD
- 1 vNIC. CDA supports Flexible and E1000 types of NIC. VMXNET2 and VMXNET3 are not supported.

CDA VM is supported on VMware hypervisor.

The latest version of CDA is available in ISO format on Cisco Downloads site:

<https://software.cisco.com/download/home/283123066/type/284724387/release/CDA>

CDA Latest version: 1.0.0.11

Patches available: Patch 1 -> Patch 6 (30 Jan 2019)

The first step must be the creation of VM, installation of CDA using the ISO image and install the patches.

To create the CDA VM we use the Guest OS CentOS 4/5 32 bits.

In this document we proceed to create the Lab using VMware Fusion on Macbook Pro with Mac OS X 10.13.6 (High Sierra).

Selecting the options mentioned we proceed to install the VM:

```

Welcome to the Cisco Context Directory Manager Installer
Cisco CDA Version: 1.0.0.011

Available boot options:

[1] Cisco CDA Installation (Keyboard/Monitor)
[2] Cisco CDA Installation (Serial Console)
[3] Recover administrator password (Keyboard/Monitor)
[4] Recover administrator password (Serial Console)
<Enter> Boot existing OS from hard disk.

Enter boot option and press <Enter>.


boot: 1
```

Welcome to CentOS

Formatting

Formatting / file system...

19%



<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Welcome to CentOS


Package Installation

Name : selinux-policy-targeted-2.4.6-255.el5-noarch
Size : 29187k
Summary: SELinux targeted base policy

100%

	Packages	Bytes	Time
Total :	402	1028M	0:01:02
Completed:	387	892M	0:00:53
Remaining:	15	136M	0:00:08

86%



<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

```
*****  
Please type 'setup' to configure the appliance  
*****  
localhost login: setup
```

```
Press 'Ctrl-C' to abort setup  
Enter hostname[]: cda  
Enter IP address[]: 172.16.1.11  
Enter IP netmask[]: 255.255.255.0  
Enter IP default gateway[]: 172.16.1.254  
Enter default DNS domain[]: cicolab.local  
Enter primary nameserver[]: 172.16.1.10  
Add secondary nameserver? Y/N : N  
Enter primary NTP server[time.nist.gov]:  
Add secondary NTP server? Y/N : N  
Enter system timezone[UTC]: Europe/Madrid  
Enter username[admin]:  
Enter password:  
Enter password again:  
Bringing up network interface...
```

```
Enter default DNS domain[]: cicolab.local
Enter primary nameserver[]: 172.16.1.10
Add secondary nameserver? Y/N : N
Enter primary NTP server[time.nist.gov]:
Add secondary NTP server? Y/N : N
Enter system timezone[UTC]: Europe/Madrid
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Virtual machine detected, configuring VMware tools...
Do not use 'Ctrl-C' from this point on...
Installing applications...
Installing cda ...
Pre install
Post Install

Application bundle (cda) installed successfully

=== Initial Setup for Application: cda ===

Generating configuration...
```



```

rtt min/avg/max/mdev = 0.488/0.700/0.924/0.160 ms

cda/admin# ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=1.53 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.519 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=128 time=0.356 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=128 time=0.449 ms

--- 172.16.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.356/0.714/1.532/0.475 ms

cda/admin# ping www.cisco.com
PING e2867.dsca.akamaiedge.net (23.223.99.108) 56(84) bytes of data.
64 bytes from 23.223.99.108: icmp_seq=1 ttl=128 time=7.83 ms
64 bytes from 23.223.99.108: icmp_seq=2 ttl=128 time=8.33 ms
64 bytes from 23.223.99.108: icmp_seq=3 ttl=128 time=8.29 ms
64 bytes from 23.223.99.108: icmp_seq=4 ttl=128 time=6.85 ms

--- e2867.dsca.akamaiedge.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 6.854/7.830/8.339/0.606 ms

cda/admin#

cda login: admin
Password:
cda/admin# sh ver

Cisco Application Deployment Engine OS Release: 2.0
ADE-OS Build Version: 2.0.2.057
ADE-OS System Architecture: i386

Copyright (c) 2005-2011 by Cisco Systems, Inc.
All rights reserved.
Hostname: cda

Version information of installed applications
-----

Cisco Context Directory Agent
-----
Version       : 1.0.0.011
Build Date    : Tue May  8 17:34:26 2012
Install Date  : Sun Mar 17 16:14:58 2019

cda/admin#

```

After the installation, we tested the connection to Domain Controller, DNS resolution and Internet connection:

```

Ping 172.16.1.254    ->    Inside ASAv Interface
Ping 172.16.1.10    ->    Domain Controller
Ping www.cisco.com  ->    DNS and Internet connection

```

The initial configuration of CDA using “show running-config” command is:

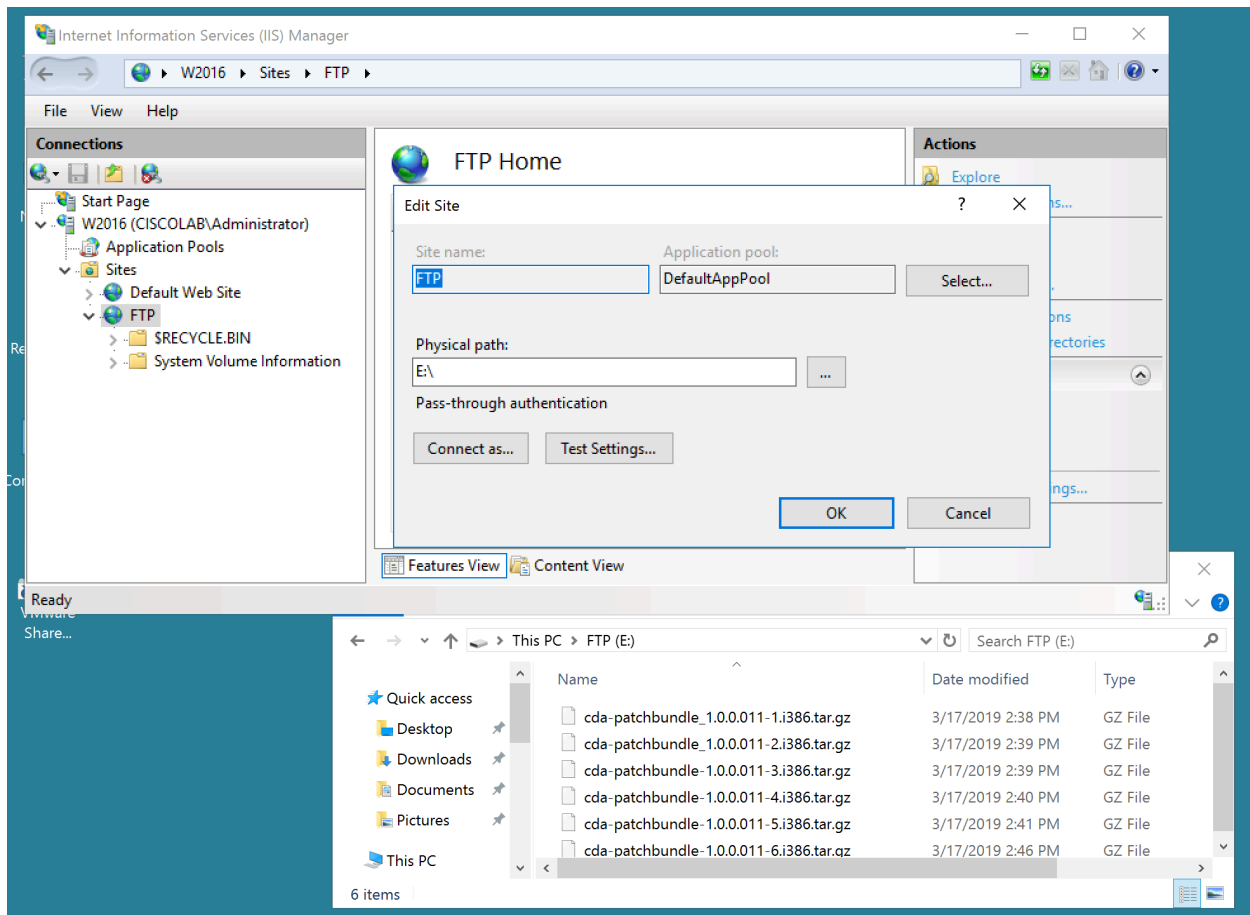
```
cda/admin# sh run
Generating configuration...
!
hostname cda
!
ip domain-name cisco-lab.local
!
interface GigabitEthernet 0
 ip address 172.16.1.11 255.255.255.0
 ipv6 address autoconfig
!
ip name-server 172.16.1.10
!
ip default-gateway 172.16.1.254
!
clock timezone Europe/Madrid
!
ntp server time.nist.gov
!
username admin password hash $1$zS1r2AV6$ABuvey5UYAyKgoPYJ1.yA0 role admin
!
service sshd
!
repository FTP
 url ftp://172.16.1.10
 user admin password hash fa1790f26edcc23e33bed639e21b2f89e8e2e596
!
password-policy
 lower-case-required
 upper-case-required
 digit-required
 no-username
 disable-cisco-passwords
 min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!
cda/admin#
```

CDA updating using CLI and FTP repository. Using the command “repository” we defined the FTP connection as repository for Backup and Patches. With command “patch” we can install the Patches using FTP repository.

```
repository FTP
 url ftp://172.16.1.10
 user admin password hash fa1790f26edcc23e33bed639e21b2f89e8e2e596
```

The repository definition includes the userid and password to access the content.

In Domain Controller we configured a FTP services (FTP IIS Services) with the Patches of CDA.



With "patch" command we proceed to update the CDA with all patches (1 -> 6):

```
cda/admin# patch install cda-patchbundle_1.0.0.011-1.i386.tar.gz FTP
```

```
cda/admin# show repository FTP
cda-patchbundle-1.0.0.011-3.i386.tar.gz
cda-patchbundle-1.0.0.011-4.i386.tar.gz
cda-patchbundle-1.0.0.011-5.i386.tar.gz
cda-patchbundle-1.0.0.011-6.i386.tar.gz
cda-patchbundle_1.0.0.011-1.i386.tar.gz
cda-patchbundle_1.0.0.011-2.i386.tar.gz
cda/admin#
cda/admin# patch install cda-patchbundle_1.0.0.011-1.i386.tar.gz FTP
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Patch installation...

Patch successfully installed
cda/admin#
```

After the updates or Patches installation we verify the status of the system:

```
cda/admin# show version
```

```
Cisco Application Deployment Engine OS Release:  
ADE-OS Build Version:  
ADE-OS System Architecture: i386
```

```
Copyright (c) 2005-2011 by Cisco Systems, Inc.  
All rights reserved.  
Hostname: cda
```

```
Version information of installed applications  
-----
```

```
Cisco Context Directory Agent  
-----
```

```
Version      : 1.0.0.011  
Build Date   : Tue May  8 17:34:26 2012  
Install Date : Sun Mar 17 16:14:58 2019
```

```
Cisco Context Directory Agent Patch  
-----
```

```
Version      : 1  
Build number : NA  
Install Date : Sun Mar 17 16:59:49 2019
```

```
Cisco Context Directory Agent Patch  
-----
```

```
Version      : 2  
Build number : NA  
Install Date : Sun Mar 17 17:02:23 2019
```

```
Cisco Context Directory Agent Patch  
-----
```

```
Version      : 3  
Build number : NA  
Install Date : Sun Mar 17 17:08:33 2019
```

```
Cisco Context Directory Agent Patch  
-----
```

```
Version      : 4  
Build number : NA  
Install Date : Sun Mar 17 17:15:25 2019
```

```
Cisco Context Directory Agent Patch  
-----
```

```
Version      : 5  
Build number : NA  
Install Date : Sun Mar 17 17:20:54 2019
```

```
Cisco Context Directory Agent Patch  
-----
```

```
Version      : 6  
Build number : NA  
Install Date : Sun Mar 17 17:26:16 2019
```

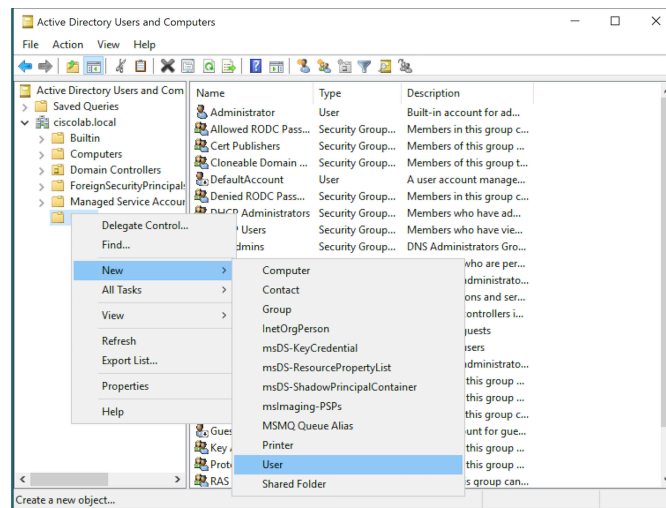
```
cda/admin#
```

Now the CDA system is ready for configuration.

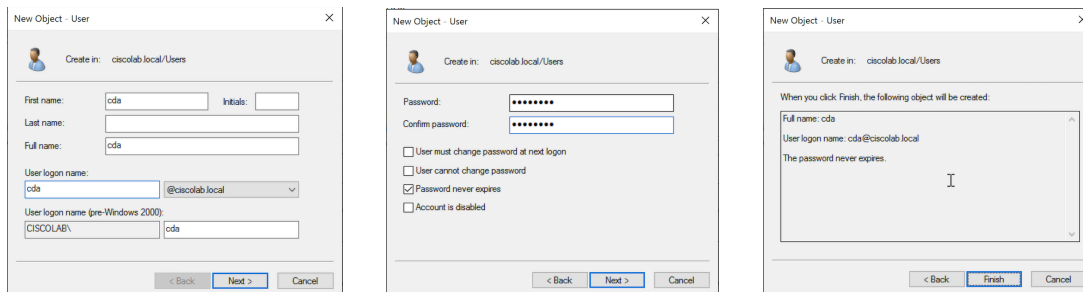
Active Directory preparation

(Below I'll try to show the screens sequence during configuration process)

- Windows Updates:
 - o Install the latest Windows Updates for Windows Server 2016.
- Create an account to use in CDA:
 - o Create an account with Administrator privilege, member of Domain Admins.

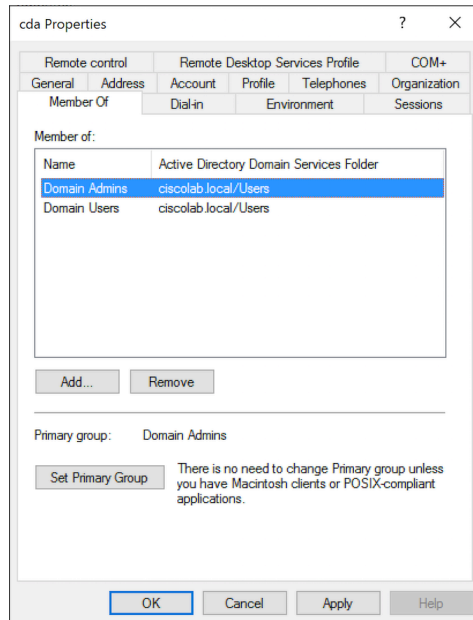


Using “Active Directory Users and Computers tool to create the user”.



Creating the user; assign name, user logon name and password.

After creating the user, we assign the user to “Domain Admins” group and set this group as Primary Group for this user.



Assign the user to Domain Admins group and set as the primary group.

- Domain Controller Firewall:

- Configuration of Windows Firewall to allow communications with CDA.

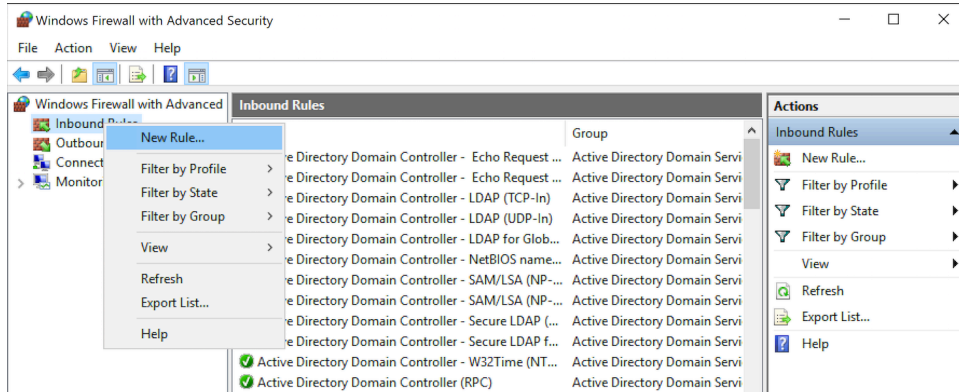
```
netsh advfirewall firewall set rule group="Windows Remote Management" new enable=yes
```

(In Windows Server 2016 exist a rule group "Windows Management Instrumentation (WMI)).

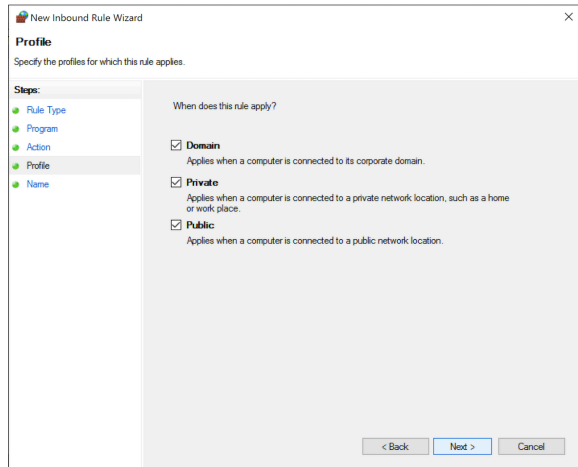
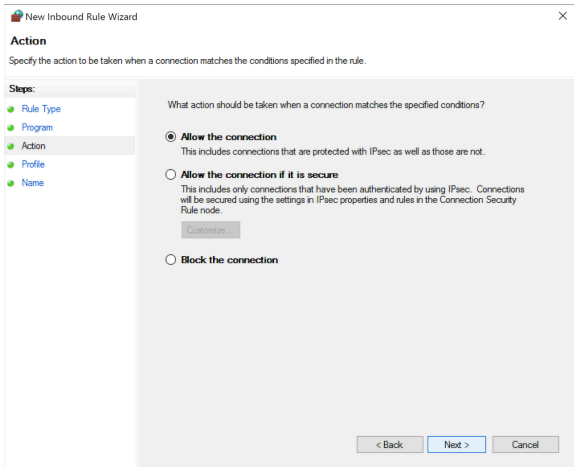
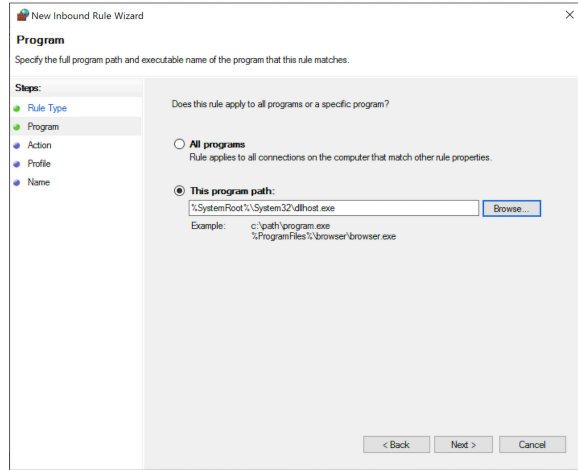
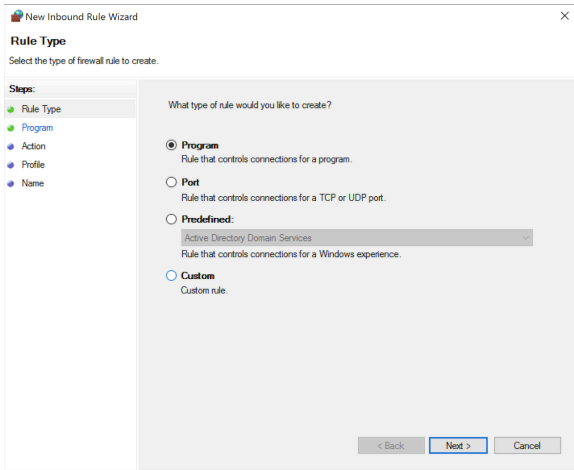
The image shows a black command prompt window with white text. The title bar reads 'Administrator: Command Prompt'. The command entered is 'C:\Users\Administrator>netsh advfirewall firewall set rule group="Windows Remote Management" new enable=yes'. The output is 'Updated 2 rule(s). Ok.'. The prompt returns to 'C:\Users\Administrator>_'.

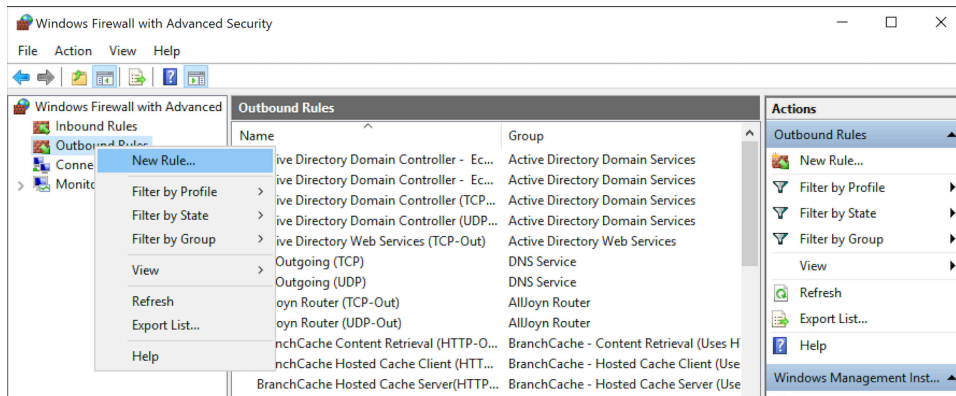
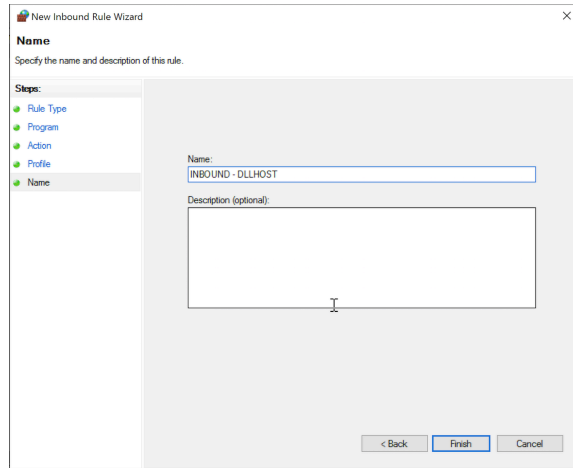
```
Administrator: Command Prompt
C:\Users\Administrator>netsh advfirewall firewall set rule group="Windows Remote Management" new enable=yes
Updated 2 rule(s).
Ok.
C:\Users\Administrator>_
```

- Firewall rules to allow traffic to “dllhost.exe”.

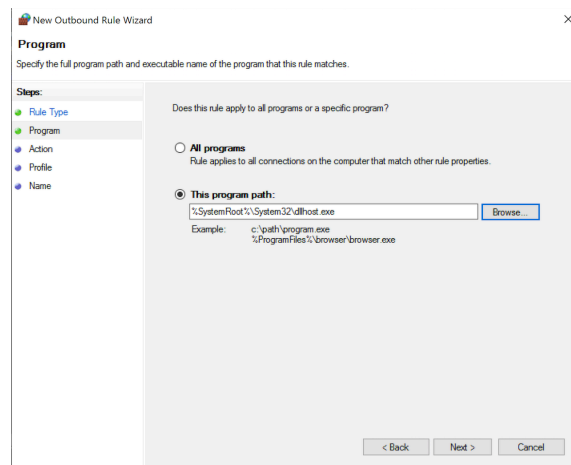
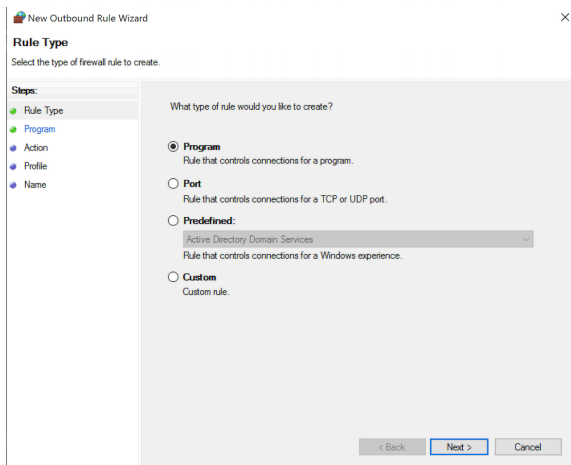


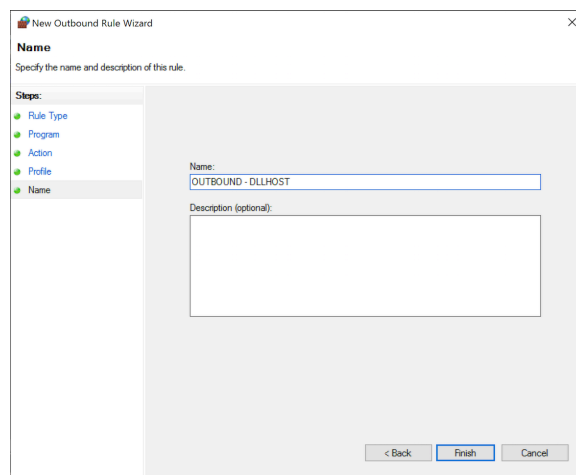
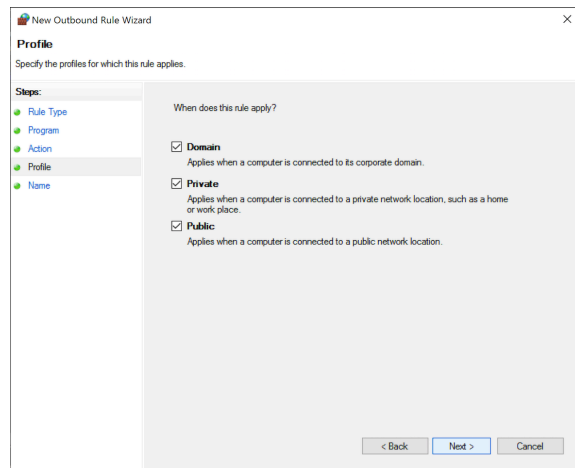
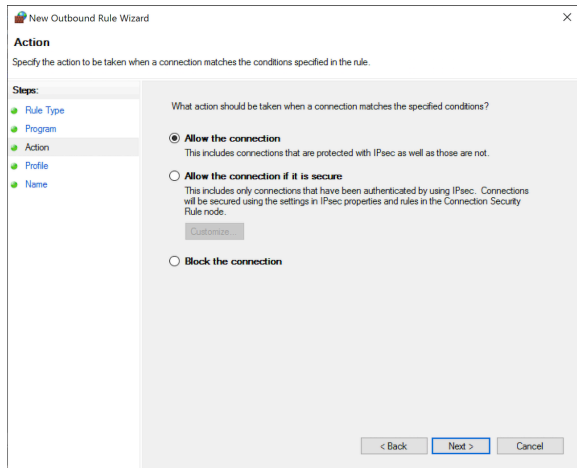
Create Inbound rule for “dllhost.exe”.





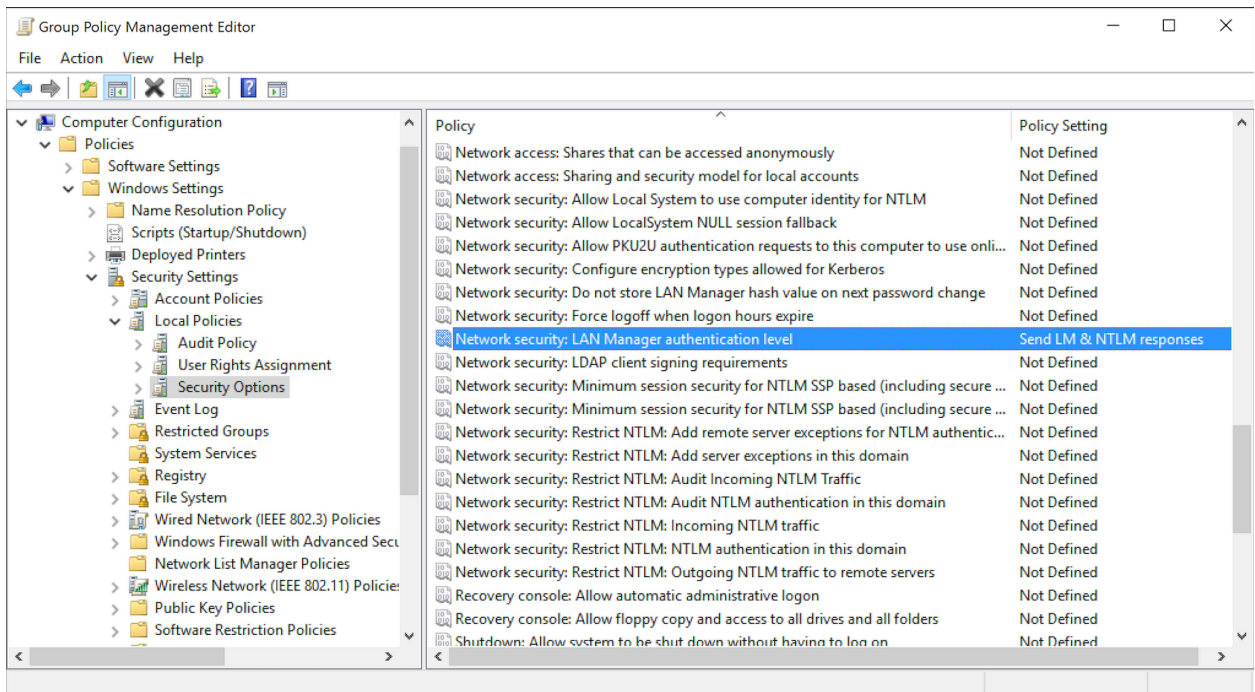
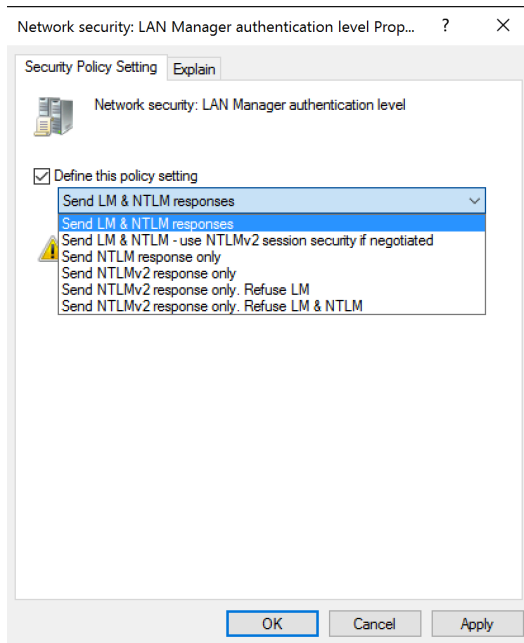
Create Outbound rule for "dllhost.exe".





- CDA require a user to communicate with Active Directory. The user can be authenticated by NTLMv1 or NTLMv2. It's important to verify this settings in Domain Controller policies.
 - o Start -> Windows Administrative Tools -> Group Policy Management: Domain Controller -> Default Domain Controllers Policy (Edit) Computer Configuration -> Windows Settings -> Security Settings Security Options -> Network Security: LAN Manager Authentication level:
 - Send LM & NTLM responses
 - Send LM & NTLM – use NTLMv2 session security if negotiated
 - Send NTLM response only
 - Send NTLMv2 response only
 - Send NTLMv2 response only. Refuse LM
 - Send NTLMv2 response only. Refue LM & NTLM

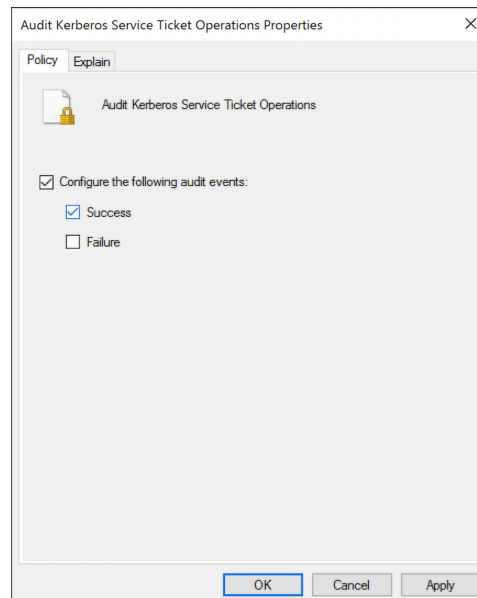
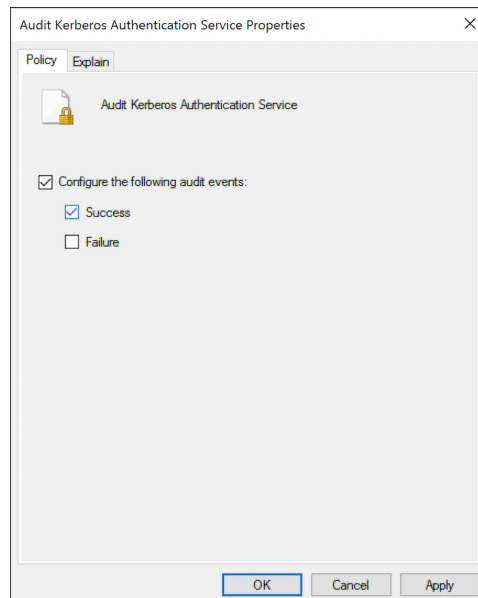
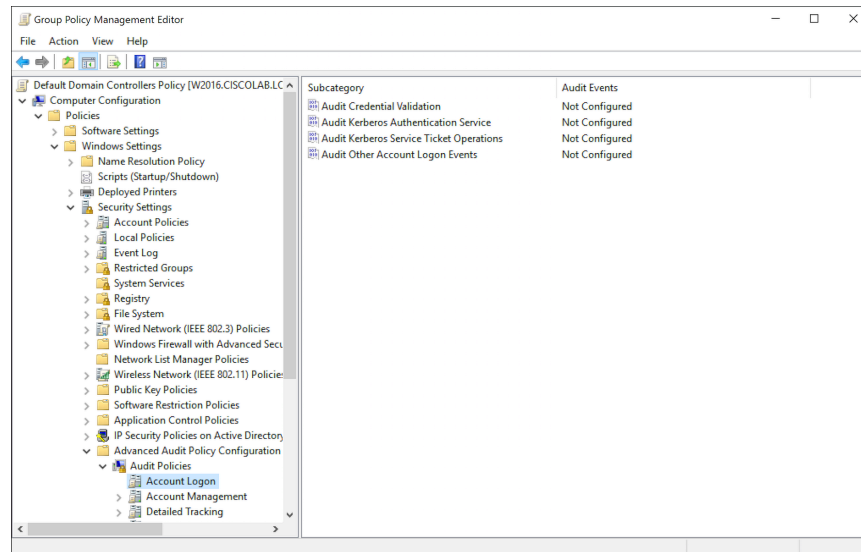
(In this example we define the “Send LM & NTLM responses” because this is a simple setting to allow NTLMv1 and NTLMv2).

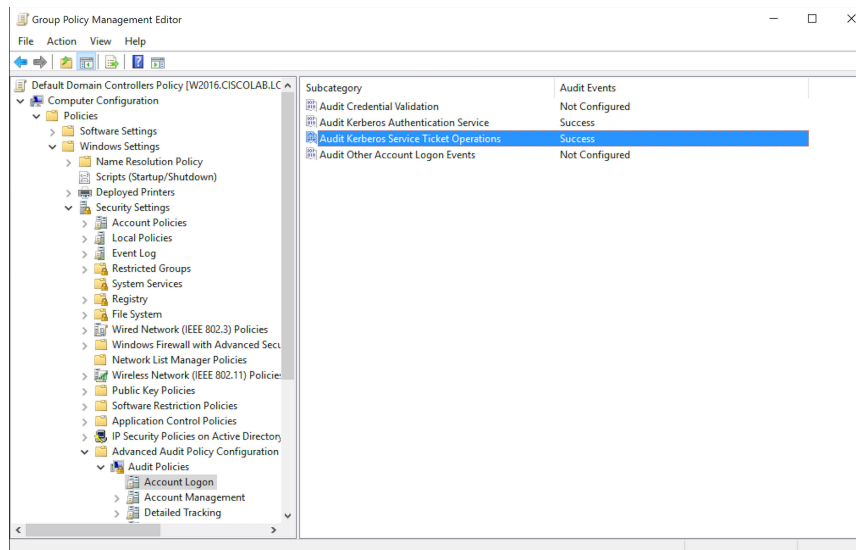


- Configuration of Audit Policy for Active Directory:

- o Start -> Windows Administrative Tools -> Group Policy Management: Domain Controller -> Default Domain Controllers Policy (Edit)
- Computer Configuration -> Windows Settings -> Security Settings
- Advanced Audit Policy Configuration -> Audit Policies -> Account Logon

- Audit Kerberos Authentication Service – Success
- Audit Kerberos Service Ticket Operation – Success





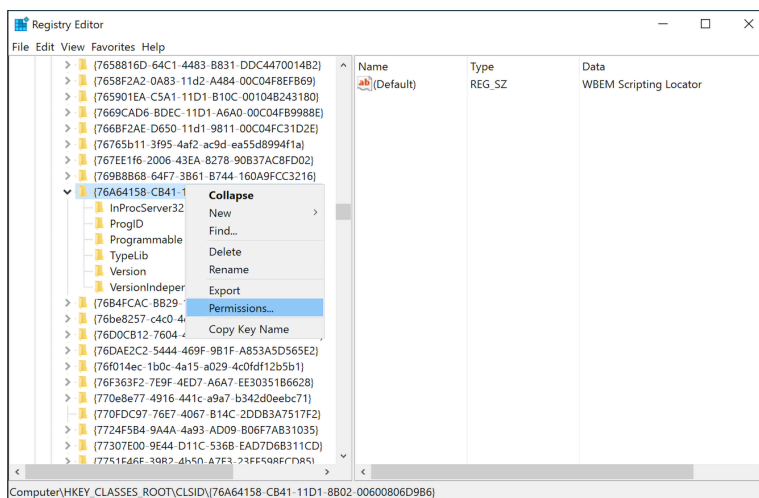
After this configuration we need to update the policies:

`gpupdate /force`

- Permissions required when an Active Directory User is a Member of the Domain Admin Group.
 - o Check the registry keys:
 - `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8D02-00600806D9B6}`
 - `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8D02-00600806D9B6}`

Assign Full Control permissions for Domain Admins group in that keys.

In order to assign Full Control permissions, the group Domain Admins must first take the ownership of the key.



Advanced Security Settings for (76A64158-CB41-11D1-8B02-00600806D9B6)

Owner: TrustedInstaller [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	TrustedInstaller	Full Control	None	This key and subkeys
Allow	SYSTEM	Read	None	This key and subkeys
Allow	Administrators (CISCOLAB\Ad...	Read	None	This key and subkeys
Allow	Users (CISCOLAB\Users)	Read	None	This key and subkeys
Allow	ALL APPLICATION PACKAGES	Read	None	This key and subkeys
Allow	Account Unknown(S-1-15-3-1...	Read	None	This key and subkeys

[Add](#) [Remove](#) [View](#)

[Enable inheritance](#)

Replace all child object permission entries with inheritable permission entries from this object

[OK](#) [Cancel](#) [Apply](#)

Advanced Security Settings for (76A64158-CB41-11D1-8B02-00600806D9B6)

Owner: Domain Admins (CISCOLAB\Domain Admins) [Change](#)

Replace owner on subcontainers and objects

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	TrustedInstaller	Full Control	None	This key and subkeys
Allow	SYSTEM	Read	None	This key and subkeys
Allow	Administrators (CISCOLAB\Ad...	Read	None	This key and subkeys
Allow	Users (CISCOLAB\Users)	Read	None	This key and subkeys
Allow	ALL APPLICATION PACKAGES	Read	None	This key and subkeys
Allow	Account Unknown(S-1-15-3-1...	Read	None	This key and subkeys

[Add](#) [Remove](#) [View](#)

[Enable inheritance](#)

Replace all child object permission entries with inheritable permission entries from this object

[OK](#) [Cancel](#) [Apply](#)

Permissions for (76A64158-CB41-11D1-8B02-00600806D9B6)

Security

Group or user names:

- ALL APPLICATION PACKAGES
- Account Unknown(S-1-15-3-1024-1065365936-128160471...)
- SYSTEM
- Administrators (CISCOLAB\Administrators)
- Domain Admins (CISCOLAB\Domain Admins)

[Add...](#) [Remove](#)

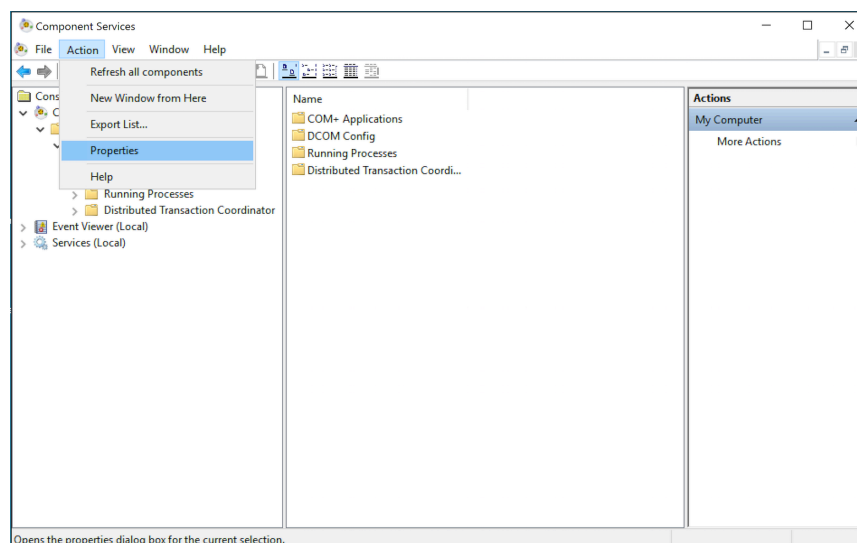
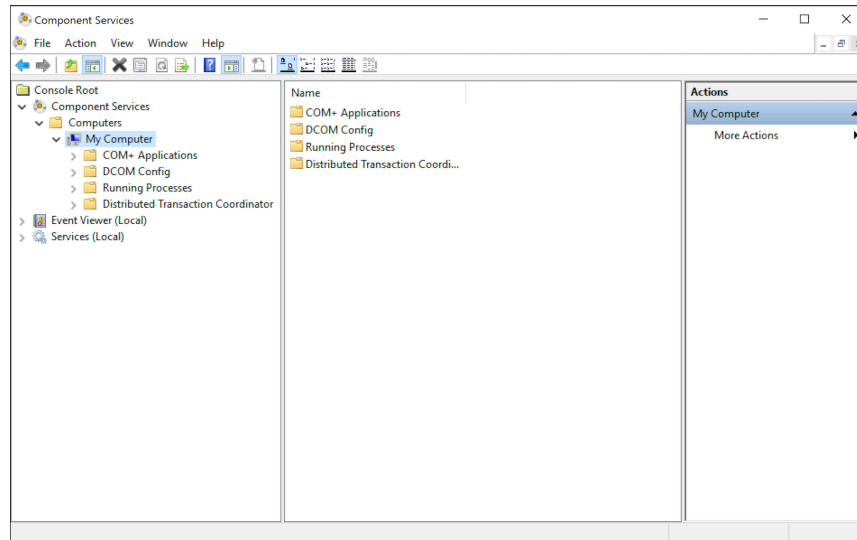
Permissions for Domain Admins

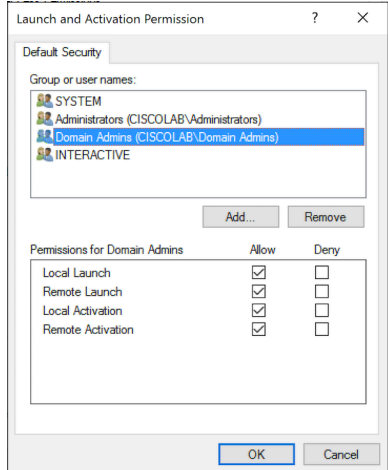
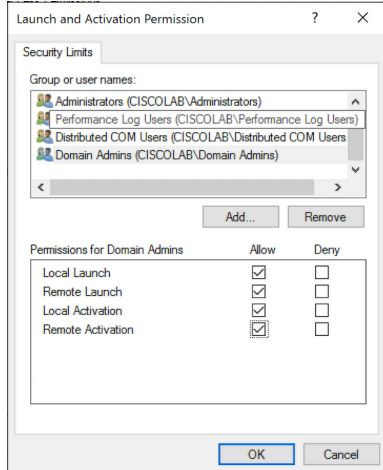
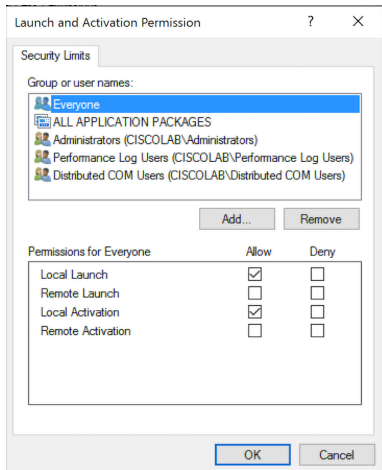
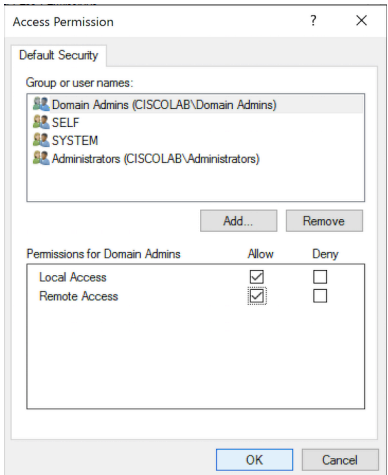
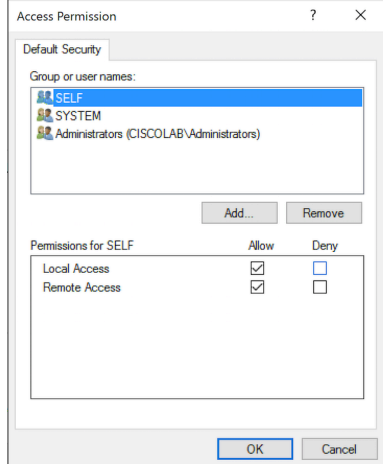
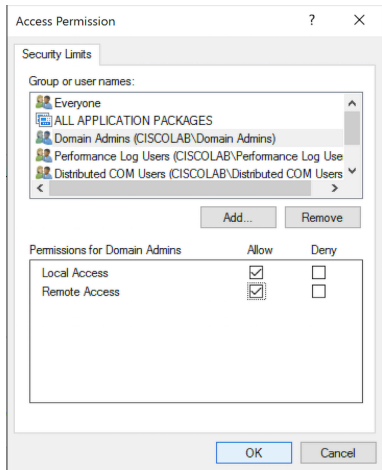
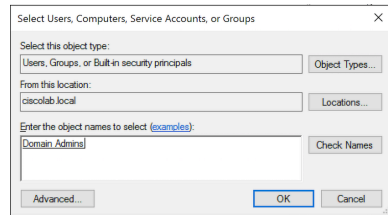
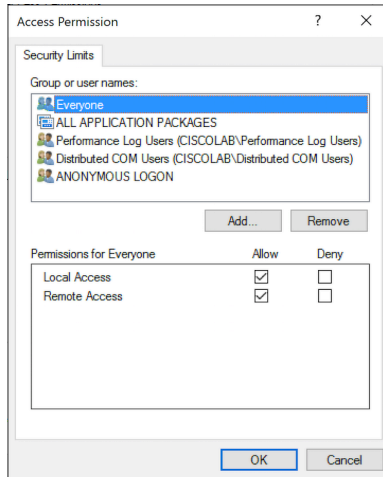
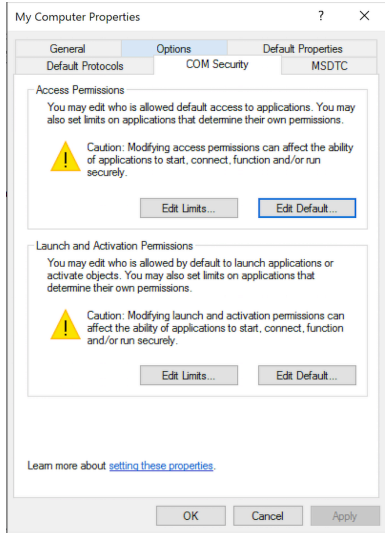
	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Special permissions	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click [Advanced](#).

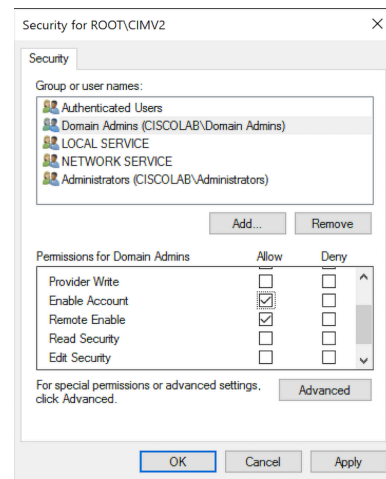
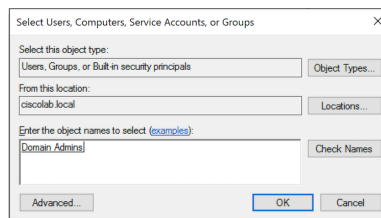
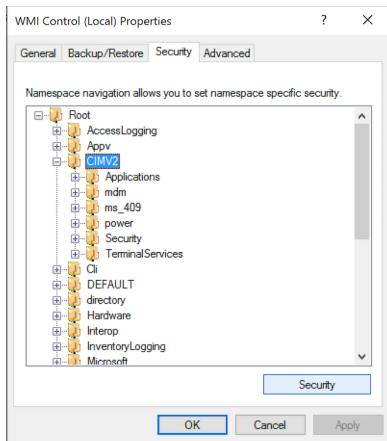
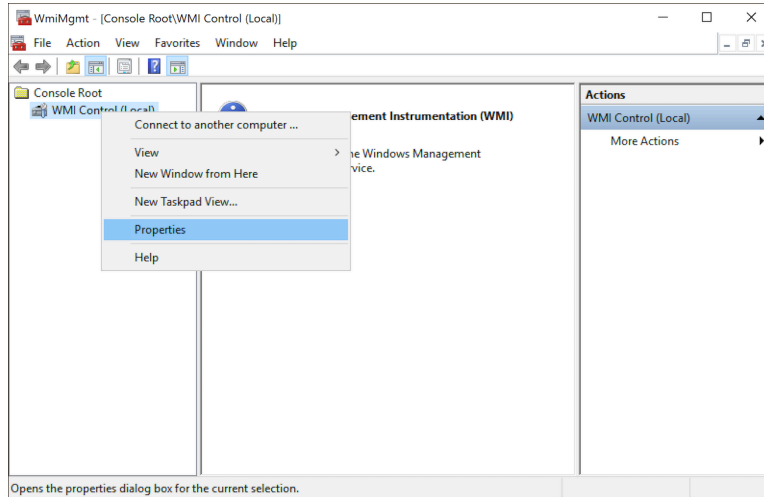
[OK](#) [Cancel](#) [Apply](#)

- Permissions to Use DCOM on the Domain Controller, including Domain Admins group:
 - o “dcomcnfg” -> Component Services -> Computers -> My Computer
 - o Select Action (My Computer) from Menu Bar and click Properties.
 - o Select COM Security.
 - o Select CDA account for; “Edit Limits”, “Edit Default” for “Access” and “Launch and Activation” with Allow permissions.

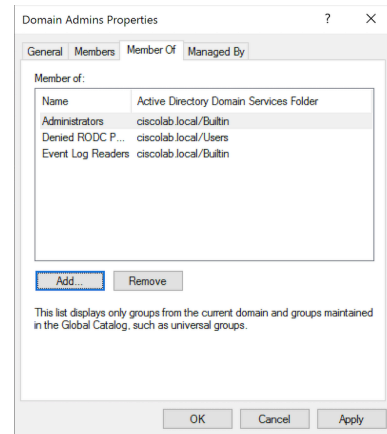
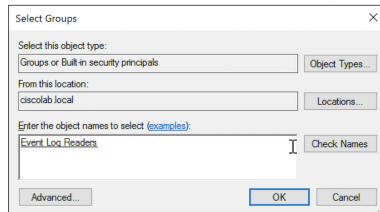
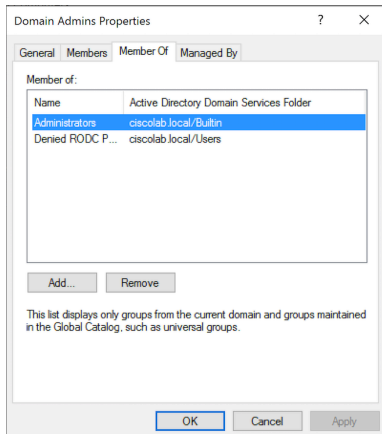
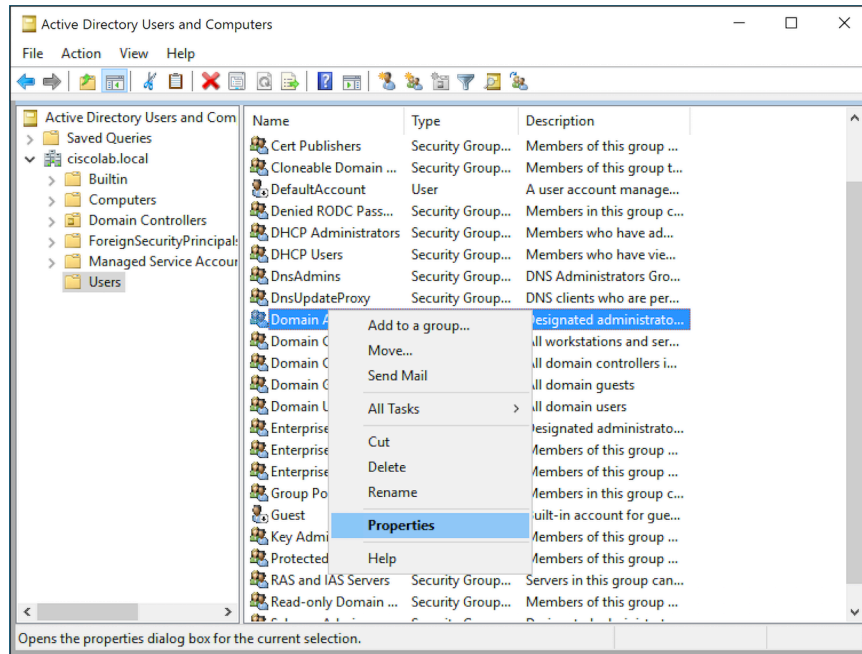




- Permissions to the WMI Root\CIMv2 Name Space:
 - o Start -> Run -> wmicmgmt.msc
 - o Right Click -> Properties
 - o Security Tab -> expand Root and choose CIMv2
 - o Click Security -> add the user and include the permissions; Allow for “Enable Account” and “Remote Enable”.



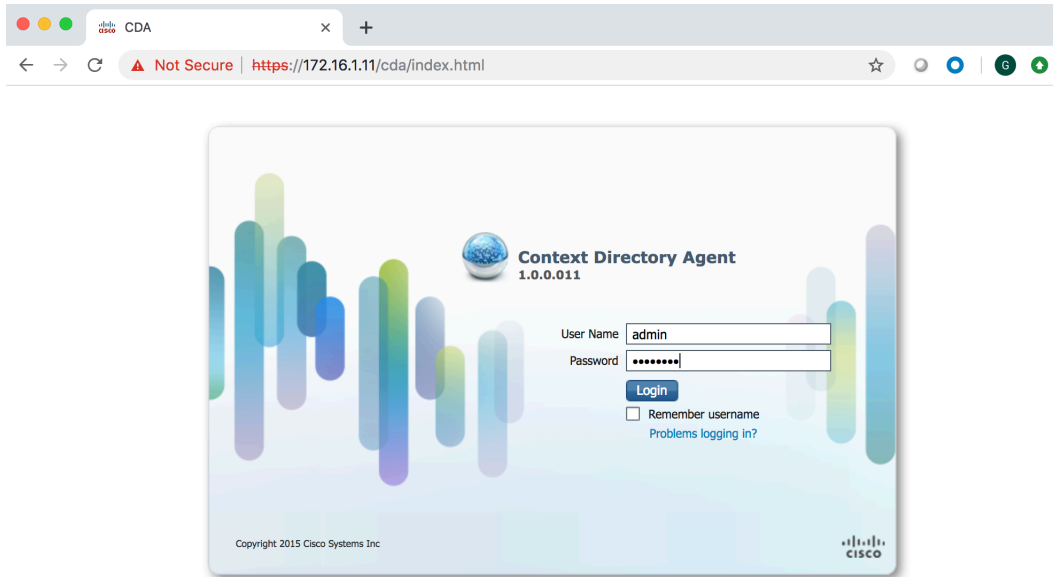
- Access to Read the Security Event Log of the Active Directory Domain Controller:
 - o Include the user to “Event Log Readers” Active Directory Group.



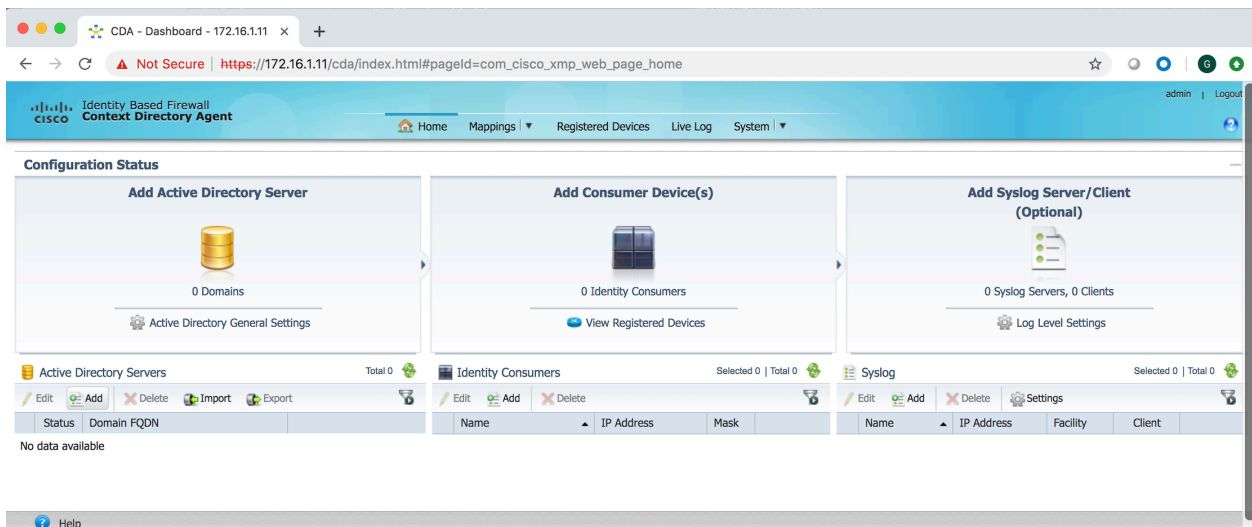
CDA configuration

Using the Web-Based user guide we proceed to configure the CDA appliance to work with the Active Directory domain controller.

Add Active Directory Server:



Using the section "Add Active Directory Server" and using the userid created and configured in domain for CDA.



Active Directory Server Configuration

General Settings

* Display Name
* Domain FQDN
* Host FQDN

Credentials

* Username
* Password

Supported OS's: Windows 2003, Windows 2003 R2, Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2, Windows 2016

The system initiates communications with domain controller.

Status	Domain FQDN
Up	ciscolab.local

Name	IP Address	Mask
------	------------	------

The logs shows the communication with AD.

Timestamp	Severity	Origin component	Message	Attributes
2019-03-24 16:31:31.329+01:00	Info	ContextManager	Domain Controller's status changed from down to up	
2019-03-24 16:31:21.321+01:00	Info	ADObserver	Connection established to Domain Controller	
2019-03-24 16:31:21.100+01:00	Info	ADObserver	Started new Domain Controller thread	
2019-03-24 16:31:20.617+01:00	Info	ADObserver	Started new Domain Controller thread	
2019-03-24 16:31:18.453+01:00	Info	Management	Configuration changed	
2019-03-24 16:30:59.313+01:00	Info	ADObserver	Disconnected from Domain Controller (planned)	
2019-03-24 16:30:47.806+01:00	Info	Management	Configuration changed	

Finally, the status of Active Directory in CDA is "OK".

The screenshot displays the Cisco Context Directory Agent (CDA) dashboard. The top navigation bar includes the Cisco logo, the text "Identity Based Firewall Context Directory Agent", and user information "admin | Logout". The main navigation menu contains "Home", "Mappings", "Registered Devices", "Live Log", and "System".

The "Configuration Status" section is divided into three panels:

- Add Active Directory Server:** Shows "1 Domain" and a link to "Active Directory General Settings".
- Add Consumer Device(s):** Shows "0 Identity Consumers" and a link to "View Registered Devices".
- Add Syslog Server/Client (Optional):** Shows "0 Syslog Servers, 0 Clients" and a link to "Log Level Settings".

Below these panels are three data tables:

- Active Directory Servers:** Total 1. Includes a table with columns: Status, Domain, FQDN. One entry is visible:

Status	Domain	FQDN
<input checked="" type="checkbox"/>	ciscolab.local	
- Identity Consumers:** Selected 0 | Total 0. Includes a table with columns: Name, IP Address, Mask.
- Syslog:** Selected 0 | Total 0. Includes a table with columns: Name, IP Address, Facility, Client.

At the bottom left, there is a "Help" link.

ASAv configuration

Next, the configuration of ASA device and the inclusion of ASA in CDA. In ASA we need to define the AAA servers for include Active Directory and CDA device.

For ASA configuration we use the following sentences in CLI:

- AAA server configuration in ASA:

```
aaa-server adserver protocol ldap
aaa-server adserver (inside) host 172.16.1.10
  server-port 389
  ldap-base-dn DC=ciscolab,DC=local
  ldap-group-base-dn CN=Users,DC=ciscolab,DC=local
  ldap-scope subtree
  ldap-login-password *****
  ldap-login-dn cn=cda,CN=Users,DC=ciscolab,DC=local
  server-type microsoft
  group-search-timeout 300
aaa-server cda protocol radius
  ad-agent-mode
aaa-server cda (inside) host 172.16.1.11
  key *****
```

In this point is important to keep in mind the description of the users dedicated to connect the ASA with Active Directory. The sentences "ldap-group-base-dn", "ldap-base-dn" and "ldap-login-dn" must include the right path of the user.

In our example the user in Active Directory was created in section before (Preparing Active Directory):

```
UserID:                cda
Primary Domain Group:  Domain Admins
Base DN:                DC=ciscolab, DC=local
"ldap-base-dn":        DC=ciscolab,DC=local
"ldap-group-base-dn":  DC=Users, DC=ciscolab,DC=local
"ldap-login-dn":       cn=cda,CN=Users,DC=ciscolab,DC=local
```

- User Identity configuration in ASA:

```
user-identity domain ciscolab aaa-server adserver
user-identity default-domain ciscolab
user-identity ad-agent aaa-server cda
```

- AAA authentication in ASA:

```
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
aaa authentication login-history
```

After configuring this part is convenient to test the access to Active Directory and LDAP using "test" command.

In the following text, the output of testing the authentication against the Active Directory. First a "show running-config" to see the configuration. After, the "debug ldap 255" to enable the debug logs to see the interaction between ASA and Active Directory LDAP, and finally the "test aaa" command to check the connection and authentication.

```
asa# sh run aaa-server
aaa-server adserver protocol ldap
aaa-server adserver (inside) host 172.16.1.10
  server-port 389
  ldap-base-dn DC=ciscolab,DC=local
  ldap-group-base-dn DC=Users,DC=ciscolab,DC=local
  ldap-scope subtree
  ldap-login-password *****
  ldap-login-dn cn=cda,CN=Users,DC=ciscolab,DC=local
  server-type microsoft
  group-search-timeout 300
aaa-server cda protocol radius
  ad-agent-mode
aaa-server cda (inside) host 172.16.1.11
  key *****
asa#
```

```
asa# debug ldap 255
debug ldap enabled at level 255
asa#
```

```
asa# test aaa-server authentication adserver username cda password Passw0rd
Server IP Address or name: 172.16.1.10
INFO: Attempting Authentication test to IP address (172.16.1.10) (timeout: 12 seconds)
```

```
[-2147483602] Session Start
[-2147483602] New request Session, context 0x00007f2a20065b28, reqType = Authentication
[-2147483602] Fiber started
[-2147483602] Creating LDAP context with uri=ldap://172.16.1.10:389
[-2147483602] Connect to LDAP server: ldap://172.16.1.10:389, status = Successful
[-2147483602] supportedLDAPVersion: value = 3
[-2147483602] supportedLDAPVersion: value = 2
[-2147483602] Binding as cda
[-2147483602] Performing Simple authentication for cda to 172.16.1.10
[-2147483602] LDAP Search:
```

```
Base DN = [DC=ciscolab,DC=local]
Filter = [sAMAccountName=cda]
Scope = [SUBTREE]
[-2147483602] User DN = [CN=cda,CN=Users,DC=ciscolab,DC=local]
[-2147483602] Talking to Active Directory server 172.16.1.10
[-2147483602] Reading password policy for cda, dn:CN=cda,CN=Users,DC=ciscolab,DC=local
[-2147483602] Read bad password count 0
[-2147483602] Binding as cda
[-2147483602] Performing Simple authentication for cda to 172.16.1.10
[-2147483602] Processing LDAP response for user cda
[-2147483602] Message (cda):
[-2147483602] Authentication successful for cda to 172.16.1.10
[-2147483602] Retrieved User Attributes:
[-2147483602]   objectClass: value = top
[-2147483602]   objectClass: value = person
[-2147483602]   objectClass: value = organizationalPerson
[-2147483602]   objectClass: value = user
[-2147483602]   cn: value = cda
[-2147483602]   givenName: value = cda
[-2147483602]   distinguishedName: value = CN=cda,CN=Users,DC=ciscolab,DC=local
[-2147483602]   instanceType: value = 4
[-2147483602]   whenCreated: value = 20190317205251.0Z
[-2147483602]   whenChanged: value = 20190317212156.0Z
[-2147483602]   displayName: value = cda
[-2147483602]   uSNCreated: value = 12711
[-2147483602]   memberOf: value = CN=Domain Users,CN=Users,DC=ciscolab,DC=local
[-2147483602]   memberOf: value = CN=Event Log Readers,CN=Builtin,DC=ciscolab,DC=local
[-2147483602]   uSNChanged: value = 12730
[-2147483602]   name: value = cda
[-2147483602]   objectGUID: value = .9.x...F.._.....
[-2147483602]   userAccountControl: value = 66048
[-2147483602]   badPwdCount: value = 0
[-2147483602]   codePage: value = 0
[-2147483602]   countryCode: value = 0
[-2147483602]   badPasswordTime: value = 0
[-2147483602]   lastLogoff: value = 0
[-2147483602]   lastLogon: value = 0
[-2147483602]   pwdLastSet: value = 131973295719460280
[-2147483602]   primaryGroupID: value = 512
[-2147483602]   objectSid: value = .....wvE>;.T...R...
[-2147483602]   adminCount: value = 1
[-2147483602]   accountExpires: value = 9223372036854775807
[-2147483602]   logonCount: value = 0
[-2147483602]   sAMAccountName: value = cda
[-2147483602]   sAMAccountType: value = 805306368
[-2147483602]   userPrincipalName: value = cda@ciscolab.local
[-2147483602]   objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=ciscolab,DC=local
[-2147483602]   dSCorePropagationData: value = 20190317212156.0Z
[-2147483602]   dSCorePropagationData: value = 16010101000000.0Z
[-2147483602] Fiber exit Tx=520 bytes Rx=2653 bytes, status=1
[-2147483602] Session End
INFO: Authentication Successful
asa#
```

Configuring ASA in CDA

The screenshot shows the Cisco Context Directory Agent (CDA) dashboard. The top navigation bar includes Home, Mappings, Registered Devices, Live Log, and System. The main content area is titled "Configuration Status" and contains three panels: "Add Active Directory Server" (1 Domain), "Add Consumer Device(s)" (0 Identity Consumers), and "Add Syslog Server/Client (Optional)" (0 Syslog Servers, 0 Clients). Below these panels are three tables: "Active Directory Servers" (Total 1), "Identity Consumers" (Selected 0 | Total 0), and "Syslog" (Selected 0 | Total 0). The "Active Directory Servers" table has columns for Status, Domain FQDN, Name, Uptime/Dow..., Host/IP, Dom..., and Versi... and contains one entry for "ciscolab.local".

Identity Consumer Configuration

* Name:

* IP Address:

Mask (range):

* Shared secret:

Show secret

This screenshot shows the CDA dashboard after the configuration. The "Add Consumer Device(s)" panel now displays "1 Identity Consumer". The "Identity Consumers" table below it has one entry: ASAv, 172.16.1.254, 32. The "Active Directory Servers" and "Syslog" tables remain the same as in the previous screenshot.

← → ↻ Not Secure | https://172.16.1.11/cda/index.html#pageld=com_cisco_xmp_web_page_consumer_devices ☆ 🔍 🌐 📶

Identity Based Firewall
Context Directory Agent admin | Logout

Home Mappings Registered Devices Live Log System

Registered Devices Total 1

Show All

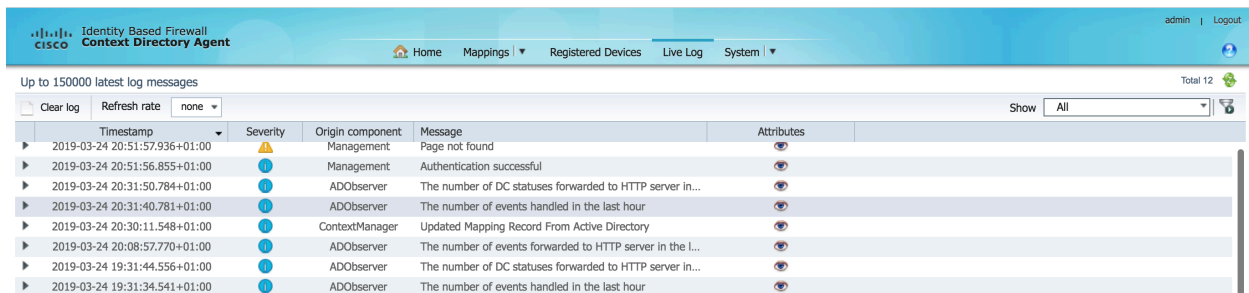
Status	IP Address	Configuration name	Configuration range
🟢	172.16.1.254	ASAv	172.16.1.254/32

“Registered Devices” indicates the ASA system registered in CDA.

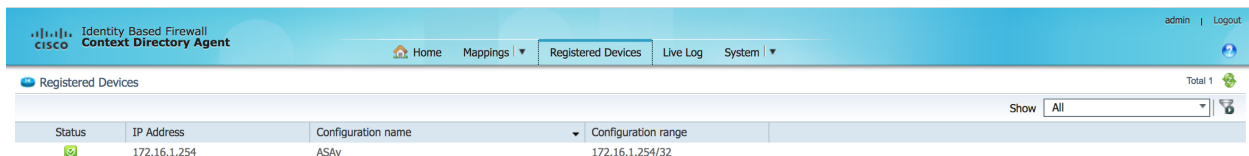
Test

During configuration we have been testing some basics points for the Identity Firewall solution:

- *The connection between CDA and Active Directory.*
Using the CDA web-based GUI in “Live Logs” we can see the activity and possible errors. The “Active Directory Servers” indicates the integration between CDA and Active Directory (green logo).



- *Connection between CDA and ASA.*
In CDA GUI we can check the status of this connection in “Registered Devices”.



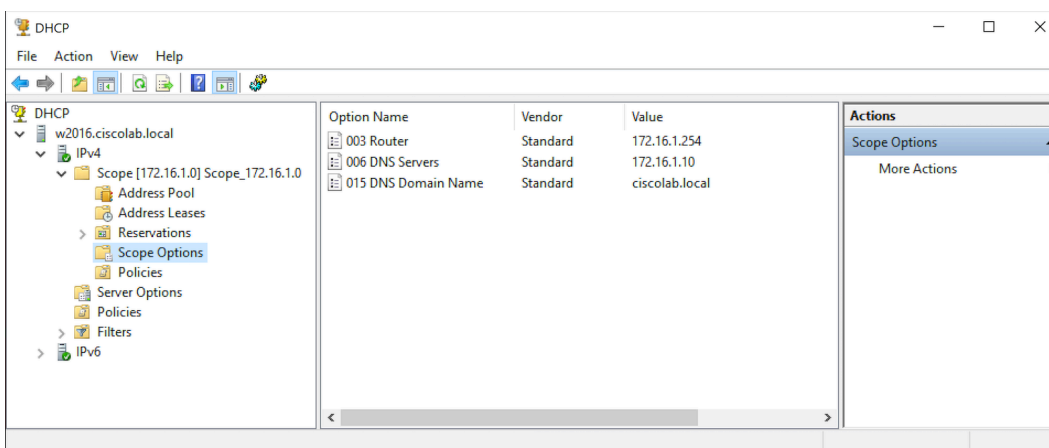
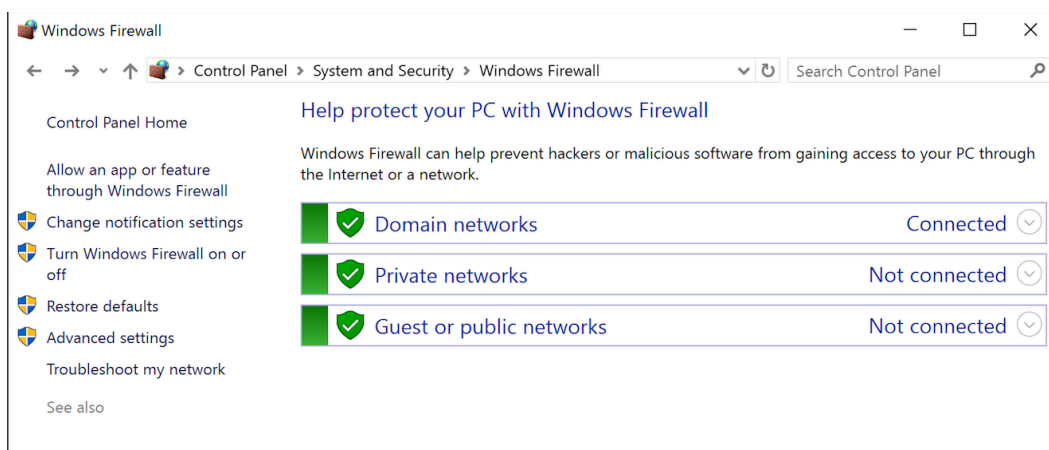
- *Connection between ASA and Active Directory.*
Using the “test” command in ASA to verify this configuration (see before in this document).

After the configuration and verification of the integration between CDA, ASA and Active Directory we can create Access Control Entries in ASA associated to Users.

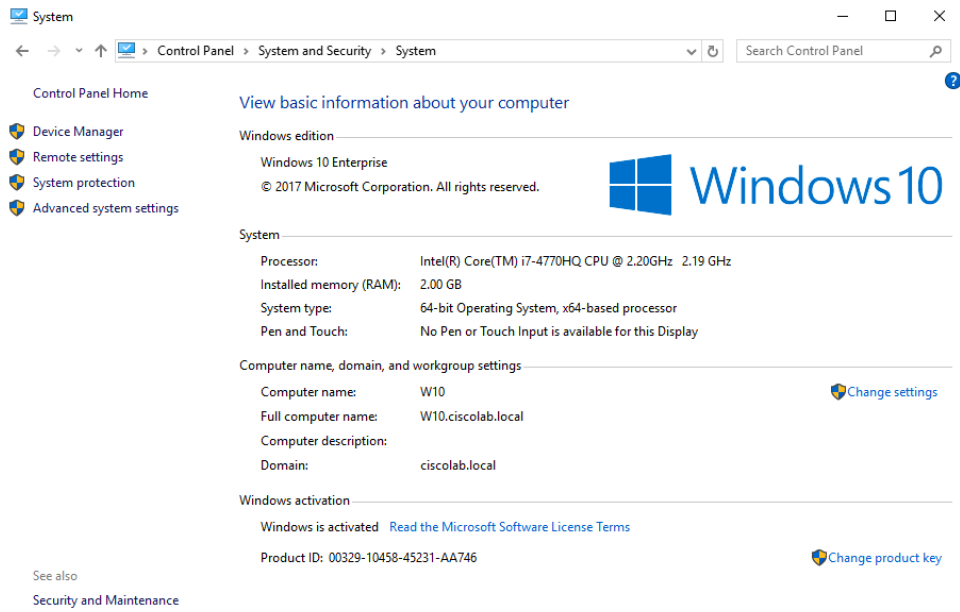
First, we will use a Windows 10 workstation (VM in Fusion in our Lab) member of Active Directory domain "cisolab.local" with a domain user.

In our example, the Domain Controller is DHCP server for inside network, the DHCP service is authorized by Active Directory domain with all needed options (Gateway, DNS domain name, DNS servers).

The following images show the status of Firewall and DHCP services in Domain Controller.



The Windows 10 workstation properties:



The screenshot shows the Windows 10 System properties window. The title bar reads "System". The breadcrumb navigation is "Control Panel > System and Security > System". The left sidebar contains "Control Panel Home", "Device Manager", "Remote settings", "System protection", and "Advanced system settings". The main content area is titled "View basic information about your computer".

Windows edition

- Windows 10 Enterprise
- © 2017 Microsoft Corporation. All rights reserved.

System

- Processor: Intel(R) Core(TM) i7-4770HQ CPU @ 2.20GHz 2.19 GHz
- Installed memory (RAM): 2.00 GB
- System type: 64-bit Operating System, x64-based processor
- Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

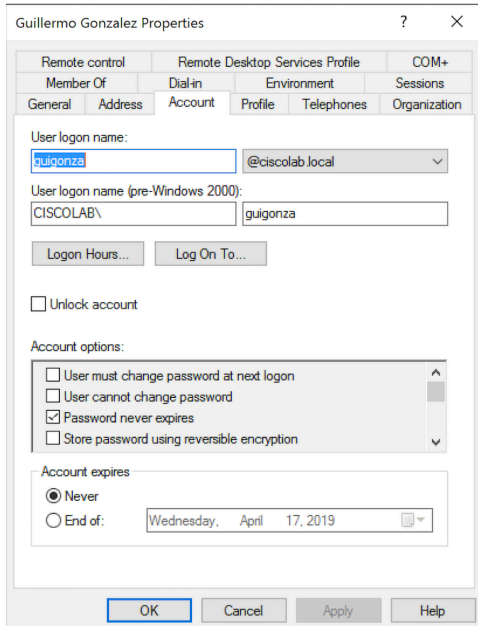
- Computer name: W10 [Change settings](#)
- Full computer name: W10.ciscolab.local
- Computer description:
- Domain: ciscolab.local

Windows activation

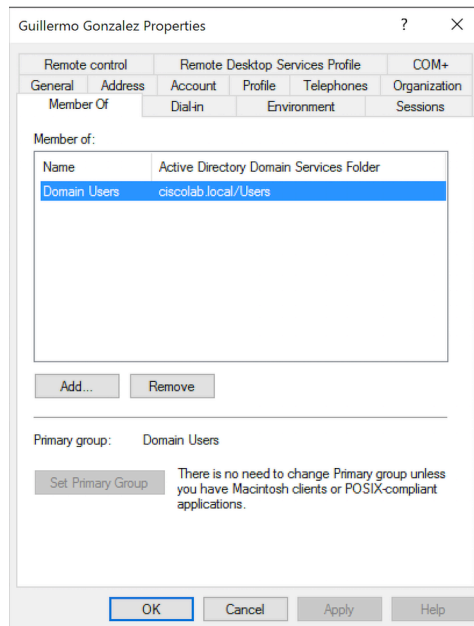
- Windows is activated [Read the Microsoft Software License Terms](#)
- Product ID: 00329-10458-45231-AA746 [Change product key](#)

See also
Security and Maintenance

User in Active Directory for tests:

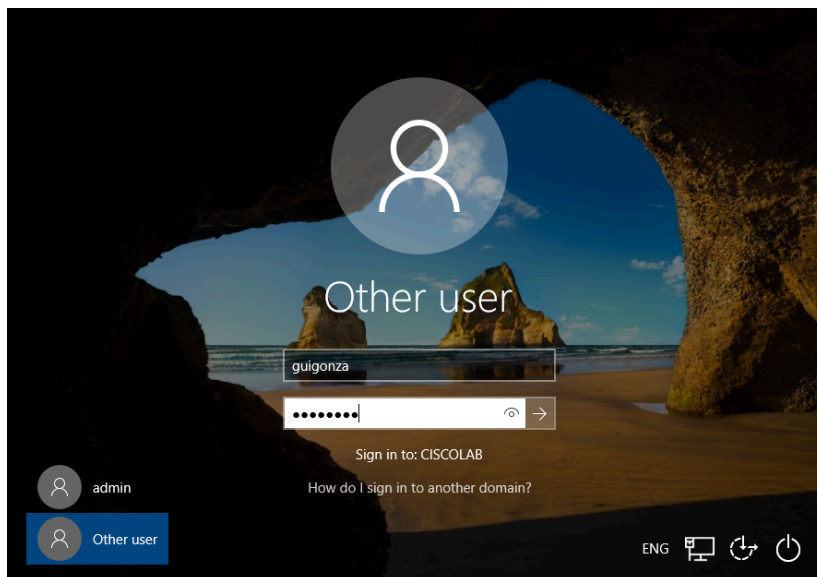


The screenshot shows the "Guillermo Gonzalez Properties" dialog box, General tab. The "User logon name" is "guigonza" with a dropdown menu showing "@ciscolab.local". The "User logon name (pre-Windows 2000)" is "CISCOLAB\guigonza". There are "Logon Hours..." and "Log On To..." buttons. The "Unlock account" checkbox is unchecked. Under "Account options", "User must change password at next logon" and "User cannot change password" are unchecked, "Password never expires" is checked, and "Store password using reversible encryption" is unchecked. Under "Account expires", "Never" is selected.

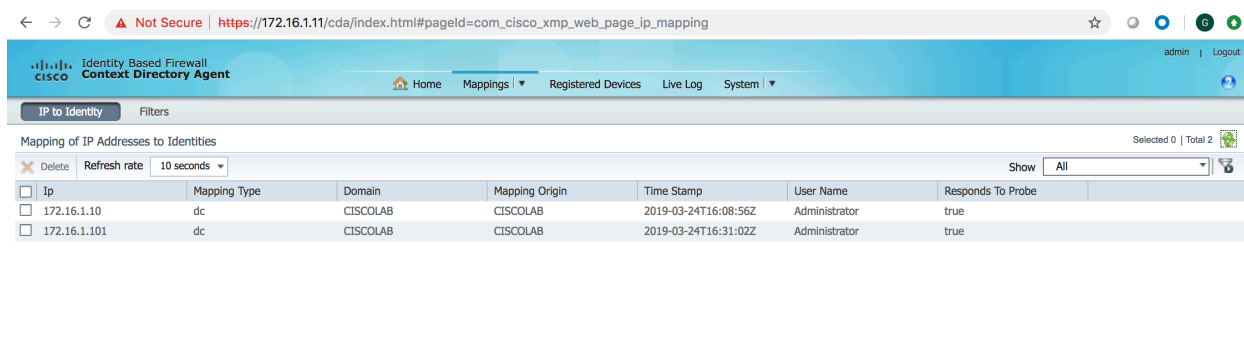


The screenshot shows the "Guillermo Gonzalez Properties" dialog box, Member Of tab. The "Member of:" list contains "Domain Users" with "Active Directory Domain Services Folder" and "ciscolab.local/Users". There are "Add..." and "Remove" buttons. The "Primary group:" is "Domain Users". A "Set Primary Group" button is present with a note: "There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications."

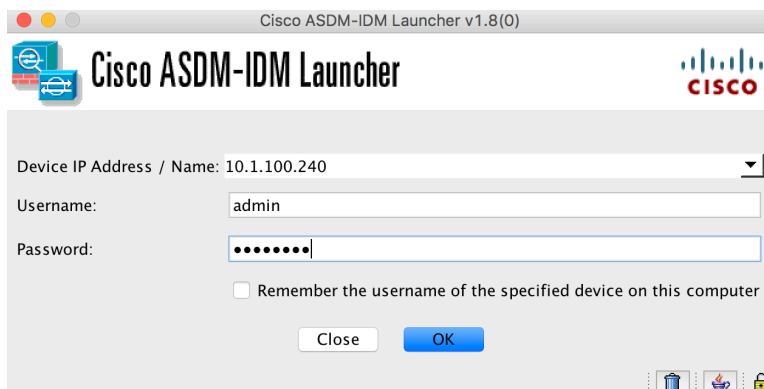
Login with userid "guigonza" in Windows W10 VM:



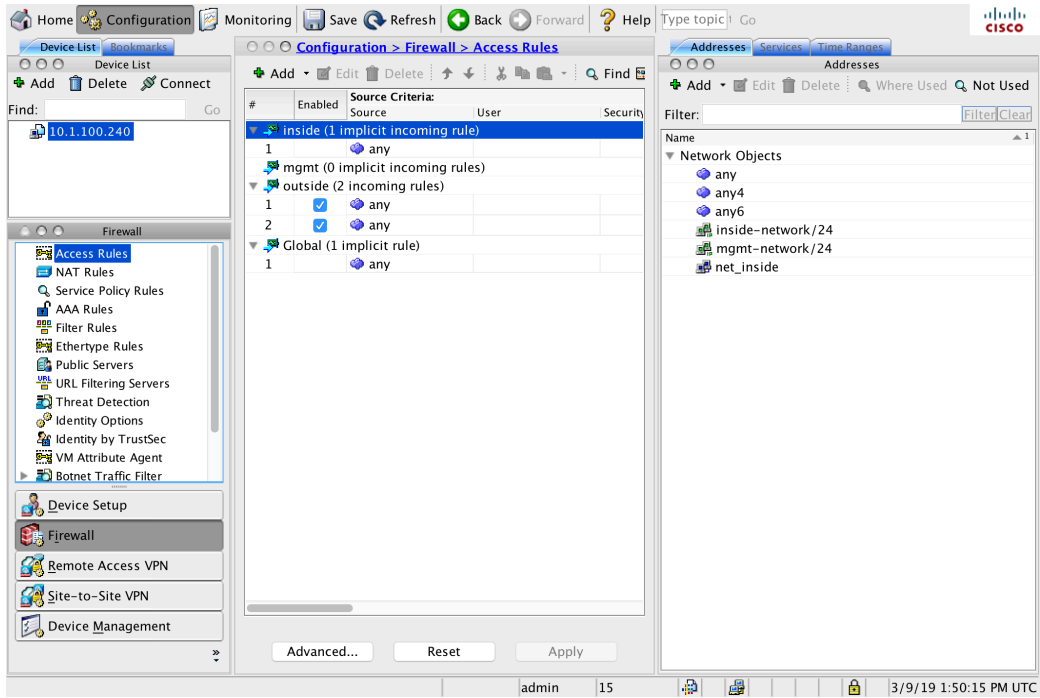
After this login, we can see the IP mapping in CDA GUI.



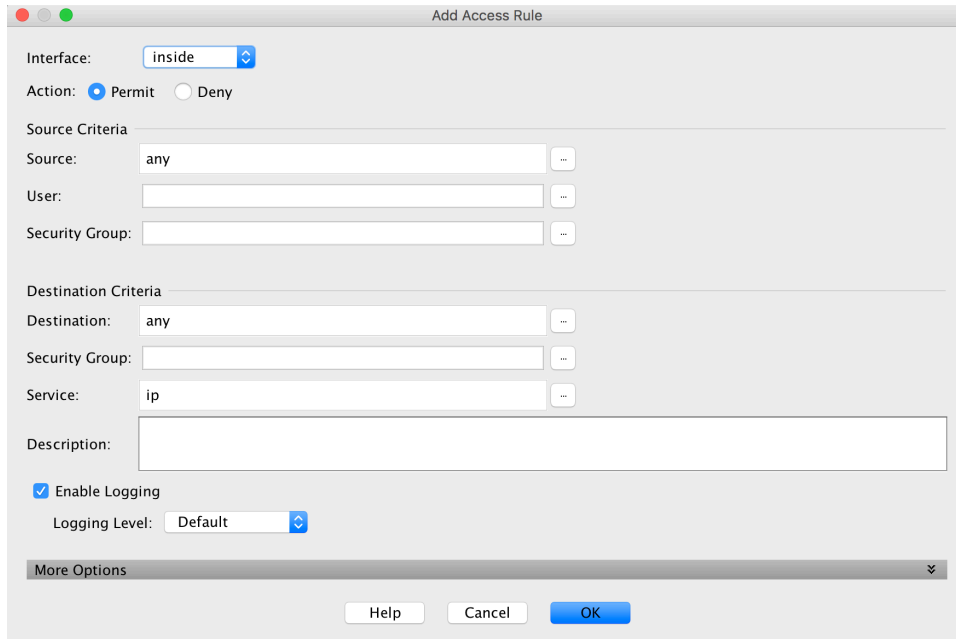
Now we proceed to configure the ACEs in ASA using ASMD.



ASDM -> Configuration -> Firewall -> Access Rules -> Add:



Configuration of ACE details:



Source Network:

➕ Add ▾ ✎ Edit 🗑️ Delete 🔍 Where Used 🔍 Not Used

Filter: Filter Clear

Name	IP Address	Netmask	Description	Object NAT Add...	Agent Name	Attribute Type	Attribute Va...
▼ Network Objects							
any							
any4							
any6							
inside-n...	172.16.1.0	255.255.2...					
mgmt-ne...	10.1.100.0	255.255.2...					
net_inside	172.16.1.0	255.255.2...					
▼ Interfaces							
inside							
mgmt							
outside							

Add Access Rule

Interface:

Action: Permit Deny

Source Criteria

Source: ...

User: ...

Security Group: ...

Destination Criteria

Destination: ...

Security Group: ...

Service: ...

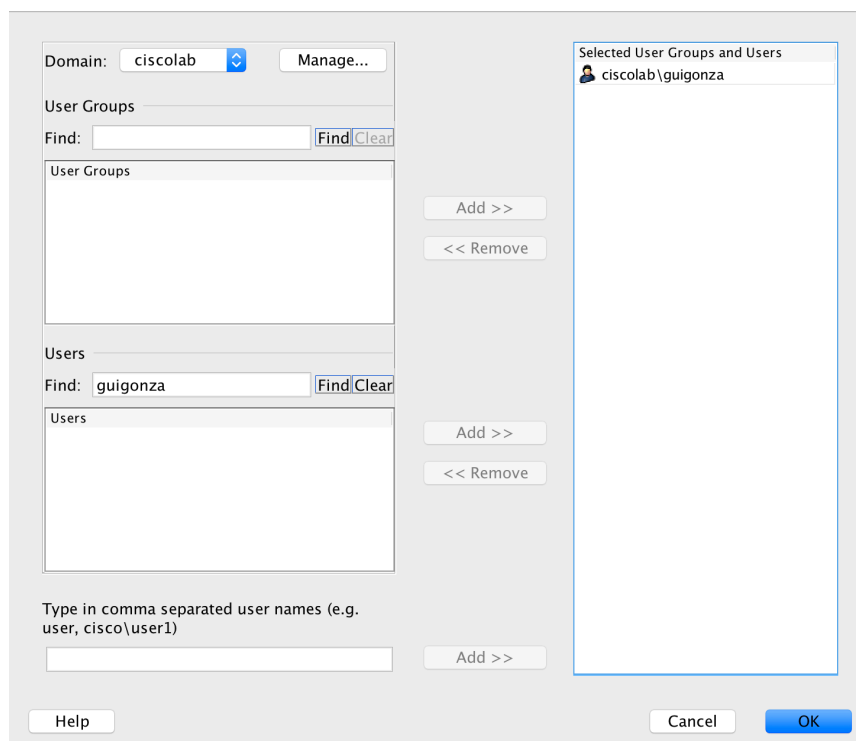
Description:

Enable Logging

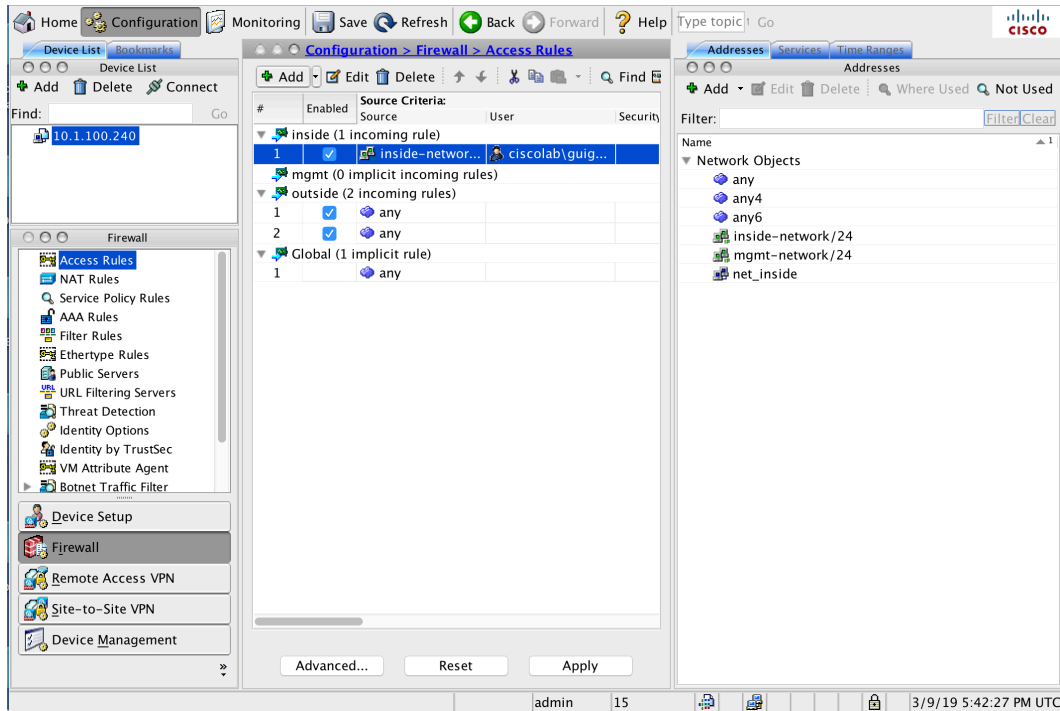
Logging Level:

More Options

User:

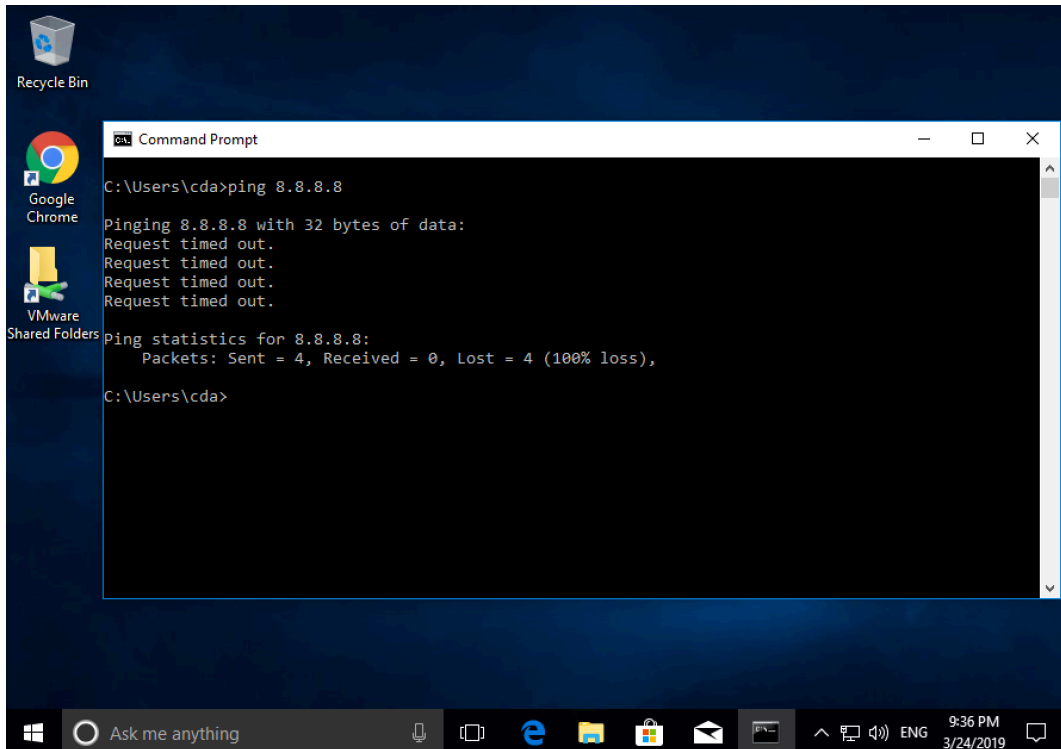


Finish and apply the rule:



The rule is an access control applied to “inside” interface to allow only access to user “guigonza”. Now login with “cda” and “guigonza” users in W10 station to test the traffic and logs in ASA.

With User “cda” the firewall register “deny access”



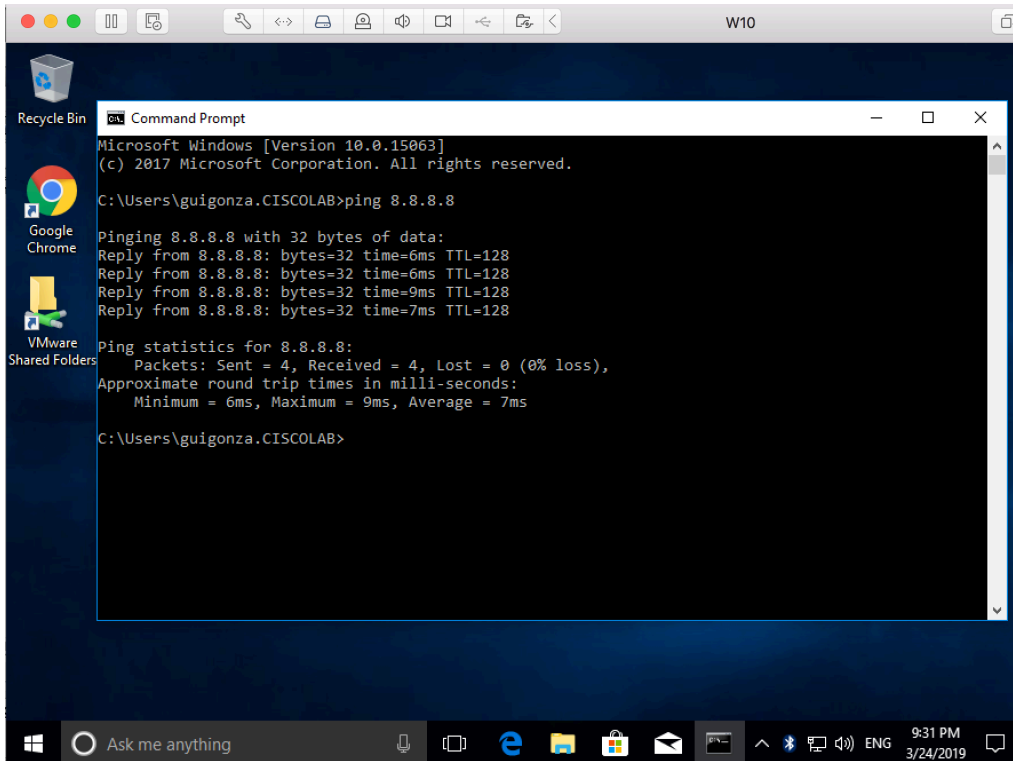
Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
6			725002	10.1.100.1	62186			Device completed SSL handshake with client mgmt:10.1.100.1/62186 to 10.1.100.240/443 for TLSv1 session
6			725003	10.1.100.1	62186			SSL client mgmt:10.1.100.1/62186 to 10.1.100.240/443 request to resume previous session
6			725001	10.1.100.1	62186			Starting SSL handshake with client mgmt:10.1.100.1/62186 to 10.1.100.240/443 for TLS session
6			302013	10.1.100.1	62186	10.1.100.240	443	Built inbound TCP connection 6062 for mgmt:10.1.100.1/62186 (10.1.100.1/62186) to identity:10.1.100.240/443
4			106023	172.16.1.101	ciscolab	8.8.8.8		Deny icmp src inside:172.16.1.101(ciscolab/cda) dst outside:8.8.8.8 (type 8, code 0) by access-group "inside_acc
4			106023	172.16.1.10	63163	8.8.8.8	53	Deny udp src inside:172.16.1.10/63163(ciscolab/Administrator) dst outside:8.8.8.8/53 by access-group "inside_e
4			106023	172.16.1.10	62431	8.8.8.8	53	Deny udp src inside:172.16.1.10/62431(ciscolab/Administrator) dst outside:8.8.8.8/53 by access-group "inside_e
6			305012	172.16.1.101	1	192.168.17...	1	Teardown dynamic ICMP translation from inside:172.16.1.101/1(ciscolab/cda) to outside:192.168.172.134/1 dura
4			106023	172.16.1.10	63031	8.8.8.8	53	Deny udp src inside:172.16.1.10/63031(ciscolab/Administrator) dst outside:8.8.8.8/53 by access-group "inside_e
4			106023	172.16.1.10	63146	192.5.6.30	53	Deny udp src inside:172.16.1.10/63146(ciscolab/Administrator) dst outside:192.5.6.30/53 by access-group "insid
4			106023	172.16.1.10	62169	8.8.8.8	53	Deny udp src inside:172.16.1.10/62169(ciscolab/Administrator) dst outside:8.8.8.8/53 by access-group "inside_e
4			106023	172.16.1.10	62751	192.5.6.30	53	Deny udp src inside:172.16.1.10/62751(ciscolab/Administrator) dst outside:192.5.6.30/53 by access-group "insid
4			106023	172.16.1.10	61732	157.56.110...	53	Deny udp src inside:172.16.1.10/61732(ciscolab/Administrator) dst outside:157.56.110.11/53 by access-group "
4			106023	172.16.1.101	ciscolab	8.8.8.8		Deny icmp src inside:172.16.1.101(ciscolab/cda) dst outside:8.8.8.8 (type 8, code 0) by access-group "inside_acc
4			106023	172.16.1.10	62228	8.8.8.8	53	Deny udp src inside:172.16.1.10/62228(ciscolab/Administrator) dst outside:8.8.8.8/53 by access-group "inside_e
4			106023	172.16.1.10	61604	8.8.8.8	53	Deny udp src inside:172.16.1.10/61604(ciscolab/Administrator) dst outside:8.8.8.8/53 by access-group "inside_e
4			106023	172.16.1.10	61824	8.8.8.8	53	Deny udp src inside:172.16.1.10/61824(ciscolab/Administrator) dst outside:8.8.8.8/53 by access-group "inside_e

Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
4			106023	172.16.1.101	ciscolab	8.8.8.8		Deny icmp src inside:172.16.1.101(ciscolab/cda) dst outside:8.8.8.8 (type 8, code 0) by access-group "inside_acc

Explanation Recommended Action Details

Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging

Using the "guigonza" user we can see the access and logs in ASA.



Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
6			302014	10.1.100.1	62169	10.1.100.240	443	Teardown TCP connection 6061 for mgmt:10.1.100.1/62169 to identity:10.1.100.240/443 duration 0:00:00 bytes
5			111010					User 'admin', running 'N/A' from IP 10.1.100.1, executed 'access-group inside_access_in in interface inside'
5			111008					User 'admin' executed the 'access-group inside_access_in in interface inside' command.
5			111010					User 'admin', running 'N/A' from IP 10.1.100.1, executed 'access-list inside_access_in line 1 extended permit ip us
5			111008					User 'admin' executed the 'access-list inside_access_in line 1 extended permit ip user ciscolab\guigonza 172.16.
5			111007					Begin configuration: 10.1.100.1 reading from http [POST]
6			725002	10.1.100.1	62169			Device completed SSL handshake with client mgmt:10.1.100.1/62169 to 10.1.100.240/443 for TLSv1 session
6			725003	10.1.100.1	62169			SSL client mgmt:10.1.100.1/62169 to 10.1.100.240/443 request to resume previous session
6			725001	10.1.100.1	62169			Starting SSL handshake with client mgmt:10.1.100.1/62169 to 10.1.100.240/443 for TLS session
6			302013	10.1.100.1	62169	10.1.100.240	443	Built inbound TCP connection 6061 for mgmt:10.1.100.1/62169 (10.1.100.1/62169) to identity:10.1.100.240/443
6			725007	10.1.100.1	62167			SSL session with client mgmt:10.1.100.1/62167 to 10.1.100.240/443 terminated
6			106015	10.1.100.1	62167	10.1.100.240	443	Deny TCP (no connection) from 10.1.100.1/62167 to 10.1.100.240/443 flags FIN ACK on interface mgmt
6			302014	10.1.100.1	62167	10.1.100.240	443	Teardown TCP connection 6060 for mgmt:10.1.100.1/62167 to identity:10.1.100.240/443 duration 0:00:00 bytes
5			111007					Begin configuration: 10.1.100.1 reading from http [POST]
6			725002	10.1.100.1	62167			Device completed SSL handshake with client mgmt:10.1.100.1/62167 to 10.1.100.240/443 for TLSv1 session
6			725003	10.1.100.1	62167			SSL client mgmt:10.1.100.1/62167 to 10.1.100.240/443 request to resume previous session
6			725001	10.1.100.1	62167			Starting SSL handshake with client mgmt:10.1.100.1/62167 to 10.1.100.240/443 for TLS session

Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
5			111008					User 'admin' executed the 'access-list inside_access_in line 1 extended permit ip user ciscolab\guigonza 172.16.1.0 any' command.

Explanation Recommended Action Details

Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging